Guia do usuário

AWS Kit de ferramentas para Visual Studio

AWS Kit de ferramentas para Visual Studio: Guia do usuário

Table of Contents

AWS Toolkit for Visual Studio

Este é o guia do usuário do AWS Toolkit for Visual Studio. Se estiver procurando pelo kit de ferramentas da AWS para VS Code, consulte o Guia do usuário do AWS Toolkit for Visual Studio Code.

O que é o kit de ferramentas para Visual Studio

AWS Toolkit for Visual Studio É um plug-in para o Visual Studio IDE que facilita o desenvolvimento, a depuração e a implantação de aplicativos.NET que usam a Amazon Web Services. O Toolkit for Visual Studio é compatível com as versões 2019 e posteriores do Visual Studio. Para obter detalhes sobre como baixar e instalar o kit, consulte o tópico Instalação e configuração neste Guia do usuário.

> **Note**
>
> O Toolkit for Visual Studio também foi lançado para as versões 2008, 2010, 2012, 2013, 2015 e 2017 do Visual Studio. Mas não há mais suporte para essas versões. Para obter mais informações, consulte o tópico Instalação e configuração neste Guia do usuário.

O kit de ferramentas para Visual Studio contém os recursos a seguir para aprimorar a experiência de desenvolvimento.

AWS Explorador

A janela de ferramentas AWS Explorer, disponível no menu Exibir do IDE, permite que você interaja com muitos dos AWS serviços de dentro do IDE do Visual Studio. Os serviços de dados compatíveis incluem Amazon Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Notification Service (Amazon SNS), Amazon Simple Queue Service (Amazon SQS) e Amazon. CloudFront AWS O Explorer também fornece acesso ao gerenciamento do Amazon Elastic Compute Cloud (Amazon EC2) AWS Identity and Access Management , ao gerenciamento de usuários e políticas (IAM), à implantação de aplicativos e funções sem servidor e AWS Lambda à implantação de aplicativos web em e. AWS Elastic Beanstalk AWS CloudFormation

Gerenciamento de credenciais e regiões

AWS O Explorer oferece suporte a várias AWS contas (incluindo contas de usuário do IAM) e regiões e permite que você altere facilmente a visualização exibida de uma conta para outra ou visualize e gerencie recursos e serviços em diferentes regiões.

Amazon EC2

No AWS Explorer, você pode visualizar as Amazon Machine Images (AMIs) disponíveis, criar instâncias do Amazon EC2 a partir dessas AMIs e, em seguida, conectar-se a essas instâncias usando o Windows Remote Desktop. AWS O Explorer também permite funcionalidades de suporte, como a capacidade de criar e gerenciar pares de chaves e grupos de segurança.

AWS Lambda

Você pode usar o Lambda para hospedar as funções C# do .NET Core e aplicações sem servidor. Use esquemas para criar rapidamente novos projetos de servidores e obter vantagem no desenvolvimento do aplicativo de servidores.

AWS CodeCommit

CodeCommit é integrado ao Visual Studio Team Explorer. Isso facilita a clonagem e a criação de repositórios mantidos e o trabalho com alterações no CodeCommit código-fonte de dentro do IDE.

Amazon DynamoDB

O DynamoDB é um serviço de banco de dados não relacional rápido, altamente escalável, altamente disponível e econômico. O kit de ferramentas para Visual Studio oferece a funcionalidade para trabalhar com o Amazon DynamoDB em um contexto de desenvolvimento. Com o kit de ferramentas para Visual Studio, você pode criar e editar atributos em tabelas do DynamoDB e executar operações de verificação em tabelas.

Amazon S3

Você pode carregar conteúdo de maneira rápida e fácil em buckets do Amazon S3 arrastando e soltando ou baixar conteúdo do Amazon S3. Você também pode definir permissões, metadados e tags de maneira prática em objetos nos buckets.

Amazon RDS

AWS O Explorer pode ajudá-lo a criar e gerenciar ativos do Amazon RDS no Visual Studio. As instâncias do Amazon RDS que usam o Microsoft SQL Server também podem ser adicionadas ao Server Explorer do Visual Studio.

AWS Elastic Beanstalk

É possível usar o Elastic Beanstalk para implantar projetos de aplicação web do .NET na AWS. Você pode implantar o aplicativo em um ambiente de instância única ou em um ambiente com balanceamento de carga total, escalado automaticamente dentro do IDE. Você também pode implantar novas versões do aplicativo rápida e praticamente sem deixar o Visual Studio. Se a aplicação usar o SQL Server no Amazon RDS, o assistente de implantação também poderá configurar a conectividade entre o ambiente de aplicações no Elastic Beanstalk e a instância do banco de dados no Amazon RDS. O kit de ferramentas para Visual Studio também inclui a ferramenta de linha de comando autônoma de implantação. Use a ferramenta de implantação para facilitar a implantação de uma parte automática do processo de compilação ou para incluir a implantação em outros cenários de script fora do Visual Studio.

AWS CloudFormation

Você pode usar o Toolkit for Visual Studio para AWS CloudFormation editar modelos no formato JSON com suporte para IntelliSense editor e realce de sintaxe. Com um AWS CloudFormation modelo, você descreve os recursos que deseja instanciar para hospedar seu aplicativo. De dentro do IDE, você implanta o modelo em AWS CloudFormation. Os recursos descritos no modelo são provisionados para você, liberando você para se concentrar no desenvolvimento da funcionalidade do aplicativo.

AWS Identity and Access Management (IAM)

No AWS Explorer, você pode criar usuários, funções e políticas do IAM e anexar políticas aos usuários.

Informações relacionadas

Para abrir um problema ou ver os problemas atualmente abertos, visite https://github.com/aws/ aws-toolkit-visual-studio /issues.

Para saber mais sobre o Visual Studio, visite https://visualstudio.microsoft.com/vs/.

Amazon Q e Amazon CodeWhisperer

O que é Amazon Q

Em 30 de abril de 2024, a Amazon agora CodeWhisperer faz parte do Amazon Q Developer, o que inclui sugestões de código embutidas e verificações de segurança.

Para saber mais sobre como trabalhar com o Amazon Q Developer no AWS Toolkit for Visual Studio, consulte o tópico Amazon Q Developer em IDEs no Amazon Q Developer User Guide. Para obter informações detalhadas sobre planos e preços do Amazon Q, consulte o guia Preços do Amazon Q.

Baixar o kit de ferramentas para Visual Studio

Você pode baixar, instalar e configurar o kit de ferramentas para Visual Studio por meio do Visual Studio Marketplace no IDE. Para obter instruções detalhadas, consulte a seção Instalar o kit de ferramentas da AWS para Visual Studio no tópico Conceitos básicos deste guia do usuário.

Baixar o kit de ferramentas usando o Visual Studio Marketplace

Baixe os arquivos de instalação do kit de ferramentas para Visual Studio acessando o site de downloads do kit da AWS para Visual Studio em seu navegador.

Kits de ferramentas de IDE adicionais da AWS

Além do Toolkit for Visual StudioAWS, também oferece kits de ferramentas IDE para VS Code e. JetBrains

Links da AWS Toolkit for Visual Studio Code

- Siga este link para baixar o AWS Toolkit for Visual Studio Code no VS Code Marketplace.
- Para saber mais sobre o AWS Toolkit for Visual Studio Code, consulte o Guia do usuário do AWS Toolkit for Visual Studio Code.

Links da AWS Toolkit for JetBrains

- Siga este link para fazer o download AWS Toolkit for JetBrains do JetBrains Marketplace.
- Para saber mais sobre o AWS Toolkit for JetBrains, consulte o Guia do usuário do AWS Toolkit for JetBrains.

Conceitos básicos

O AWS Toolkit for Visual Studio faz possibilita que seus serviços e recursos da AWS fiquem disponíveis diretamente no ambiente de desenvolvimento integrado (IDE) do Visual Studio.

Para ajudar você a começar, os tópicos a seguir descrevem como instalar, definir e configurar o AWS Toolkit for Visual Studio.

Tópicos

Instalando e configurando o AWS Toolkit for Visual Studio

Os tópicos a seguir descrevem como baixar, instalar, configurar e desinstalar o AWS Toolkit for Visual Studio.

Tópicos

Pré-requisitos

Veja a seguir os pré-requisitos para configurar versões compatíveis do AWS Toolkit for Visual Studio.

- Visual Studio 19 ou uma versão posterior
- Windows 10 ou uma versão posterior do Windows
- Acesso de administrador ao Windows e ao Visual Studio
- Credenciais ativas AWS do IAM

> **Note**
>
> Versões não suportadas do AWS Toolkit for Visual Studio estão disponíveis para o Visual Studio 2008, 2010, 2012, 2013, 2015 e 2017. Para baixar uma versão não compatível, acesse a página inicial do AWS Toolkit for Visual Studio e escolha a versão desejada na lista de links de download.
> Para saber mais sobre as credenciais do IAM ou se inscrever em uma conta, acesse o gateway do Console da AWS.

Instalando o AWS Toolkit for Visual Studio

Para instalar o AWS Toolkit for Visual Studio, encontre sua versão do Visual Studio nos procedimentos a seguir e conclua as etapas necessárias. Os links para download de todas as versões do AWS Toolkit for Visual Studio podem ser encontrados na página de AWS Toolkit for Visual Studiodestino.

> **Note**
>
> Se você encontrar problemas ao instalar o AWS Toolkit for Visual Studio, consulte o tópico Solução de problemas de instalação neste guia.

Instalando o AWS Toolkit for Visual Studio para o Visual Studio 2022

Para instalar o AWS Toolkit for Visual Studio 2022 a partir do Visual Studio, conclua as seguintes etapas:

1. No Menu principal, navegue até Extensões e escolha Gerenciar extensões.
2. Na caixa de pesquisa, pesquise AWS.
3. Escolha o botão Baixar referente à versão relevante do Visual Studio 2022 e siga as instruções de instalação.

   > **Note**
   >
   > Talvez seja necessário fechar e reiniciar manualmente o Visual Studio para concluir o processo de instalação.

4. Quando o download e a instalação estiverem concluídos, você poderá abrir o AWS Toolkit for Visual Studio escolhendo AWS Explorer no menu Exibir.

Instalando o AWS Toolkit for Visual Studio para o Visual Studio 2019

Para instalar o AWS Toolkit for Visual Studio 2019 a partir do Visual Studio, conclua as seguintes etapas:

1. No Menu principal, navegue até Extensões e escolha Gerenciar extensões.
2. Na caixa de pesquisa, pesquise AWS.
3. Escolha o botão Baixar referente ao Visual Studio 2017 e 2019 e siga as instruções.

> **Note**
>
> Talvez seja necessário fechar e reiniciar manualmente o Visual Studio para concluir o processo de instalação.

4. Quando o download e a instalação estiverem concluídos, você poderá abrir o AWS Toolkit for Visual Studio escolhendo AWS Explorer no menu Exibir.

Desinstalando o AWS Toolkit for Visual Studio

Para desinstalar o AWS Toolkit for Visual Studio, encontre sua versão do Visual Studio nos procedimentos a seguir e conclua as etapas necessárias.

Desinstalando o AWS Toolkit for Visual Studio para Visual Studio 2022

Para desinstalar AWS Toolkit for Visual Studio 2022 do Visual Studio, conclua as seguintes etapas:

1. No Menu principal, navegue até Extensões e escolha Gerenciar extensões.
2. No menu de navegação Gerenciar extensões, expanda o título Instalado.
3. Localize a extensão AWS Toolkit for Visual Studio 2022 e escolha o botão Desinstalar.

> **Note**
>
> Se o AWS Toolkit for Visual Studio não estiver visível na seção Instalado do menu de navegação, talvez seja necessário reiniciar o Visual Studio.

4. Siga os prompts na tela para concluir o processo de desinstalação.

Desinstalando o AWS Toolkit for Visual Studio para Visual Studio 2019

Para desinstalar o AWS Toolkit for Visual Studio 2019 do Visual Studio, conclua as seguintes etapas:

1. No Menu principal, navegue até Ferramentas e escolha Gerenciar extensões.
2. No menu de navegação Gerenciar extensões, expanda o título Instalado.
3. Localize a extensão AWS Toolkit for Visual Studio 2019 e escolha o botão Desinstalar.
4. Siga os prompts na tela para concluir o processo de desinstalação.

Desinstalando o AWS Toolkit for Visual Studio para Visual Studio 2017

Para desinstalar AWS Toolkit for Visual Studio 2017 no Visual Studio, conclua as seguintes etapas:

1. No Menu principal, navegue até Ferramentas e escolha Extensões e atualizações.
2. No menu de navegação Gerenciar extensões, expanda o título Instalado.
3. Localize a extensão AWS Toolkit for Visual Studio 2017 e escolha o botão Desinstalar.
4. Siga os prompts na tela para concluir o processo de desinstalação.

Desinstalando o AWS Toolkit for Visual Studio para Visual Studio 2013 ou 2015

Para desinstalar AWS Toolkit for Visual Studio 2013 ou 2015, conclua as seguintes etapas:

1. No Painel de Controle do Windows, abra Programas e Recursos.

   > **Note**
   >
   > Você pode abrir Programas e Recursos imediatamente executando `appwiz.cpl` em de um prompt de comando do Windows ou na caixa de diálogo Executar do Windows.

2. Na lista de programas instalados, abra o menu de contexto (clique com o botão direito) de Ferramentas da AWS para Windows.
3. Escolha Desinstalar e siga as instruções para concluir o processo de desinstalação.

> **Note**
>
> Seu diretório Amostras não é excluído durante o processo de desinstalação. Esse diretório é preservado caso você tenha modificado as amostras. Esse diretório deve ser removido manualmente.

Conectando-se a AWS

A maioria dos serviços e recursos da Amazon Web Services (AWS) são gerenciados por meio de uma AWS conta. Não é necessária uma AWS conta para usar o AWS Toolkit for Visual Studio, no entanto, as funções do Toolkit são limitadas sem uma conexão.

Se você já configurou uma AWS conta e autenticação por meio de outro AWS serviço (como o AWS Command Line Interface), o Toolkit for Visual Studio detectará automaticamente suas credenciais.

Pré-requisitos

Se você é novo AWS ou não criou uma conta, há três etapas principais para conectar o Toolkit for Visual Studio à AWS sua conta:

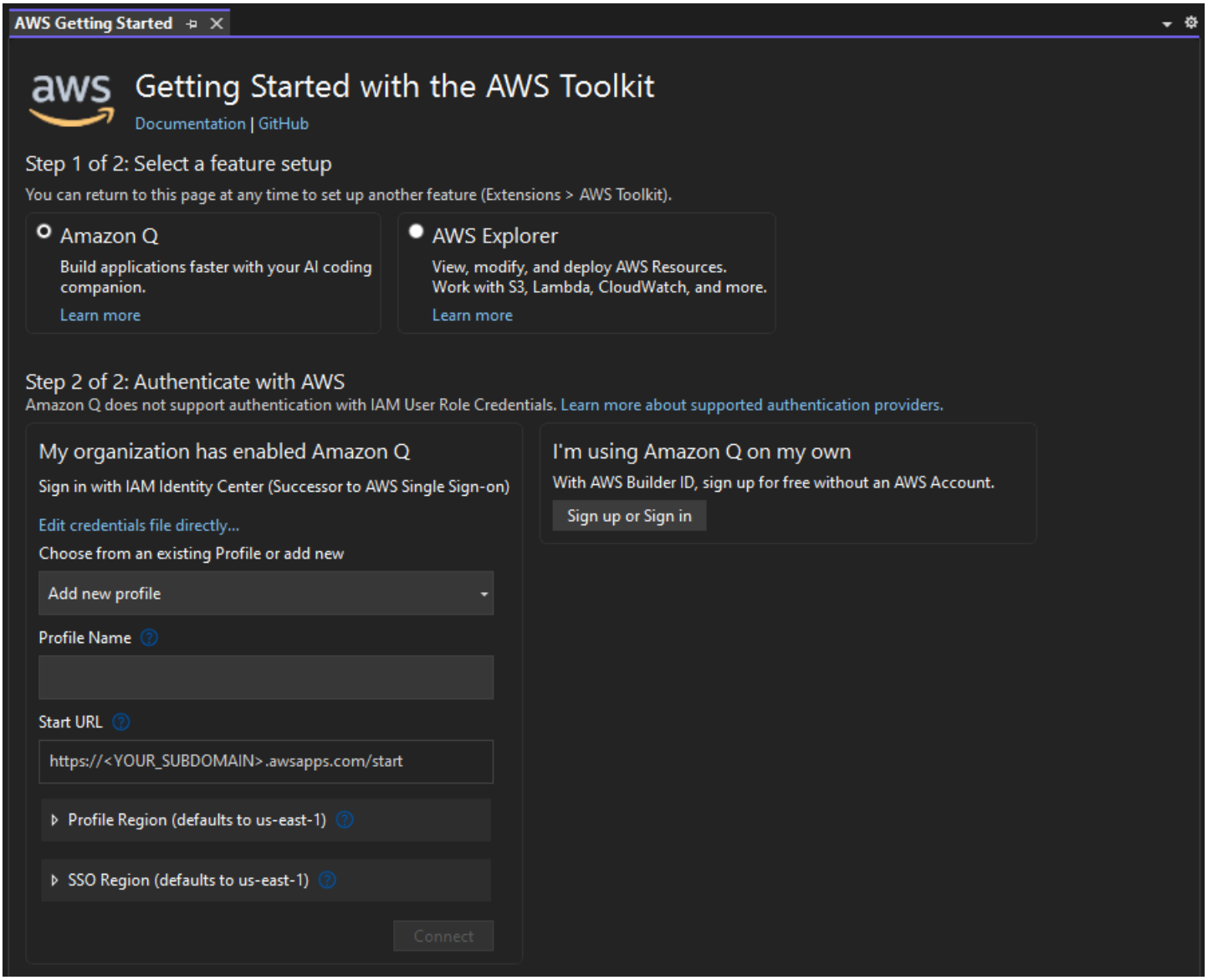
1. Inscrevendo-se AWS em uma conta: Você pode se inscrever AWS em uma conta no portal de AWS inscrição. Para obter informações detalhadas sobre como configurar uma nova AWS conta, consulte o tópico Visão geral no Guia do usuário de AWS configuração.
2. Configurando a autenticação: há três métodos principais para se autenticar com sua AWS conta no Toolkit for Visual Studio. Para saber mais sobre cada um desses métodos, consulte o tópico Autenticação e acesso neste guia do usuário.
3. Autenticação com o Kit AWS de Ferramentas: Você pode se conectar à sua AWS conta a partir do Kit de Ferramentas concluindo os procedimentos nas seções a seguir deste Guia do Usuário.

Conectando-se a AWS partir do kit de ferramentas

Para se conectar às suas AWS contas a partir do Toolkit for Visual Studio, abra o Guia de introdução à interface do usuário AWS do kit de ferramentas (interface de usuário de conexão) concluindo o procedimento a seguir.

1. No menu principal do Visual Studio, expanda Extensões e, em seguida, expanda o AWS Toolkit.

2. Nas opções do menu AWS Kit de ferramentas, escolha Introdução.
3. A interface de usuário de conexão do AWS kit de ferramentas é aberta no Visual Studio.



A tabela a seguir descreve quais métodos de autenticação são compatíveis com cada recurso. Para saber mais sobre cada um dos três métodos de autenticação AWS IAM Identity Center, AWS Identity and Access Management credenciais e AWS Builder ID, consulte o índice de autenticação e acesso neste Guia do usuário.

> **Note**
>
> No momento, ao trabalhar com CodeCatalyst o Toolkit for Visual Studio, você só precisa autorizar com AWS sua ID do Builder ao clonar um repositório de terceiros.

Amazon Q Developer	AWS Explorador	Amazon CodeCatalyst
☑ ID do AWS construtor	☒ ID do AWS construtor	☑ ID do AWS construtor
☑ Centro de Identidade do IAM	☑ Centro de Identidade do IAM	☒ Centro de identidade do IAM
☒ Credenciais AWS do IAM	☑ Credenciais AWS do IAM	☒ Credenciais AWS do IAM

Autenticação para Amazon Q Developer

Para começar a usar o Amazon Q Developer, autentique e conecte-se com suas credenciais AWS IAM Identity Center ou com suas credenciais de ID do AWS Builder.

Os procedimentos a seguir descrevem como autenticar e conectar o kit de ferramentas com sua conta da AWS .

Fazer a autenticação e conectar-se com o Centro de Identidade do IAM

1. Na interface de usuário de conexão do AWS kit de ferramentas, selecione o radial do Amazon Q Developer para expandir as opções de autenticação do Amazon Q Developer.

   > **Note**
   >
   > Se não houver credenciais armazenadas, vá para a Etapa 3 para adicionar ou atualizar suas credenciais do IAM Identity Center.

2. Na seção Minha organização habilitou o Amazon Q Developer, expanda a opção Escolher de um perfil existente ou adicione um novo menu suspenso para escolher entre sua lista de credenciais armazenadas.
3. No menu suspenso Tipo de perfil, escolha AWS IAM Identity Center

4. No campo de texto Nome do perfil, insira o perfil **`Profile Name`** do IAM Identity Center com o qual você deseja se autenticar.
5. No campo de texto URL inicial, insira o **`Start URL`** que está anexado às suas credenciais do IAM Identity Center.
6. No menu suspenso Região do perfil (o padrão é us-east-1), escolha a região do perfil definida pelo perfil de usuário do IAM Identity Center com o qual você está se autenticando.
7. No menu suspenso Região do SSO (o padrão é us-east-1), escolha a região do SSO definida pelas credenciais do IAM Identity Center e, em seguida, escolha o botão Conectar para abrir a caixa de diálogo Fazer login com o IAM Identity Center. AWS
8. Na caixa de diálogo Fazer login com o AWS IAM Identity Center, escolha o botão Prosseguir para o navegador para abrir o site de solicitação de AWS autorização em seu navegador padrão.
9. Confirme se o código de segurança em seu IDE corresponde ao código de confirmação de solicitação de AWS autorização exibido em seu navegador da web e escolha o botão Enviar e continuar para continuar.
10. Siga as instruções em seu navegador da Web padrão, você será notificado quando o processo de autorização for concluído, é seguro fechar o navegador e retornar ao Visual Studio.

Autentique e conecte-se com um AWS Builder ID

1. Na interface de usuário de conexão do AWS kit de ferramentas, selecione o radial do Amazon Q Developer para expandir as opções de autenticação do Amazon Q Developer.
2. Na seção Estou usando o Amazon Q Developer por conta própria, escolha o botão Inscrever-se ou Entrar para abrir a caixa de diálogo Fazer login com ID do AWS construtor.
3. Escolha o botão Prosseguir para o navegador para abrir o site AWS de solicitação de autorização em seu navegador padrão.
4. Confirme se o código de segurança em seu IDE corresponde ao código de confirmação de solicitação de AWS autorização exibido em seu navegador da web e escolha o botão Enviar e continuar para continuar.
5. Siga as instruções em seu navegador da Web padrão, você será notificado quando o processo de autorização for concluído, é seguro fechar o navegador e retornar ao Visual Studio.

Autenticação para o AWS Explorer

Para começar a trabalhar com o AWS Explorer a partir do Toolkit, autentique-se e conecte-se com suas credenciais do IAM Identity Center ou do IAM.

Os procedimentos a seguir descrevem como autenticar e conectar o kit de ferramentas com sua conta da AWS .

Fazer a autenticação e conectar-se com o Centro de Identidade do IAM

1. Na interface de usuário de conexão do AWS kit de ferramentas, selecione o radial do AWS Explorer para expandir as opções de autenticação do Amazon Q Developer.
2. No menu suspenso **`Profile Type`**, escolha AWS IAM Identity Center.
3. No campo de texto Nome do perfil, insira o **`Profile Name`** perfil do IAM Identity Center que você deseja usar.
4. No campo de texto URL inicial, insira o **`Start URL`** que está anexado às suas credenciais do IAM Identity Center.
5. No menu suspenso Região do perfil (o padrão é us-east-1), escolha a região do perfil definida pelo perfil de usuário do IAM Identity Center com o qual você está se autenticando.
6. No menu suspenso Região de SSO (o padrão é us-east-1), escolha a região de SSO definida pelas credenciais do IAM Identity Center.
7. Escolha o botão Prosseguir para o navegador para abrir o site AWS Autorizar solicitação em seu navegador padrão.
8. Confirme se o código de segurança em seu IDE corresponde ao código de confirmação de solicitação de AWS autorização exibido em seu navegador da web e escolha o botão Enviar e continuar para continuar.
9. Siga as instruções em seu navegador da Web padrão, você será notificado quando o processo de autorização for concluído, é seguro fechar o navegador e retornar ao Visual Studio.

Faze a autenticação e conectar-se com as credenciais do IAM

1. Na interface de usuário de conexão do AWS kit de ferramentas, selecione o radial do AWS Explorer para expandir as opções de autenticação do Amazon Q Developer.
2. No menu **`Profile Type`** suspenso, escolha Função de usuário do IAM.
3. No campo de texto Nome do perfil, insira o **`Profile Name`** perfil com o qual você deseja se autenticar.

4. No campo de texto ID da chave de acesso, insira o **`Access Key ID`** do perfil com o qual você deseja se autenticar.
5. No campo de texto Chave secreta, insira o **`Secret Key`** do perfil com o qual você deseja se autenticar.
6. No menu suspenso Local de armazenamento (o padrão é Arquivo de Credenciais Compartilhado), especifique se você deseja armazenar suas credenciais com um arquivo de Credenciais Compartilhadas ou com o.NET Encrypted Stored.
7. No menu suspenso Região do perfil (o padrão é us-east-1), escolha a Região do perfil que está anexada ao perfil com o qual você deseja se autenticar.

Solução de problemas de instalação do AWS Toolkit for Visual Studio

Sabe-se que as informações a seguir resolvem problemas comuns de instalação durante a instalação doAWS Toolkit for Visual Studio.

Se você encontrar um erro ao instalar o AWS Toolkit for Visual Studio ou não estiver claro se a instalação foi concluída ou não, revise as informações em cada uma das seções a seguir.

Permissões de administrador para o Visual Studio

A AWS Toolkit for Visual Studio extensão exige permissões de administrador para garantir que todos os AWS serviços e recursos estejam acessíveis.

Se você tiver permissões de administrador local, é possível que suas permissões de administrador não se estendam diretamente à sua instância do Visual Studio.

Para iniciar o Visual Studio com permissões de administrador localmente:

1. No Windows, localize o inicializador de aplicativos do Visual Studio (ícone).
2. Abra o menu de contexto (clique com o botão direito do mouse) no ícone do Visual Studio para abrir o menu de contexto.
3. Selecione Executar como administrador no menu de contexto.

Para iniciar o Visual Studio com permissões de administrador remotamente:

1. No Windows, localize o inicializador de aplicativos do aplicativo que você está usando para se conectar à sua instância remota do Visual Studio.
2. Abra o menu de contexto (clique com o botão direito do mouse) no aplicativo para abrir o menu de contexto.
3. Selecione Executar como administrador no menu de contexto.

> **Note**
>
> Se você estiver iniciando o programa localmente ou se conectando remotamente, o Windows poderá solicitar que você confirme suas credenciais administrativas.

Obtenção de um registro de instalação

Se você concluiu as etapas na seção anterior de permissões do administrador localizada acima e foi confirmado que você está executando ou se conectando ao Visual Studio com permissões de administrador, a obtenção de um arquivo de log de instalação pode ajudar a diagnosticar outros problemas.

Para instalar manualmente o a AWS Toolkit for Visual Studio partir de um `.vsix` arquivo e gerar um arquivo de log de instalação, conclua as etapas a seguir.

1. Na página AWS Toolkit for Visual Studioinicial, siga o link Download e salve o `.vsix` arquivo da AWS Toolkit for Visual Studio versão que você deseja instalar.
2. No menu principal do Visual Studio, expanda o cabeçalho Ferramentas, expanda o submenu Linha de Comando e escolha Visual Studio Developer Command Prompt.
3. No prompt de comando do Visual Studio Developer, digite o `vsixinstaller` comando com o seguinte formato:

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

4. `[file path to log file]`Substitua pelo nome do arquivo e pelo caminho completo do diretório em que você deseja que o log de instalação seja criado. Um exemplo do `vsixinstaller` comando com o caminho e o nome do arquivo especificados é semelhante ao seguinte:

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

5. `[file path to Toolkit installation file]`Substitua pelo caminho completo do arquivo do diretório em que o `AWSToolkitPackage.vsix` está localizado.

   Um exemplo do `vsixinstaller` comando com o caminho completo do arquivo de instalação do Toolkit deve ser semelhante ao seguinte:

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

6. Verifique se o nome e os caminhos do arquivo estão corretos e execute o `vsixinstaller` comando.

   Um exemplo de um `vsixinstaller` comando completo é semelhante ao seguinte:

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

Instalando diferentes extensões do Visual Studio

Se você obteve um arquivo de log de instalação e ainda não consegue determinar por que o processo de instalação está falhando, verifique se consegue instalar outras extensões do Visual Studio. A instalação de diferentes extensões do Visual Studio pode fornecer informações adicionais sobre seus problemas de instalação. Caso você não consiga instalar nenhuma extensão do Visual Studio, pode ser necessário solucionar problemas com o Visual Studio, em vez deAWS Toolkit for Visual Studio.

Entrar em contato com o suporte

Se você revisou todas as seções contidas neste guia e precisa de recursos ou suporte adicionais, você pode ver edições anteriores ou abrir uma nova edição no site AWS Toolkit for Visual StudioGithub Issues.

Para ajudar a agilizar uma solução para seu problema:

- Verifique os problemas anteriores e atuais para ver se outras pessoas enfrentaram uma situação semelhante.
- Faça anotações detalhadas de cada etapa que você tomou para resolver o problema.

- Salve todos os arquivos de log obtidos com a instalação dessa AWS Toolkit for Visual Studio ou de outras extensões.
- Anexe seus arquivos AWS Toolkit for Visual Studio de log de instalação à nova edição.

Perfis e encadernação de janelas

Perfis e vinculação de janelas para o Toolkit for Visual Studio

Ao trabalhar com as ferramentas de publicação, assistentes e outros recursos do Toolkit for Visual Studio, observe o seguinte:

- A janela doAWS Explorer está vinculada a um único perfil e região por vez. O Windows foi aberto a partir doAWS Explorer padrão para esse perfil e região vinculados.
- Depois que uma nova janela for aberta, você poderá usar essa instância doAWS Explorer para mudar para um perfil ou região diferente.
- As ferramentas e recursos de publicação do Toolkit for Visual Studio são automaticamente padronizados para o perfil e a região definidos noAWS Explorer.
- Se um novo perfil ou região for especificado em uma ferramenta, assistente ou recurso de publicação: todos os recursos criados posteriormente continuarão usando as novas configurações de perfil e região.
- Se você tiver várias instâncias do Visual Studio abertas, cada instância poderá ser vinculada a um perfil e região diferentes.
- OAWS Explorer salva o último perfil e a região que foram especificados e a última instância do Visual Studio fechada terá seus valores persistidos.

Autenticação e acesso

Você não precisa se autenticar para começar AWS a trabalhar com o AWS Toolkit for Visual Studio. No entanto, a maioria dos AWS recursos é gerenciada por meio de uma AWS conta. Para acessar todos os serviços e recursos do AWS Toolkit for Visual Studio, você precisará de pelo menos dois tipos de autenticação de conta:

1. Ou AWS Identity and Access Management (IAM) ou AWS IAM Identity Centerautenticação para suas AWS contas. A maioria dos AWS serviços e recursos é gerenciada por meio do IAM e do IAM Identity Center.
2. Uma ID do AWS construtor é opcional para alguns outros AWS serviços.

Os tópicos a seguir contêm detalhes adicionais e instruções de configuração para cada tipo de credencial e método de autenticação.

Tópicos

AWS Credenciais do IAM Identity Center em AWS Toolkit for Visual Studio

AWS IAM Identity Center é a melhor prática recomendada para gerenciar a autenticação AWS da sua conta.

Para obter instruções detalhadas sobre como configurar o IAM Identity Center para kits de desenvolvimento de software (SDKs) e o AWS Toolkit for Visual Studio, consulte a seção de autenticação do IAM Identity Center do Guia de referência de AWS SDKs e ferramentas.

Autenticação com o IAM Identity Center a partir do AWS Toolkit for Visual Studio

Para se autenticar com o IAM Identity Center a partir do AWS Toolkit for Visual Studio adicionando um perfil do IAM Identity Center ao seu `config` arquivo `credentials` or, conclua as etapas a seguir.

1. No editor de texto de sua preferência, abra as informações de AWS credenciais armazenadas no `<hone-directory>\.aws\credentials` arquivo.
2. No `credentials file` abaixo da seção `[default]`, adicione um modelo para um perfil nomeado do Centro de Identidade do IAM. Veja o seguinte exemplo de modelo:

   > **Important**
   >
   > Não use a palavra perfil ao criar uma entrada no arquivo `credential` porque isso cria um conflito com as convenções de nomenclatura do arquivo `credential`.
   > Inclua o prefixo `profile_` somente ao configurar um perfil nomeado no arquivo `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`**: o URL que aponta para o portal de usuário do Centro de Identidade do IAM de sua organização.
- **`sso_region`**: a AWS região que contém o host do portal do IAM Identity Center. Isso pode ser diferente da AWS região especificada posteriormente no `region` parâmetro padrão.
- **`sso_account_id`**: o ID da AWS conta que contém a função do IAM com a permissão que você deseja conceder a esse usuário do IAM Identity Center.
- **`sso_role_name`**: o nome do perfil do IAM que define as permissões do usuário ao usar esse perfil para obter credenciais por meio do Centro de Identidade do IAM.

- **`region`**: a AWS região padrão na qual esse usuário do IAM Identity Center faz login.

> **Note**
>
> Você também pode adicionar um perfil habilitado para o IAM Identity Center ao seu AWS CLI executando o `aws configure sso` comando. Depois de executar esse comando, você fornece valores para a URL inicial do IAM Identity Center (`sso_start_url`) e a AWS Região (`region`) que hospeda o diretório do IAM Identity Center.
> Para obter mais informações, consulte Configurando a AWS CLI para AWS usar o Single Sign-On no Guia do usuário.AWS Command Line Interface

Fazer login com o Centro de Identidade do IAM

Ao fazer login com um perfil do Centro de Identidade do IAM, o navegador padrão é iniciado de acordo com o `sso_start_url` especificado no `credential file`. Você deve verificar seu login do IAM Identity Center antes de poder acessar seus AWS recursos em AWS Toolkit for Visual Studio. Se suas credenciais expirarem, você precisará repetir o processo de conexão para obter novas credenciais temporárias.

AWS Credenciais do IAM

AWS As credenciais do IAM são autenticadas com sua AWS conta por meio de chaves de acesso armazenadas localmente.

As seções a seguir descrevem como configurar as credenciais do IAM para se autenticar com sua AWS conta a partir do. AWS Toolkit for Visual Studio

> **Important**
>
> Antes de configurar as credenciais do IAM para autenticação com sua AWS conta, observe que:
>
> - Se você já definiu as credenciais do IAM por meio AWS de outro serviço (como o AWS AWS CLI), o AWS Toolkit for Visual Studio detectará automaticamente essas credenciais.
> - AWS recomenda o uso da AWS IAM Identity Center autenticação. Para obter mais informações sobre as melhores práticas AWS do IAM, consulte a seção Práticas

recomendadas de segurança no IAM do Guia do usuário do AWS Identity and Access Management.

- Para evitar riscos de segurança, não use usuários do IAM para autenticação ao desenvolver software com propósito específico ou trabalhar com dados reais. Em vez disso, use a federação com um provedor de identidade, como AWS IAM Identity Center. Para obter mais informações, consulte O que é o IAM Identity Center? no Guia do usuário do AWS IAM Identity Center .

Criar um usuário do IAM.

Antes de configurar a autenticação com sua AWS conta, você precisa concluir AWS Toolkit for Visual Studio a Etapa 1: Criar seu usuário do IAM e a Etapa 2: Obter suas chaves de acesso no tópico Autenticar usando credenciais de longo prazo no Guia de referência de AWS SDKs e ferramentas.

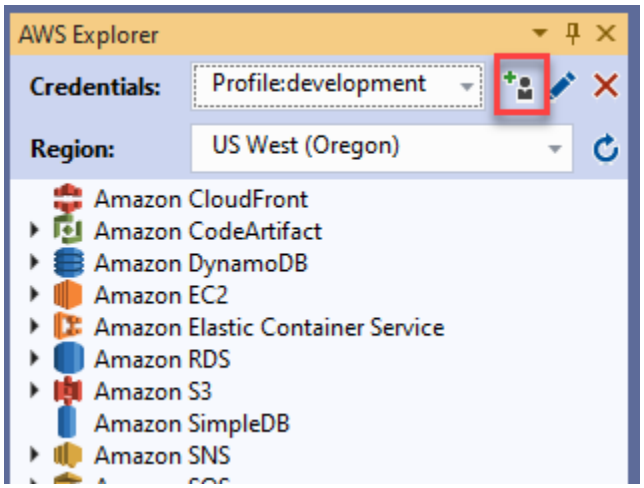
> **Note**
>
> A Etapa 3: atualizar o arquivo credentials compartilhado é opcional.
> Se você concluir a Etapa 3, o AWS Toolkit for Visual Studio detectará automaticamente suas credenciais do. `credentials file`
> Se você não concluiu a Etapa 3, ela o AWS Toolkit for Visual Studio guiará pelo processo de criação de um `credentials file` conforme descrito na AWS Toolkit for Visual Studio seção Criação de um arquivo de credenciais, localizada abaixo.

Criar um arquivo de credenciais

Para adicionar um usuário ou criar um `credentials file` pelo AWS Toolkit for Visual Studio:

> **Note**
>
> Quando um novo perfil de usuário é adicionado por meio do kit de ferramentas:
>
> - Se um `credentials file` já existir, as novas informações do usuário serão adicionadas ao arquivo existente.
> - Se um `credentials file` não existir, um arquivo será criado.

1. No AWS Explorer, escolha o ícone Novo perfil de conta para abrir a caixa de diálogo Novo perfil de conta.



2. Preencha os campos obrigatórios na caixa de diálogo Novo perfil da conta e escolha o botão OK para criar o usuário do IAM.

Editar credenciais de usuário do IAM pelo kit de ferramentas

Para editar credenciais do usuário do IAM pelo kit de ferramentas, conclua as seguintes etapas:

1. No menu suspenso Credenciais no AWS Explorer, escolha a credencial de usuário do IAM que você deseja editar.
2. Escolha o ícone Editar perfil para abrir a caixa de diálogo Editar perfil.
3. Na caixa de diálogo Editar perfil, conclua suas atualizações e escolha o botão OK para salvá-las.

Para excluir credenciais do usuário do IAM pelo kit de ferramentas, conclua as seguintes etapas:

1. No menu suspenso Credenciais no AWS Explorer, escolha a credencial de usuário do IAM que você deseja excluir.
2. Escolha o ícone Excluir perfil para abrir o prompt Excluir perfil.
3. Confirme que você deseja excluir o perfil para removê-lo do `Credentials file`.

> **Important**
>
> Perfis que comportam recursos de acesso avançados, como o Centro de Identidade do IAM ou a autenticação multifator (MFA) na caixa de diálogo Editar perfil, não podem ser editados

no AWS Toolkit for Visual Studio. Para fazer alterações nesses tipos de perfil, você deve editar o `credentials file` usando um editor de texto.

Editar credenciais de usuário do IAM usando um editor de texto

Além de gerenciar usuários do IAM com o AWS Toolkit for Visual Studio, você pode editar usando seu editor `credential files` de texto preferido. A localização padrão do `credential file` no Windows é `C:\Users\`*`USERNAME`*`\.aws\credentials`.

Para obter mais detalhes sobre a localização e a estrutura de `credential files`, consulte a seção Arquivos de configuração e credenciais compartilhados do Guia de referência de SDKs e ferramentas da AWS .

Criação de usuários do IAM a partir do AWS Command Line Interface (AWS CLI)

Essa AWS CLI é outra ferramenta que você pode usar para criar um usuário do IAM no`credentials file`, usando o comando`aws configure`.

Para obter informações detalhadas sobre a criação de usuários do IAM a partir do, AWS CLI consulte Configuração dos AWS CLI tópicos no Guia do AWS CLI usuário.

O kit de ferramentas para Visual Studio comporta as seguintes propriedades de configuração:

```
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 do construtor

AWS O Builder ID é um método de AWS autenticação adicional que pode ser necessário para usar determinados serviços ou recursos, como clonar um repositório de terceiros na Amazon. CodeCatalyst

Para obter informações detalhadas sobre o método de autenticação do AWS Builder ID, consulte o tópico Entrar com o AWS Builder ID no Guia do usuário AWS de login.

Para obter informações adicionais sobre a clonagem de um repositório a CodeCatalyst partir de AWS Toolkit for Visual Studio, consulte o CodeCatalyst tópico Trabalhando com a Amazon neste Guia do usuário.

Autenticação multifator (MFA) no kit de ferramentas para Visual Studio

A autenticação multifator (MFA) é uma segurança adicional para AWS suas contas. O MFA exige que os usuários forneçam credenciais de login e autenticação exclusiva de um mecanismo de AWS MFA compatível ao acessar sites ou serviços. AWS

AWS suporta uma variedade de dispositivos virtuais e de hardware para autenticação de MFA. Veja a seguir um exemplo de um dispositivo MFA virtual habilitado por meio de um aplicativo para smartphone. Para obter mais informações sobre opções de dispositivo MFA, consulte Uso de autenticação multifator (MFA) na AWS no Guia do usuário do IAM.

Etapa 1: criar um perfil do IAM para delegar acesso aos usuários do IAM

O procedimento a seguir descreve como configurar a delegação de perfis para atribuir permissões a um usuário do IAM. Para obter informações detalhadas sobre a delegação de perfis, consulte Criação de uma função para delegar permissões a um usuário do IAM no Guia do usuário do AWS Identity and Access Management .

1. Acesse o console do IAM: https://console.aws.amazon.com/iam.
2. Na barra de navegação, escolha Perfis e selecione Criar perfil.
3. Na página Criar perfil, escolha Outra conta da AWS .
4. Insira o ID da conta necessário e marque a caixa de seleção Exigir MFA.

> **Note**
>
> Para encontrar o número da sua conta (ID) de 12 dígitos, acesse a barra de navegação no console e escolha Suporte, Centro de suporte.

5. Selecione Next: Permissions (Próximo: permissões).
6. Anexe políticas existentes ao perfil ou crie uma política para ele. As políticas que você escolhe nesta página determinam quais AWS serviços o usuário do IAM pode acessar com o Toolkit.
7. Depois de anexar as políticas, escolha Próximo: Tags para ter a opção de adicionar tags do IAM ao perfil. Depois escolha Próximo: Revisão para continuar.
8. Na página Revisão, insira o nome do perfil necessário (toolkit-role, por exemplo). Você também tem a opção de adicionar uma descrição do perfil.
9. Selecione Criar função.
10. Quando a mensagem de confirmação for exibida (“O perfil do kit de ferramentas foi criado”, por exemplo), escolha o nome do perfil na mensagem.
11. Na página Resumo, escolha o ícone de cópia para copiar o ARN do perfil e colá-lo em um arquivo. (Você precisa desse ARN ao configurar o usuário do IAM para assumir o perfil.)

Etapa 2: criar um usuário do IAM que assume as permissões do perfil

Esta etapa cria um usuário do IAM sem permissões para que uma política em linha possa ser adicionada.

1. Acesse o console do IAM: https://console.aws.amazon.com/iam.
2. Escolha Usuários na barra de navegação e selecione Adicionar usuário.
3. Na página Adicionar usuário, insira o nome do usuário necessário (toolkit-user, por exemplo) e marque a caixa de seleção Acesso programático.
4. Escolha Próximo: Permissões, Próximo: Tags e Próximo: Revisão para percorrer as próximas páginas. Você não está adicionando permissões neste estágio porque o usuário assumirá as permissões do perfil.
5. Na página Revisão, você recebe a notificação Este usuário não tem permissões. Selecione Criar usuário.

6. Na página Êxito, selecione Baixar .csv para baixar o arquivo contendo o ID da chave de acesso e a chave de acesso secreta. (Você precisa de ambos ao definir o perfil do usuário no arquivo de credenciais.)
7. Escolha Fechar.

Etapa 3: adicionar uma política para permitir que o usuário do IAM assuma o perfil

O procedimento a seguir cria uma política em linha que permite que o usuário assuma o perfil (e as respectivas permissões).

1. Na página Usuários do console do IAM, escolha o usuário do IAM que você acabou de criar (toolkit-user, por exemplo).
2. Na guia Permissões, na página Permissões, escolha Adicionar política em linha.
3. Na página Criar política, selecione Escolher um serviço, insira STS em Encontrar um serviço e escolha STS nos resultados.
4. Para Ações, comece a inserir o termo AssumeRole. Marque a AssumeRolecaixa de seleção quando ela aparecer.
5. Na seção Recurso, verifique se a opção Específico está selecionada e clique em Adicionar ARN para restringir o acesso.
6. Na caixa de diálogo Adicionar ARNs, para Especificar ARN para o perfil, adicione o ARN do perfil que você criou na Etapa 1.

   Depois de adicionar o ARN do perfil, a conta confiável e o nome do perfil associados a esse perfil são exibidos em Conta e Nome do perfil com caminho.
7. Escolha Adicionar.
8. De volta à página Criar política, escolha Especificar condições de solicitação (opcional), marque a caixa de seleção MFA necessária e selecione Fechar para confirmar.
9. Escolha Review policy (Revisar política)
10. Na página Revisar política, insira um Nome para a política e escolha Criar política.

    A guia Permissões exibe a nova política em linha anexada diretamente ao usuário do IAM.

Etapa 4: gerenciar um dispositivo MFA virtual para o usuário do IAM

1. Baixe e instale um aplicativo MFA virtual no smartphone.

   Para obter uma lista de aplicativos compatíveis, consulte a página de recursos Autenticação multifator.
2. No console do IAM, escolha Usuários na barra de navegação e selecione o usuário que está assumindo um perfil (toolkit-user, nesse caso).
3. Na página Resumo, escolha a guia Credenciais de segurança e, em Dispositivo MFA atribuído, escolha Gerenciar.
4. No assistente Gerenciar dispositivo MFA, escolha Dispositivo MFA virtual e selecione Continuar.
5. No painel Configurar dispositivo MFA virtual, escolha Mostrar código QR e digitalize o código usando o aplicativo MFA virtual que você instalou no smartphone.
6. Depois de digitalizar o código QR, o aplicativo MFA virtual gera códigos de MFA únicos. Insira dois códigos de MFA consecutivos em Código MFA 1 e Código MFA 2.
7. Escolha Assign MFA.
8. De volta à guia Credenciais de segurança do usuário, copie o ARN do novo Dispositivo MFA atribuído.

   O ARN inclui o ID da sua conta de 12 dígitos e o formato é semelhante ao seguinte: `arn:aws:iam::123456789012:mfa/toolkit-user`. Esse ARN será necessário ao definir o perfil de MFA na próxima etapa.

Etapa 5: criar perfis para permitir a MFA

O procedimento a seguir cria os perfis que permitem o MFA ao acessar AWS serviços do Toolkit for Visual Studio.

Os perfis que você cria incluem três informações que você copiou e armazenou nas etapas anteriores:

- Chaves de acesso (ID de chave de acesso e chave de acesso secreta) para o usuário do IAM
- ARN do perfil que está delegando permissões ao usuário do IAM
- ARN do dispositivo MFA virtual atribuído ao usuário do IAM

No arquivo de credencial AWS compartilhado ou no SDK Store que contém suas AWS credenciais, adicione as seguintes 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
```

Há dois perfis definidos no exemplo fornecido:

- O perfil `[toolkit-user]` inclui a chave de acesso e a chave de acesso secreta que foram geradas e salvas quando você criou o usuário do IAM na Etapa 2.
- O perfil `[mfa]` define como a autenticação multifator é aceita. Existem três entradas:

  ◦ `source_profile`: especifica o perfil cujas credenciais são usadas para assumir o perfil especificado por essa configuração `role_arn` nesse perfil. Neste caso, é o perfil `toolkit-user`.

  ◦ `role_arn`: especifica o nome do recurso da Amazon (ARN) do perfil do IAM que você deseja usar para realizar as operações solicitadas usando esse perfil. Neste caso, é o ARN do perfil que você criou na Etapa 1.

  ◦ `mfa_serial`: especifica a identificação ou o número de série do dispositivo MFA que o usuário deve usar ao assumir um perfil. Neste caso, é o ARN do dispositivo virtual que você configurou na Etapa 3.

Configurar credenciais externas

Se você tiver um método para gerar ou pesquisar credenciais que não seja aceito diretamente AWS, poderá adicionar ao arquivo compartilhado de credenciais um perfil que contenha a configuração `credential_process`. Essa configuração especifica um comando externo que é executado para gerar ou recuperar credenciais de autenticação a serem usadas. Por exemplo, você pode incluir uma entrada semelhante à seguinte no arquivo `config`:

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

Para obter mais informações sobre o uso de credenciais externas e os riscos de segurança associados, consulte Credenciais de origem com um processo externo no Guia do usuário da AWS Command Line Interface .

Trabalhando com AWS serviços

Os tópicos a seguir descrevem como começar a trabalhar com AWS serviços do AWS Toolkit for Visual Studio.

Tópicos

Amazon CodeCatalyst para o AWS kit de ferramentas para Visual Studio

O que é o Amazon CodeCatalyst?

A Amazon CodeCatalyst é um espaço de colaboração baseado em nuvem para equipes de desenvolvimento de software. Usando o AWS Toolkit for Visual Studio, você pode visualizar e

gerenciar CodeCatalyst recursos diretamente do AWS Toolkit for Visual Studio. Para obter mais informações sobre issoCodeCatalyst, consulte o Guia CodeCatalyst do usuário da Amazon.

Os tópicos a seguir descrevem como conectar o AWS kit de ferramentas do Visual Studio CodeCatalyst e como trabalhar com ele CodeCatalyst por meio do AWS kit de ferramentas do Visual Studio.

Tópicos

Introdução à Amazon CodeCatalyst e ao AWS kit de ferramentas do Visual Studio

Para começar a trabalhar com a Amazon a CodeCatalyst partir do AWS Toolkit for Visual Studio, preencha o seguinte.

Tópicos

Instalando o AWS kit de ferramentas para Visual Studio

Antes de integrar o AWS Toolkit for Visual Studio às suas CodeCatalyst contas, verifique se você está usando uma versão atual do AWS Toolkit for Visual Studio. Para obter detalhes sobre como instalar e configurar a versão mais recente do AWS Toolkit para Visual Studio, consulte a seção Configurando o AWS kit de ferramentas para o Visual Studio deste Guia do usuário.

Criação de uma CodeCatalyst conta e AWS Builder ID

Além de instalar a versão mais recente do AWS Toolkit para Visual Studio, você deve ter uma ID e uma CodeCatalyst conta do AWS Builder ativas para se conectar ao AWS Toolkit for Visual Studio. Se você não tiver uma CodeCatalyst conta ou ID ativa do AWS Builder, consulte a CodeCatalyst seção Configuração com no Guia do CodeCatalystusuário.

> **Note**
>
> Uma ID AWS do Builder é diferente de suas AWS credenciais. Para obter instruções sobre como se inscrever e se autenticar com uma ID do AWS Builder, consulte o tópico Autenticação e acesso: ID do AWS Builder neste Guia do usuário.
> Para obter informações detalhadas sobre IDs AWS de construtor, consulte o tópico AWSBuilder ID no Guia do usuário de referência AWS geral.

Conectando o AWS kit de ferramentas para Visual Studio com CodeCatalyst

Para conectar o AWS Toolkit for Visual Studio à sua CodeCatalyst conta, conclua as etapas a seguir.

1. No item de menu Git no Visual Studio, escolha Clonar repositório... .
2. Na seção Navegar em um repositório, selecione Amazon CodeCatalyst como provedor.
3. Na seção Conexão, escolha Conectar com o AWS Builder ID para abrir o CodeCatalyst console em seu navegador preferido.
4. No seu navegador, insira sua ID do AWS Builder no campo fornecido e siga as instruções para continuar.
5. Quando solicitado, escolha Permitir para confirmar a conexão entre o AWS Toolkit for Visual Studio e sua CodeCatalyst conta. Quando o processo de conexão estiver concluído, CodeCatalyst exibirá uma confirmação indicando que é seguro fechar o navegador.

Trabalhando com CodeCatalyst recursos da Amazon a partir do AWS Toolkit for Visual Studio

As seções a seguir fornecem uma visão geral dos recursos de gerenciamento de CodeCatalyst recursos da Amazon Amazon que estão disponíveis para o AWS Toolkit for Visual Studio.

Tópicos

- Clonar um repositório

Clonar um repositório

CodeCatalysté um serviço baseado em nuvem que exige que você esteja conectado à nuvem para trabalhar em CodeCatalyst projetos. Para trabalhar em um projeto localmente, você pode clonar

CodeCatalyst repositórios em sua máquina local e sincronizar com seu CodeCatalyst projeto na próxima vez em que se conectar à nuvem.

Para clonar um repositório em sua máquina local, conclua as etapas a seguir.

1. No item de menu Git no Visual Studio, escolha Clonar repositório... .
2. Na seção Navegar em um repositório, selecione Amazon CodeCatalyst como provedor.

> **Note**
>
> Se a seção Conexão exibir uma `Not Connected` mensagem, conclua as etapas na seção Autenticação e acesso: ID do AWS construtor deste Guia do usuário antes de continuar.

3. Escolha o Espaço e o Projeto dos quais você deseja clonar um repositório.
4. Na seção Repositórios, escolha o repositório que você deseja clonar.
5. Na seção Caminho, escolha a pasta para a qual você deseja clonar seu repositório.

> **Note**
>
> Inicialmente, essa pasta deve estar vazia para que a clonagem seja bem-sucedida.

6. Selecione Clonar para começar a clonar o repositório.
7. Depois que o repositório for clonado, o Visual Studio carregará sua solução clonada

> **Note**
>
> Se o Visual Studio não abrir a solução no repositório clonado, suas opções do Visual Studio poderão ser ajustadas na configuração Carregar automaticamente a solução ao abrir um repositório Git, localizada nas Configurações globais do Git, do menu Controle de código-fonte.

Solução de problemas

A seguir estão os tópicos de solução de problemas para resolver problemas conhecidos ao trabalhar com a Amazon a CodeCatalyst partir do AWS Toolkit for Visual Studio.

Tópicos

Credenciais

Se você encontrar uma caixa de diálogo solicitando credenciais ao tentar clonar um repositório baseado em gitCodeCatalyst, seu auxiliar de AWS CodeCommit credenciais poderá estar configurado globalmente, causando interferência com. CodeCatalyst Para obter informações adicionais sobre o auxiliar de AWS CodeCommit credenciais, consulte a seção Configurar conexões HTTPS com AWS CodeCommit repositórios no Windows com o auxiliar de credenciais da AWS CLI do Guia do usuário. AWSCodeCommit

Para limitar o auxiliar de AWS CodeCommit credenciais a lidar somente com CodeCommit URLs, conclua as etapas a seguir.

1. abra o arquivo de configuração global do git em: `%userprofile%\.gitconfig`
2. Localize a seguinte seção em seu arquivo:

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

3. Altere essa seção para o seguinte:

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

4. Salve suas alterações e conclua as etapas para clonar seu repositório.

Amazônia CloudWatch Integração de logs for Visual Studio

Amazon CloudWatch Integração de logs doAWSO Toolkit for Visual Studio oferece a capacidade de monitorar, armazenar e acessar CloudWatch Registra recursos sem precisar sair do IDE. Para saber

mais sobre a configuração do CloudWatch serviço e como trabalhar com o CloudWatch Recursos de registros, escolha entre os tópicos a seguir.

Tópicos

Configurar o CloudWatch Integração de logs for Visual Studio

Antes de poder usar o Amazon CloudWatch Faça a integração dos logs com o Toolkit for Visual Studio, será necessário umAWSconta. Você pode criar um novoAWSconta daAWSFaça loginsite. A maioria dos CloudWatch Os recursos de registros que estão disponíveis no Toolkit for Visual Studio podem ser acessados comAWSCredenciais da . Se um recurso específico exigir configuração adicional, os requisitos serão incluídos nas seções relevantes doTrabalho com CloudWatch Logsguide.

Para obter informações adicionais e opções sobre como configurar CloudWatch Logs, consulte oComeçar a usarseção da Amazônia CloudWatch Guia de registros.

Trabalho com CloudWatch Log

Amazônia CloudWatch A integração de log permite monitorar, armazenar e acessar CloudWatch Logs doAWSToolkit for Visual Studio. Ter acesso a CloudWatch Os recursos de registros — sem a necessidade de sair do IDE — melhoram a eficiência simplificando o CloudWatch Registra o processo de desenvolvimento e reduz as interrupções no seu fluxo de trabalho. Os tópicos a seguir descrevem como trabalhar com os recursos e funções do CloudWatch Integração de logs.

Tópicos

CloudWatch Grupos de logs

UMA`log group`é um grupo de`log streams`que compartilham as mesmas configurações de retenção, monitoramento e controle de acesso. Não há limite para o número de streams de log que podem pertencer a um grupo de logs.

Visualização de grupos de logs

O`View Log Groups`exibe uma lista de grupos de grupos de grupos de na CloudWatchExplorador de grupos de.

Para acessar o recurso Exibir grupos de logs e abrir o CloudWatch Explorador de grupos de, conclua as etapas a seguir.

1. From theAWSExplorer, expandaAmazônia CloudWatch.
2. Faça duploGrupos de logsou abra o menu de contexto (clique com o botão direito do mouse) eExibir, para abrir oCloudWatch Explorador de grupos.

> **Note**
>
> O CloudWatch O Explorador de Grupos de Log será aberto no mesmo local da janela que o Solutions Explorer.

Filtragem de grupos

Sua conta individual pode conter milhares de grupos de log diferentes. Para simplificar sua pesquisa por grupos específicos, use o`filtering`recurso descrito abaixo.

1. From theCloudWatch Explorador de grupos, coloque o cursor na barra de pesquisa localizada na parte superior da janela.
2. Comece a digitar um prefixo relacionado aos grupos de logs que você está procurando.
3. CloudWatch Explorador de gruposO é atualizado automaticamente para mostrar resultados correspondentes aos termos de pesquisa especificados na etapa anterior.

Excluir grupos de logs

Para excluir um grupo de log, consulte o procedimento a seguir.

1. From theCloudWatch Explorador de grupos, clique com o botão direito do mouse no Grupo de para o que deseja excluir.
2. Quando solicitado, confirme que você deseja excluir o Grupo de para o.
3. Escolhendo osimexclui o grupo de logs selecionado e, em seguida, atualiza oCloudWatch Explorador de grupos.

Grupos de logs de atualização

Para atualizar a lista atual de grupos de logs exibida naCloudWatch Explorador de grupos, escolha oÍcone de atualizaçãolocalizado nabarra de ferramentas.

Copiar ARN do grupo de logs

Para copiar o ARN de um grupo de logs específico, conclua as etapas descritas abaixo.

1. From theCloudWatch Explorador de grupos, clique com o botão direito do mouse no Grupo de logs do qual deseja copiar um ARN.
2. Selecione oCopiar ARNopção do menu.
3. O ARN agora está copiado para a área de transferência local e pronto para colar.

CloudWatch Fluxos de log

Uma transmissão de log é uma sequência de eventos de log que compartilham a mesma fonte.

> **Note**
>
> Ao visualizar os streams do, esteja ciente das seguintes propriedades:
>
> - Por padrão, os fluxos de log são classificados pelo carimbo de data/hora do evento mais recente.
> - As colunas associadas a um fluxo de log podem ser classificadas em ordem crescente ou decrescente, alternando acircunflexolocalizado nos cabeçalhos das colunas.
> - As entradas filtradas só podem ser classificadas porLog Stream Name (Nome do fluxo de logs).

Exibição de Fluxos

1. From theCloudWatch Explorador de gruposclique duas vezes em um Grupo de log ou clique com o botão direito do mouse em um grupoVisualizar fluxo de logsno menu de contexto.
2. Uma nova guia será aberta na nadocumento, que contém uma lista de fluxos de log associados ao seu grupo de logs.

Filtragem de fluxos

1. From theFluxos de log, na guiadocumento, coloque o cursor na barra de pesquisa.
2. Comece a digitar um prefixo relacionado ao fluxo de log que você está procurando.
3. À medida que você digita, a exibição atual é atualizada automaticamente para filtrar seus Fluxos de Log por sua entrada.

Atualizar Fluxos

Para atualizar a lista atual de fluxos de log exibidos nadocumento, escolha oÍcone de atualização, localizado nabarra de ferramentas, próximo aobarra de pesquisa.

ARN

Para copiar o ARN de um fluxo de log específico, conclua as etapas descritas abaixo.

1. From theFluxos de log, na guiadocumento, clique com o botão direito do mouse no fluxo de para o qual deseja copiar um ARN.
2. Selecione oCopiar ARNopção do menu.
3. O ARN agora está copiado para a área de transferência local e pronto para colar.

Baixar Fluxos

OFluxo de logs de exportaçãobaixa e armazena o fluxo de log selecionado localmente, onde ele pode ser acessado por ferramentas e software personalizados para processamento adicional.

1. From theFluxos de log, na guiadocumento, clique com o botão direito do mouse no fluxo de para download.
2. SelecioneFluxo de logs de exportaçãopara abrir oExportar para um arquivo de textodiálogo.

3. Escolha o local onde você deseja armazenar o arquivo localmente e especifique um nome no campo de texto fornecido.
4. Confirme o download selecionandoOK. O status do download é exibido naCentro de status de tarefas do Visual Studio

CloudWatch Eventos de log

Os eventos do são registros da atividade registrada pelo aplicativo ou recurso que estiver sendo monitorado pelo CloudWatch.

Ações de eventos de log

Os eventos de log são exibidos como uma tabela. Por padrão, os eventos são classificados do evento mais antigo ao mais recente.

As ações a seguir estão associadas a eventos de log no Visual Studio:

- Modo de texto embrulhado: Você pode alternar o texto agrupado clicando em um evento.
- Botão de quebra de texto: localizado na`document window` **`toolbar`**, esse botão ativa e desativa a quebra de texto para todas as entradas.
- Copiar mensagens para a área de transferência: selecione as mensagens que deseja copiar, clique com o botão direito do mouse na seleção e escolhaCopiar(atalho de teclado)`Ctrl + C`).

Visualização de eventos de log

1. From thedocumento, escolha uma guia que contenha uma lista de fluxos de log.
2. Clique duas vezes em um fluxo de log ou clique com o botão direito em um fluxo de logVisualizar fluxo de logsdo menu.
3. Um novoevento de logserá aberta na guiadocumento, que contém uma tabela de eventos de log associados ao fluxo de log escolhido.

Filtragem de eventos

Há três maneiras de filtrar eventos de log: por conteúdo, intervalo de tempo ou ambos. Para filtrar seus eventos de log por conteúdo e intervalo de tempo, comece filtrando suas mensagens por conteúdo ou intervalo de tempo e, em seguida, filtre esses resultados pelo outro método.

Para filtrar seus eventos de log por conteúdo:

1. From theevento de log, na guiadocumento, coloque o cursor na barra de pesquisa, localizada na parte superior da janela.
2. Comece a digitar um termo ou frase relacionado aos eventos de log que você está pesquisando.
3. À medida que você digita, a exibição atual começa automaticamente a filtrar seus eventos de log.

> **Note**
>
> Os padrões de filtro diferenciam letras maiúsculas de minúsculas. Você pode melhorar os resultados da delimitação de termos e frases exatas com caracteres não alfanuméricos entre aspas duplas (*""*). Para obter informações mais detalhadas sobre os padrões do, consulte oSintaxe do padrão e do filtrotópico na Amazônia CloudWatch (Guia).

Para exibir eventos de log gerados durante um intervalo de tempo específico:

1. From theevento de log, na guiadocumento, escolha oÍcone de calendário, localizado nabarra de ferramentas.
2. Usando os campos fornecidos, especifique o intervalo de tempo que você deseja pesquisar.
3. Os resultados filtrados são atualizados automaticamente à medida que você especifica as restrições de data e hora.

> **Note**
>
> OLimpar filtroopção limpa todas as suas date-and-time seleções de filtro.

Eventos de atualização

Para atualizar a lista atual de eventos de log exibida naevento de log, escolha oÍcone de atualização, localizado nabarra de ferramentas.

Acesso adicional a CloudWatchLogs

Você pode acessar CloudWatch LogAWSserviços e recursos diretamente doAWSKit de ferramentas no Visual Studio.

Lambda

Para visualizar fluxos de log associados a uma função do Lambda:

> **Note**
>
> Sua função de execução do Lambda deve ter as permissões apropriadas para o CloudWatchRegistros. Para obter mais informações sobre Lambda do para o CloudWatch Logs, consulte ohttps://docs.aws.amazon.com/lambda/latest/dg/monitoring-cloudwatchlogs.html#monitoring-cloudwatchlogs-prereqs

1. From theAWSToolkit Explorer, expandaLambda.
2. clique com o botão direito do mouse na função que deseja visualizar, em seguida,Visualizar logspara abrir os fluxos de log associados nadocumento(Janela).

Para visualizar fluxos de log usando a integração com o Lambda`function view`:

1. From theAWSToolkit Explorer, expandaLambda.
2. clique com o botão direito do mouse na função que deseja visualizar, em seguida,Função Visualizarpara abrir a visualização da função nadocumento(Janela).
3. From the`function view`, (SIM) como YESLogs, os fluxos de log associados à função Lambda escolhida são exibidos.

ECS

Para exibir os recursos de log associados a um contêiner de tarefas do ECS, conclua o procedimento a seguir.

> **Note**
>
> Para que o serviço Amazon ECS envie logs para CloudWatch, cada contêiner para uma determinada tarefa do Amazon ECS deve atender à configuração necessária. Para obter informações adicionais sobre a configuração e as configurações necessárias, consulte o guiaUsar oAWSDriver de log de logs.

1. From theAWSToolkit Explorer, expandaAmazon ECS.

2. Escolha o cluster do que você deseja visualizar para abrir um novoCluster do ECS, na guiadocumento(Janela).
3. No menu de navegação, localizado no lado esquerdo doCluster do ECS, selecioneTarefaspara listar todas as tarefas associadas ao cluster.
4. From theTarefas, selecione uma tarefa e escolha aVisualizar logslink, localizado no canto inferior esquerdo.

   > **Note**
   >
   > Essa exibição lista todas as tarefas contidas no cluster, a`View Logs`O link só é visível para cada tarefa que atenda à configuração de registros necessária.
   >
   > - Se uma Tarefa estiver associada somente a um único contêiner, oVisualizar logsO link abre o fluxo de log desse contêiner.
   > - Se uma tarefa estiver associada a vários contêineres, oVisualizar logsabre o linkExibir CloudWatch Logs para tarefas do ECS, use a caixa de diálogoContêiner:menu suspenso para escolher o contêiner para o qual você deseja visualizar os registros e, em seguida, escolhaOK.

5. Uma nova guia será aberta na nadocumentojanela exibindo os fluxos de log associados à sua seleção de contêiner.

Gerenciar instâncias do Amazon EC2

AWSO Explorer apresenta visualizações detalhadas das instâncias da Amazon Machine Images (AMI — Imagens de máquina da Amazon) e do Amazon Elastic Compute Cloud (Amazon EC2). Nessas visualizações, você pode executar uma instância do Amazon EC2 em uma AMI, conectar-se a essa instância e parar ou encerrar a instância, tudo isso dentro do ambiente de desenvolvimento do Visual Studio. Você pode usar a visualização de instâncias para criar AMIs com base nas instâncias. Para obter mais informações, consulte Criar uma AMI a partir de uma instância do Amazon EC2.

As visualizações de imagens de máquina da Amazon e de instâncias do Amazon EC2

NoAWSNo Explorer, você pode exibir visualizações das AMIs e das instâncias do Amazon EC2. DentroAWSExplorer, expanda oAmazon EC2Nó.

Para exibir a visualização das AMIs, no primeiro subnó, AMIs, abra o menu de contexto (clique com o botão direito do mouse) e escolha View (Exibir).

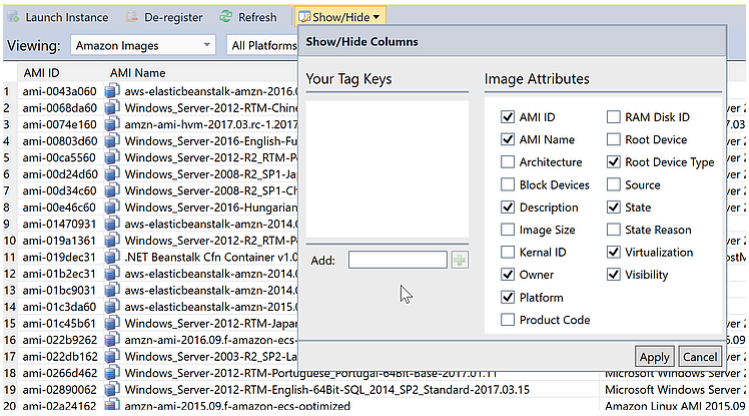
Para exibir a visualização das instâncias do Amazon EC2, no nó Instances (Instâncias), abra o menu de contexto (clique com o botão direito do mouse) e escolha View (Exibir).

Você também pode exibir a visualização clicando duas vezes no nó indicado.

- As visualizações têm escopo para a região especificada emAWSExplorador (por exemplo, Oeste dos EUA (Norte da Califórnia).
- Você pode reorganizar colunas clicando e arrastando-as. Para classificar os valores em uma coluna, clique no cabeçalho da coluna.
- Você pode usar as listas suspensas e a caixa de filtro em Viewing (Exibição) para configurar visualizações. A visualização inicial exibe AMIs de qualquer tipo de plataforma (Windows ou Linux) de propriedade da conta especificada emAWSExplorador.

Mostrar/ocultar colunas

Você também pode escolher o menu suspenso Show/Hide (Mostrar/ocultar) na parte superior da visualização para configurar quais colunas são exibidas. A escolha de colunas persistirá se você fechar a visualização e reabri-la.



Interface do usuário Show/Hide Columns (Mostrar/ocultar colunas) para visualizações de AMI e instâncias

Marcação de AMIs, instâncias e volumes

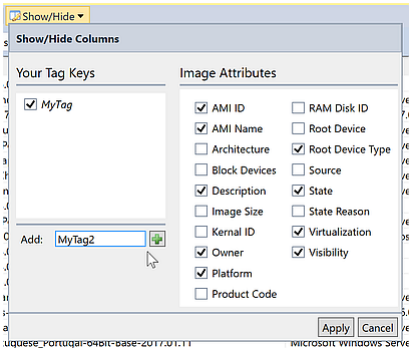
Você também pode usar oMostrar/ocultarLista suspensa para adicionar tags para AMIs, instâncias do Amazon EC2 ou volumes próprios. Tags são pares nome/valor que permitem anexar metadados a AMIs, instâncias e volumes. Os nomes de tags têm escopo para a conta e também são separados

para as AMIs e as instâncias. Por exemplo, não haveria conflito se você tivesse usado o mesmo nome de tag para as AMIs e as instâncias. Os nomes de tag não diferenciam maiúsculas de minúsculas.

Para obter mais informações sobre tags, acesseComo usar tagsnoGuia do usuário do Amazon EC2 para instâncias do Linux.

Para adicionar uma tag

1. Na caixa Add (Adicionar), digite um nome para a tag. Escolha o botão verde com o sinal de adição (+) e selecione Apply (Aplicar).



   Adicionar uma tag a uma instância da AMI ou do Amazon EC2

   A nova tag é exibida em itálico, o que indica que ainda não há valores associados a essa tag.

   Na visualização em lista, o nome da tag é exibido como uma nova coluna. Quando pelo menos um valor tiver sido associado à tag, ela estará visível noAWS Management Console.
2. Para adicionar um valor à tag, clique duas vezes em uma célula na coluna dessa tag e digite um valor. Para excluir o valor da tag, clique duas vezes na célula e exclua o texto.

   Se você limpar a tag na lista suspensa Show/Hide (Mostrar/ocultar), a coluna correspondente desaparecerá da visualização. A tag é preservada, com todos os valores de tag associados a AMIs, instâncias ou volumes.

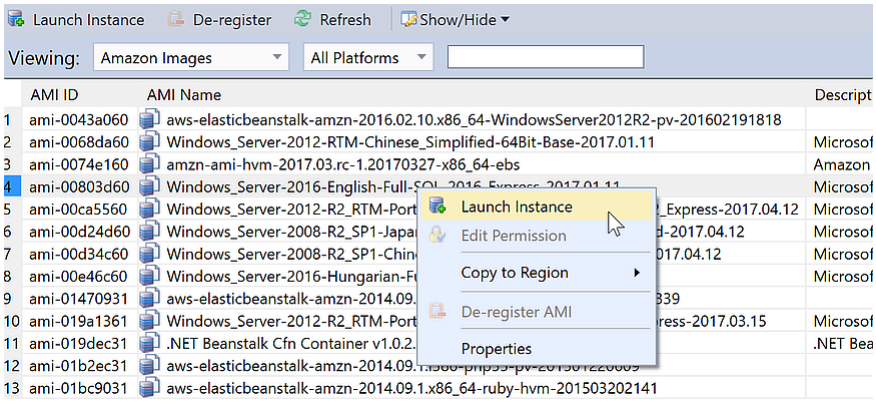
> **Note**
>
> Se você limpar uma tag naMostrar/ocultarlista suspensa que não tem valores associados, oAWSO Toolkit excluirá totalmente a tag. Ela deixará de ser exibida na visualização em lista ou na lista suspensa Show/Hide (Mostrar/ocultar). Para reutilizar essa tag, use a caixa de diálogo Show/Hide (Mostrar/ocultar) para recriá-la.

Executar uma instância do Amazon EC2

AWSO Explorer oferece toda a funcionalidade necessária para executar uma instância do Amazon EC2. Nesta seção, iremos selecionar uma Amazon Machine Image (AMI – Imagem de máquina da Amazon), configurar e iniciá-la como uma instância do Amazon EC2.

Para executar uma instância do Amazon EC2 do Windows Server

1. Na parte superior da visualização das AMIs, na lista suspensa à esquerda, escolha Amazon Images (Imagens da Amazon). Na lista suspensa à direita, escolha Windows. Na caixa de filtro, digite `ebs` para Elastic Block Storage. Pode demorar um pouco para a visualização ser atualizada.
2. Escolha uma AMI na lista, abra o menu de contexto (clique com o botão direito do mouse) e escolha Launch Instance (Executar instância).



Lista de AMIs

3. Na caixa de diálogo Launch New Amazon EC2 Instance (Executar nova instância do Amazon EC2), configure a AMI do aplicativo.

   Tipo de instância

   Escolha o tipo da instância do EC2 para iniciar. Você pode encontrar uma lista de tipos de instância e informações sobre a definição de preço na página Definição de preço do EC2.

   Name (Nome)

   Digite um nome para a instância. Esse nome não pode ser maior que 256 caracteres.

   Par de chaves

   Um par de chaves é usado para obter a senha do Windows usada por você para fazer login na instância do EC2 usando o Remote Desktop Protocol (RDP). Escolha um par de chaves para

o qual você tenha acesso à chave privada ou a opção para criar um par de chaves. Se criar o par de chaves no Toolkit, o Toolkit poderá armazenar a chave privada para você.

Os pares de chaves armazenados no Toolkit são criptografados. Você pode encontrá-los em`%LOCALAPPDATA%\AWSToolkit\keypairs`(normalmente: `C:\Users\<user>\AppData\Local\AWSToolkit\keypairs`). Você pode exportar o key pair criptografadas em um`.pem`file.

a. No Visual Studio, selecioneExibirE clique emAWSExplorer.

b. Clique em Amazon EC2 e selecione Key Pairs (Pares de chaves).

c. Os pares de chaves serão listados e aqueles criados/gerenciados pelo Toolkit serão marcados como Stored in AWSToolkit (Armazenado no AWSToolkit).

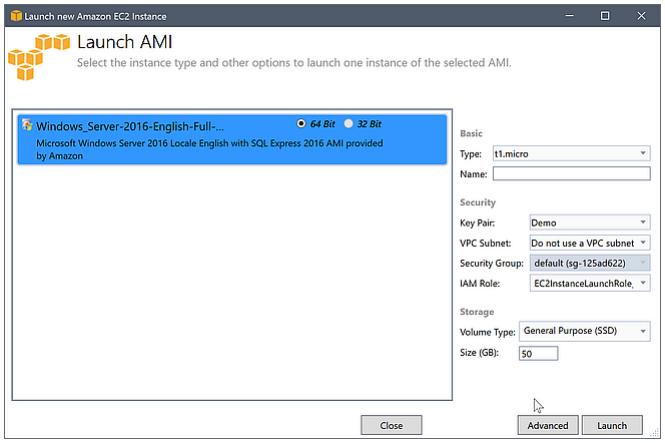
d. Clique com o botão direito do mouse no par de chaves criado e selecione Export Private Key (Exportar chave privada). A chave privada não será criptografada e armazenada no local especificado por você.

Security group

O security group controla o tipo de tráfego de rede a instância do EC2 aceitará. Escolha um security group que permitirá o tráfego recebido na porta 3389, a porta usada por RDP, de maneira que você possa se conectar à instância do EC2. Para obter informações sobre como usar o Toolkit para criar security groups, consulteGerenciamento de security groups emAWSExplorer.

Perfil da instância

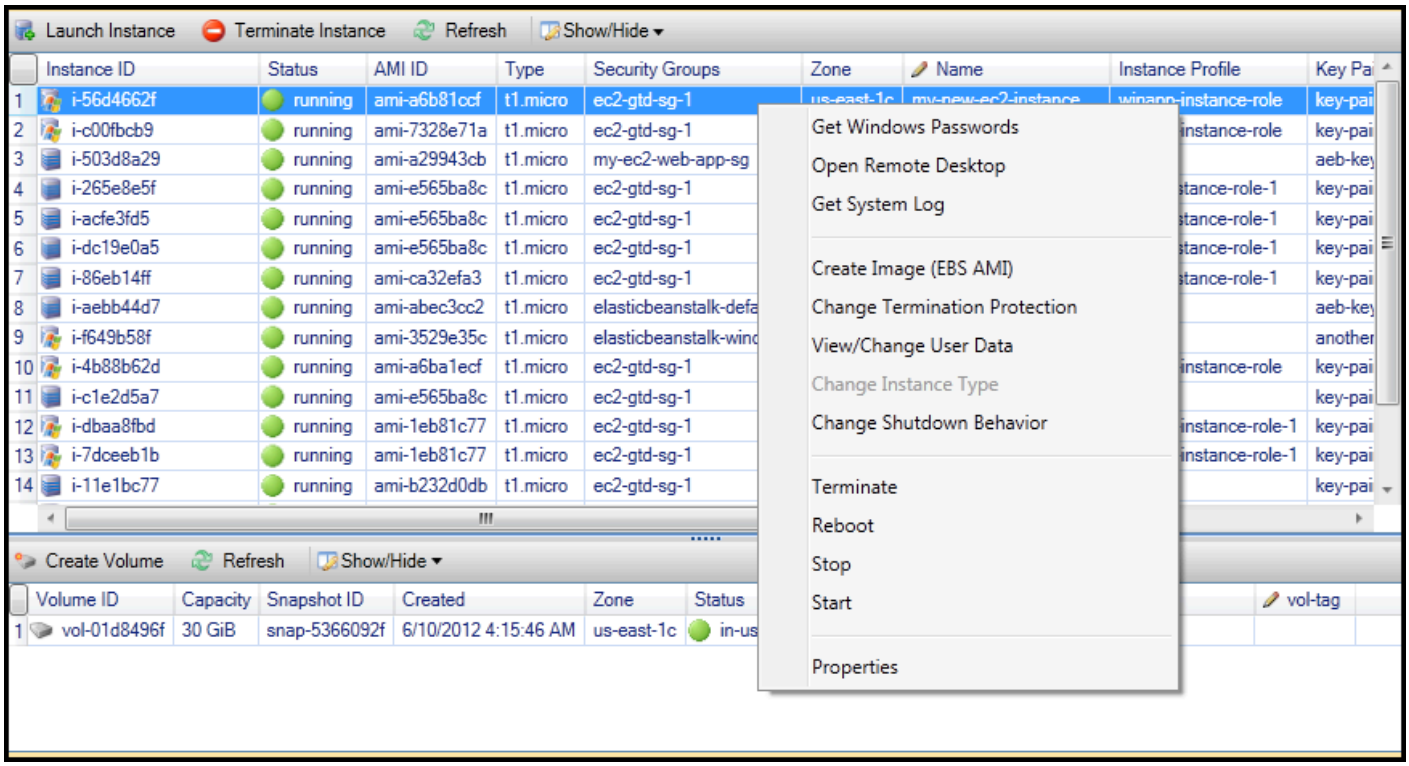
O perfil da instância é um contêiner lógico para uma função do IAM. Ao escolher um perfil da instância, você associa a função do IAM correspondente à instância do EC2. As funções do IAM são configuradas com políticas que especificam o acesso à Amazon Web Services e recursos de conta. Quando uma instância do EC2 está associada a uma função do IAM, o software aplicativo executado na instância é executado com as permissões especificadas pela função do IAM. Isso permite que o software aplicativo seja executado sem a necessidade de especificar nenhumAWSAs credenciais próprias, que torna o software mais seguro. Para obter mais informações sobre as funções do IAM, consulte o Guia do usuário do IAM.



Caixa de diálogo Launch AMI (Executar AMI) do EC2

4. Escolha Executar.

DentroAWSExplorer, noInstânciassubnó deAmazon EC2, abra o menu de contexto (clique com o botão direito do mouse) e escolhaExibir. OAWSO Toolkit exibe a lista de instâncias do Amazon EC2 associadas à conta ativa. Você talvez precise escolher Refresh (Atualizar) para ver a nova instância. Quando a instância for exibida pela primeira vez, ela poderá estar em um estado pendente, mas depois de alguns instantes, ela mudará para um estado em execução.



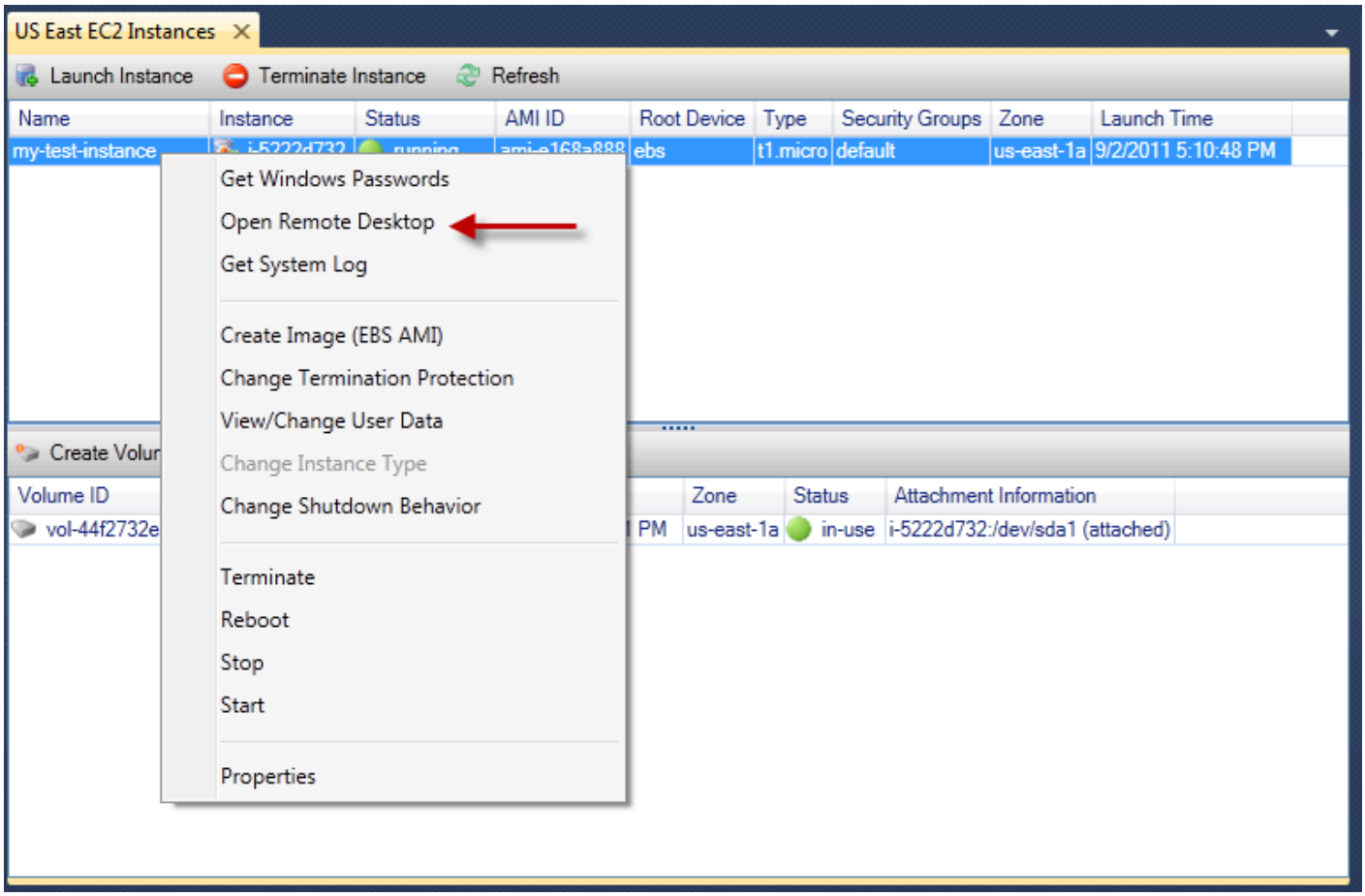
Conectar a uma instância do Amazon EC2

Você pode usar a Área de Trabalho Remota para se conectar a uma instância do Windows Server. Para autenticação, oAWSO Toolkit permite recuperar a senha de administrador da instância, ou basta usar o key pair armazenadas associado à instância. No procedimento a seguir, usaremos o par de chaves armazenadas.

Para se conectar a uma instância do Windows Server usando a Área de Trabalho Remota do Windows

1. Na lista de instâncias do EC2, clique com o botão direito do mouse na instância do Windows Server a que você deseja se conectar. No menu de contexto, escolha Open Remote Desktop (Abrir área de trabalho remota).

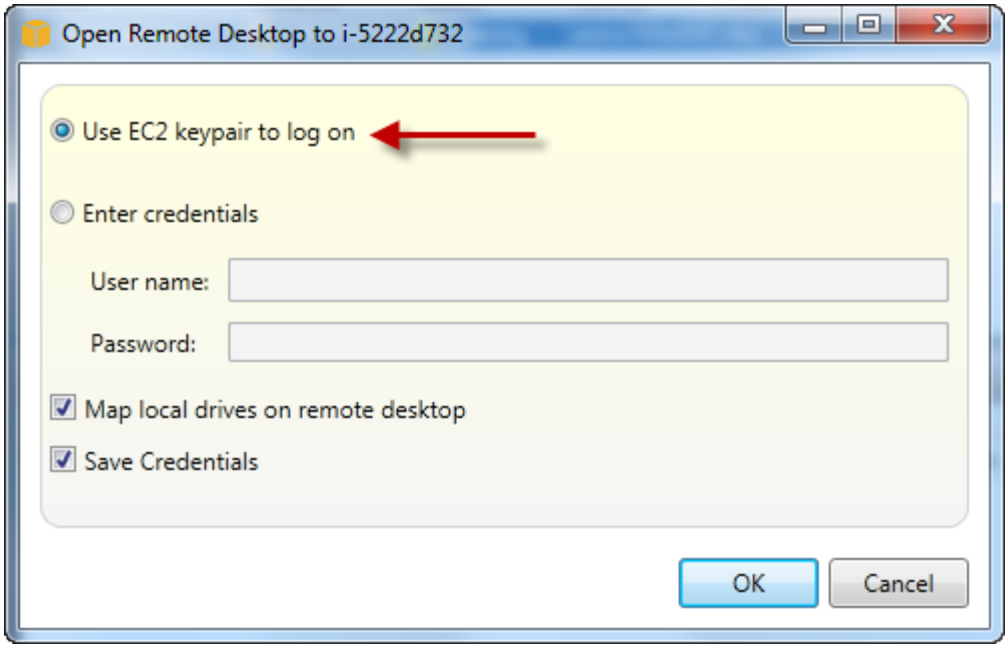
   Se quiser autenticar usando a senha de administrador, escolha Get Windows Passwords (Obter senhas do Windows).



   Menu de contexto EC2 Instance

2. Na caixa de diálogo Open Remote Desktop (Abrir área de trabalha remota), escolha Use EC2 keypair to log on (Usar par de chaves do EC2 para fazer login) e selecione OK.

   Se você não tiver armazenado um key pair com oAWSKit de ferramentas, especifique o arquivo PEM que contém a chave privada.

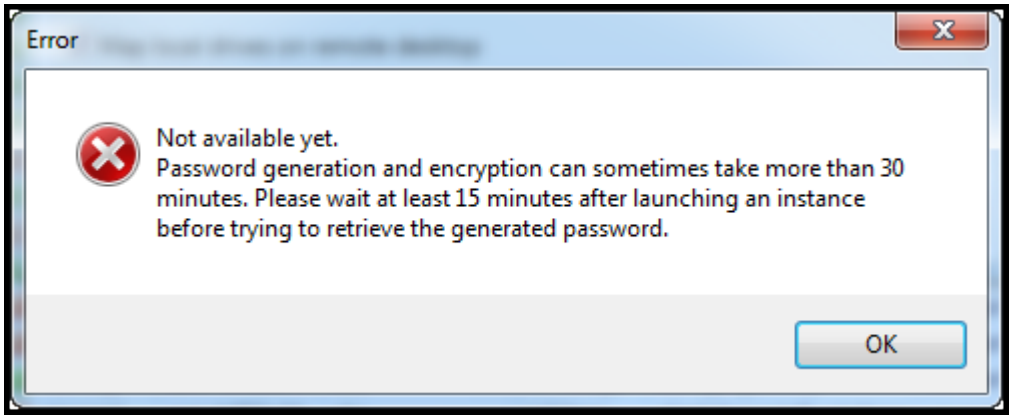


   Caixa de diálogo Open Remote Desktop (Abrir área de trabalha remota)

3. A janela Remote Desktop (Área de trabalho remota) será aberta. Você não precisa fazer login porque a autenticação ocorreu com o par de chaves. Você será o administrador na instância do Amazon EC2.

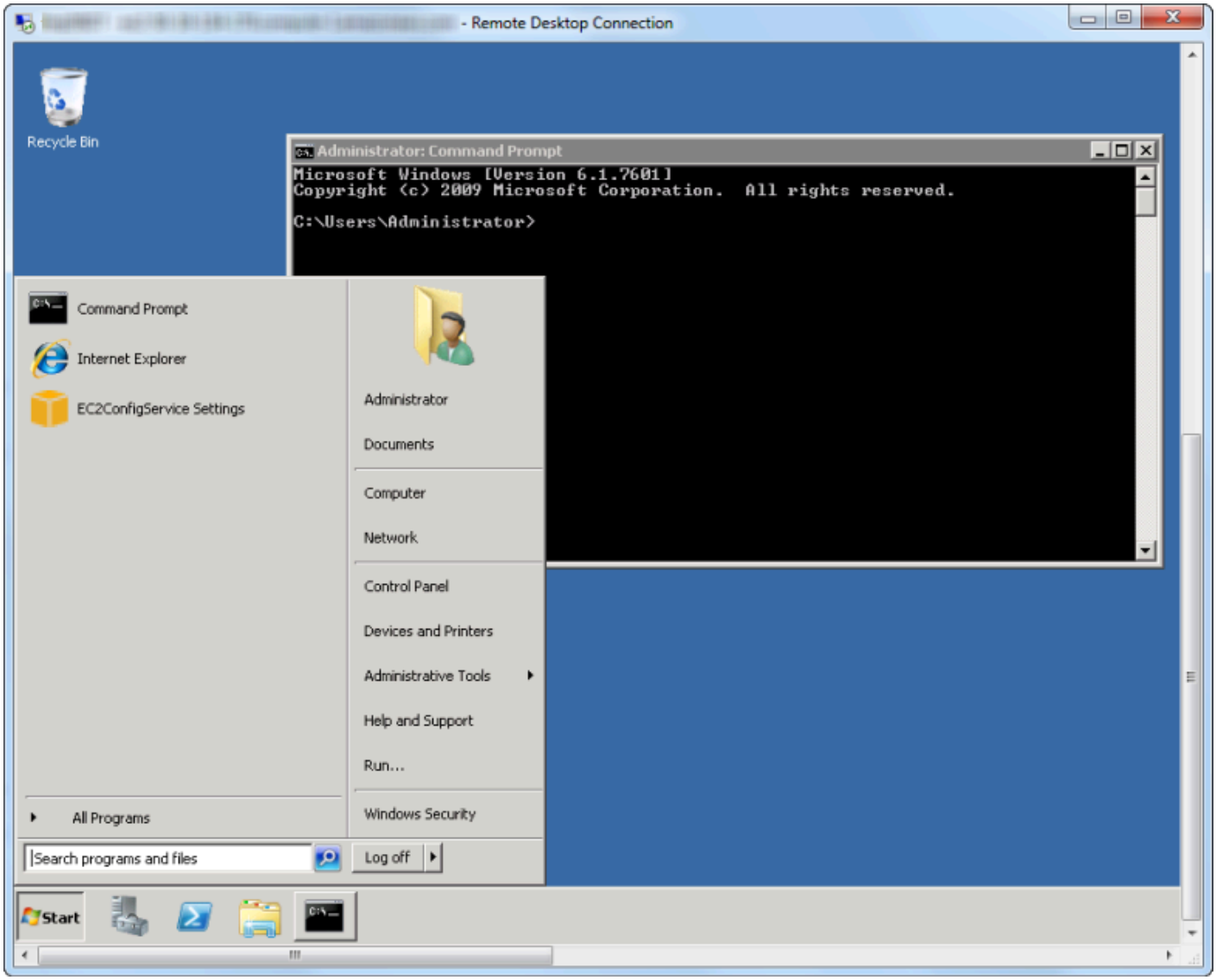
   Se a instância do EC2 tiver sido iniciada apenas recentemente, talvez você não consiga se conectar por dois motivos possíveis:

   - O serviço de Área de Trabalho Remota talvez ainda não esteja em execução. Aguarde alguns minutos e tente novamente.
   - As informações sobre a senha talvez ainda não tenham sido transferidas para a instância. Nesse caso, você verá uma caixa de mensagem semelhante à seguinte.



A senha ainda não está disponível

A captura de tela a seguir mostra um usuário conectado como administrador por meio da Área de Trabalho Remota.



Desktop Remoto

Encerrar uma instância do Amazon EC2

Usar oAWSNo Toolkit, você pode parar ou encerrar uma instância do Amazon EC2 em execução no Visual Studio. Para interromper a instância, a instância do EC2 deve estar usando um volume do Amazon EBS. Se a instância do EC2 não estiver usando um volume do Amazon EBS, sua única opção será encerrar a instância.

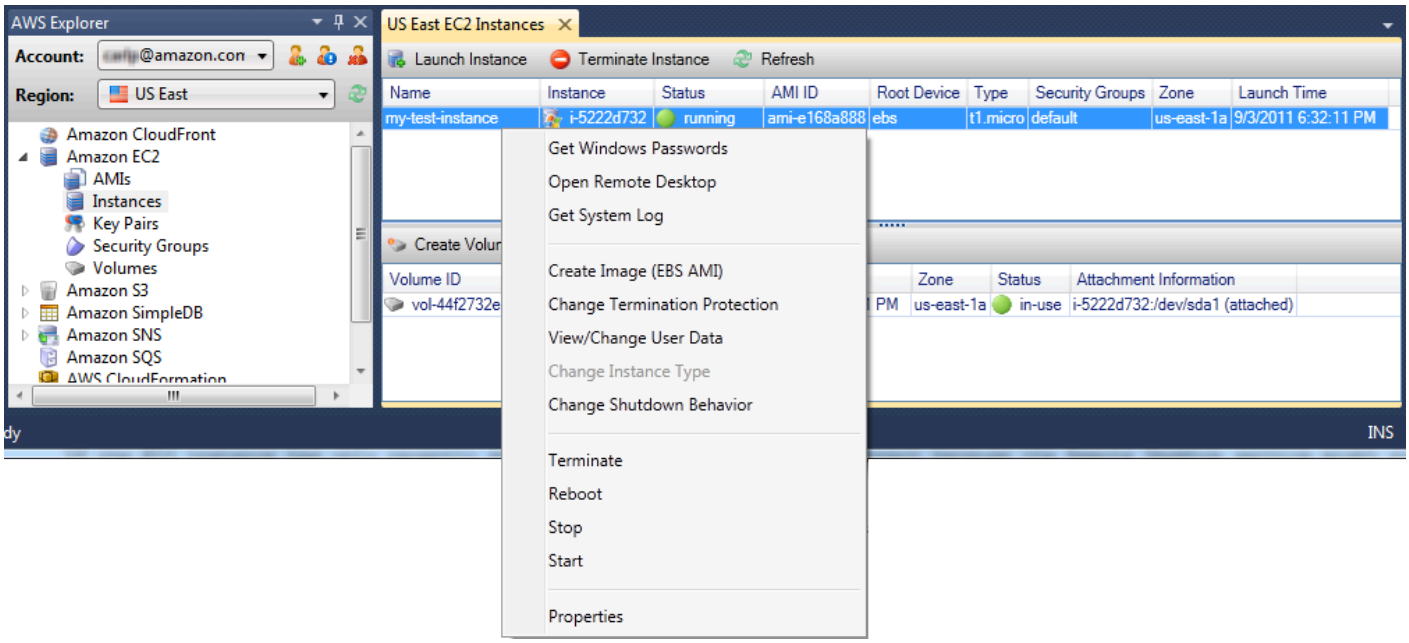
Se você parar a instância, os dados armazenados no volume do EBS serão mantidos. Se você encerrar a instância, todos os dados armazenados no dispositivo de armazenamento da instância local serão perdidos. Em ambos os casos, parar ou encerrar, você não continuará sendo cobrado

pela instância do EC2. No entanto, se parar uma instância, você continuará sendo cobrado pelo armazenamento do EBS que persistente depois que a instância for interrompida.

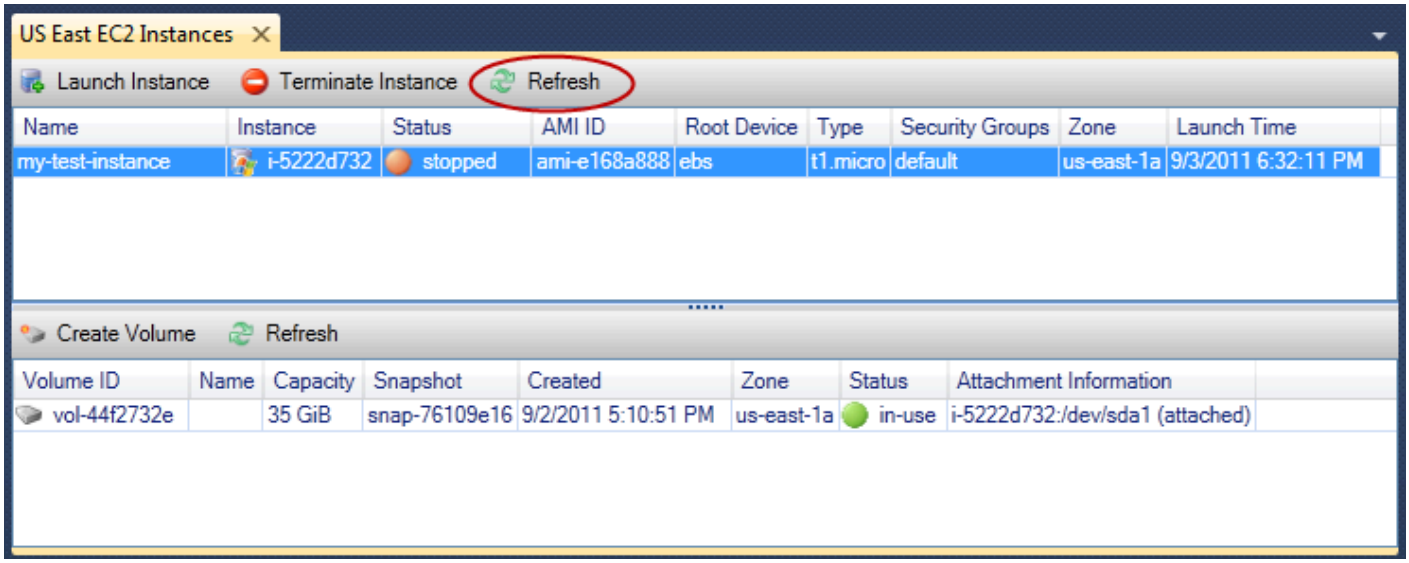
Outra maneira possível de encerrar uma instância é usar a Área de Trabalho Remota para se conectar à instância e, no menu Iniciar do Windows, usar Desligar. Você pode configurar a instância para ser interrompida ou encerrada nesse cenário.

Para interromper uma instância do Amazon EC2

1. DentroAWSExplorer, expanda oAmazon EC2Nó, abra o menu de contexto (clique com o botão direito do mouseInstânciasE, depois, escolhaExibir. Na lista Instances (Instâncias), clique com o botão direito do mouse na instância que você deseja parar e escolha Stop (Interromper) no menu de contexto. Escolha Yes (Sim) para confirmar que você deseja parar a instância.

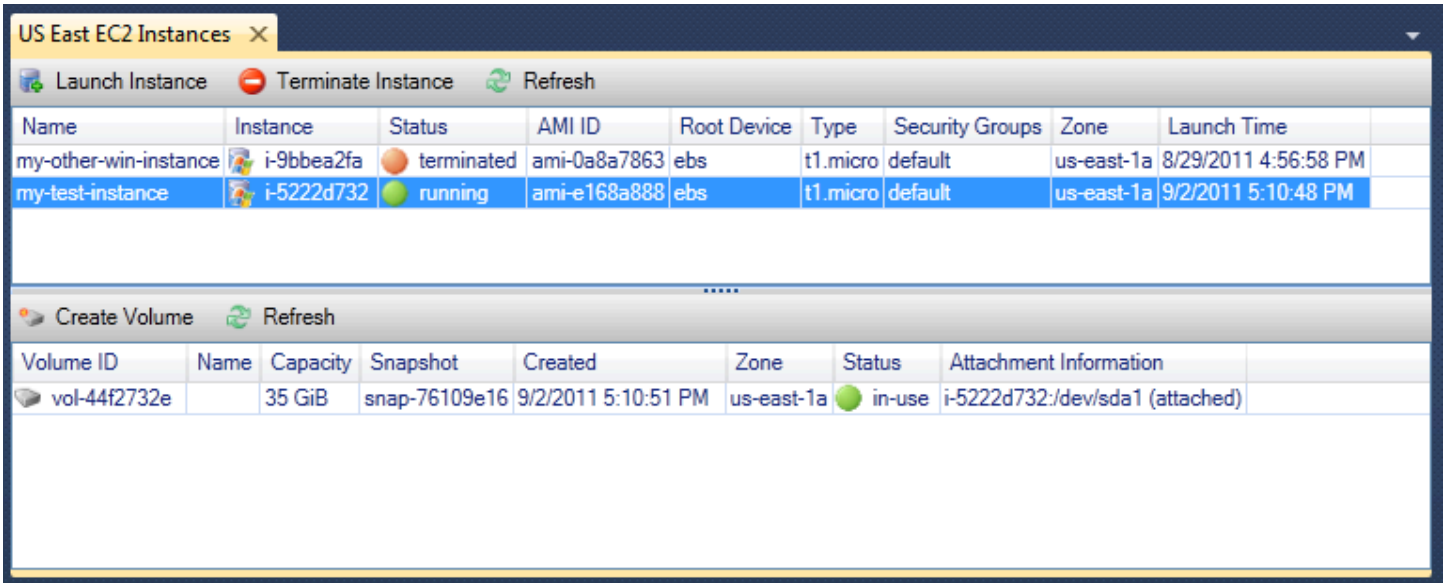


2. Na parte superior da lista Instances (Instâncias), escolha Refresh (Atualizar) para ver a alteração feita no status da instância do Amazon EC2. Como paramos, em vez de encerrar, a instância, o volume do EBS associado à instância continua ativa.



Instâncias encerradas permanecem visíveis

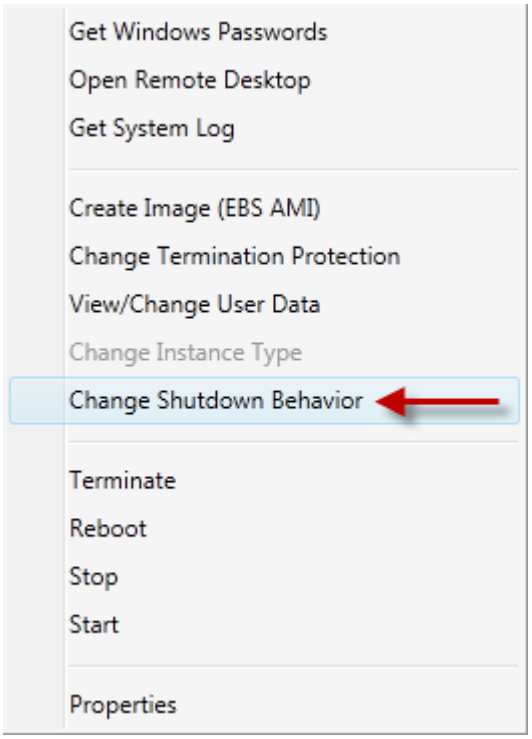
Se você encerrar uma instância, ela continuará sendo exibida na lista Instance (Instância) com instâncias em execução ou interrompidas. Por fim,AWSRecupera essas instâncias e elas desaparecem da lista. Você não será cobrado por instâncias em um estado encerrado.



Para especificar o comportamento de uma instância do EC2 no desligamento

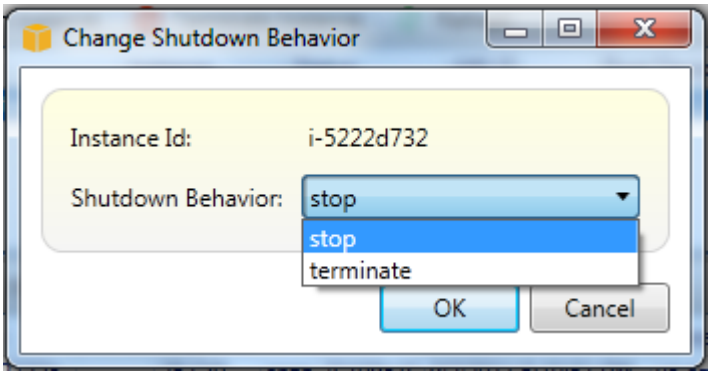
OAWSO Toolkit permite especificar se uma instância do Amazon EC2 será interrompida ou encerrada seDesligamentoé selecionado a partir doIniciarmenu.

1. Na lista Instances (Instâncias), clique com o botão direito do mouse em uma instância do Amazon EC2 e escolha Change shutdown behavior (Alterar comportamento de desligamento).



Item de menu Change Shutdown Behavior (Alterar comportamento de desligamento)

2. Na caixa de diálogo Change Shutdown Behavior (Alterar comportamento de desligamento), na lista suspensa Shutdown Behavior (Comportamento de desligamento), escolha Stop (Interromper) ou Terminate (Encerrar).



Gerenciar instâncias do Amazon ECS

AWSO Amazon Elastic Container Service (Amazon ECS) de clusters do Amazon Elastic Container Service (Amazon ECS). Você pode criar, excluir e gerenciar detalhes de clusters e contêineres de dentro do ambiente de desenvolvimento do Visual Studio.

Modificar propriedades do serviço

Você pode ver detalhes, eventos e propriedades de serviços na visualização do cluster.

1. DentroAWSNo Explorer, abra o menu de contexto (clique com o botão direito) do cluster a ser gerenciado e escolhaExibir.
2. Na visualização do cluster do ECS, clique em Services (Serviços) à esquerda e clique na guia Details (Detalhes) na visualização de detalhes. Você pode clicar em Events (Eventos) para ver as mensagens de eventos e Deployments (Implantações) para ver o status da implantação.
3. Clique em Edit. É possível alterar a contagem de tarefas desejadas e a porcentagem mínima e máxima de integridade.
4. Clique em Save (Salvar) para aceitar as alterações ou em Cancel (Cancelar) para reverter os valores existentes.

Interrupção de uma tarefa

Você pode ver o status atual das tarefas e interromper uma ou mais tarefas na visualização do cluster.

Para interromper uma tarefa

1. DentroAWSNo Explorer, abra o menu de contexto (clique com o botão direito) do cluster com as tarefas que você deseja interromper e escolhaExibir.
2. Na visualização do cluster do ECS, clique em Tasks (Tarefas) à esquerda.
3. Certifique-se de que Desired Task Status (Status desejado da tarefa) esteja definido como `Running`. Escolha as tarefas individuais para interromper e clique em Stop (Interromper) ou clique em Stop All (Interromper tudo) para selecionar e interromper todas as tarefas em execução.
4. Na caixa de diálogo Stop Tasks (Interromper tarefas), escolha Yes (Sim).

Excluir um serviço

Você pode excluir serviços de um cluster a partir da visualização do cluster.

Para excluir um serviço de cluster

1. DentroAWSNo Explorer, abra o menu de contexto (clique com o botão direito) do cluster com um serviço que você deseja excluir e escolhaExibir.
2. Na visualização do cluster do ECS, clique em Services (Serviços) à esquerda e clique em Delete (Excluir).
3. Na caixa de diálogo Delete Cluster (Excluir cluster), se houver um load balancer e um grupo de destino no cluster, você poderá optar por excluí-los com o cluster. Eles não serão usados quando o serviço for excluído.
4. Na caixa de diálogo Delete Cluster (Excluir cluster), escolha OK. Quando o cluster for excluído, ele será removido doAWSExplorador.

Excluir um cluster

Você pode excluir um cluster do Amazon Elastic Container Service doAWSExplorador.

Para excluir um cluster

1. DentroAWSNo Explorer, abra o menu de contexto (clique com o botão direito) do cluster que você deseja excluir noClustersNó doAmazon ECSEscolha e, depois, escolhaExcluir.
2. Na caixa de diálogo Delete Cluster (Excluir cluster), escolha OK. Quando o cluster for excluído, ele será removido doAWSExplorador.

Criar um repositório

Você pode criar um repositório do Amazon Elastic Container Registry doAWSExplorador.

Para criar um repositório

1. DentroAWSNo menu de contexto (clique com o botão direito do mouse) doRepositóriosnó abaixoAmazon ECSEscolha e, depois, escolhaCriar repositório do.
2. Na caixa de diálogo Create Repository (Criar repositório), forneça o nome do repositório e escolha OK.

Excluir um repositório

Você pode excluir um repositório do Amazon Elastic Container Registry doAWSExplorador.

Para excluir um repositório

1. DentroAWSNo menu de contexto (clique com o botão direito do mouse) doRepositóriosnó abaixoAmazon ECSEscolha e, depois, escolhaDelete repositório.
2. Na caixa de diálogo Delete Repository (Excluir repositório), você poderá optar por excluir o repositório, mesmo que ele contenha imagens. Caso contrário, ele será excluído somente se estiver vazio. Clique em Yes (Sim).

Gerenciamento de security groups emAWSExplorer

O Toolkit for Visual Studio permite criar e configurar security groups para usar com instâncias do Amazon Elastic Compute Cloud (Amazon EC2) eAWS CloudFormation. Ao executar instâncias do Amazon EC2 ou implantar um aplicativo emAWS CloudFormationVocê especifica um security group para associar às instâncias do Amazon EC2. (Implantação emAWS CloudFormationCrie instâncias do Amazon EC2.)

Um security group funciona como um firewall no tráfego de rede recebido. O security group especifica quais tipos de tráfego de rede são permitidos em uma instância do Amazon EC2. Ele também pode especificar que o tráfego de entrada só será aceito de determinados endereços IP ou de usuários especificados ou ainda apenas de outros security groups.

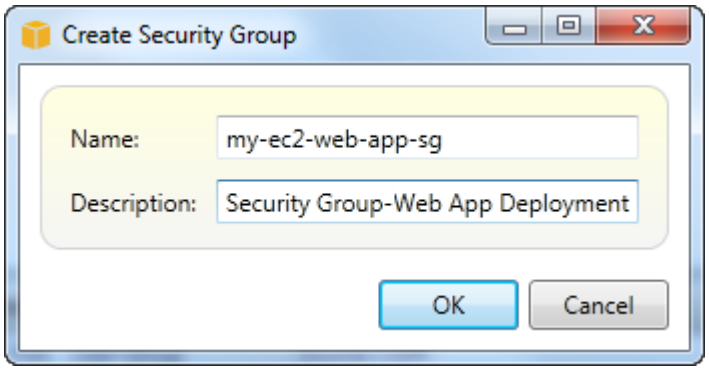
Criar um grupo de segurança

Nesta seção, criaremos um security group. Depois de ter sido criado, o security group não terá permissões configuradas. Configurar permissões é algo processado por meio de uma operação adicional.

Como criar um grupo de segurança

1. DentroAWSExplorer, sob aAmazon EC2, abra o menu de contexto (clique com o botão direito do mouse) noSecurity groups donó e, em seguida, escolhaExibir.
2. Na guia EC2 Security Groups (Grupos de segurança do EC2), escolha Create Security Group (Criar grupo de segurança).

3. Na caixa de diálogo Create Security Group (Criar grupo de segurança), digite um nome e uma descrição para o grupo de segurança e escolha OK.

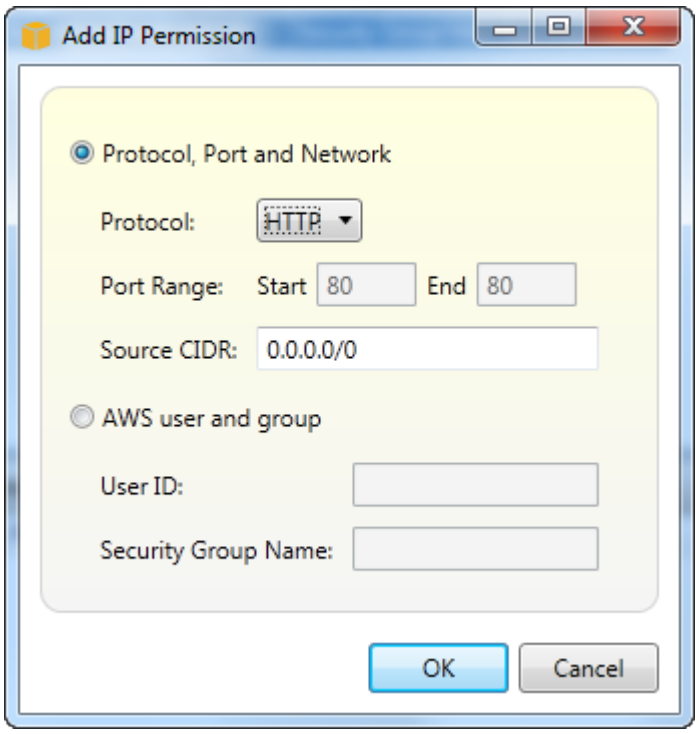


Adicionar permissões a security groups

Nesta seção, adicionaremos permissões ao security group para permitir o tráfego da web por meio dos protocolos HTTP e HTTPS. Também permitiremos que outros computadores se conectem usando o Windows Remote Desktop Protocol (RDP).

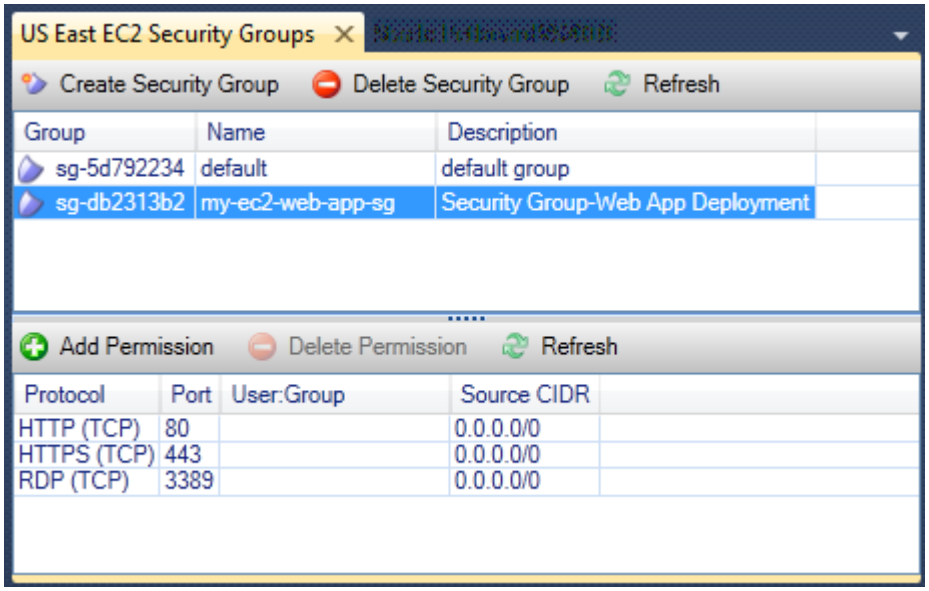
Para adicionar permissões a um security group

1. Na guia EC2 Security Groups (Grupos de segurança do EC2), escolha um grupo de segurança e selecione o botão Add Permission (Adicionar permissão).
2. Na caixa de diálogo Add IP Permission (Adicionar permissão de IP), escolha o botão de opção Protocol, Port and Network (Protocolo, porta e rede) e, na lista suspensa Protocol (Protocolo), escolha HTTP. O intervalo de portas se ajusta automaticamente à porta 80, a porta padrão para HTTP. O campo Source CIDR (CIDR de origem) assume como padrão 0.0.0.0/0, o que especifica que o tráfego de rede HTTP será aceito em qualquer endereço IP externo. Escolha OK.



Abrir a porta 80 (HTTP) desse security group

3. Repita esse processo para HTTPS e RDP. As permissões de security groups já devem ser semelhantes às permissões a seguir.



Você também pode definir permissões no security group especificando um ID de usuário e um nome de security group. Neste caso, as instâncias do Amazon EC2 nesse security group aceitarão todo o tráfego de rede recebido de instâncias do Amazon EC2 no security group especificado. Você

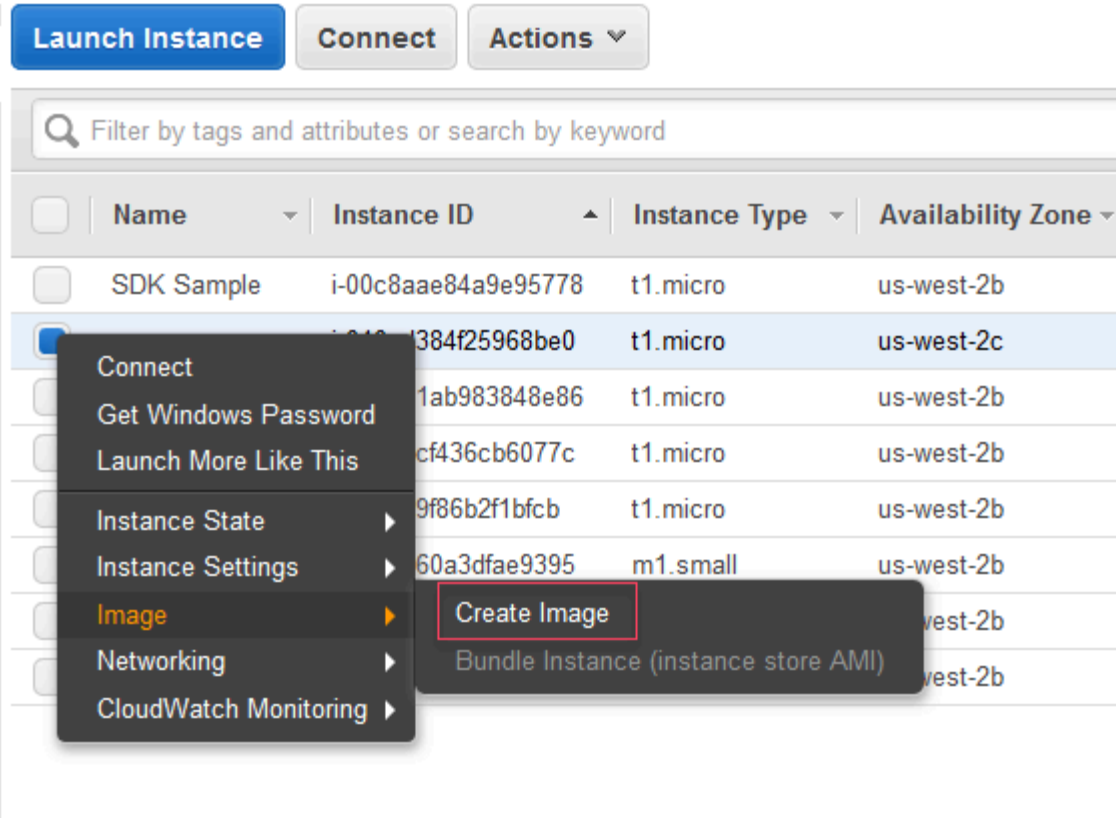
também deve especificar o ID do usuário como uma maneira de diferenciar o nome do security group; os nomes de security group não precisam ser exclusivos em todosAWS. Para obter mais informações sobre grupos de segurança, acesse a documentação do EC2.

Criar uma AMI com base em uma instância do Amazon EC2

Na visualização Amazon EC2 Instances (Instâncias do Amazon EC2), você pode criar imagens de máquina da Amazon (AMIs) com base em instâncias em execução ou paradas. Para obter informações mais detalhadas sobre AMIs, consulte o tópico Amazon Machine Images (AMI) no Guia do usuário do Amazon Elastic Compute Cloud para instâncias do Windows.

Para criar uma AMI a partir de uma instância

1. Clique com o botão direito do mouse na instância que você deseja usar como base para a AMI e escolha Create Image (Criar imagem) no menu de contexto.

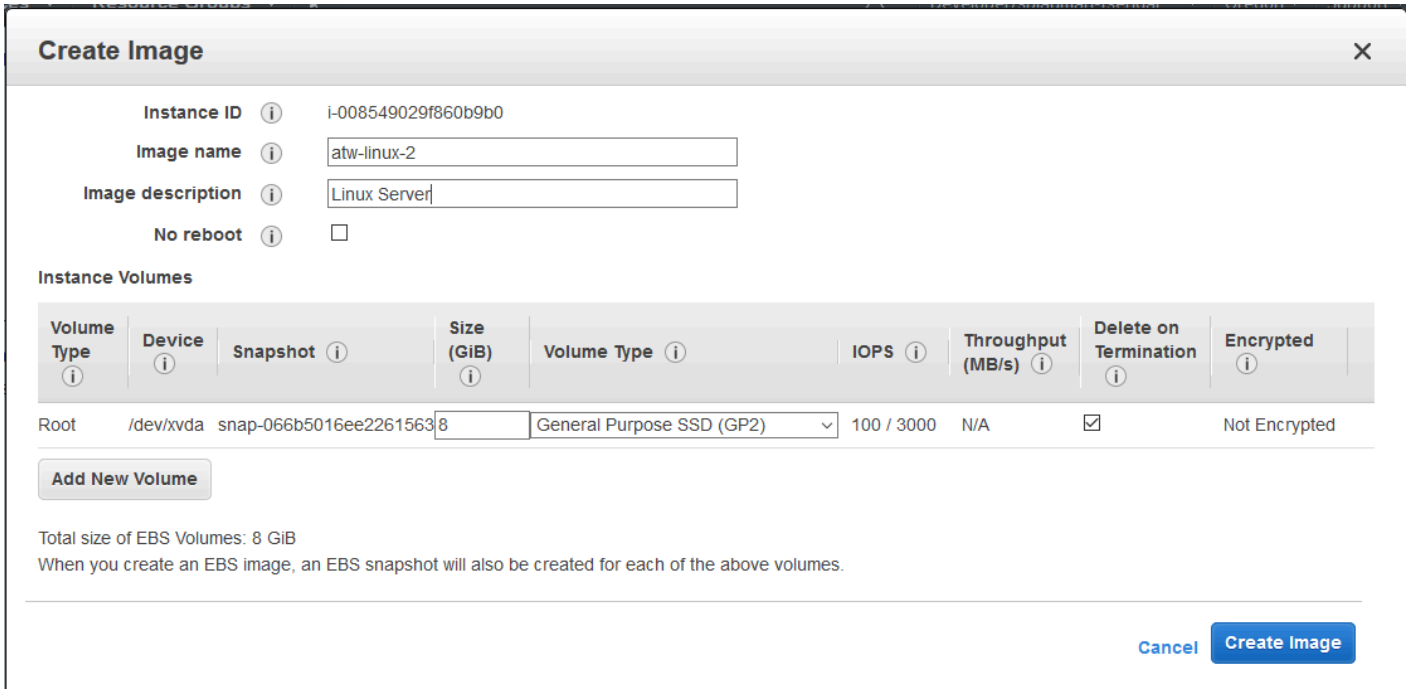


Menu de contexto Create Image (Criar imagem)

2. Na caixa de diálogo Create Image (Criar imagem), digite um nome exclusivo e uma descrição, além de escolher Create Image (Criar imagem). Por padrão, o Amazon EC2 encerra a instância,

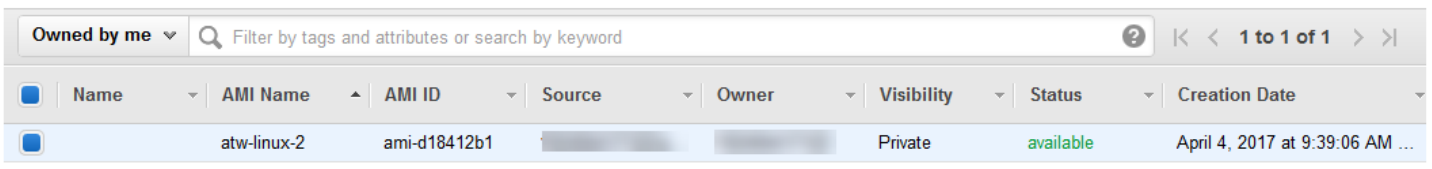
faz snapshots dos volumes anexados, cria e registra a AMI e, em seguida, reinicializa a instância. Escolha Sem reinicialização se você não quiser que sua instância seja encerrada.

> **Warning**
>
> Se você escolher No reboot (Sem reinicialização), não poderemos garantir a integridade do sistema de arquivos da imagem criada.



Caixa de diálogo Create Image (Criar imagem)

Pode demorar alguns minutos para a AMI ser criada. Depois de criado, ele aparecerá na visualização de AMIs noAWS Explorer. Para exibir essa visualização, clique duas vezes no nó Amazon EC2 | AMIs noAWS Explorer. Para ver as AMIs, na lista suspensa Viewing (Em exibição), escolha Owned By Me (De minha propriedade). Talvez seja necessário escolher Refresh (Atualizar) para visualizar a AMI. Quando a AMI for exibida pela primeira vez, ela poderá estar em um estado pendente, mas depois de alguns instantes, ela mudará para um estado disponível.



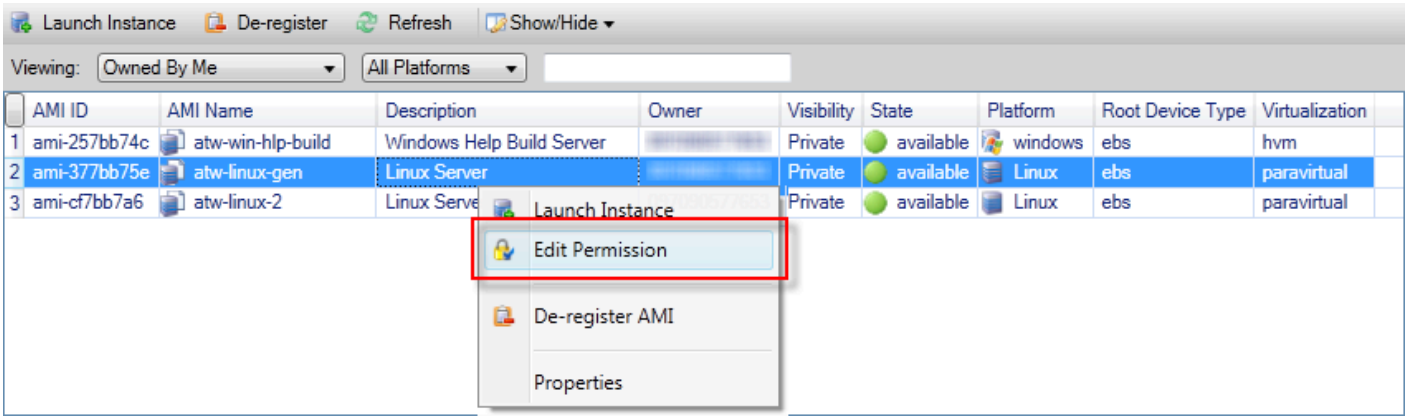
Lista de AMIs criadas

Definir permissões de execução em uma imagem de máquina da Amazon

Você pode definir permissões de execução nas imagens de máquina da Amazon (AMIs) naAMIsComo visualizarAWSExplorador. Você pode usar a caixa de diálogo Set AMI Permissions (Definir permissões da AMI) para copiar permissões de AMIs.

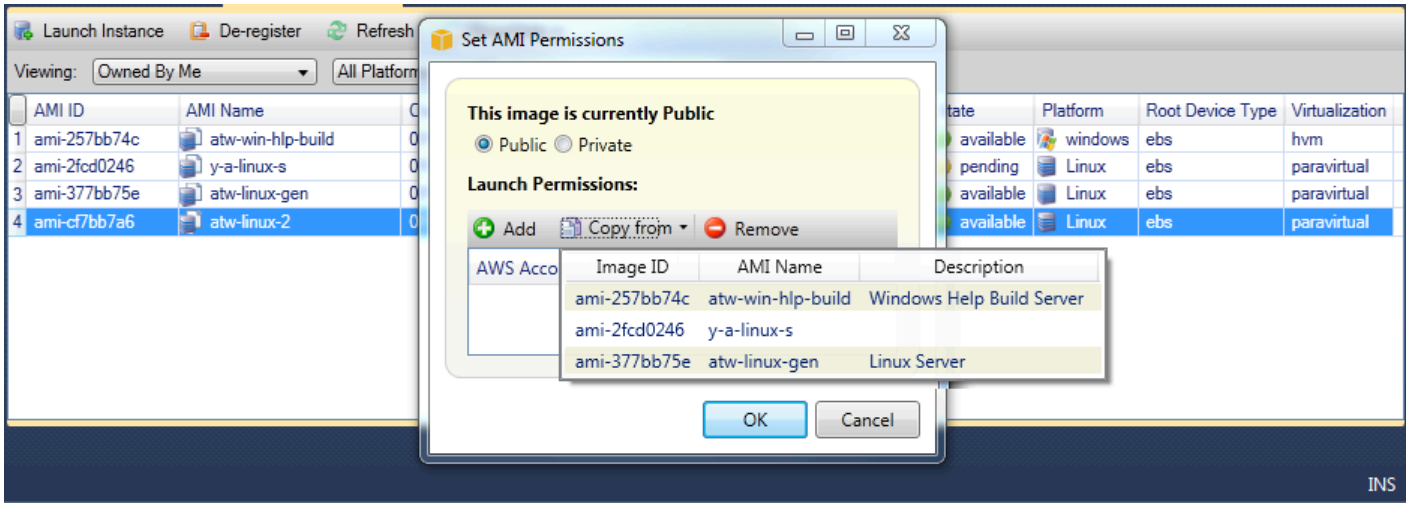
Para definir permissões em uma AMI

1. NoAMIsComo visualizarAWSNo Explorer, abra o menu de contexto (botão direito do mouse) em uma AMI e escolhaEditar permissão.



2. Existem três opções disponíveis na caixa de diálogo Set AMI Permissions (Definir permissões da AMI):
   - Para dar permissão de lançamento, escolhaAdicionare digite o número da conta para oAWSusuário a quem você está dando permissão de lançamento.
   - Para remover permissão de execução, escolha o número da conta daAWSO usuário de quem você está removendo permissão de execução e escolhaRemover.
   - Para copiar permissões de uma AMI para outra, escolha uma AMI na lista e Copy from (Copiar de). Os usuários que tiverem permissões de execução na AMI escolhida por você receberão permissões de execução na AMI atual. Você pode repetir esse processo com outras AMIs na lista Copy-from (Copiar-de) para copiar permissões de várias AMIs para a AMI de destino.

     OCOPY deA lista só contém essas AMIs de propriedade da conta que estava ativa quando oAMIsexibição foi exibida deAWSExplorador. Assim, a lista Copy-from (Copiar-de) talvez não exiba nenhuma AMI caso nenhuma outra AMI seja de propriedade da conta ativa.



Caixa de diálogo Copy AMI permissions (Copiar permissões da AMI)

Amazon Virtual Private Cloud (VPC)

A Amazon Virtual Private Cloud (Amazon VPC) permite executar recursos da Amazon Web Services em uma rede virtual definida por você. Essa rede virtual se assemelha a uma rede tradicional que você operaria no seu datacenter, com os benefícios de usar a infraestrutura dimensionável doAWS. Para obter mais informações, acesse o Guia do usuário da Amazon VPC.

O Toolkit for Visual Studio permite que um desenvolvedor acesse a funcionalidade da VPC semelhante à exposta peloAWS Management Consolemas do ambiente de desenvolvimento do Visual Studio. OAmazon VPCNó doAWSO Explorer inclui subnós das áreas a seguir.

- VPCs
- Sub-redes
- IPs elásticos
- Gateways da Internet
- Network ACLs
- Tabelas de rotas
- Security Groups (Grupos de segurança)

Criar uma VPC pública/privada para implantação comAWS Elastic Beanstalk

Esta seção descreve como criar uma Amazon VPC que contém as sub-redes privadas e públicas. A sub-rede pública contém uma instância do Amazon EC2 que realiza a Network Address Translation (NAT — conversão de endereços de rede) para habilitar instâncias na sub-rede privada para se comunicar com a internet pública. As duas sub-redes devem residir na mesma Availability Zone (AZ – Zona de disponibilidade).

Essa é a configuração da VPC mínima necessária para implantar um ambiente do AWS Elastic Beanstalk em uma VPC. Nesse cenário, as instâncias do Amazon EC2 que hospedam o aplicativo residem na sub-rede privada; o load balancer do Elastic Load Balancing que roteia tráfego recebido para o aplicativo reside na sub-rede pública.

Para obter mais informações sobre a NAT, acesse Instâncias NAT no Guia do usuário da Amazon Virtual Private Cloud. Para obter um exemplo de como configurar a implantação para usar uma VPC, consulte Implantação no Elastic Beanstalk.

Para criar uma VPC de sub-rede privada/pública

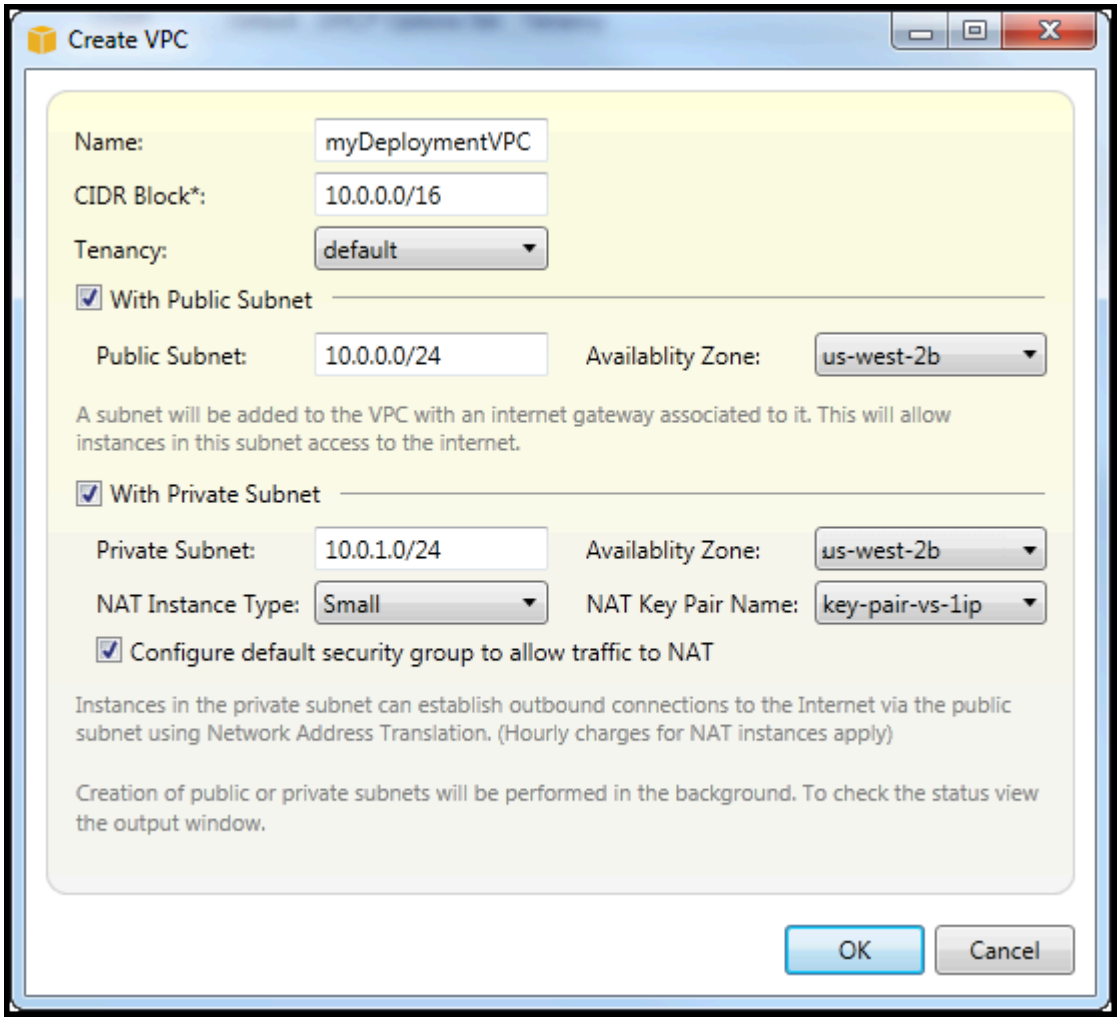
1. NoAmazon VPCNó doAWSExplorer, abra a guiaVPCsUm subnó e, depois, escolhaCriar a VPC.

2. Configure a VPC desta forma:
   - Digite um nome para a VPC.
   - Marque as caixas de seleção With Public Subnet (Com sub-rede pública) e With Private Subnet (Com sub-rede privada).

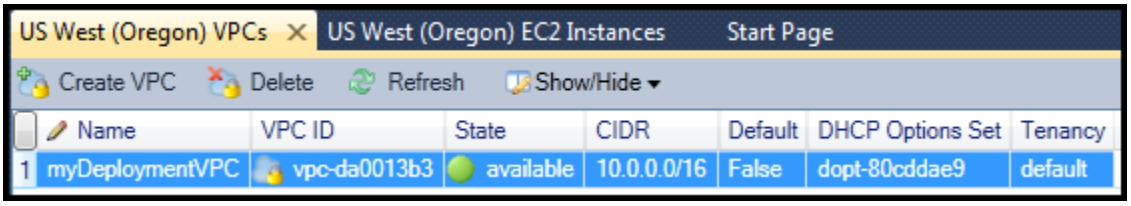
- Na lista suspensa Availability Zone (Zona de disponibilidade) de cada sub-rede, escolha uma zona de disponibilidade. Use o mesmo AZ para ambas as sub-redes.
- Para a sub-rede privada, em NAT Key Pair Name (Nome do par de chaves NAT), forneça um par de chaves. Esse key pair é usado na instância do Amazon EC2 que realiza a conversão de endereços de rede da sub-rede privada na Internet pública.
- Marque a caixa de seleção Configure default security group to allow traffic to NAT (Configurar grupo de segurança padrão para permitir tráfego ao NAT).

Digite um nome para a VPC. Marque as caixas de seleção With Public Subnet (Com sub-rede pública) e With Private Subnet (Com sub-rede privada). Na lista suspensa Availability Zone (Zona de disponibilidade) de cada sub-rede, escolha uma zona de disponibilidade. Use o mesmo AZ para ambas as sub-redes. Para a sub-rede privada, em NAT Key Pair Name (Nome do par de chaves NAT), forneça um par de chaves. Esse key pair é usado na instância do Amazon EC2 que realiza a conversão de endereços de rede da sub-rede privada na Internet pública. Marque a caixa de seleção Configure default security group to allow traffic to NAT (Configurar grupo de segurança padrão para permitir tráfego ao NAT).

Escolha OK.

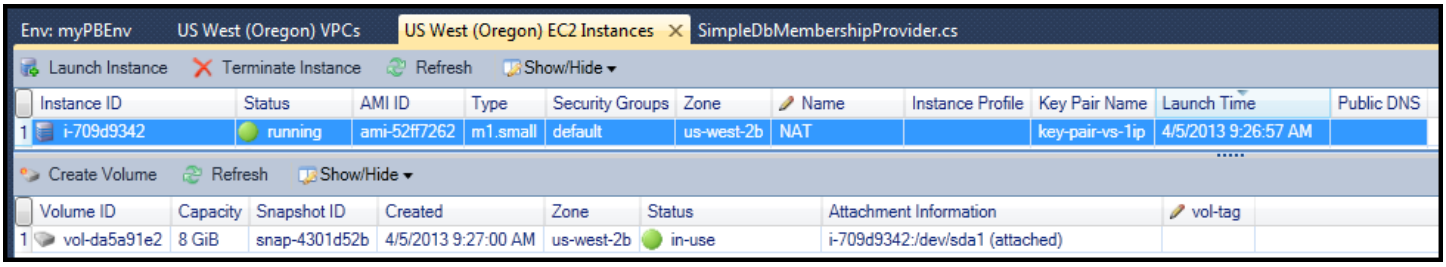


Você pode visualizar a nova VPC noVPCsGuia noAWSExplorador.



A instância NAT pode levar alguns minutos para ser iniciada. Quando estiver disponível, você poderá visualizá-la expandindo aAmazon EC2Nó doAWSExplorer e, em seguida, abrir oInstânciassubnó.

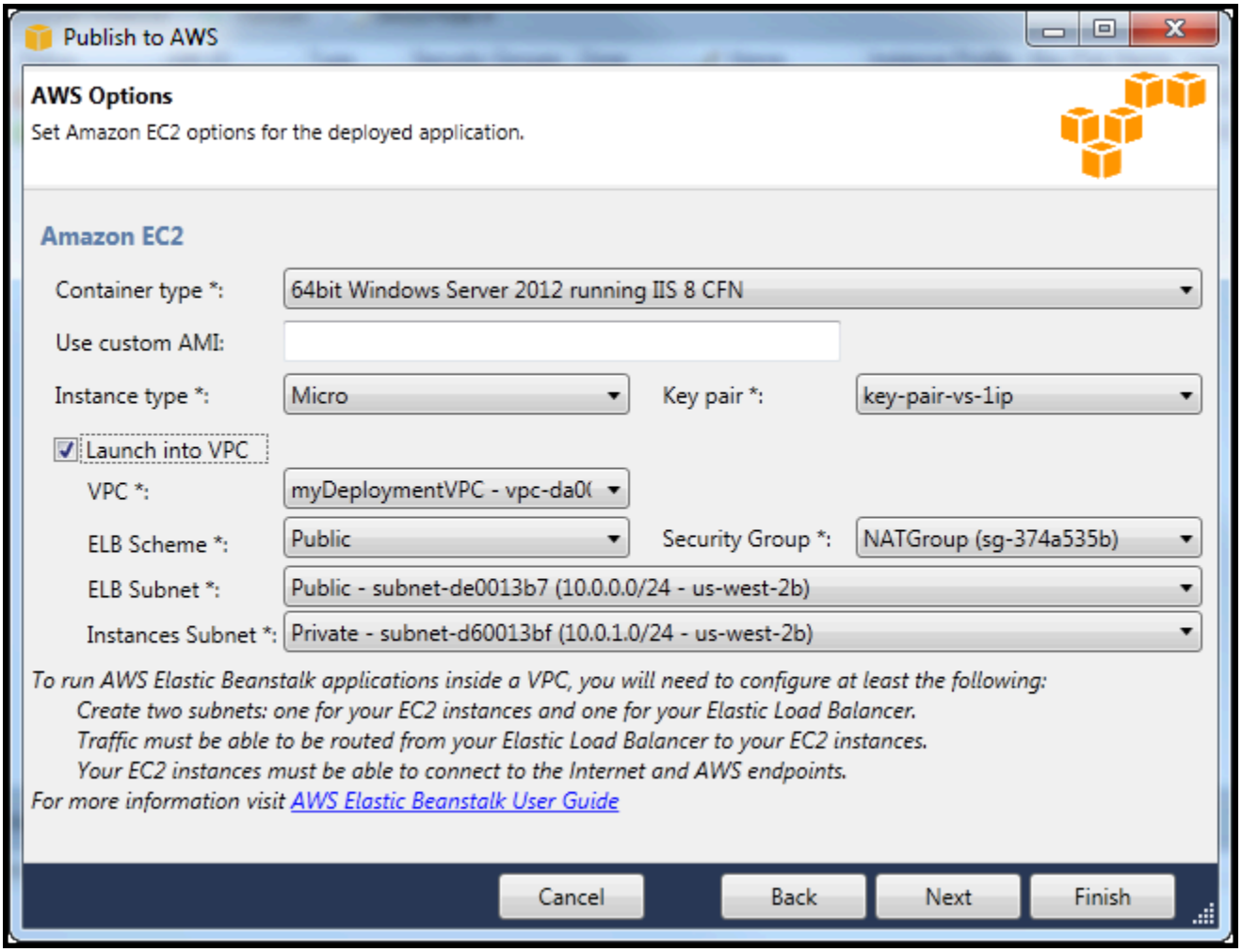
UmaAWS Elastic BeanstalkO volume do (Amazon EBS) é criado para a instância NAT automaticamente. Para obter mais informações sobre o Elastic Beanstalk, acesseAWS Elastic Beanstalk(EBS)noGuia do usuário do Amazon EC2 para instâncias do Linux.



Se vocêImplantar um aplicativo do em umAWS Elastic Beanstalkmeio Ambientee optar por iniciar o ambiente em uma VPC, o Toolkit preencherá oPublish to (Publicar no &CW;)Amazon Web Servicescaixa de diálogo com as informações de configuração da VPC.

O Toolkit preenche a caixa de diálogo com informações apenas de VPCs que foram criadas no Toolkit, e não de VPCs criadas usando aAWS Management Console. Isso acontece porque quando o Toolkit cria uma VPC, ele identifica os componentes da VPC, de maneira que ele possa acessar as informações.

A captura de tela a seguir do Assistente de implantação mostra um exemplo de uma caixa de diálogo preenchida com valores de uma VPC criada no Toolkit.



Para excluir uma VPC

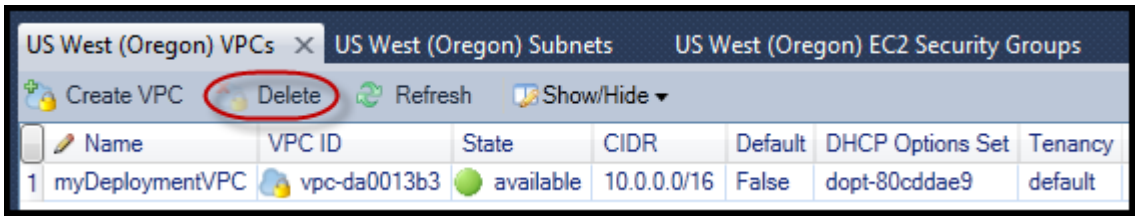
Para excluir a VPC, você deve primeiramente encerrar todas as instâncias do Amazon EC2 na VPC.

1. Se você tiver implantado um aplicativo em um ambiente do AWS Elastic Beanstalk na VPC, exclua o ambiente. Isso encerrará todas as instâncias do Amazon EC2 que hospedam o aplicativo com o load balancer do Elastic Load Balancing.

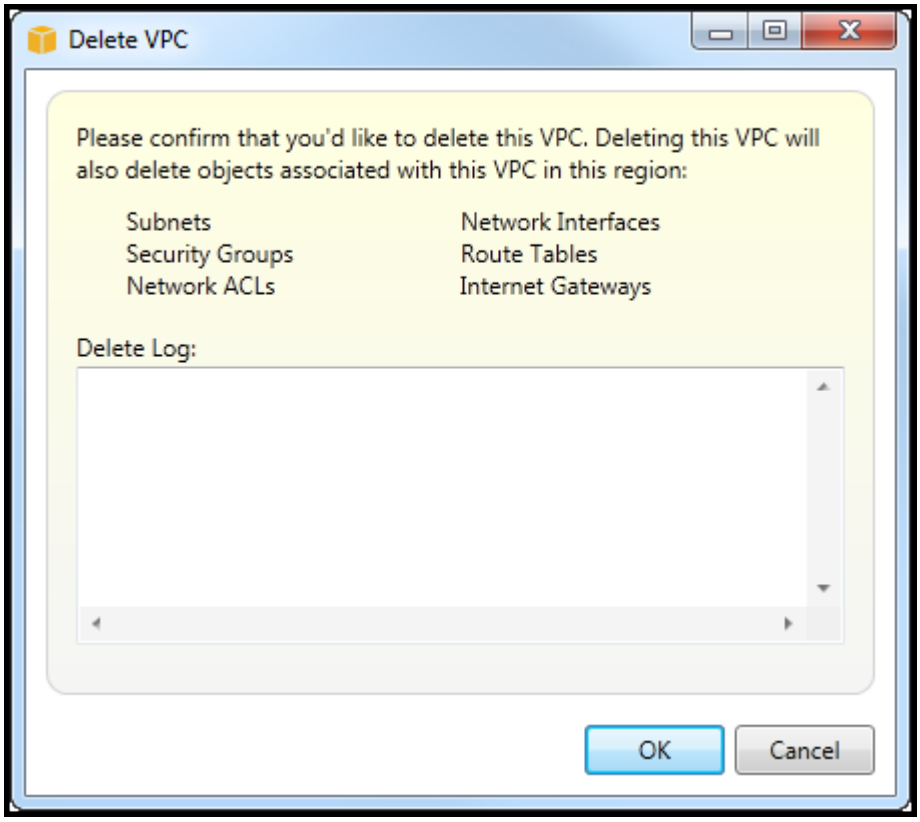
   Se você tentar encerrar diretamente as instâncias que hospedam o aplicativo sem excluir o ambiente, o serviço Auto Scaling criará automaticamente novas instâncias para substituir as excluídas. Para obter mais informações, acesse o Guia do desenvolvedor do Auto Scaling.
2. Exclua a instância NAT da VPC.

   Você não precisa excluir o volume do Amazon EBS associado à instância NAT para excluir a VPC. No entanto, se não excluir o volume, você continuará sendo cobrado por ele, mesmo se excluir a instância NAT e a VPC.

3. Na guia VPC, escolha o link Delete (Excluir) para excluir a VPC.



4. Na caixa de diálogo Delete VPC (Excluir VPC), escolha OK.



Usando o Editor AWS CloudFormation de modelos para Visual Studio

O Toolkit for Visual Studio inclui AWS CloudFormation um editor de modelos AWS CloudFormation e projetos de modelo para o Visual Studio. Entre os recursos compatíveis estão:

- Criação de novos modelos (vazios ou copiados de uma pilha existente ou modelo de amostra) usando o tipo de projeto AWS CloudFormation modelo fornecido.
- Editar modelos com validação JSON automática, preenchimento automático, code folding e realce de sintaxe.

- Sugestão automática de funções intrínsecas e parâmetros de referência de recursos para os valores de campo no modelo.
- Itens de menu para realizar ações comuns para seu modelo do Visual Studio.

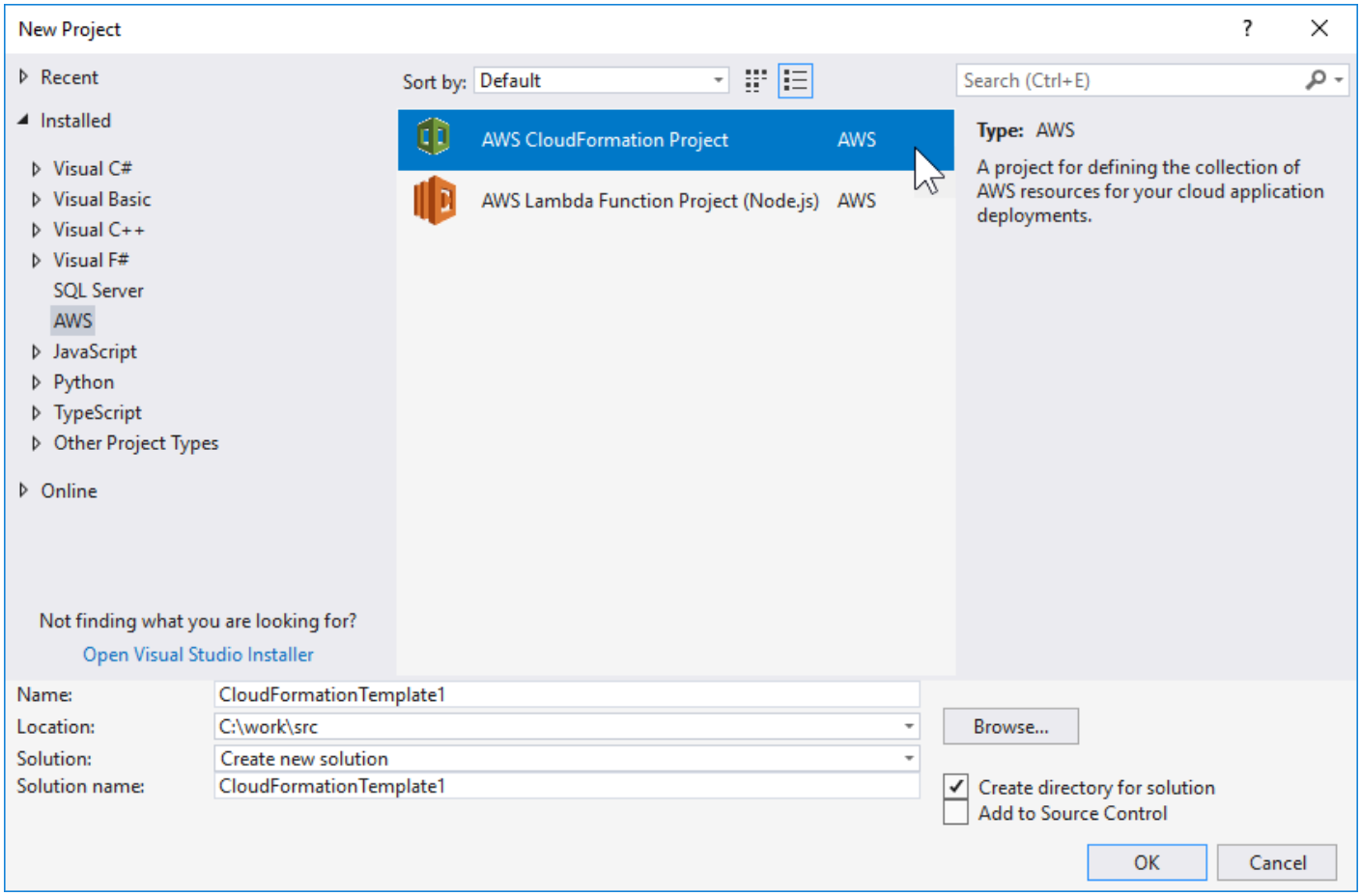
Tópicos

Criar um projeto de modelo do AWS CloudFormation no Visual Studio

Para criar um projeto de modelo

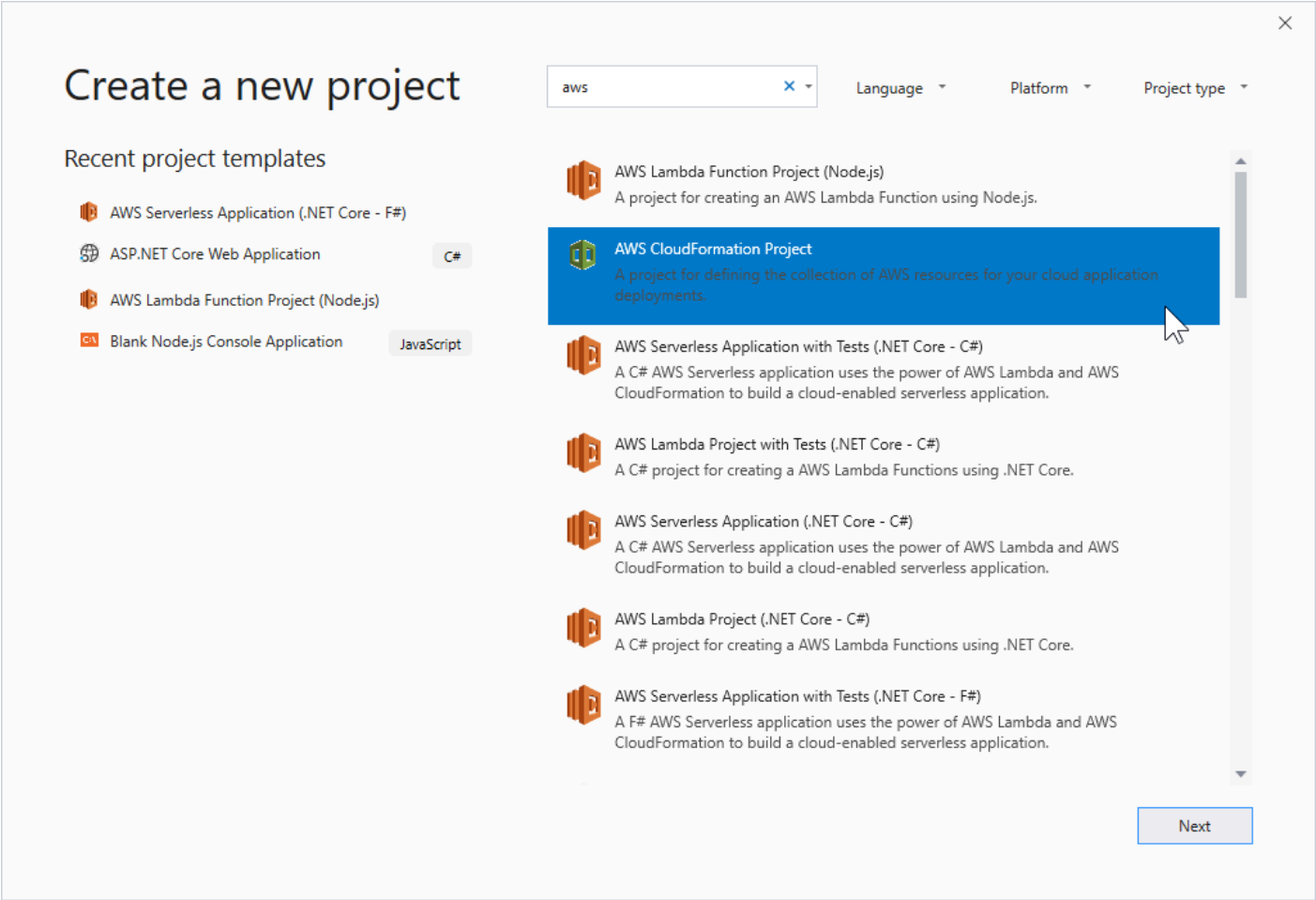
1. No Visual Studio, escolha File (Arquivo), New (Novo) e Project (Projeto).
2. No Visual Studio 2017:

   NoNovo projeto doCaixa de diálogo, expandirInstaladoe selecioneAWS.



No Visual Studio 2019:

Na caixa de diálogo New Project (Novo projeto), verifique se as caixas suspensas Language (Idioma), Platform (Plataforma) e Project type (Tipo de projeto) estão definidas como "All..." (Todos) e digite aws no campo Search (Pesquisar).



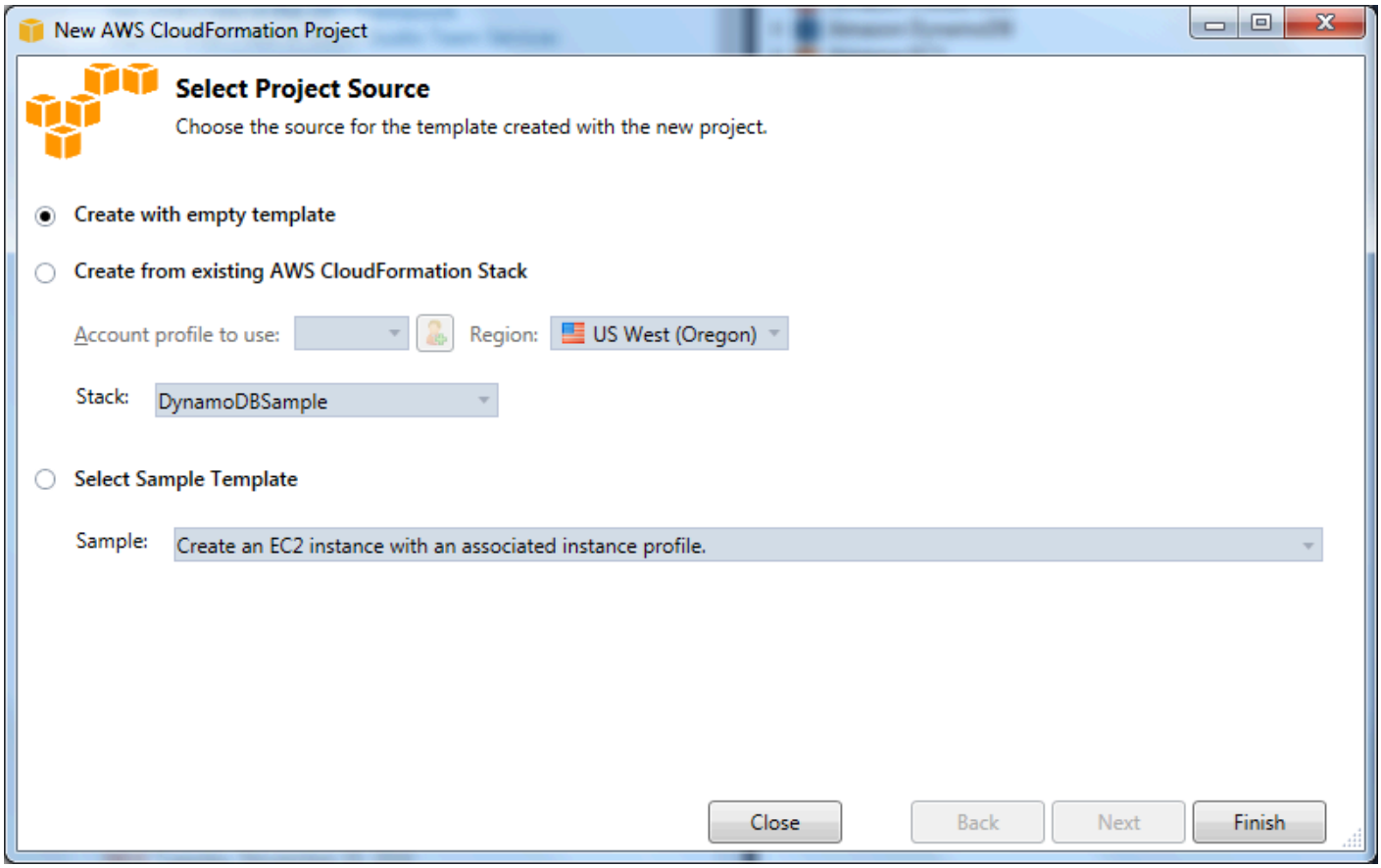
3. SELECT theAWSProjeto CloudFormationModelo.
4. No Visual Studio 2017:

   Digite o Name (Nome), o Location (Local) etc. para o seu projeto de modelo e, depois, clique em OK.

   No Visual Studio 2019:

   Clique em Next. Na próxima caixa de diálogo, insira o Name (Nome), o Location (Local) etc. para o seu projeto de modelo e clique em Create (Criar).
5. Na página Select Project Source (Selecionar fonte de projetos), escolha a origem do modelo que você criará:
   - Create with empty template (Criar com modelo vazio) gera um novo modelo do AWS CloudFormation vazio.
   - Criar a partir de existente doAWS|CFN| pilhaGera um modelo de uma pilha existente noAWSconta. (A pilha não precisa ter um status `CREATE_COMPLETE`.)

- Select sample template (Selecionar modelo de exemplo) gera um modelo com base em um dos modelos de exemplo do AWS CloudFormation.

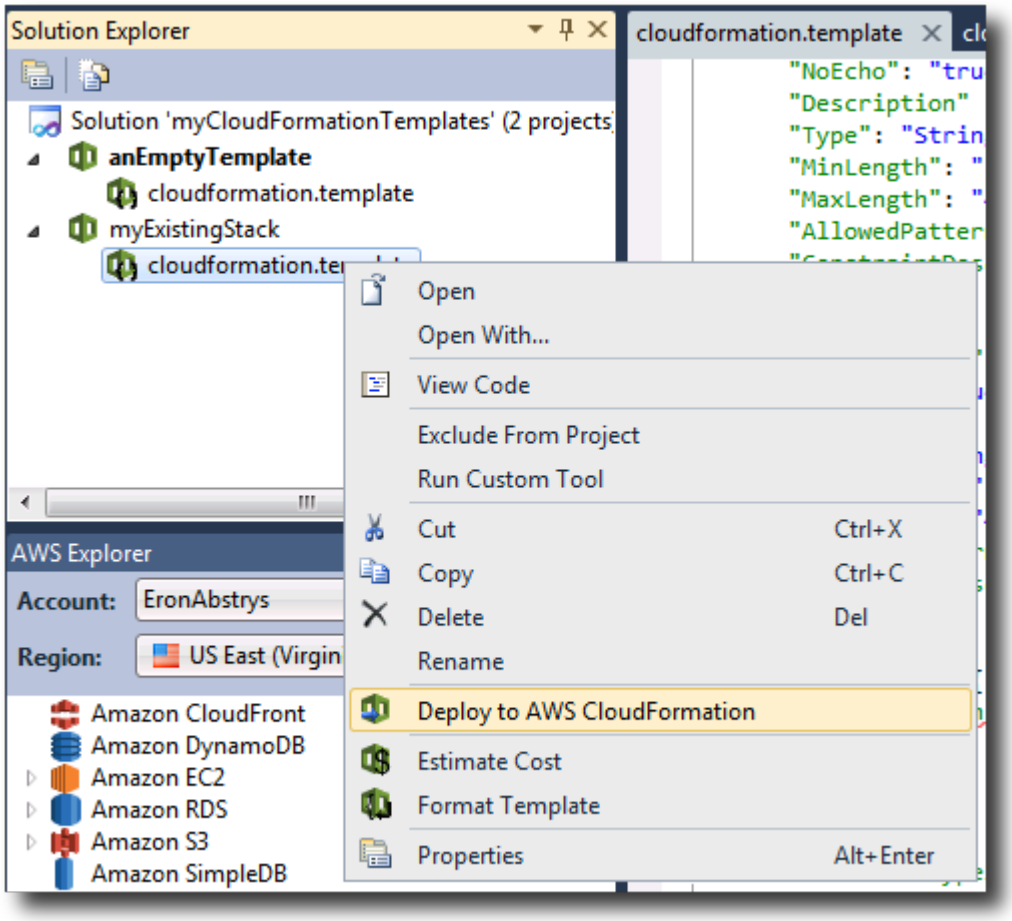


6. Para concluir a criação do projeto de modelo do AWS CloudFormation, escolha Finish (Concluir).

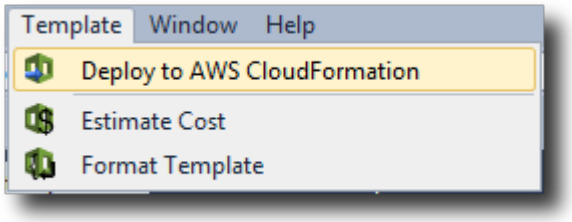
Implantar um modelo do AWS CloudFormation no Visual Studio

Para implantar um modelo do CFN

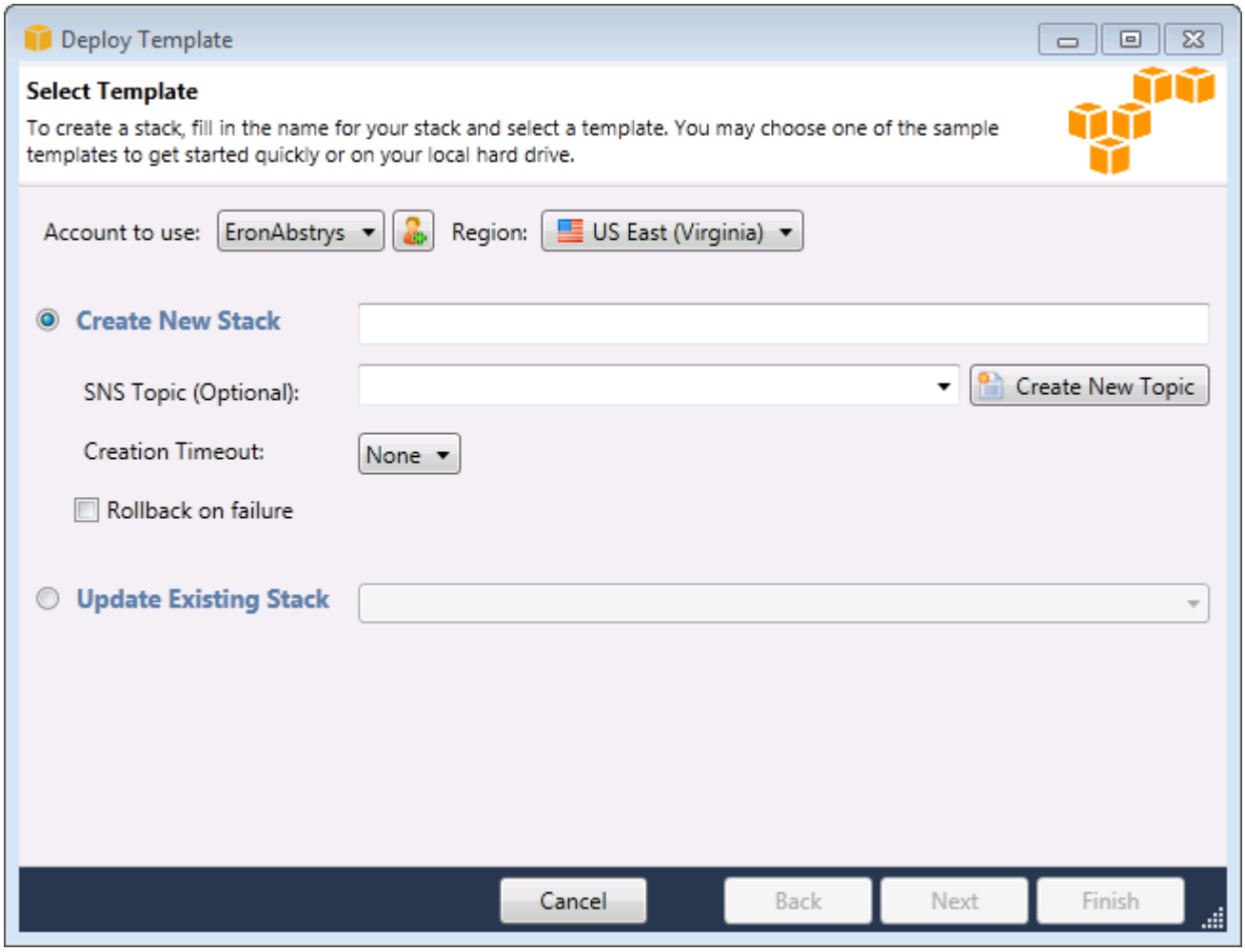
1. Em Solution Explorer, abra o menu de contexto (botão direito do mouse) do modelo que você deseja implantar e escolhaImplantação noAWS CloudFormation.



Como alternativa, para implantar o modelo que você está editando no momento, a partir doTemplate (Modelo)menu, selecioneImplantação noAWS CloudFormation.



2. NoImplantar modeloNa página, selecione oConta da AWSPara usar para executar a pilha e a região onde ela será iniciada.

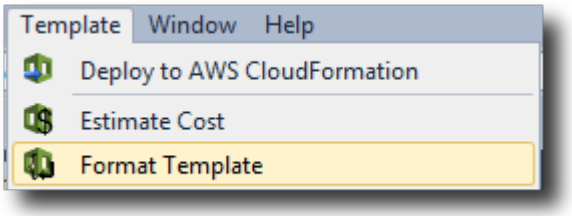


3. Escolha Create New Stack (Criar nova pilha) e digite um nome para a pilha.
4. Escolha qualquer uma das seguintes opções (ou nenhuma):
   - Para receber notificações sobre o progresso da pilha, na lista suspensa SNS Topic (Tópico do SNS), escolha um tópico do SNS. Você também pode criar um tópico do SNS escolhendo Create New Topic (Criar novo tópico) e digitando um endereço de e-mail na caixa.
   - Use Creation Timeout (Tempo limite para criação) para especificar por quanto tempo o AWS CloudFormation deve permitir que a pilha seja criada antes de ser declarada falha (e revertida, a menos que a opção Rollback on failure (Reverter em caso de falha) esteja desmarcada).
   - Use Rollback on failure (Reverter em caso de falha) se você quiser que a pilha seja revertida (isto é, excluída) em caso de falha. Deixe essa opção desmarcada se você quiser que a stack permaneça ativa, para fins de depuração, mesmo que ela tenha deixado de ser iniciada por completo.
5. Escolha Finish (Concluir) para executar a pilha.

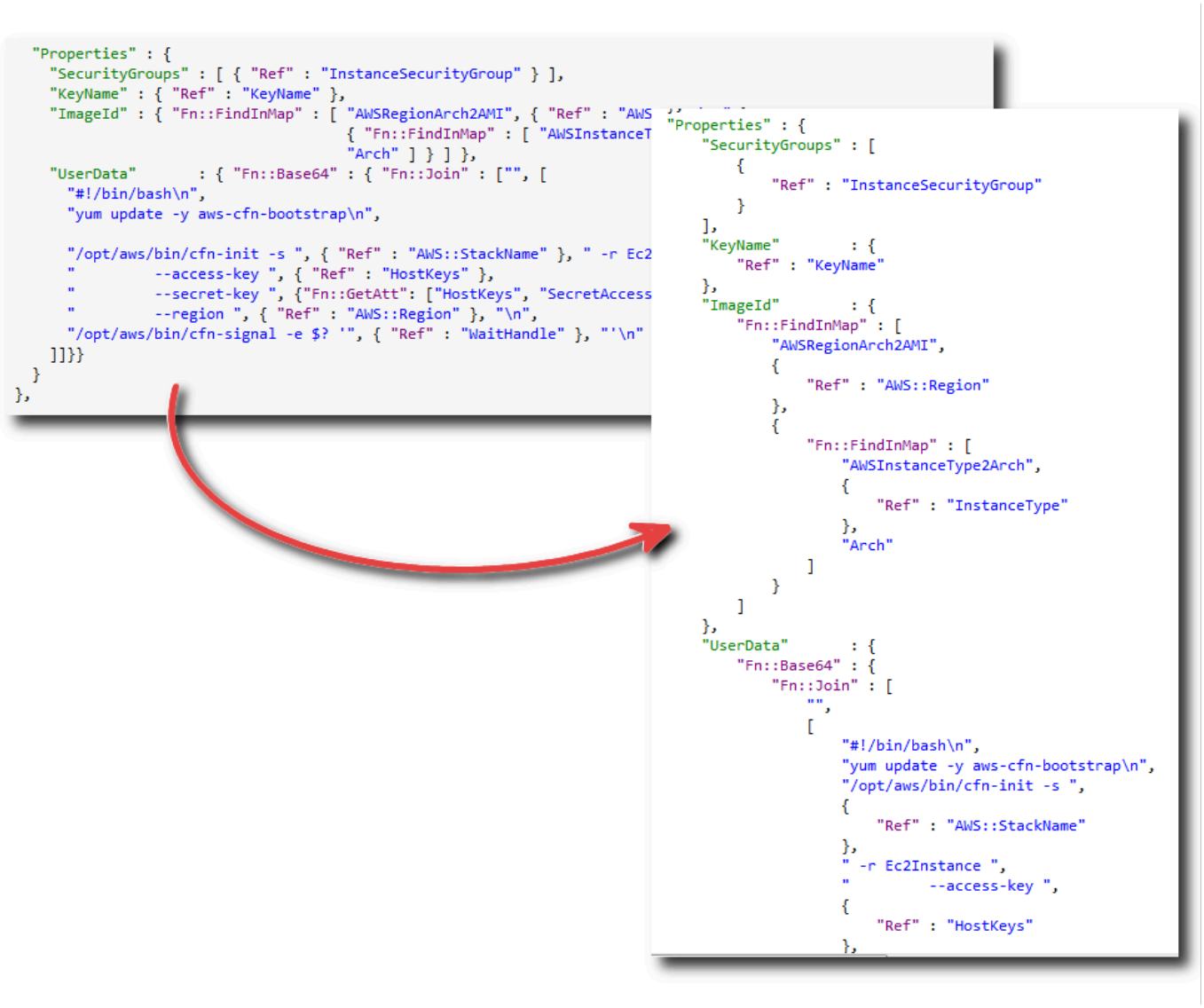
Formatar um modelo do AWS CloudFormation no Visual Studio

- Em Solution Explorer, abra o menu de contexto (botão direito do mouse) do modelo e escolha Format Template (Formatar modelo).

  Como alternativa, para formatar o modelo que você está editando no momento, no menu Template (Modelo), escolha Format Template (Formatar modelo).

  O código JSON será formatado de maneira que a estrutura seja apresentada claramente.



Uso do Amazon S3 a partir deAWSExplorer

O Amazon Simple Storage Service (Amazon S3) permite armazenar e recuperar dados de qualquer conexão com a Internet. Todos os dados armazenados no Amazon S3 são associados à conta e, por padrão, só podem ser acessados por você. O Toolkit for Visual Studio permite armazenar dados no Amazon S3 e visualizar, gerenciar, recuperar e distribuir esses dados.

O Amazon S3 usa o conceito de buckets, que você pode considerar como sendo semelhante a sistemas de arquivos ou unidades de disco lógicas. Os buckets podem conter pastas, que são semelhantes a diretórios e objetos, semelhantes a arquivos. Nesta seção, usaremos esses conceitos em meio à funcionalidade do Amazon S3 exposta pelo Toolkit for Visual Studio.

> **Note**
>
> Para usar essa ferramenta, a política IAM deve conceder permissões para `os3:GetBucketAcl`,`s3:GetBucket`, `es3:ListBucket`ações. Para obter mais informações, consulteVisão geral doAWSPolíticas do IAM.

Criando um Bucket do Amazon S3

O bucket é a unidade de armazenamento mais fundamental no Amazon S3.

Para criar um bucket do S3

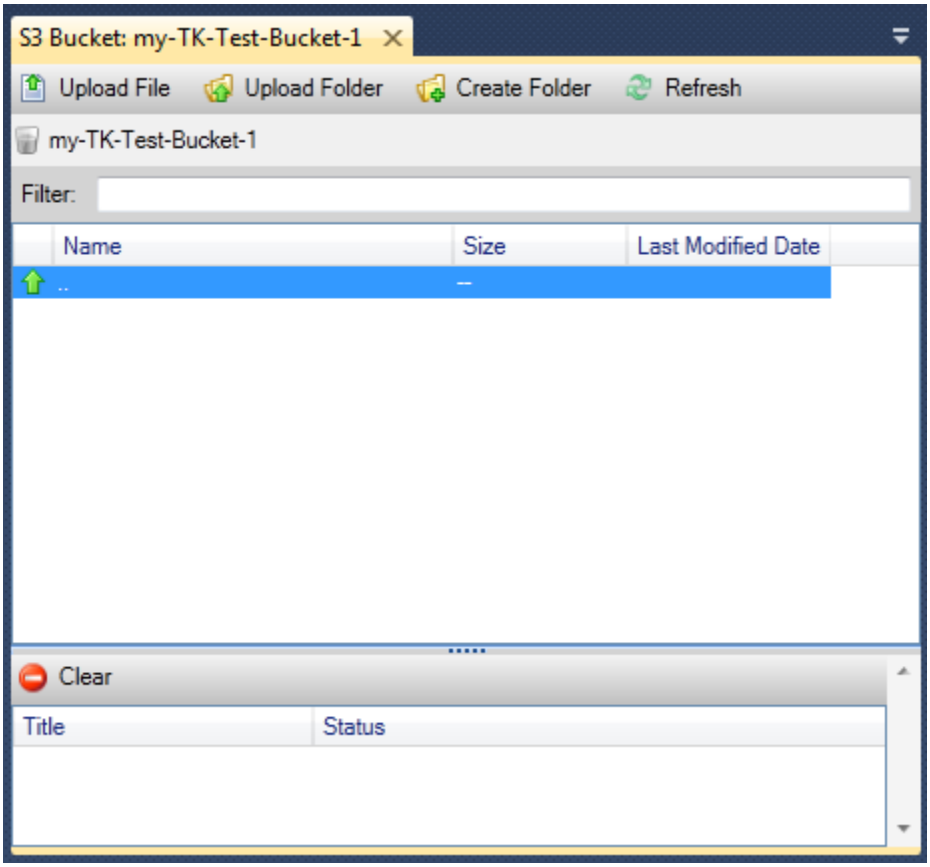
1. DentroAWSExplorer, abra o menu de contexto (clique com o botão direito do mouse) doAmazon S3nó e, em seguida, escolhaCriar bucket.
2. Na caixa de diálogo Create Bucket (Criar bucket), digite um nome para o bucket. Os nomes de bucket devem ser exclusivos noAWS. Para obter informações sobre outras restrições, acesse a documentação do Amazon S3.
3. Escolha OK.

Gerenciar buckets do Amazon S3 a partir deAWSExplorer

DentroAWSExplorer, as operações a seguir são disponibilizadas quando você abre um menu de contexto (clique com o botão direito do mouse) de um bucket do Amazon S3.

Navegar

Exibe uma visualização dos objetos contidos no bucket. Aqui, você pode criar pastas ou fazer upload de arquivos ou diretórios inteiros e pastas do computador local. O painel inferior exibe mensagens de status sobre o processo de upload. Para apagar essas mensagens, escolha o ícone Clear (Apagar). Você também pode acessar essa visualização do bucket clicando duas vezes no nome do bucket noAWSExplorador.



Properties

Exibe uma caixa de diálogo onde você pode fazer o seguinte:

- Defina as permissões do Amazon S3 com escopo para:
  - você como o proprietário do bucket.
  - todos os usuários que tenham sido autenticados noAWS.
  - todos com acesso à Internet.
- Ative o registro em log para o bucket.
- Configure uma notificação usando o Amazon Simple Notification Service (Amazon SNS), de maneira que, se estiver usando Reduced Redundancy Storage (RRS), você será notificado em caso de perda de dados. RRS é uma opção de armazenamento do Amazon S3 que oferece menos durabilidade do que o armazenamento padrão, mas a custo reduzido. Para obter mais informações, consulte Perguntas frequentes do S3.
- Crie um site estático usando os dados no bucket.

Política

Permite configurar as políticas do AWS Identity and Access Management (IAM) para o bucket. Para obter mais informações, acesse a documentação do IAM e os casos de uso do IAM e do S3.

Criar Pre-Signed URL

Permite gerar um URL limitado por tempo que você pode distribuir para dar acesso ao conteúdo do bucket. Para obter mais informações, consulte Como criar um pre-signed URL.

Visualizar multipart uploads

Permite visualizar multipart uploads. O Amazon S3 dá suporte à quebra de grandes uploads de objetos em partes para tornar o processo de upload mais eficiente. Para obter mais informações, acesse a discussão de multipart uploads na documentação do S3.

Excluir

Permite excluir o bucket. Você só pode excluir buckets vazios.

Carregar arquivos e pastas no Amazon S3

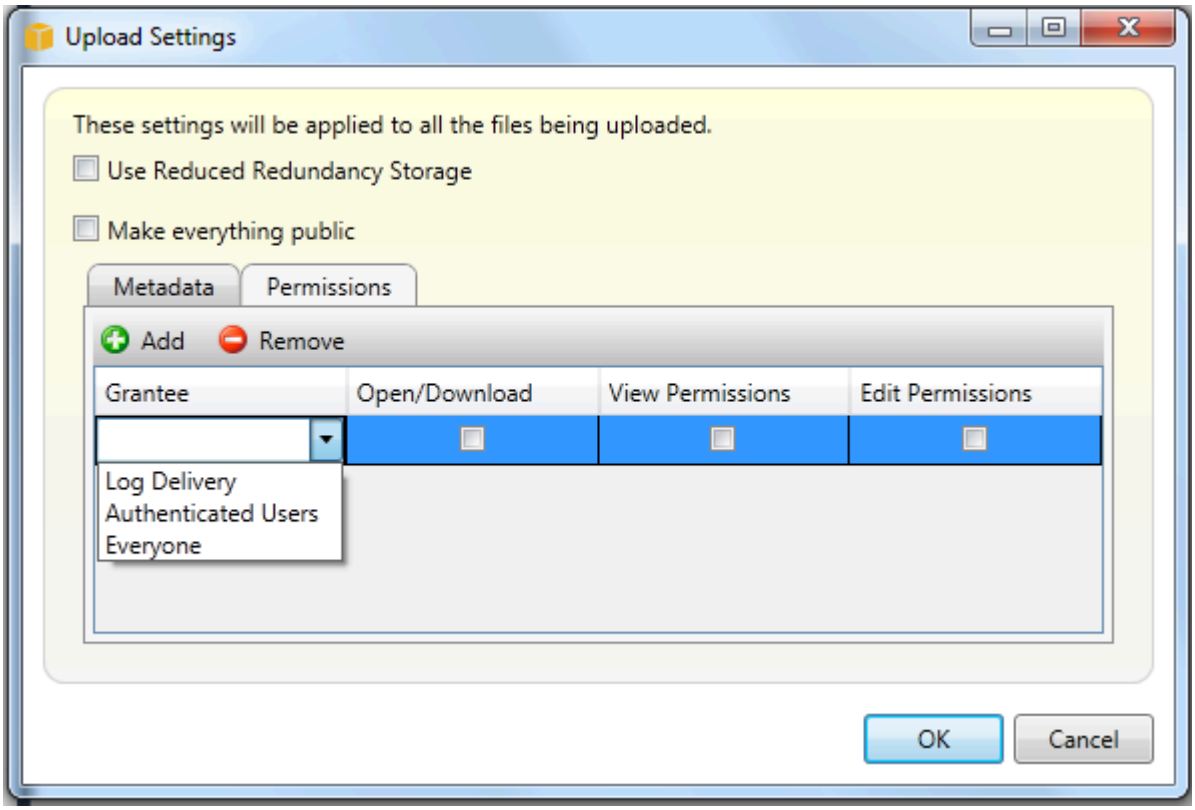
Você pode usarAWSExplorador de arquivos ou pastas inteiras do computador local para qualquer um dos buckets.

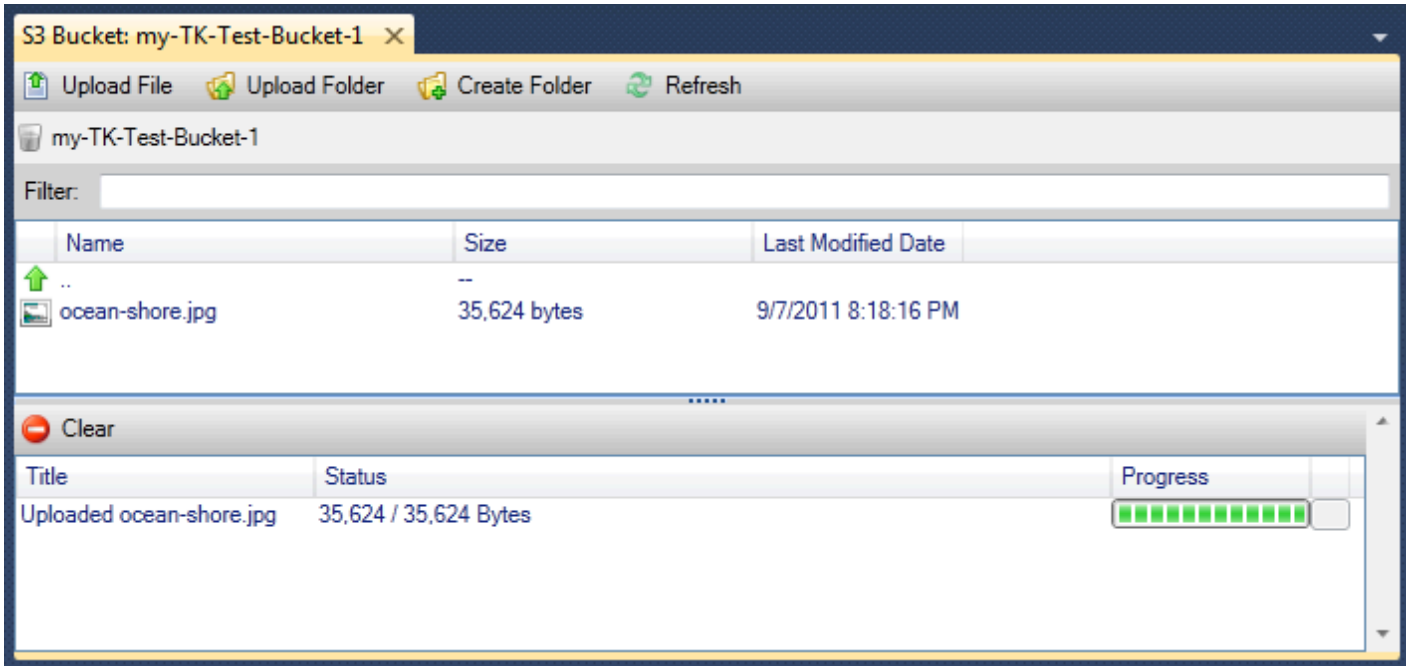
> **Note**
>
> Se você fizer upload de arquivos ou pastas que tenham o mesmo nome de arquivos ou pastas já existentes no bucket do Amazon S3, os arquivos carregados substituirão os arquivos existentes sem aviso.

Para fazer upload de um arquivo no S3

1. DentroAWSExplorer, expanda oAmazon S3E clique duas vezes em um bucket ou abra o menu de contexto (clique com o botão direito do mouse) do bucket e escolhaNavegar.
2. Na visualização Browse (Navegar) do bucket, escolha Upload File (Fazer upload de arquivo) ou Upload Folder (Fazer upload de pasta).
3. Na caixa de diálogo File-Open (Arquivo-abrir), navegue até os arquivos para fazer upload, selecione-os e escolha Open (Abrir). Se você estiver fazendo upload de uma pasta, navegue até, escolha essa pasta e selecione Open (Abrir).

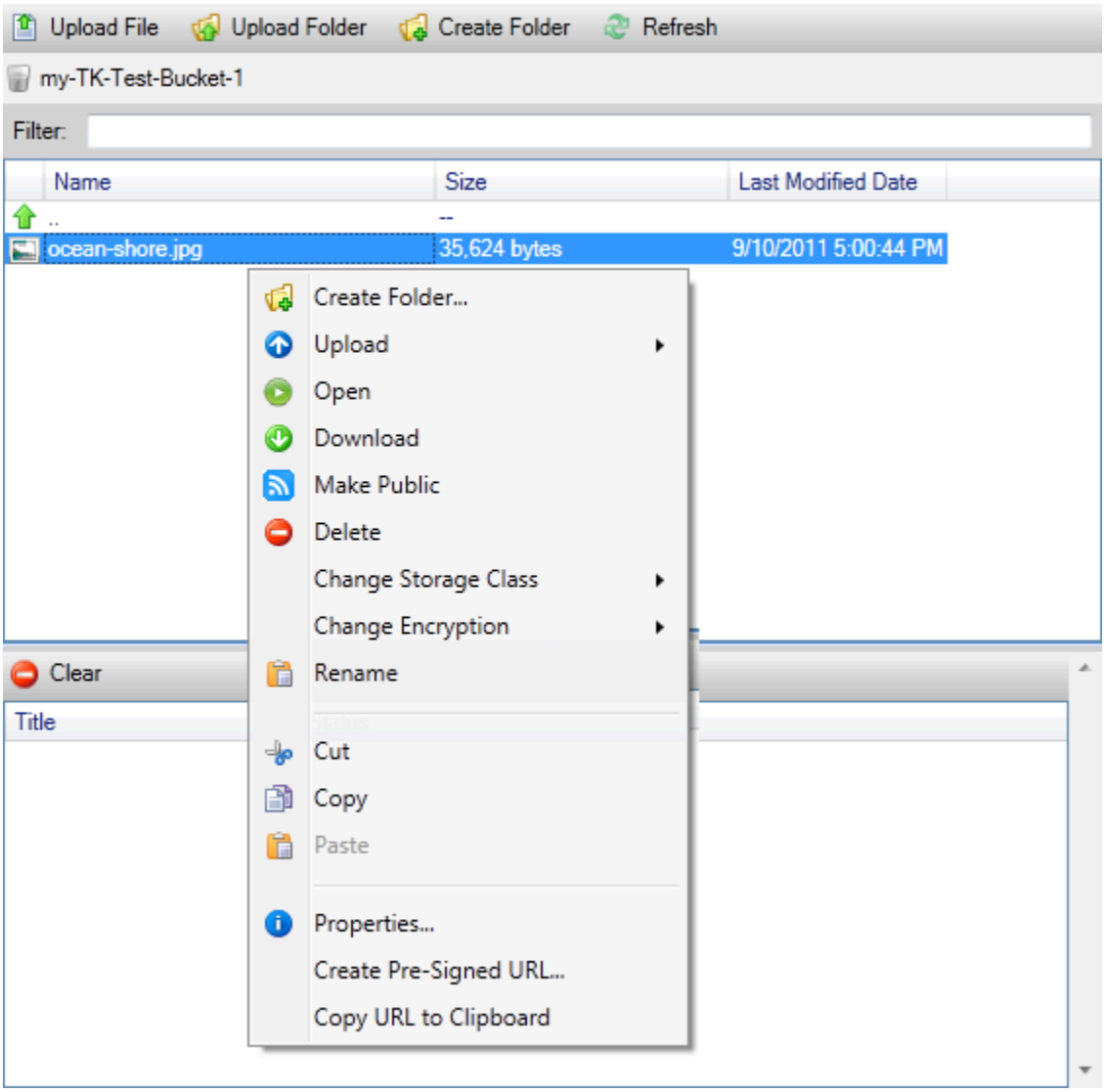
A caixa de diálogo Upload Settings (Configurações de upload) permite definir metadados e permissões nos arquivos ou na pasta que você está fazendo upload. Marcar a caixa de seleção Make everything public (Tornar tudo público) equivale a configurar as permissões Open/Download (Abrir/fazer download) para Everyone (Todos). Você pode selecionar a opção para usar Armazenamento de redundância reduzida para os arquivos carregados.





Operações de arquivos do Amazon S3AWSToolkit for Visual Studio

Se escolher um arquivo no Amazon S3 visualizar e abrir o menu de contexto (clique com o botão direito do mouse), você poderá realizar diversas operações no arquivo.



Criar pasta

Permite criar uma pasta no bucket atual. (Equivalente a escolher o link Create Folder (Criar pasta).)

Carregar

Permite fazer upload de arquivos ou pastas. (Equivalente a escolher os links Upload File (Fazer upload de arquivo) ou Upload Folder (Fazer upload de pasta).)

Aberto

Tentativas de abrir o arquivo selecionado no navegador padrão. Dependendo do tipo de arquivo e dos recursos do navegador padrão, o arquivo talvez não seja exibido. Ele pode ser simplesmente baixado pelo navegador.

Baixar

Abre uma caixa de diálogo Folder-Tree (Pasta-árvore) pasta permitir o download do arquivo selecionado.

Tornar público

Define permissões no arquivo selecionado para Open/Download (Abrir/fazer download) e Everyone (Todos). (Equivalente a marcar a caixa de seleção Make everything public (Tornar tudo público) na caixa de diálogo Upload Settings (Configurações de upload).)

Excluir

Exclui os arquivos selecionados ou as pastas. Você também pode excluir arquivos ou pastas escolhendo-os e pressionando `Delete`.

Alterar a classe de armazenamento

Define a classe de armazenamento como Standard ou Reduced Redundancy Storage (RRS). Para visualizar a configuração de classe de armazenamento atual, escolha Properties (Propriedades).

Alterara a criptografia

Permite definir criptografia no lado do servidor no arquivo. Para visualizar a configuração de criptografia atual, escolha Properties (Propriedades).

Rename (Renomear)

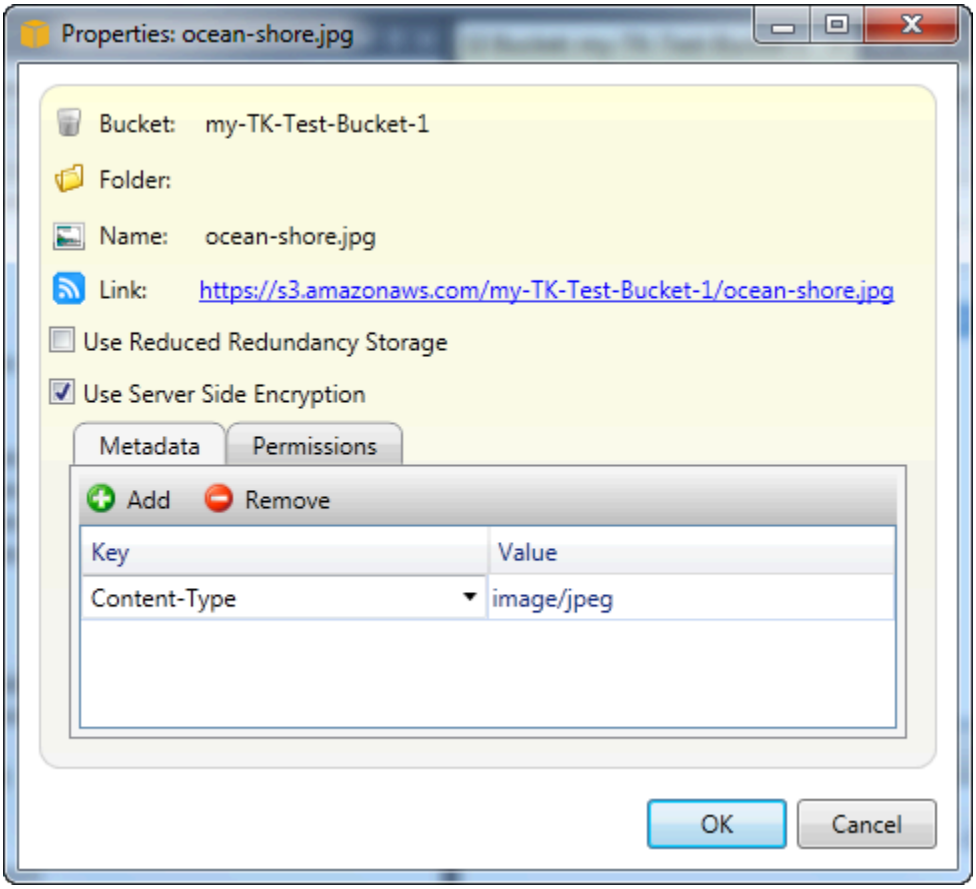
Permite renomear um arquivo. Não é possível renomear uma pasta.

Cortar | Copiar | Colar

Permite recortar, copiar e colar arquivos ou pastas entre pastas ou entre buckets.

Properties

Exibe uma caixa de diálogo que permite definir metadados e permissões para o arquivo, bem como alternar o armazenamento para o arquivo entre Reduced Redundancy Storage (RRS) e Standard, além de definir a criptografia no lado do servidor para o arquivo. Essa caixa de diálogo também exibe um link https para o arquivo. Se você escolher esse link, o Toolkit for Visual Studio abrirá o arquivo no navegador padrão. Se você tiver permissões no arquivo definidas como Open/Download (Abrir/fazer download) e Everyone (Todos), outras pessoas poderão acessar o arquivo por meio desse link. Em vez de distribuir esse link, recomendamos criar e distribuir pre-signed URLs.



Criar Pre-Signed URL

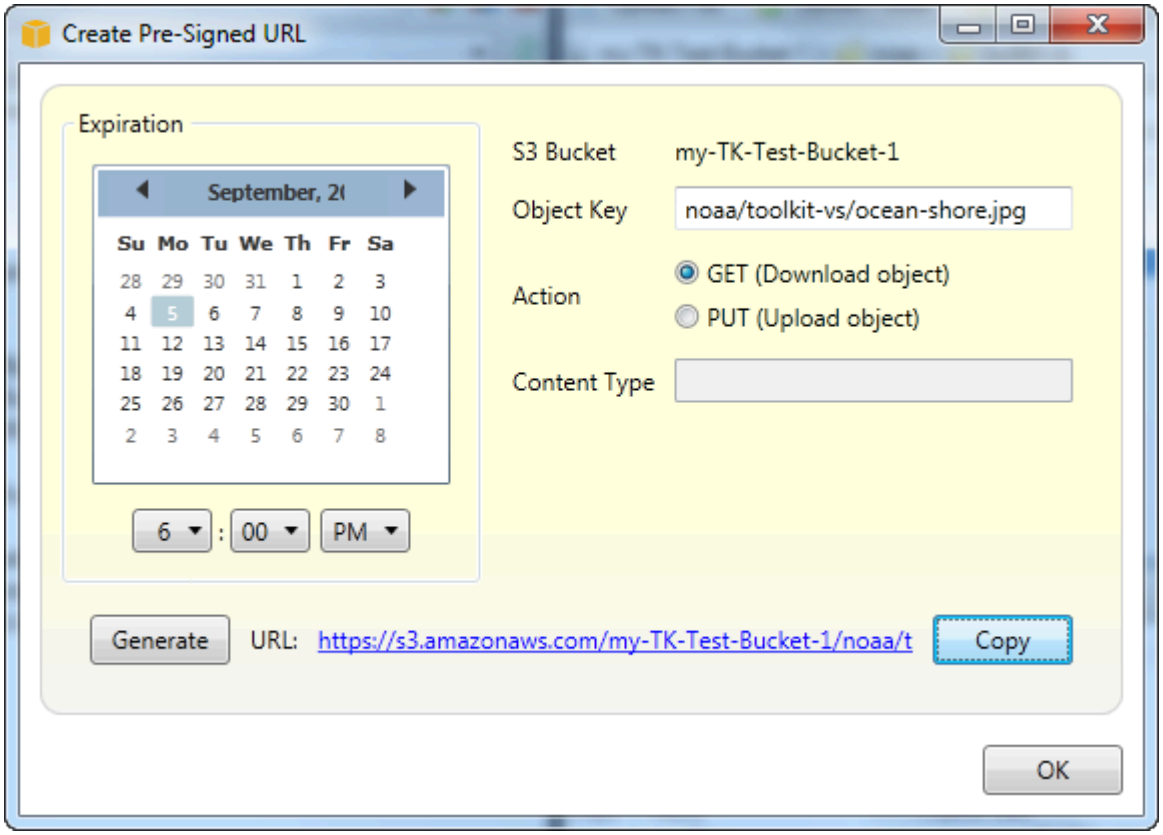
Permite criar um pre-signed URL limitado por tempo que você pode distribuir para permitir que outras pessoas acessem o conteúdo armazenado no Amazon S3.

Como criar um pre-signed URL

Você pode criar um pre-signed URL para um bucket ou arquivos em um bucket. Outras pessoas podem usar esse URL para acessar o bucket ou o arquivo. O URL vai expirar depois de um período especificado ao criar o URL.

Para criar um pre-signed URL

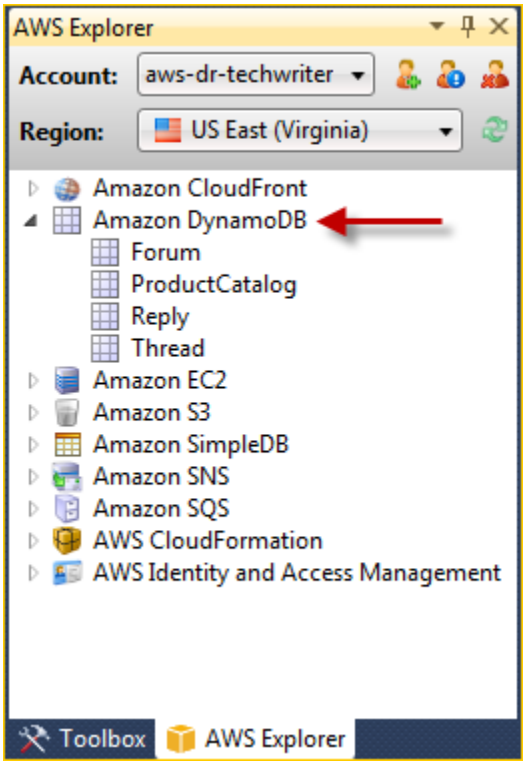
1. Na caixa de diálogo Create Pre-Signed URL (Criar pre-signed URL), defina a data de expiração e a hora do URL. A configuração padrão é uma hora adiante da hora atual.
2. Escolha o botão Generate (Gerar).
3. Para copiar o URL para a área de transferência, escolha Copy (Copiar).



Usar DynamoDB noAWSExplorer

O Amazon DynamoDB é um serviço de banco de dados rápido, altamente disponível, altamente escalável, econômico e não relacional. O DynamoDB remove limitações de escalabilidade tradicionais sobre armazenamento de dados, mantendo, ao mesmo tempo, a baixa latência e o desempenho previsível. O Toolkit for Visual Studio oferece a funcionalidade para trabalhar com o DynamoDB em um contexto de desenvolvimento. Para obter mais informações sobre o DynamoDB, consulteDynamoDBno site da Amazon Web Services.

No Toolkit for Visual Studio,AWSO Explorer exibe todas as tabelas do DynamoDB do associadas ao ativoConta da AWS.



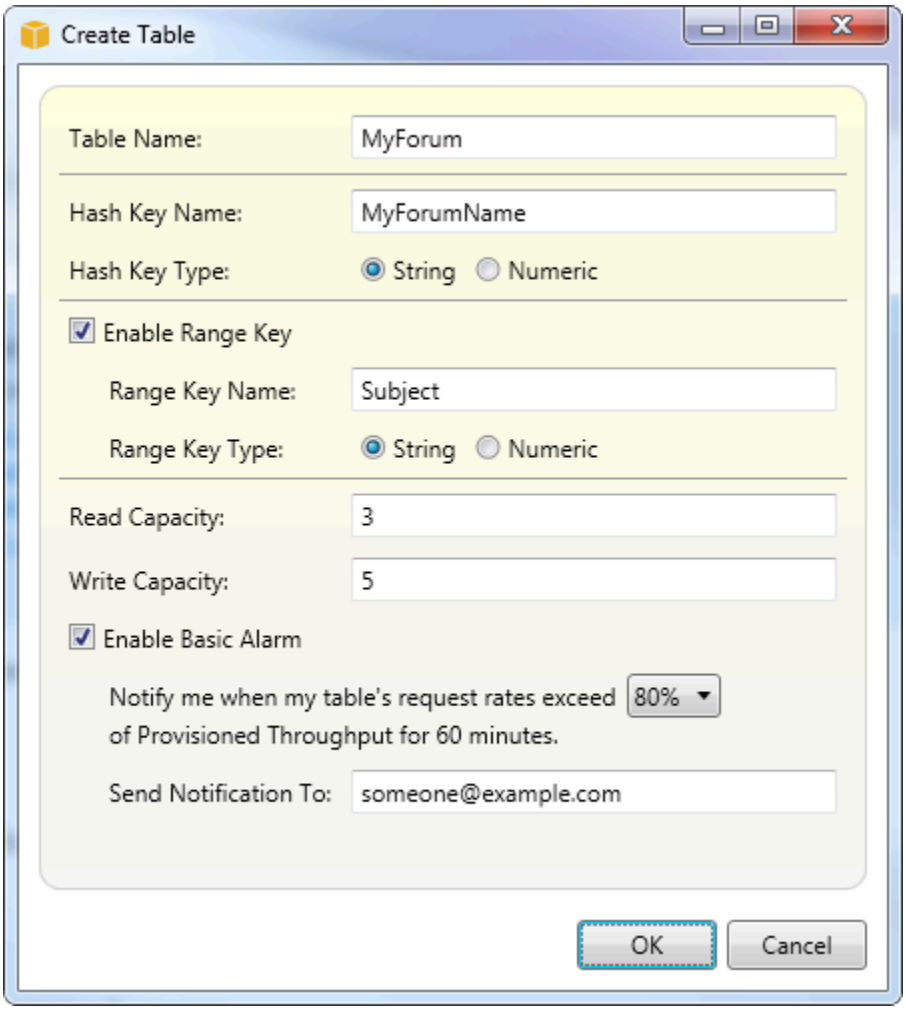
Criação de uma tabela do DynamoDB

Você pode usar o Toolkit for Visual Studio para criar uma tabela do DynamoDB.

Para criar uma tabela noAWSExplorer

1. DentroAWSVisualizar, abra o menu de contexto (clique com o botão direito do mouse)Amazon DynamoDBe, depois, escolhaCriar tabela.
2. No assistente Create Table (Criar tabela), em Table Name (Nome da tabela), digite um nome para a tabela.
3. NoNome da chave de hash, digite um atributo de chave de hash primário e a partir doTipo de chave de hashBotões, escolha o tipo de chave de hash. O DynamoDB compila um índice de hash não classificado usando o atributo de chave primária e um índice de intervalo classificado opcional usando o atributo de chave primária de intervalo. Para obter mais informações sobre o atributo de chave de hash primária, acesseChave primáriana seçãoGuia do desenvolvedor do Amazon DynamoDB.
4. (Opcional) Selecione Enable Range Key (Habilitar chave de intervalo). No campo Range Key Name (Nome da chave de intervalo), digite um atributo de chave de intervalo e, nos botões Range Key Type (Tipo de chave de intervalo), escolha um tipo de chave de intervalo.

5. No campo Read Capacity (Capacidade de leitura), digite o número de unidades de capacidade de leitura. No campo Write Capacity (Capacidade de gravação), digite o número de unidades de capacidade de gravação. Você deve especificar pelo menos três unidades de capacidade de leitura e cinco unidades de capacidade de gravação. Para obter mais informações sobre unidades de capacidade de leitura e gravação, vá até Taxa de transferência provisionada no DynamoDB.
6. (Opcional) Selecione Enable Basic Alarm (Habilitar alarme básico) para alertar quando as taxas de solicitação da tabela estiverem muito altas. Escolha a porcentagem de throughput provisionado por 60 minutos que deve ser excedida antes do envio do alerta. In Send Notifications To (Enviar notificações para), digite um endereço de e-mail.
7. Clique em OK para criar a tabela.

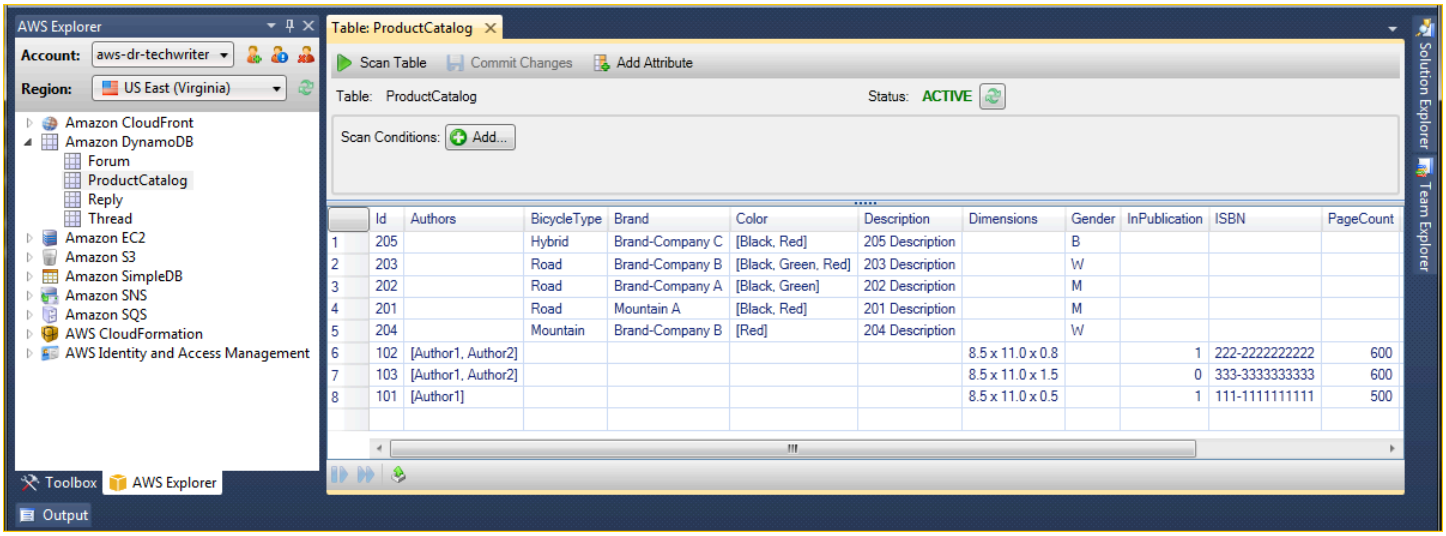


Para obter mais informações sobre tabelas do DynamoDB, acesseConceitos do modelo de dados — tabelas, itens e atributos.

Visualizar uma tabela do DynamoDB como uma grade

Para abrir uma visualização em grade das tabelas do DynamoDB noAWSExplorador, clique duas vezes no subnó correspondente à tabela. Na visualização em grade, você pode visualizar os itens, os atributos e os valores armazenados na tabela. Cada linha corresponde a um item na tabela. As colunas da tabela correspondem aos atributos. Cada célula da tabela mantém os valores associados a esse atributo do item.

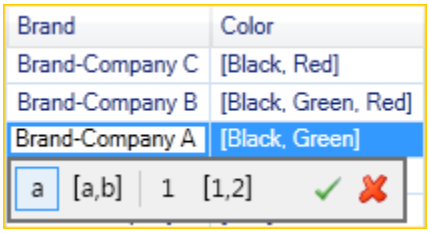
Um atributo pode ter um valor que seja uma string ou um número. Alguns atributos têm um valor que consiste em um conjunto de strings ou números. Os valores definidos são exibidos como uma lista separada por vírgulas entre colchetes.



	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

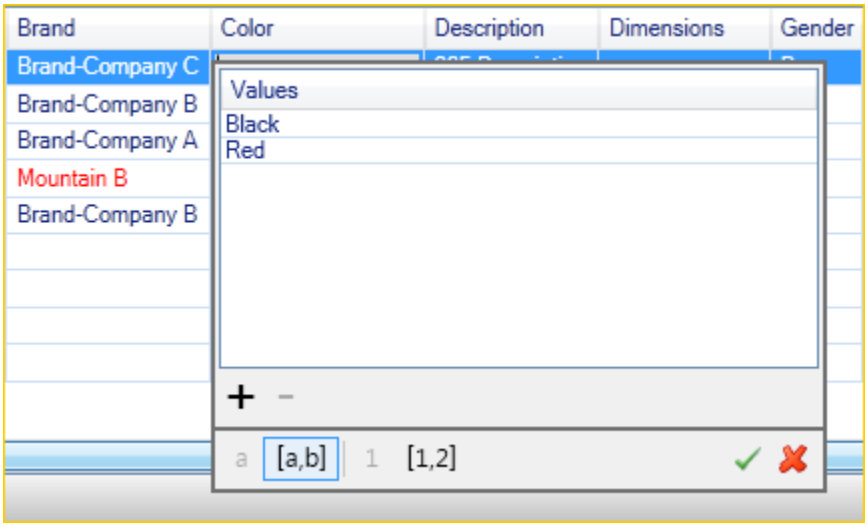
Editar e adicionar atributos e valores

Clicando duas vezes em uma célula, você pode editar os valores do atributo correspondente do item. Para atributos set-value, você também pode adicionar ou excluir valores individuais do conjunto.



Além de alterar o valor de um atributo, você também pode, com algumas limitações, alterar o formato do valor de um atributo. Por exemplo, um valor de qualquer número pode ser convertido em um valor de string. Se você tiver um valor de string, cujo conteúdo seja um número, como 125, o editor de células permitirá converter o formato do valor de string em número. Você também pode converter um

single-value em um set-value. No entanto, você normalmente não pode converter de um set-value em um single-value; uma exceção é quando o set-value tem, na verdade, apenas um elemento no conjunto.

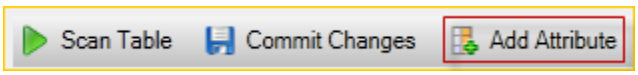


Depois de editar o valor do atributo, escolha a marca de seleção verde para confirmar as alterações. Se você quiser descartar as alterações, escolha o X vermelho.

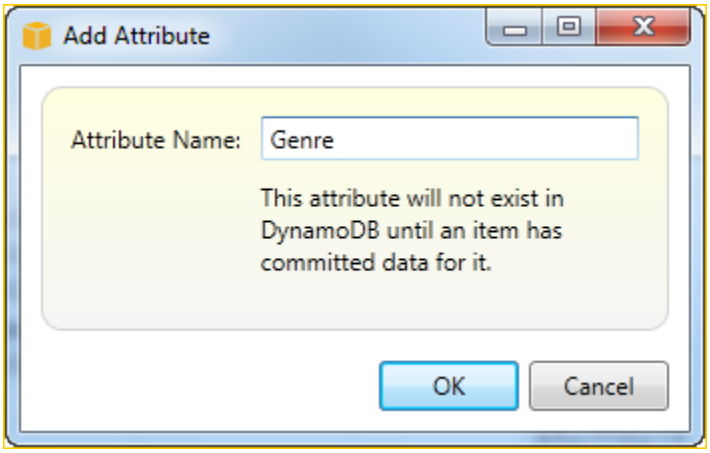
Depois que você tiver confirmado as alterações, o valor do atributo será exibido em vermelho. Isso indica que o atributo foi atualizado, mas que o novo valor não foi regravado no banco de dados do DynamoDB. Para regravar as alterações no DynamoDB, escolhaAlterações de confirmação. Para descartar as alterações, escolha Scan Table (Varrer tabela) e, quando o Toolkit perguntar se você gostaria de confirmar as alterações antes da varredura, escolha No (Não).

Como adicionar um atributo

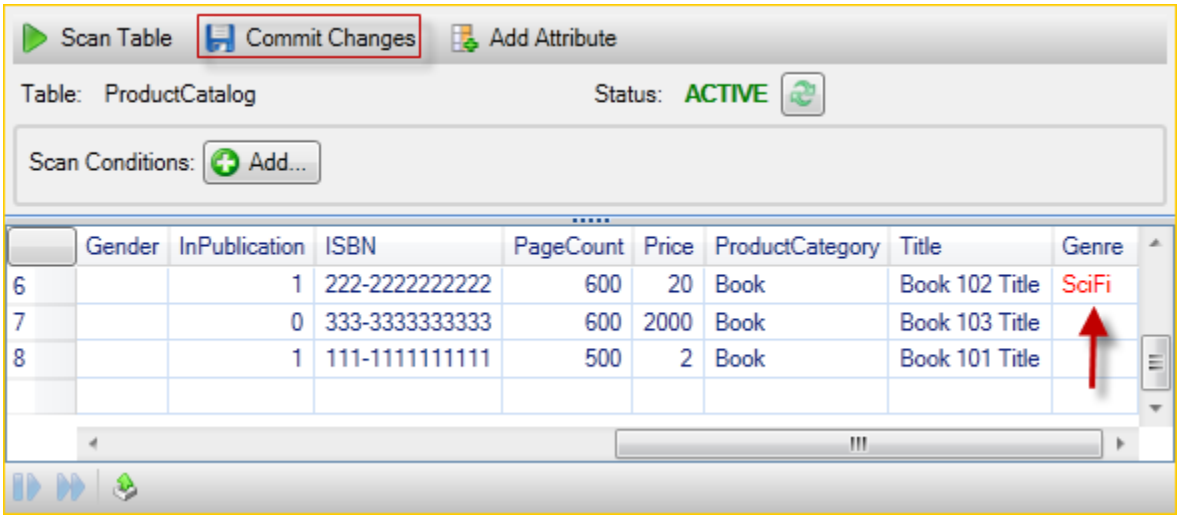
Na visualização em grade, você também pode adicionar atributos à tabela. Para adicionar um novo atributo, escolha Add Attribute (Adicionar atributo).



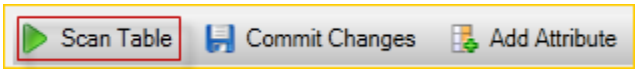
Na caixa de diálogo Add Attribute (Adicionar atributo), digite um nome para o atributo e escolha OK.



Para tornar o novo atributo parte da tabela, você deve adicionar um valor a ela para pelo menos um item e escolher o botão Commit Changes (Confirmar alterações). Para descartar o novo atributo, basta fechar a visualização em grade da tabela sem escolher Commit Changes (Confirmar alterações).



Verificar uma tabela do DynamoDB

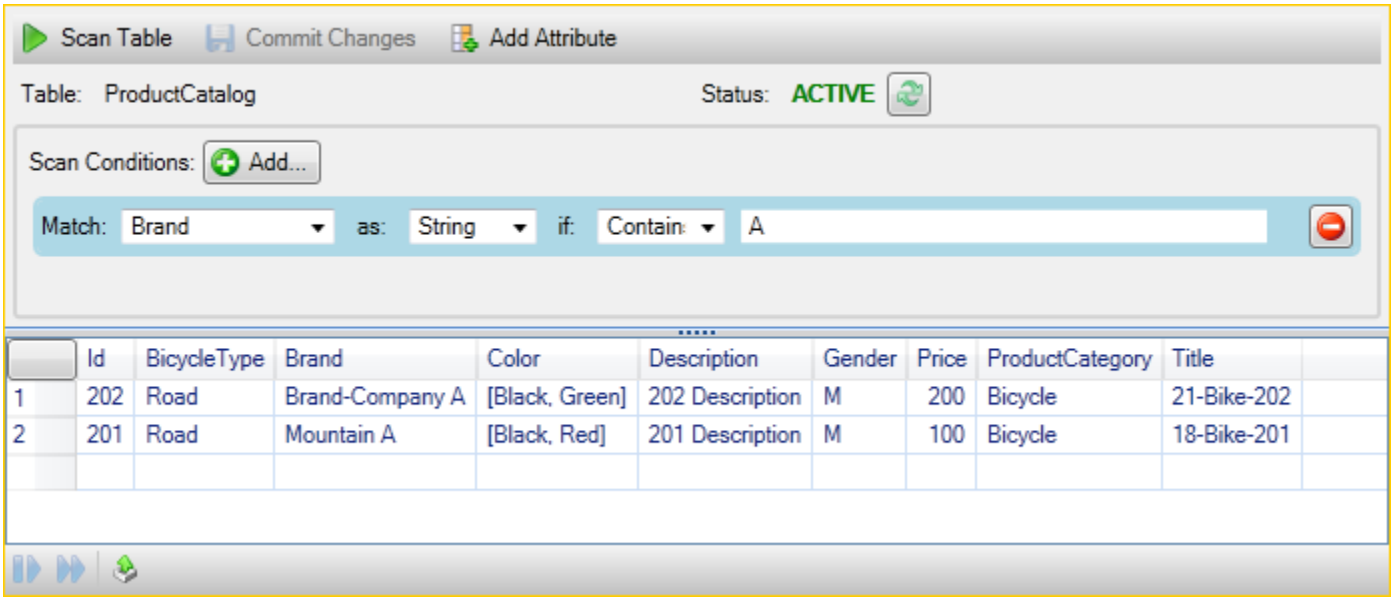


Você pode realizar varreduras nas tabelas do DynamoDB no Toolkit. Em uma varredura, você define um conjunto de critérios e a varredura retorna todos os itens da tabela correspondentes aos critérios. As varreduras são operações caras e devem ser usadas com cuidado para evitar interromper um tráfego de produção de prioridade maior na tabela. Para obter mais informações sobre como usar a operação de varredura, acesseGuia do desenvolvedor do Amazon DynamoDB.

Para realizar uma varredura em uma tabela do DynamoDB noAWSExplorer

1. Na visualização em grade, escolha o botão scan conditions: add (modificações de varredura: adicionar).
2. No editor de cláusulas de varredura, escolha o atributo correspondente, como o valor do atributo deve ser interpretado (string, número, valor definido), como ele deve ser analisado (por exemplo, Começa com ou Contém) e o valor literal correspondente.
3. Adicione mais cláusulas de varredura, conforme necessário, para a pesquisa. A varredura só retornará os itens correspondentes aos critérios de todas as cláusulas de varredura. A varredura realizará uma comparação diferenciando maiúsculas de minúsculas em relação a valores de string.
4. Na barra de botões na parte superior da visualização em grade, escolha Scan Table (Varrer tabela).

Para remover uma cláusula de varredura, escolha o botão vermelho com a linha branca à direita de cada cláusula.



Para retornar à visualização da tabela que inclui todos os itens, remova todas as cláusulas de varredura e escolha Scan Table (Varrer tabela) novamente.

Paginar resultados da varredura

Na parte inferior da visualização, existem três botões.

Os dois primeiros botões azuis fornecem paginação para resultados da varredura. O primeiro botão exibirá uma página adicional de resultados. O segundo botão exibirá dez páginas adicionais de resultados. Neste contexto, uma página é igual a 1 MB de conteúdo.

Exportar o resultado da varredura para CSV

O terceiro botão exporta os resultados da varredura atual para um arquivo CSV.

O uso doAWS CodeCommitCom o Visual Studio Team Explorer

Você pode usarAWS Identity and Access ManagementContas de usuário (IAM) para criar credenciais do Git e usá-las para criar e clonar repositórios dentro do Team Explorer.

Tipos de credencial do AWS CodeCommit

A maioriaAWS Toolkit for Visual Studioos usuários estão cientes da configuraçãoAWSOs perfis de credencial que contêm as chaves de acesso e secretas. Esses perfis de credencial são usados no Toolkit for Visual Studio para permitir as chamadas a APIs de serviço, por exemplo, para listar buckets do Amazon S3 emAWSExplorer ou executar uma instância do Amazon EC2. A integração do AWS CodeCommit com o Team Explorer também usa esses perfis de credencial. No entanto, para trabalhar com o Git propriamente dito, você precisa de credenciais adicionais, especificamente, as credenciais do Git para conexões HTTPS. Você pode ler sobre essas credenciais (um nome de usuário e senha) emConfiguração para usuários de HTTPS usando credenciais do GitnoAWS CodeCommitGuia do usuário do.

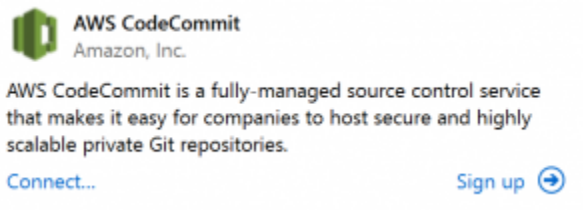
Você pode criar as credenciais do Git paraAWS CodeCommitsomente para contas de usuário do IAM. Você não pode criá-las para uma conta raiz. Você pode criar até dois conjuntos dessas credenciais para o serviço e, embora possa marcar um conjunto de credenciais como inativo, os conjuntos inativos continuam contando para o limite de dois conjuntos. Você pode excluir e recriar credenciais a qualquer momento. Quando você usaAWS CodeCommitde dentro do Visual Studio, seu tradicionalAWSAs credenciais são usadas para trabalhar com o serviço propriamente dito, por exemplo, quando você está criando e listando repositórios. Trabalhando com os repositórios do Git reais hospedados no AWS CodeCommit, você deve usar as credenciais do Git.

Como parte do suporte paraAWS CodeCommit, o Toolkit for Visual Studio cria e gerencia automaticamente essas credenciais do Git para você e os associa aoAWSPerfil de credencial. Você não precisa se preocupar em ter conjunto certo de credenciais à disposição para realizar operações do Git dentro do Team Explorer. Depois de se conectar ao Team Explorer com seuAWSO perfil de

credencial, as credenciais do Git associadas são usadas automaticamente sempre que você trabalha com um Git remoto.

Como conectar-se ao AWS CodeCommit

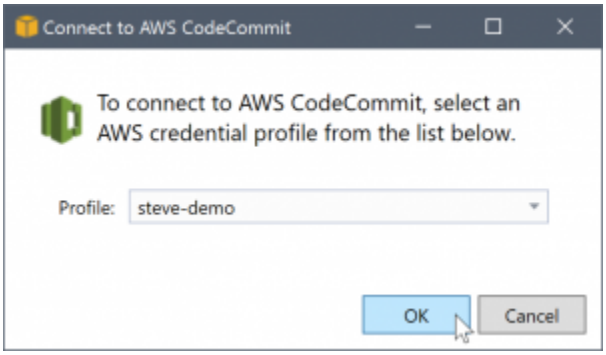
Ao abrir a janela Team Explorer no Visual Studio de 2015 ou posterior, você verá uma entrada do AWS CodeCommit na seção Hosted Service Providers de Manage Connections.



EscolhendoCadastrar-seAbre a página inicial da Amazon Web Services em uma janela do navegador. O que acontece quando você escolherConecte-seDepende se o Toolkit for Visual Studio pode encontrar um perfil de credencial comAWSchaves de acesso e secretas para permitir que ele faça chamadas paraAWSEm seu nome. Você pode configurar um perfil de credencial usando a nova página Getting Started exibida no IDE quando o Toolkit for Visual Studio não consegue encontrar credenciais armazenadas localmente. Ou você pode ter usado o Toolkit for Visual Studio, oAWS Tools for Windows PowerShell, ou oAWS CLIe já temAWSOs perfis de credencial disponíveis para o Toolkit for Visual Studio usar.

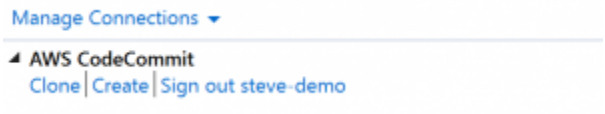
Quando você escolherConecte-se, o Toolkit for Visual Studio inicia o processo para encontrar um perfil de credencial a ser usado na conexão. Se o Toolkit for Visual Studio não conseguir encontrar um perfil de credencial, ele abrirá uma caixa de diálogo convidando você a inserir as chaves de acesso e secretas para oConta da AWS. É altamente recomendável usar uma conta de usuário do IAM, e não as credenciais raiz. Além disso, conforme observado anteriormente, as credenciais do Git de que você precisará só podem ser criadas para usuários do IAM. Assim que as chaves de acesso e secretas forem fornecidas e o perfil de credencial for criado, a conexão entre o Team Explorer e o AWS CodeCommit estará pronta para ser usada.

Se o Toolkit for Visual Studio encontrar mais de umAWSO perfil de credencial é solicitado a selecionar a conta que deseja usar dentro do Team Explorer.



Se tiver apenas um perfil de credencial, o Toolkit for Visual Studio ignorará a caixa de diálogo de seleção do perfil e você será conectado imediatamente:

Quando uma conexão é estabelecida entre o Team Explorer e o AWS CodeCommit por meio dos perfis de credencial, a caixa de diálogo de convite é fechada e o painel de conexão é exibido.

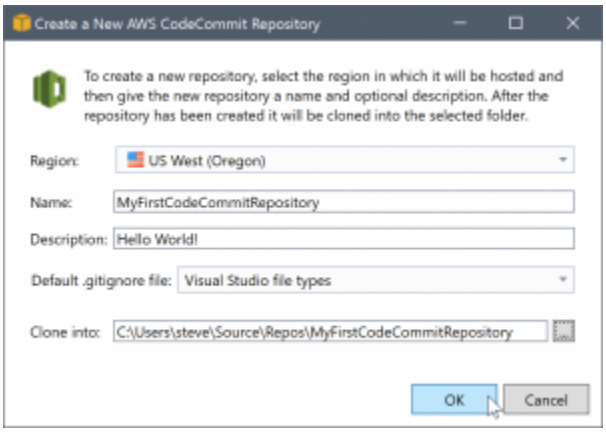


Como você não tem repositórios clonados localmente, o painel mostra apenas as operações que você pode executar: Clone,Criar, eSign out. Como outros provedores,AWS CodeCommitNo Team Explorer só pode ser vinculado a umAWSO perfil de credencial em um determinado momento. Para alternar contas, use Sign out (Sair) para remover a conexão, de maneira que possa iniciar uma nova conexão usando uma conta diferente.

Agora que estabeleceu uma conexão, você pode criar um repositório clicando no link Create (Criar).

Criação de um repositório

Quando você clica noCriarlink, oCriar um novoAWS CodeCommitRepositórioA caixa de diálogo é aberta.



Os repositórios do AWS CodeCommit são organizados por região. Assim, em Region (Região), você pode selecionar a região na qual hospedar o repositório. A lista tem todas as regiões nas quais o AWS CodeCommit é compatível. Você fornece o nome (obrigatório) e a descrição (opcional) para o novo repositório.

O comportamento padrão da caixa de diálogo é de sufixo do local da pasta para o novo repositório com o nome do repositório (à medida que você insere o nome, o local da pasta também se atualiza). Para usar um nome de pasta diferente, edite o caminho da pasta Clone into (Clonar para) depois de terminar de inserir o nome do repositório.

Você também pode optar por criar automaticamente um arquivo `.gitignore` inicial para o repositório. O AWS Toolkit for Visual Studio fornece um padrão incorporado para tipos de arquivo do Visual Studio. Você também pode optar por não ter arquivo algum ou usar um arquivo existente personalizado que gostaria de reutilizar em todos os repositórios. Basta selecionar Use custom (Usar personalizado) na lista e navegue até o arquivo personalizado a ser usado.

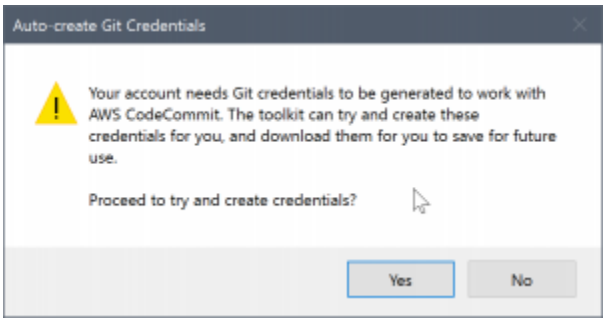
Assim que tiver um nome de repositório e um local, você estará pronto para clicar em OK e começar a criar o repositório. O Toolkit for Visual Studio solicita que o serviço crie o repositório e acabe clonando o novo repositório localmente, adicionando uma confirmação inicial para o arquivo .gitignore, caso você esteja usando um. É nesse ponto que você começa a trabalhar com o Git remoto, de maneira que o Toolkit for Visual Studio precise de acesso às credenciais do Git descritos anteriormente.

Configurar credenciais do Git

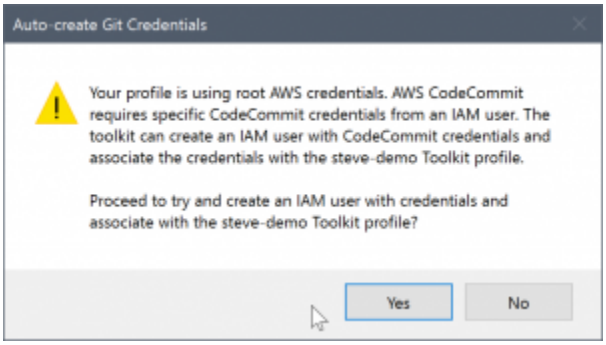
Até este ponto você tem usadoAWSAs chaves de acesso e secretas para solicitar que o serviço crie o repositório. Agora você precisa trabalhar com o Git propriamente dito para fazer a operação de clonagem real, e o Git não compreendeAWSchaves de acesso e secretas. Em vez disso, você precisa fornecer as credenciais de nome do usuário e senha ao Git a ser usado em uma conexão HTTPS com o remoto.

Conforme observado em Configurar credenciais do Git, as credenciais do Git que você usará devem ser associadas a um usuário do IAM. Você não pode gerá-las para credenciais raiz. Você deve sempre configurar oAWSOs perfis de credencial para conter chaves de acesso de usuário e secretas do IAM, e não chaves raiz. O Toolkit for Visual Studio pode tentar configurar as credenciais do Git paraAWS CodeCommitpara você, e associe-os com oAWSperfil de credencial usado para se conectar no Team Explorer anteriormente.

Quando você escolherOKnoCriar um novoAWS CodeCommitRepositóriocaixa de diálogo e criar o repositório com êxito, o Toolkit for Visual Studio verifica aAWSperfil de credencial conectado no Team Explorer para determinar se credenciais do Git paraAWS CodeCommitexistem e estão associados localmente ao perfil. Nesse caso, o Toolkit for Visual Studio instrui o Team Explorer a iniciar a operação de clonagem no novo repositório. Se as credenciais do Git não estiverem disponíveis localmente, o Toolkit for Visual Studio verificará o tipo de credenciais de conta que foram usadas na conexão com o Team Explorer. Se as credenciais se destinarem a um usuário do IAM, conforme recomendamos, a mensagem a seguir será mostrada.

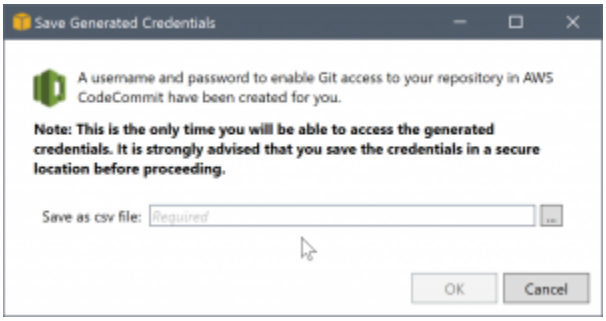


Se as credenciais forem credenciais raiz, a mensagem a seguir será mostrada em seu lugar.



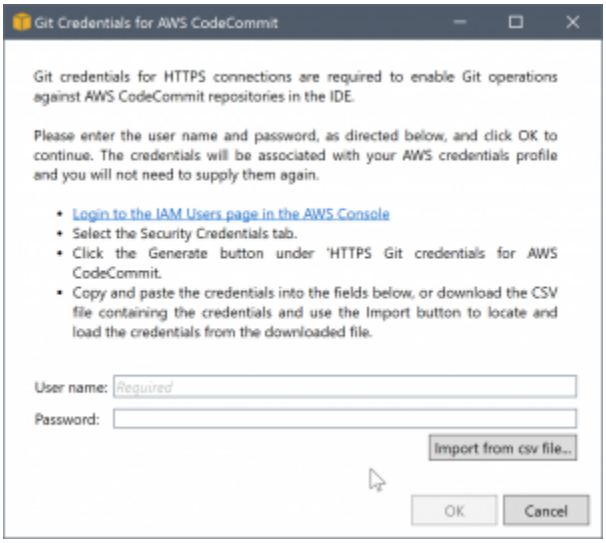
Em ambos os casos, o Toolkit for Visual Studio se oferece para tentar fazer o trabalho para criar as credenciais do Git necessárias para você. No primeiro cenário, tudo o que precisa ser feito é criar um conjunto de credenciais do Git para o usuário do IAM. Quando uma conta raiz estiver em uso, o Toolkit for Visual Studio tentará primeiramente criar um usuário do IAM e avançar à criação de credenciais do Git para esse novo usuário. Se o Toolkit for Visual Studio precisar criar um novo usuário, ele aplicará aAWS CodeCommitPolítica gerenciada pelo usuário avançado para essa nova conta de usuário. Essa política só permite acesso ao AWS CodeCommit e permite que todas as operações sejam realizadas com o AWS CodeCommit, exceto a exclusão do repositório.

Quando estiver criando credenciais, você só poderá visualizá-las uma vez. Portanto, o Toolkit for Visual Studio solicita salvar as credenciais recém-criadas como um `.csv`Arquivo antes de continuar.



Isso também é algo altamente recomendável, e não se esqueça de salvá-las em um local seguro!

Pode haver casos em que o Toolkit for Visual Studio não consiga criar automaticamente as credenciais. Por exemplo, você já pode ter criado o número máximo de conjuntos de credenciais do Git paraAWS CodeCommit(dois) ou não ter direitos programáticos suficientes para o Toolkit for Visual Studio para fazer o trabalho (se você tiver feito login como um usuário do IAM). Nesses casos, você pode fazer login noAWS Management ConsolePara gerenciar as credenciais ou obtê-las junto ao administrador. Em seguida, você pode inseri-los noCredenciais do Git paraAWS CodeCommitA caixa de diálogo, exibida pelo Toolkit for Visual Studio.

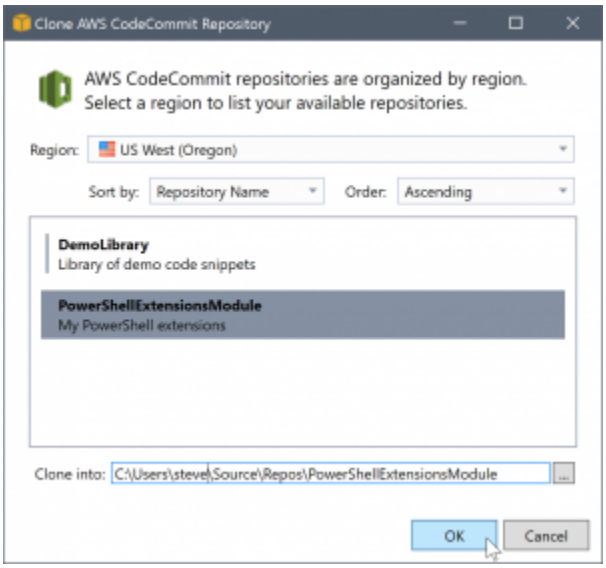


Agora que as credenciais do Git estão disponíveis, a operação de clonagem do novo repositório continua (consulte a indicação do progresso da operação dentro do Team Explorer). Se você tiver optado por aplicar um arquivo `.gitignore` padrão, ele será confirmado para o repositório com um comentário 'Initial Commit'.

Isso é tudo para configurar credenciais e criar um repositório dentro do Team Explorer. Assim que as credenciais necessárias forem implantadas, tudo o que você verá ao criar novos repositórios no futuro será oCriar um novoAWS CodeCommitRepositórioCaixa de diálogo propriamente dito.

Clonar um repositório

Para clonar um repositório existente, retorne ao painel de conexão do AWS CodeCommit no Team Explorer. Clique no ícone da barra de ferramentasClonelink para abrir oCloneAWS CodeCommitRepositórioA caixa de diálogo e selecione o repositório a ser clonado e o local no disco onde você deseja colocá-lo.



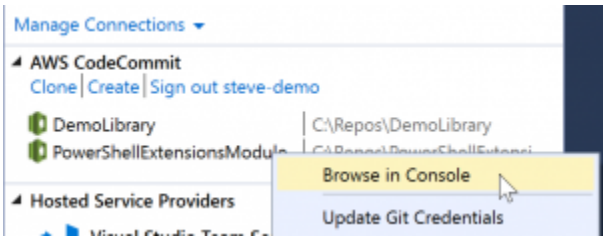
Assim que você escolher a região, o Toolkit para o Visual Studio consultará o serviço para descobrir os repositórios disponíveis na região e exibi-los na parte da lista central da caixa de diálogo. O nome e a descrição opcional de cada repositório também são exibidos. Você pode reorganizar a lista para classificá-la por nome de repositório ou pela data da última modificação e classificar cada uma em ordem crescente ou decrescente.

Assim que selecionar o repositório, você poderá escolher o local para clonagem. O padrão é o mesmo local de repositório usado em outros plug-ins para o Team Explorer, mas você pode procurar ou inserir qualquer outro local. Por padrão, o nome do repositório é incluído como sufixo no caminho selecionado. No entanto, se você quiser um caminho específico, bastará editar a caixa de texto depois de selecionar a pasta. Todo o texto na caixa quando você clicar em OK será a pasta na qual encontrará o repositório clonado.

Tendo selecionado o repositório e uma pasta local, você acaba clicando em OK para continuar a operação de clonagem. Assim como acontece com a criação de um repositório, você pode ver o progresso da operação de clonagem informada no Team Explorer.

Trabalhar com repositórios do

Quando você clona ou cria repositórios, observe que os repositórios locais da conexão estão listados no painel de conexão no Team Explorer nos links da operação. Essas entradas dão a você uma maneira prática de acessar o repositório para procurar conteúdo. Basta clicar com o botão direito do mouse no repositório e escolher Browse in Console (Navegar no console).



Você também pode usar Update Git Credentials (Atualizar credenciais do Git) para atualizar as credenciais do Git armazenadas associadas ao perfil de credencial. Isso será útil se você tiver girado as credenciais. O comando abre oCredenciais do Git paraAWS CodeCommitCaixa de diálogo onde você pode inserir ou importar as novas credenciais.

As operações do Git nos repositórios funcionam como você esperaria. Você pode fazer confirmações locais e, quando estiver pronto para compartilhar, usar a opção Sync no Team Explorer. Porque as credenciais do Git já estão armazenadas localmente e associadas ao nosso conectadoAWSO perfil de credencial não será solicitado a fornecê-las novamente para operações em relação aoAWS CodeCommitremoto.

Usando o CodeArtifact no Visual Studio

AWS CodeArtifactO é um serviço de repositório de artefatos totalmente gerenciado que ajuda as organizações a armazenar e compartilhar pacotes de software usados para desenvolvimento de aplicativos. Você pode usar o CodeArtifact com ferramentas de compilação populares e gerenciadores de pacotes, como NuGet e .NET Core CLIs e Visual Studio. Você também pode configurar o CodeArtifact para extrair pacotes de um repositório público externo, comoNuGet.org.

No CodeArtifact, seus pacotes são armazenados em repositórios que são armazenados em um domínio. OAWS Toolkit for Visual Studiosimplifica a configuração do Visual Studio com seus repositórios CodeArtifact, facilitando o consumo de pacotes no Visual Studio a partir do CodeArtifact diretamente e do NuGet.org.

Adicione seu repositório CodeArtifact como uma fonte de pacote NuGet

Para consumir pacotes de seu CodeArtifact, você precisará adicionar seu repositório como uma fonte de pacote naGerenciador de pacotes NuGetno Visual Studio

Para adicionar seu repositório como fonte de pacote

1. DentroAWSExplorer, navegue até o repositório noAWS CodeArtifactNó.
2. Abra o menu de contexto (clique com o botão direito do mouse) do repositório que você deseja adicionar e escolhaEndpoint de código-fonte do NuGet.
3. Navegue atéOrigens de pacotedebaixo doGerenciador de pacotes NuGetNó do noFerramentas > Opçõesmenu.
4. DentroOrigens de pacoteSelecione o sinal de adição (+), edite o nome e cole o URL do endpoint de origem do NuGet que você copiou anteriormente noOrigemcampo.
5. Marque a caixa de seleção ao lado da fonte de pacote recém-adicionada para habilitá-la.

> **Note**
>
> Recomendamos adicionar uma conexão externa aoNuGet.orgpara o seu CodeArtifact e desabilitando onuget.orgcódigo-fonte do pacote no Visual Studio. Ao usar uma conexão externa, todas as dependências foram retiradasNuGet.orgsão armazenados em CodeArtifact. SeNuGet.orgcai por qualquer motivo, os pacotes que você precisa ainda estarão disponíveis. Para obter mais informações sobre conexões externas, consulteAdicionar uma conexão externanoAWS CodeArtifactGuia do usuário do.

6. SelecioneOKpara fechar o menu.

Para obter mais informações sobre como usar o CodeArtifact com o Visual Studio, consulteUse o CodeArtifact com o Visual StudionoAWS CodeArtifactGuia do usuário do.

Amazon RDS deAWSExplorer

O Amazon Relational Database Service (Amazon RDS) é um serviço que permite provisionar e gerenciar sistemas de banco de dados relacional do SQL na nuvem. O Amazon RDS dá suporte a três tipos de sistemas de banco de dados:

- MySQL Community Edition

- Oracle Database Enterprise Edition
- Microsoft SQL Server (edições Express, Standard ou Web)

Para obter mais informações, consulte o Guia do usuário do Amazon RDS.

Muitas das funcionalidades abordadas aqui também são disponibilizadas por meio doAWSManagement Consolepara Amazon RDS.

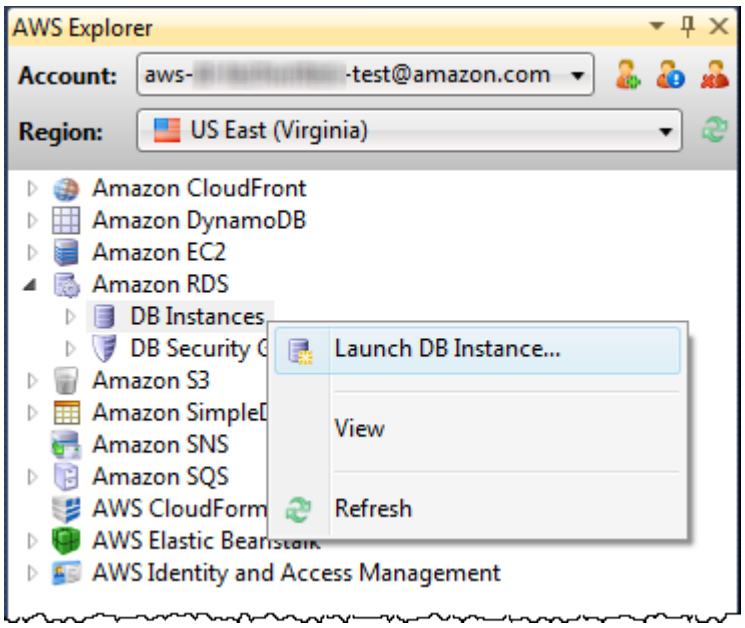
Tópicos

Iniciar uma instância de banco de dados do Amazon RDS

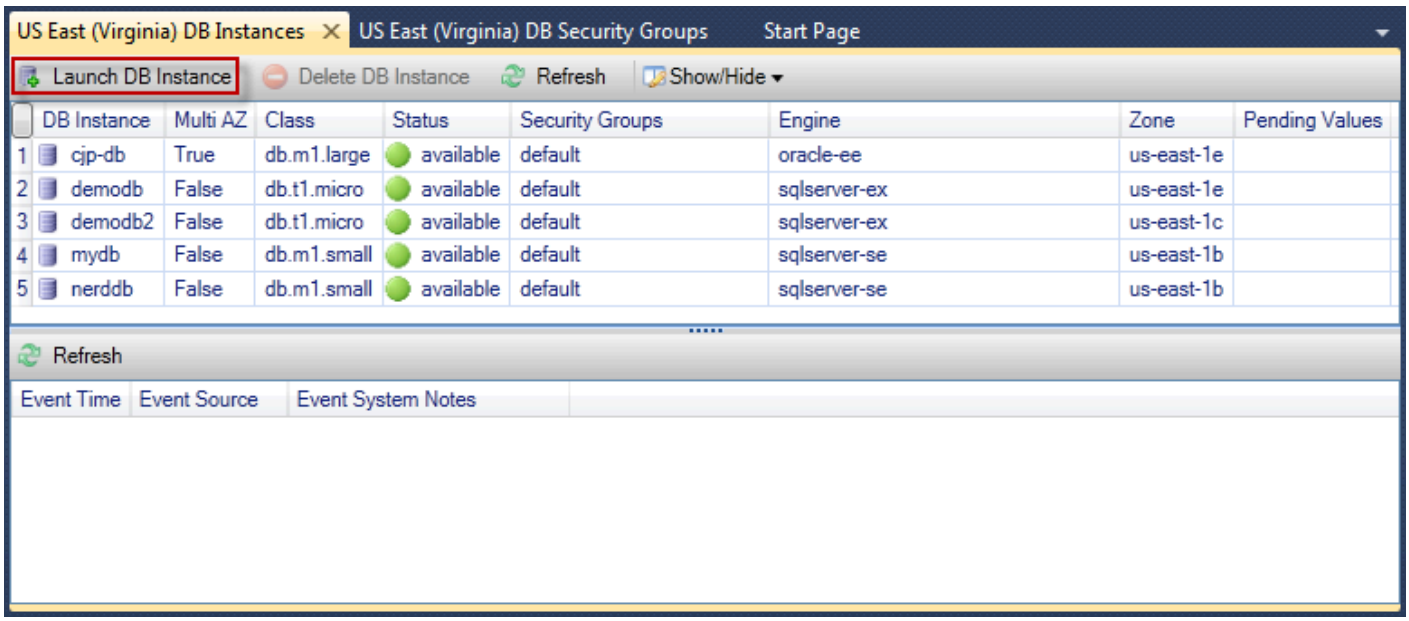
comAWSExplorador, você pode executar uma instância de qualquer um dos mecanismos de banco de dados compatíveis com o Amazon RDS. A descrição a seguir mostra a experiência do usuário para executar uma instância do Microsoft SQL Server Standard Edition, mas a experiência do usuário é semelhante em todos os mecanismos compatíveis.

Para executar uma instância do Amazon RDS

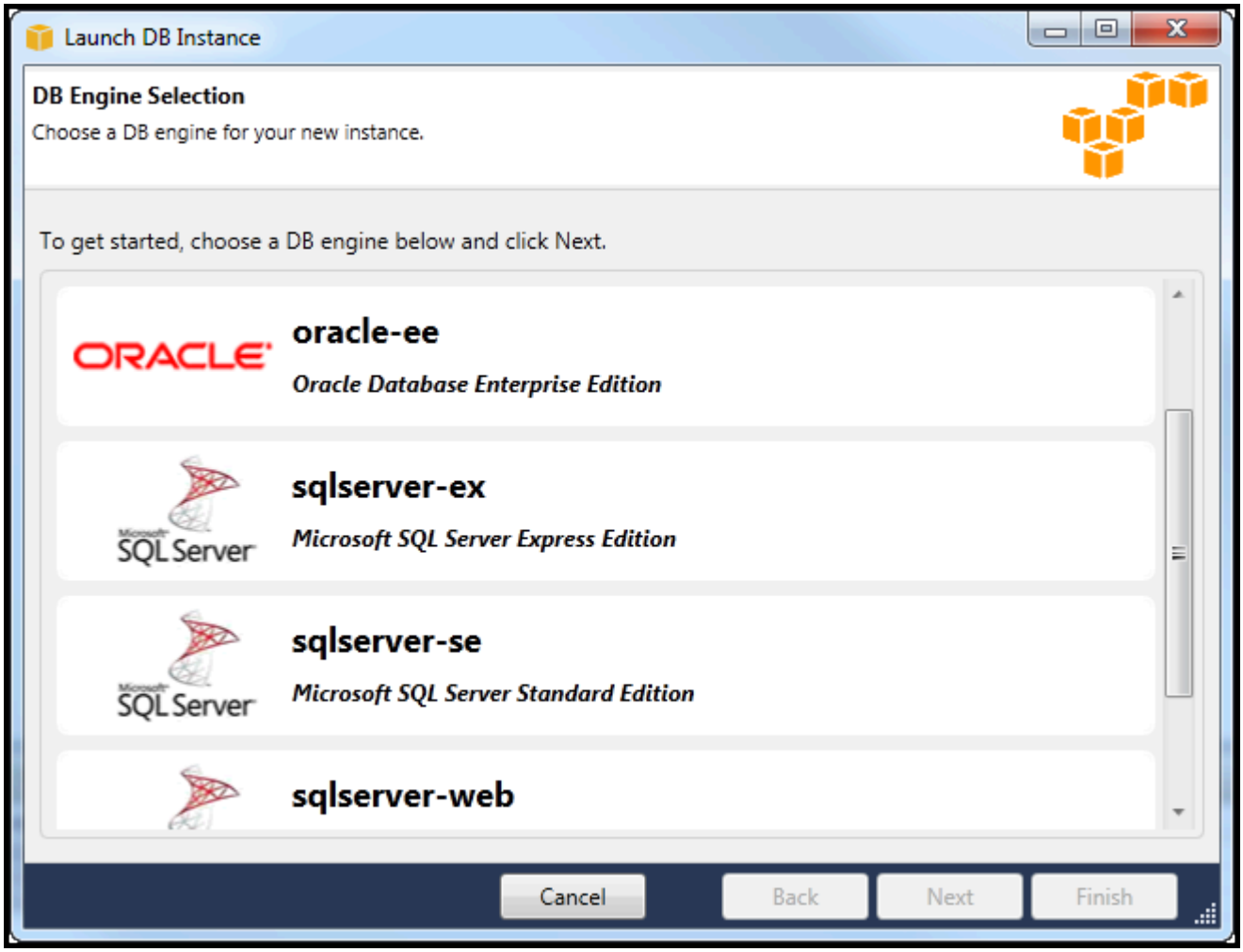
1. DentroAWSExplorer, abra o menu de contexto (clique com o botão direito do mouse) doAmazon RDSnó e escolhaExecutar instância de banco.



Como alternativa, na guia DB Instances (Instâncias de banco de dados), escolha Launch DB Instance (Executar instância de banco de dados).



2. Na caixa de diálogo DB Engine Selection (Seleção do mecanismo de banco de dados), escolha o tipo de mecanismo de banco de dados a ser iniciado. Para esta descrição, escolha o Microsoft SQL Server Standard Edition (sqlserver-se) e Next (Próximo).



3. Na caixa de diálogo DB Engine Instance Options (Opções de instância do mecanismo de banco de dados), escolha as opções de configuração.

   Na seção DB Engine Instance Options and Class (Opções e classe de instância do mecanismo de banco de dados), você pode especificar as seguintes configurações:

   Modelo de licença

Tipo de mecanismo	License (Licença)
Microsoft SQL Server	license-included
MySql	general-public-license
Oracle	bring-your-own-license

O modelo de licença varia de acordo com o tipo de mecanismo de banco de dados. Engine Type License Microsoft SQL Server license-included MySql general-public-license Oracle bring-your-own-license

Versão da instância de banco de dados

Escolha a versão do mecanismo de banco de dados que você gostaria de usar. Se apenas uma versão for compatível, ela será selecionada para você.

Classe da instância de banco de dados

Escolha a classe de instância do mecanismo de banco de dados. A definição de preço das classes de instância varia. Para obter mais informações, consulte Definição de preço do Amazon RDS.

Realizar uma implantação Multi AZ

Selecione essa opção a fim de criar uma implantação Multi-AZ é ativada para durabilidade e disponibilidade de dados avançadas. O Amazon RDS provisiona e mantém uma cópia reserva do banco de dados em uma zona de disponibilidade diferente para failover automático em caso de uma paralisação programada ou não planejada. Para obter informações sobre a definição de preço para implantações Multi-AZ, consulte a seção de definição de preço da página de detalhes Amazon RDS. Essa opção não é compatível com o Microsoft SQL Server.

Atualizar versões secundárias automaticamente

Selecione esta opção para terAWSExecutar automaticamente atualizações da versão secundária nas instâncias do RDS para você.

Na seção RDS Database Instance (Instância de banco de dados do RDS), você pode especificar as configurações a seguir.

Allocated Storage (Armazenamento alocado)

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

Mecanismo	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

Os mínimos e os máximos para armazenamento alocado dependem do tipo de mecanismo de banco de dados. Engine Minimum (GB) Maximum (GB) MySQL 5 1024 Oracle Enterprise Edition 10 1024 Microsoft SQL Server Express Edition 30 1024 Microsoft SQL Server Standard Edition 250 1024 Microsoft SQL Server Web Edition 30 1024

DB Instance Identifier

Especifique um nome para a instância de banco de dados. Esse nome não diferencia maiúsculas de minúsculas. Ele será exibido em minúsculas emAWSExplorador.

Master User Name

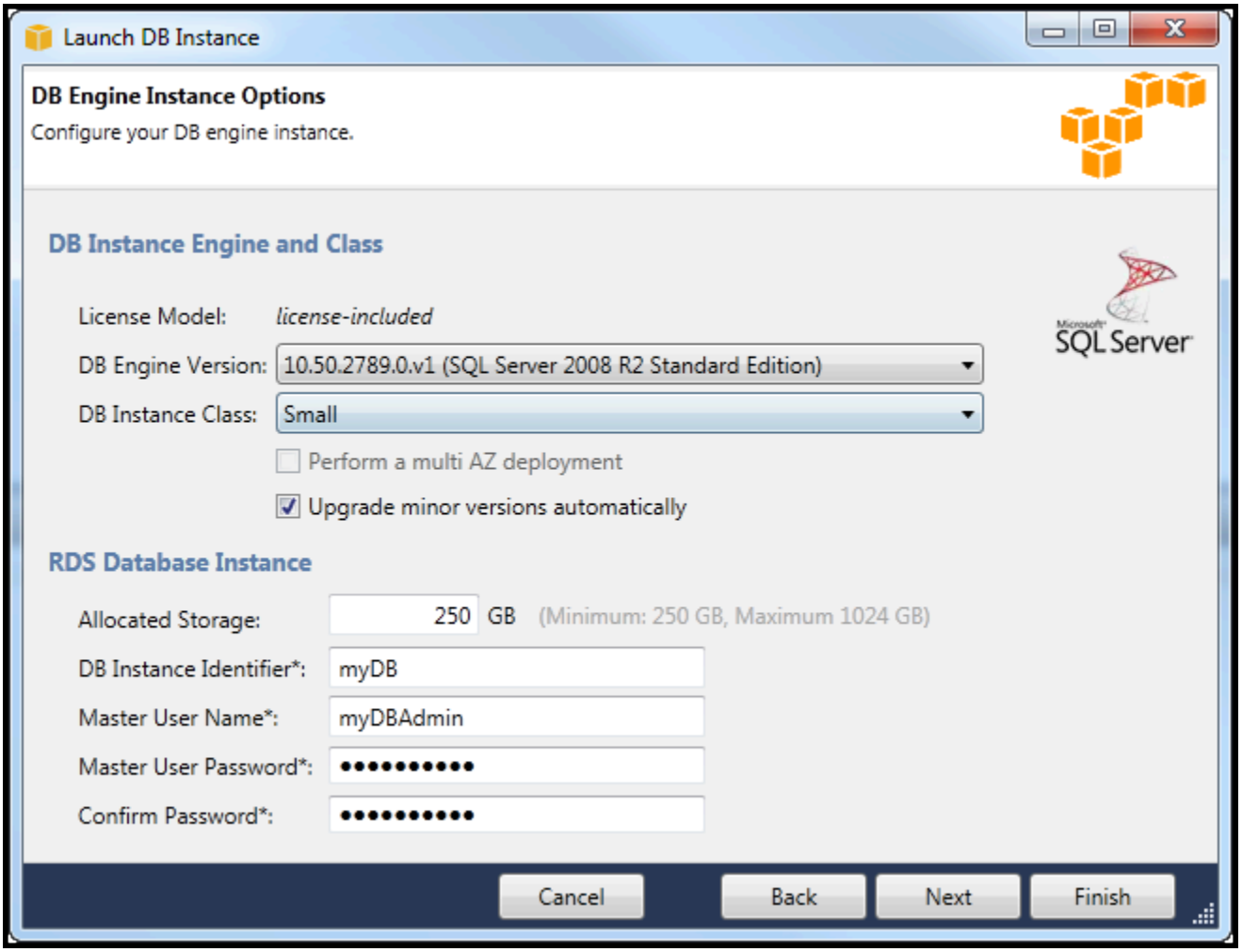
Digite um nome para o administrador da instância de banco de dados.

Master User Password (Senha do usuário mestre)

Digite uma senha para o administrador da instância de banco de dados.

Confirm Password (Confirmar senha)

Digite a senha novamente para verificar se ela está correta.



1. Na caixa de diálogo Additional Options (Opções adicionais), você pode especificar as configurações a seguir.

   Database Port

   Essa é a porta TCP que a instância usará para se comunicar na rede. Se o computador acessar a Internet por meio de um firewall, defina esse valor como uma porta por meio da qual o firewall permite o tráfego.

   Availability Zone

   Use essa opção caso você queira que a instância seja iniciada em uma determinada zona de disponibilidade na região. A instância de banco de dados especificada por você talvez não esteja disponível em todas as zonas de disponibilidade em uma determinada região.

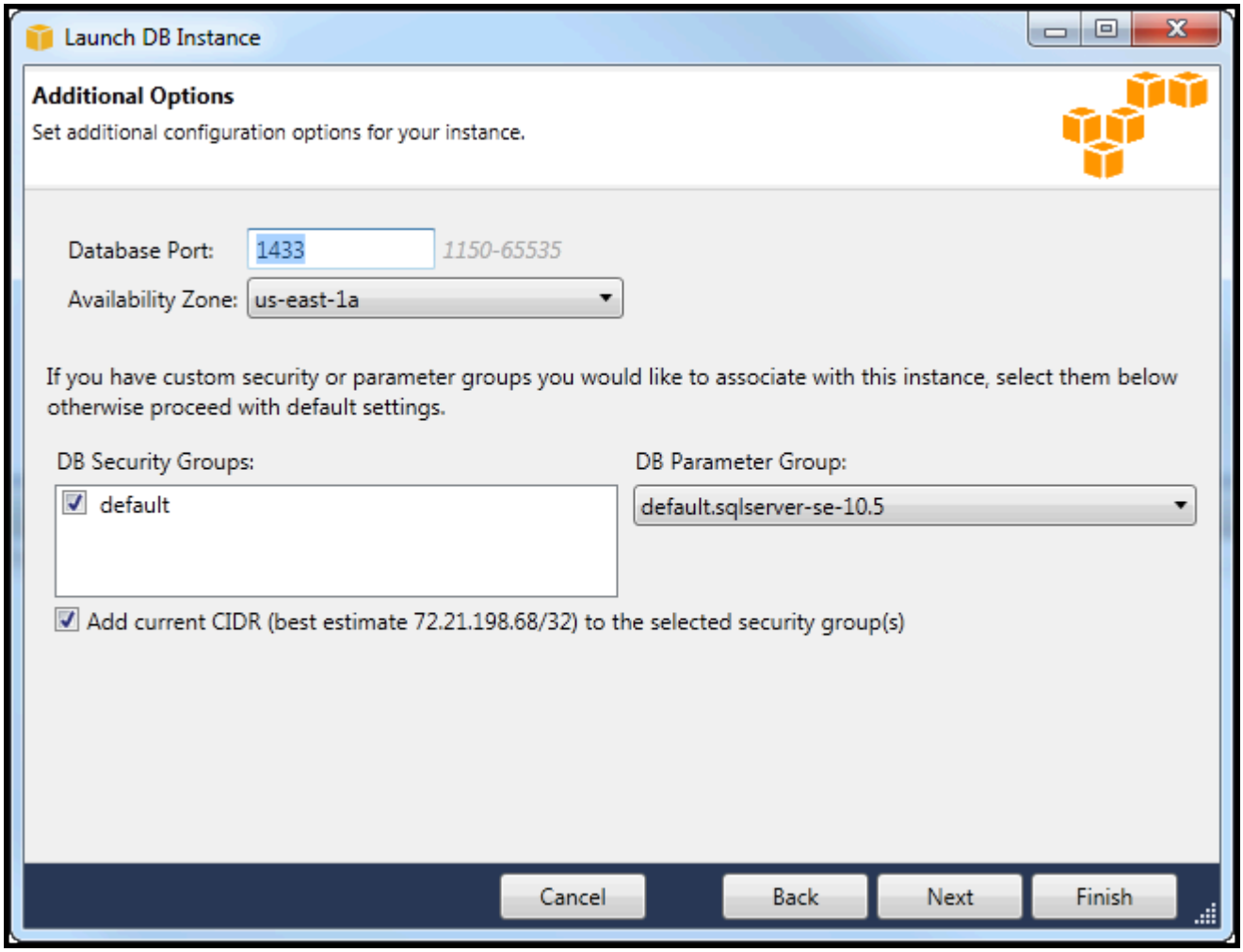
Grupo de segurança do RDS

Selecione um security group (ou grupos) do RDS associado à instância. Os security groups do RDS especificam o endereço IP, as instâncias do Amazon EC2 eContas da AWSque têm permissão para acessar sua instância. Para obter mais informações sobre grupos de segurança do RDS, consulte Grupos de segurança do Amazon RDS. O Toolkit for Visual Studio tenta determinar o endereço IP atual e dá a opção de adicionar esse endereço aos security groups associados à instância. No entanto, se o computador acessar a Internet por meio de um firewall, o endereço IP gerado pelo Toolkit para o computador poderá não ser preciso. Para determinar qual endereço IP usar, consulte o administrador do sistema.

Parameter group do banco de dados

(Opcional) Nesta lista suspensa, escolha um parameter group de banco de dados a ser associado à instância. Parameter groups de banco de dados permitem alterar a configuração padrão da instância. Para obter mais informações, acesse o Guia do usuário do Amazon Relational Database Service e este artigo.

Quando você tiver especificado configurações nessa caixa de diálogo, escolha Next (Próximo).

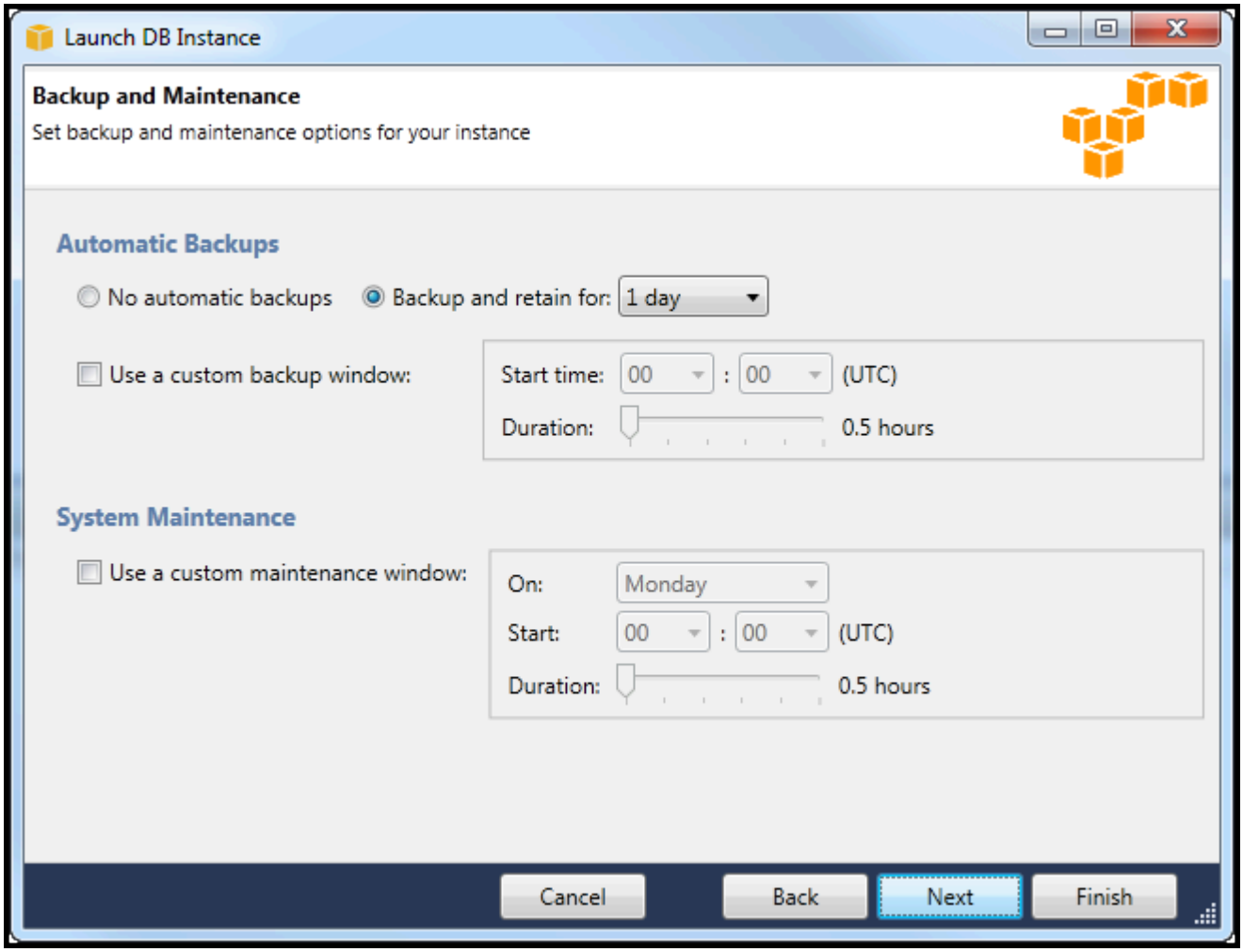


2. OBackup e manutençãoA caixa de diálogo permite especificar se o Amazon RDS deve fazer backup da instância e, assim, por quanto tempo o backup deve ser mantido. Você também pode especificar uma janela de tempo durante a qual os backups devem ocorrer.

   Essa caixa de diálogo também permite especificar se você gostaria que o Amazon RDS realizasse a manutenção do sistema na instância. A manutenção inclui patches de rotina e atualizações de versão secundária.

   A janela de tempo especificada por você para a manutenção do sistema não pode se sobrepor à janela especificada para backups.

   Escolha Next (Próximo).



3. A caixa de diálogo final no assistente permite revisar as configurações da instância. Se você precisar modificar as configurações, use o botão Back (Voltar). Se todas as configurações estiverem corretas, escolha Launch (Executar).

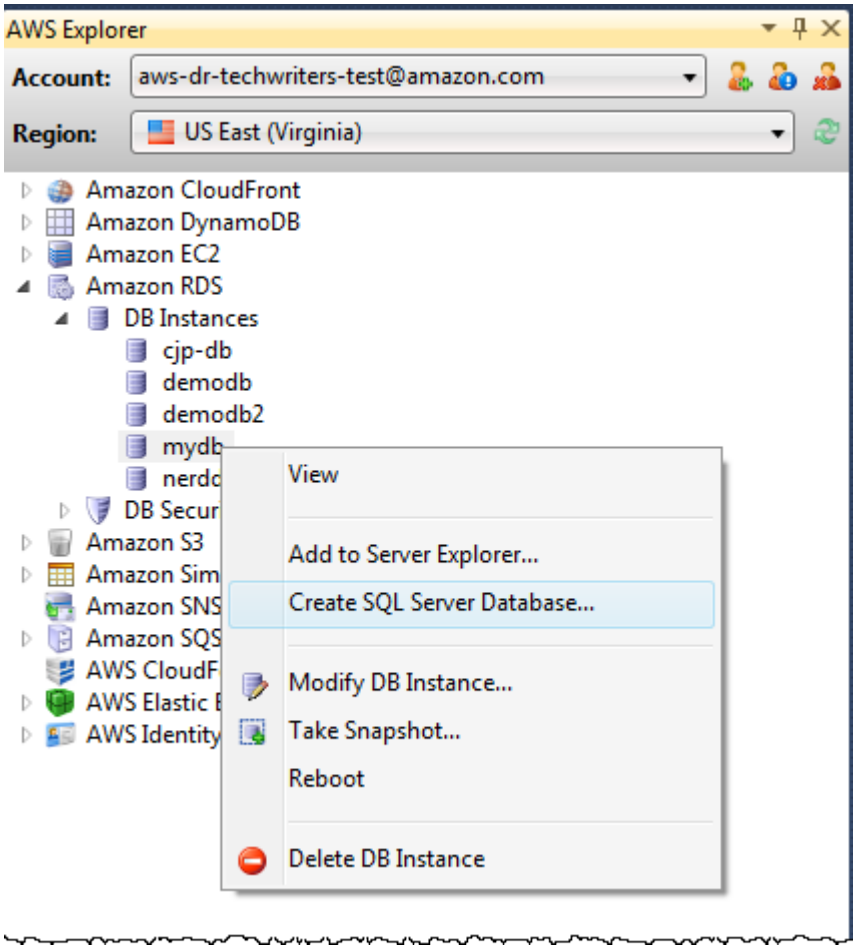
Criar um banco de dados do Microsoft SQL Server em uma instância do RDS

O Microsoft SQL Server foi projetado de maneira que, depois de iniciar uma instância do Amazon RDS, você precisará criar um banco de dados do SQL Server na instância do RDS.

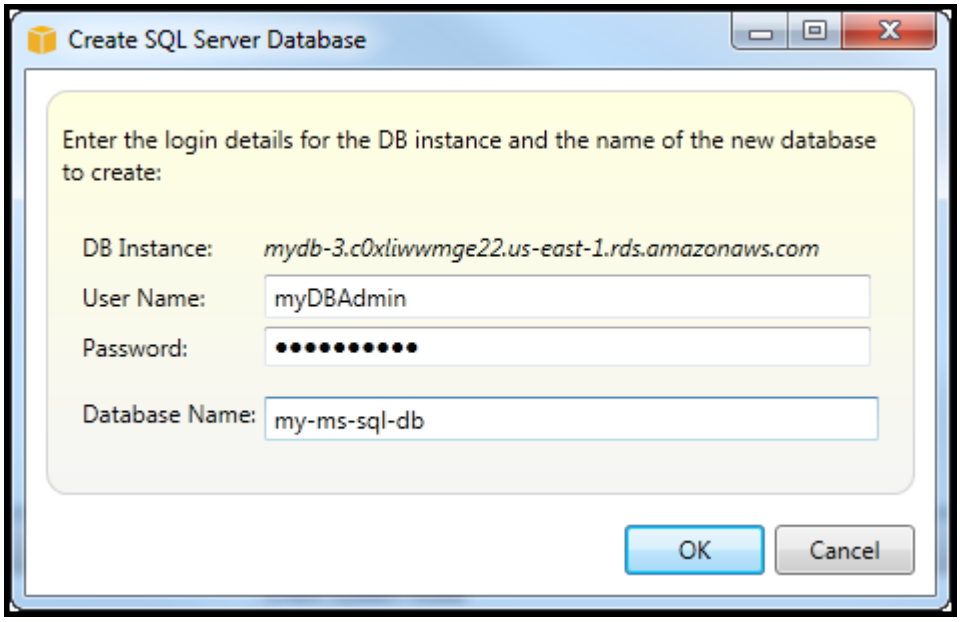
Para obter informações sobre como criar uma instância do Amazon RDS, consulte Para executar uma instância de banco de dados do Amazon RDS.

Para criar um banco de dados do Microsoft SQL Server

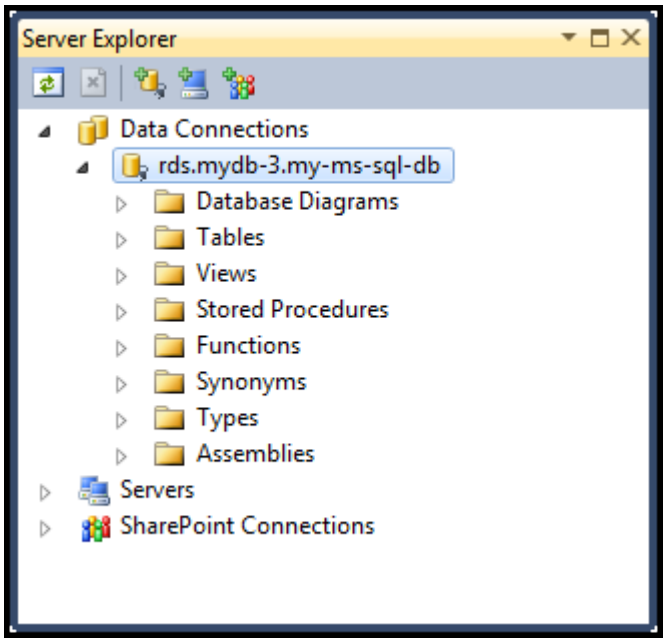
1. DentroAWSPara Explorer, abra o menu de contexto (clique com o botão direito) do nó correspondente à instância do RDS do Microsoft SQL Server e escolhaCrie um banco de dados SQL Server.



2. Na caixa de diálogo Create SQL Server Database (Criar um banco de dados do SQL Server), digite a senha especificada por você quando criou a instância do RDS, digite um nome para o banco de dados do Microsoft SQL Server e escolha OK.



3. O Toolkit for Visual Studio cria o banco de dados do Microsoft SQL Server e o adiciona ao Visual Studio Server Explorer.



Grupos de segurança do Amazon RDS

Os security groups do Amazon RDS permitem gerenciar o acesso à rede para as instâncias do Amazon RDS. Com security groups, você especifica conjuntos de endereços IP usando notação CIDR, e somente o tráfego de rede com origem nesses endereços é reconhecido pela instância do Amazon RDS.

Embora eles funcionem de maneira semelhante, os security groups do Amazon RDS são diferentes dos grupos de segurança do Amazon EC2. É possível adicionar um security group do EC2 ao security group do RDS. Todas as instâncias do EC2 membros do security group do EC2 poderão acessar as instâncias do RDS membros do security group do RDS.

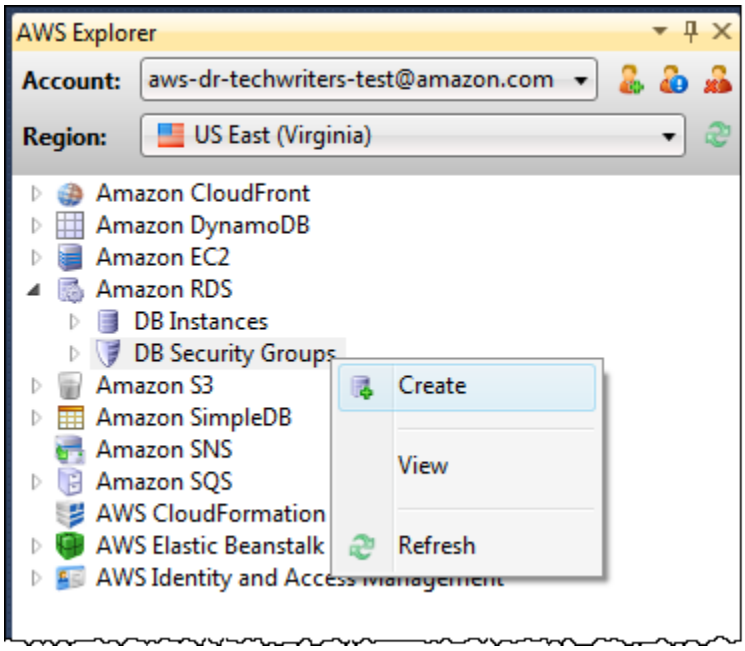
Para obter mais informações sobre grupos de segurança do Amazon RDS, vá até oGrupos de segurança do RDS. Para obter mais informações sobre grupos de segurança do Amazon EC2, vá até oGuia do usuário do EC2.

Criar um security group do Amazon RDS

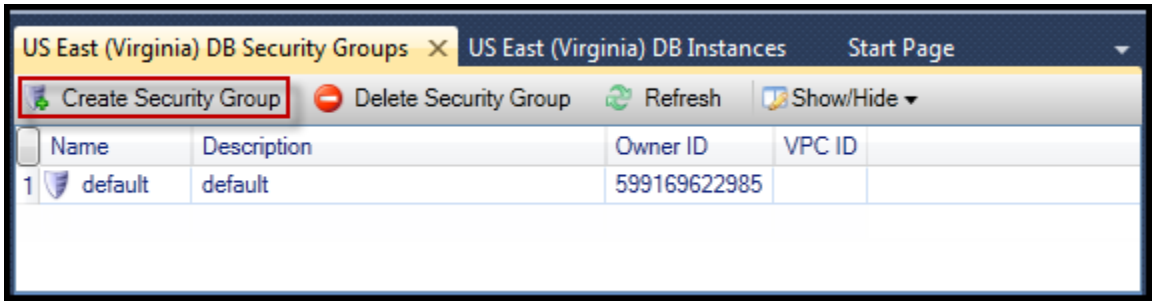
Você pode usar o Toolkit for Visual Studio para criar um security group do RDS. Se você usar oAWSPara iniciar uma instância do RDS, o assistente permitirá especificar um security group do RDS a ser usado com a instância. Você pode usar o procedimento a seguir para criar esse security group antes de iniciar o assistente.

Para criar um security group do Amazon RDS

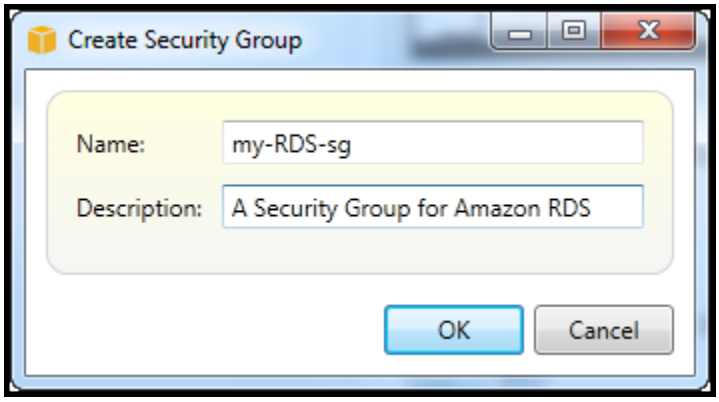
1. DentroAWSExplorer, expanda oAmazon RDSAbra o menu de contexto (clique com o botão direito do mouse) doGrupos de segurança de banco de dadossubnó e escolhaCriar.



   Como alternativa, na guia Security Groups (Grupos de segurança), escolha Create Security Group (Criar grupo de segurança). Se essa guia não for exibida, abra o menu de contexto (clique com o botão direito do mouse) do subnó DB Security Groups (Grupos de segurança do banco de dados) e escolha View (Exibir).



2. Na caixa de diálogo Create Security Group (Criar grupo de segurança), digite um nome e uma descrição para o grupo de segurança e escolha OK.



Definir permissões de acesso para um security group do Amazon RDS

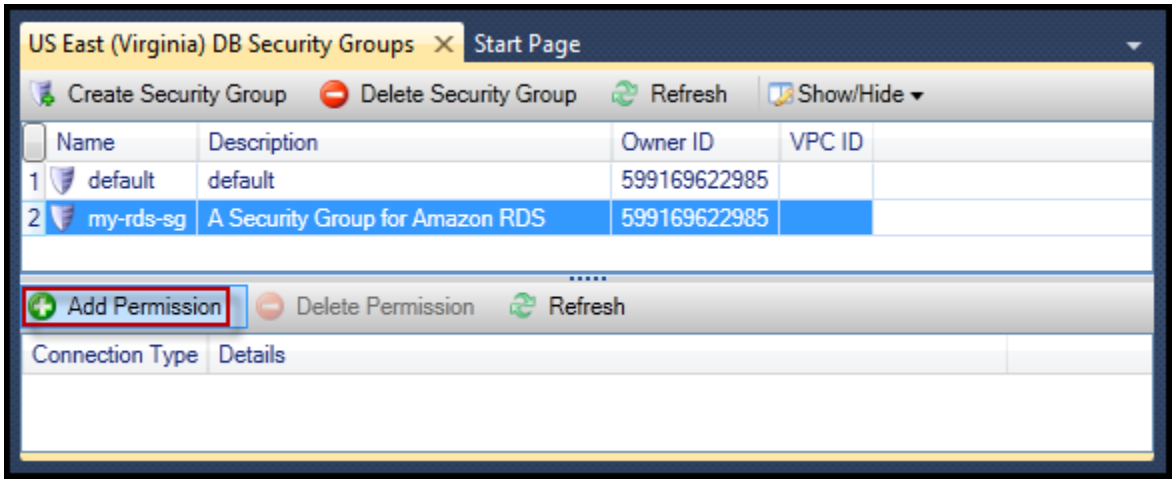
Por padrão, um novo security group do Amazon RDS não dá acesso à rede. Para permitir acesso a instâncias do Amazon RDS que usem o security group, use o procedimento a seguir para definir as permissões de acesso.

Para definir o acesso para um security group do Amazon RDS

1. Na guia Security Groups (Grupos de segurança), escolha o grupo de segurança na visualização de lista. Se o grupo de segurança não for exibido na lista, escolha Refresh (Atualizar). Se o security group ainda não for exibido na lista, verifique se você está visualizando a lista para o corretoAWSregião. Security groupGuias noAWSO Toolkit é específico para a região.

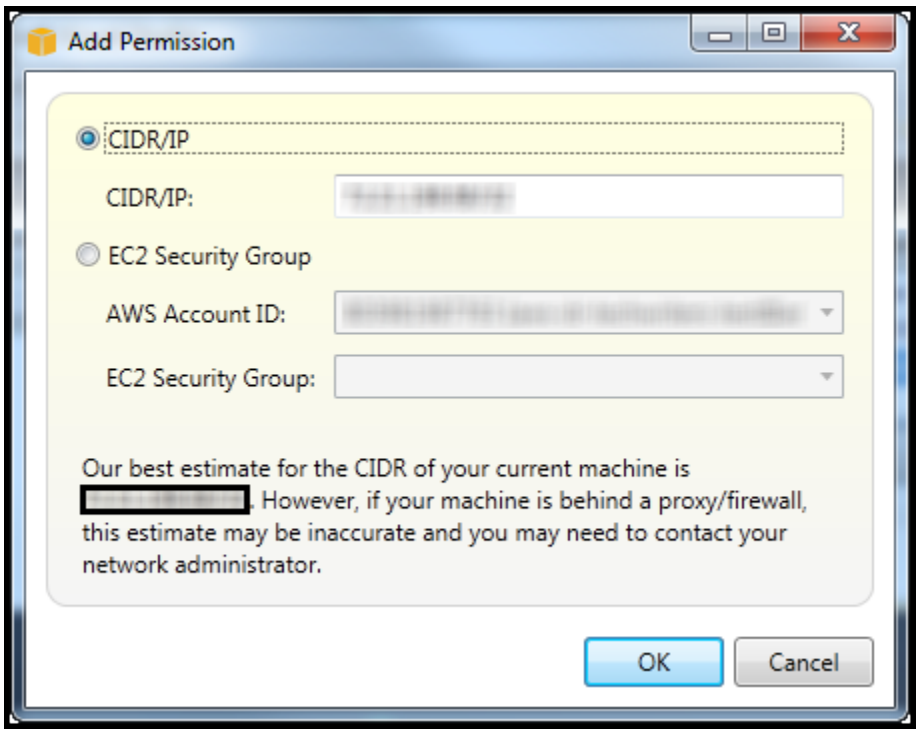
   Se nãoSecurity groupabas aparecem, emAWSExplorer, abra o menu de contexto (clique com o botão direito do mouse) doGrupos de segurança de banco de dadossubnó e escolhaExibir.

2. Escolha Add Permission.



Botão Add Permissions (Adicionar permissões) na guia Security Groups (Grupos de segurança)

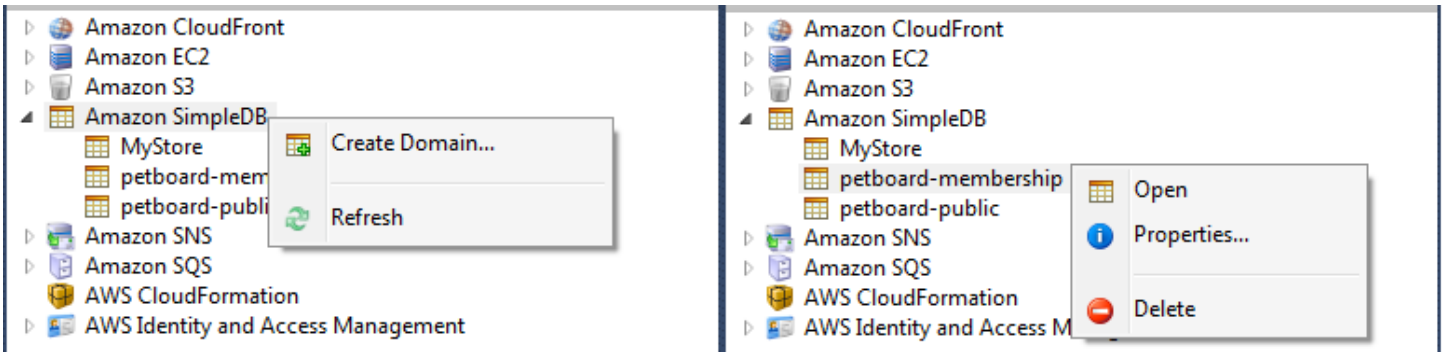
3. Na caixa de diálogo Add Permission (Adicionar permissão), você pode usar a notação CIDR para especificar quais endereços IP podem acessar a instância do RDS ou especificar quais grupos de segurança do EC2 podem acessar a instância do RDS. Quando você escolherGrupo de segurança do EC2, você pode especificar o acesso para todas as instâncias do EC2 associadas a umConta da AWSSe você tiver acesso, ou você pode escolher um security group do EC2 na lista suspensa.



OAWSO Toolkit tenta determinar o endereço IP e preencher automaticamente a caixa de diálogo com a especificação CIDR apropriada. No entanto, se o computador acessar a Internet por meio de um firewall, o CIDR determinado pelo Toolkit poderá não ser preciso.

Usando o Amazon SimpleDBAWSExplorer

AWSO Amazon SimpleDB exibe todos os ativos domínios do Amazon SimpleDB associados ao ativoAWSconta. NoAWSExplorer, você pode criar ou excluir domínios do Amazon SimpleDB.

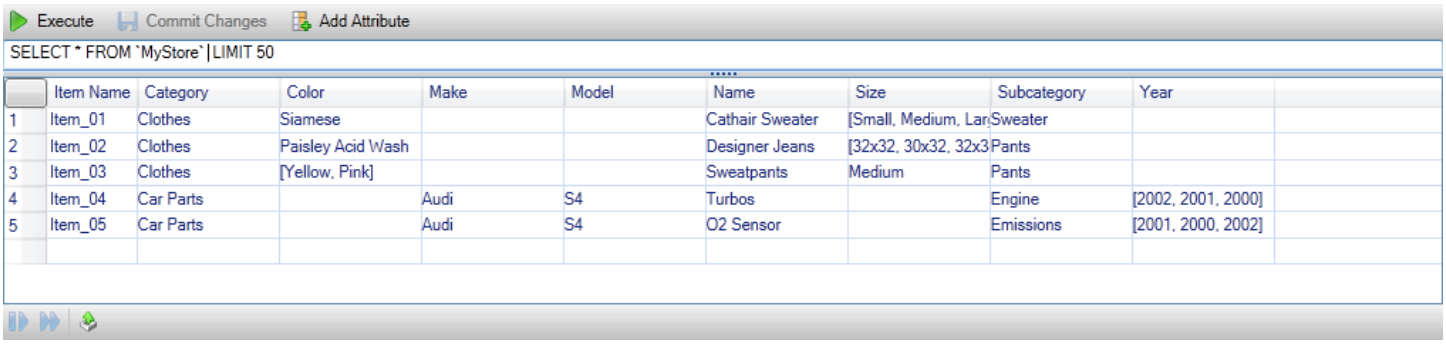


Create, delete, or open Amazon SimpleDB domains associated with your account

Execução de consultas e edição dos resultados

AWSO Amazon SimpleDB também pode exibir uma visualização em grade de um domínio do Amazon SimpleDB na qual você pode visualizar os itens, os atributos e os valores nesse domínio. Você pode executar consultas de maneira que somente um subconjunto dos itens do domínio seja exibido. Clicando duas vezes em uma célula, você pode editar os valores do atributo correspondente desse item. Você também pode adicionar novos atributos ao domínio.

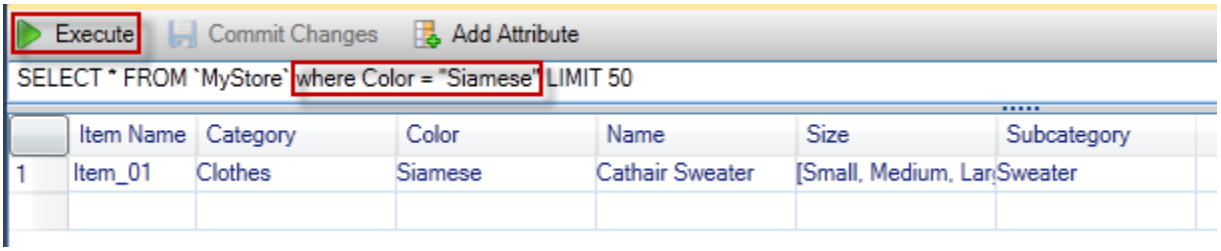
O domínio exibido aqui é do exemplo do Amazon SimpleDB incluído com oAWS SDK for .NET.



	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 executar uma consulta, edite a consulta na caixa de texto na parte superior da visualização em grade e escolha Execute (Executar). A visualização é filtrada para mostrar apenas os itens correspondentes à consulta.

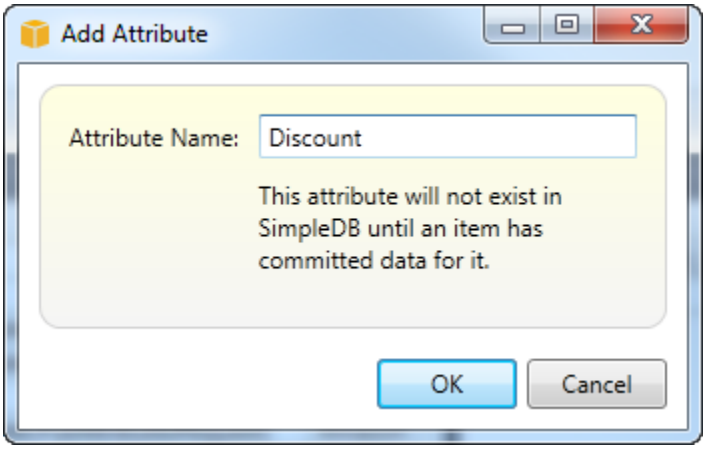


Execute query from AWS Explorer

Para editar os valores associados a um atributo, clique duas vezes na célula correspondente, edite os valores e escolha Commit Changes (Confirmar alterações).

Como adicionar um atributo

Para adicionar um atributo, na parte superior da visualização, escolha Add Attribute (Adicionar atributo).



Adicionar atributo dialog box

Para tornar o atributo parte do domínio, você deve adicionar um valor a pelo menos um item e escolher Commit Changes (Confirmar alterações).

Commit changes for a new attribute

Paginação do resultados da consulta

Existem três botões na parte inferior da visualização.

Paginate and export buttons

Os dois primeiros botões fornecem paginação para resultados da consulta. Para exibir uma página adicional de resultados, escolha o primeiro botão. Para exibir dez páginas adicionais de resultados, escolha o segundo botão. Neste contexto, uma página será igual a 100 linhas ou o número de resultados especificados pelo valor LIMIT, se estiver incluído na consulta.

Exportar para CSV

O último button exporta os resultados atuais para um arquivo CSV.

Uso do Amazon SQS a partir deAWSExplorer

O Amazon Simple Queue Service (Amazon SQS) é um serviço de fila flexível que permite a passagem da mensagem entre processos diferentes de execução em um aplicativo de software. As filas do Amazon SQS estão localizadas naAWSNo entanto, os processos que estão passando mensagens podem estar localizados localmente, em instâncias do Amazon EC2, ou em uma combinação deles. O Amazon SQS é ideal para coordenar a distribuição de trabalho em vários computadores.

O Toolkit for Visual Studio permite visualizar filas do Amazon SQS associadas à conta ativa, criar e excluir filas, além de enviar mensagens por meio de filas. (Por conta ativa, queremos dizer a conta selecionada emAWSExplorador.)

Para obter mais informações sobre o Amazon SQS, consulteIntrodução ao SQSnoAWSdocumentação.

Criação de uma fila

Você pode criar uma fila do Amazon SQS a partir deAWSExplorador. O ARN e o URL da fila se basearão no número da conta ativa e no nome da fila especificado por você na criação.

Para criar uma fila

1. DentroAWSNo Explorer, abra o menu de contexto (clique com o botão direito do mouse)Amazon SQSnó e, em seguida, escolhaCriar fila.
2. Na caixa de diálogo Create Queue (Criar fila), especifique o nome da fila, o tempo limite de visibilidade padrão e o atraso na entrega padrão. O tempo limite de visibilidade padrão e o atraso na entrega padrão são especificados em segundos. O tempo limite de visibilidade padrão é o valor de tempo em que uma mensagem será invisível para o recebimento de processos em potencial depois que um determinado processo tiver adquirido a mensagem. O atraso na entrega padrão é o valor de tempo desde o momento em que a mensagem é enviada até o momento em que ela se torna visível inicialmente para o recebimento de processos em potencial.
3. Escolha OK. A nova fila será exibida como um subnó no nó Amazon SQS.

Exclusão de uma fila

Você pode excluir filas existentes doAWSExplorador. Se você excluir uma fila, todas as mensagens associadas à fila deixarão de estar disponíveis.

Para excluir uma fila

1. DentroAWSExplorador, abra os menus de contexto (clique com o botão direito do mouse) da fila que você deseja excluir e escolhaExcluir.

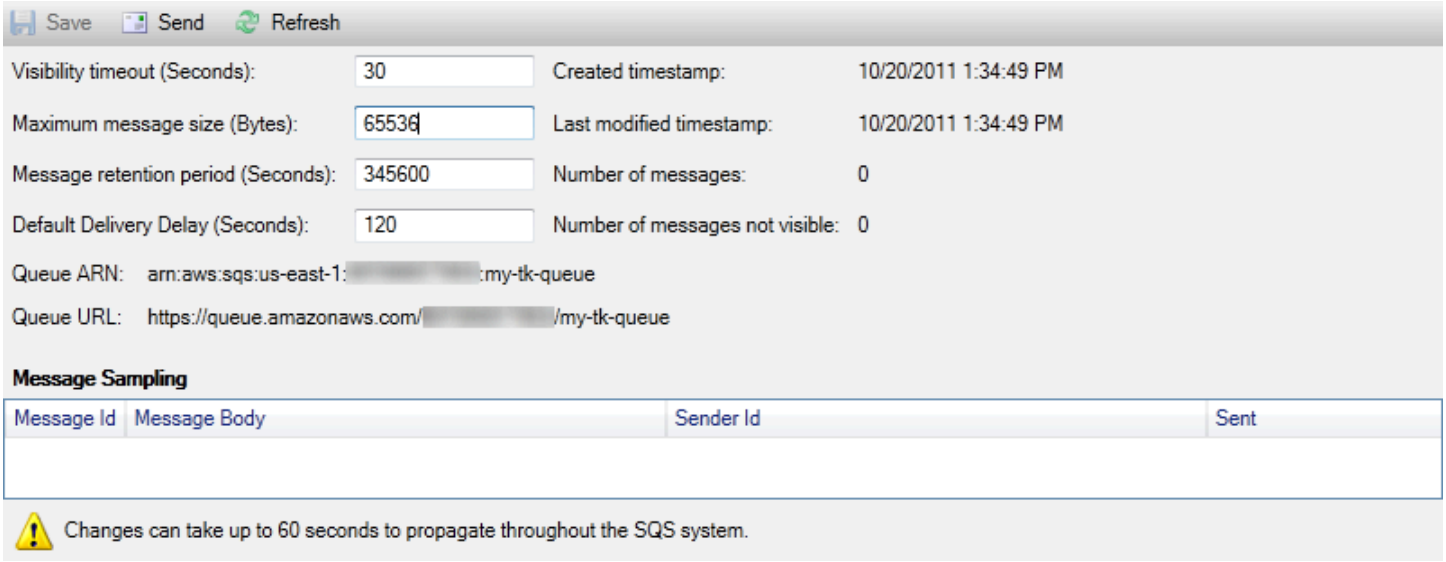
Gerenciar propriedades da fila

Você pode visualizar e editar as propriedades de qualquer uma das filas exibidas noAWSExplorador. Você também pode enviar mensagens para a fila nessa visualização de propriedades.

Para gerenciar propriedades da fila

- DentroAWSExplorador, abra o menu de contexto (clique com o botão direito do mouse) da fila cujas propriedades você deseja gerenciar e escolhaVisualizar fila.

  Na visualização de propriedades da fila, você pode editar o tempo limite de visibilidade, o tamanho de mensagem máximo, o período de retenção da mensagem e o atraso na entrega padrão. O atraso na entrega padrão pode ser substituído quando você envia uma mensagem. Na captura de tela a seguir, o texto obscurecido é o componente do número da conta do ARN e do URL da fila.



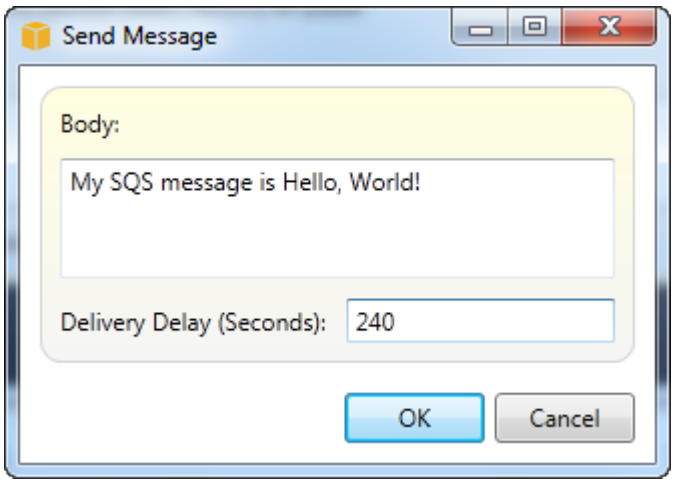
SQS queue properties view

Enviar uma mensagem para uma fila

Na visualização de propriedades da fila, você pode enviar uma mensagem para a fila.

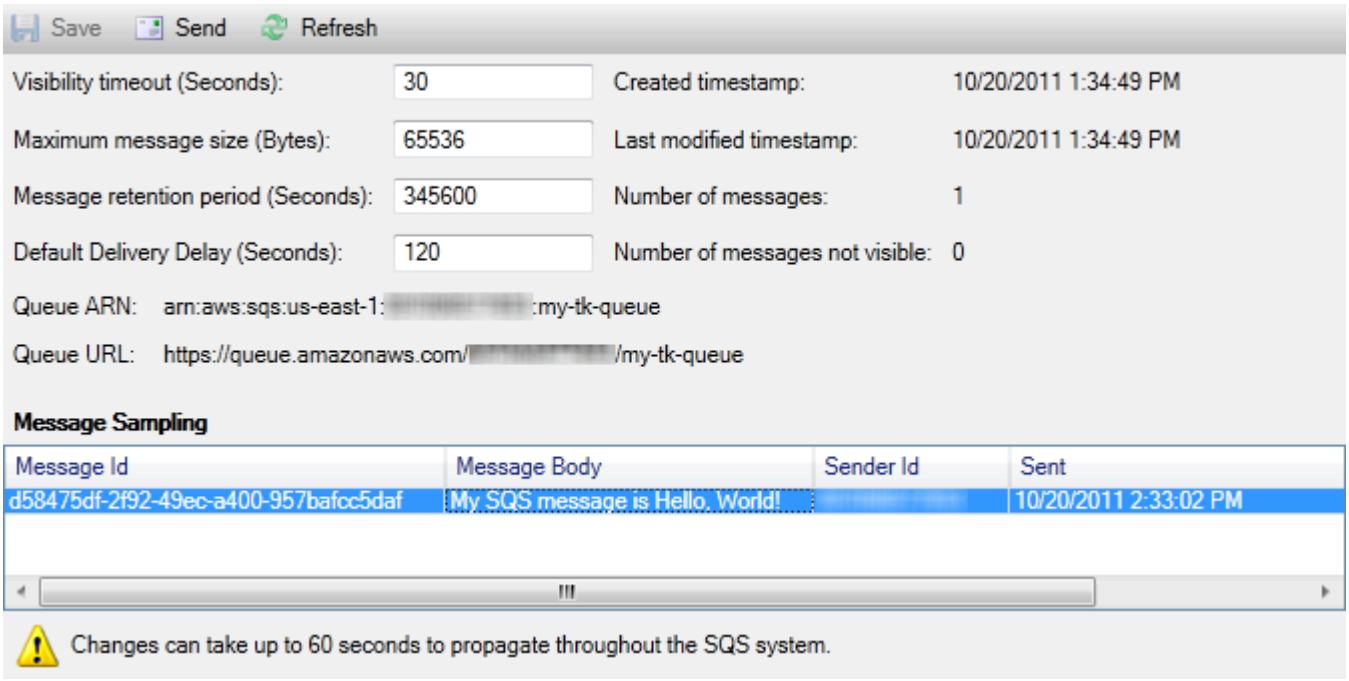
Para enviar uma mensagem

1. Na parte superior da visualização de propriedades da fila, escolha o botão Send (Enviar).
2. Digite a mensagem. (Opcional) Insira um atraso na entrega que substituirá o atraso na entrega padrão da fila. No exemplo a seguir, substituímos o atraso por um valor de 240 segundos. Escolha OK.



Enviar mensagem dialog box

3. Aguarde aproximadamente 240 segundos (quatro minutos). A mensagem será exibida na seção Message Sampling (Amostragem de mensagem) da visualização de propriedades da fila.



SQS properties view with sent message

A data e hora na visualização de propriedades da fila é o momento em que você escolhe o botão Send (Enviar). Isso não inclui o atraso. Por isso, o momento em que a mensagem é exibida na fila e está disponível para os destinatários pode ser posterior à data e hora. A data e hora é exibida no horário local do computador.

Identity and Access Management

AWS Identity and Access ManagementO (IAM) permite gerenciar com mais segurança o acesso aoContas da AWSe recursos. Com o IAM, você pode criar vários usuários em seu primário (raiz)Conta da AWS. Esses usuários podem ter as próprias credenciais: senha, ID de chave de acesso e chave secreta, mas todos os usuários do IAM compartilham um único número de conta.

Você pode gerenciar o nível de acesso ao recurso do usuário do IAM anexando políticas do IAM ao usuário. Por exemplo, você pode anexar uma política a um usuário do IAM que dá ao usuário acesso ao serviço do Amazon S3 e aos recursos relacionados na conta, mas que não dá acesso a nenhum outro serviço ou recurso.

Para obter um gerenciamento de acesso mais eficiente, você pode criar grupos do IAM, que são coleções de usuários. Quando você anexar uma política ao grupo, ela afetará todos os usuários membros desse grupo.

Além de gerenciar permissões nos níveis do usuário e do grupo, o IAM também dá suporte ao conceito de funções do IAM. Assim como usuários e grupos, você pode anexar políticas a funções do IAM. Depois, você pode associar a função do IAM a uma instância do Amazon EC2. Os aplicativos executados na instância do EC2 podem acessarAWSUsando as permissões fornecidas pela função do IAM. Para obter mais informações sobre como usar funções do IAM com o Toolkit, consulte Criar uma função do IAM. Para obter mais informações sobre o IAM, acesseManual do usuário do IAM.

Criar e configurar um usuário do IAM

Os usuários do IAM permitem conceder a outras pessoas acesso aoConta da AWS. Como pode anexar políticas a usuários do IAM, você pode limitar com precisão os recursos que um usuário do IAM pode acessar e as operações que eles podem realizar nesses recursos.

Como prática recomendada, todos os usuários que acessam umConta da AWSVocê deve fazer isso como usuários do IAM — até mesmo o proprietário da conta. Isso garante que, se as credenciais para um dos usuários do IAM são estiverem comprometidas, apenas essas credenciais poderão ser desativadas. Não há necessidade de desativar nem alterar as credenciais raiz da conta.

No Toolkit for Visual Studio, você pode atribuir permissões a um usuário do IAM anexando uma política do IAM ao usuário ou atribuindo o usuário a um grupo. Os usuários do IAM atribuídos a um grupo derivam as permissões das políticas anexadas ao grupo. Para obter mais informações, consulte Criar um grupo do IAM e Adicionar um usuário do IAM a um grupo do IAM.

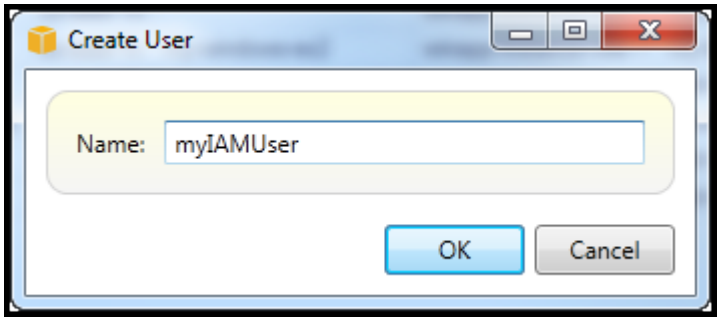
No Toolkit for Visual Studio, você também pode gerarAWSAs credenciais (ID de chave de acesso e chave secreta) para o usuário do IAM. Para obter mais informações, consulte Gerar credenciais para um usuário do IAM

O Toolkit for Visual Studio oferece suporte à especificação de credenciais do usuário do IAM para acessar serviços por meio deAWSExplorador. Como os usuários do IAM normalmente não têm acesso total a todos os Amazon Web Services, parte da funcionalidade doAWSO Explorer pode não estar disponível. Se você usarAWSPara alterar recursos enquanto a conta ativa for um usuário do IAM e, em seguida, alternar a conta para a conta raiz, as alterações poderão não estar visíveis até você atualizar a exibição noAWSExplorador. Para atualizar a exibição, escolha o botão refresh ().

Para obter informações sobre como configurar usuários do IAM noAWS Management Console, vá paraTrabalhar com usuários e gruposno Guia do usuário do IAM.

Para criar um usuário do IAM

1. DentroAWSExplorer, expanda oAWS Identity and Access Management, abra o menu de contexto (clique com o botão direito do mouse) paraUsuários doEscolha e, depois, escolhaCriar usuário.
2. NoCriar usuáriocaixa de diálogo, digite um nome para o usuário do IAM e escolhaOK. Este é o IAMnome amigável. Para obter informações sobre restrições quanto a nomes de usuários do IAM, acesse oManual do usuário do IAM.



Create an IAM user

O novo usuário será exibido como um subnó emUsuários doSobAWS Identity and Access ManagementNó.

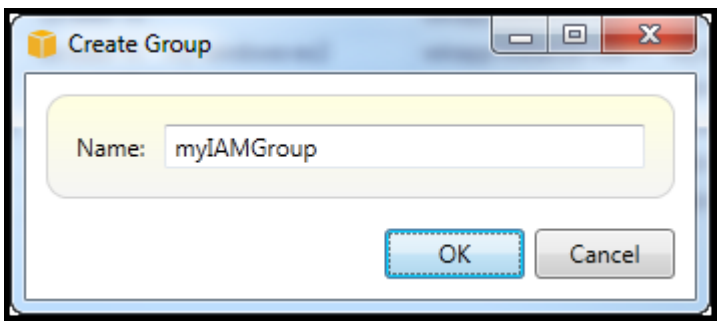
Para obter informações sobre como criar uma política e anexá-la ao usuário, consulte Criar uma política do IAM.

Criar um grupo do IAM

Os grupos são uma maneira de aplicar políticas do IAM a um conjunto de usuários. Para obter informações sobre como gerenciar usuários e grupos do IAM, acesseTrabalhar com usuários e gruposno Guia do usuário do IAM.

Para criar um grupo do IAM

1. DentroAWSExplorador, sobIdentity and Access Management, abra o menu de contexto (clique com o botão direito do mouse)Grupos doe escolhaCriar grupo.
2. NoCriar grupocaixa de diálogo, digite um nome para o grupo do IAM e escolhaOK.



Create IAM group

O novo grupo do IAM aparecerá sob oGrupos dosubnó deIdentity and Access Management.

Para obter informações sobre como criar uma política e anexá-la ao grupo do IAM, consulteCriar uma política do IAM.

Adicionar um usuário do IAM a um grupo do IAM

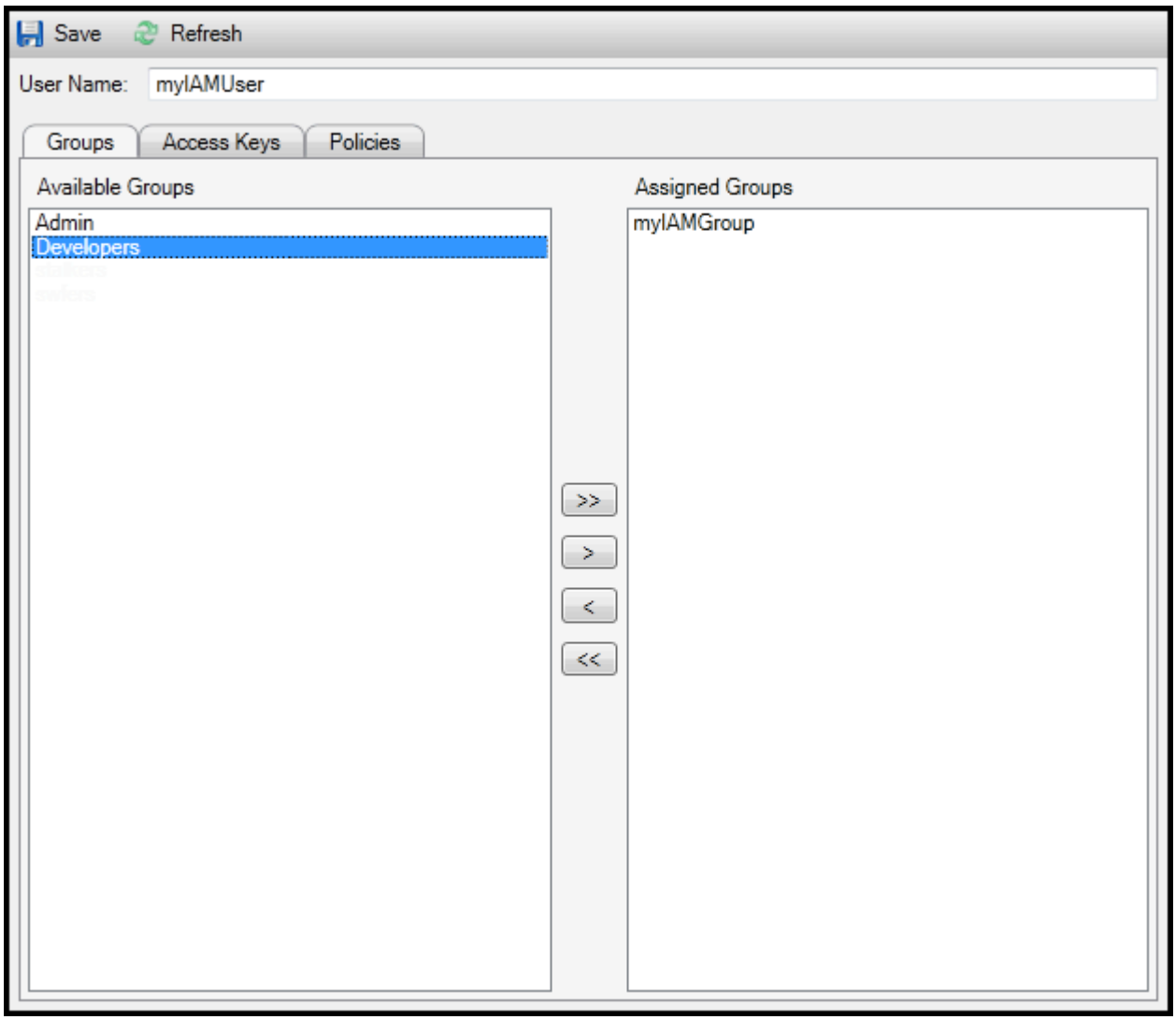
Os usuários do IAM membros de um grupo do IAM derivam permissões de acesso das políticas anexadas ao grupo. A finalidade de um grupo do IAM é facilitar o gerenciamento de permissões em um conjunto de usuários do IAM.

Para obter informações sobre como as políticas anexadas a um grupo do IAM interagem com as políticas anexadas a usuários do IAM membros desse grupo do IAM, acesseGerenciar políticas do IAM no Guia do usuário do IAM.

DentroAWSExplorador, você adiciona usuários do IAM a grupos do IAM noUsuários dosubnó, não oGrupos dosubnó.

Para adicionar um usuário do IAM a um grupo do IAM

1. DentroAWSExplorador, sobIdentity and Access Management, abra o menu de contexto (clique com o botão direito do mouse)Usuários doe escolhaEdite.



Assign an IAM user to a IAM group

2. O painel esquerdo doGrupos doexibe os grupos do IAM disponíveis. O painel direito exibe os grupos dos quais o usuário do IAM especificado já é membro.

   Para adicionar o usuário do IAM a um grupo, no painel esquerdo, escolha o grupo do IAM e, em seguida, escolha o grupo do IAM e o>.

   Para adicionar o usuário do IAM a um grupo, no painel direito, escolha o grupo do IAM e, em seguida, escolha o grupo do IAM e o<.

   Para adicionar o usuário do IAM a todos os grupos do IAM, escolha o>>. Da mesma maneira, para remover o usuário do IAM de todos os grupos, escolha o<<.

   Para escolher vários grupos, escolha-os em sequência. Você não precisa manter pressionada a tecla Control. Para limpar um grupo da seleção, basta escolhê-lo uma segunda vez.

3. Ao terminar de atribuir o usuário do IAM a grupos do IAM, escolhaSalvar.

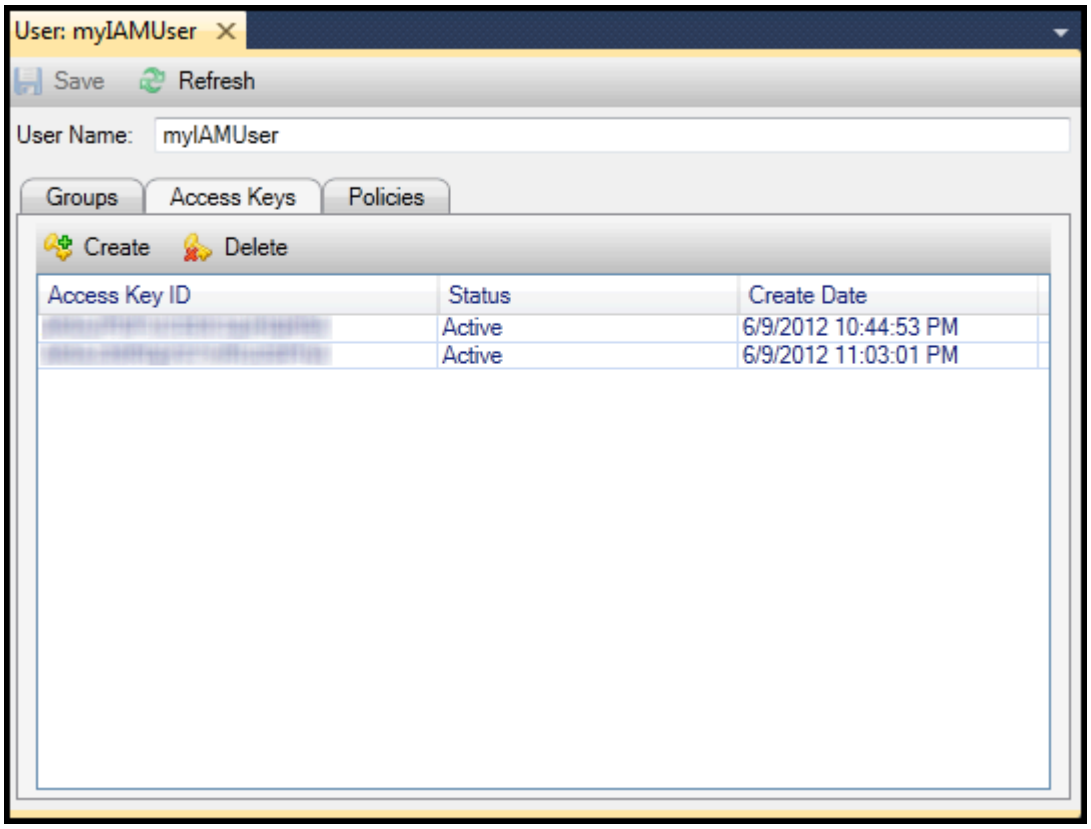
Gerar credenciais para um usuário do IAM

Com o Toolkit for Visual Studio, você pode gerar o ID de chave de acesso e a chave secreta usados para fazer chamadas à API paraAWS. Essas chaves também podem ser especificadas para acessar a Amazon Web Services por meio do Toolkit. Para obter mais informações sobre como especificar as credenciais a serem usadas com o Toolkit, consulte creds. Para obter mais informações sobre como lidar com credenciais com segurança, consulteMelhores práticas doAWSChaves de acesso.

O Toolkit não pode ser usado para gerar uma senha para um usuário do IAM.

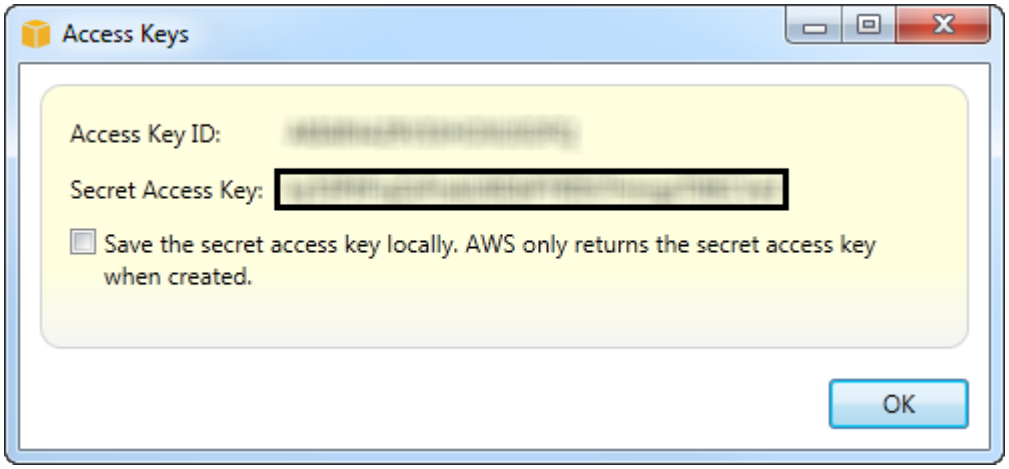
Para gerar credenciais de um usuário do IAM

1. DentroAWSExplorer, abra o menu de contexto (clique com o botão direito do mouse) de um usuário do IAM e escolhaEdite.



2. Para gerar credenciais, na guia Access Keys (Chaves de acesso), escolha Create (Criar).

Você só pode gerar dois conjuntos de credenciais por usuário do IAM. Se já tiver dois conjuntos de credenciais e precisar criar um conjunto adicional, você deverá excluir um dos conjuntos existentes.

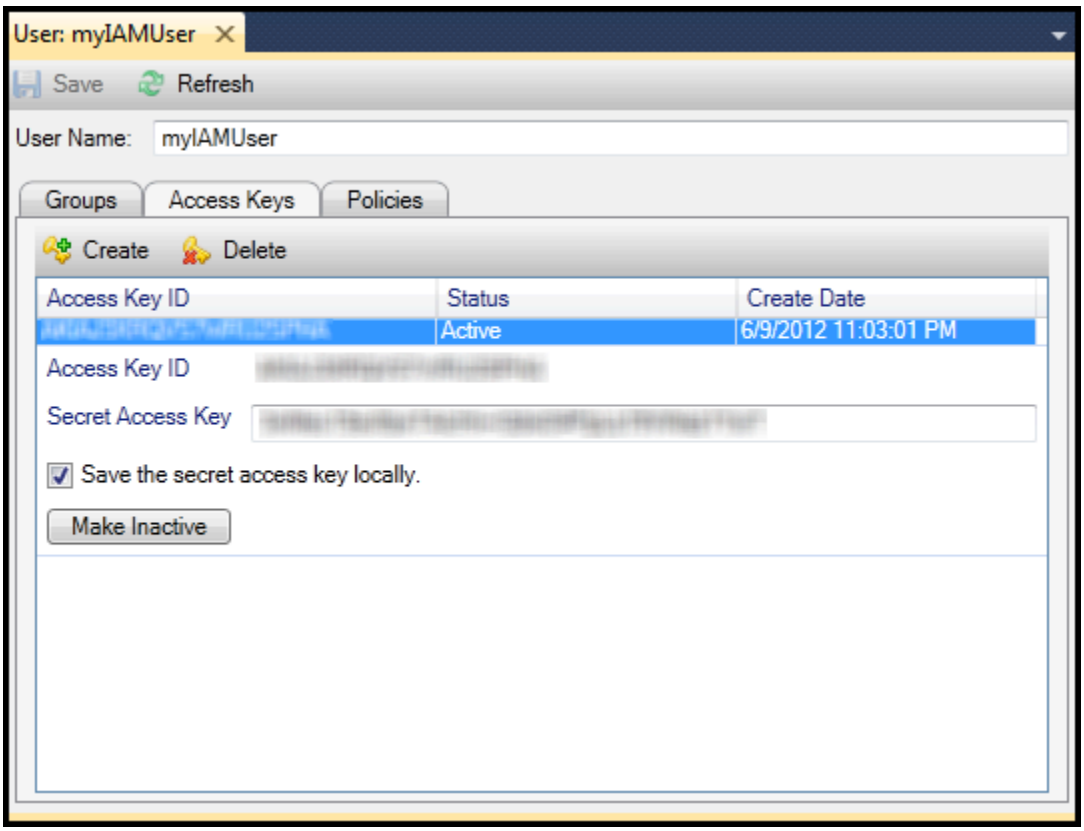


reate credentials for IAM user

Se você quiser que o Toolkit salve uma cópia criptografada da chave de acesso secreta na unidade de disco local, selecioneSalve a chave de acesso secreta localmente.AWSSomente retorna a chave de acesso secreta quando criada. Você também pode copiar a chave de acesso secreta na caixa de diálogo e salvá-la em um local seguro.

3. Escolha OK.

Depois de gerar as credenciais, você poderá visualizá-las na guia Access Keys (Chaves de acesso). Se você tiver selecionado a opção para que o Toolkit salve a chave secreta localmente, ela será exibida aqui.



Create credentials for IAM user

Se você tiver salvado a chave secreta por conta própria e também quiser que o Toolkit a salve, na caixa Secret Access Key (Chave de acesso secreta), digite a chave de acesso secreta e selecione Save the secret access key locally (Salvar a chave de acesso secreta localmente).

Para desativar as credenciais, escolha Make Inactive (Tornar inativa). (Convém fazer isso caso você suspeite que as credenciais tenham sido comprometidas. Você poderá reativar as credenciais se receber uma garantia de que elas sejam seguras.)

Criar uma função do IAM

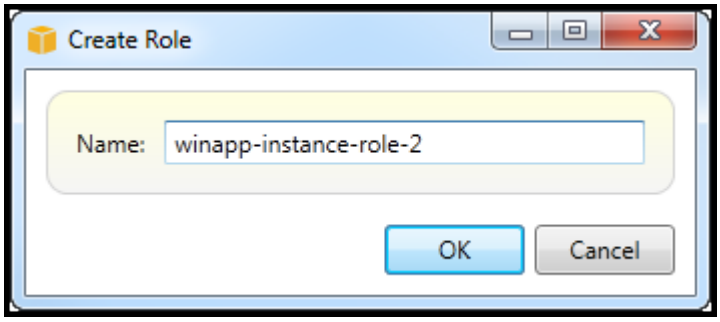
O Toolkit for Visual Studio oferece suporte à criação e à configuração de funções do IAM. Assim como acontece com usuários e grupos, você pode anexar políticas a funções do IAM. Depois, você pode associar a função do IAM a uma instância do Amazon EC2. A associação à instância do EC2 é controlada por meio de um perfil de instância, que é um contêiner lógico para a função. Os aplicativos executados na instância do EC2 recebem automaticamente o nível de acesso especificado pela política associada à função do IAM. Isso é verdadeiro mesmo quando o aplicativo não tiver especificado outroAWSCredenciais da .

Por exemplo, você pode criar uma função e anexar uma política a essa função que limita o acesso apenas ao Amazon S3. Depois de associar essa função a uma instância do EC2, você poderá executar um aplicativo nessa instância, e o aplicativo terá acesso ao Amazon S3, mas não a nenhum outro serviço ou recurso. A vantagem dessa abordagem é que você não precisa se preocupar com a transferência segura e o armazenamento.AWScredenciais na instância do EC2.

Para obter mais informações sobre as funções do IAM, consulteComo trabalhar com funções do IAM no Guia do usuário do IAM. Para exemplos de programas que acessamAWSusando a função do IAM associada a uma instância do Amazon EC2, vá para aAWSGuias do desenvolvedor do paraJava,.NET,PHP, e Ruby (Definir credenciais usando o IAM,Criar uma função do IAM, eTrabalhar com políticas do IAM).

Para criar uma função do IAM

1. DentroAWSExplorador, sobIdentity and Access Management, abra o menu de contexto (clique com o botão direito do mouse)Funções doEscolha e, depois, escolhaCriar funções.
2. NoCriar função docaixa de diálogo, digite um nome para a função do IAM e escolhaOK.



Create IAM role

A nova função do IAM aparecerá emFunções doemIdentity and Access Management.

Para obter informações sobre como criar uma política e anexá-la à função, consulte Criar uma política do IAM.

Criar uma política do IAM

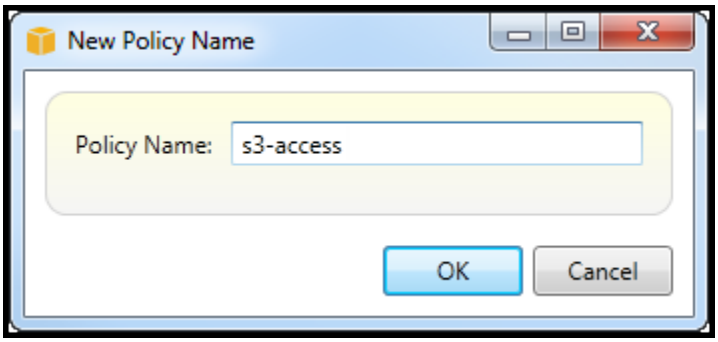
As políticas são fundamentais para o IAM. As políticas podem ser associadas ao IAMentidadesComo usuários, grupos ou funções do. As políticas especificam o nível de acesso habilitado para um usuário, grupo ou função.

Para criar uma política do IAM

DentroAWSExplorer, expanda oAWS Identity and Access Managementnó e, em seguida, expanda o nó para o tipo de entidade (Grupos do,Funções do, ouUsuários do) ao qual você anexará a política. Por exemplo, abra um menu de contexto para uma função do IAM e escolhaEdite.

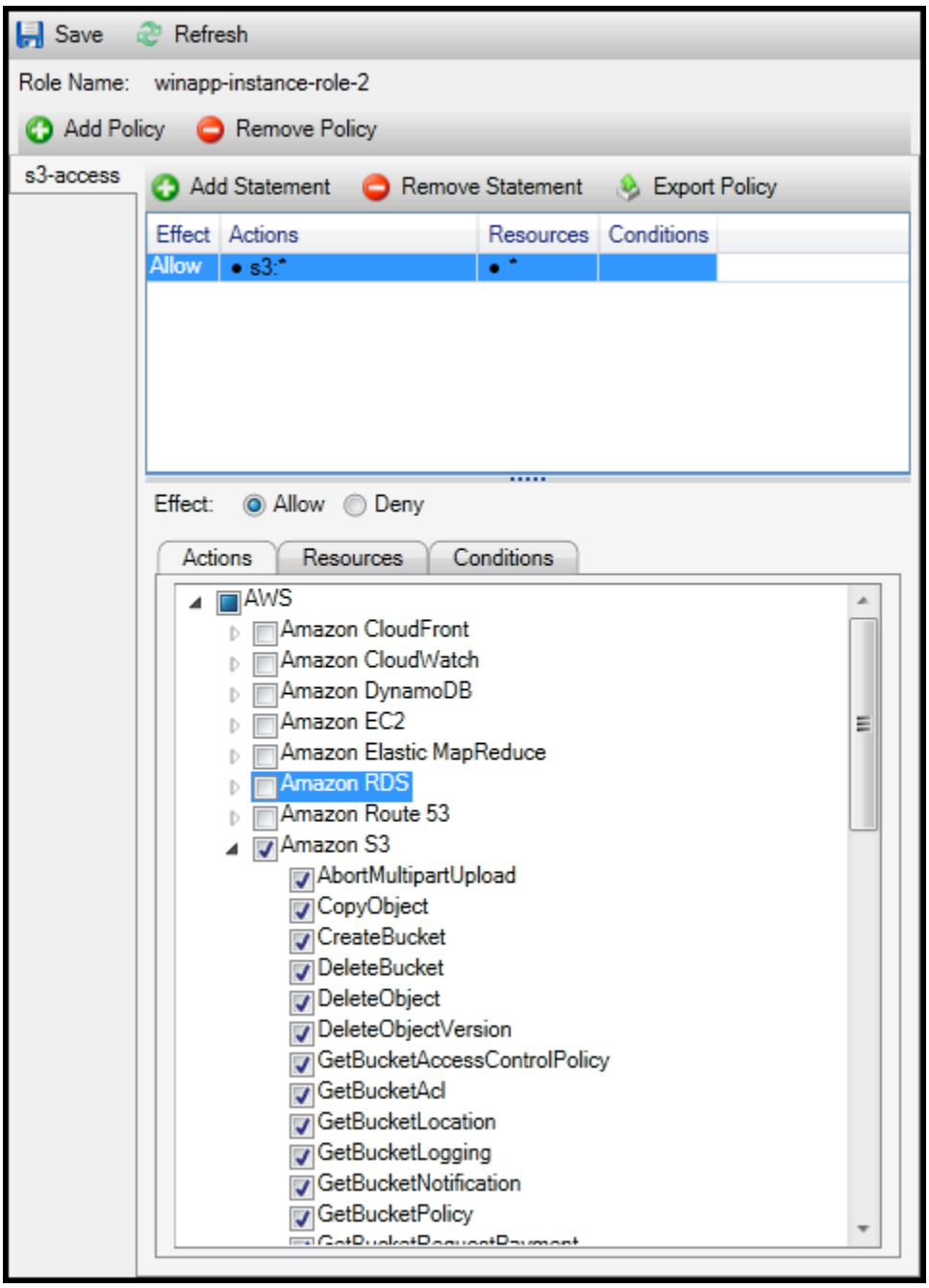
Uma guia associada à função será exibida noAWSExplorador. Escolha o link Add Policy (Adicionar política).

Na caixa de diálogo New Policy Name (Nome da nova política), digite um nome para a política (por exemplo, s3-access).



New Policy Name dialog box

No editor de políticas, adicione declarações de política para especificar o nível de acesso a ser dado à função (neste exemplo, winapp-instance-role-2) associada à política. Neste exemplo, uma política dá acesso total ao Amazon S3, mas não a todos os outros recursos.



Specify IAM policy

Para obter controle de acesso mais preciso, você pode expandir os subnós no editor de políticas a fim de permitir ou não ações associadas à Amazon Web Services.

Depois de editar a política, escolha Save (Salvar).

AWS Lambda

Desenvolva e implante suas funções C# Lambda baseadas em .NET Core com o. AWS Toolkit for Visual Studio AWS Lambda é um serviço de computação que permite executar código sem provisionar ou gerenciar servidores. O Toolkit for Visual Studio AWS Lambda inclui modelos de projeto do.NET Core para Visual Studio.

Para obter mais informações sobre AWS Lambda, consulte o AWS Lambda Developer Guide.

Para obter mais informações sobre o.NET Core, consulte o guia do Microsoft.NET Core. Para obter os pré-requisitos e as instruções de instalação do .NET Core para plataformas Windows, macOS e Linux, consulte Downloads do .NET Core.

Os tópicos a seguir descrevem como trabalhar com o AWS Lambda uso do Toolkit for Visual Studio.

Tópicos

Projeto básico do AWS Lambda

Você pode criar uma função Lambda usando modelos de projeto do Microsoft.NET Core, no. AWS Toolkit for Visual Studio

Criar um projeto do Lambda do Visual Studio .NET Core

Você pode usar modelos e esquemas do Lambda-Visual Studio para ajudar a acelerar a inicialização do seu projeto. Os blueprints do Lambda contêm funções pré-escritas que simplificam a criação de uma base de projeto flexível.

> **Note**
>
> O serviço Lambda tem limites de dados em diferentes tipos de pacotes. Para obter informações detalhadas sobre limites de dados, consulte o tópico de cotas do Lambda no Guia do usuário do Lambda AWS .

Para criar um projeto Lambda no Visual Studio

1. No Visual Studio, expanda o menu Arquivo, expanda Novo e escolha Projeto.
2. Na caixa de diálogo Novo projeto, defina as caixas suspensas Idioma, Plataforma e Tipo de projeto como “Tudo” e digite aws lambda no campo Pesquisar. Escolha o modelo do Projeto AWS Lambda (.NET Core - C#).
3. No campo Nome, insira**`AWSLambdaSample`**, especifique o local do arquivo desejado e escolha Criar para continuar.
4. Na página Selecionar blueprint, selecione o blueprint de função vazia e escolha Finalizar para criar o projeto do Visual Studio.

Revisar os arquivos de projeto

Há dois arquivos de projeto revisar: `aws-lambda-tools-defaults.json` e `Function.cs`.

O exemplo a seguir mostra o `aws-lambda-tools-defaults.json` arquivo, que é criado automaticamente como parte do seu projeto. Você pode definir opções de compilação usando os campos desse arquivo.

> **Note**
>
> Os modelos de projeto no Visual Studio contêm muitos campos diferentes, observe o seguinte:
>
> - function-handler: especifica o método que é executado quando a função Lambda é executada
> - A especificação de um valor no campo do manipulador de funções preenche previamente esse valor no assistente de publicação.
> - Se você renomear a função, classe ou montagem, também precisará atualizar o campo correspondente no `aws-lambda-tools-defaults.json` arquivo.

```
{
  "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.",
```

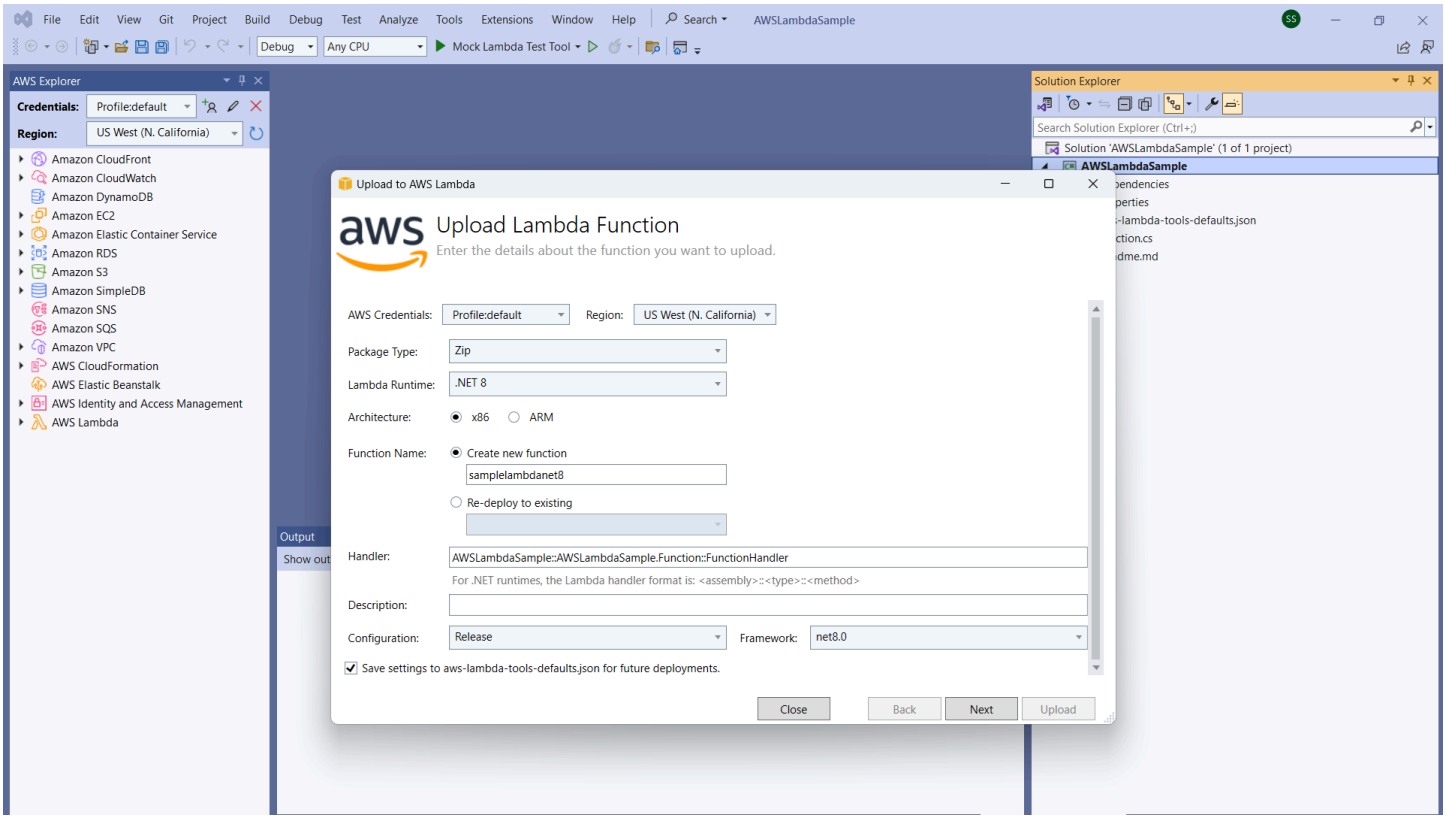
```
    "dotnet lambda help",
    "All the command line options for the Lambda command can be specified in this
 file."
  ],
  "profile": "default",
  "region": "us-west-2",
  "configuration": "Release",
  "function-architecture": "x86_64",
  "function-runtime": "dotnet8",
  "function-memory-size": 512,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

Examine o arquivo `Function.cs`. O `Function.cs` define as funções c# a serem expostas como funções do Lambda. Esse `FunctionHandler` é a funcionalidade do Lambda que é executada quando a função do Lambda é executada. Neste projeto, há uma função definida: `FunctionHandler`, que chama `ToUpper()` no texto de entrada.

O projeto já está pronto para ser publicado no Lambda.

Publicando na Lambda

O procedimento e a imagem a seguir demonstram como carregar sua função no Lambda usando o. AWS Toolkit for Visual Studio



Publicando sua função no Lambda

1. Navegue até o AWS Explorer expandindo Exibir e escolhendo AWS Explorer.
2. No Solution Explorer, abra o menu de contexto do projeto que você deseja publicar (clique com o botão direito do mouse) e escolha Publish to AWS Lambda para abrir a janela Carregar função Lambda.
3. Na janela Carregar função Lambda, preencha os seguintes campos:

    a. Tipo de embalagem: Escolha**`Zip`**. Um arquivo ZIP será criado como resultado do processo de compilação e será carregado no Lambda. Como alternativa, você pode escolher Package Type**`Image`**. O tutorial: Projeto básico do Lambda criando uma imagem do Docker descreve como publicar usando o Package Type. **`Image`**

    b. Lambda Runtime: escolha seu Lambda Runtime no menu suspenso.

    c. Arquitetura: selecione o radial para sua arquitetura preferida.

    d. Nome da função: selecione o radial para Criar nova função e, em seguida, insira um nome de exibição para sua instância Lambda. Esse nome é referenciado tanto pelo AWS Explorer quanto pelas AWS Management Console telas.

e. Manipulador: use esse campo para especificar um manipulador de funções. Por exemplo: **`AWSLambdaSample::AWSLambdaSample.Function::FunctionHandler`**.

f. (Opcional) Descrição: insira um texto descritivo para exibir com sua instância, de dentro do AWS Management Console.

g. Configuração: Escolha sua configuração preferida no menu suspenso.

h. Estrutura: Escolha sua estrutura preferida no menu suspenso.

i. Salvar configurações: selecione essa caixa para salvar suas configurações atuais `aws-lambda-tools-defaults.json` como padrão para futuras implantações.

j. Escolha Avançar para prosseguir até a janela Detalhes avançados da função.

4. Na janela Detalhes avançados da função, preencha os seguintes campos:

a. Nome da função: escolha uma função associada à sua conta. A função fornece credenciais temporárias para todas as chamadas de AWS serviço feitas pelo código na função. Se você não tiver uma função, role para localizar Nova função com base na política AWS gerenciada no seletor suspenso e escolha. AWSLambdaBasicExecutionRole Essa função tem permissões de acesso mínimas.

> **Note**
>
> Sua conta deve ter permissão para executar a ListPolicies ação do IAM, ou a lista de nomes da função ficará vazia e você não poderá continuar.

b. (Opcional) Se sua função Lambda acessar recursos em uma Amazon VPC, selecione as sub-redes e os grupos de segurança.

c. (Opcional) Defina todas as variáveis de ambiente que sua função Lambda precisa. As chaves são criptografadas automaticamente pela chave de serviço padrão, que é gratuita. Como alternativa, você pode especificar uma AWS KMS chave, pela qual há uma cobrança. KMS é um serviço gerenciado que você pode usar para criar e controlar chaves de criptografia usadas para criptografar os dados. Se você tiver uma AWS KMS chave, poderá selecioná-la na lista.

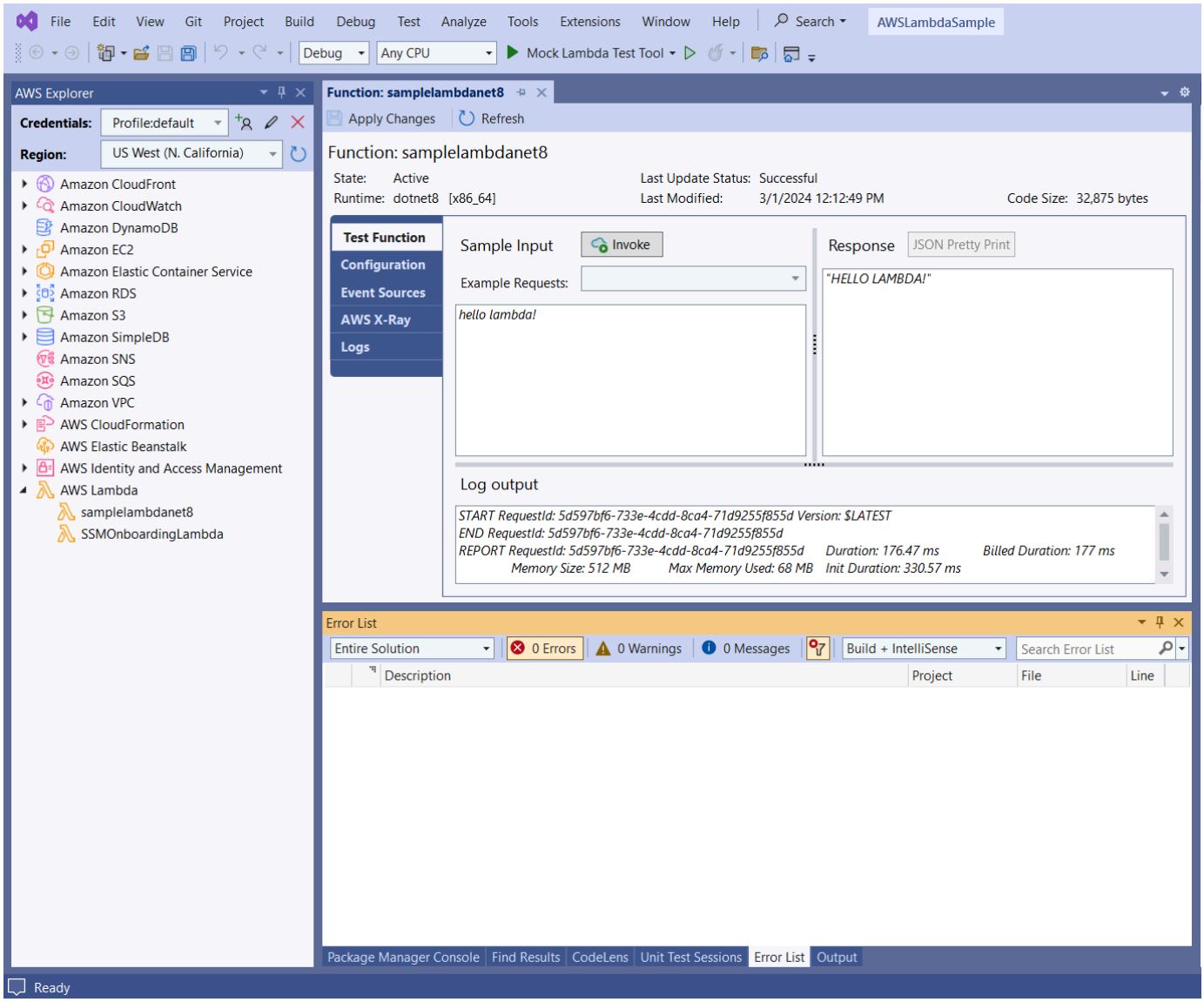
5. Escolha Carregar para abrir a janela Função de Upload e iniciar o processo de upload.

> **Note**
>
> A página Função de Uploading é exibida enquanto a função está sendo carregada para. AWS Para manter o assistente aberto após o upload, de maneira que você possa

visualizar o relatório, desmarque Fechar o assistente automaticamente após a conclusão bem-sucedida na parte inferior do formulário antes da conclusão do upload.
Depois que a função for carregada, sua função do Lambda estará ativa. A página Função: é aberta e exibe a configuração da sua nova função do Lambda.

6. Na guia Função de teste, insira o `hello lambda!` campo de entrada de texto e escolha Invocar para invocar manualmente sua função Lambda. Seu texto aparece na guia Resposta, convertido em maiúsculas.

> **Note**
>
> Você pode reabrir a visualização Função: a qualquer momento clicando duas vezes na instância implantada, localizada no AWS Explorer abaixo do nó AWS Lambda.



7. (Opcional) Para confirmar que você publicou com sucesso sua função Lambda, faça login no AWS Management Console e escolha Lambda. O console exibe todas as funções do Lambda publicadas, incluindo a que você acabou de criar.

Limpeza

Se você não quiser continuar desenvolvendo com este exemplo, exclua a função que implantada para que você não receba cobranças por recursos não utilizados em sua conta.

> **Note**
>
> O Lambda monitora automaticamente as funções do Lambda para você, relatando métricas por meio da Amazon. CloudWatch Para monitorar e solucionar problemas de sua função, consulte o tópico Solução de problemas e monitoramento de funções AWS Lambda com a CloudWatch Amazon no Guia AWS Lambda do desenvolvedor.

Como excluir uma função

1. No AWS Explorer, expanda o AWS Lambdanó.
2. Clique com o botão direito na instância implantada e escolha Excluir.

Projeto básico do AWS Lambda de criação de imagem do Docker

Você pode usar o Toolkit for Visual Studio para implantar AWS Lambda sua função como uma imagem do Docker. Usando o Docker, você tem mais controle sobre seu tempo de execução. Por exemplo, você pode escolher tempos de execução personalizados, como o.NET 8.0. A imagem do Docker é implantada da mesma forma que qualquer outra imagem de contêiner. Este tutorial é muito semelhante ao Tutorial: Projeto básico do Lambda, com duas diferenças:

- Um Dockerfile está incluído no projeto.
- Uma configuração de publicação alternativa é escolhida.

Para obter informações sobre imagens de contêiner do Lambda, consulte Pacotes de implantação do Lambda no Guia do desenvolvedor do AWS Lambda .

Para obter informações adicionais sobre como trabalhar com o Lambda AWS Toolkit for Visual Studio, consulte Usando os AWS Lambda modelos no AWS Toolkit for Visual Studio tópico deste Guia do usuário.

Criar um projeto do Lambda do Visual Studio .NET Core

Você pode usar modelos e esquemas do Lambda Visual Studio para ajudar a acelerar a inicialização do seu projeto. Os blueprints do Lambda contêm funções pré-escritas que simplificam a criação de uma base de projeto flexível.

Como criar um projeto do Lambda do Visual Studio .NET Core

1. No Visual Studio, expanda o menu Arquivo, expanda Novo e escolha Projeto.
2. Na caixa de diálogo Novo projeto, defina as caixas suspensas Idioma, Plataforma e Tipo de projeto como “Tudo” e digite **`aws lambda`** no campo Pesquisar. Escolha o modelo do Projeto AWS Lambda (.NET Core - C#).
3. No campo Nome do projeto, insira**`AWSLambdaDocker`**, especifique a localização do arquivo e escolha Criar.
4. Na página Selecionar esquema, escolha o blueprint .NET 8 (imagem de contêiner) e, em seguida, escolha Concluir para criar o projeto do Visual Studio. Você já pode revisar a estrutura do projeto e o código.

Revisando arquivos de projeto

As seções a seguir examinam os três arquivos de projeto criados pelo blueprint do.NET 8 (Container Image):

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

1. Dockerfile

A `Dockerfile` executa três ações principais:

- `FROM`: estabelece a imagem base a ser utilizada para essa imagem. Essa imagem base fornece o runtime do .NET, runtime do Lambda e um script de shell que oferece um ponto de entrada para o processo do .NET para Lambda.
- `WORKDIR`: estabelece o diretório de trabalho interno da imagem como`/var/task`.
- `COPY`: copiará os arquivos gerados pelo processo de construção de sua localização local para o diretório de trabalho da imagem.

A seguir estão as `Dockerfile` ações opcionais que você pode especificar:

- `ENTRYPOINT`: a imagem base já inclui um`ENTRYPOINT`, que é o processo de inicialização executado quando a imagem é iniciada. Se você desejar especificar o seu, essa ação substituirá esse ponto de entrada básico.
- `CMD`: instrui AWS qual código personalizado você deseja executar. Ele espera um nome totalmente qualificado para seu método personalizado. Essa linha precisa ser incluída diretamente no Dockerfile ou pode ser especificada durante o processo de publicação.

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

Veja a seguir um exemplo de um Dockerfile criado pelo 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

O `aws-lambda-tools-defaults.json` arquivo é usado para especificar valores padrão para o assistente de implantação do Toolkit for Visual Studio e a CLI do.NET Core. A lista a seguir descreve os campos que você pode definir no seu `aws-lambda-tools-defaults.json` arquivo.

- `profile`: define seu AWS perfil.
- `region`: define a AWS região em que seus recursos são armazenados.

- `configuration`: define a configuração usada para publicar sua função.
- `package-type`: define o tipo de pacote de implantação como uma imagem de contêiner ou arquivo de arquivo.zip.
- `function-memory-size`: define a alocação de memória para sua função em MB.
- `function-timeout`: o tempo limite é o tempo máximo em segundos que uma função Lambda pode ser executada. Você pode ajustar isso em incrementos de 1 segundo até um valor máximo de 15 minutos.
- `docker-host-build-output-dir`: define o diretório de saída do processo de construção que se correlaciona com as instruções no. `Dockerfile`
- `image-command`: é um nome totalmente qualificado para seu método, o código que você deseja que a função Lambda execute. A sintaxe é: `{Assembly}::{Namespace}.{ClassName}::{MethodName}`. Para obter mais informações, consulte Handler signatures. Aqui, a configuração `image-command` preenche automaticamente esse valor no assistente de publicação do Visual Studio em um momento posterior.

Veja a seguir um exemplo de um aws-lambda-tools-defaults .json criado pelo 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

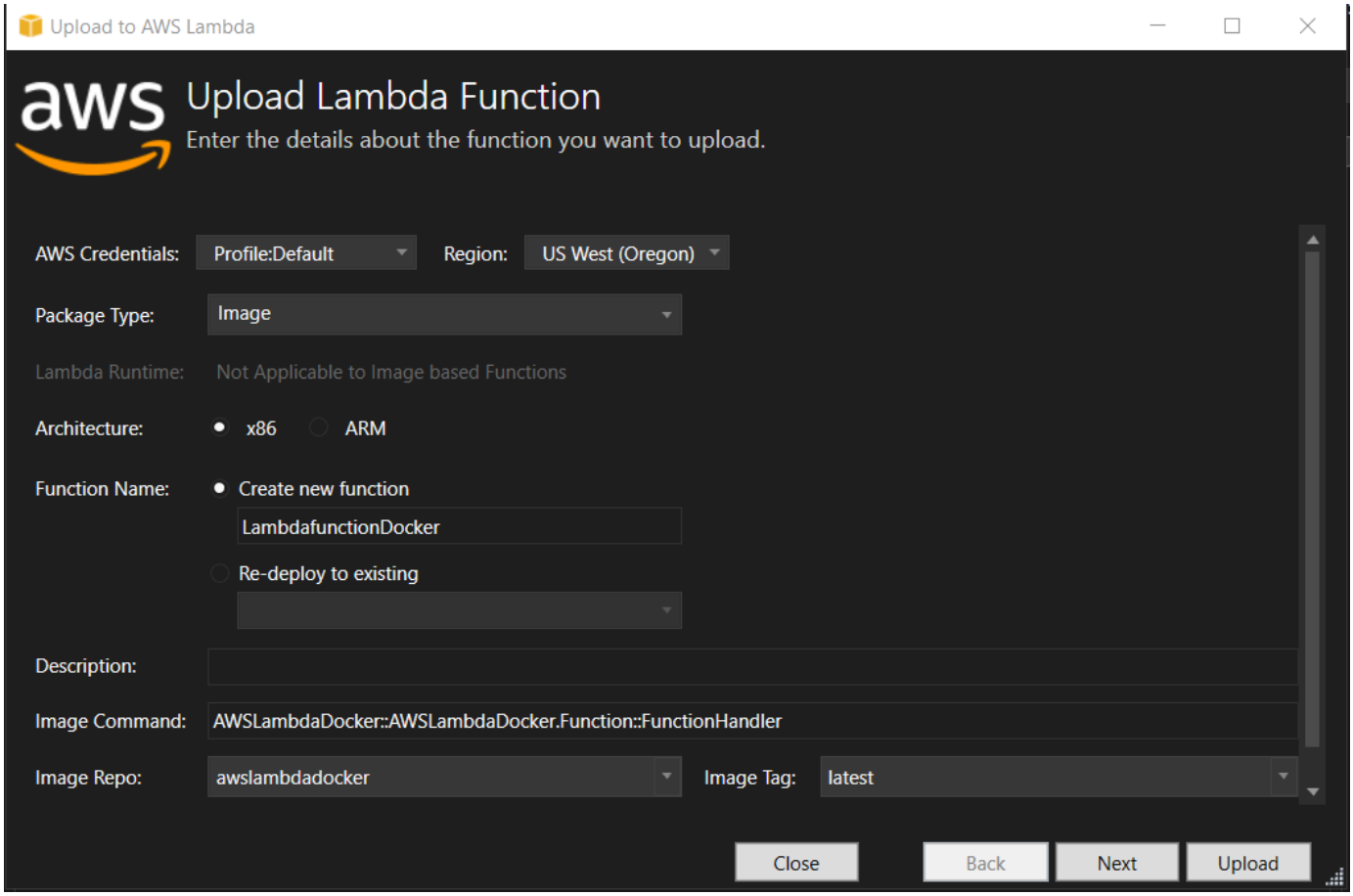
O `Function.cs` arquivo define as funções c# a serem expostas como funções Lambda. Esse `FunctionHandler` é a funcionalidade do Lambda que é executada quando a função do Lambda é executada. Neste projeto, `FunctionHandler` chama `ToUpper()` o texto de entrada.

Publicar no Lambda

As imagens do Docker que são geradas pelo processo de compilação são carregadas no Amazon Elastic Container Registry (Amazon ECR). O Amazon ECR é um registro de contêiner do Docker totalmente gerenciado que facilita o armazenamento, o gerenciamento e a implantação de imagens de contêiner do Docker. O Amazon ECR hospeda a imagem, à qual o Lambda então se refere para fornecer a funcionalidade programada do Lambda quando invocada.

Como publicar uma função no Lambda

1. No Solution Explorer, abra o menu de contexto do projeto (clique com o botão direito do mouse) e escolha Publish to AWS Lambda para abrir a janela Carregar função Lambda.
2. Na página Carregar função Lambda, faça o seguinte:



a. Em Tipo de pacote, **`Image`** foi selecionado automaticamente como seu Tipo de pacote porque o assistente de publicação detectou um `Dockerfile` em seu projeto.

b. Em Nome da função, insira um nome de exibição para sua instância do Lambda. Esse nome é o nome de referência exibido no AWS Explorer no Visual Studio e no AWS Management Console.

c. Em Descrição, insira o texto a ser exibido com sua instância no AWS Management Console.

d. Em Comando de imagem, insira um caminho totalmente qualificado para o método que você deseja que a função do Lambda execute: **`AWSLambdaDocker::AWSLambdaDocker.Function::FunctionHandler`**.

> **Note**
>
> Qualquer nome de método inserido aqui substituirá qualquer instrução CMD no Dockerfile. A inserção do comando de imagem é opcional somente se o `Dockerfile` incluir uma `CMD` para instruir como iniciar a função do Lambda.

e. Em Repositório de imagens, insira o nome de um Amazon Elastic Container Registry novo ou existente. A imagem do Docker que o processo de compilação cria é carregada nesse registro. A definição do Lambda que está sendo publicada fará referência a essa imagem do Amazon ECR.

f. Em Tag da imagem, insira uma tag do Docker para associá-la à sua imagem no repositório.

g. Selecione Next (Próximo).

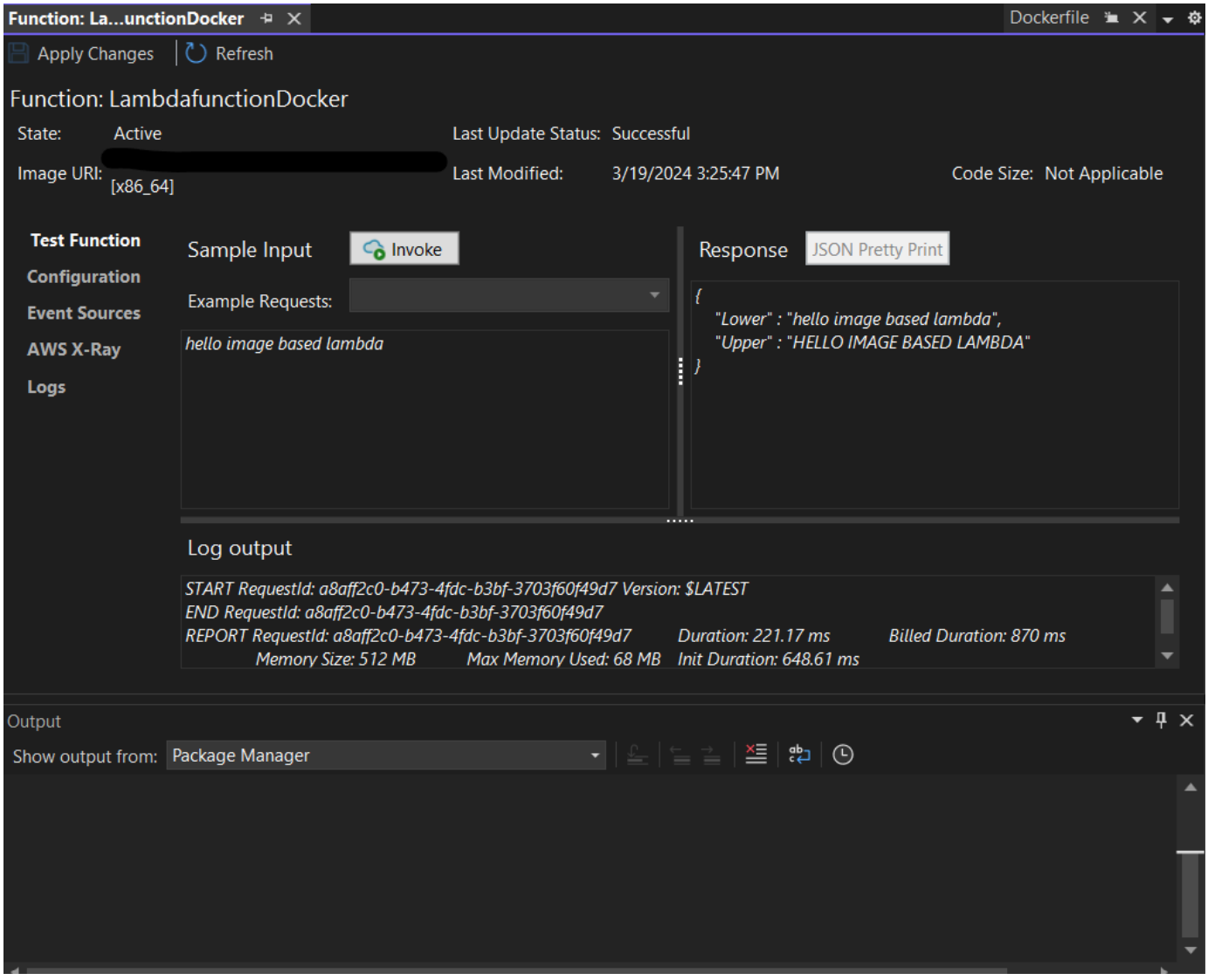
3. Na página Detalhes avançados da função, em Nome da função, escolha uma função associada à sua conta. A função é usada para fornecer credenciais para todas as chamadas à Amazon Web Services feitas pelo código na função. Se você não tiver uma função, escolha Nova função com base na política AWS gerenciada e, em seguida, escolha AWSLambdaBasicExecutionRole.

> **Note**
>
> Sua conta precisa ter permissão para executar a ListPolicies ação do IAM, ou a lista de nomes da função ficará vazia.

4. Escolha Carregar para iniciar os processos de upload e publicação.

> **Note**
>
> A página Carregando a função é exibida enquanto a função está sendo carregada. Em seguida, o processo de publicação cria a imagem com base nos parâmetros de configuração, cria o repositório do Amazon ECR, se necessário, carrega a imagem no repositório e cria o Lambda faz referência a esse repositório com essa imagem. Depois que a função é carregada, a página Função é aberta e exibe a configuração da nova função do Lambda.

5. Para invocar manualmente a função do Lambda, na guia Função de teste, insira `hello image based lambda` no campo de entrada de texto livre da solicitação e escolha Invocar. Seu texto, convertido em maiúsculas, aparecerá em Resposta.



6. Para visualizar o repositório, no AWS Explorer, em Amazon Elastic Container Service, escolha Repositórios.

   Você pode reabrir a visualização Função: a qualquer momento clicando duas vezes na instância implantada, localizada no AWS Explorer abaixo do nó AWS Lambda.

   > **Note**
   >
   > Se a janela do AWS Explorer não estiver aberta, você pode encaixá-la via Exibir -> AWS Explorer

7. Observe as opções adicionais de configuração específicas da imagem na guia Configuração. Essa guia possibilita substituir o `ENTRYPOINT`, `CMD` e `WORKDIR` que podem ter sido especificados no Dockerfile. Descrição é a descrição que você inseriu (se for o caso) durante o upload/publicação.

Limpeza

Se você não quiser continuar desenvolvendo com este exemplo, lembre-se de excluir a função e a imagem do ECR que foram implantadas para que você não receba cobranças por recursos não utilizados em sua conta.

- As funções podem ser excluídas clicando com o botão direito na instância implantada, localizada no AWS Explorer abaixo do nó AWS Lambda.
- Os repositórios podem ser excluídos no AWS Explorer em Amazon Elastic Container Service -> Repositórios.

Próximos Passos

Para obter informações sobre como criar e testar imagens do Lambda, consulte Trabalhar com imagens de contêiner do Lambda.

Para obter informações sobre implantação, permissões e substituição de configurações de imagens de contêiner, consulte Configurar funções.

Tutorial: Crie e teste um aplicativo sem servidor com AWS Lambda

Você pode criar um aplicativo Lambda sem servidor usando um modelo. AWS Toolkit for Visual Studio Os modelos de projeto Lambda incluem um para um aplicativo AWS sem servidor, que é a AWS Toolkit for Visual Studio implementação do modelo de aplicativo AWS sem servidor (SAM).AWS Usando esse tipo de projeto, você pode desenvolver uma coleção de AWS Lambda funções e implantá-las com todos os AWS recursos necessários como um aplicativo inteiro, usando AWS CloudFormation para orquestrar a implantação.

Para obter pré-requisitos e informações sobre como configurar o AWS Toolkit for Visual Studio, consulte Usando os modelos AWS Lambda no Toolkit for Visual Studio AWS.

Tópicos

Criar um projeto de aplicação sem servidor da AWS

AWS Projetos de aplicativos sem servidor criam funções Lambda com um modelo sem servidor. AWS CloudFormation AWS CloudFormation os modelos permitem que você defina recursos adicionais, como bancos de dados, adicione funções do IAM e implante várias funções ao mesmo tempo. Isso difere dos projetos AWS Lambda, que se concentram no desenvolvimento e na implantação de uma única função Lambda.

O procedimento a seguir descreve como criar um novo projeto de aplicativo AWS sem servidor.

1. No Visual Studio, expanda o menu Arquivo, expanda Novo e escolha Projeto.
2. Na caixa de diálogo Novo projeto, verifique se as caixas suspensas Idioma, Plataforma e Tipo de projeto estão definidas como “Tudo...” e insira **`aws lambda`** no campo Pesquisar.
3. Selecione o modelo AWS Serverless Application with Tests (.NET Core - C#).

> **Note**
>
> É possível que o modelo Aplicativo AWS sem servidor com testes (.NET Core - C#) não seja preenchido na parte superior dos resultados.

4. Clique em Avançar para abrir a caixa de diálogo Configurar seu novo projeto.
5. Na caixa de diálogo Configurar seu novo projeto, insira **`ServerlessPowertools`** o Nome e preencha os campos restantes de acordo com sua preferência. Escolha o botão Criar para prosseguir até a caixa de diálogo Selecionar blueprint.
6. Na caixa de diálogo Selecionar esquema, escolha o Powertools para o AWS Lambda blueprint e, em seguida, escolha Concluir para criar o projeto do Visual Studio.

Revisando os arquivos do aplicativo sem servidor

As seções a seguir fornecem uma visão detalhada de três arquivos de aplicativos sem servidor criados para seu projeto:

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

1. modelo sem servidor

Um `serverless.template` arquivo é um AWS CloudFormation modelo para declarar suas funções sem servidor e outros recursos. AWS O arquivo incluído neste projeto contém uma declaração para uma única função Lambda que será exposta por meio do Amazon API Gateway como uma HTTP `*Get*` operação. Você pode editar esse modelo para personalizar a função existente ou adicionar mais funções e outros recursos exigidos pelo seu aplicativo.

Este é um exemplo de um arquivo `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 muitos dos campos de `...AWS:: Serverless::Function...` declaração são semelhantes aos campos de uma implantação do projeto Lambda. O registro, as métricas e o rastreamento do Powertools são configurados por meio das seguintes variáveis de ambiente:

- POWERTOOLS_SERVICE_NAME= ServerlessGreeting
- PowerTools_log_level=Informações
- POWERTOOLS_LOGGER_CASE= PascalCase
- PowerTools_tracer_capture_response=Verdadeiro
- PowerTools_tracer_capture_error=Verdadeiro
- POWERTOOLS_METRICS_NAMESPACE= ServerlessGreeting

Para obter definições e detalhes adicionais sobre as variáveis de ambiente, consulte o site Powertools for AWS Lambda references.

2. Functions.cs

`Functions.cs`é um arquivo de classe contendo um método C# mapeado para uma única função declarada no arquivo de modelo. A função Lambda responde aos `HTTP Get` métodos do API Gateway. Veja a seguir um exemplo do `Functions.cs` arquivo:

```
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`fornece os valores padrão para o assistente de AWS implantação dentro do Visual Studio e os AWS Lambda comandos adicionados à CLI do.NET Core. Veja a seguir um exemplo do `aws-lambda-tools-defaults.json` arquivo incluído neste projeto:

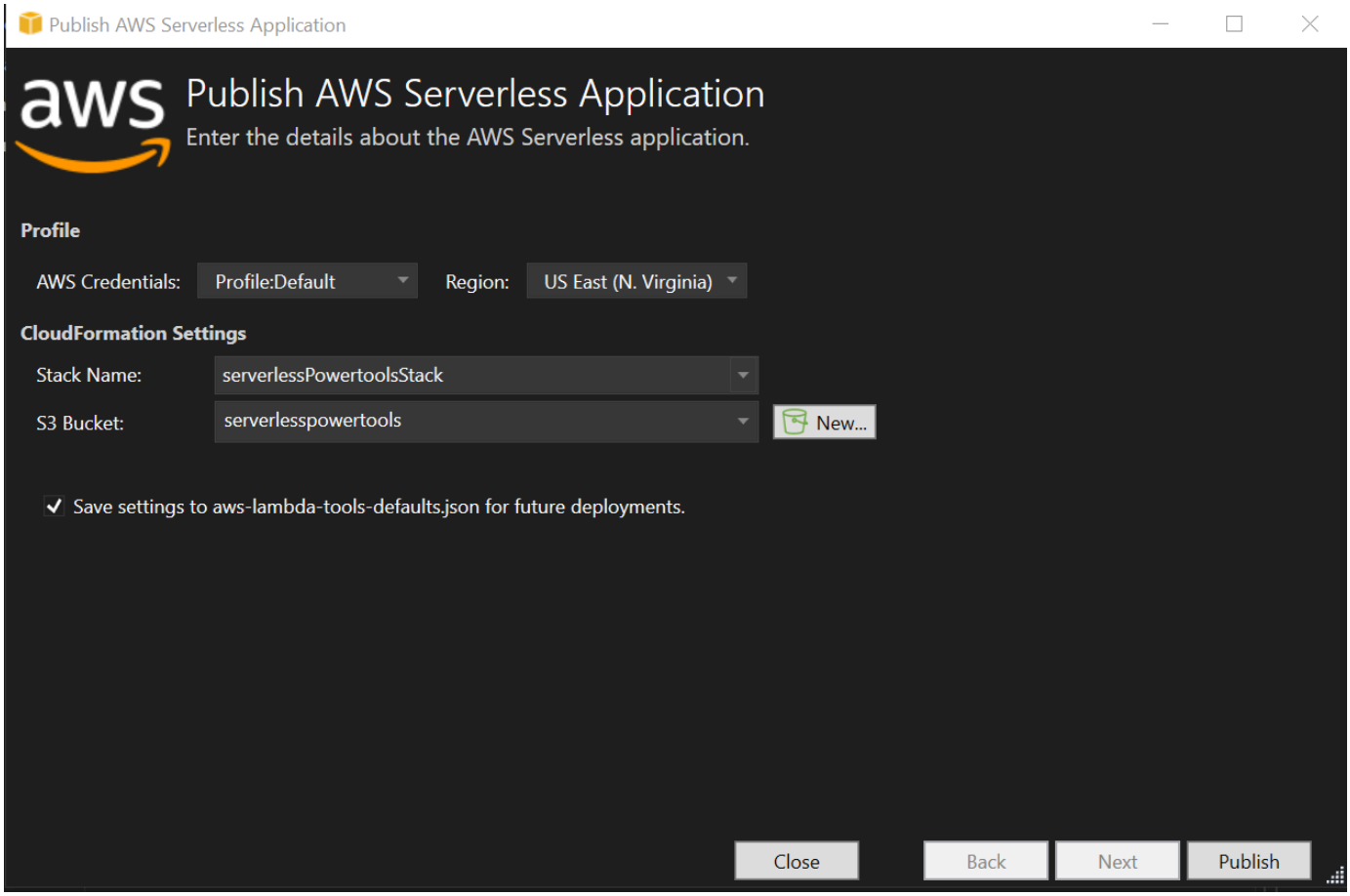
```
{
  "profile": "Default",
  "region": "us-east-1",
  "configuration": "Release",
  "s3-prefix": "ServerlessPowertools/",
  "template": "serverless.template",
  "template-parameters": ""
}
```

Implantar o aplicativo sem servidor

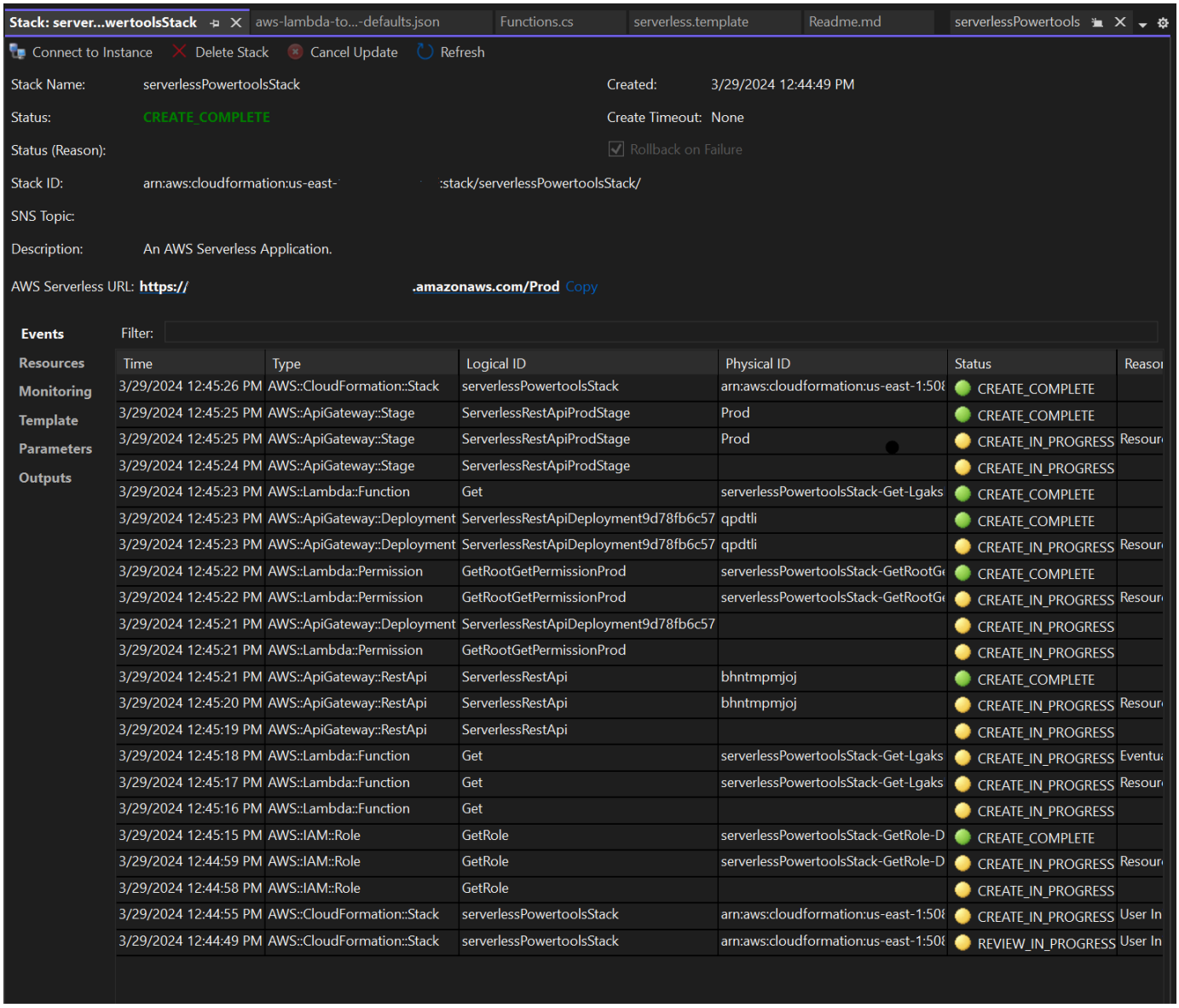
Para implantar seu aplicativo sem servidor, conclua as etapas a seguir:

1. No Solution Explorer, abra o menu de contexto do seu projeto (clique com o botão direito do mouse) e escolha Publish to AWS Lambda para abrir a caixa de diálogo Publish AWS Serverless Application.
2. Na caixa de diálogo Publicar aplicativo AWS sem servidor, insira um nome para o contêiner da AWS CloudFormation pilha no campo Nome da pilha.
3. No campo S3 Bucket, escolha um bucket Amazon S3 para o qual seu pacote de aplicativos será carregado ou escolha o Novo... botão e insira o nome de um novo bucket do Amazon S3. Em seguida, escolha Publicar para publicar para implantar seu aplicativo.

> **Note**
>
> Sua AWS CloudFormation pilha e o Amazon S3 Bucket devem existir na mesma região AWS . As configurações restantes do seu projeto são definidas no `serverless.template` arquivo.



4. A janela Stack View é aberta durante o processo de publicação, quando a implantação é concluída, o campo Status exibe:`CREATE_COMPLETE`.



Testar o aplicativo sem servidores

Quando a criação da pilha estiver concluída, você poderá visualizar seu aplicativo usando o URL sem AWS servidor. Se você concluiu este tutorial sem adicionar nenhuma função ou parâmetro adicional, acessar seu URL AWS sem servidor exibe a seguinte frase em seu navegador da web:. `Hello Powertools for AWS Lambda (.NET)`

Tutorial: Creating an Amazon Rekognition Lambda Application

Este tutorial mostra como criar uma aplicação do Lambda que usa o Amazon Rekognition para marcar objetos do Amazon S3 com rótulos detectados.

Para obter pré-requisitos e informações sobre como configurar o AWS Toolkit for Visual Studio, consulte Usando os modelos AWS Lambda no Toolkit for Visual Studio AWS.

Criar um projeto do Image Rekognition do Lambda do Visual Studio .NET Core

O procedimento a seguir descreve como criar um aplicativo Amazon Rekognition Lambda a partir do. AWS Toolkit for Visual Studio

> **Note**
>
> Após a criação, seu aplicativo tem uma solução com dois projetos: o projeto de origem que contém o código da função Lambda para implantação no Lambda e um projeto de teste usando o xUnit para testar sua função localmente.
> Às vezes, o Visual Studio não consegue encontrar todas as NuGet referências para seus projetos. Isso ocorre porque os blueprints exigem dependências que devem ser recuperadas. NuGet Quando novos projetos são criados, o Visual Studio extrai apenas referências locais e não referências remotas de NuGet. Para corrigir NuGet erros: clique com o botão direito do mouse nas referências e escolha Restaurar pacotes.

1. No Visual Studio, expanda o menu Arquivo, expanda Novo e escolha Projeto.
2. Na caixa de diálogo Novo projeto, verifique se as caixas suspensas Idioma, Plataforma e Tipo de projeto estão definidas como “Tudo...” e insira **`aws lambda`** no campo Pesquisar.
3. Selecione o modelo AWS Lambda com testes (.NET Core - C#).
4. Clique em Avançar para abrir a caixa de diálogo Configurar seu novo projeto.
5. Na caixa de diálogo Configurar seu novo projeto, insira ImageRekognition "" como Nome e preencha os campos restantes de acordo com sua preferência. Escolha o botão Criar para prosseguir até a caixa de diálogo Selecionar blueprint.
6. Na caixa de diálogo Selecionar esquema, escolha o blueprint Detectar rótulos de imagem e, em seguida, escolha Concluir para criar o projeto do Visual Studio.

> **Note**
>
> Esse esquema fornece o código para escutar eventos do Amazon S3 e usa o Amazon Rekognition para detectar rótulos e adicioná-los ao objeto do S3 como tags.

Revisando arquivos de projeto

As seções a seguir examinam esses arquivos de projeto:

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

1. Function.cs

Dentro do `Function.cs` arquivo, o primeiro segmento do código é o atributo assembly, localizado na parte superior do arquivo. Por padrão, o Lambda só aceita parâmetros de entrada e tipos de tipo de retorno. `System.IO.Stream` Você deve registrar um serializador para usar classes digitadas para parâmetros de entrada e tipos de retorno. O atributo assembly registra o serializador Lambda JSON, que é `Newtonsoft.Json` usado para converter fluxos em classes digitadas. Você pode definir o serializador no nível de assembly ou método.

Veja a seguir um exemplo do 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
```

A classe tem dois construtores. O primeiro é um construtor padrão usado quando o Lambda invoca a função. Esse construtor cria os clientes de serviços Amazon S3 e Amazon Rekognition. O construtor também recupera AWS as credenciais desses clientes da função do IAM que você atribui à função ao implantá-la. A AWS região dos clientes é definida como a região em que sua função Lambda está sendo executada. Neste esquema, você só quer adicionar tags ao objeto Amazon S3 se o serviço Amazon Rekognition tiver um nível mínimo de confiança sobre o rótulo. Esse construtor verifica a variável de ambiente `MinConfidence` para determinar o nível de confiança aceitável. Você pode definir essa variável de ambiente ao implantar a função do Lambda.

Veja a seguir um exemplo do primeiro construtor de classe em: `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}");
    }
}
```

O exemplo a seguir demonstra como o segundo construtor pode ser utilizado para testes. O projeto de teste configura seus próprios clientes S3 e Rekognition e os transmite:

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

Veja a seguir um exemplo do `FunctionHandler` método dentro do `Function.cs` arquivo.

```
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` é o método que o Lambda chamará depois de construir a instância. O parâmetro de entrada é do tipo `S3Event`, e não um `Stream`. Você pode fazer isso por causa do serializador JSON do Lambda registrado. O `S3Event` contém todas as informações sobre o evento acionado no Amazon S3. A função percorre todos os objetos do S3 que fizeram parte do evento e pede ao Rekognition para detectar rótulos. Depois que os rótulos forem detectados, eles serão adicionados como tags ao objeto do S3.

> **Note**
>
> O código contém chamadas para`Console.WriteLine()`. Quando a função está sendo executada no Lambda, todas as chamadas são `Console.WriteLine()` redirecionadas para o Amazon Logs. CloudWatch

2. aws-lambda-tools-defaults.json

O `aws-lambda-tools-defaults.json` arquivo contém valores padrão que o blueprint definiu para preencher previamente alguns dos campos no assistente de implantação. Também é útil para definir opções de linha de comando para integração com a CLI do.NET Core.

Para acessar a integração da CLI do.NET Core, navegue até o diretório do projeto da função e digite. **`dotnet lambda help`**

> **Note**
>
> O manipulador da função indica qual método o Lambda deve chamar em resposta à função invocada. O formato desse campo é:`<assembly-name>::<full-type-name>::<method-name>`. O namespace deve ser incluído com o nome do tipo.

Implantar a função

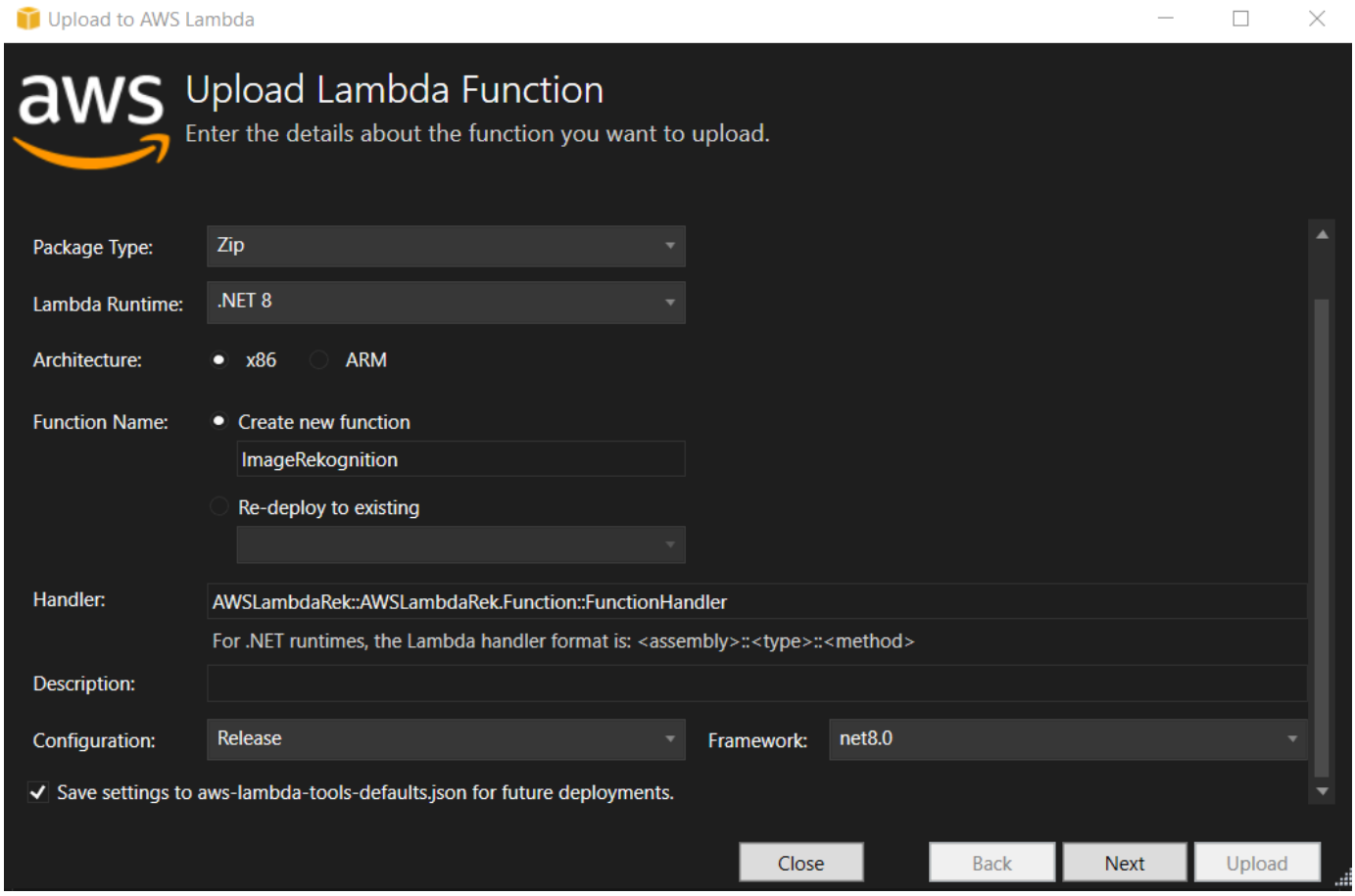
O procedimento a seguir descreve como implantar sua função Lambda.

1. No Solution Explorer, clique com o botão direito do mouse no projeto Lambda e escolha Publish to AWS Lambda para abrir a janela Upload to. AWS Lambda

> **Note**
>
> Os valores predefinidos são recuperados do `aws-lambda-tools-defaults.json` arquivo.

2. AWS Lambda Na janela Carregar para, insira um nome no campo Nome da função e escolha o botão Avançar para avançar até a janela Detalhes avançados da função.

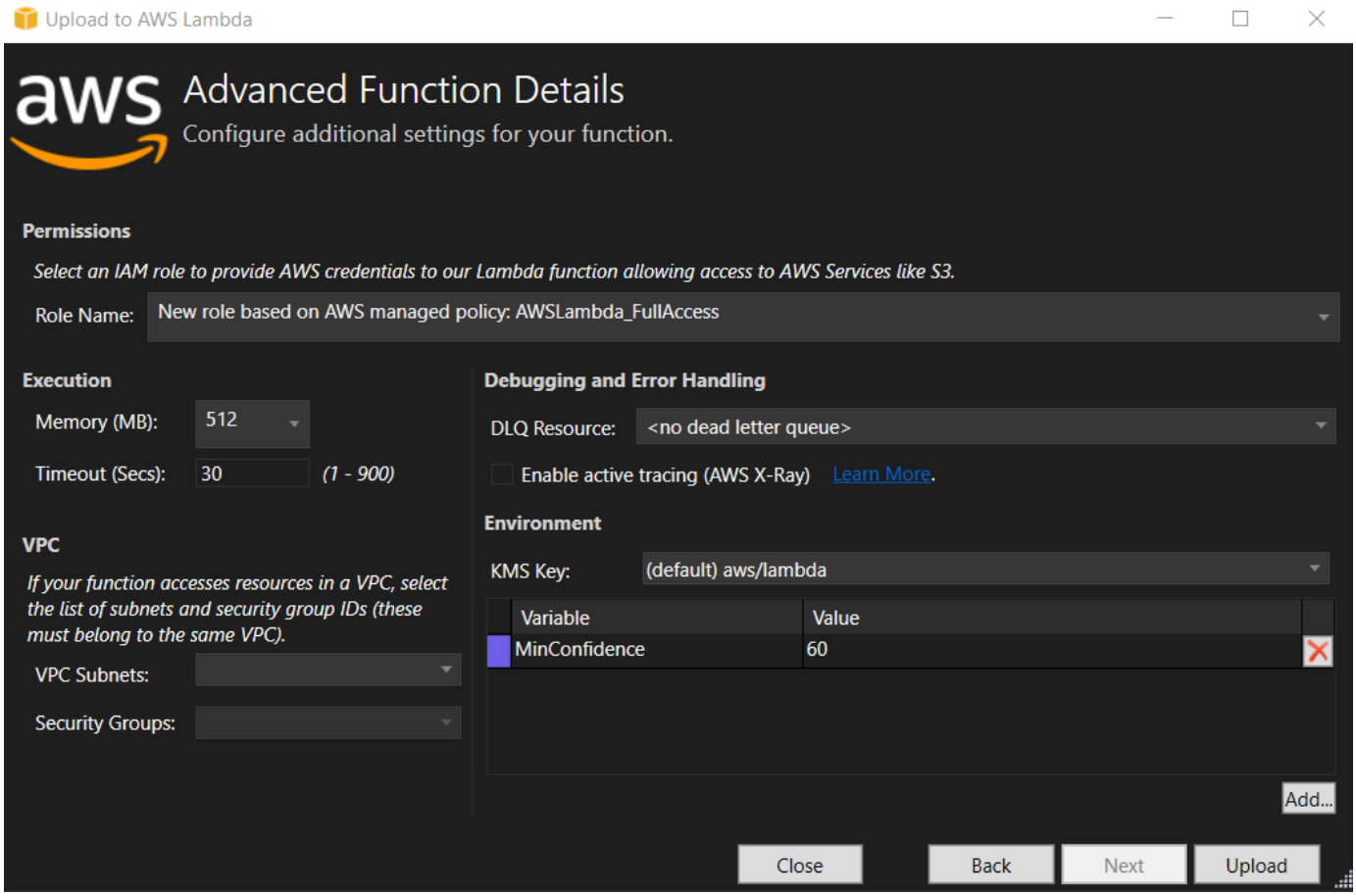
> **Note**
>
> Este exemplo usa o nome da função**`ImageRekognition`**.



3. Na janela Advanced Function Details, selecione uma função do IAM que permita que seu código acesse seus recursos do Amazon S3 e do Amazon Rekognition.

> **Note**
>
> Se você estiver acompanhando esse exemplo, selecione a `AWSLambda_FullAccess` função.

4. Defina `MinConfidence` a variável de ambiente como 60 e escolha Carregar para iniciar o processo de implantação. O processo de publicação é concluído quando a visualização Função é exibida no AWS Explorer.



5. Após uma implantação bem-sucedida, configure o Amazon S3 para enviar seus eventos para sua nova função navegando até a guia Fontes de eventos.

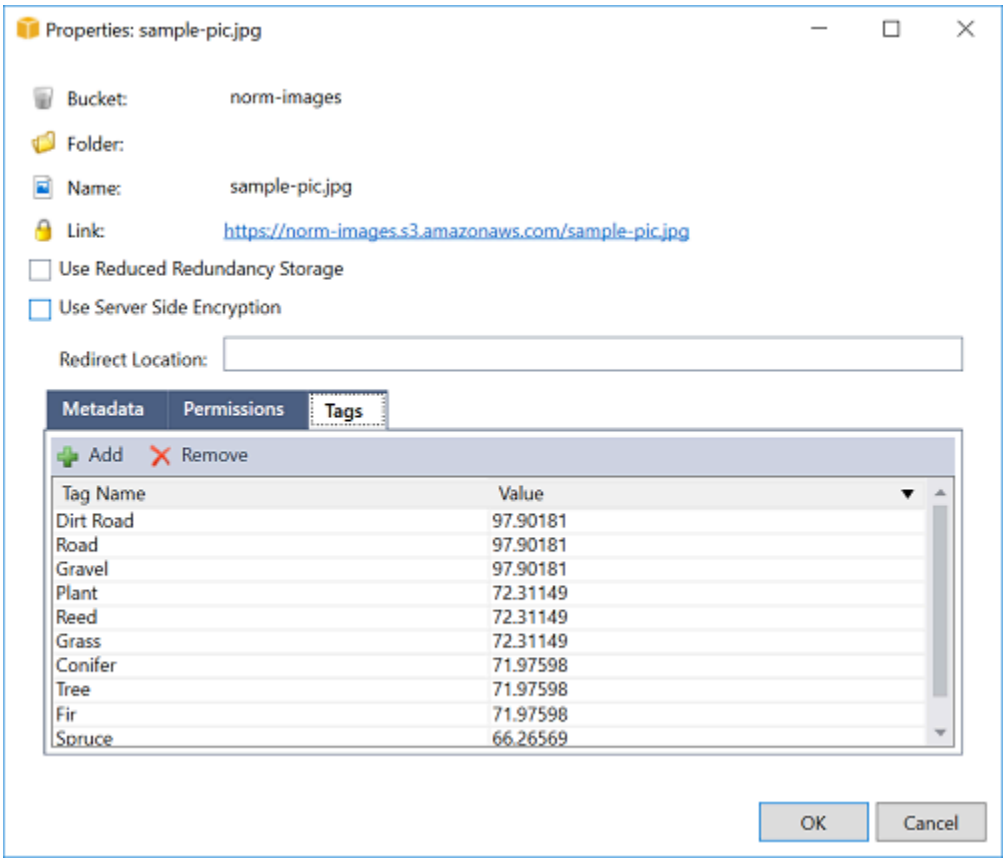
6. Na guia Fontes de eventos, escolha o botão Adicionar e, em seguida, selecione o bucket do Amazon S3 para se conectar à sua função Lambda.

> **Note**
>
> O bucket deve estar na mesma AWS região da sua função Lambda.

Testar a função do

Agora que a função está implantada e um bucket do S3 está configurado como uma fonte de eventos para ele, abra o navegador de buckets do S3 no AWS Explorer para o bucket selecionado por você. Em seguida, faça upload de algumas imagens.

Quando o upload estiver concluído, você poderá confirmar se a função foi executada observando os logs na visualização da função. Ou clique com o botão direito do mouse no navegador de buckets e escolha Properties (Propriedades). Na guia Tags, você pode visualizar as tags que foram aplicadas ao objeto.



Tutorial: Usando o Amazon Logging Frameworks AWS Lambda para criar registros de aplicativos

Você pode usar o Amazon CloudWatch Logs para monitorar, armazenar e acessar os registros do seu aplicativo. Para inserir dados de registro no CloudWatch Logs, use um AWS SDK ou instale o agente do CloudWatch Logs para monitorar determinadas pastas de registro. CloudWatch O Logs é integrado a várias estruturas populares de registro do.NET, simplificando os fluxos de trabalho.

Para começar a trabalhar com estruturas de registro de CloudWatch registros e do.NET, adicione o NuGet pacote apropriado e a fonte de saída de CloudWatch registros ao seu aplicativo e, em seguida, use sua biblioteca de registros normalmente. Isso permite que seu aplicativo registre mensagens com sua estrutura do.NET, enviando-as para o CloudWatch Logs e exibindo as mensagens de registro do seu aplicativo no console do CloudWatch Logs. Você também pode configurar métricas e alarmes no console de CloudWatch registros, com base nas mensagens de registro do seu aplicativo.

As estruturas de registro do.NET suportadas incluem:

- NLog: para ver, consulte o pacote nuget.org NLog.
- Log4net: Para ver, consulte o pacote nuget.org Log4net.
- Estrutura de registro do ASP.NET Core: para ver, consulte o pacote nuget.org ASP.NET Core logging Framework.

Veja a seguir um exemplo de um `NLog.config` arquivo que habilita o CloudWatch Logs e o console como saída para mensagens de log adicionando o `AWS.Logger.NLog` NuGet pacote e o AWS destino em`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>
```

Os plug-ins de registro são todos criados com base no AWS SDK for .NET e autenticam suas AWS credenciais em um processo semelhante ao SDK. O exemplo a seguir detalha as permissões exigidas pelas credenciais do plug-in de registro para acessar o CloudWatch Logs:

> **Note**
>
> Os plug-ins de registro AWS do.NET são um projeto de código aberto. Para obter mais informações, exemplos e instruções, consulte os tópicos de exemplos e instruções no GitHubrepositório.NET do AWS Logging.

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

Implantar no AWS

O Toolkit for Visual Studio oferece suporte à implantação de aplicativos emAWS Elastic Beanstalk contêineres ouAWS CloudFormation pilhas.

> **Note**
>
> Se você estiver usando o Visual Studio Express Edition:
>
> - Você pode usar o Docker CLI para implantar aplicativos em contêineres do Amazon ECS.
> - Você pode usar o AWSManagement Console para implantar aplicativos em contêineres do Elastic Beanstalk.
>
> Para implantações do Elastic Beanstalk, você deve primeiro criar um pacote de implantação na web. Para obter mais informações, consulte Como criar um pacote de implantação web no Visual Studio. Para a implantação do Amazon ECS, você deve ter uma imagem do Docker. Para obter mais informações, consulte Ferramentas do Visual Studio para Docker.

Tópicos

Trabalhar com o Publicar noAWSno Visual Studio

Publish to (Publicar no &CW;)AWSé uma experiência de implantação interativa que ajuda você a publicar seus aplicativos.NET noAWSdestinos de implantação, com suporte a aplicativos direcionados ao .NET Core 3.1 e posteriores. Trabalhar com o Publicar noAWSmantém seu fluxo de trabalho dentro do Visual Studio disponibilizando esses recursos de implantação, diretamente do seu IDE:

- A capacidade de implantar seu aplicativo com um único clique.
- Recomendações de implantação com base em seu aplicativo.

- Criação automática de Dockerfile, conforme relevante e exigido pelo ambiente do seu destino de implantação (destino de implantação).
- Configurações otimizadas para criar e empacotar seus aplicativos, conforme exigido pelo seu destino de implantação.

> **Note**
>
> Para obter informações adicionais sobre a publicação de aplicativos .NET Framework, consulte o guiaCriar e implantar aplicações .NET no Elastic Beanstalk
> Você também pode acessar Publicar noAWSdo CLI do .NET. Para obter mais informações, consulte o .Implantação de aplicativos .NET noAWSguide.

Tópicos

Pré-requisitos

Para publicar com êxito aplicativos .NET em umAWSserviço, instale o seguinte em seu dispositivo local:

- .NET Core 3.1+ (que inclui .NET5 e .NET6): Para obter informações adicionais sobre esses produtos e informações de download, visite oSite de download da Microsoft.
- Versão do Node.js 14.x ou posterior: O Node.js é necessário para ser executadoAWS Cloud Development Kit (AWS CDK). Para baixar ou obter mais informações sobre o Node.js, visite oSite de download Node.js.

> **Note**
>
> Publish to (Publicar no &CW;)AWSutilizaAWS CDKpara implantar seu aplicativo e toda a sua infraestrutura de implantação como um único projeto. Para obter mais informações sobreAWS CDKconsulte oCloud Development Kitguide.

- (Opcional) O Docker é usado ao implantar em um serviço baseado em contêiner, como o Amazon ECS. Para obter mais informações e para fazer download do Docker, consulte oDownload do Dockersite.

Tipos de aplicativos com suporte

Antes de publicar em um destino novo ou existente, comece criando ou abrindo um dos seguintes tipos de projeto no Visual Studio:

- Aplicativo ASP.NET Core
- Aplicativo .NET Console
- Blazor WebAssembly aplicativo

Publicar aplicativos noAWStem como alvo

Ao publicar em um novo destino, Publicar emAWSO orientará você durante o processo fazendo recomendações e usando configurações comuns. Se você precisar publicar em um destino configurado anteriormente, suas preferências serão armazenadas e poderão ser ajustadas ou estarão imediatamente disponíveis para implantação com um clique.

Publicar em um novo destino

A seguir, veja a descrição de como configurar o Publicar no.AWSpreferências de implantação, quando você estiver publicando em um novo destino.

1. Do atéAWSExplorer, expandaCredenciaise depois escolha oAWSperfil que corresponde à região eAWSserviços que são necessários para sua implantação.
2. Expandir oRegiãoe depois escolha oAWSregião que contém aAWSserviços que são necessários para sua implantação.
3. Do Visual StudioExplorer de soluções, abra o menu de contexto do (clique com o botão direito) do nome do projeto e escolhaPublish to (Publicar no &CW;)AWS. Isso abriráPublish to (Publicar no &CW;)AWS.
4. NoPublish to (Publicar no &CW;)AWS, escolhaPublicar no novo destinopara configurar uma nova implantação.

> **Note**
>
> Para modificar suas credenciais de implantação padrão, escolha ou clique no botãoEditelink localizado ao lado doCredenciaisseção, noPublish to (Publicar no &CW;)AWS.
> Para ignorar o processo de configuração de destino, escolhaPublicar no destino existentee escolha sua configuração preferida na lista de destinos de implantação anteriores.

5. Do atéPublicar destinospainel, escolha umAWSserviço para gerenciar a implantação do aplicativo.
6. Quando estiver satisfeito com sua configuração, escolhaPublicarpara iniciar o processo de implantação.

> **Note**
>
> Depois de iniciar uma implantação,Publish to (Publicar no &CW;)AWSO exibe as seguintes atualizações de status:
>
> - Durante o processo de implantação,Publish to (Publicar no &CW;)AWSexibe informações sobre o progresso da implantação.
> - Após o processo de implantação,Publish to (Publicar no &CW;)AWSindica se a implantação foi bem-sucedida ou não.
> - Após uma implantação bem-sucedida, oRecursosoferece informações adicionais sobre o recurso que foi criado. Essas informações variarão dependendo do tipo de aplicativo e da configuração da implantação.

Publicar em um destino existente

O seguinte descreve como republicar seu aplicativo .NET em um existenteAWSdestino.

1. Do atéAWSExplorer, expandaCredenciaise depois escolha oAWSperfil que corresponde à região eAWSserviços que são necessários para sua implantação.
2. Expandir oRegiãoe depois escolha oAWSregião que contém aAWSserviços que são necessários para sua implantação.

3. Do Visual StudioExplorer de soluções, clique com o botão do mouse no nome do projeto e escolhaPublish to (Publicar no &CW;)AWSAbrirPublish to (Publicar no &CW;)AWS.
4. NoPublish to (Publicar no &CW;)AWS, escolhaPublicar no destino existentepara selecionar seu ambiente de implantação em uma lista de destinos existentes.

> **Note**
>
> Se você publicou recentemente algum aplicativo para oAWSNuvem, esses aplicativos são exibidos em Publicar emAWS.

5. Selecione o destino de publicação no qual você deseja implantar o aplicativo e clique emPublicarpara iniciar o processo de implantação.

Implantar umAWS LambdaProjeto do com a CLI do .NET Core

O AWS Toolkit for Visual Studio inclui modelos de projeto do .NET Core do AWS Lambda para o Visual Studio. Você pode implantar funções do Lambda incorporadas no Visual Studio usando a Command Line Line Line Line Line Line Line Line Line Line Line Line Line Line Line

Tópicos

- Pré-requisitos
- Tópicos relacionados
- Listar os comandos do Lambda disponibilizados pela CLI do .NET Core
- Publicar um projeto do Lambda do .NET Core na CLI do .NET Core

Pré-requisitos

Antes de trabalhar com a CLI do .NET Core para implantar funções do Lambda, você deve cumprir os seguintes pré-requisitos:

- Certifique-se de que o Visual Studio 3 esteja instalado.
- Install.NET Core para Windows.
- Configurar a CLI do .NET Core para trabalhar com o Lambda. Para obter mais informações, consulteCLI do .NET CorenoAWS LambdaGuia do desenvolvedor.

- Instalar o Toolkit for Visual Studio. Para obter mais informações, consulte Instalando o AWS Toolkit for Visual Studio.

Tópicos relacionados

Os seguintes tópicos relacionados podem ser úteis ao usar a CLI do .NET Core para implantar funções do Lambda:

- Para obter mais informações sobre funções do Lambda, consulteO que é oAWSLambda?noAWS LambdaGuia do desenvolvedor.
- Para obter informações sobre como criar funções do Lambda no Visual Studio, consulteAWS Lambda.
- Para obter mais informações sobre o Microsoft .NET Core, consulte.NET Corena documentação online da Microsoft.

Listar os comandos do Lambda disponibilizados pela CLI do .NET Core

Para listar os comandos do Lambda que estão disponíveis na CLI do .NET Core, faça o seguinte.

1. Abra uma janela do prompt de comando e navegue até a pasta que contém um projeto do Lambda do Visual Studio .NET Core.
2. Digite `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>
```

Publicar um projeto do Lambda do .NET Core na CLI do .NET Core

As instruções a seguir pressupõem que você tenha criado uma função do .NET Core do AWS Lambda no Visual Studio.

1. Abra uma janela do prompt de comando e navegue até a pasta que contém o projeto do Lambda do Visual Studio .NET Core.
2. Digite `dotnet lambda deploy-function`.
3. Insira o nome da função a ser implantada. Ele pode ser um nome novo ou o nome de uma função existente.
4. Insira oAWSRegion (a região na qual a função do Lambda será implantada).
5. Quando solicitado, selecione ou crie a função do IAM que o Lambda vai pressupor ao executar a função.

Mediante uma conclusão bem-sucedida, a mensagem New Lambda function created (Nova função do Lambda criada) é exibida.

```
C:\Lambda\AWSLambda1\AWSLambda1>dotnet lambda deploy-function
Executing publish command
... invoking 'dotnet publish', working folder 'C:\Lambda\AWSLambda1\AWSLambda1\bin
\Release\netcoreapp1.0\publish'
... publish: Publishing AWSLambda1 for .NETCoreApp,Version=v1.0
... publish: Project AWSLambda1 (.NETCoreApp,Version=v1.0) will be compiled because
 expected outputs are missing
```

```
... publish: Compiling AWSLambda1 for .NETCoreApp,Version=v1.0
... publish: Compilation succeeded.
... publish:     0 Warning(s)
... publish:     0 Error(s)
... publish: Time elapsed 00:00:01.2479713
... publish:
... publish: publish: Published to C:\Lambda\AWSLambda1\AWSLambda1\bin\Release
\netcoreapp1.0\publish
... publish: Published 1/1 projects successfully
Zipping publish folder C:\Lambda\AWSLambda1\AWSLambda1\bin\Release
\netcoreapp1.0\publish to C:\Lambda\AWSLambda1\AWSLamb
da1\bin\Release\netcoreapp1.0\AWSLambda1.zip
Enter Function Name: (AWS Lambda function name)
DotNetCoreLambdaTest
Enter AWS Region: (The region to connect to AWS services)
us-west-2
Creating new Lambda function
Select IAM Role that Lambda will assume when executing function:
    1) lambda_exec_LambdaCoreFunction
    2) *** Create new IAM Role ***
1
New Lambda function created
```

Se você implantar uma função existente, a função de implantação só solicitará oAWSRegião :

```
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
```

Depois que a função do Lambda for implantada, ela estará pronta para ser usada. Para obter mais informações, consulteExemplos de como usar oAWSLambda.

O Lambda monitora automaticamente as funções do Lambda para você, informando métricas por meio da Amazon CloudWatch. Para monitorar e solucionar problemas de função do Lambda, consulteSolução de problemas e monitoramentoAWSFunções do Lambda com a Amazon CloudWatch.

Implantar no Elastic Beanstalk

AWS Elastic BeanstalkO é um serviço que simplifica o processo de provisionarAWSrecursos do para o aplicativo. O Elastic Beanstalk fornece todas asAWSinfraestrutura necessária para implantar seu aplicativo. Essa infraestrutura inclui:

- As instâncias do Amazon EC2 que hospedam os executáveis e o conteúdo do aplicativo.
- Um grupo de Auto Scaling para manter o número apropriado de instâncias do Amazon EC2 para dar suporte ao aplicativo.
- Um load balancer do Elastic Load Balancing que roteia o tráfego recebido para a instância do Amazon EC2 com a maior largura de banda.

O Toolkit for Visual Studio fornece um assistente que simplifica a publicação de aplicativos por meio do Elastic Beanstalk. Esse assistente é descrito nas seções a seguir.

Para obter mais informações sobre o Elastic Beanstalk, acesseDocumentação do Elastic Beanstalk.

Tópicos

- Implante um aplicativo ASP.NET tradicional no Elastic Beanstalk
- Implantar uma aplicação ASP.NET Core no Elastic Beanstalk (Legacy)
- Como especificar oAWSCredenciais de segurança do aplicativo
- Como republicar seu aplicativo em um ambiente Elastic Beanstalk (legado)
- Implantações de aplicativo Elastic Beanstalk personalizadas
- Implantações personalizadas do Elastic Beanstalk do ASP.NET Core personalizadas
- Support de vários aplicativos para o .NET e o Elastic Beanstalk

Implante um aplicativo ASP.NET tradicional no Elastic Beanstalk

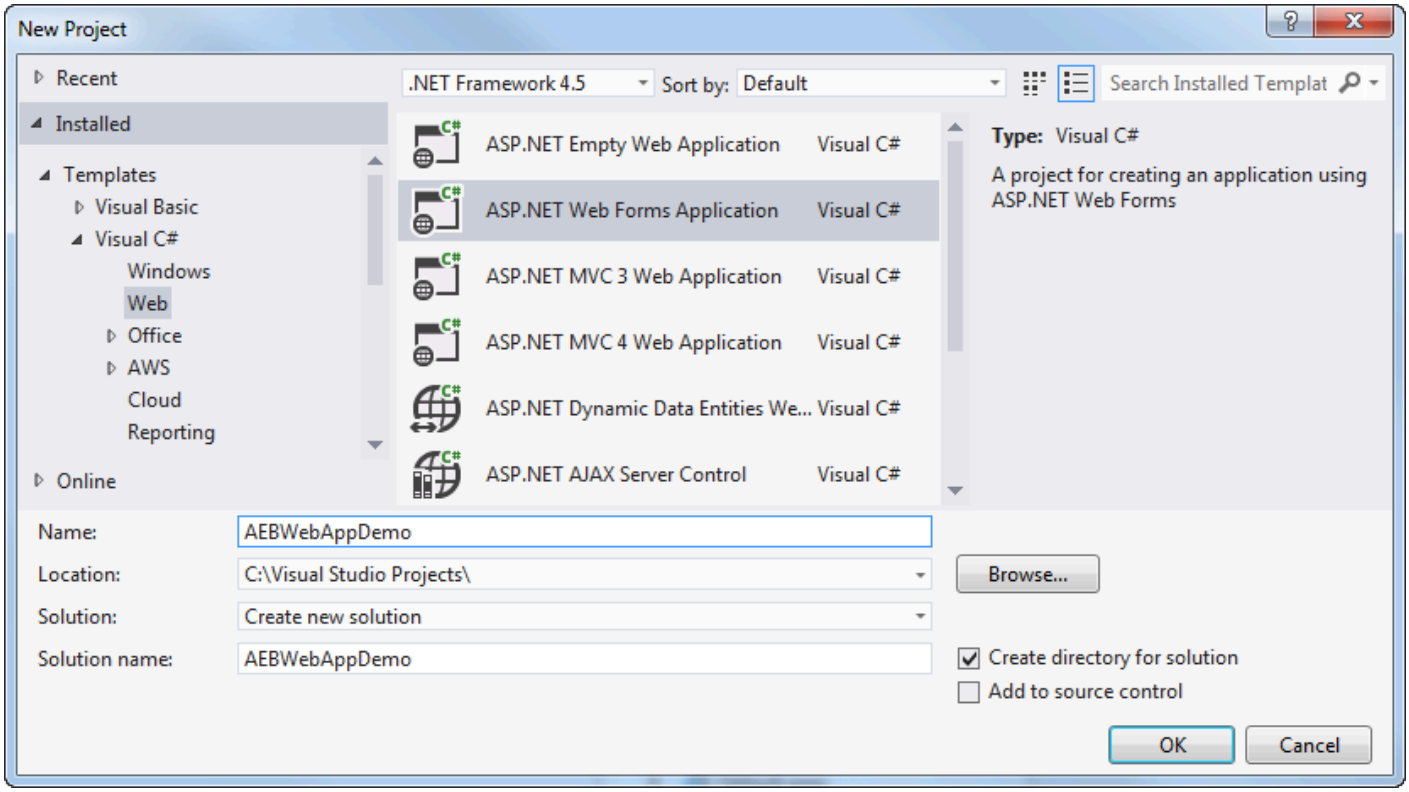
Esta seção descreve como usar o assistente Publish to Elastic Beanstalk, fornecido como parte do Toolkit for Visual Studio, para implantar um aplicativo por meio do Elastic Beanstalk. Para praticar, você pode usar uma instância de um projeto inicial de aplicativo web compilado no Visual Studio ou usar o próprio projeto.

> **Note**
>
> O assistente também dá suporte à implantação de aplicativos do ASP.NET Core. Para obter informações sobre o ASP.NET Core, consulte o guia da ferramenta de implantaçãoAWS .NET e a atualização Implantando noAWS sumário.

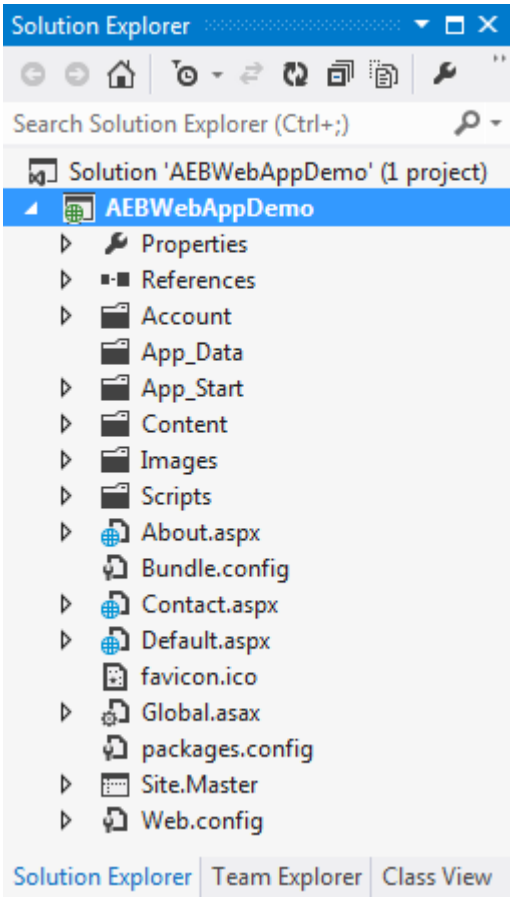
> **Note**
>
> Antes de usar o assistente Publish to Elastic Beanstalk (Publicar no Elastic Beanstalk), é necessário fazer download e instalar Web Deploy. O assistente depende do Web Deploy para implantar aplicativos web e sites aos servidores web do Internet Information Services (IIS).

Para criar um projeto inicial de aplicativo web de exemplo

1. No Visual Studio, no menu File (Arquivo), escolha New (Novo) e Project (Projeto).
2. No painel de navegação da caixa de diálogo Novo projeto, expanda Instalado, Modelos, Visual C# e escolha Web.
3. Na lista de modelos de projeto da web, escolha qualquer modelo que contenha as palavras `Web` e `Application` na descrição. Para este exemplo, escolha ASP.NET Web Forms Application (Aplicativo de formulários web do ASP.NET).

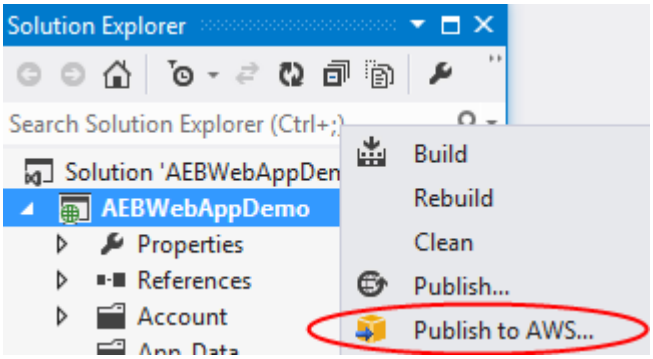


4. Na caixa Name (Nome), digite `AEBWebAppDemo`.
5. Na caixa Location (Local), digite o caminho para uma pasta de solução na máquina de desenvolvimento ou escolha Browse (Navegar) e navegue até e escolha uma pasta de solução e escolha Select Folder (Selecionar pasta).
6. Confirme se a caixa Criar diretório para solução está marcada. Na lista suspensa Solution (Solução), confirme se Create new solution (Criar nova solução) está selecionado e escolha OK. O Visual Studio criará uma solução e um projeto com base no modelo de projeto ASP.NET Web Forms Application. O Visual Studio acabará exibindo o Solution Explorer, onde a nova solução e o projeto são exibidos.

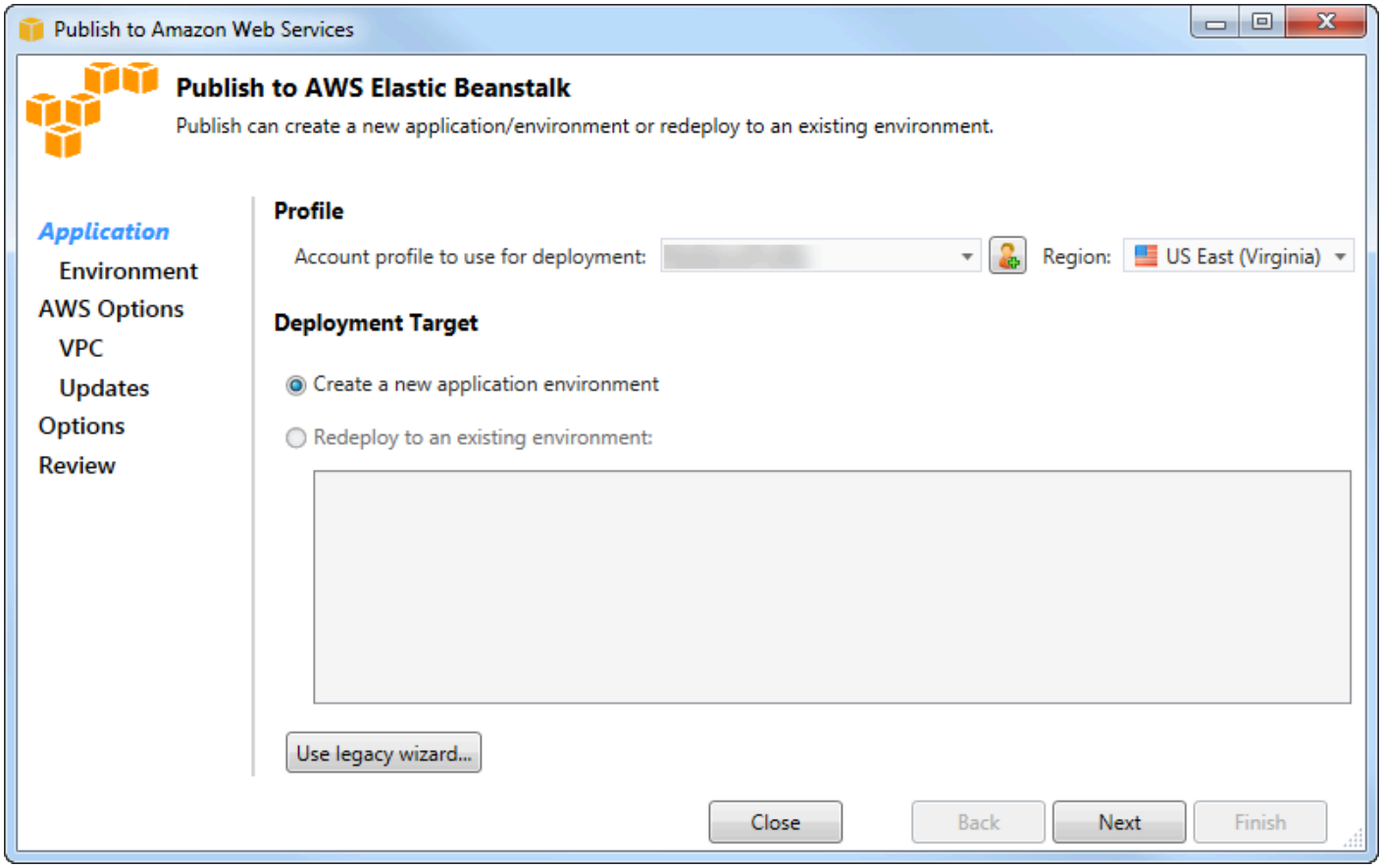


Para implantar um aplicativo usando o assistente Publish to Elastic Beanstalk

1. No Solution Explorer, abra o menu de contexto (clique com o botão direito do mouse) da pasta do projeto AEBWebAppDemo do projeto que você criou na seção anterior ou abra o menu de contexto da pasta do projeto do seu próprio aplicativo e escolha Publicar noAWS Elastic Beanstalk.



   O assistente Publish to Elastic Beanstalk (Publicar no Elastic Beanstalk) é exibido.



2. Em Perfil, na lista suspensa Perfil da conta a ser usado para implantação, escolha o perfil daAWS conta que você deseja usar para a implantação.

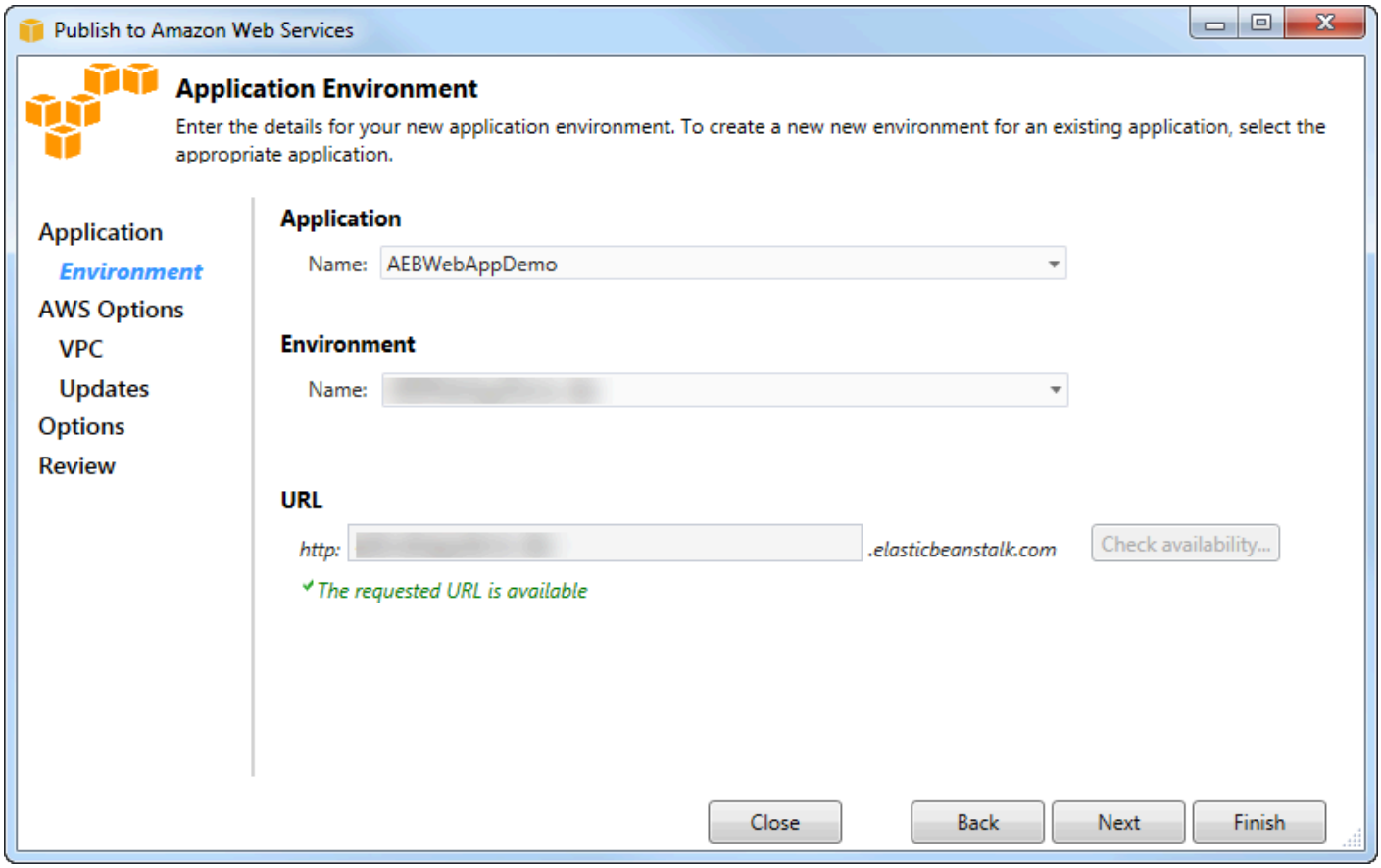
   Opcionalmente, se você tiver umaAWS conta que deseja usar, mas ainda não tiver criado um perfil deAWS conta para ela, poderá escolher o botão com o símbolo de mais (+) para adicionar um perfil deAWS conta.

3. Na lista suspensa Região, escolha a região na qual você deseja que o Elastic Beanstalk implante o aplicativo.

4. Em Deployment Target (Destino de implantação), você pode escolher Create a new application environment (Criar um novo ambiente de aplicativo) para realizar uma implantação inicial de um aplicativo ou Redeploy to an existing environment (Reimplantar em um ambiente existente) para reimplantar um aplicativo já implantado. (As implantações anteriores podem ter sido realizadas com o assistente ou com a obsoleta Ferramenta de Implantação Autônoma.) Se você escolher Redeploy to an existing environment (Reimplantar em um ambiente existente), poderá haver um atraso enquanto o assistente recupera informações de implantações anteriores em execução no momento.

> **Note**
>
> Se você escolher Redeploy to an existing environment (Reimplantar em um ambiente existente), escolha um ambiente na lista e Next (Próximo), e o assistente levará você diretamente até a página Application Options (Opções de aplicativo). Se você seguir essa rota, passe diretamente às instruções posteriormente nesta seção que descrevem como usar a página Application Options (Opções de aplicativo).

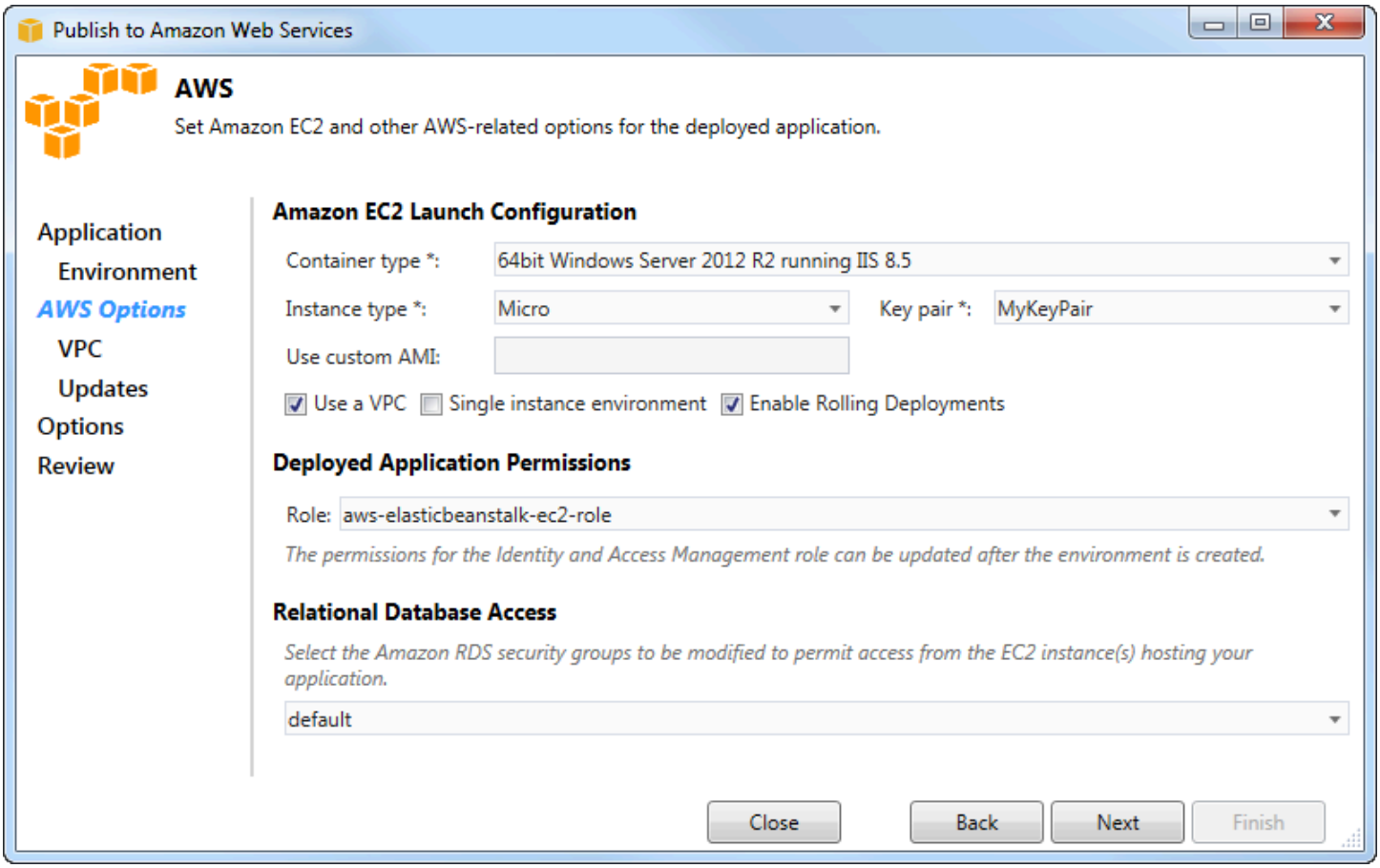
5. Escolha Next (Próximo).



6. Na página Application Environment (Ambiente de aplicativo), na área Application (Aplicativo), a lista suspensa Name (Nome) propõe um nome padrão para o aplicativo. Você pode alterar o nome padrão escolhendo um nome diferente na lista suspensa.
7. Na área Ambiente, na lista suspensa Nome, digite um nome para seu ambiente Elastic Beanstalk. Nesse contexto, o termo ambiente se refere à infraestrutura que o Elastic Beanstalk fornece para seu aplicativo. Um nome padrão já pode ter sido proposto nessa lista suspensa. Se um nome padrão ainda não tiver sido proposto, você poderá digitar um ou escolher um na lista suspensa,

se nomes adicionais estiverem disponíveis. O nome do ambiente não pode ter mais que 23 caracteres.

8. Na área URL, a caixa propõe um subdomínio padrão de `.elasticbeanstalk.com` que será o URL do aplicativo web. Você pode alterar o subdomínio padrão digitando um novo nome de subdomínio.
9. Escolha Check availability (Verificar disponibilidade) para verificar se o URL do aplicativo web ainda não está em uso.
10. Se o URL do aplicativo da web puder ser usado, escolha Next (Próximo).



1. Na página AWSOpções, na Configuração de inicialização do Amazon EC2, na lista suspensa Tipo de contêiner, escolha um tipo de imagem de máquina da Amazon (AMI) que será usado para seu aplicativo.
2. Na lista suspensa Tipo de instância, especifique um tipo de instância do Amazon EC2 a ser usada. Para este exemplo, recomendamos usar Micro. Isso minimizará o custo associado à

execução da instância. Para obter mais informações sobre preços do Amazon EC2, consulte Preço do EC2.

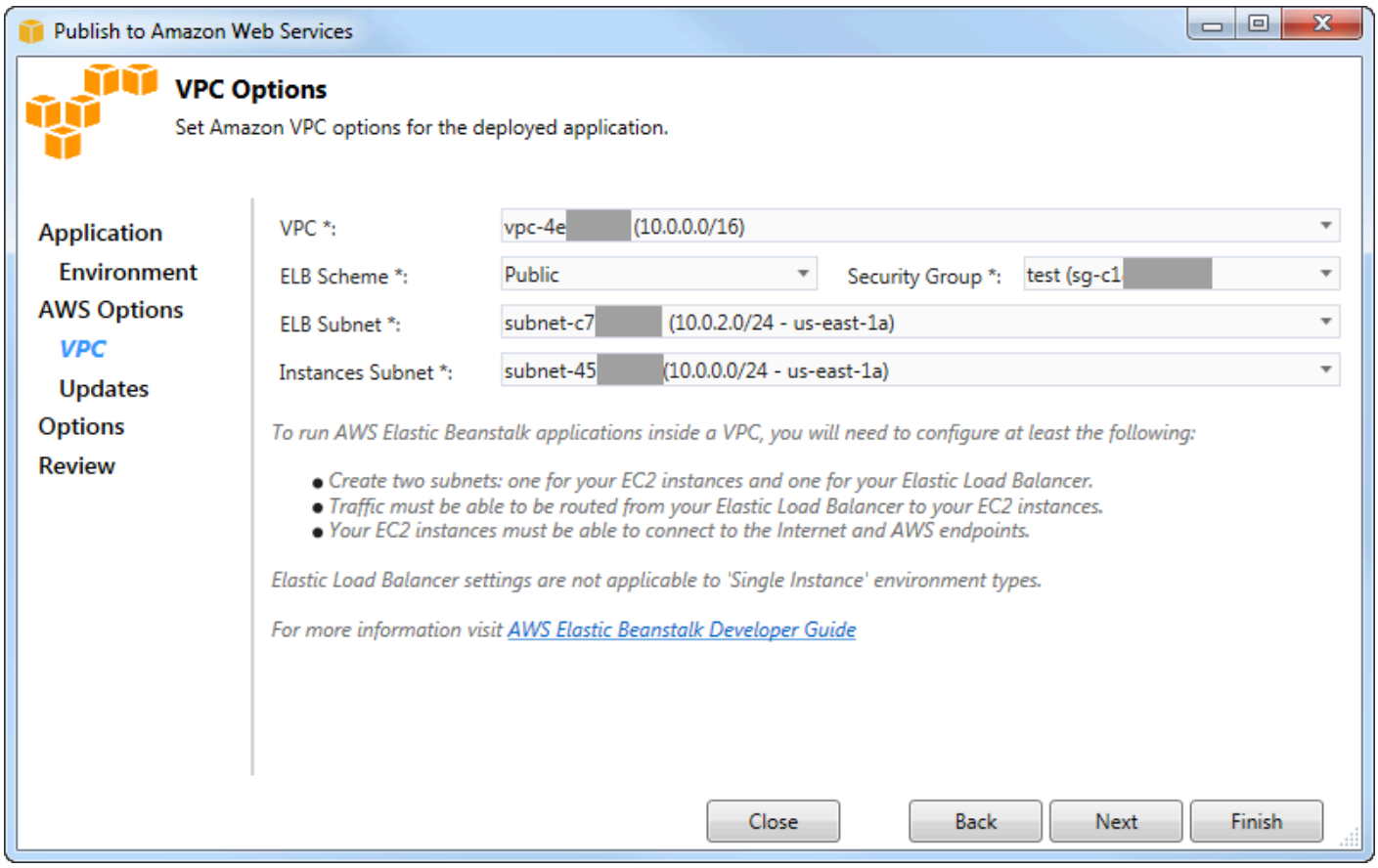
3. Na lista suspensa Par de chaves, escolha um key pair de instância do Amazon EC2 para usar para fazer login nas instâncias que serão usadas para seu aplicativo.
4. Como opção, na caixa Use custom AMI (Usar AMI personalizada), você pode especificar uma AMI personalizada que substituirá a AMI especificada na lista suspensa Container type (Tipo de contêiner). Para obter mais informações sobre como criar uma AMI personalizada, acesse Usando AMIs personalizadas no Guia do desenvolvedor doAWS Elastic Beanstalk e Crie uma AMI a partir de uma instância do Amazon EC2.
5. Se você quiser iniciar as instâncias em uma VPC, marque a caixa Use a VPC (Usar uma VPC).
6. Opcionalmente, se você quiser iniciar uma única instância do Amazon EC2 e depois implantar seu aplicativo nela, selecione a caixa Ambiente de instância única.

   Se você selecionar essa caixa, o Elastic Beanstalk ainda criará um grupo de Auto Scaling, mas não o configurará. Se quiser configurar o grupo Auto Scaling posteriormente, você pode usarAWS Management Console o.
7. Se você quiser controlar as condições nas quais o aplicativo é implantado nas instâncias, marque a caixa Enable Rolling Deployments (Habilitar a liberação de implantações). Você só poderá marcar essa caixa se não tiver marcado a caixa Single instance environment (Ambiente de única instância).
8. Se seu aplicativo usaAWS serviços como Amazon S3 e DynamoDB, a melhor maneira de fornecer credenciais é usar uma função do IAM. Na área Permissões de aplicativos implantados, você pode escolher uma função existente do IAM ou criar uma que o assistente usará para iniciar seu ambiente. Os aplicativos que usam oAWS SDK for .NET usarão automaticamente as credenciais fornecidas por essa função do IAM ao fazer uma solicitação a umAWS serviço.
9. Se seu aplicativo acessar um banco de dados do Amazon RDS, na lista suspensa na área Acesso ao banco de dados relacional, selecione as caixas ao lado de qualquer grupo de segurança do Amazon RDS que o assistente atualizará para que suas instâncias do Amazon EC2 possam acessar esse banco de dados.
10. Escolha Next (Próximo).
    - Se você tiver selecionado Use a VPC (Usar uma VPC), a página VPC Options (Opções da VPC) será exibida.
    - Se você tiver selecionado Enable Rolling Deployments (Habilitar a liberação de implantações), mas não Use a VPC (Usar uma VPC), a página Rolling Deployments (Liberação de

implantações) será exibida. Passe diretamente às instruções posteriormente nesta seção que descrevem como usar a página Rolling Deployments (Liberação de implantações).

- Se você não tiver selecionado Use a VPC (Usar uma VPC) ou Enable Rolling Deployments (Habilitar a liberação de implantações), a página Application Options (Opções de aplicativo) será exibida. Passe diretamente às instruções posteriormente nesta seção que descrevem como usar a página Application Options (Opções de aplicativo).

11. Se você tiver selecionado Use a VPC (Usar uma VPC), especifique as informações na página VPC Options (Opções de VPC) para iniciar o aplicativo em uma VPC.



A VPC já deve ter sido criada. Se você criou a VPC no Toolkit for Visual Studio, o Toolkit for Visual Studio preencherá essa página para você. Se você criou a VPC no AWSManagement Console, digite as informações sobre sua VPC nesta página.

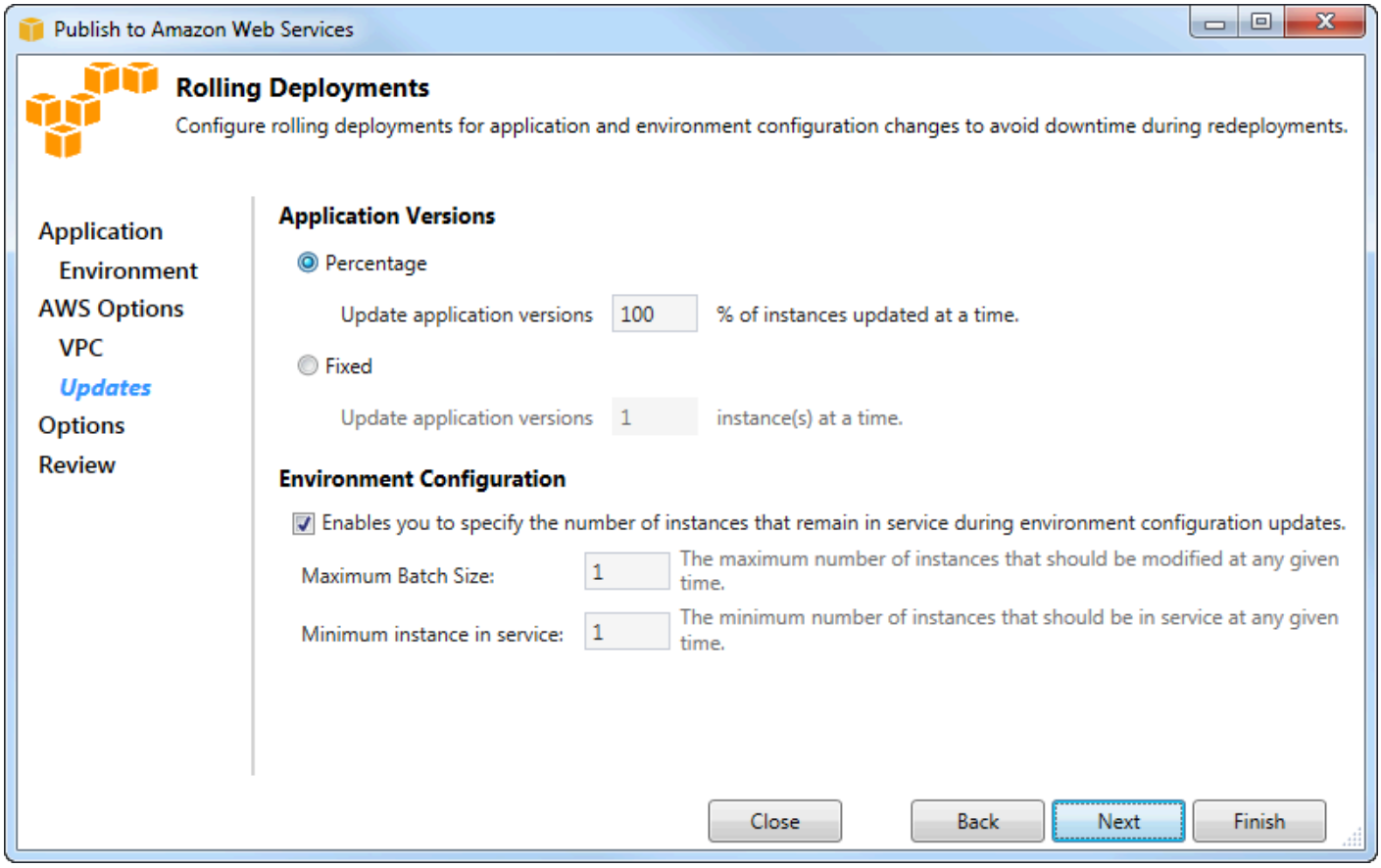
Considerações fundamentais para a implantação em uma VPC

- A VPC precisa de pelo menos uma pública e uma sub-rede privada.

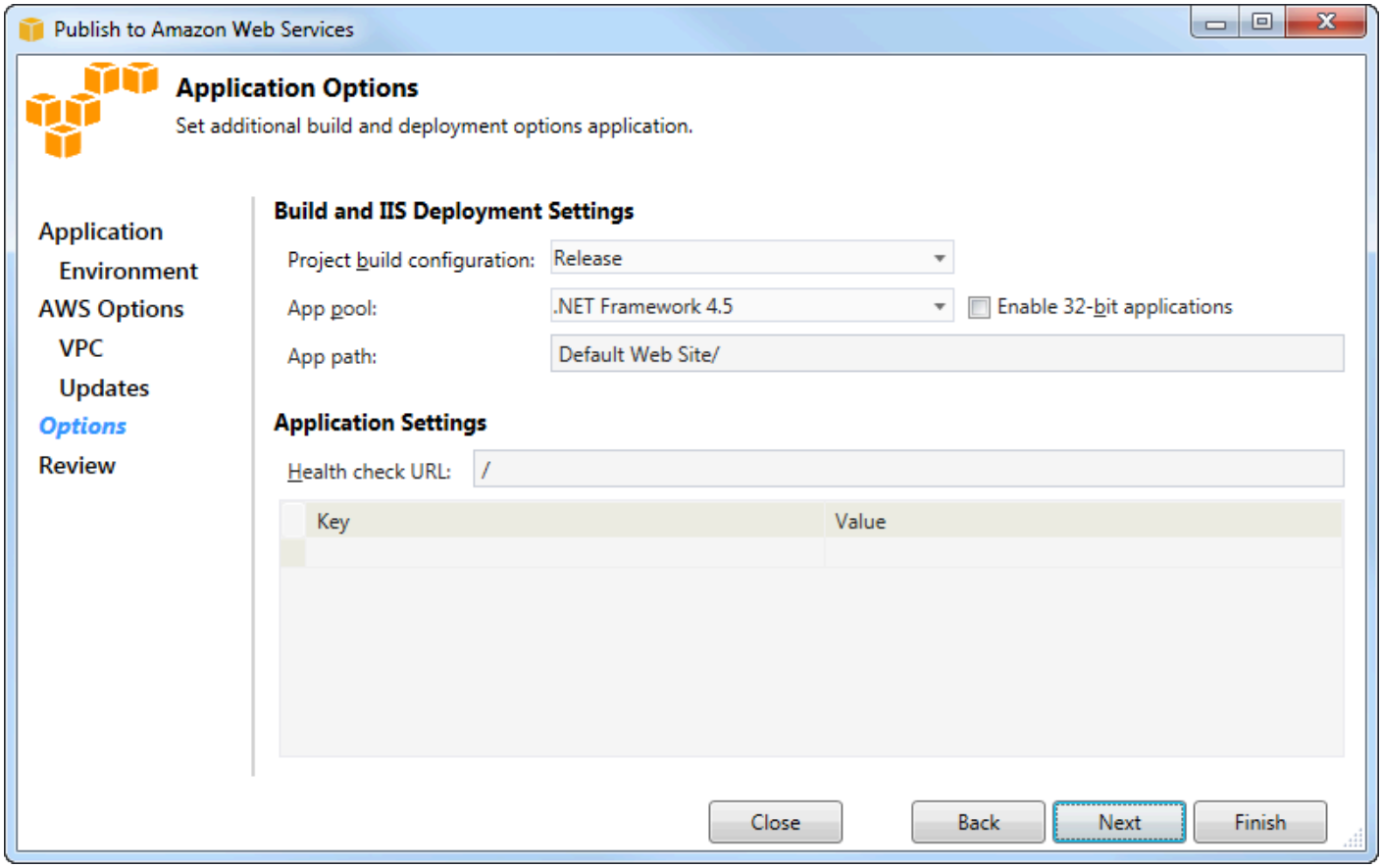
- Na lista suspensa ELB Subnet (Sub-rede do ELB), especifique a sub-rede pública. O Toolkit for Visual Studio implanta o balanceador de carga Elastic Load Balancing para seu aplicativo na sub-rede pública. A sub-rede pública é associada a uma tabela de roteamento com uma entrada apontando para um Internet Gateway. Você pode reconhecer um Internet Gateway porque ele possui um ID que começa com `igw-` (por exemplo, `igw-83cddaex`). As sub-redes públicas que você cria usando o Toolkit for Visual Studio têm valores de tag que as identificam como públicas.
- Na lista suspensa Instances Subnet (Sub-rede de instâncias), especifique a sub-rede privada. O Toolkit for Visual Studio implanta as instâncias do Amazon EC2 para seu aplicativo na sub-rede privada.
- As instâncias do Amazon EC2 do seu aplicativo se comunicam da sub-rede privada para a Internet por meio de uma instância do Amazon EC2 na sub-rede pública que executa a conversão de endereços de rede (NAT). Para permitir essa comunicação, você precisará de um grupo de segurança da VPC que permite o fluxo de tráfego da sub-rede para a instância NAT. Especifique esse grupo de segurança da VPC na lista suspensa Security Group (Grupo de segurança).

Para obter mais informações sobre como implantar um aplicativo Elastic Beanstalk em uma VPC, acesse o Guia do desenvolvedor doAWS Elastic Beanstalk.

1. Depois que você tiver preenchido todas as informações na página VPC Options (Opções da VPC), escolha Next (Próximo).
   - Se você tiver selecionado Enable Rolling Deployments (Habilitar a liberação de implantações), a página Rolling Deployments (Liberação de implantações) será exibida.
   - Se você não tiver selecionado Enable Rolling Deployments (Habilitar a liberação de implantações), a página Application Options (Opções de aplicativo) será exibida. Passe diretamente às instruções posteriormente nesta seção que descrevem como usar a página Application Options (Opções de aplicativo).
2. Se tiver selecionado Enable Rolling Deployments (Habilitar a liberação de implantações), você especifica informações na página Rolling Deployments (Liberação de implantações) para configurar como novas versões dos aplicativos são implantadas nas instâncias em um ambiente com balanceamento de carga. Por exemplo, se tiver quatro instâncias no ambiente e quiser alterar o tipo de instância, você poderá configurar o ambiente para alterar duas instâncias por vez. Isso ajuda a garantir que o aplicativo ainda esteja em execução enquanto as alterações estão sendo feitas.



3. Na área Application Versions (Versões de aplicativo), escolha uma opção para controlar implantações em uma porcentagem ou número de instâncias por vez. Especifique a porcentagem ou o número desejado.
4. Como opção, na área Environment Configuration (Configuração do ambiente), marque a caixa se você quiser especificar o número de instâncias que permanecem em serviço durante as implantações. Se você marcar essa caixa, especifique o número máximo de instâncias que devem ser modificadas por vez, o número mínimo de instâncias que devem permanecer em serviço por vez, ou ambos.
5. Escolha Next (Próximo).
6. Na página Application Options (Opções de aplicativo), você especifica informações sobre a compilação, o Internet Information Services (IIS) e as configurações do aplicativo.

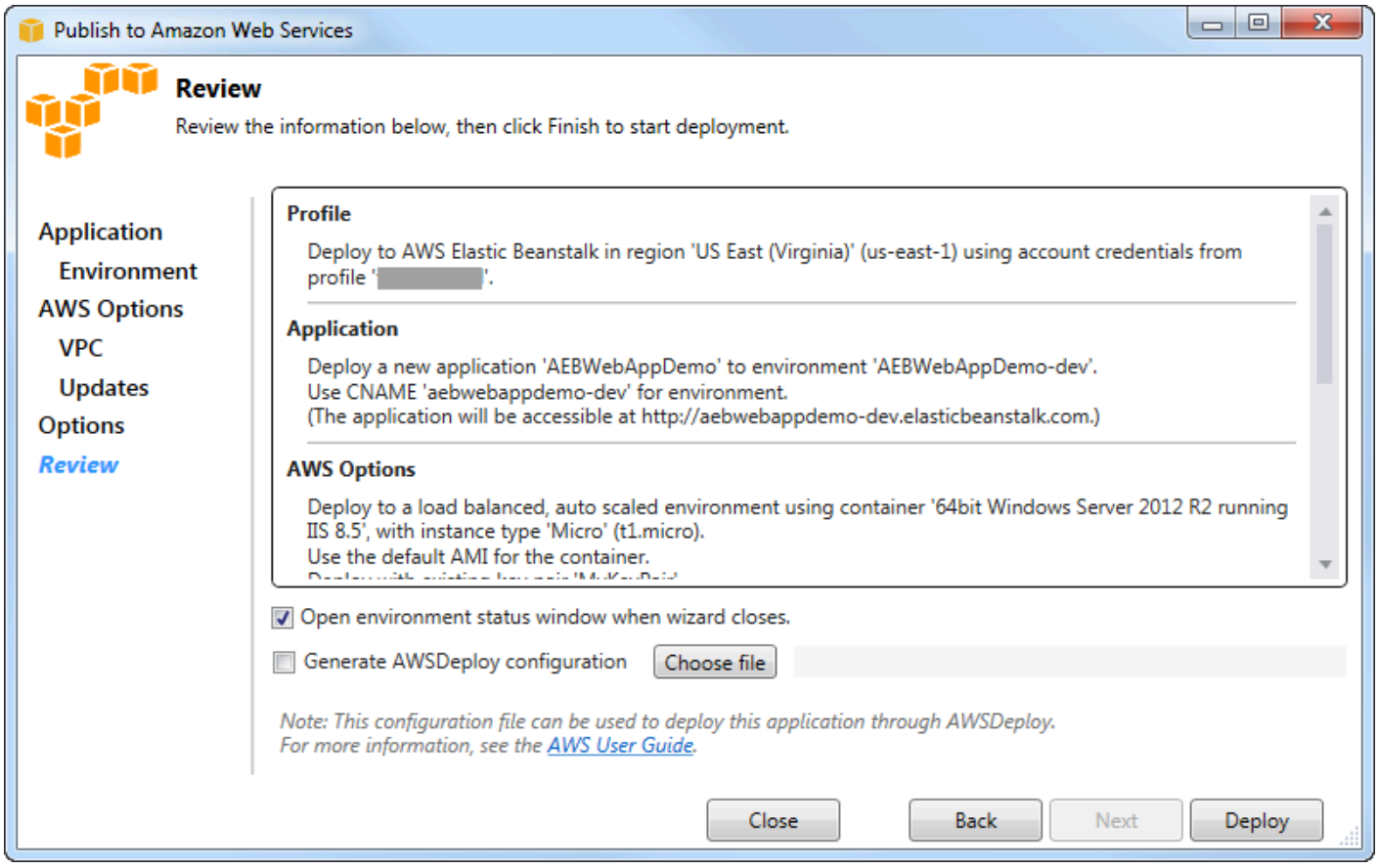


7. Na área Build and IIS Deployment Settings (Configurações de compilação e implantação IIS), na lista suspensa Project build configuration (Configuração de compilação do projeto), escolha a configuração da compilação de destino. Se o assistente conseguir encontrá-la, Release (Liberar) será exibida, e a configuração ativa é mostrada nessa caixa.
8. Na lista suspensa App pool (Grupo de aplicativos), escolha a versão do .NET Framework exigida pelo aplicativo. A versão do .NET Framework correta já deve ser exibida.
9. Se o aplicativo for 32 bits, marque a caixa Enable 32-bit applications (Habilitar aplicativos de 32 bits).
10. Na caixa App path (Caminho de aplicativo), especifique o caminho que o IIS usará para implantar o aplicativo. Por padrão, Default Web Site/ é especificado, o que normalmente se converte no caminho `c:\inetpub\wwwroot`. Se especificar um caminho diferente de Default Web Site/, o assistente colocará um redirecionamento no caminho Default Web Site/ apontando para o caminho especificado por você.
11. Na área Configurações do aplicativo, na caixa URL de verificação de Health, digite uma URL para que o Elastic Beanstalk verifique se seu aplicativo web ainda está responsivo. Este URL é relativo ao URL do servidor raiz. O URL do servidor raiz é especificado por padrão. Por exemplo, se o URL completo fosse `example.com/site-is-up.html`, você digitaria `/site-is-up.html`.

12 Na área de Key (Chave) e Value (Valor), você pode especificar os pares de chave e valor que deseja adicionar ao arquivo `Web.config` do aplicativo.

> **Note**
>
> Embora não seja recomendado, você pode usar a área de Chave e Valor para especificar asAWS credenciais sob as quais seu aplicativo deve ser executado. A abordagem preferida é especificar uma função do IAM na lista suspensa da função de Identity and Access Management na página AWSOpções. No entanto, se você precisar usarAWS credenciais em vez de uma função do IAM para executar seu aplicativo, na linha Chave, escolha AWSAccessKey. Na linha Value (Valor), digite a chave de acesso. Repita essas etapas para AWSSecretKey.

13 Escolha Next (Próximo).



14 Na página Review (Análise), revise as opções configuradas por você anteriormente e marque a caixa Open environment status window when wizard closes (Abrir a janela de status do ambiente ao fechar o assistente).

15 Se tudo estiver aparentemente correto, escolha Deploy (Implantar).

> **Note**
>
> Quando você implanta o aplicativo, a conta ativa incorrerá em cobranças pelosAWS recursos usados pelo aplicativo.

As informações sobre a implantação serão exibidas na barra de status do Visual Studio e na janela Output (Saída). Isso pode demorar muitos minutos. Quando a implementação estiver concluída, uma mensagem de confirmação será exibida na janela Output (Saída).

16. Para excluir a implantação, noAWS Explorer, expanda o nó do Elastic Beanstalk, abra o menu de contexto (botão direito do mouse) e selecione Excluir. O processo de exclusão pode demorar alguns minutos.

Implantar uma aplicação ASP.NET Core no Elastic Beanstalk (Legacy)

> **Important**
>
> Esta documentação se refere a serviços e recursos antigos. Para guias e conteúdos atualizados, consulte o guia da ferramenta de implantaçãoAWS do.NET e a atualização Implantando noAWS sumário.

AWS Elastic Beanstalké um serviço que simplifica o processo de provisionamento deAWS recursos para seu aplicativo. AWS Elastic Beanstalkfornece toda aAWS infraestrutura necessária para implantar seu aplicativo.

O Toolkit for Visual Studio oferece suporte à implantação de aplicativos ASP.NET CoreAWS usando o Elastic Beanstalk. O ASP.NET Core é a reformulação do ASP.NET com uma arquitetura modularizada que minimiza a sobrecarga de dependência e aprimora a execução do aplicativo na nuvem.

AWS Elastic Beanstalkfacilita a implantação de aplicativos em vários idiomas diferentes noAWS. O Elastic Beanstalk oferece suporte aos aplicativos tradicionais do ASP.NET e aos aplicativos do ASP.NET Core. Este tópico descreve como implantar os aplicativos do ASP.NET Core.

Usar o Deployment Wizard

A maneira mais fácil de Implantar Aplicações ASP.NET Core no Elastic Beanstalk é com o Toolkit for Visual Studio.

Se tiver usado o toolkit antes de implantar aplicativos do ASP. NET tradicionais, você verá que a experiência no ASP.NET Core é muito semelhante. Nas etapas abaixo, percorreremos a experiência de implantação.

Se nunca usou o toolkit, a primeira coisa que você precisará fazer após instalá-lo será inscrever-se com asAWS credenciais da com o toolkit. Consulte Como especificar as credenciaisAWS de segurança para seu aplicativo para a documentação do Visual Studio para obter detalhes sobre como fazer isso.

Para implantar um aplicativo web ASP.NET Core, clique com o botão direito do mouse no projeto no Solution Explorer e selecione Publicar emAWS...

Na primeira página do assistente Publish toAWS Elastic Beanstalk deployment, escolha criar um novo aplicativo Elastic Beanstalk. Uma aplicação do Elastic Beanstalk é uma coleção lógica de componentes do Elastic Beanstalk, incluindo ambientes, versões e configurações de ambiente. O assistente de implantação gera um aplicativo que, por sua vez, contém um conjunto de versões dos aplicativos e ambientes. Os ambientes contêm osAWS recursos reais que executam uma versão do aplicativo. Sempre que você implanta um aplicativo, uma nova versão do aplicativo é criada, e o assistente aponta o ambiente para essa versão. Você pode saber mais sobre esses conceitos em Componentes do Elastic Beanstalk.

Depois, defina nomes para o aplicativo e o primeiro ambiente. Cada ambiente tem um CNAME exclusivo associado que você pode usar para acessar o aplicativo quando a implantação é concluída.

A próxima página, AWSOpções, permite configurar o tipo deAWS recursos a serem usados. Para este exemplo, deixe os valores padrão, exceto para a seção Key pair (Par de chaves). Os pares de chaves permitem recuperar a senha de administrador do Windows, de maneira que você possa fazer login na máquina. Se você ainda não tiver criado um par de chaves, convém selecionar Create new key pair (Criar um novo par de chaves).

Permissões

A página Permissões é usada para atribuirAWS credenciais às instâncias do EC2 que executam seu aplicativo. Isso é importante se seu aplicativo usar oAWS SDK for .NET para acessar outrosAWS

serviços. Se não estiver usando nenhum outro serviço pelo aplicativo, você poderá deixar essa página no padrão.

Opções de aplicativo

Os detalhes na página Opções de aplicativo são diferentes dos especificados durante a implantação de aplicativos do ASP.NET tradicionais. Aqui você especifica a configuração da compilação e a estrutura usadas para empacotar o aplicativo, além de especificar o caminho do recurso do IIS para o aplicativo.

Depois de preencher a página Opções de aplicativo, clique em Next (Próximo) para examinar as configurações e clique em Deploy (Implantar) para iniciar o processo de implantação.

Verificar status do ambiente

Depois que o aplicativo é empacotado e carregadoAWS, você pode verificar o status do ambiente Elastic Beanstalk abrindo a visualização de status do ambiente noAWS Explorer no Visual Studio.

Os eventos são exibidos na barra de status à medida que o ambiente fica online. Quando tudo estiver pronto, o status do ambiente mudará para um estado íntegro. Você pode clicar no URL para visualizar o site. A partir daqui, você também pode extrair os registros do ambiente ou da área de trabalho remota para as instâncias do Amazon EC2 que fazem parte do seu ambiente Elastic Beanstalk.

A primeira implantação de qualquer aplicativo demorará um pouco mais do que as reimplantações subsequentes, pois cria novosAWS recursos. À medida que realiza a iteração no aplicativo durante o desenvolvimento, você poderá reimplantar rapidamente voltando no assistente ou selecionando a opção Republish (Republicar) quando clicar com o botão direito do mouse no projeto.

Republique pacotes de seu aplicativo usando as configurações da execução anterior por meio do assistente de implantação e carrega o pacote de aplicativos para o ambiente existente do Elastic Beanstalk.

Como especificar oAWSCredenciais de segurança do aplicativo

OAWSconta que você especificar naPublicar no Elastic Beanstalkassistente é oAWSconta que o assistente usará para implantação no Elastic Beanstalk.

Embora não seja recomendado, também pode ser necessário especificarAWScredenciais de conta que seu aplicativo usará para acessarAWSserviços depois de ter sido implantado. A abordagem

preferida é especificar uma função do IAM. NoPublicar no Elastic Beanstalkassistente, isso é feito por meio doIdentity and Access Management Rolena lista suspensaAWSOpções. No legadoPublicar na Amazon Web Servicesassistente, isso é feito por meio doIAM Rolena lista suspensaAWSOpções.

Se você precisar usarAWScredenciais de conta em vez de uma função do IAM, você pode especificar oAWSCredenciais da conta do para o aplicativo usando uma das seguintes formas:

- Faça referência a um perfil correspondente aoAWSCredenciais da na`appSettings`elemento do projeto`Web.config`file. (Para criar um perfil, consulte oConfigurar oAWSCredenciais.) O exemplo a seguir especifica credenciais cujo nome de perfil é `myProfile`.

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

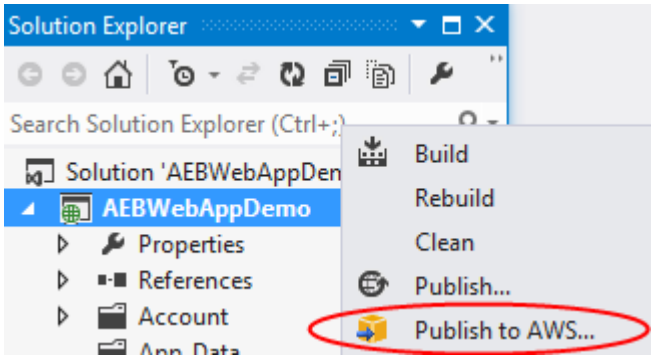
- Se você estiver usando oPublicar no Elastic Beanstalkfeiticeiro, naOpções de aplicativonaKey (Chave)linha doKey (Chave)eValorárea, escolhaAWSAccessKey. Na linha Value (Valor), digite a chave de acesso. Repita essas etapas para oAWSSecretKey.
- Se estiver usando o assistente Publish to Amazon Web Services (Publicar na Amazon Web Services) legado, na página Application Options (Opções de aplicativo), na área Application Credentials (Credenciais de aplicativo), escolha Use these credentials (Usar essas credenciais) e digite a chave de acesso e a chave de acesso secreta nas caixas Access Key (Chave de acesso) e Secret Key (Chave secreta).

Como republicar seu aplicativo em um ambiente Elastic Beanstalk (legado)

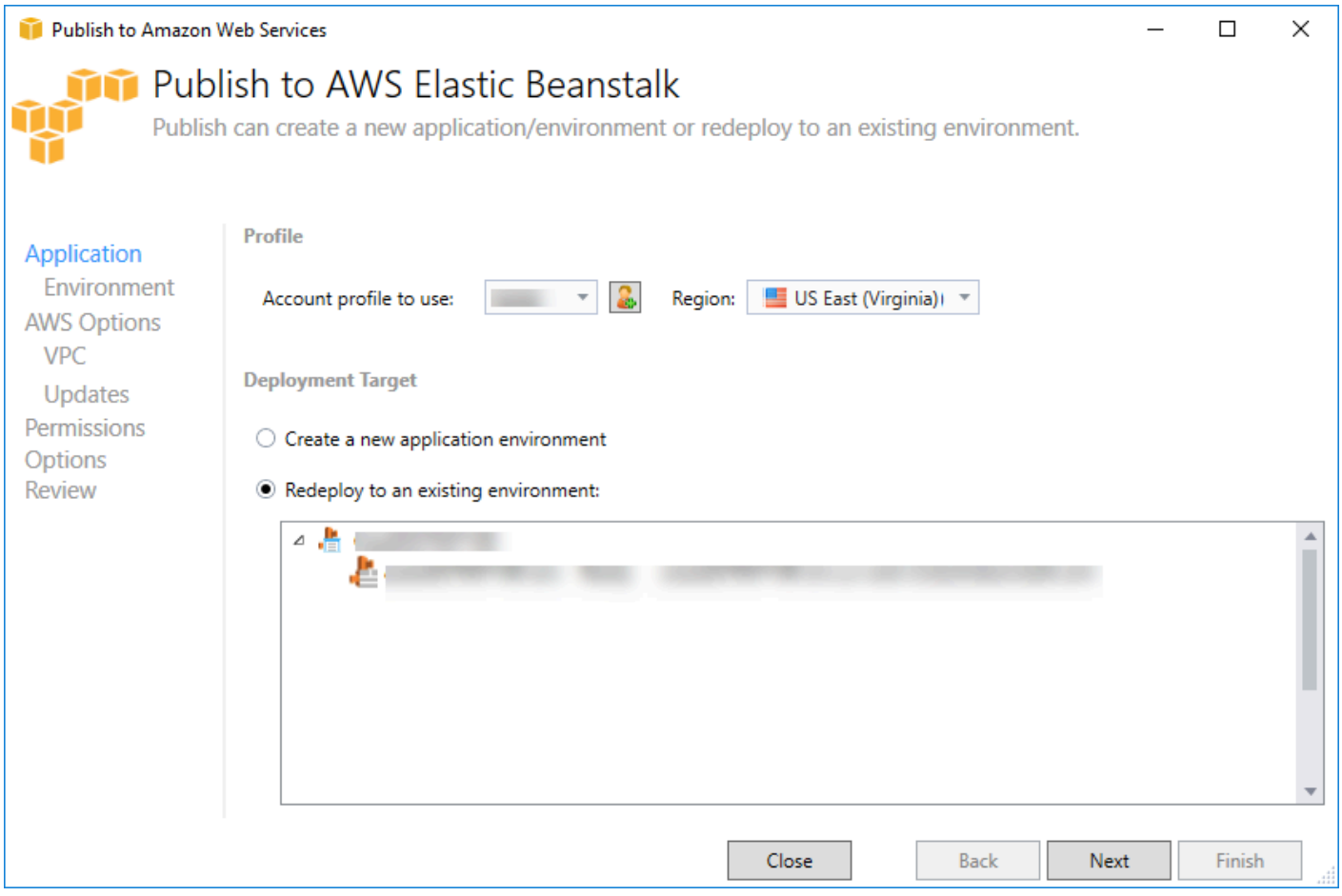
> **Important**
>
> Esta documentação se refere a serviços e recursos antigos. Para guias e conteúdos atualizados, consulte o guia da ferramenta de implantaçãoAWS .NET e a atualização Implantando noAWS sumário.

Você pode iterar em seu aplicativo fazendo alterações discretas e depois republicando uma nova versão em seu ambiente Elastic Beanstalk já lançado.

1. Em Solution Explorer, abra o menu de contexto (clique com o botão direito do mouse) da pastaWebAppDemo do projeto AEB do projeto publicado na seção anterior e escolha Publish to (Publicar no)AWS Elastic Beanstalk.

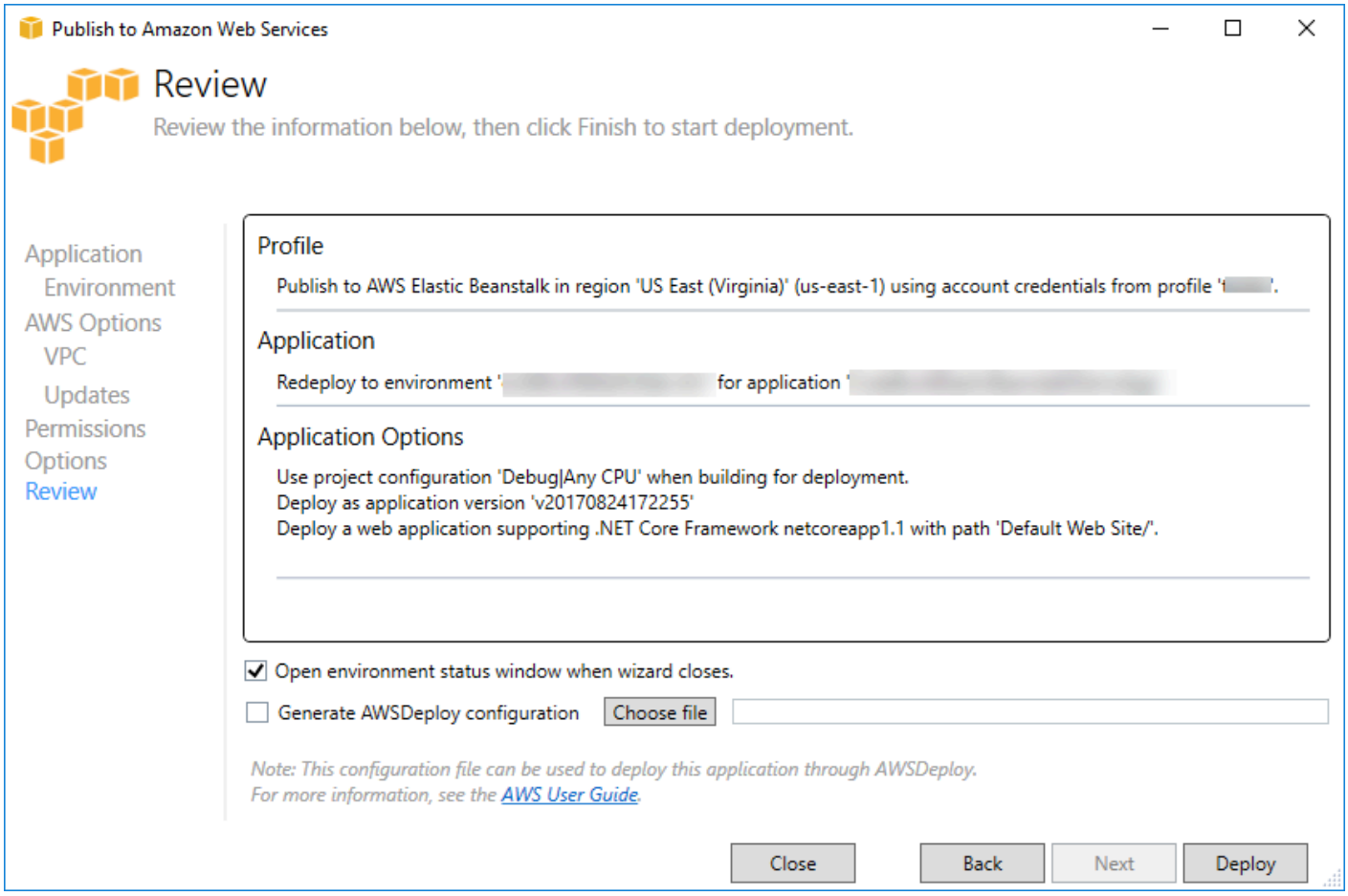


O assistente Publish to Elastic Beanstalk (Publicar no Elastic Beanstalk) é exibido.



2. Selecione Redeploy to an existing environment (Reimplantar em um ambiente existente) e escolha o ambiente onde você publicou anteriormente. Clique em Next.

   O assistente Review (Análise) é exibido.



3. Clique em Deploy (Implantar). O aplicativo será reimplantado no mesmo ambiente.

Você não poderá republicar se o aplicativo estiver no processo de execução ou encerramento.

Implantações de aplicativo Elastic Beanstalk personalizadas

Este tópico descreve como o manifesto de implantação do contêiner do Microsoft Windows do Elastic Beanstalk é compatível com as implantações de aplicativo personalizadas.

As implantações de aplicativo personalizadas são um recurso eficiente para usuários avançados que desejam utilizar a força do Elastic Beanstalk para criar e gerenciar asAWSrecursos, mas deseja controle total sobre como o aplicativo deles é implantado. Para uma implantação de aplicativo personalizada, você pode criar scripts do Windows PowerShell para as três ações diferentes realizadas pelo Elastic Beanstalk. A ação de instalação é usada quando uma implantação é iniciada, a reinicialização é usada quando a API `RestartAppServer` é chamada pelo toolkit ou pelo console da web e a desinstalação é invocada em qualquer implantação anterior sempre que ocorre uma nova implantação.

Por exemplo, convém ter um aplicativo ASP.NET que você deseja implantar, e a equipe de documentação cria um site estático que deseja incluir na implantação. Você pode fazer isso escrevendo o manifesto de implantação assim:

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

Os scripts listados para cada ação devem estar no pacote de aplicativos de implantação relativo ao arquivo manifesto. Neste exemplo, o pacote de aplicativos também conterá um arquivo documentation.zip que contém um site estático criado pela equipe de documentação.

O script `install.ps1` extrai o arquivo zip e configura o caminho do 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}
```

Como o aplicativo está execução no IIS, a ação de reinicialização invocará uma redefinição do IIS.

```
iisreset /timeout:1
```

Para desinstalar scripts, é importante limpar todas as configurações e arquivos usados durante o estágio de instalação. Dessa maneira, durante a fase de instalação para a nova versão, você pode evitar qualquer colisão com implantações anteriores. Neste exemplo, você precisa remover o aplicativo do IIS do site estático e remover os arquivos do site.

```
powershell.exe -Command {Remove-WebApplication -Name documentation}
Remove-Item -Recurse -Force 'c:\inetpub\wwwroot\documentation'
```

Com esses arquivos de script e o arquivo documentation.zip incluídos no pacote de aplicativos, a implantação cria o aplicativo ASP.NET e implanta o local da documentação.

Neste exemplo, escolhemos um exemplo simples que implanta um site estático simples, mas com a implantação de aplicativos personalizada, você pode implantar qualquer tipo de aplicativo e permitir o Elastic Beanstalk gerenciar aAWSrecursos para isso.

Implantações personalizadas do Elastic Beanstalk do ASP.NET Core personalizadas

Este tópico descreve como a implantação funciona e o que você pode fazer para personalizar implantações ao criar aplicativos do ASP.NET Core com o Elastic Beanstalk e o Toolkit for Visual Studio.

Depois de concluir o assistente de implantação no Toolkit for Visual Studio, o toolkit vai empacotar o aplicativo e enviá-lo para o Elastic Beanstalk. A primeira etapa na criação do pacote de aplicativos é usar a nova CLI dotnet a fim de preparar o aplicativo para publicação usando o comando publish. A estrutura e a configuração são passadas pelas configurações no assistente para o comando publish. Assim, se você tiver selecionado Release para `configuration` e netcoreapp1.0 para o `framework`, o toolkit executará o seguinte comando:

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

Quando o comando publish é concluído, o toolkit grava o novo manifesto de implantação na pasta de publicação. O manifesto de implantação é um arquivo JSON chamadoaws-windows-deployment-manifest.json, que o contêiner do Windows do Elastic Beanstalk (versão 1.2 ou posterior) do lê para determinar como implantar o aplicativo. Por exemplo, para um aplicativo do ASP.NET Core que você queira implantar na raiz do IIS, o toolkit gera um arquivo manifesto semelhante a este:

```
{
  "manifestVersion": 1,
  "deployments": {

    "aspNetCoreWeb": [
      {
        "name": "app",
        "parameters": {
          "appBundle": ".",
          "iisPath": "/",
          "iisWebSite": "Default Web Site"
        }
      }
    ]
  }
}
```

A propriedade `appBundle` indica onde os bits do aplicativo estão em relação ao arquivo manifesto. Essa propriedade pode apontar para um diretório ou um arquivo ZIP. As propriedades `iisPath` e `iisWebSite` indicam onde hospedar o aplicativo no IIS.

Personalizar o manifesto

O toolkit só gravará o arquivo manifesto se um ainda não existir na pasta de publicação. Se o arquivo não existir, o toolkit atualizará as propriedades `appBundle`, `iisPath` e `iisWebSite` no primeiro aplicativo listado na seção `aspNetCoreWeb` do manifesto. Isso permite adicionar o aws-windows-deployment-manifest.json ao projeto e personalizar o manifesto. Para fazer isso para um aplicativo web do ASP.NET Core no Visual Studio, adicione um novo arquivo JSON à raiz do projeto e o nomeie como aws-windows-deployment-manifest.json.

O manifesto deve ser chamado de aws-windows-deployment-manifest.json e deve estar na raiz do projeto. O contêiner do Elastic Beanstalk procura o manifesto na raiz e, se o encontrar, ele invocará

as ferramentas de implantação. Se o arquivo não existir, o contêiner do Elastic Beanstalk recorrerá às ferramentas de implantação anteriores, o que pressupõe que o arquivo seja ummsdeployArquivo.

Para garantir que o comando `publish` da CLI do dotnet inclua o manifesto, atualize o arquivo `project.json` para incluir o arquivo manifesto na seção include em `include` em `publishOptions`.

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

Agora que já declarou o manifesto de maneira que ele esteja incluído no pacote de aplicativos, você pode configurar como deseja implantar o aplicativo. Você pode personalizar a implantação além da compatibilidade do assistente de implantação.AWSA AWS definiu um esquema JSON para oArquivo aws-windows-deployment-manifest.jsone, ao instalar o Toolkit for Visual Studio, a configuração registrou o URL do esquema.

Ao abrir `windows-deployment-manifest.json`, você verá o URL do esquema selecionado na caixa suspensa Schema. Você pode navegar até o URL para obter uma descrição completa do que pode ser definido no manifesto. Com o esquema selecionado, o Visual Studio fornecerá o IntelliSense enquanto você estiver editando o manifesto.

Uma personalização que você pode fazer é configurar o grupo de aplicativos do IIS no qual o aplicativo será executado. O exemplo a seguir mostra como você pode definir um grupo de aplicativos do IIS ("customPool") que recicle o processo a cada 60 minutos e o atribui ao aplicativo usando `"appPool": "customPool"`.

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

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

Além disso, o manifesto pode declarar scripts do Windows PowerShell a serem executados antes e depois das ações de instalação, reinicialização e desinstalação. Por exemplo, o manifesto a seguir executa o script do Windows PowerShell `PostInstallSetup.ps1` para fazer mais trabalho de configuração após a implantação do aplicativo ASP.NET Core no IIS. Ao adicionar scripts assim, certifique-se de que os scripts sejam adicionados à seção include em publishOptions no arquivo `project.json`, da mesma maneira como você fez com o arquivo `aws-windows-deployment-manifest.json`. Se você não fizer isso, os scripts não serão incluídos como parte do comando publish da CLI do dotnet.

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

```
}
```

E .ebextensions?

O Elastic Beanstalk.ebextensionsOs arquivos de configuração são compatíveis como todos os outros contêineres do Elastic Beanstalk. Para incluir ebextensions em um aplicativo do ASP.NET Core, adicione o diretório `.ebextensions` à seção `include` em `publish0ptions` no arquivo `project.json`. Para obter mais informações sobre .ebextensions, confira o Guia do desenvolvedor do Elastic Beanstalk.

Support de vários aplicativos para o .NET e o Elastic Beanstalk

Usando o manifesto de implantação, você tem a capacidade de implantar vários aplicativos no mesmo ambiente do Elastic Beanstalk.

O manifesto de implantação oferece suporte a aplicativos web ASP.NET Core, bem como a arquivos msdeploy de aplicativos ASP.NET tradicionais. Imagine um cenário onde você tenha escrito um novo aplicativo incrível usando o ASP.NET Core para o front-end e um projeto de API web para uma API de extensões. Você também tem um aplicativo admin que escreveu usando o ASP.NET tradicional.

O assistente de implantação do toolkit se concentra na implantação de um único projeto. Para aproveitar a implantação de vários aplicativos, você precisa construir o pacote de aplicativos manualmente. Para começar, escreva o manifesto. Para este exemplo, você escreverá o manifesto na raiz da solução.

A seção de implantação no manifesto tem dois filhos: uma matriz de aplicativos web do ASP.NET Core a ser implantada e uma matriz de arquivos msdeploy a ser implantada. Para cada aplicativo, você define o caminho do IIS e o local dos bits do aplicativo em relação ao manifesto.

```
{
  "manifestVersion": 1,
  "deployments": {

    "aspNetCoreWeb": [
      {
        "name": "frontend",
        "parameters": {
          "appBundle": "./frontend",
          "iisPath": "/frontend"
        }
```

```
      },
      {
        "name": "ext-api",
        "parameters": {
          "appBundle": "./ext-api",
          "iisPath": "/ext-api"
        }
      }
    ],
    "msDeploy": [
      {
        "name": "admin",
        "parameters": {
          "appBundle": "AmazingAdmin.zip",
          "iisPath": "/admin"
        }
      }
    ]
  }
}
```

Com o manifesto escrito, você usará o Windows PowerShell para criar o pacote de aplicativos e atualizar um ambiente do Elastic Beanstalk existente para executá-lo. O script é escrito pressupondo-se que será executado na pasta que contém a solução do Visual Studio.

A primeira coisa que você precisa fazer no script é configurar uma pasta de workspace na qual criar o pacote de aplicativos.

```
$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
}
```

Assim que você tiver criado a pasta, será o momento de preparar o front-end. Assim como acontece com o assistente de implantação, use a CLI do dotnet para publicar o aplicativo.

```
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
```

A subpasta "frontend" foi usada para a pasta de saída, de acordo com a pasta definida por você no manifesto. Agora você precisa fazer a mesma coisa para o projeto da 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
```

O site admin é um aplicativo do ASP.NET tradicional, de maneira que você não pode usar a CLI do dotnet. Para o aplicativo admin, você deve usar msbuild, passando o pacote de destino da compilação para criar o arquivo msdeploy. Por padrão, o destino do pacote cria o arquivo msdeploy na pasta `obj\Release\Package`, logo, você precisará copiar o arquivo para o workspace de publicação.

```
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 informar ao ambiente do Elastic Beanstalk o que fazer com todos esses aplicativos, copie o manifesto da solução para o workspace de publicação e compacte a pasta.

```
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)
```

Agora que tem o pacote de aplicativos, você pode ir até o console web e fazer upload do arquivo para um ambiente do Elastic Beanstalk. Você também pode continuar a usar oAWSCmdlets do PowerShell para atualizar o ambiente do Elastic Beanstalk com o pacote de aplicativos. Verifique se você definiu o perfil e a região atuais segundo o perfil e a região que contêm o ambiente do Elastic Beanstalk usando`Set-AWSCredentials`e`Set-DefaultAWSRegion`cmdlets do .

```
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
```

Agora verifique o status da atualização usando página de status do ambiente do Elastic Beanstalk no toolkit ou no console web. Depois de terminar, você poderá navegar até cada um dos aplicativos que implantou no caminho do IIS definido no manifesto da implantação.

Implantar no Amazon EC2 Container Service

> **Important**
>
> O NovoPublish to (Publicar no &CW;)AWSé projetado para simplificar a forma como você publica aplicativos .NET paraAWS. Você pode ser perguntado se deseja mudar para essa experiência de publicação depois de escolherPublicar contêiner noAWS. Para obter mais informações, consulte Trabalhar com o Publicar noAWSno Visual Studio.

O Amazon Elastic Container Service é um serviço de gerenciamento de contêiner de alta performance e altamente escalável que oferece suporte aos contêineres do Docker e permite que você execute facilmente seus aplicativos em um cluster gerenciado de instâncias do Amazon EC2.

Para implantar aplicações no Amazon Elastic Container Service, os componentes das aplicações devem ser desenvolvidos para execução em um contêiner do Docker. Um contêiner do Docker é uma unidade padronizada de desenvolvimento de software, contendo tudo que seu aplicativo de software precisar para executar: código, tempo de execução, ferramentas de sistema, bibliotecas de sistema, etc.

O Toolkit for Visual Studio fornece um assistente que simplifica a publicação de aplicativos por meio do Amazon ECS. Esse assistente é descrito nas seções a seguir.

Para obter mais informações sobre o Amazon ECS, acesseDocumentação Elastic Container Service. Ela inclui uma visão geral dos conceitos básicos do Docker e da criação de um cluster.

Tópicos

Especifique oAWSCredenciais para seu aplicativo ASP.NET Core 2

Há dois tipos de credenciais em uso quando você implanta seu aplicativo em um contêiner do Docker: as credenciais de implantação e as credenciais de instância.

As credenciais de implantação são usadas pelo Publicar contêiner noAWSassistente para criar o ambiente no Amazon ECS. Isso inclui itens como tarefas, serviços, funções do IAM, um repositório de contêineres do Docker e, se você optar, um load balancer.

As credenciais de instância são usadas pela instância (incluindo o aplicativo) para acessar diferentes serviços da AWS. Por exemplo, se um aplicativo ASP.NET Core 2.0 lê e grava em objetos do Amazon S3, ele precisará de permissões apropriadas. Você pode fornecer credenciais diferentes usando métodos diferentes de acordo com o ambiente. Por exemplo, seu aplicativo ASP.NET Core 2 pode ter como objetivo os ambientes de desenvolvimento e produção. Você poderia usar uma instância local e as credenciais do Docker para o desenvolvimento e uma função definida na produção.

Especificar credenciais de implantação

OAWSconta especificada naPublicar contêiner noAWSassistente é oAWSconta que o assistente usará para implantação no Amazon ECS. O perfil da conta deve ter permissões para o Amazon Elastic Compute Cloud, o Amazon Elastic Container Service eAWS Identity and Access Management.

Se você observar a ausência de algumas opções na lista suspensa, pode ser devido à ausência de permissões. Por exemplo, se você tiver criado um cluster para seu aplicativo mas não o vê noPublicar contêiner noAWSpágina Cluster do assistente. Se isso acontecer, adicione as permissões ausentes e tente executar o assistente novamente.

Especificar credenciais de instância para o desenvolvimento

Para ambientes que não sejam de produção, você pode configurar suas credenciais no arquivo appsettings.<environment>.json. Por exemplo, para configurar suas credenciais no arquivo appsettings.Development.json no Visual Studio 2017:

1. Adicione o pacote AWSSDK.Extensions.NETCore.Setup NuGet ao seu projeto.
2. AdicionarAWSConfigurações para appsettings.Development.json. A configuração abaixo define `Profile` e `Region`.

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

Especificar credenciais de instância para a produção

Para instâncias de produção, recomendamos que você use uma função do IAM para controlar o que o seu aplicativo (e o serviço) pode acessar. Por exemplo, para configurar uma função do IAM usando o Amazon ECS como o serviço principal com permissões para o Amazon Simple Storage Service e o Amazon DynamoDB doAWS Management Console:

1. Faça login no AWS Management Console e abra o console do IAM em https://console.aws.amazon.com/iam/.
2. No painel de navegação do console do IAM, escolha Roles (Funções) e, em seguida, Create role (Criar função).
3. Selecione oAWSServiçoTipo de função e escolhaEC2 Container Service.
4. Escolha o caso de uso EC2 Container Service Task (Tarefa do EC2 Container Service). Casos de uso são definidos pelo serviço para incluir a política de confiança exigida pelo serviço. Depois, selecione Next (Próximo): Permissions
5. Escolha as políticas de permissões AmazonS3FullAccess e AmazonDynamoDBFullAccess. Marque a caixa ao lado de cada política e escolhaPróximo: Review (Revisar),
6. Em Role name (Nome da função), digite um nome de função ou sufixo de nome para a função que ajude você a identificar a finalidade dessa função. Os nomes de função devem ser exclusivos em

sua conta da AWS. Eles não são diferenciados por letras maiúsculas e minúsculas. Por exemplo, não é possível criar funções chamadas `PRODROLE` e `prodrole`. Como várias entidades podem fazer referência à função, não é possível editar o nome da função depois que ela é criada.

7. (Opcional) Em Descrição da função, digite uma descrição para a nova função.
8. Revise a função e escolha Create role.

Você pode usar essa função como oFunção de tarefanoDefinição de tarefas do ECSPágina doPublicar contêiner noAWSassistente.

Para obter mais informações, consulte Uso de funções baseadas em serviços.

Implantação de um aplicativo ASP.NET Core 2.0 no Amazon ECS (Fargate) (Legacy)

> **Important**
>
> Esta documentação se refere a serviços e recursos antigos. Para guias e conteúdos atualizados, consulte o guia da ferramenta de implantaçãoAWS .NET e a atualização Implantando noAWS sumário.

Esta seção descreve como usar oAWS assistente Publish Container to, fornecido como parte do Toolkit for Visual Studio, para implantar um aplicativo ASP.NET Core 2.0 em contêiner voltado para Linux por meio do Amazon ECS usando o tipo de inicialização Fargate. Como um aplicativo web é destinado a funcionar continuamente, ele será implantado como um serviço.

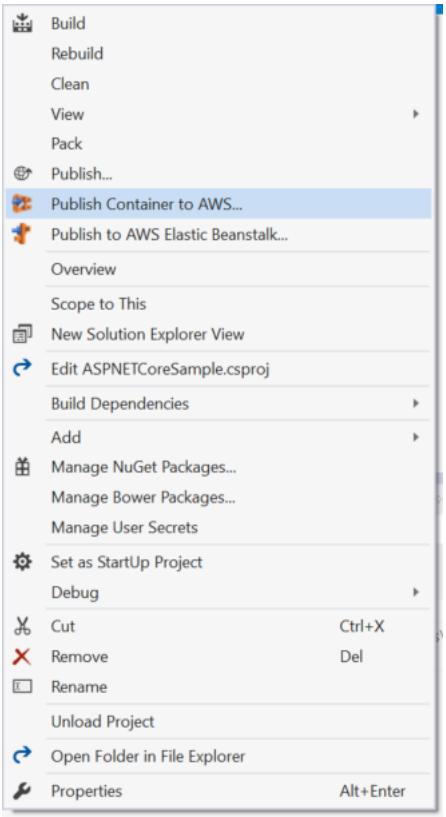
Antes de publicar o contêiner

Antes de usar oAWS assistente Publish Container to para implantar seu aplicativo ASP.NET Core 2.0:

- Especifique suasAWS credenciais e faça a configuração com o Amazon ECS.
- Instale o Docker. Existem algumas opções de instalação diferentes, incluindo o Docker para Windows.
- No Visual Studio, crie (ou abra) um projeto para um aplicativo em contêiner do ASP.NET Core 2.0 voltado para Linux.

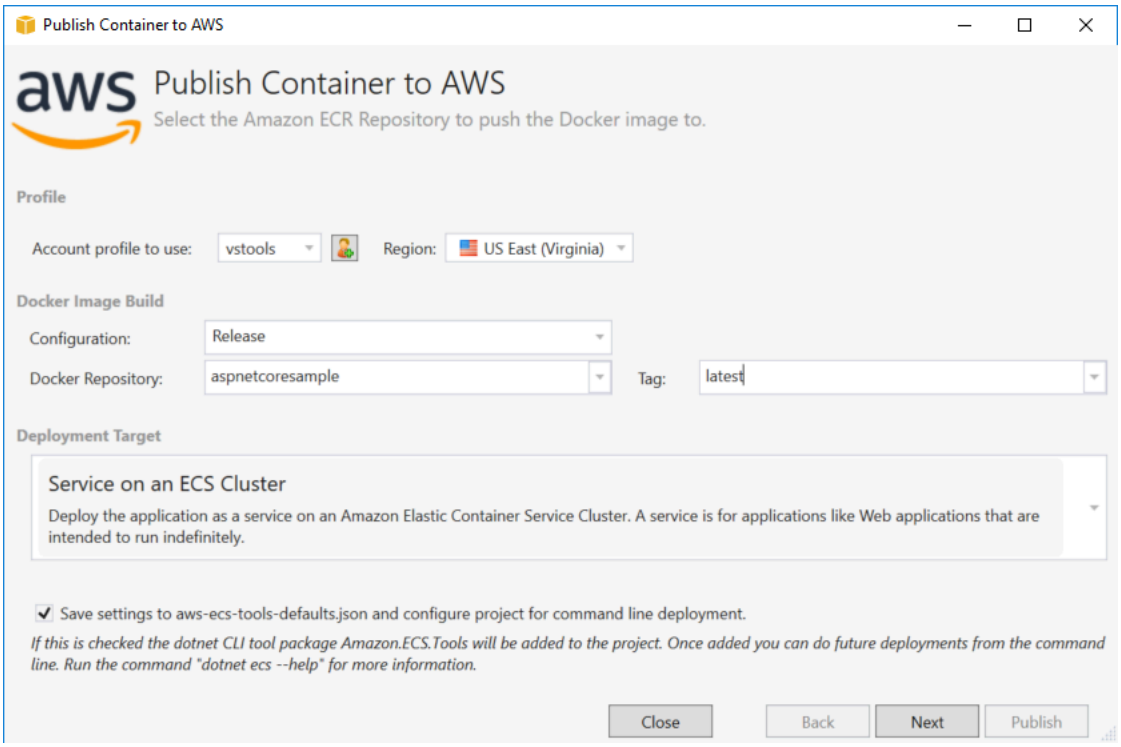
Acessando oAWS assistente Publish Container to

Para implantar um aplicativo em contêiner do ASP.NET Core 2.0 voltado para Linux, clique com o botão direito do mouse no projeto no Solution Explorer e selecione Publicar contêiner emAWS.



Você também pode selecionar Publicar contêiner paraAWS no menu Construção do Visual Studio.

Publicar contêiner noAWS assistente



Perfil de conta a usar — selecione o perfil de conta a ser usado.

Região — escolha a região de implantação. O perfil e a região são usados para configurar os recursos do ambiente de implantação e para selecionar o registro padrão do Docker.

Configuração — selecione a configuração da compilação para a imagem do Docker.

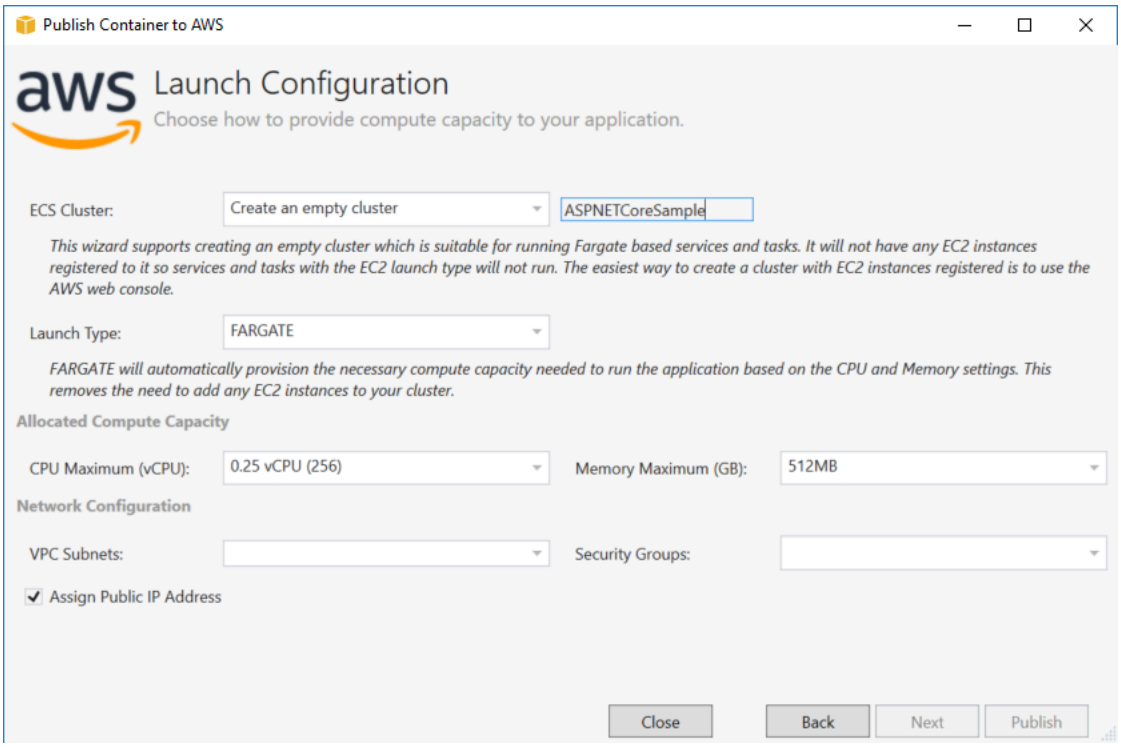
Repositório do Docker — escolha um repositório existente do Docker ou digite o nome de um novo repositório e ele será criado. Este é o repositório para onde o contêiner de compilação é enviado.

Tag — selecione uma tag existente ou digite o nome de uma nova tag. As tags podem rastrear detalhes importantes, como versão, opções ou outros elementos exclusivos da configuração de contêineres do Docker.

Destino da implantação — selecione Service on an ECS Cluster (Serviço em um cluster ECS). Use esta opção de implantação para os aplicativos de execução prolongada (como um aplicativo web ASP.NET).

Salve as configurações**`aws-docker-tools-defaults.json`** e configure o projeto para implantação na linha de comando - Marque essa opção se quiser a flexibilidade de implantar a partir da linha de comando. Use `dotnet ecs deploy` a partir do diretório do projeto para implantar e para `dotnet ecs publish` o contêiner.

Página de configuração da execução



Cluster do ECS — selecione o cluster que executará a imagem do Docker. Se você optar por criar um cluster vazio, forneça um nome para o novo cluster.

Tipo de execução — escolha FARGATE.

Máximo de CPU (vCPU) — escolha a quantidade máxima de capacidade computacional necessária para o seu aplicativo. Para ver os intervalos permitidos de valores para CPU e memória, consulte tamanho da tarefa.

Máximo de memória (GB) — selecione a quantidade máxima de memória disponível para o seu aplicativo.

Sub-redes da VPC — escolha uma ou mais sub-redes em uma única VPC. Se você escolher mais de uma sub-rede, suas tarefas serão distribuídas entre elas. Isso pode melhorar a disponibilidade. Para obter mais informações, consulte VPC e sub-redes padrão.

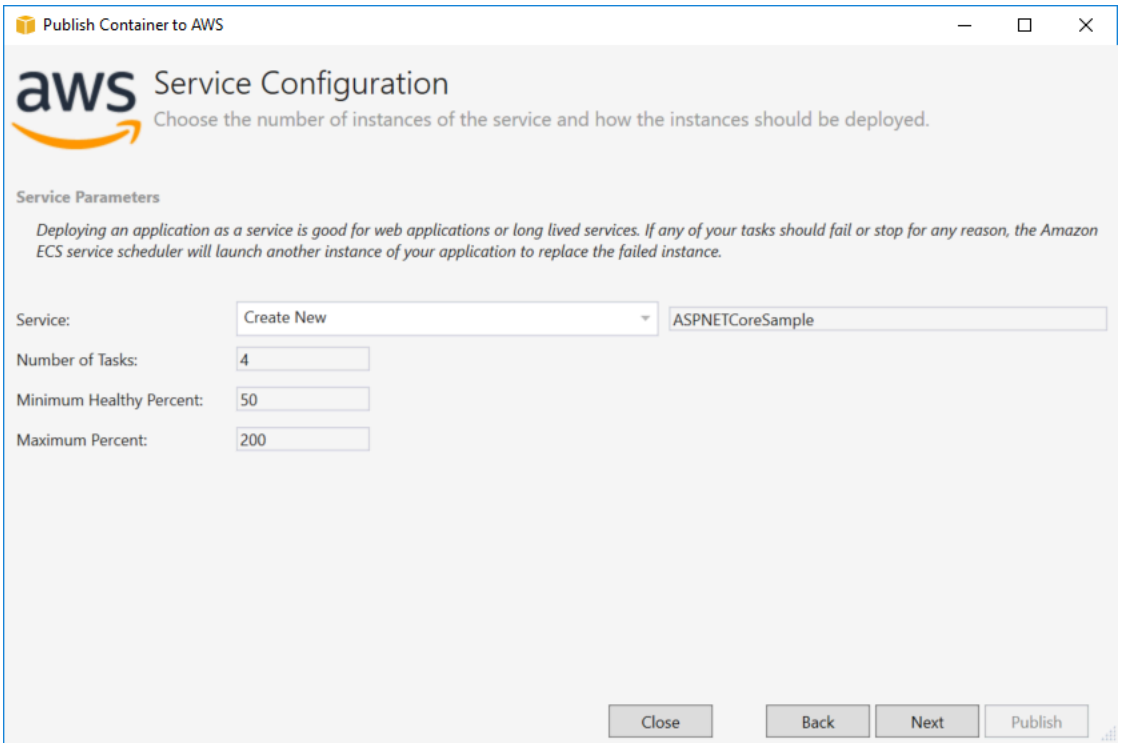
Grupos de segurança — escolha um grupo de segurança.

Um security group funciona como um firewall para as instâncias associadas do Amazon EC2, controlando o tráfego de entrada e de saída no nível da instância.

Grupos de segurança padrão são configurados para permitir o tráfego de entrada das instâncias atribuídas ao mesmo grupo de segurança e a todo o tráfego de saída do IPv4. Você precisa que a saída seja permitida para que o serviço possa alcançar o repositório do contêiner.

Atribuir endereço IP público — marque esta opção para tornar sua tarefa acessível pela Internet.

Página de configuração do serviço



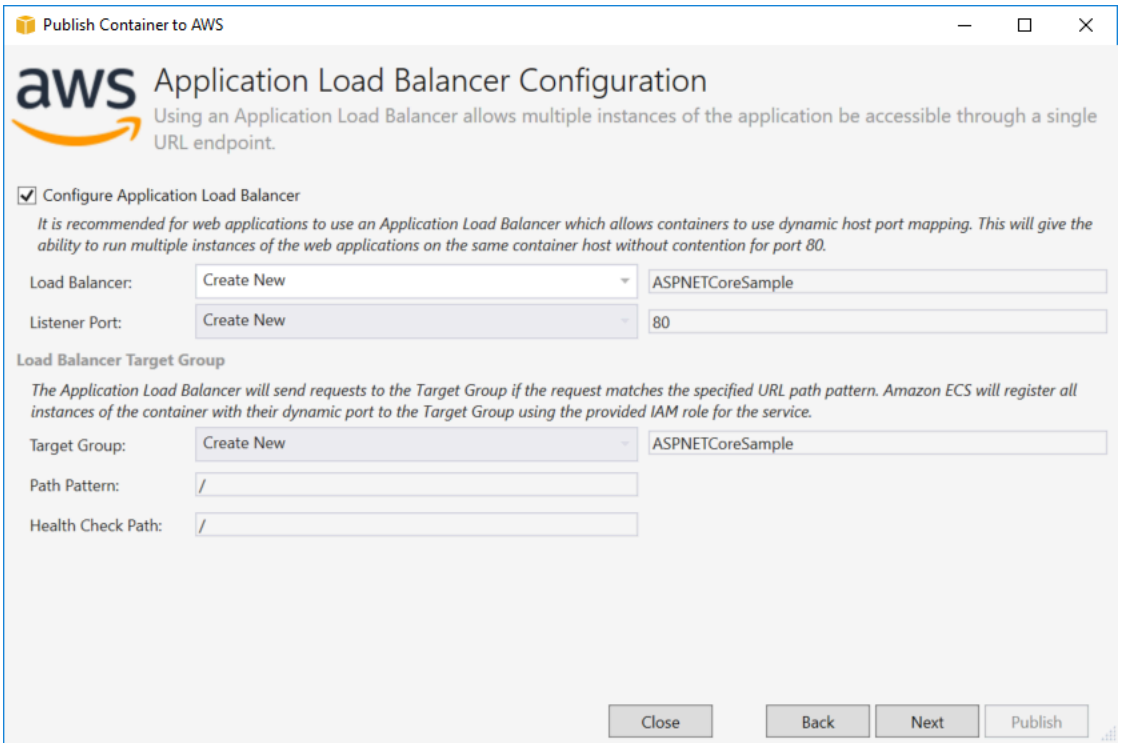
Serviço — selecione um dos serviços na caixa suspensa para implantar seu contêiner em um serviço existente. Ou escolha Create New (Criar novo) para criar um novo serviço. Os nomes de serviço devem ser exclusivos em um cluster, mas é possível ter serviços nomeados similarmente em vários clusters de uma ou várias regiões.

Número de tarefas — o número de tarefas a implantar e manter em execução em seu cluster. Cada tarefa é uma instância do seu contêiner.

Porcentagem de integridade mínima — a porcentagem de tarefas que precisam permanecer em estado `RUNNING` durante uma implantação, arredondada para cima e para o valor inteiro mais próximo.

Porcentagem máxima — a porcentagem de tarefas que são permitidas no estado `RUNNING` ou `PENDING` durante uma implantação, arredondada para baixo e para o valor inteiro mais próximo.

Página do application load balancer



Configurar Application Load Balancer — marque para configurar um Application Load Balancer.

Load balancer — selecione um load balancer existente ou escolha Create New (Criar novo) e digite o nome do novo load balancer.

Porta de ouvinte — selecione uma porta de ouvinte ou escolha Create New (Criar nova) e digite um número de porta. O padrão, a porta `80`, é adequado para a maioria dos aplicativos web.

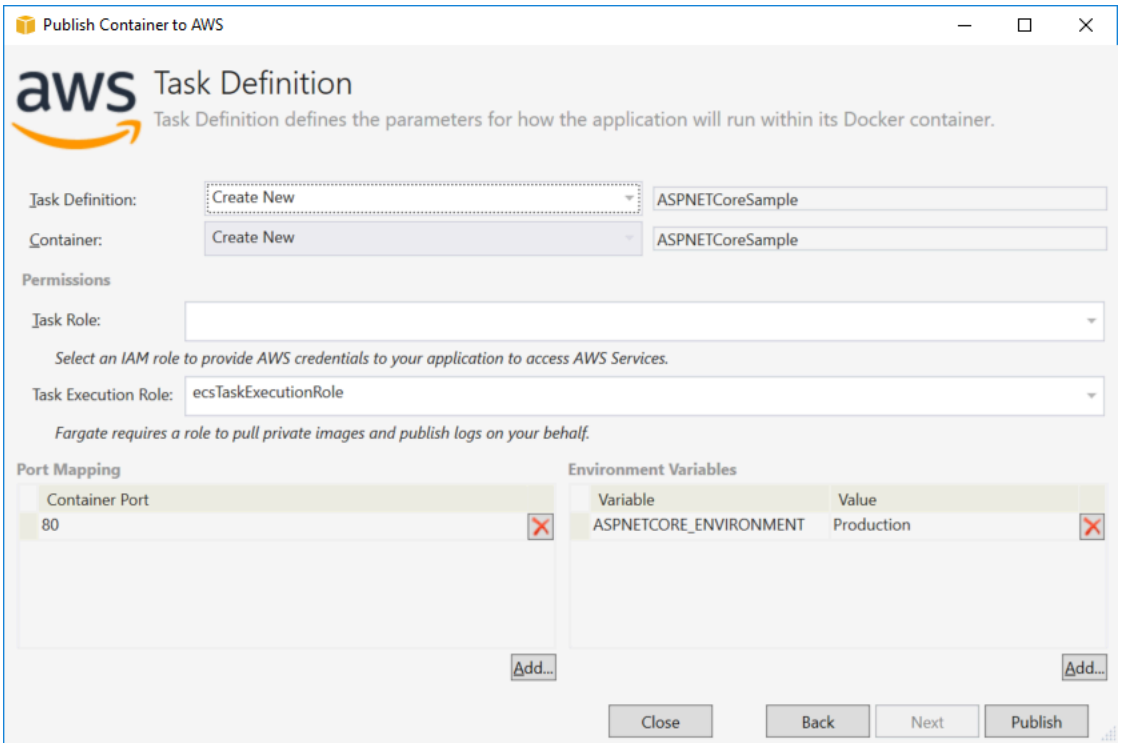
Grupo-alvo - Selecione o grupo-alvo para o qual o Amazon ECS registrará as tarefas no serviço.

Padrão do caminho — o load balancer usará o roteamento com base no caminho. Aceite o padrão `/` ou forneça um padrão diferente. O padrão do caminho diferencia maiúsculas de minúsculas, pode ter até 128 caracteres e conter um conjunto de caracteres selecionados.

Caminho de verificação de integridade — o caminho de ping que é usado como destino para as verificações de integridade. O padrão é `/`. Insira um caminho diferente, se necessário. Se o caminho inserido for inválido, a verificação de integridade falhará e será considerada não íntegra.

Se você implantar vários serviços, e cada serviço for implantado em um caminho ou local diferente, você precisará de caminhos de verificação personalizados.

Página de definição de tarefas



Definição de tarefa — selecione uma definição de tarefa existente ou escolha Create New (Criar nova) e digite o nome da nova definição de tarefa.

Contêiner — selecione um contêiner existente ou escolha Create New (Criar novo) e digite o nome do novo contêiner.

Função de tarefa - selecione uma função do IAM que tenha as credenciais de que seu aplicativo precisa para acessarAWS os Serviços. Esta é a forma como as credenciais são passadas para o seu aplicativo. Veja como especificar as credenciais deAWS segurança para seu aplicativo.

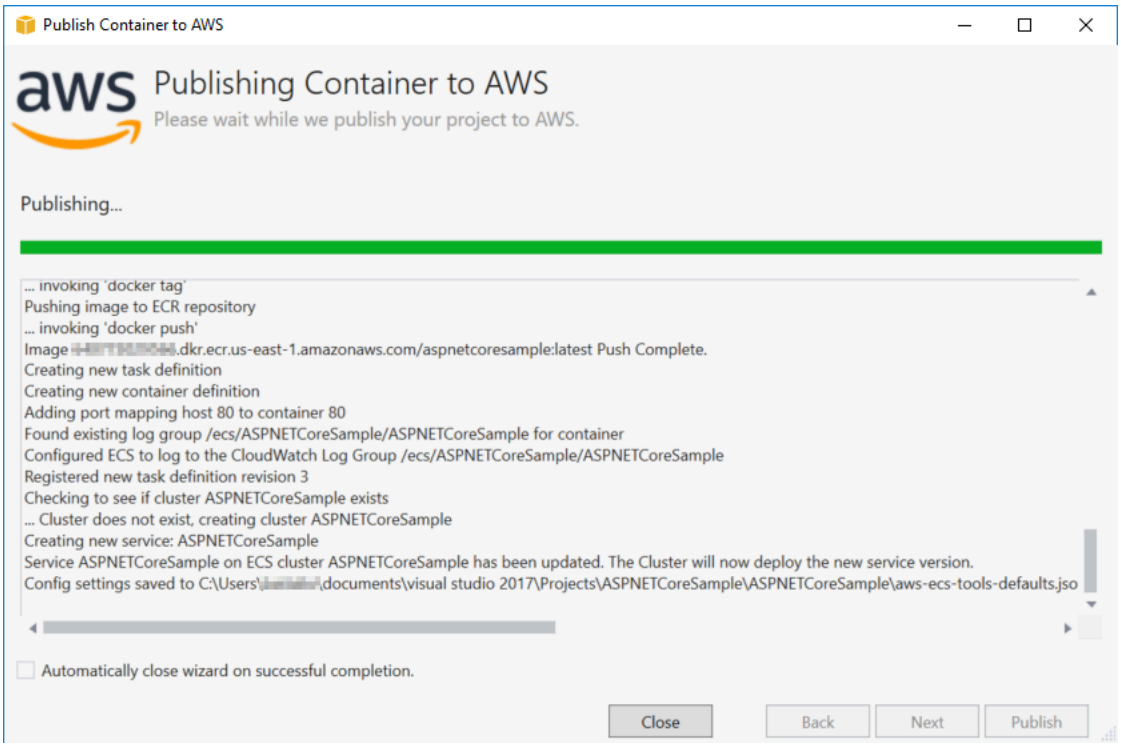
Função de execução de tarefas - Selecione uma função com permissões para extrair imagens privadas e publicar registros. AWS A Fargate o usará em seu nome.

Mapeamento de porta — escolha o número da porta no contêiner que é vinculado à porta host atribuída automaticamente.

Variáveis do ambiente — adicione, modifique ou exclua as variáveis de ambiente do contêiner. Você pode modificá-las de acordo com a sua implantação.

Quando estiver satisfeito com a configuração, clique em Publish (Publicar) para iniciar o processo de implantação.

Contêiner de publicação paraAWS



Os eventos são exibidos durante a implantação. O assistente é fechado automaticamente quando a conclusão é bem-sucedida. Você pode substituir isso desmarcando a caixa na parte inferior da página.

Você pode encontrar o URL de suas novas instâncias noAWS Explorer. Expanda o Amazon ECS e os clusters e, em seguida, clique no seu cluster.

Implantação de um aplicativo ASP.NET Core 2.0 no Amazon ECS (EC2)

Esta seção descreve como usar oPublicar contêiner noAWSAssistente, fornecido como parte do Toolkit for Visual Studio, para implantar um aplicativo ASP.NET Core 2.0 em contêineres direcionados para Linux por meio do Amazon ECS usando o tipo de execução do EC2. Como um aplicativo web é destinado a funcionar continuamente, ele será implantado como um serviço.

Antes de publicar o contêiner

Antes de usar oPublicar contêiner noAWSPara implantar seu aplicativo ASP.NET Core 2.0:

- Especificar seuAWSCredenciaiseObter configuração com o Amazon ECS.
- Instale o Docker. Existem algumas opções de instalação diferentes, incluindo o Docker para Windows.

- Crie um cluster do Amazon ECS de acordo com as necessidades de seu aplicativo web. São necessárias apenas algumas etapas.
- No Visual Studio, crie (ou abra) um projeto para um aplicativo ASP.NET Core 2.0 em contêineres direcionados para Linux.

Acessar o Publish Container to (AWSfeiticeiro

Para implantar um aplicativo ASP.NET Core 2.0 em contêineres direcionados para Linux, clique com o botão direito do mouse no projeto no Solution Explorer e selecionePublicar contêiner noAWS.

Você também pode selecionarPublicar contêiner noAWSNo menu Build (Compilar) do Visual Studio.

Publicar contêiner noAWSFeiticeiro

Perfil de conta a usar — selecione o perfil de conta a ser usado.

Região — escolha uma região de implantação. O perfil e a região são usados para configurar os recursos do ambiente de implantação e selecionar o registro padrão do Docker.

Configuração — selecione a configuração da compilação para a imagem do Docker.

Repositório do Docker — escolha um repositório existente do Docker ou digite o nome de um novo repositório e ele será criado. Este é o repositório para onde a imagem do contêiner de compilação é enviada.

Tag — selecione uma tag existente ou digite o nome de uma nova tag. As tags podem rastrear detalhes importantes, como versão, opções ou outros elementos exclusivos da configuração de contêineres do Docker.

Implantação — selecione Service on an ECS Cluster (Serviço em um cluster do ECS). Use esta opção de implantação para aplicativos de execução prolongada (como um aplicativo web ASP.NET Core 2.0).

Salvar configurações no**`aws-docker-tools-defaults.json`**e configure o projeto para implantação de linha de comando- Marque essa opção se você deseja ter flexibilidade para implantar pela linha de comando. Use `dotnet ecs deploy` a partir do diretório do projeto para implantar e para `dotnet ecs publish` o contêiner.

Página de configuração da execução

Cluster do ECS — selecione o cluster que executará a imagem do Docker. Você podeCriar um cluster do ECSUsar oAWSConsole de gerenciamento.

Tipo de execução — escolha EC2. Para usar o tipo de execução Fargate, consulte Implantar de um aplicativo ASP.NET Core 2.0 no Amazon ECS (Fargate).

Página de configuração do serviço

Serviço — selecione um dos serviços na caixa suspensa para implantar seu contêiner em um serviço existente. Ou escolha Create New (Criar novo) para criar um novo serviço. Os nomes de serviço devem ser exclusivos em um cluster, mas é possível ter serviços nomeados similarmente em vários clusters de uma ou várias regiões.

Número de tarefas — o número de tarefas a implantar e manter em execução em seu cluster. Cada tarefa é uma instância do seu contêiner.

Porcentagem de integridade mínima — a porcentagem de tarefas que precisam permanecer em estado `RUNNING` durante uma implantação, arredondada para cima e para o valor inteiro mais próximo.

Porcentagem máxima — a porcentagem de tarefas que são permitidas no estado `RUNNING` ou `PENDING` durante uma implantação, arredondada para baixo e para o valor inteiro mais próximo.

Modelos de posicionamento — selecione um modelo de posicionamento de tarefas.

Quando você inicia uma tarefa em um cluster, o Amazon ECS precisa determinar onde posicionar a tarefa com base nos requisitos especificados na definição da tarefa, como CPU e memória. Do mesmo modo, quando você reduz proporcionalmente a contagem de tarefas, o Amazon ECS deve determinar que tarefas serão concluídas.

O modelo de posicionamento controla como as tarefas são executadas em um cluster:

- AZ Balanced Spread (Distribuição balanceada de AZ) – Distribua tarefas por zonas de disponibilidade e entre instâncias de contêiner na zona de disponibilidade.
- AZ Balanced BinPack (BinPack balanceado de AZ) – Distribua tarefas por zonas de disponibilidade e entre instâncias de contêiner com a menor memória disponível.
- BinPack – distribua tarefas com base na menor quantidade disponível de CPU ou memória.

- One Task Per Host (Uma tarefa por host) – Posicione, no máximo, uma tarefa do serviço em cada instância de contêiner.

Para obter mais informações, consulte Posicionamento de tarefas no Amazon ECS.

Página do application load balancer

Configurar Application Load Balancer — marque para configurar um Application Load Balancer.

Selecionar função do IAM para o serviço — selecione uma função existente ou escolha Create New (Criar nova) e uma nova função será criada.

Load balancer — selecione um load balancer existente ou escolha Create New (Criar novo) e digite o nome do novo load balancer.

Porta de ouvinte — selecione uma porta de ouvinte ou escolha Create New (Criar nova) e digite um número de porta. O padrão, a porta `80`, é adequado para a maioria dos aplicativos web.

Grupo de destino — por padrão, o load balancer envia solicitações para destinos registrados usando a porta e o protocolo especificados por você para o grupo de destino. Você pode substituir essa porta ao registrar cada destino no grupo de destino.

Padrão do caminho — o load balancer usará o roteamento com base no caminho. Aceite o padrão `/` ou forneça um padrão diferente. O padrão do caminho diferencia maiúsculas de minúsculas, pode ter até 128 caracteres e conter um conjunto de caracteres selecionados.

Caminho de verificação de integridade — o caminho de ping que é usado como destino para as verificações de integridade. Por padrão, é `/`, e é adequado para a maioria dos aplicativos web. Insira um caminho diferente, se necessário. Se o caminho inserido for inválido, a verificação de integridade falhará e será considerada não íntegra.

Se você implantar vários serviços, e cada serviço for implantado em um caminho ou local diferente, você poderá precisar de caminhos de verificação personalizados.

Página de definição de tarefas do ECS

Definição de tarefa — selecione uma definição de tarefa existente ou escolha Create New (Criar nova) e digite o nome da nova definição de tarefa.

Contêiner — selecione um contêiner existente ou escolha Create New (Criar novo) e digite o nome do novo contêiner.

Memória (MiB) — forneça valores para o Limite flexível ou Limite rígido, ou ambos.

O limite flexível (em MiB) de memória a ser reservado para o contêiner. O Docker tenta manter a memória do contêiner abaixo do limite flexível. O contêiner poderá consumir mais memória, até o limite rígido especificado pelo parâmetro de memória (se aplicável), ou toda a memória disponível na instância do contêiner, o que ocorrer primeiro.

O limite rígido (em MiB) de memória a ser apresentado ao contêiner. Caso tente exceder a memória especificada aqui, o contêiner será excluído.

Função de tarefa- Selecione uma função de tarefa para uma função do IAM que permita que a permissão do contêiner chame oAWSAs APIs especificadas nas políticas associadas em seu nome. Esta é a forma como as credenciais são passadas para o seu aplicativo. ConsulteComo especificarAWSCredenciais de segurança para seu aplicativo.

Mapeamento de porta — adicione, modifique ou exclua os mapeamentos de portas para o contêiner. Se um load balancer estiver ativo, a porta do host será definida por padrão como 0 e a atribuição de portas será dinâmica.

Variáveis do ambiente — adicione, modifique ou exclua as variáveis de ambiente do contêiner.

Quando estiver satisfeito com a configuração, clique em Publish (Publicar) para iniciar o processo de implantação.

Publicar contêiner noAWS

Os eventos são exibidos durante a implantação. O assistente é fechado automaticamente quando a conclusão é bem-sucedida. Você pode substituir isso desmarcando a caixa na parte inferior da página.

Você pode encontrar o URL de suas novas instâncias noAWSExplorador. Expanda o Amazon ECS e os clusters e, em seguida, clique no seu cluster.

Solução de problemas do AWS Toolkit for Visual Studio

As seções a seguir contêm informações gerais sobre solução de problemas AWS Toolkit for Visual Studio e como trabalhar com AWS os serviços do kit de ferramentas.

> **Note**
>
> As informações sobre instalação e set-up-specific solução de problemas estão disponíveis no tópico Solução de problemas de instalação, localizado neste Guia do usuário.

Tópicos

Práticas recomendadas de solução de problemas

A seguir estão as melhores práticas recomendadas para solucionar AWS Toolkit for Visual Studio problemas.

- Tente recriar seu problema ou erro antes de enviar um relatório.
- Faça anotações detalhadas de cada etapa, configuração e mensagem de erro durante o processo de recriação.
- Colete registros AWS do kit de ferramentas. Para obter uma descrição detalhada de como localizar seus registros do AWS Toolkit, consulte o procedimento Como localizar seus AWS registros, localizado neste tópico do guia.
- Verifique se há solicitações abertas, soluções conhecidas ou relate seu problema não resolvido na seção AWS Toolkit for Visual Studio Problemas do AWS Toolkit for Visual Studio GitHub repositório.

Como localizar seus registros do AWS Toolkit

1. No menu principal do Visual Studio, expanda Extensões.
2. Escolha o AWS kit de ferramentas para expandir o menu do kit de AWS ferramentas e, em seguida, escolha Exibir registros do kit de ferramentas.

3. Quando a pasta de registros do AWS Toolkit abrir em seu sistema operacional, classifique os arquivos por data e localize qualquer arquivo de log que contenha informações relevantes ao seu problema atual.

O CodeWhisperer login e a saída da Amazon estão desativados

Se você estiver enfrentando um problema com o CodeWhisperer serviço em que os itens do menu Entrar e Sair estão desativados, solucione o problema concluindo as etapas a seguir.

1. No Explorador de Arquivos do Windows, navegue até a pasta de cache do AWS Toolkit localizada em:`%LOCALAPPDATA%/aws/toolkits/language-servers/CodeWhisperer`.
2. Limpe o conteúdo da pasta de cache.
3. Feche e reabra a solução atual.

Segurança para AWS Toolkit for Visual Studio

A segurança da nuvem na Amazon Web Services (AWS) é a nossa maior prioridade. Como cliente da AWS , você contará com um data center e uma arquitetura de rede criados para atender aos requisitos das organizações com as maiores exigências de segurança. A segurança é uma responsabilidade compartilhada entre você AWS e você. O modelo de responsabilidade compartilhada descreve isso como a Segurança da nuvem e a Segurança na nuvem.

Segurança da nuvem — AWS é responsável por proteger a infraestrutura que executa todos os serviços oferecidos na AWS nuvem e fornecer serviços que você possa usar com segurança. Nossa responsabilidade de segurança é a maior prioridade em AWS, e a eficácia de nossa segurança é regularmente testada e verificada por auditores terceirizados como parte dos Programas de AWS Conformidade.

Segurança na nuvem — Sua responsabilidade é determinada pelo AWS serviço que você está usando e por outros fatores, incluindo a sensibilidade de seus dados, os requisitos da sua organização e as leis e regulamentos aplicáveis.

Esse AWS produto ou serviço segue o modelo de responsabilidade compartilhada por meio dos serviços específicos da Amazon Web Services (AWS) que ele suporta. Para AWS obter informações sobre segurança do AWS serviço, consulte a página de documentação de segurança do serviço e os AWS serviços que estão no escopo dos esforços de AWS conformidade do programa de conformidade.

Tópicos

Proteção de dados em AWS Toolkit for Visual Studio

O modelo de responsabilidade AWS compartilhada se aplica à proteção de dados no AWS Toolkit for Visual Studio. Conforme descrito neste modelo, AWS é responsável por proteger a

infraestrutura global que executa todos os Nuvem AWS. Você é responsável por manter o controle sobre seu conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para ter mais informações sobre a privacidade de dados, consulte as Perguntas frequentes sobre privacidade de dados. Para ter mais informações sobre a proteção de dados na Europa, consulte a AWS postagem do blog Shared Responsibility Model and GDPR no AWS Blog de segurança da.

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Dessa maneira, cada usuário receberá apenas as permissões necessárias para cumprir suas obrigações de trabalho. Recomendamos também que você proteja seus dados das seguintes formas:

- Use uma autenticação multifator (MFA) com cada conta.
- Use SSL/TLS para se comunicar com os recursos. AWS Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail.
- Use soluções de AWS criptografia, juntamente com todos os controles de segurança padrão Serviços da AWS.
- Use serviços gerenciados de segurança avançada, como o Amazon Macie, que ajuda a localizar e proteger dados sigilosos armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-2 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para ter mais informações sobre endpoints do FIPS, consulte Federal Information Processing Standard (FIPS) 140-2.

É altamente recomendável que nunca sejam colocadas informações de identificação confidenciais, como endereços de email dos seus clientes, em marcações ou campos de formato livre, como um campo Name (Nome). Isso inclui quando você trabalha com o Toolkit for Visual Studio ou Serviços da AWS outro usando o console, a API AWS ou os AWS CLI SDKs. Quaisquer dados inseridos em tags ou campos de texto de formato livre usados para nomes podem ser usados para logs de faturamento ou de diagnóstico. Se você fornecer um URL para um servidor externo, recomendemos fortemente que não sejam incluídas informações de credenciais no URL para validar a solicitação a esse servidor.

Identity and Access Management

AWS Identity and Access Management (IAM) é uma ferramenta AWS service (Serviço da AWS) que ajuda o administrador a controlar com segurança o acesso aos AWS recursos. Os administradores do IAM controlam quem pode ser autenticado (conectado) e autorizado (tem permissões) a usar AWS os recursos. O IAM é um AWS service (Serviço da AWS) que você pode usar sem custo adicional.

Tópicos

Público

A forma como você usa AWS Identity and Access Management (IAM) difere, dependendo do trabalho que você faz AWS.

Usuário do serviço — Se você Serviços da AWS costuma fazer seu trabalho, seu administrador fornece as credenciais e as permissões de que você precisa. À medida que você usa mais AWS recursos para fazer seu trabalho, talvez precise de permissões adicionais. Entender como o acesso é gerenciado pode ajudar você a solicitar as permissões corretas ao seu administrador. Se você não conseguir acessar um recurso no AWS, consulte Solução de problemas AWS de identidade e acesso ou o guia do usuário do AWS service (Serviço da AWS) que você está usando.

Administrador de serviços — Se você é responsável pelos AWS recursos da sua empresa, provavelmente tem acesso total AWS a. É seu trabalho determinar quais AWS recursos e recursos seus usuários do serviço devem acessar. Assim, você deve enviar solicitações ao administrador do IAM para alterar as permissões dos usuários de seu serviço. Revise as informações nesta página para entender os Introdução ao IAM. Para saber mais sobre como sua empresa pode usar o IAM com AWS, consulte o guia do usuário do AWS service (Serviço da AWS) que você está usando.

Administrador do IAM: Se você for um administrador do IAM, talvez queira saber detalhes sobre como pode gravar políticas para gerenciar acesso ao AWS. Para ver exemplos de políticas AWS

baseadas em identidade que você pode usar no IAM, consulte o guia do usuário do AWS service (Serviço da AWS) que você está usando.

Autenticando com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado (conectado AWS) como o Usuário raiz da conta da AWS, como usuário do IAM ou assumindo uma função do IAM.

Você pode entrar AWS como uma identidade federada usando credenciais fornecidas por meio de uma fonte de identidade. AWS IAM Identity Center Usuários (IAM Identity Center), a autenticação de login único da sua empresa e suas credenciais do Google ou do Facebook são exemplos de identidades federadas. Quando você faz login como identidade federada, o administrador já configurou anteriormente a federação de identidades usando perfis do IAM. Ao acessar AWS usando a federação, você está assumindo indiretamente uma função.

Dependendo do tipo de usuário que você é, você pode entrar no AWS Management Console ou no portal de AWS acesso. Para obter mais informações sobre como fazer login AWS, consulte Como fazer login Conta da AWS no Guia do Início de Sessão da AWS usuário.

Se você acessar AWS programaticamente, AWS fornece um kit de desenvolvimento de software (SDK) e uma interface de linha de comando (CLI) para assinar criptograficamente suas solicitações usando suas credenciais. Se você não usa AWS ferramentas, você mesmo deve assinar as solicitações. Para obter mais informações sobre como usar o método recomendado para assinar solicitações por conta própria, consulte Assinatura de solicitações de AWS API no Guia do usuário do IAM.

Independente do método de autenticação usado, também pode ser exigido que você forneça informações adicionais de segurança. Por exemplo, AWS recomenda que você use a autenticação multifator (MFA) para aumentar a segurança da sua conta. Para saber mais, consulte Autenticação Multifator no AWS IAM Identity Center Guia do Usuário. Usar a autenticação multifator (MFA) na AWS no Guia do Usuário do IAM.

Conta da AWS usuário root

Ao criar uma Conta da AWS, você começa com uma identidade de login que tem acesso completo a todos Serviços da AWS os recursos da conta. Essa identidade é chamada de usuário Conta da AWS raiz e é acessada fazendo login com o endereço de e-mail e a senha que você usou para criar a conta. É altamente recomendável não usar o usuário raiz para tarefas diárias. Proteja as credenciais do usuário raiz e use-as para executar as tarefas que somente ele pode executar. Para obter a lista

completa das tarefas que exigem login como usuário raiz, consulte Tarefas que exigem credenciais de usuário raiz no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que usuários humanos, incluindo usuários que precisam de acesso de administrador, usem a federação com um provedor de identidade para acessar Serviços da AWS usando credenciais temporárias.

Uma identidade federada é um usuário do seu diretório de usuários corporativo, de um provedor de identidade da web AWS Directory Service, do diretório do Identity Center ou de qualquer usuário que acesse usando credenciais fornecidas Serviços da AWS por meio de uma fonte de identidade. Quando as identidades federadas são acessadas Contas da AWS, elas assumem funções, e as funções fornecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos usar o . AWS IAM Identity Center Você pode criar usuários e grupos no IAM Identity Center ou pode se conectar e sincronizar com um conjunto de usuários e grupos em sua própria fonte de identidade para uso em todos os seus Contas da AWS aplicativos. Para obter mais informações sobre o Centro de Identidade do IAM, consulte O que é o Centro de Identidade do IAM? no AWS IAM Identity Center Manual do Usuário do.

Usuários e grupos do IAM

Um usuário do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas para uma única pessoa ou aplicativo. Sempre que possível, recomendamos depender de credenciais temporárias em vez de criar usuários do IAM com credenciais de longo prazo, como senhas e chaves de acesso. No entanto, se você tiver casos de uso específicos que exijam credenciais de longo prazo com usuários do IAM, recomendamos alternar as chaves de acesso. Para obter mais informações, consulte Alterne Chaves de Acesso Regularmente para Casos de Uso que exijam Credenciais de Longo Prazo no Guia do Usuário do IAM.

Um grupo do IAM é uma identidade que especifica uma coleção de usuários do IAM. Não é possível fazer login como um grupo. É possível usar grupos para especificar permissões para vários usuários de uma vez. Os grupos facilitam o gerenciamento de permissões para grandes conjuntos de usuários. Por exemplo, você pode ter um nome de grupo IAMAdmins e atribuir a esse grupo permissões para administrar recursos do IAM.

Usuários são diferentes de perfis. Um usuário é exclusivamente associado a uma pessoa ou a um aplicativo, mas uma função pode ser assumida por qualquer pessoa que precisar dela. Os usuários têm credenciais permanentes de longo prazo, mas os perfis fornecem credenciais temporárias.

Para saber mais, consulte Quando Criar um Usuário do IAM (Ao Invés de uma Função) no Guia do Usuário do IAM.

Perfis do IAM

Uma função do IAM é uma identidade dentro da sua Conta da AWS que tem permissões específicas. Ele é semelhante a um usuário do IAM, mas não está associado a uma pessoa específica. Você pode assumir temporariamente uma função do IAM no AWS Management Console trocando de funções. Você pode assumir uma função chamando uma operação de AWS API AWS CLI ou usando uma URL personalizada. Para obter mais informações sobre métodos para usar perfis, consulte Usando Funções do IAM no Guia do Usuário do IAM.

Funções do IAM com credenciais temporárias são úteis nas seguintes situações:

- Acesso de usuário federado: para atribuir permissões a identidades federadas, você pode criar um perfil e definir permissões para ele. Quando uma identidade federada é autenticada, essa identidade é associada ao perfil e recebe as permissões definidas pelo mesmo. Para obter mais informações sobre perfis para federação, consulte Criando um Perfil para um Provedor de Identidades Terceirizado no Guia do Usuário do IAM. Se você usa o IAM Identity Center, configure um conjunto de permissões. Para controlar o que suas identidades podem acessar após a autenticação, o IAM Identity Center correlaciona o conjunto de permissões a um perfil no IAM. Para obter informações sobre conjuntos de permissões, consulte Conjuntos de Permissões no AWS IAM Identity Center Manual do Usuário.
- Permissões de usuários temporárias do IAM: um usuário ou perfil do IAM pode assumir um perfil do IAM para obter temporariamente permissões diferentes para uma tarefa específica.
- Acesso entre contas: você pode usar um perfil do IAM para permitir que alguém (uma entidade principal confiável) acesse recursos na sua conta de uma conta diferente. As funções são a forma primária de conceder acesso entre contas. No entanto, com alguns Serviços da AWS, você pode anexar uma política diretamente a um recurso (em vez de usar uma função como proxy). Para aprender a diferença entre funções e políticas baseadas em recurso para acesso entre contas, consulte Como as Funções do IAM Diferem das Políticas Baseadas em Recurso no Guia do Usuário do IAM.
- Acesso entre serviços — Alguns Serviços da AWS usam recursos em outros Serviços da AWS. Por exemplo, quando você faz uma chamada em um serviço, é comum que esse serviço execute aplicativos no Amazon EC2 ou armazene objetos no Amazon S3. Um serviço pode fazer isso usando as permissões de chamada da entidade principal, uma função de serviço ou uma função vinculada ao serviço.

- Sessões de acesso direto (FAS) — Quando você usa um usuário ou uma função do IAM para realizar ações AWS, você é considerado principal. Ao usar alguns serviços, você pode executar uma ação que inicia outra ação em um serviço diferente. O FAS usa as permissões do diretor chamando um AWS service (Serviço da AWS), combinadas com a solicitação AWS service (Serviço da AWS) para fazer solicitações aos serviços posteriores. As solicitações do FAS são feitas somente quando um serviço recebe uma solicitação que requer interações com outros Serviços da AWS ou com recursos para ser concluída. Nesse caso, você precisa ter permissões para executar ambas as ações. Para obter detalhes da política ao fazer solicitações de FAS, consulte Encaminhar sessões de acesso.
- Função de Serviço: uma função de serviço é uma função do IAM que um serviço assume para realizar ações em seu nome. Um administrador do IAM pode criar, modificar e excluir um perfil de serviço do IAM. Para obter mais informações, consulte Criando um Perfil para Delegar Permissões a um AWS service (Serviço da AWS) no Guia do Usuário do IAM.
- Função vinculada ao serviço — Uma função vinculada ao serviço é um tipo de função de serviço vinculada a um. AWS service (Serviço da AWS) O serviço pode assumir o perfil de executar uma ação em seu nome. As funções vinculadas ao serviço aparecem em você Conta da AWS e são de propriedade do serviço. Um administrador do IAM pode visualizar, mas não pode editar as permissões para funções vinculadas a serviço.

- Aplicativos em execução no Amazon EC2 — Você pode usar uma função do IAM para gerenciar credenciais temporárias para aplicativos que estão sendo executados em uma instância do EC2 e fazendo AWS CLI solicitações de API. AWS É preferível fazer isso a armazenar chaves de acesso na instância do EC2. Para atribuir uma AWS função a uma instância do EC2 e disponibilizá-la para todos os seus aplicativos, você cria um perfil de instância anexado à instância. Um perfil de instância contém a perfil e permite que os programas em execução na instância do EC2 obtenham credenciais temporárias. Para mais informações, consulte Usar uma função do IAM para conceder permissões a aplicativos em execução nas instâncias do Amazon EC2 no Guia do usuário do IAM.

Para aprender se deseja usar perfis do IAM, consulte Quando Criar uma Função do IAM (em Vez de um Usuário) no Guia do Usuário do IAM.

Gerenciando acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política é um objeto AWS que, quando associada a uma identidade ou recurso, define suas permissões. AWS avalia essas políticas quando um principal (usuário, usuário raiz ou sessão de função) faz uma solicitação. As permissões nas políticas determinam se a solicitação será permitida

ou negada. A maioria das políticas é armazenada AWS como documentos JSON. Para obter mais informações sobre a estrutura e o conteúdo de documentos de políticas JSON, consulte Visão Geral das Políticas JSON no Guia do Usuário do IAM.

Os administradores podem usar políticas AWS JSON para especificar quem tem acesso ao quê. Ou seja, qual entidade principal pode executar ações em quais recursos e em que condições.

Por padrão, usuários e funções não têm permissões. Para conceder aos usuários permissão para executar ações nos recursos de que eles precisam, um administrador do IAM pode criar políticas do IAM. O administrador pode então adicionar as políticas do IAM às funções e os usuários podem assumir as funções.

As políticas do IAM definem permissões para uma ação, independente do método usado para executar a operação. Por exemplo, suponha que você tenha uma política que permite a ação `iam:GetRole`. Um usuário com essa política pode obter informações de função da AWS Management Console AWS CLI, da ou da AWS API.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissões JSON que você pode anexar a uma identidade, como usuário do IAM, grupo de usuários ou perfil do IAM. Essas políticas controlam quais ações os usuários e funções podem realizar, em quais recursos e em quais condições. Para saber como criar uma política baseada em identidade, consulte Criar políticas do IAM no Guia do usuário do IAM.

As políticas baseadas em identidade também podem ser categorizadas como políticas em linha ou políticas gerenciadas. As políticas em linha são incorporadas diretamente a um único usuário, grupo ou função. As políticas gerenciadas são políticas autônomas que você pode associar a vários usuários, grupos e funções em seu Conta da AWS. As políticas AWS gerenciadas incluem políticas gerenciadas e políticas gerenciadas pelo cliente. Para saber como selecionar entre uma política gerenciada ou uma política em linha, consulte Selecionar entre políticas gerenciadas e políticas em linha no Guia do usuário do IAM.

Políticas baseadas em recursos

Políticas baseadas em recursos são documentos de políticas JSON que você anexa a um recurso. São exemplos de políticas baseadas em recursos as políticas de confiança de função do IAM e as políticas do bucket do Amazon S3. Em serviços que suportem políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. Para o recurso ao qual a política está anexada, a política define quais ações uma entidade principal

especificada pode executar nesse recurso e em que condições. Você deve especificar uma entidade principal em uma política baseada em recursos. Os diretores podem incluir contas, usuários, funções, usuários federados ou. Serviços da AWS

Políticas baseadas em atributos são políticas em linha que estão localizadas nesse serviço. Você não pode usar políticas AWS gerenciadas do IAM em uma política baseada em recursos.

Listas de controle de acesso (ACLs)

As listas de controle de acesso (ACLs) controlam quais entidades principais (membros, usuários ou funções da conta) têm permissão para acessar um recurso. As ACLs são semelhantes as políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o Amazon VPC são exemplos de serviços que oferecem suporte a ACLs. AWS WAF Saiba mais sobre ACLs em Configurações da lista de controle de acesso (ACL) no Guia do Desenvolvedor do Amazon Simple Storage Service.

Outros tipos de política

AWS oferece suporte a tipos de políticas adicionais menos comuns. Esses tipos de política podem definir o máximo de permissões concedidas a você pelos tipos de política mais comuns.

- Limites de permissões: um limite de permissões é um recurso avançado no qual você define o máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM (usuário ou perfil do IAM). É possível definir um limite de permissões para uma entidade. As permissões resultantes são a interseção das políticas baseadas em identidade de uma entidade e dos seus limites de permissões. As políticas baseadas em atributo que especificam o usuário ou o perfil no campo `Principal` não são limitadas pelo limite de permissões. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações sobre limites de permissões, consulte Limites de Permissões para Entidades do IAM no Guia do Usuário do IAM.
- Políticas de controle de serviço (SCPs) — SCPs são políticas JSON que especificam as permissões máximas para uma organização ou unidade organizacional (OU) em. AWS Organizations AWS Organizations é um serviço para agrupar e gerenciar centralmente vários Contas da AWS que sua empresa possui. Se você habilitar todos os atributos em uma organização, poderá aplicar políticas de controle de serviço (SCPs) a qualquer uma ou a todas as contas. O SCP limita as permissões para entidades nas contas dos membros, incluindo cada uma Usuário raiz da conta da AWS. Para obter mais informações sobre o Organizações e SCPs, consulte Como os SCPs Funcionam no AWS Organizations Manual do Usuário do.

- Políticas de sessão: são políticas avançadas que você transmite como um parâmetro quando cria de forma programática uma sessão temporária para uma função ou um usuário federado. As permissões da sessão resultante são a interseção das políticas baseadas em identidade do usuário ou do perfil e das políticas de sessão. As permissões também podem ser provenientes de uma política baseada em atributo. Uma negação explícita em qualquer uma dessas políticas substitui a permissão. Para obter mais informações, consulte Políticas de sessão no Guia do usuário do IAM.

Vários tipos de política

Quando vários tipos de política são aplicáveis a uma solicitação, é mais complicado compreender as permissões resultantes. Para saber como AWS determinar se uma solicitação deve ser permitida quando vários tipos de políticas estão envolvidos, consulte Lógica de avaliação de políticas no Guia do usuário do IAM.

Como Serviços da AWS trabalhar com o IAM

Para ter uma visão de alto nível de como Serviços da AWS funciona com a maioria dos recursos do IAM, consulte AWS os serviços que funcionam com o IAM no Guia do usuário do IAM.

Para saber como usar um específico AWS service (Serviço da AWS) com o IAM, consulte a seção de segurança do Guia do usuário do serviço relevante.

Solução de problemas AWS de identidade e acesso

Use as informações a seguir para ajudá-lo a diagnosticar e corrigir problemas comuns que você pode encontrar ao trabalhar com AWS um IAM.

Tópicos

- Não estou autorizado a realizar uma ação em AWS
- Não estou autorizado a realizar iam: PassRole
- Quero permitir que pessoas fora da minha Conta da AWS acessem meus AWS recursos

Não estou autorizado a realizar uma ação em AWS

Se você receber uma mensagem de erro informando que não tem autorização para executar uma ação, suas políticas deverão ser atualizadas para permitir que você realize a ação.

O erro do exemplo a seguir ocorre quando o usuário do IAM `mateojackson` tenta usar o console para visualizar detalhes sobre um atributo *`my-example-widget`* fictício, mas não tem as permissões `awes:`*`GetWidget`* fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 awes:GetWidget on resource: my-example-widget
```

Nesse caso, a política do usuário `mateojackson` deve ser atualizada para permitir o acesso ao recurso *`my-example-widget`* usando a ação `awes:`*`GetWidget`*.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Não estou autorizado a realizar iam: PassRole

Se você receber uma mensagem de erro informando que não está autorizado a executar a ação `iam:PassRole`, as suas políticas devem ser atualizadas para permitir que você passe uma função para o AWS.

Alguns Serviços da AWS permitem que você passe uma função existente para esse serviço em vez de criar uma nova função de serviço ou uma função vinculada ao serviço. Para fazê-lo, você deve ter permissões para passar o perfil para o serviço.

O exemplo de erro a seguir ocorre quando uma usuária do IAM chamada `marymajor` tenta utilizar o console para executar uma ação no AWS. No entanto, a ação exige que o serviço tenha permissões concedidas por um perfil de serviço. Mary não tem permissões para passar o perfil para o serviço.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

Nesse caso, as políticas de Mary devem ser atualizadas para permitir que ela realize a ação `iam:PassRole`.

Se precisar de ajuda, entre em contato com seu AWS administrador. Seu administrador é a pessoa que forneceu suas credenciais de login.

Quero permitir que pessoas fora da minha Conta da AWS acessem meus AWS recursos

Você pode criar uma função que os usuários de outras contas ou pessoas fora da sua organização possam usar para acessar seus recursos. Você pode especificar quem é confiável para assumir o

perfil. Para serviços que oferecem suporte a políticas baseadas em recursos ou listas de controle de acesso (ACLs), você pode usar políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se é AWS compatível com esses recursos, consulteComo Serviços da AWS trabalhar com o IAM.
- Para saber como fornecer acesso aos seus recursos em todos os Contas da AWS que você possui, consulte Como fornecer acesso a um usuário do IAM em outro Conta da AWS que você possui no Guia do usuário do IAM.
- Para saber como fornecer acesso aos seus recursos a terceiros Contas da AWS, consulte Como fornecer acesso Contas da AWS a terceiros no Guia do usuário do IAM.
- Saiba como conceder acesso por meio da federação de identidades consultando Concedendo Acesso a Usuários Autenticados Externamente (Federação de Identidades) no Guia do Usuário do IAM.
- Para saber a diferença entre usar perfis e políticas baseadas em recursos para acesso entre contas, consulte Como os perfis do IAM diferem de políticas baseadas em recursos no Guia do usuário do IAM.

Validação de conformidade para este AWS produto ou serviço

Para saber se um AWS service (Serviço da AWS) está dentro do escopo de programas de conformidade específicos, consulte Serviços da AWS Escopo por Programa de Conformidade Serviços da AWS e escolha o programa de conformidade em que você está interessado. Para obter informações gerais, consulte Programas de AWS conformidade Programas AWS de .

Você pode baixar relatórios de auditoria de terceiros usando AWS Artifact. Para obter mais informações, consulte Baixar relatórios em AWS Artifact .

Sua responsabilidade de conformidade ao usar Serviços da AWS é determinada pela confidencialidade de seus dados, pelos objetivos de conformidade de sua empresa e pelas leis e regulamentações aplicáveis. AWS fornece os seguintes recursos para ajudar na conformidade:

- Guias de início rápido sobre segurança e conformidade — Esses guias de implantação discutem considerações arquitetônicas e fornecem etapas para a implantação de ambientes básicos AWS focados em segurança e conformidade.

- Arquitetura para segurança e conformidade com a HIPAA na Amazon Web Services — Este whitepaper descreve como as empresas podem usar AWS para criar aplicativos qualificados para a HIPAA.

> **Note**
>
> Nem todos Serviços da AWS são elegíveis para a HIPAA. Para obter mais informações, consulte Referência dos Serviços Qualificados pela HIPAA.

- AWS Recursos de https://aws.amazon.com/compliance/resources/ de conformidade — Essa coleção de pastas de trabalho e guias pode ser aplicada ao seu setor e local.
- AWS Guias de conformidade do cliente — Entenda o modelo de responsabilidade compartilhada sob a ótica da conformidade. Os guias resumem as melhores práticas de proteção Serviços da AWS e mapeiam as diretrizes para controles de segurança em várias estruturas (incluindo o Instituto Nacional de Padrões e Tecnologia (NIST), o Conselho de Padrões de Segurança do Setor de Cartões de Pagamento (PCI) e a Organização Internacional de Padronização (ISO)).
- Avaliação de recursos com regras no Guia do AWS Config desenvolvedor — O AWS Config serviço avalia o quão bem suas configurações de recursos estão em conformidade com as práticas internas, as diretrizes e os regulamentos do setor.
- AWS Security Hub— Isso AWS service (Serviço da AWS) fornece uma visão abrangente do seu estado de segurança interno AWS. O Security Hub usa controles de segurança para avaliar os atributos da AWS e verificar a conformidade com os padrões e as práticas recomendadas do setor de segurança. Para obter uma lista dos serviços com suporte e controles aceitos, consulte a Referência de controles do Security Hub.
- Amazon GuardDuty — Isso AWS service (Serviço da AWS) detecta possíveis ameaças às suas cargas de trabalho Contas da AWS, contêineres e dados monitorando seu ambiente em busca de atividades suspeitas e maliciosas. GuardDuty pode ajudá-lo a atender a vários requisitos de conformidade, como o PCI DSS, atendendo aos requisitos de detecção de intrusões exigidos por determinadas estruturas de conformidade.
- AWS Audit Manager— Isso AWS service (Serviço da AWS) ajuda você a auditar continuamente seu AWS uso para simplificar a forma como você gerencia o risco e a conformidade com as regulamentações e os padrões do setor.

Esse AWS produto ou serviço segue o modelo de responsabilidade compartilhada por meio dos serviços específicos da Amazon Web Services (AWS) que ele suporta. Para AWS obter informações sobre segurança do AWS serviço, consulte a página de documentação de segurança do serviço

e os AWS serviços que estão no escopo dos esforços de AWS conformidade do programa de conformidade.

Resiliência para este AWS produto ou serviço

A infraestrutura AWS global é construída em torno Regiões da AWS de zonas de disponibilidade.

Regiões da AWS fornecem várias zonas de disponibilidade fisicamente separadas e isoladas, conectadas a redes de baixa latência, alta taxa de transferência e alta redundância.

Com as zonas de disponibilidade, é possível projetar e operar aplicações e bancos de dados que automaticamente executam o failover entre as zonas sem interrupção. As zonas de disponibilidade são mais altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de datacenter tradicionais.

Para obter mais informações sobre AWS regiões e zonas de disponibilidade, consulte Infraestrutura AWS global.

Esse AWS produto ou serviço segue o modelo de responsabilidade compartilhada por meio dos serviços específicos da Amazon Web Services (AWS) que ele suporta. Para AWS obter informações sobre segurança do AWS serviço, consulte a página de documentação de segurança do serviço e os AWS serviços que estão no escopo dos esforços de AWS conformidade do programa de conformidade.

Segurança da infraestrutura para este AWS produto ou serviço

Esse AWS produto ou serviço usa serviços gerenciados e, portanto, é protegido pela segurança de rede AWS global. Para obter informações sobre serviços AWS de segurança e como AWS proteger a infraestrutura, consulte AWS Cloud Security. Para projetar seu AWS ambiente usando as melhores práticas de segurança de infraestrutura, consulte Proteção de infraestrutura no Security Pillar AWS Well-Architected Framework.

Você usa chamadas de API AWS publicadas para acessar este AWS Produto ou Serviço pela rede. Os clientes devem ser compatíveis com:

- Transport Layer Security (TLS). Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Conjuntos de criptografia com Perfect Forward Secrecy (PFS) como DHE (Ephemeral Diffie-Hellman) ou ECDHE (Ephemeral Elliptic Curve Diffie-Hellman). A maioria dos sistemas modernos, como Java 7 e versões posteriores, suporta esses modos.

Além disso, as solicitações devem ser assinadas utilizando um ID da chave de acesso e uma chave de acesso secreta associada a uma entidade principal do IAM. Ou é possível usar o AWS Security Token Service (AWS STS) para gerar credenciais de segurança temporárias para assinar solicitações.

Esse AWS produto ou serviço segue o modelo de responsabilidade compartilhada por meio dos serviços específicos da Amazon Web Services (AWS) que ele suporta. Para AWS obter informações sobre segurança do AWS serviço, consulte a página de documentação de segurança do serviço e os AWS serviços que estão no escopo dos esforços de AWS conformidade do programa de conformidade.

Análise de configuração e vulnerabilidade em AWS Toolkit for Visual Studio

O kit de ferramentas para Visual Studio será liberado para o Visual Studio Marketplace à medida que novos recursos ou correções forem desenvolvidos. Como essas atualizações às vezes incluem atualizações de segurança, é importante manter o kit de ferramentas para Visual Studio atualizado.

Para verificar se as atualizações automáticas para extensões estão habilitadas

1. Abra o gerenciador de extensões escolhendo Ferramentas, Extensões e atualizações (Visual Studio 2017) ou Extensões, Gerenciar extensões (Visual Studio 2019).
2. Escolha Alterar configurações de extensões e atualizações (Visual Studio 2017) ou Alterar configurações para extensões (Visual Studio 2019).
3. Ajuste as configurações do seu ambiente.

Se você optar por desabilitar atualizações automáticas para extensões, verifique em intervalos apropriados se há atualizações do kit de ferramentas para Visual Studio para o seu ambiente.

Histórico do documento do Guia AWS Toolkit for Visual Studio do usuário

Última atualização de documentação: 21 de abril de 2021

Histórico do documento

A tabela a seguir descreve as importantes mudanças recentes do Guia AWS Toolkit for Visual Studio do usuário. Para receber notificações sobre atualizações dessa documentação, inscreva-se em um feed RSS.

Alteração	Descrição	Data
Atualizações e manutenção de conteúdo	Atualização do conteúdo para alterações na interface do usuário e nas diretrizes de AWS estilo.	6 de março de 2024
Atualizações e manutenção de conteúdo	Atualização do conteúdo para alterações na interface do usuário e nas diretrizes de AWS estilo.	6 de março de 2024
Atualizações e manutenção de conteúdo	Atualização do conteúdo para alterações na interface do usuário e nas diretrizes de AWS estilo.	6 de março de 2024
Atualizações e manutenção de conteúdo	Atualização do conteúdo para alterações na interface do usuário e nas diretrizes de AWS estilo.	6 de março de 2024
Atualizações e manutenção de conteúdo	Atualização do conteúdo para alterações na interface do usuário e nas diretrizes de AWS estilo.	6 de março de 2024

Atualizações para configuração e autenticação	Os tópicos de configuração e autenticação foram atualizados para melhorar a segurança e a experiência de integração do kit de ferramentas. Consulte o sumário dos tópicos Conceitos e Autenticação e acesse para ver as alterações.	22 de junho de 2023
Autenticação e acesso	Fornecer AWS credenciais agora é autenticação e acesso. Refatorando o TOC e os subtópicos para atender aos requisitos AWS de estilo e segurança.	4 de maio de 2023
Novo tópico geral de solução de problemas	O tópico Solução de problemas contém informações gerais de solução de problemas para AWS Toolkit for Visual Studio os serviços associados.	12 de abril de 2023
Atualizações nos tópicos e seções de configuração	Os tópicos e seções de Setting up the AWS Toolkit for Visual Studio deste guia do usuário foram atualizados para melhorar a experiência de integração do AWS Toolkit for Visual Studio.	30 de janeiro de 2023

Atualizações nos tópicos e seções de configuração	Os tópicos e seções de Setting up the AWS Toolkit for Visual Studio deste guia do usuário foram atualizados para melhorar a experiência de integração do AWS Toolkit for Visual Studio.	30 de janeiro de 2023
AWS Toolkit for Visual Studio Informações adicionadas para 2022	Support for Visual Studio 2022 foi adicionado ao AWS Toolkit for Visual Studio.	20 de dezembro de 2022
Atualizações do Publish to AWS guide	Atualizações da documentação para refletir as alterações feitas no serviço para lançamento de disponibilidade geral (GA).	6 de julho de 2022
Atualizações e realocação de títulos	Pequenas alterações no título foram feitas para refletir melhor o conteúdo. O guia agora está localizado no AWS guia Publishing to.	6 de julho de 2022

Implantação em AWS: atualizações de título e conteúdo	A seção do guia, formalmente intitulada: Implantação usando o AWS kit de ferrament as, tem um sumário (TOC) atualizado e agora é intitulad a: Implantação em. AWS Os guias a seguir foram descontin uados e não estão mais acessíveis: Implantação no Elastic Beanstalk (Legacy) e Implantação no (Legacy). AWS CloudFormation O conteúdo atualizado sobre a implantação no Elastic Beanstalk e no Cloudform ation pode ser encontrado no sumário atualizado neste guia.	6 de julho de 2022
Implantar uma aplicação ASP.NET Core 2.0 (Fargate) agora é um guia herdado	Esta documentação refere-se a serviços e recursos herdados. Para obter guias e conteúdos atualizados, consulte o guia AWS .NET Deployment tool e o sumário atualizado de Implantar na AWS.	6 de julho de 2022
Implantar uma aplicação ASP.NET agora é um guia herdado	Esta documentação refere-se a serviços e recursos herdados. Para obter guias e conteúdos atualizados, consulte o guia AWS .NET deployment tool e o sumário atualizado de Implantar na AWS.	6 de julho de 2022

Implantar uma aplicação ASP.NET agora é um guia herdado	Esta documentação refere-se a serviços e recursos herdados. Para obter guias e conteúdos atualizados, consulte o guia AWS .NET deployment tool e o sumário atualizado de Implantar na AWS.	6 de julho de 2022
Novo tópico do guia: Trabalhando com CloudWatch registros no Visual Studio	Foi criado um novo tópico de visão geral para o guia de integração do Amazon CloudWatch Logs no Visual Studio.	29 de junho de 2022
Novo tópico do guia: Configurando a integração de CloudWatch registros para o Visual Studio	Foi criada uma nova seção de configuração para o guia de integração do Amazon CloudWatch Logs no Visual Studio.	29 de junho de 2022
CloudWatch Integração de registros para Visual Studio	Criou um novo guia para a integração do Amazon CloudWatch Logs no Visual Studio, incluindo tópicos do guia: Configurando CloudWatch registros para o Visual Studio e trabalhando com CloudWatch registros no Visual Studio.	29 de junho de 2022
Publicar em AWS	Publicar em não AWS está mais em pré-visualização. Atualizações para refletir as mudanças na interface de usuário e as melhorias nas sugestões de publicação.	1º de junho de 2022

Nova publicação AWS disponível para pré-visualização	Experiência de implantação aprimorada que fornece orientação sobre qual AWS serviço é adequado para seu aplicativo.	21 de outubro de 2021
Suporte de SSO e MFA para credenciais AWS	Atualizado para documentar o novo suporte para AWS Single Sign-On (IAM Identity Center) e autenticação multifator em credenciais. AWS	21 de abril de 2021
AWS Lambda Projeto básico de criação de imagem Docker	Adicionado suporte a imagens de contêiner do Lambda.	1º de dezembro de 2020
Conteúdo de segurança	Conteúdo de segurança adicionado.	6 de fevereiro de 2020
Fornecimento de AWS credenciais	Atualizado com informações sobre como criar perfis de credenciais no arquivo compartilhado de credenciais da AWS .	20 de junho de 2019
Usando o Projeto AWS Lambda no AWS Toolkit for Visual Studio	O suporte para o Visual Studio 2019 foi adicionado ao AWS Toolkit for Visual Studio.	28 de março de 2019
Tutorial: Creating an Amazon Rekognition Lambda Application	O suporte para o Visual Studio 2019 foi adicionado ao AWS Toolkit for Visual Studio.	28 de março de 2019
Tutorial: Crie e teste um aplicativo sem servidor com o Lambda AWS	O suporte para o Visual Studio 2019 foi adicionado ao AWS Toolkit for Visual Studio.	28 de março de 2019

Configurando o AWS Toolkit for Visual Studio	Support for Visual Studio 2019 foi adicionado ao AWS Toolkit for Visual Studio.	28 de março de 2019
Implantar uma aplicação ASP.NET Core 2.0 (Fargate)	O suporte para o Visual Studio 2019 foi adicionado ao AWS Toolkit for Visual Studio.	28 de março de 2019
Implantar uma aplicação ASP.NET Core 2.0 (EC2)	O suporte para o Visual Studio 2019 foi adicionado ao AWS Toolkit for Visual Studio.	28 de março de 2019
Criando um projeto AWS CloudFormation modelo no Visual Studio	O suporte para o Visual Studio 2019 foi adicionado ao AWS Toolkit for Visual Studio.	28 de março de 2019
Visualizações detalhadas do Container Service	Foram adicionadas informaçõ es sobre as visualizações detalhadas dos clusters e repositórios de contêineres do Amazon Elastic Container Service que são fornecidos pelo AWS Explorer.	16 de fevereiro de 2018
Implantar no Amazon EC2 Container Service	Foram adicionadas informaçõ es sobre a implantação no Amazon EC2 Container Service.	16 de fevereiro de 2018
Implantar o Container Service usando o Fargate	Adicionadas informações sobre como implantar um aplicativo do ASP.NET Core 2.0 em contêiner destinado ao Linux por meio do Amazon ECS usando o tipo de execução Fargate.	16 de fevereiro de 2018

Implantar o Container Service usando o EC2	Adicionadas informações sobre como implantar um aplicativo do ASP.NET Core 2.0 em contêiner direciona do ao Linux por meio do Amazon ECS usando o tipo de execução do EC2.	16 de fevereiro de 2018
Credenciais para implantaç ão no Amazon EC2 Container Service	Adicionadas informações sobre como especificar credenciais ao implantar no Amazon EC2 Container Service.	16 de fevereiro de 2018

As traduções são geradas por tradução automática. Em caso de conflito entre o conteúdo da tradução e da versão original em inglês, a versão em inglês prevalecerá.