

Manual do usuário

AWS Kit de ferramentas com Amazon Q



AWS Kit de ferramentas com Amazon Q: Manual do usuário

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

As marcas comerciais e imagens comerciais da Amazon não podem ser usadas no contexto de nenhum produto ou serviço que não seja da Amazon, nem de qualquer maneira que possa gerar confusão entre os clientes ou que deprecie ou desprestige a Amazon. Todas as outras marcas comerciais que não pertencem à Amazon pertencem a seus respectivos proprietários, que podem ou não ser afiliados, patrocinados pela Amazon ou ter conexão com ela.

Table of Contents

AWS Kit de ferramentas com Amazon Q	1
O que é o AWS Toolkit for Visual Studio com o Amazon Q	1
AWS Explorador	1
Amazon Q	1
Informações relacionadas	2
Amazon Q	3
O que é o Amazon Q?	3
Baixar o kit de ferramentas	4
Baixar o kit de ferramentas usando o Visual Studio Marketplace	4
Kits de ferramentas de IDE adicionais da AWS	4
Conceitos básicos	5
Instalar e configurar	5
Pré-requisitos	5
Instalando o AWS kit de ferramentas	6
Desinstalando o kit de ferramentas AWS	7
Conectando-se a AWS	9
Pré-requisitos	9
Conectando-se a AWS partir do kit de ferramentas	9
Amazon Q Developer	10
AWS Kit de ferramentas	1
Documentação e tutoriais	14
Solucionar problemas de instalação	14
Permissões de administrador do Visual Studio	15
Obter um log de instalação	15
Instalar diferentes extensões do Visual Studio	17
Entrar em contato com o suporte	17
Perfis e vinculação de janelas	17
Perfis e vinculação de janelas para o kit de ferramentas para Visual Studio	17
Autenticação e acesso	19
Centro de Identidade do IAM	19
Autenticação com o IAM Identity Center a partir do AWS Toolkit for Visual Studio	20
Credenciais do IAM	21
Criar um usuário do IAM.	22
Criar um arquivo de credenciais	22

Editar credenciais de usuário do IAM pelo kit de ferramentas	23
Editar credenciais de usuário do IAM usando um editor de texto	24
Criação de usuários do IAM a partir do AWS Command Line Interface (AWS CLI)	24
AWS ID do construtor	25
Autenticação multifatorial (MFA)	25
Etapa 1: criar um perfil do IAM para delegar acesso aos usuários do IAM	25
Etapa 2: criar um usuário do IAM que assume as permissões do perfil	26
Etapa 3: adicionar uma política para permitir que o usuário do IAM assuma o perfil	27
Etapa 4: gerenciar um dispositivo MFA virtual para o usuário do IAM	28
Etapa 5: criar perfis para permitir a MFA	28
Credenciais externas	29
Atualização de firewalls e gateways	30
AWS Toolkit for Visual Studio Endpoints	30
Endpoints do plug-in do Amazon Q	30
Endpoints do Amazon Q Developer	31
Endpoints do Amazon Q Code Transform	31
Endpoints de autenticação	31
Endpoints de identidade	32
Telemetria	32
Referências	33
Trabalhar com os serviços da AWS	34
Amazon CodeCatalyst	34
O que é a Amazon CodeCatalyst?	34
Começando com CodeCatalyst	35
Trabalhando com CodeCatalyst	36
Solução de problemas	38
Integração do CloudWatch Logs	39
Configurar o CloudWatch Logs	39
Trabalhando com CloudWatch registros	39
Gerenciar instâncias do Amazon EC2	46
As visualizações de imagens de máquina da Amazon e de instâncias do Amazon EC2	46
Executar uma instância do Amazon EC2	49
Conectar a uma instância do Amazon EC2	52
Encerrar uma instância do Amazon EC2	55
Gerenciar instâncias do Amazon ECS	59
Modificar propriedades do serviço	59

Interrupção de uma tarefa	59
Excluir um serviço	60
Excluir um cluster	60
Criar um repositório	60
Excluir um repositório	61
Gerenciar grupos de segurança no AWS Explorer	61
Criar um grupo de segurança	61
Adicionar permissões a security groups	62
Criar uma AMI com base em uma instância do Amazon EC2	64
Definir permissões de execução em uma imagem de máquina da Amazon	64
Amazon Virtual Private Cloud (VPC)	66
Criação de uma VPC público-privada para implantação com AWS Elastic Beanstalk	66
Usar o Editor de modelos do CloudFormation para Visual Studio	71
Criando um projeto CloudFormation modelo no Visual Studio	72
Implantar um modelo do CloudFormation no Visual Studio	74
Formatar um modelo do CloudFormation no Visual Studio	77
Usando o Amazon S3 a partir do Explorer AWS	78
Criando um Bucket do Amazon S3	79
Gerenciando buckets do Amazon S3 a partir do Explorer AWS	79
Carregar arquivos e pastas no Amazon S3	81
Operações de arquivos do Amazon S3 a partir do AWS Toolkit for Visual Studio	83
AWSUsar o DynamoDB no Explorer	87
Criar uma tabela do DynamoDB	88
Visualizar uma tabela do DynamoDB como uma grade	90
Editar e adicionar atributos e valores	90
Realizar verificações em uma tabela do DynamoDB	92
Usar o AWS CodeCommit com o Visual Studio Team Explorer	94
Tipos de credencial do AWS CodeCommit	94
Como se conectar à AWS CodeCommit	95
Criação de um repositório	96
Configurar credenciais do Git	97
Clonar um repositório	100
Trabalho com repositórios	101
Usar o CodeArtifact no Visual Studio	101
Adicione seu repositório do CodeArtifact como uma fonte de pacotes no Visual Studio.	102
Amazon RDS no AWS Explorer	102

Executar uma instância do banco de dados do Amazon RDS	103
Criar um banco de dados do Microsoft SQL Server em uma instância do RDS	111
Grupos de segurança do Amazon RDS	113
Usar o Amazon SimpleDB no AWS Explorer	117
Usar o Amazon SQS no AWS Explorer	119
Criação de uma fila	119
Exclusão de uma fila	120
Gerenciar propriedades da fila	120
Enviar uma mensagem para uma fila	121
Gerenciamento de Identidade e Acesso	122
Criar e configurar um usuário do IAM	123
Criar um grupo do IAM	124
Adicionar um usuário do IAM a um grupo do IAM	125
Gerar credenciais para um usuário do IAM	127
Criar um perfil do IAM	129
Criar uma política do IAM	130
AWS Lambda	133
AWS Lambda Projeto básico	133
AWS Lambda Projeto básico de criação de imagem Docker	140
Tutorial: Crie e teste um aplicativo sem servidor com AWS Lambda	148
Tutorial: Creating an Amazon Rekognition Lambda Application	155
Tutorial: Usando o Amazon Logging Frameworks AWS Lambda para criar registros de aplicativos	163
Implantar no AWS	166
Publicar no AWS	166
Pré-requisitos	167
Tipos de aplicação compatíveis	168
Publicar aplicações em destinos da AWS	168
AWS Lambda	170
Pré-requisitos	171
Tópicos relacionados	171
Listar os comandos do Lambda disponibilizados por meio da CLI do .NET Core	171
Publicar um projeto do Lambda do .NET Core na CLI do .NET Core	172
Implantando em AWS Elastic Beanstalk	174
Implantar um aplicativo do ASP.NET (tradicional)	175
Implantar uma aplicação ASP.NET (.NET Core) (herdado)	187

Especificar AWS credenciais	189
Republicar no Elastic Beanstalk (herdado)	190
Implantações personalizadas (tradicionais)	192
Implantações personalizadas (.NET Core)	194
Suporte a vários aplicativos	198
Implantar no Amazon EC2 Container Service	201
Especificar AWS credenciais	202
Implantar uma aplicação ASP.NET Core 2.0 (Fargate) (herdado)	204
Implantar uma aplicação ASP.NET Core 2.0 (EC2)	211
Solução de problemas	216
Práticas recomendadas de solução de problemas	216
Visualizar e filtrar as verificações de segurança do Amazon Q	217
O AWS kit de ferramentas não está instalado corretamente	218
Configurações de firewall e proxy	219
Solucionar problemas nas configurações de firewall e proxy	219
Certificados personalizados	219
Permitir listagem e etapas adicionais	220
Segurança	222
Proteção de dados	222
Gerenciamento de Identidade e Acesso	224
Público	224
Autenticação com identidades	225
Gerenciar o acesso usando políticas	226
Como Serviços da AWS trabalhar com o IAM	228
Solução de problemas AWS de identidade e acesso	228
Validação de conformidade	230
Resiliência	231
Segurança da infraestrutura	231
Análise de configuração e vulnerabilidade	232
Histórico do documento	233
Histórico do documentos	233
.....	ccxlii

AWS Kit de ferramentas com Amazon Q

Este é o guia do usuário do kit de ferramentas da AWS para Visual Studio com Amazon Q. Se você estiver procurando o kit de ferramentas da AWS para VS Code, consulte o [Guia do usuário do AWS Toolkit for Visual Studio Code](#).

O que é o AWS Toolkit for Visual Studio com o Amazon Q

O AWS Toolkit for Visual Studio com Amazon Q é uma extensão do Visual Studio IDE que facilita o desenvolvimento, a depuração e a implantação de aplicativos.NET que usam o Amazon Web Services. O AWS Toolkit com Amazon Q é compatível com as versões 2022 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 kit de ferramentas para Visual Studio também foi lançado para o Visual Studio 2008, 2010, 2012, 2013, 2015, 2017 e 2019. Mas não há mais suporte para essas versões. Para obter mais informações, consulte o tópico [Instalação e configuração](#) neste Guia do usuário.

O AWS kit de ferramentas com o Amazon Q contém os seguintes recursos para aprimorar sua experiência de desenvolvimento.

AWS Explorador

A janela da ferramenta AWS Explorer pode ser acessada no menu Exibir do IDE e permite que você interaja com AWS os serviços no Visual Studio. Para obter uma lista dos AWS serviços e recursos compatíveis, consulte o tópico [Trabalhando com AWS serviços](#) neste Guia do usuário.

Amazon Q

Converse com o Amazon Q Developer no Visual Studio para fazer perguntas sobre a criação AWS e obter ajuda com o desenvolvimento de software. O Amazon Q pode explicar conceitos de codificação e trechos de código, gerar testes de código e de unidade e aprimorar o código por meio de depuração ou refatoração.

Para instalar e configurar o Amazon Q para o kit de ferramentas para Visual Studio, consulte o tópico [Conceitos básicos](#) neste Guia do usuário. Para saber mais sobre como trabalhar com o Amazon Q Developer, consulte o IDEs tópico do [Amazon Q Developer no Amazon Q Developer User Guide](#). Para obter informações detalhadas sobre planos e preços do Amazon Q, consulte o guia [Preços do Amazon Q](#).

Informações relacionadas

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

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

Amazon Q

O que é o Amazon Q?

Desde 30 de abril de 2024, o Amazon CodeWhisperer faz parte do Amazon Q Developer, incluindo sugestões de código em linha 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 Guia do usuário do Amazon Q Developer. 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 kit de ferramentas para Visual Studio, a AWS também oferece kits de ferramentas de 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 [baixar o AWS Toolkit for JetBrains](#) no 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](#)
- [Conectando-se a AWS](#)
- [Solucionar problemas de instalação do AWS Toolkit for Visual Studio](#)
- [Perfis e vinculação de janelas](#)

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](#)
- [Instalando o AWS Toolkit for Visual Studio](#)
- [Desinstalando o AWS Toolkit for Visual Studio](#)

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 Studio](#) destino.

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

As seções a seguir descrevem como começar a usar o AWS Toolkit for Visual Studio com o Amazon Q. Na primeira vez que você inicia o Visual Studio depois de instalar a extensão, uma Introdução é exibida na janela do editor. Você pode concluir as seguintes ações na guia Conceitos básicos.

- Ative ou desative o Amazon Q e o AWS Toolkit.
- Adicionar e se autenticar com novas credenciais.
- Autenticar-se com as credenciais existentes.
- Acessar a documentação e os tutoriais para ajudar você a começar a usar o Amazon Q e o kit de ferramentas da AWS .

Pré-requisitos

Para começar a trabalhar com o Amazon Q e o AWS Toolkit, você precisa se autenticar com AWS credenciais. Se você já configurou uma AWS conta e autenticação por meio de outra AWS ferramenta ou serviço (como o AWS Command Line Interface), o AWS Toolkit detecta automaticamente suas credenciais. Se você é novo AWS ou não criou uma conta, então você pode se inscrever para uma AWS 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.

Conectando-se a AWS partir do kit de ferramentas

Para se conectar às suas AWS contas a partir do AWS Kit de ferramentas, abra a guia Introdução a qualquer momento preenchendo o seguinte.

Abrir a guia Conceitos básicos no Visual Studio

1. No Visual Studio, expanda Extensões no menu principal e, em seguida, expanda o submenu AWS Toolkit.
2. Escolha Conceitos básicos.
3. A guia Introdução é aberta na janela do editor do Visual Studio.

Na guia Conceitos básicos, há duas seções principais:

- Funcionalidades: Nesta seção, você pode ativar ou desativar recursos como o Amazon Q e o AWS Toolkit.
- Documentação e tutoriais: uma coleção de referências sobre os recursos habilitados.

Note

A seção Documentação e tutoriais fica visível somente quando um ou mais recursos estão habilitados.

Amazon Q Developer

Na seção Amazon Q da guia Conceitos básicos, você pode habilitar ou desabilitar o Amazon Q, adicionar uma nova conexão ou mudar para outra conexão da AWS . Antes que você possa visualizar ou acessar qualquer uma dessas ações, o Amazon Q deve ser habilitado. Para habilitar o Amazon Q, clique no botão Habilitar.

Quando o Amazon Q é desabilitado, todos os recursos e funções do Amazon Q são completamente removidos do Visual Studio. A habilitação do Amazon Q abre automaticamente a tela Configurar autenticação para o Amazon Q na guia Conceitos básicos. Para continuar, você deve se autenticar com suas Centro de Identidade do AWS IAM credenciais para acessar o Nível Profissional ou seu ID do AWS Construtor para acessar o Nível Gratuito. Para saber mais detalhes sobre cada uma das opções de nível, consulte o tópico [Noções básicas dos níveis de serviço do Amazon Q Developer](#) no Guia do usuário do Amazon Q Developer.

Para continuar, execute um dos procedimentos a seguir.

Autenticação no nível profissional com o Centro de Identidade do IAM

Note

Os campos Nome do perfil, URL inicial, Região do perfil ou Região do SSO necessários para autenticação no nível profissional geralmente são informados por um administrador da sua empresa ou organização. Para obter informações detalhadas sobre as credenciais do Centro de Identidade do IAM, consulte o tópico [O que é o Centro de Identidade do IAM?](#) no Guia do usuário do Centro de Identidade do AWS IAM.

1. Na tela Getting Started: AWS Toolkit with Amazon Q, escolha o botão Sign in no quadro Amazon Q para navegar até a tela Configurar autenticação para Amazon Q.
2. Na tela Configurar autenticação para o Amazon Q, acesse a seção Nível profissional, preencha os campos obrigatórios e clique no botão Conectar.
3. Confirme que você deseja abrir o portal AWS de solicitação de autorização em seu navegador padrão.
4. Conclua as etapas exigidas pelo portal de solicitação de AWS autorização, você será notificado quando for seguro fechar o navegador e retornar ao Visual Studio
5. Na guia Conceitos básicos, o Amazon Q é atualizado para mostrar que você se conectou com o Centro de Identidade do IAM quando o processo é concluído.

Autenticação de nível gratuito com AWS Builder ID

Note

Para obter detalhes adicionais sobre o AWS Builder ID, consulte o tópico [Entrar com o AWS Builder ID](#) no Guia do usuário AWS de login.

1. Na tela Getting Started: AWS Toolkit with Amazon Q, escolha o botão Sign in no quadro Amazon Q para navegar até a tela Configurar autenticação para Amazon Q.
2. Na tela Configurar autenticação para o Amazon Q, acesse a seção Nível gratuito e clique no botão Inscrever-se ou iniciar sessão.
3. Confirme que você deseja abrir o portal AWS de solicitação de autorização em seu navegador padrão.

4. Conclua as etapas exigidas pelo portal de solicitação de AWS autorização, você será notificado quando for seguro fechar o navegador e retornar ao Visual Studio.
5. Na guia Getting Started, o Amazon Q é atualizado para mostrar que você está conectado ao seu AWS Builder ID quando o processo é concluído.

Depois de se autenticar com suas credenciais do IAM Identity Center ou AWS Builder ID, você pode acessar o Amazon Q no Visual Studio. Além disso, você pode realizar as seguintes ações na guia Conceitos básicos:

- Sair: encerra sua conexão de credenciais atual de todas as funções do Amazon Q. O Amazon Q continua habilitado, mas a maioria dos recursos não funciona.
- Desabilitar o Amazon Q: desabilita completamente todos os recursos do Amazon Q no Visual Studio.

AWS Kit de ferramentas

Na seção AWS Kit de ferramentas na guia Introdução ao AWS kit de ferramentas, você pode ativar ou desativar o AWS kit de ferramentas, adicionar uma nova conexão ou alternar para uma conexão diferente. AWS Antes que você possa visualizar ou acessar qualquer uma dessas ações, o AWS Toolkit deve estar ativado. Para ativar o AWS kit de ferramentas, clique no botão Ativar.

Quando o AWS kit de ferramentas está ativado, a autenticação de configuração do AWS kit de ferramentas é carregada automaticamente na guia Introdução ao kit de AWS ferramentas. Para continuar, você deve se autenticar usando as credenciais do Centro de Identidade do AWS IAM ou as credenciais do Perfil de usuário do IAM.

Note

Para obter informações detalhadas sobre as credenciais do Centro de Identidade do IAM, consulte o tópico [O que é o Centro de Identidade do IAM?](#) no Guia do usuário do Centro de Identidade do AWS IAM. Para obter informações detalhadas sobre as credenciais da função de usuário do IAM, consulte o tópico [Chaves de AWS acesso: credenciais de longo prazo](#) no guia de referência de ferramentas AWS SDKs e ferramentas.

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

1. Na tela Getting Started: AWS Toolkit with Amazon Q, escolha o botão Sign in no quadro AWS Toolkit para navegar até a tela Configurar autenticação para o AWS Toolkit.
2. Na tela Configurar autenticação para o AWS kit de ferramentas, escolha IAM Identity Center (sucessor do Single Sign-on) no menu suspenso Tipo de perfil.
3. No menu suspenso Escolher um perfil existente ou adicionar novo, escolha um perfil existente ou selecione Adicionar novo perfil para adicionar as informações do novo perfil.

Note

Se escolher um perfil existente, vá para a etapa 7.

4. No campo Nome do perfil, insira o **profile name** associado à conta do Centro de Identidade do IAM com a qual você deseja se autenticar.
5. No campo de texto URL inicial, insira o **Start URL** que está anexado às suas credenciais do Centro de Identidade IAM.
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 (padrão: us-east-1), escolha a Região do SSO definida pelas suas credenciais do Centro de Identidade do IAM.
8. Clique no botão Conectar para abrir o site de Solicitação de autorização da AWS em seu navegador da web padrão.
9. Siga as instruções no navegador da web padrão. Você receberá a notificação de que é seguro fechar o navegador e retornar ao Visual Studio quando o processo for concluído.
10. Na guia Conceitos básicos, a seção Kit de ferramentas da AWS é atualizada para mostrar que você se conectou com o Centro de Identidade do IAM quando o processo é concluído.

Autenticar-se e conectar-se com credenciais do perfil de usuário do IAM

1. Na tela Getting Started: AWS Toolkit with Amazon Q, escolha o botão Sign in no quadro AWS Toolkit para navegar até a tela Configurar autenticação para o AWS Toolkit.
2. Na tela Configurar autenticação para o AWS kit de ferramentas, escolha Função de usuário do IAM no menu suspenso Tipo de perfil.
3. No menu suspenso Escolher um perfil existente ou adicionar novo, escolha **Add new profile**.

Note

Se escolher um nome de perfil existente na lista, vá para a Etapa 8.

4. No campo de texto Nome do perfil, insira um nome para o novo perfil.
5. No campo de texto ID da chave de acesso, insira o **Access Key ID** do perfil com o qual deseja se autenticar.
6. No campo de texto Chave secreta, insira o **Secret Key** do perfil com o qual deseja se autenticar.
7. No menu suspenso Local de armazenamento (padrão: arquivo de credenciais compartilhadas), especifique se deseja armazenar as credenciais em um arquivo de Credenciais compartilhadas ou no Armazenamento criptografado .NET.
8. Nos menus suspensos Região do perfil (padrão: us-east-1), escolha a Partição e a Região do perfil que estão anexadas ao perfil com o qual deseja se autenticar.
9. Escolha o botão Conectar para adicionar esse perfil ao seu local de AWS armazenamento com AWS o qual and/or se autenticar.
10. Na guia Conceitos básicos, a seção Kit de ferramentas da AWS é atualizada para mostrar que você se conectou com suas credenciais do perfil de usuário do IAM quando o processo é concluído.

Depois de se autenticar com suas credenciais do IAM Identity Center ou do IAM User Role, você pode acessar o AWS Explorer no Toolkit for Visual Studio. Além disso, você pode Sair e Desabilitar o kit de ferramentas da AWS para Visual Studio com Amazon Q na guia Conceitos básicos.

Documentação e tutoriais

A seção de documentação e tutoriais é atualizada automaticamente com sugestões de documentação e tutoriais com base em suas preferências AWS de serviços e recursos. Essas referências são visíveis somente quando pelo menos um recurso foi habilitado.

Solucionar problemas de instalação do AWS Toolkit for Visual Studio

Sabemos que as informações a seguir podem resolver problemas comuns de instalação durante a configuração do AWS Toolkit for Visual Studio.

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

Permissões de administrador do Visual Studio

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

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

Para iniciar localmente o Visual Studio com permissões de administrador:

1. No Windows, localize o inicializador de aplicações do Visual Studio (ícone).
2. Abra o menu de contexto (clique com o botão direito) do ícone do Visual Studio e abra o menu de contexto.
3. Escolha Executar como administrador no menu de contexto.

Para iniciar remotamente o Visual Studio com permissões de administrador:

1. No Windows, localize o inicializador de aplicações que você está usando para se conectar à instância remota do Visual Studio.
2. Abra o menu de contexto (clique com o botão direito) do ícone do Visual Studio e abra o menu de contexto.
3. Escolha 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.

Obter um log de instalação

Se você concluiu as etapas na seção Permissões de 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 AWS Toolkit for Visual Studio por meio de um arquivo `.vsix` e gerar um arquivo de log de instalação, conclua as etapas a seguir.

1. Na página inicial do [AWS Toolkit for Visual Studio](#), siga o link Baixar e salve o arquivo `.vsix` da versão do AWS Toolkit for Visual Studio que você deseja instalar.
2. No menu principal do Visual Studio, expanda o cabeçalho Ferramentas e o submenu Linha de comando e escolha Prompt de comando de desenvolvedor do Visual Studio.
3. No Prompt de comando de desenvolvedor do Visual Studio, digite o comando `vsixinstaller` com o seguinte formato:

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

4. Substitua `[file path to log file]` pelo nome do arquivo e pelo caminho completo do diretório no qual você deseja que o log de instalação seja criado. Um exemplo do comando `vsixinstaller` 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. Substitua `[file path to Toolkit installation file]` pelo caminho completo do arquivo do diretório em que o `AWSToolkitPackage.vsix` está localizado.

Um exemplo do comando `vsixinstaller` com o caminho completo do arquivo de instalação do kit de ferramentas 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 comando `vsixinstaller`.

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

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

Instalar 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 apresentando falha, verifique se consegue instalar outras extensões do Visual Studio. A instalação de diferentes extensões do Visual Studio pode fornecer informações adicionais sobre problemas de instalação. Caso você não consiga instalar nenhuma extensão do Visual Studio, talvez seja necessário solucionar problemas do Visual Studio, e não do AWS 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 os problemas anteriores ou abrir um novo problema no menu [Issues do Github da AWS Toolkit for Visual Studio](#).

Para ajudar a agilizar uma solução para seu problema:

- Verifique os problemas anteriores e atuais para ver se outras pessoas se depararam com uma situação semelhante.
- Faça anotações detalhadas de cada etapa que você executou para resolver o problema.
- Salve todos os arquivos de log que você obteve da instalação do AWS Toolkit for Visual Studio ou de outras extensões.
- Anexe os arquivos de log de instalação do AWS Toolkit for Visual Studio ao novo problema.

Perfis e vinculação de janelas

Perfis e vinculação de janelas para o kit de ferramentas para Visual Studio

Ao trabalhar com ferramentas de publicação, assistentes e outros recursos do kit de ferramentas para Visual Studio, observe o seguinte:

- A janela AWS Explorer é vinculada a um único perfil e região por vez. As janelas abertas no AWS Explorer assumem esse perfil e região vinculados por padrão.
- Depois que uma nova janela for aberta, você poderá usar essa instância do AWS Explorer para alternar para um perfil ou região diferente.
- Os recursos e ferramentas de publicação do kit de ferramentas para Visual Studio assumem automaticamente como padrão o perfil e a região definidos no AWS Explorer.

- Se um novo perfil ou região for especificado em um assistente, recurso ou ferramenta de publicação: todos os recursos criados posteriormente vão 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 diferente.
- O AWS Explorer salva o perfil e região que foram especificados pela última vez, e os valores da última instância do Visual Studio fechada serão mantidos.

Autenticação e acesso

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

1. Ou AWS Identity and Access Management (IAM) ou Centro de Identidade do AWS IAM autenticação 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 Credenciais do IAM](#)
- [AWS ID do construtor](#)
- [Autenticação multifator \(MFA\) no kit de ferramentas para Visual Studio](#)
- [Configurar credenciais externas](#)
- [Atualizar firewalls e gateways para permitir o acesso](#)

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

Centro de Identidade do AWS IAM 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 AWS](#) SDKs e o Guia de referência de 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 `<home-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 CLI), o AWS Toolkit for Visual Studio detectará automaticamente essas credenciais.
- AWS recomenda o uso da Centro de Identidade do AWS IAM 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 Centro de Identidade do AWS IAM. Para obter mais informações, consulte [O que é o IAM Identity Center?](#) no Guia do usuário do Centro de Identidade do AWS IAM .

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 ferramentas 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

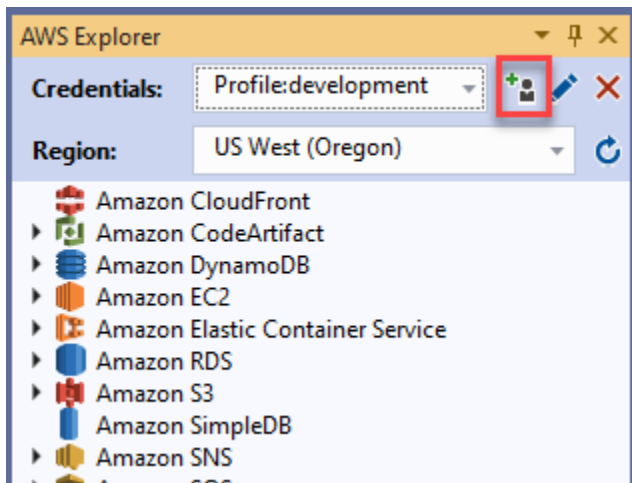
Para adicionar um usuário ou criar um `credentials file` pelo AWS Toolkit for Visual Studio:

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 compartilhados de configuração e credenciais](#) do AWS SDKs guia de referência de ferramentas.

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 `nocredentials` 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 em <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. Escolha 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 perfil.
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 em <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 **AssumeRole** caixa 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 .

Atualizar firewalls e gateways para permitir o acesso

Se você filtrar o acesso a AWS domínios ou endpoints de URL específicos usando uma solução de filtragem de conteúdo da web, os seguintes endpoints devem ser listados como permissão para acessar todos os serviços e recursos disponíveis por meio do e do AWS Toolkit for Visual Studio Amazon Q. Para obter etapas detalhadas sobre como solucionar problemas nas configurações de firewall e proxy do Toolkit AWS com o Amazon Q, consulte a seção [Configurações de firewall e proxy](#) no tópico Solução de problemas deste Guia do usuário. Para obter informações detalhadas sobre como configurar um proxy corporativo para o Amazon Q, consulte o tópico [Configurar um proxy corporativo no Amazon Q](#) no Guia do usuário do Amazon Q Developer.

AWS Toolkit for Visual Studio Endpoints

A seguir estão listas de endpoints e referências AWS Toolkit for Visual Studio específicos que precisam ser listados com permissão.

Endpoints

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

Endpoints do plug-in do Amazon Q

A seguir está uma lista de endpoints e referências específicos do plug-in Amazon Q que precisam ser listados com permissão.

```
https://idetoolkits-hostedfiles.amazonaws.com/* (Plugin for configs)
https://idetoolkits.amazonwebservices.com/* (Plugin for endpoints)
```

```
https://aws-toolkit-language-servers.amazonaws.com/* (Language Server Process)
https://client-telemetry.us-east-1.amazonaws.com/ (Telemetry)
https://cognito-identity.us-east-1.amazonaws.com (Telemetry)
https://aws-language-servers.us-east-1.amazonaws.com (Language Server Process)
```

Endpoints do Amazon Q Developer

A seguir está uma lista de endpoints e referências específicos do Amazon Q Developer que precisam ser listados com permissão.

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

Endpoints do Amazon Q Code Transform

A seguir está uma lista de endpoints e referências específicos do Amazon Q Code Transform que precisam ser listados com permissão.

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

Endpoints de autenticação

A seguir está uma lista de endpoints e referências de autenticação que precisam ser listados como permitidos.

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

```
*.awsstatic.com
*.console.aws.a2z.com
*.sso.amazonaws.com
```

Endpoints de identidade

As listas a seguir contêm endpoints específicos da identidade, como Centro de Identidade do AWS IAM o AWS Builder ID.

Centro de Identidade do AWS IAM

Para obter detalhes sobre os endpoints necessários para o IAM Identity Center, consulte o tópico [Habilitar o IAM Identity Center](#) no Guia do usuário Centro de Identidade do AWS IAM.

IAM Identity Center do Enterprise

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

AWS ID do construtor

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

Telemetria

Veja a seguir um endpoint específico para telemetria que precisa ser incluído na lista de permissões.

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

Referências

A seguir está uma lista de referências de endpoints.

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

Trabalhar com os serviços da AWS

Os tópicos a seguir descrevem como começar a usar os serviços da AWS por meio do kit de ferramentas da AWS para Visual Studio com Amazon Q.

Tópicos

- [Amazon CodeCatalyst para o AWS kit de ferramentas para Visual Studio com o Amazon Q](#)
- [Integração do Amazon CloudWatch Logs para o Visual Studio](#)
- [Gerenciar instâncias do Amazon EC2](#)
- [Gerenciar instâncias do Amazon ECS](#)
- [Gerenciar grupos de segurança no AWS Explorer](#)
- [Criar uma AMI com base em uma instância do Amazon EC2](#)
- [Definir permissões de execução em uma imagem de máquina da Amazon](#)
- [Amazon Virtual Private Cloud \(VPC\)](#)
- [Usar o Editor de modelos do CloudFormation para Visual Studio](#)
- [Usando o Amazon S3 a partir do Explorer AWS](#)
- [AWS Usar o DynamoDB no Explorer](#)
- [Usar o AWS CodeCommit com o Visual Studio Team Explorer](#)
- [Usar o CodeArtifact no Visual Studio](#)
- [Amazon RDS no AWS Explorer](#)
- [Usar o Amazon SimpleDB no AWS Explorer](#)
- [Usar o Amazon SQS no AWS Explorer](#)
- [Gerenciamento de Identidade e Acesso](#)
- [AWS Lambda](#)

Amazon CodeCatalyst para o AWS kit de ferramentas para Visual Studio com o Amazon Q

O que é a 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 com o Amazon Q, você pode

visualizar e CodeCatalyst gerenciar recursos diretamente AWS do Toolkit for Visual Studio com o Amazon Q. Para CodeCatalyst obter mais informações, consulte [o Guia do Usuário da CodeCatalyst Amazon](#).

Os tópicos a seguir descrevem como conectar o AWS Toolkit for Visual Studio com o Amazon Q e como trabalhar CodeCatalyst CodeCatalyst com AWS o Toolkit for Visual Studio com o Amazon Q.

Tópicos

- [Introdução à Amazon CodeCatalyst e ao AWS Toolkit for Visual Studio com o Amazon Q](#)
- [Trabalhando com CodeCatalyst recursos da Amazon a partir do AWS Toolkit for Visual Studio com o Amazon Q](#)
- [Solução de problemas](#)

Introdução à Amazon CodeCatalyst e ao AWS Toolkit for Visual Studio com o Amazon Q

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

Tópicos

- [Instalando o AWS Toolkit for Visual Studio com o Amazon Q](#)
- [Criação de uma CodeCatalyst conta e ID do AWS construtor](#)
- [Conectando o AWS Toolkit for Visual Studio com o Amazon Q com CodeCatalyst](#)

Instalando o AWS Toolkit for Visual Studio com o Amazon Q

Antes de integrar o AWS Toolkit for Visual Studio com o Amazon Q com CodeCatalyst suas contas, certifique-se de usar uma versão atual do Toolkit for Visual Studio com o Amazon Q. Para obter detalhes sobre como instalar e configurar a AWS versão mais recente AWS do Toolkit for Visual Studio com o Amazon Q, consulte a seção Configurando o Kit de Ferramentas para Visual Studio com o Amazon Q, consulte a seção [Configurando AWS o Toolkit para Visual Studio](#) com o Amazon Q deste Guia do usuário.

Criação de uma CodeCatalyst conta e ID do AWS construtor

Além de instalar a versão mais recente do AWS Toolkit for Visual Studio AWS com o Amazon Q, você deve ter uma ID CodeCatalyst e uma conta do Builder AWS ativas para se conectar ao Toolkit

for Visual Studio com o Amazon Q. Se você não tiver AWS uma CodeCatalyst ID ou conta ativa do Builder, [consulte a seção CodeCatalyst CodeCatalystConfiguração](#) com no Guia do usuário.

Note

Uma ID de AWS construtor é diferente das suas AWS credenciais. Para obter instruções sobre como se inscrever e se autenticar com um AWS Builder ID, consulte o tópico [Autenticação e acesso: AWS Builder ID](#) neste Guia do usuário.

Para obter informações detalhadas sobre o AWS Builder IDs, consulte o tópico [AWS Builder ID](#) no Guia do usuário de referência AWS geral.

Conectando o AWS Toolkit for Visual Studio com o Amazon Q com CodeCatalyst

Para conectar o AWS Toolkit for Visual Studio ao Amazon Q com CodeCatalyst sua 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 AWS Builder ID para abrir o CodeCatalyst console em seu navegador preferido.
4. No seu navegador, insira seu ID do AWS construtor 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 com o Amazon Q e CodeCatalyst sua conta. Quando o processo de conexão estiver concluído, CodeCatalyst será exibida uma confirmação indicando que é seguro fechar o navegador.

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

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 com o Amazon Q.

Tópicos

- [Clonar um repositório](#)

Clonar um repositório

CodeCatalyst é 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 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: AWS Builder ID](#) 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 deseja clonar.
5. Na seção Caminho, escolha a pasta na qual você deseja clonar o repositório.

Note

Inicialmente, essa pasta deve estar vazia para ser clonada com sucesso.

6. Selecione Clonar para começar a clonar o repositório.
7. Depois que o repositório for clonado, o Visual Studio carregará a 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 em Configurações globais do Git do menu Controle de 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 com o Amazon Q.

Tópicos

- [Credenciais](#)

Credenciais

Se você encontrar uma caixa de diálogo solicitando credenciais ao tentar clonar um repositório baseado em git CodeCatalyst, seu auxiliar de AWS CodeCommit credenciais pode estar configurado globalmente, causando interferência no. CodeCatalyst Para obter informações adicionais sobre o auxiliar de AWS CodeCommit credenciais, consulte a seção [Configurar etapas para conexões HTTPS com AWS CodeCommit repositórios no Windows com o auxiliar de credenciais AWS CLI](#) do Guia do Usuário. AWS CodeCommit

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

1. Abra o arquivo de configuração global do git em: %userprofile%\gitconfig.
2. Localize a seguinte seção no arquivo:

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

3. Altere a seção para o seguinte:

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

4. Salve as alterações e conclua as etapas para clonar o repositório.

Integração do Amazon CloudWatch Logs para o Visual Studio

A integração do Amazon CloudWatch Logs com o kit de ferramentas da AWS para Visual Studio com Amazon Q possibilita monitorar, armazenar e acessar os recursos do CloudWatch Logs, sem precisar sair do IDE. Para saber mais sobre como configurar o serviço CloudWatch e como trabalhar com os recursos do CloudWatch Logs, escolha um dos tópicos a seguir.

Tópicos

- [Configurar a integração do CloudWatch Logs para o Visual Studio](#)
- [Trabalhando com CloudWatch registros no Visual Studio](#)

Configurar a integração do CloudWatch Logs para o Visual Studio

Antes de usar a integração do Amazon CloudWatch Logs com o kit de ferramentas da AWS com Amazon Q, você precisa de uma conta da AWS. Você pode criar uma conta da AWS no site de [login da AWS](#). A maioria dos recursos do CloudWatch Logs que estão disponíveis no kit de ferramentas da AWS com Amazon Q podem ser acessados com credenciais ativas da AWS. Se um recurso específico exigir configuração adicional, os requisitos serão incluídos nas seções relevantes do tópico [Trabalhar com o CloudWatch Logs](#) deste guia.

Para obter informações e opções adicionais sobre a configuração do CloudWatch Logs, consulte a seção [Comece a usar](#) do Guia do Amazon CloudWatch Logs.

Trabalhando com CloudWatch registros no Visual Studio

A integração do Amazon CloudWatch Logs permite monitorar, armazenar e acessar CloudWatch registros do AWS Toolkit for Visual Studio com o Amazon Q. Ter acesso aos recursos do Logs, sem CloudWatch a necessidade de sair do IDE, melhora a eficiência simplificando o processo de desenvolvimento de registros e reduzindo as interrupções CloudWatch no fluxo de trabalho. Os tópicos a seguir descrevem como trabalhar com os recursos e funções básicos da integração do CloudWatch Logs.

Tópicos

- [CloudWatch Grupos de registros](#)
- [CloudWatch Fluxos de log](#)
- [CloudWatch Registrar eventos](#)
- [Acesso adicional aos CloudWatch registros](#)

CloudWatch Grupos de registros

Um `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.

Visualizar grupos de logs

O `View Log Groups` recurso exibe uma lista de grupos de CloudWatch log no `Log Groups Explorer`.

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

1. No `AWS Explorer`, expanda a `Amazon CloudWatch`.
2. Clique duas vezes em `Grupos de registros` ou abra o menu de contexto (clique com o botão direito do mouse) e selecione `Exibir` para abrir o `Explorador de grupos de CloudWatch registros`.

Note

O `CloudWatch Log Groups Explorer` abrirá no mesmo local da janela que o `Solutions Explorer`.

Filtrar grupos de logs

Sua conta individual pode conter milhares de grupos de logs diferentes. Para simplificar a busca de grupos específicos, use o recurso `filtering` descrito abaixo.

1. No `CloudWatch Log Groups Explorer`, 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 Log Groups Explorer` é atualizado automaticamente para mostrar resultados que correspondam aos termos de pesquisa que você especificou na etapa anterior.

Excluir grupos de logs

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

1. No CloudWatch Log Groups Explorer, clique com o botão direito do mouse no Grupo de Log que você deseja excluir.
2. Quando solicitado, confirme que deseja excluir o grupo de logs selecionado no momento.
3. Escolher o botão Sim exclui o grupo de log selecionado e, em seguida, atualiza o CloudWatch Log Groups Explorer.

Atualizar grupos de logs

Para atualizar a lista atual de grupos de registros exibida no Explorer de grupos de CloudWatch registros, escolha o botão do ícone Atualizar localizado na barra de ferramentas.

Copiar ARN do grupo de logs

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

1. No CloudWatch Log Groups Explorer, clique com o botão direito do mouse no Grupo de Log do qual você deseja copiar um ARN.
2. Escolha a opção Copiar ARN no menu.
3. O ARN agora está copiado para a área de transferência local e pronto para ser colado.

CloudWatch Fluxos de log

Fluxo de logs é uma sequência de eventos de log que compartilham a mesma origem.

Note

Ao visualizar os fluxos de logs, atente-se para as seguintes propriedades:

- Por padrão, os fluxos de logs são classificados pelo registro de data e hora do evento mais recente.
- As colunas associadas a um fluxo de logs podem ser classificadas em ordem crescente ou decrescente, alternando o cursor localizado nos cabeçalhos das colunas.
- As entradas filtradas só podem ser classificadas pelo Nome do fluxo de logs.

Visualizar fluxos de logs

1. No Explorer de grupos de CloudWatch registros, clique duas vezes em um grupo de registros ou clique com o botão direito do mouse em um grupo de registros e selecione Exibir fluxo de registros no menu de contexto.
2. Uma nova guia será aberta na janela do documento, que contém uma lista dos fluxos de logs associados ao grupo de logs.

Filtrar fluxos de logs

1. Na guia Fluxos de logs, na janela do documento, coloque o cursor na barra de pesquisa.
2. Comece a digitar um prefixo relacionado ao fluxo de logs que você está procurando.
3. Conforme você digita, a tela atual é atualizada automaticamente para filtrar os fluxos de log de acordo com sua entrada.

Atualizar fluxos de logs

Para atualizar a lista atual de fluxos de logs exibidos na janela do documento, escolha o botão do ícone Atualizar, localizado na barra de ferramentas, ao lado da barra de pesquisa.

Copiar ARN dos fluxos de logs

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

1. Na guia Fluxos de logs, na janela do documento, clique com o botão direito no fluxo de logs do qual você deseja copiar um ARN.
2. Escolha a opção Copiar ARN no menu.
3. O ARN agora está copiado para a área de transferência local e pronto para ser colado.

Baixar fluxos de logs

O recurso Exportar fluxo de logs baixa e armazena o fluxo de logs selecionado localmente, onde ele pode ser acessado por ferramentas e software personalizados para processamento adicional.

1. Na guia Fluxos de logs, na janela do documento, clique com o botão direito no fluxo de logs que você deseja baixar.
2. Escolha Exportar fluxo de logs para abrir a caixa de diálogo Exportar para um arquivo de texto.

3. Escolha o local onde você deseja armazenar o arquivo localmente e especifique um nome no campo de texto fornecido.
4. Confirme o download selecionando OK. O status do download é exibido no Centro de Status de Tarefas do Visual Studio.

CloudWatch Registrar eventos

Eventos de log são registros de atividades registradas pelo aplicativo ou recurso que está sendo monitorado pelo CloudWatch.

Ações de eventos de logs

Os eventos de logs são exibidos como uma tabela. Por padrão, os eventos são classificados do evento mais antigo para o mais recente.

As seguintes ações estão associadas a eventos de logs no Visual Studio:

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

Visualizar eventos de logs


1. Na janela do documento, escolha uma guia que contenha uma lista de fluxos de logs.
2. Clique duas vezes em um fluxo de logs ou clique com o botão direito em um fluxo de logs e selecione Visualizar fluxo de logs no menu.
3. Uma nova guia de evento de logs será aberta na janela do documento, que contém uma tabela de eventos de logs associados ao fluxo de logs escolhido.

Filtrar eventos de logs

Há três maneiras de filtrar eventos de logs: por conteúdo, intervalo de tempo ou ambos. Para filtrar eventos de logs por conteúdo e intervalo de tempo, primeiro filtre as mensagens por conteúdo ou intervalo de tempo e, em seguida, filtre esses resultados pelo outro método.

Para filtrar eventos de logs por conteúdo:


1. Na guia de Evento de logs, na janela do documento, coloque o cursor na barra de pesquisa, localizada na parte superior da janela.
2. Comece a digitar um termo ou frase relacionada aos eventos de logs que você está procurando.
3. Conforme você digita, a exibição atual começa automaticamente a filtrar os eventos de logs.

 Note

Os padrões de filtro diferenciam letras maiúsculas de minúsculas. Você pode melhorar os resultados da pesquisa colocando termos exatos e frases com caracteres não alfanuméricos entre aspas duplas ("****"). Para obter informações mais detalhadas sobre padrões de filtro, consulte o tópico [Filtro e sintaxe de padrões](#) no CloudWatch guia da Amazon.

Para visualizar eventos de logs gerados durante um intervalo de tempo específico:

1. Na guia de Evento de logs, na janela do documento, escolha o botão do ícone do Calendário, localizado na barra de ferramentas.
2. Usando os campos fornecidos, especifique o intervalo de tempo que você deseja pesquisar.
3. Os resultados filtrados são atualizados automaticamente conforme você especifica as restrições de data e hora.

 Note

A opção Limpar filtro limpa todas as suas seleções de date-and-time filtro atuais.

Atualizar eventos de logs

Para atualizar a lista atual de eventos de logs exibida na guia Eventos de logs, escolha o botão do ícone Atualizar, localizado na barra de ferramentas.

Acesso adicional aos CloudWatch registros

Você pode acessar CloudWatch os registros associados a outros AWS serviços e recursos diretamente do AWS kit de ferramentas no Visual Studio.

Lambda

Para visualizar os fluxos de logs associados a uma função do Lambda:

Note

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

1. No AWS Toolkit Explorer, expanda Lambda.
2. Clique com o botão direito na função que você deseja visualizar e escolha Visualizar logs para abrir os fluxos de logs associados na janela do documento.

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

1. No AWS Toolkit Explorer, expanda Lambda.
2. Clique com o botão direito na função que você deseja visualizar e escolha Visualizar função para abrir a visualização de função na janela do documento.
3. Em `function view`, alterne para a guia Logs. Os fluxos de log associados à função do Lambda escolhida são exibidos.

ECS

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

Note

Para que o serviço Amazon ECS envie registros para CloudWatch, cada contêiner de uma determinada tarefa do Amazon ECS deve atender à configuração necessária. Para obter informações adicionais sobre a instalação e as configurações necessárias, consulte o guia [Usando o driver de registro de AWS registros](#).

1. No AWS Toolkit Explorer, expanda o Amazon ECS.

2. Escolha o cluster do Amazon ECS que você deseja visualizar para abrir uma nova guia Cluster do ECS, na janela do documento.
3. No menu de navegação, localizado no lado esquerdo da guia Cluster do ECS, escolha Tarefas para listar todas as tarefas associadas ao cluster.
4. Na visualização Tarefas, selecione uma tarefa e escolha o link Visualizar logs, localizado no canto inferior esquerdo.

Note

Essa visualização lista todas as tarefas contidas no cluster. O link de View Logs só fica visível para cada tarefa que atende à configuração de logs necessária.

- Se uma tarefa estiver associada a um único contêiner, o link Visualizar logs abrirá o fluxo de logs desse contêiner.
- Se uma tarefa estiver associada a vários contêineres, o link Exibir registros abrirá a caixa de diálogo Exibir CloudWatch registros da tarefa do ECS, use o menu suspenso Contêiner: para escolher o contêiner do qual você deseja visualizar os registros e, em seguida, escolha OK.

5. Uma nova guia é aberta na janela do documento exibindo os fluxos de logs associados à sua seleção de contêineres.

Gerenciar instâncias do Amazon EC2

O AWS Explorer apresenta visualizações detalhadas de imagens de máquina da Amazon (AMIs) e instâncias 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

No AWS Explorer, você pode exibir visualizações das AMIs e das instâncias do Amazon EC2. No AWS Explorer, expanda o nó Amazon EC2.

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).

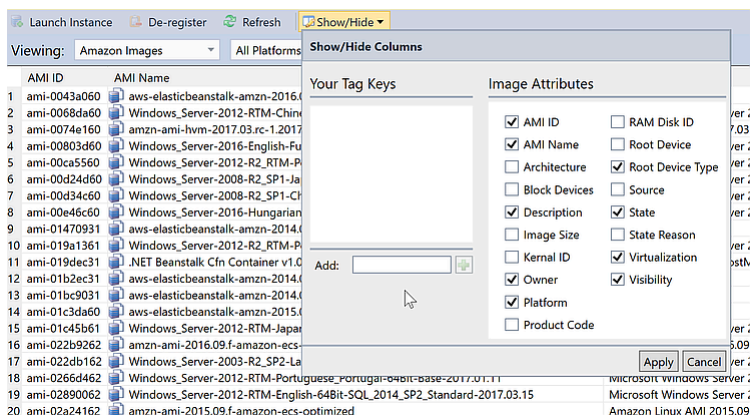
Para exibir a visualização das instâncias do Amazon EC2, no nó Instances (Instâncias), abra o menu de contexto (clique com o botão direito do mouse) e escolha View (Exibir).

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

- As visualizações têm escopo para a região especificada no AWS Explorer (por exemplo, região 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 no AWS Explorer.

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

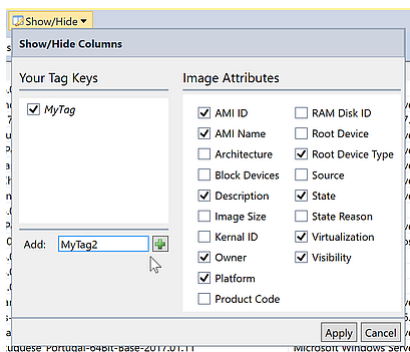
Você também pode usar a lista suspensa Mostrar/ocultar a fim de adicionar tags para AMIs, instâncias do Amazon EC2 ou volumes próprios. Tags são pares nome/valor que permitem anexar metadados a AMIs, instâncias e volumes. Os nomes de tags têm escopo para a conta e também são

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, consulte [Using tags](#), no Manual do usuário para instâncias do Linux do Amazon EC2.

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 no [Console de gerenciamento da AWS](#).

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

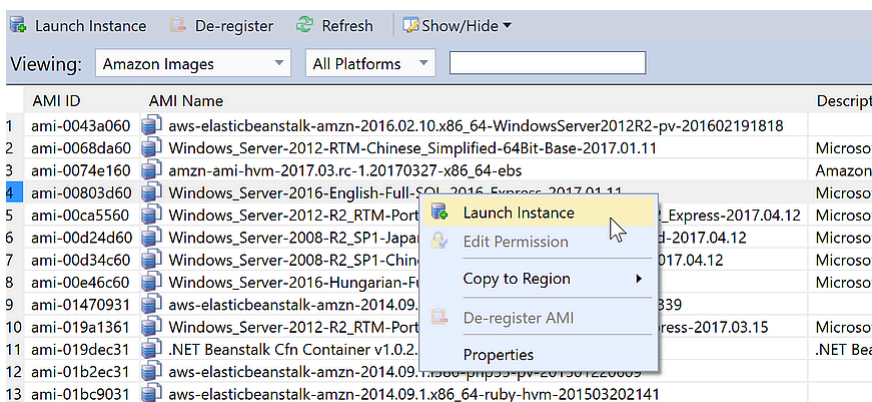
Se você limpar uma tag na lista suspensa Mostrar/ocultar sem valores associados, o kit de ferramentas da AWS excluirá a tag por completo. Ela deixará de ser exibida na visualização em lista ou na lista suspensa Show/Hide (Mostrar/ocultar). Para reutilizar essa tag, use a caixa de diálogo Show/Hide (Mostrar/ocultar) para recriá-la.

Executar uma instância do Amazon EC2

O AWS 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

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\\AppData\Local\AWSToolkit\keypairs). Você pode exportar o par de chaves criptografadas em um arquivo .pem.

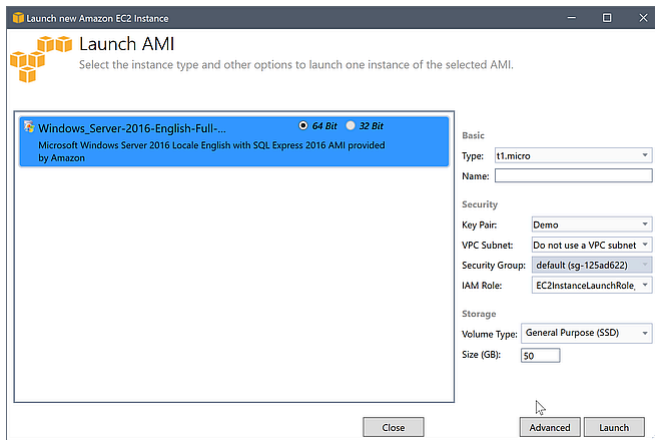
- a. No Visual Studio, selecione Visualizar e clique em AWS Explorer.
- b. Clique em Amazon EC2 e selecione Key Pairs (Pares de chaves).
- c. Os pares de chaves serão listados e aqueles criados/gerenciados pelo Toolkit serão marcados como Stored in AWSToolkit (Armazenado no AWSToolkit).
- d. Clique com 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.

Grupo de segurança

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 criar grupos de segurança usando o kit de ferramentas, consulte [Gerenciar grupos de segurança no AWS Explorer](#).

Perfil da instância

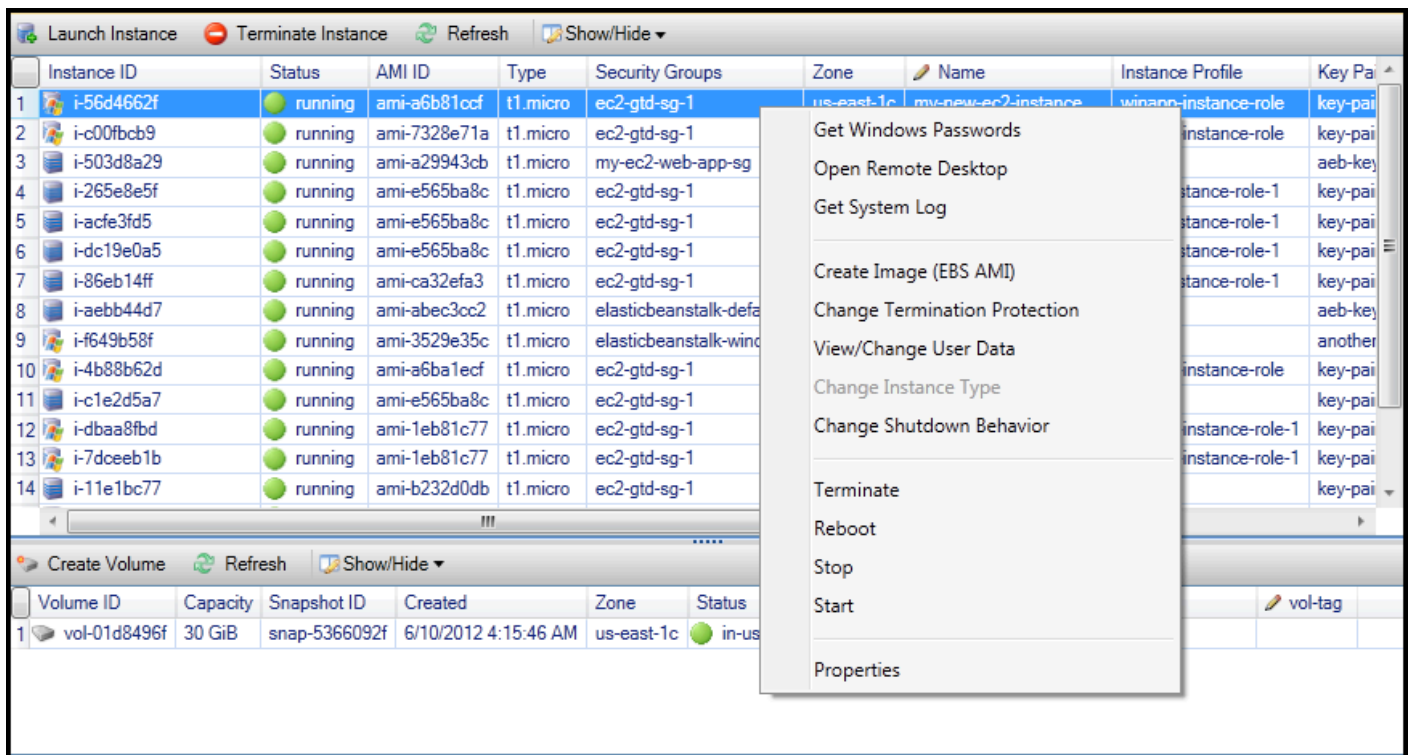
O perfil da instância é um contêiner lógico para uma função do IAM. Ao escolher um perfil da instância, você associa a função do IAM correspondente à instância do EC2. Os perfis do IAM são configurados com políticas que especificam o acesso a à Amazon Web Services e recursos de conta. Quando uma instância 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 de aplicação seja executado sem a necessidade de especificar credenciais da AWS 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.

No AWS Explorer, no subnó Instâncias do Amazon EC2, abra o menu de contexto (clique com o botão direito) do nó Amazon EC2 e escolha Visualizar. O kit de ferramentas da AWS 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.



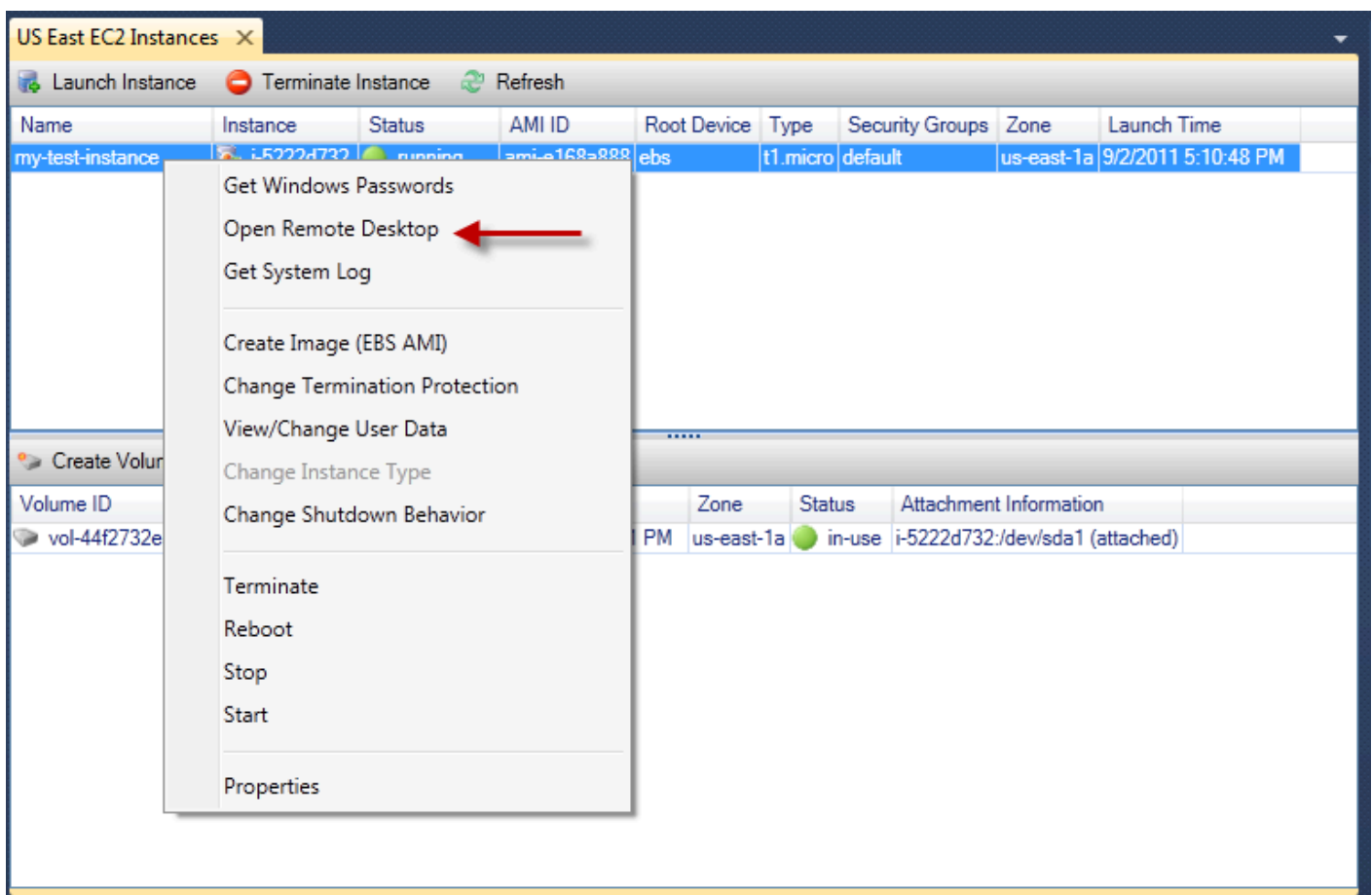
Conectar a uma instância do Amazon EC2

Você pode usar a Área de Trabalho Remota para se conectar a uma instância do Windows Server. Na autenticação, o kit de ferramentas da AWS permite recuperar a senha de administrador da instância, ou basta usar o par de chaves 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 Abrir área de trabalho remota.

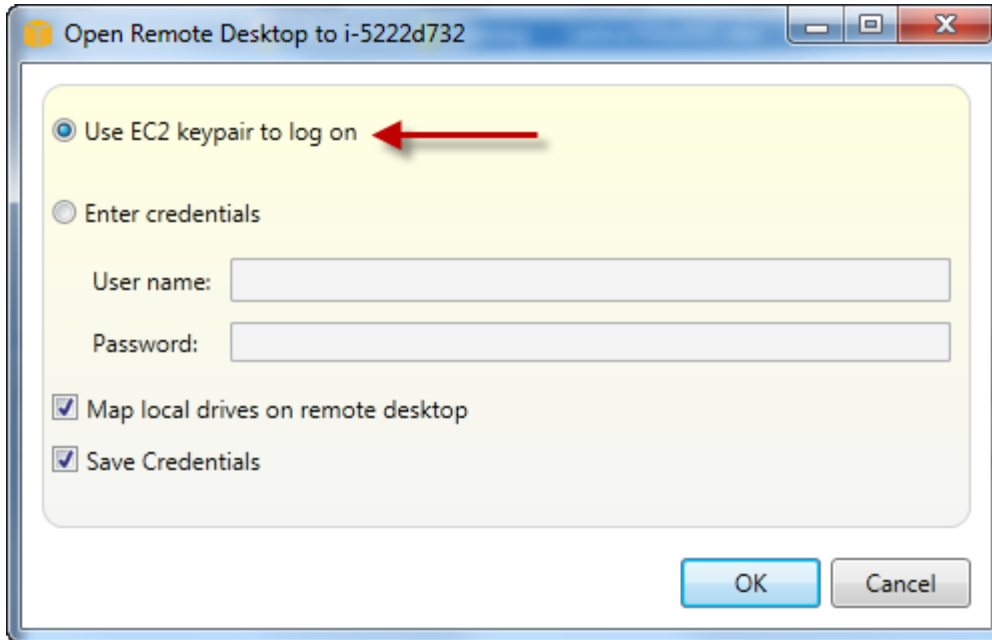
Se quiser autenticar usando a senha de administrador, escolha Get Windows Passwords (Obter senhas do Windows).



Menu de contexto EC2 Instance

2. Na caixa de diálogo Open Remote Desktop (Abrir área de trabalho 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 par de chaves com o kit de ferramentas da AWS, especifique o arquivo PEM que contém a chave privada.

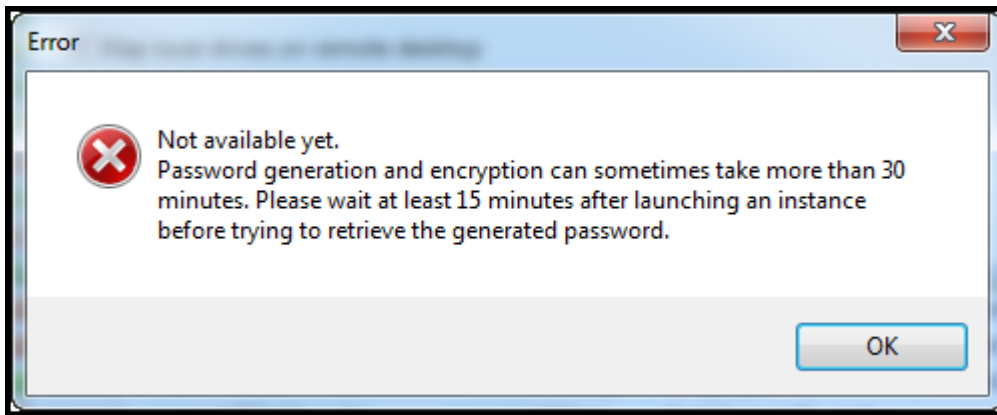


Caixa de diálogo Open Remote Desktop (Abrir área de trabalho remota)

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.

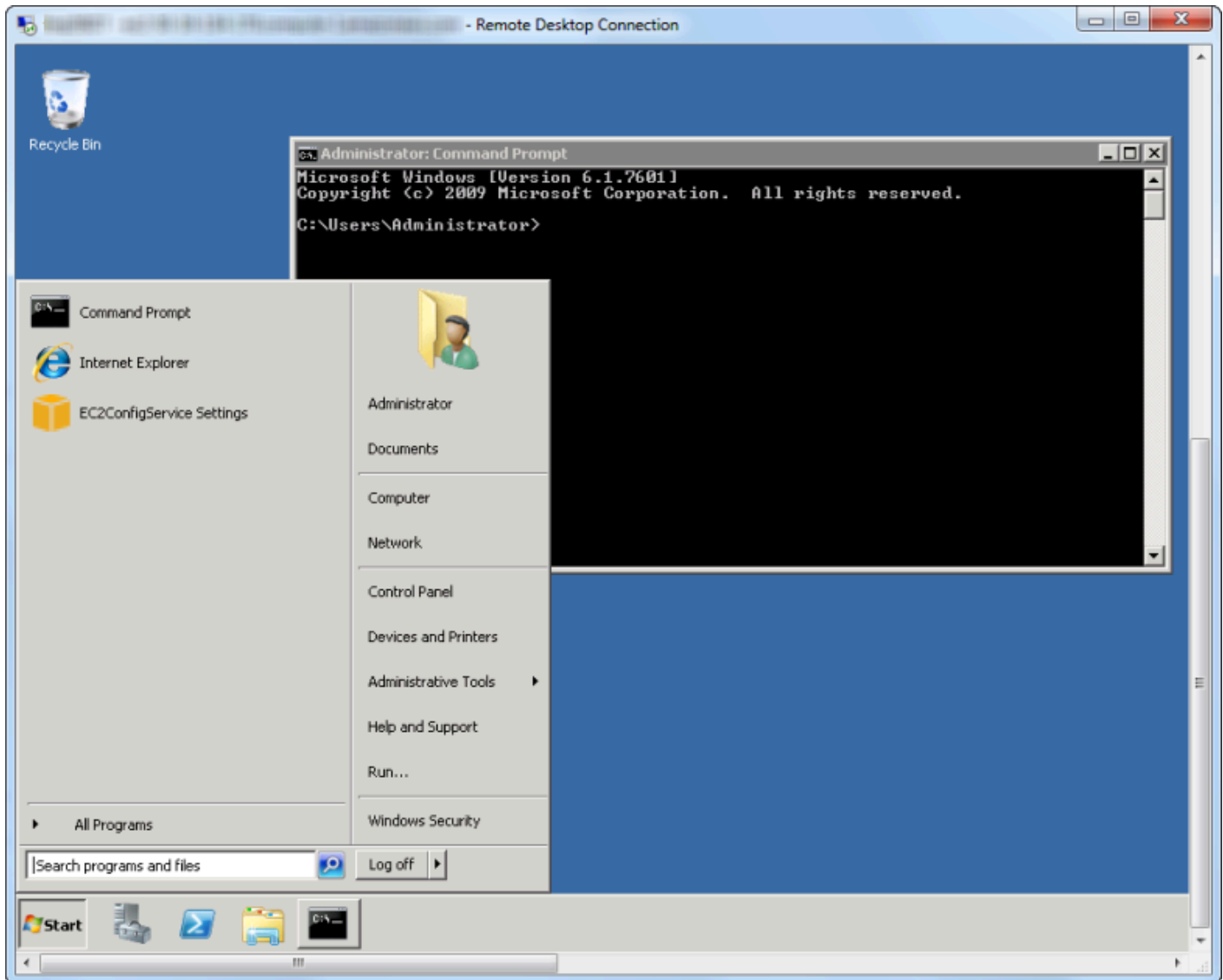
Se a instância do EC2 tiver sido iniciada apenas recentemente, talvez você não consiga se conectar por dois motivos possíveis:

- 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

Usando o kit de ferramentas da AWS, 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, a única opção será encerrá-la.

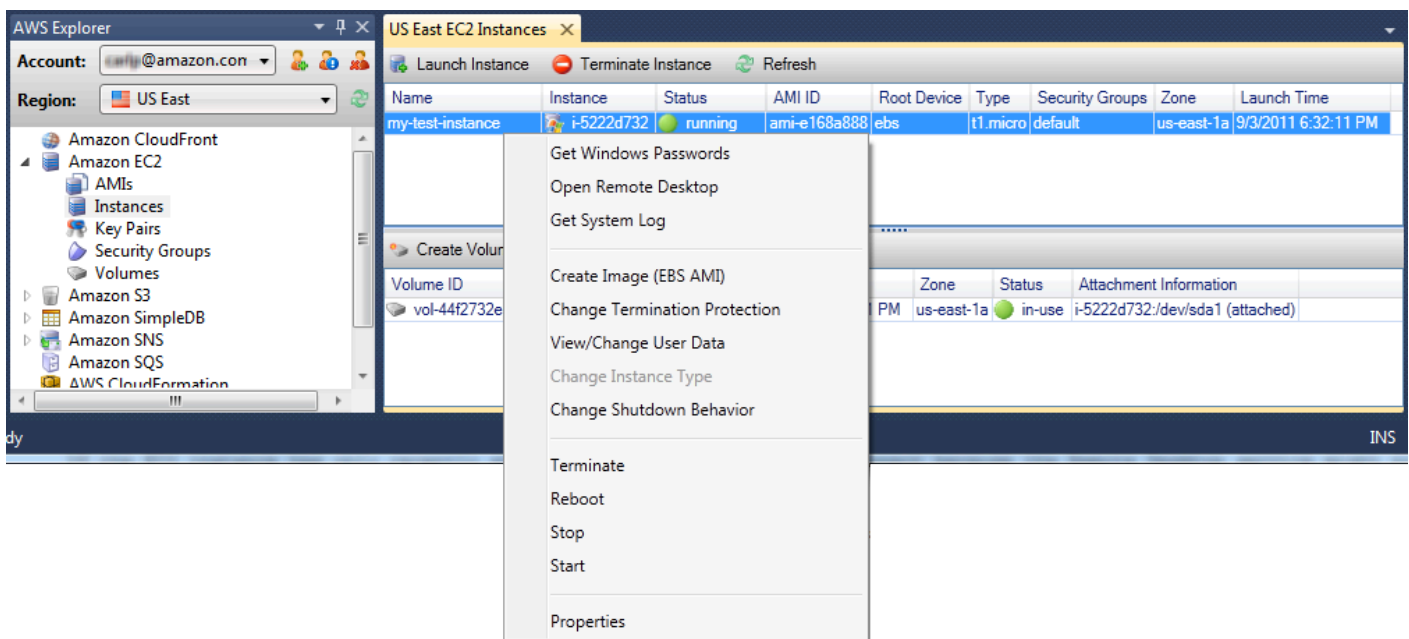
Se você parar a instância, os dados armazenados no volume do EBS serão mantidos. Se você encerrar a instância, todos os dados armazenados no dispositivo de armazenamento da instância local serão perdidos. Em ambos os casos, parar ou encerrar, você não continuará sendo cobrado

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 EC

1. No AWS Explorer, expanda o nó Amazon EC2, abra o menu de contexto (clique com o botão direito) de Instâncias e escolha Visualizar. 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.

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

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

Below the instances table, there are buttons for 'Create Volume' and 'Refresh'. Below that is a table of volumes:

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

Instâncias encerradas permanecem visíveis

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

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

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

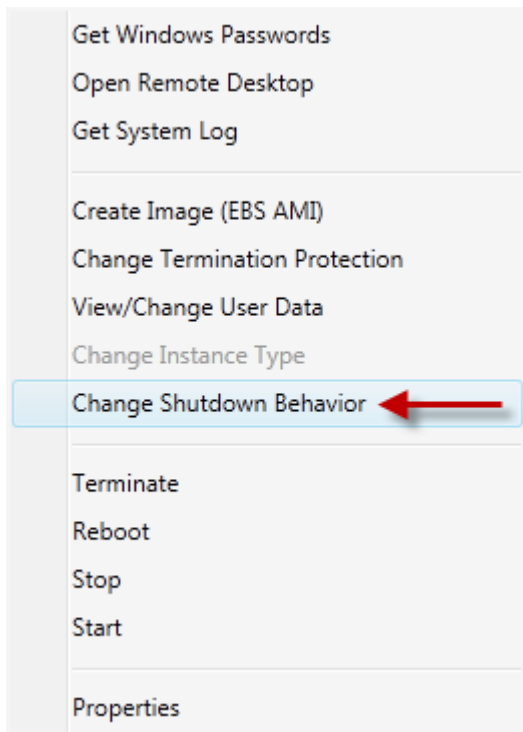
Below the instances table, there are buttons for 'Create Volume' and 'Refresh'. Below that is a table of volumes:

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

Para especificar o comportamento de uma instância do EC2 no desligamento

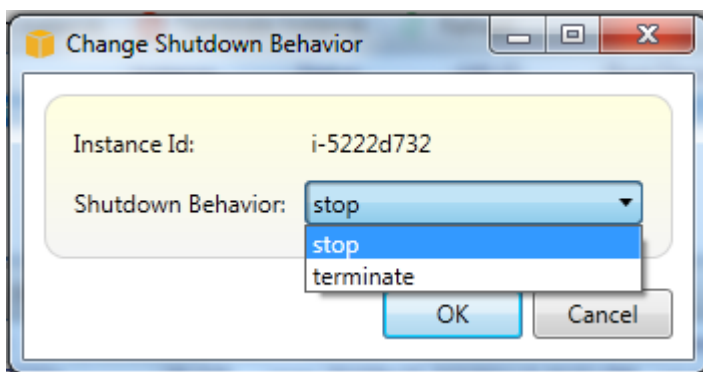
O kit de ferramentas da AWS permite especificar se uma instância do Amazon EC2 será interrompida ou encerrada se Desligar for selecionado no menu Iniciar.

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

AWS O Explorer fornece visualizações detalhadas dos clusters e repositórios de contêineres 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. No AWS Explorer, abra o menu de contexto (clique com o botão direito do mouse) do cluster a ser gerenciado e escolha Exibir.
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 Eventos para ver as mensagens de eventos e Implantações para ver o respectivo status.
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. No AWS Explorer, abra o menu de contexto (clique com o botão direito do mouse) do cluster com as tarefas que você deseja interromper e escolha Exibir.
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. No AWS Explorer, abra o menu de contexto (clique com o botão direito do mouse) do cluster com um serviço que você deseja excluir e escolha Exibir.
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 do AWS Explorer.

Excluir um cluster

Você pode excluir um cluster do Amazon Elastic Container Service do AWS Explorer.

Para excluir um cluster

1. No AWS Explorer, abra o menu de contexto (clique com o botão direito do mouse) do cluster que você deseja excluir no nó Clusters do Amazon ECS e escolha Excluir.
2. Na caixa de diálogo Delete Cluster (Excluir cluster), escolha OK. Quando o cluster for excluído, ele será removido do AWS Explorer.

Criar um repositório

Você pode criar um repositório Amazon Elastic Container Registry a partir do AWS Explorer.

Para criar um repositório

1. No AWS Explorer, abra o menu de contexto (clique com o botão direito do mouse) do nó Repositórios no Amazon ECS e escolha Criar repositório.
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 Amazon Elastic Container Registry do AWS Explorer.

Para excluir um repositório

1. No AWS Explorer, abra o menu de contexto (clique com o botão direito do mouse) do nó Repositórios no Amazon ECS e escolha Excluir 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).

Gerenciar grupos de segurança no AWS Explorer

O kit de ferramentas para Visual Studio permite que você crie e configure grupos de segurança para usar com instâncias do Amazon Elastic Compute Cloud (Amazon EC2) e o CloudFormation. Ao executar instâncias do Amazon EC2 ou implantar uma aplicação no CloudFormation, você especifica um grupo de segurança a ser associado às instâncias do Amazon EC2. (A implantação no CloudFormation cria instâncias do EC2.)

Um security group funciona como um firewall no tráfego de rede recebido. O grupo de segurança 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.

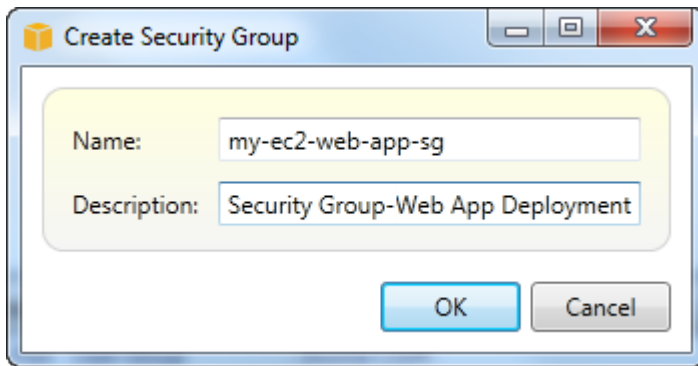
Criar um grupo de segurança

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. No AWS Explorer, no nó Amazon EC2, abra o menu de contexto (clique com o botão direito) do nó Grupos de segurança e escolha Visualizar.
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.

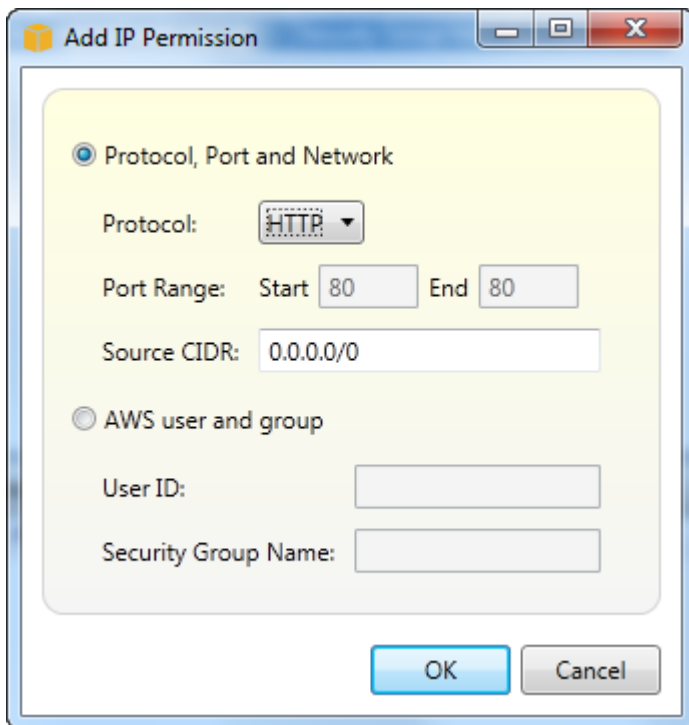


Adicionar permissões a security groups

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.

Group	Name	Description
sg-5d792234	default	default group
sg-db2313b2	my-ec2-web-app-sg	Security Group-Web App Deployment

Protocol	Port	User:Group	Source CIDR
HTTP (TCP)	80		0.0.0.0/0
HTTPS (TCP)	443		0.0.0.0/0
RDP (TCP)	3389		0.0.0.0/0

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 grupo de segurança aceitarão todo tráfego de rede de entrada de instâncias do Amazon EC2 no grupo de segurança especificado.

Você também deve especificar o ID do usuário como uma maneira de diferenciar o nome do grupo de segurança; os nomes de grupo de segurança não precisam ser exclusivos em toda a AWS. Para obter mais informações sobre grupos de segurança, acesse a [documentação do EC2](#).

Criar uma AMI com base em uma instância do Amazon EC2

Você pode criar uma imagem de máquina da Amazon (AMI) com o AWS Toolkit for Visual Studio. Para obter informações mais detalhadas sobre isso AMIs, consulte o tópico [Amazon Machine Images \(AMI\)](#) no Guia do usuário do Amazon Elastic Compute Cloud for Windows Instances.

Para criar uma AMI em uma instância do Amazon EC2 existente, conclua o procedimento a seguir.

Criar uma AMI com base em uma instância existente do Amazon EC2

1. No AWS Toolkit Explorer, expanda o Amazon EC2 e escolha Instâncias para ver uma lista de suas instâncias existentes.
2. Clique com o botão direito do mouse na instância que deseja usar como base para a AMI e selecione Criar imagem (AMI ABS) para abrir a janela de diálogo Criar imagem.
3. Na janela de diálogo Criar imagem, adicione um nome e uma descrição para a imagem nos campos fornecidos e clique no botão OK para continuar.
4. A janela de confirmação Imagem criada é aberta no Visual Studio quando a imagem é criada. Clique no botão OK para continuar.

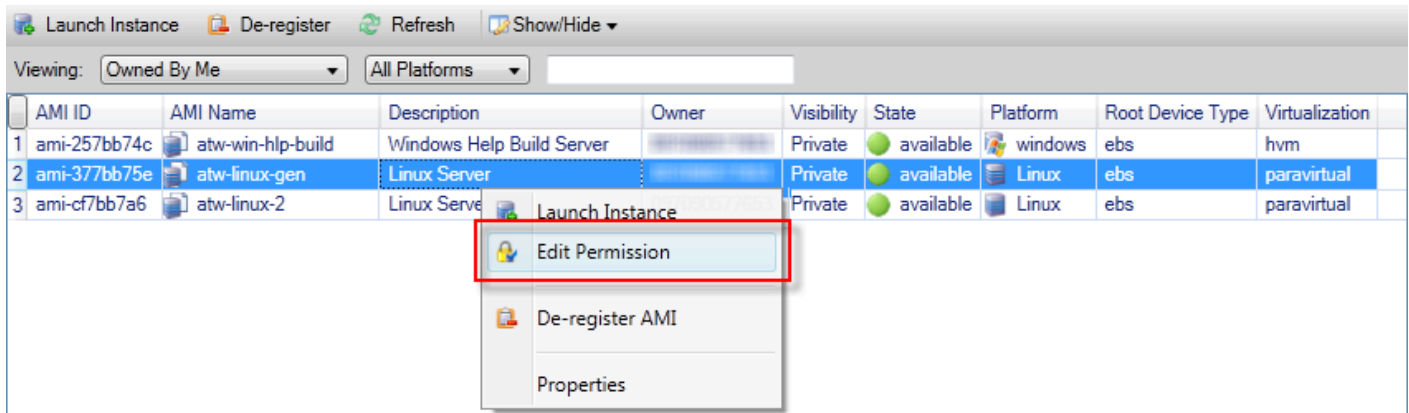
Para visualizar sua nova AMI com o AWS Toolkit, expanda o Amazon EC2 e AMIs clique duas vezes para abrir uma janela no painel do Editor do Visual Studio que exibe uma lista das suas existentes. AMIs Caso não veja a nova AMI na lista, clique no botão Atualizar na parte superior da janela de AMIs.

Definir permissões de execução em uma imagem de máquina da Amazon

Você pode definir permissões de lançamento em suas Amazon Machine Images (AMIs) a partir da AMIs visualização no AWS Explorer. Você pode usar a caixa de diálogo Definir permissões de AMI para copiar permissões de AMIs.

Para definir permissões em uma AMI

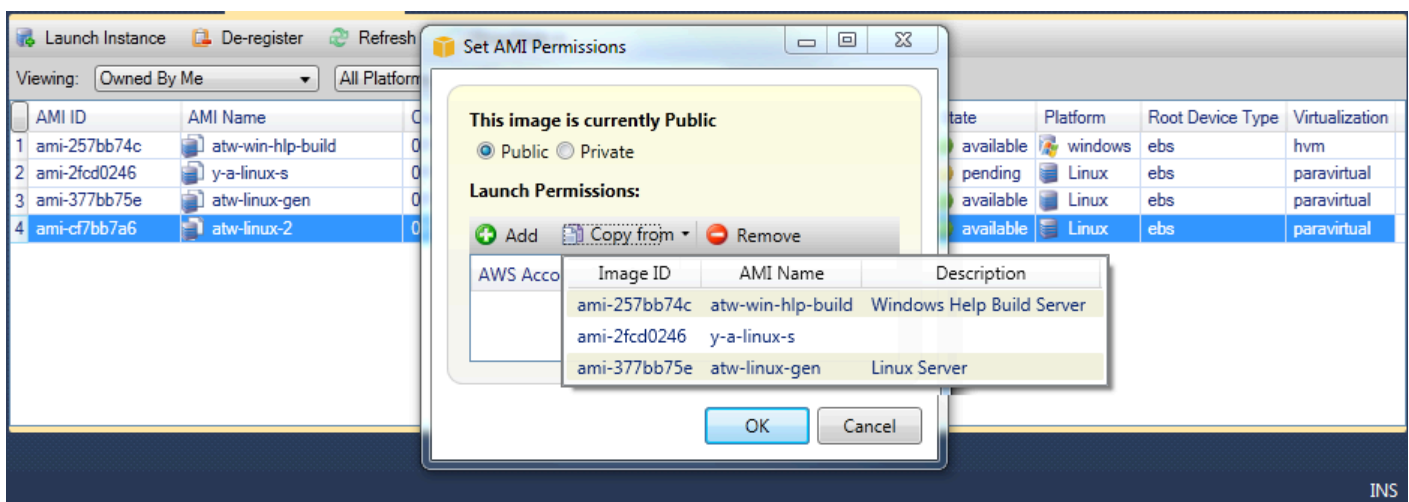
1. Na AMI exibição no AWS Explorer, abra o menu de contexto (clique com o botão direito do mouse) em uma AMI e escolha Editar permissão.



2. Existem três opções disponíveis na caixa de diálogo Set AMI Permissions (Definir permissões da AMI):

- Para dar permissão de lançamento, escolha Adicionar e digite o número da conta do AWS usuário ao qual você está dando permissão de lançamento.
- Para remover a permissão de lançamento, escolha o número da conta do AWS usuário do qual você está removendo a permissão de lançamento e escolha Remover.
- 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 outros AMIs na lista Copiar de para copiar permissões de várias AMIs para a AMI de destino.

A lista Copiar de contém somente aqueles AMIs pertencentes à conta que estava ativa quando a AMI exibição foi exibida no Explorer. AWS Como resultado, a lista Copiar de pode não ser exibida AMIs se nenhuma outra AMIs for de propriedade da conta ativa.



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

Amazon Virtual Private Cloud (VPC)

O Amazon Virtual Private Cloud (Amazon VPC) permite iniciar recursos da Amazon Web Services em uma rede virtual definida por você. Essa rede virtual é semelhante a uma rede tradicional que você operaria no próprio datacenter, com os benefícios de usar a infraestrutura escalável da AWS. Para obter mais informações, acesse o [Guia do usuário da Amazon VPC](#).

O kit de ferramentas para Visual Studio permite que um desenvolvedor acesse a funcionalidade da VPC de maneira semelhante à exposta pelo [Console de gerenciamento da AWS](#), mas no ambiente de desenvolvimento do Visual Studio. O nó Amazon VPC do AWS Explorer inclui subnós para as seguintes áreas.

- [VPCs](#)
- [Sub-redes](#)
- [Elástica IPs](#)
- [Gateways da Internet](#)
- [Rede ACLs](#)
- [Tabelas de rotas](#)
- [Grupos de segurança](#)

Criação de uma VPC público-privada para implantação com AWS Elastic Beanstalk

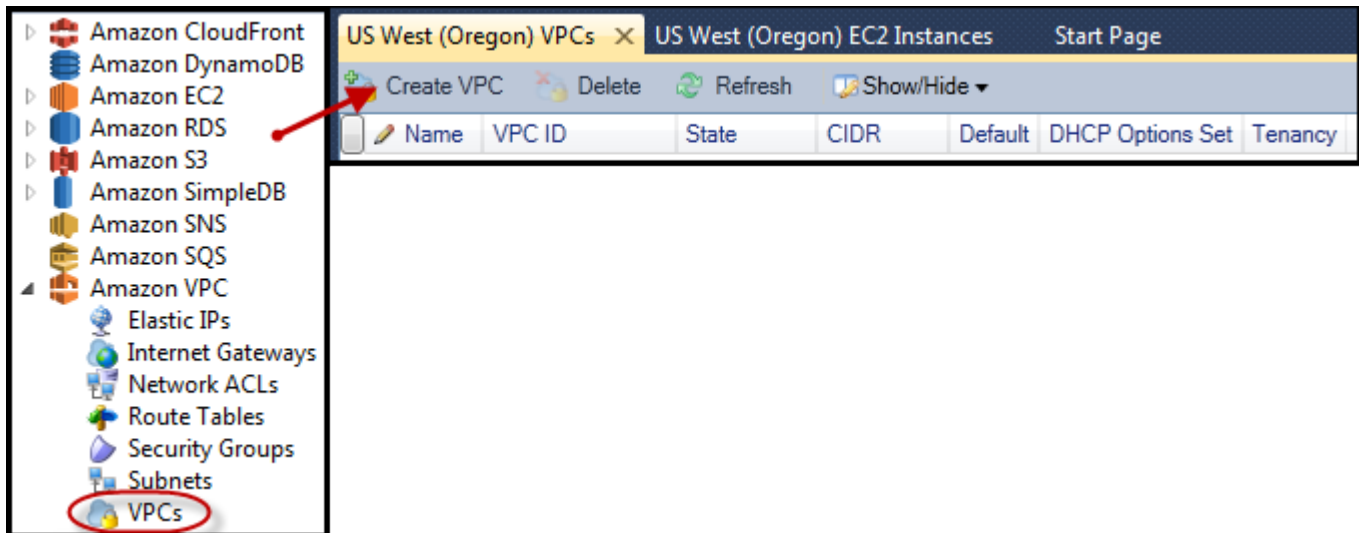
Esta seção descreve como criar um Amazon VPC que contém as sub-redes privadas e públicas. A sub-rede pública contém uma EC2 instância da Amazon que realiza a conversão de endereços de rede (NAT) para permitir que instâncias na sub-rede privada se comuniquem com a Internet pública. As duas sub-redes devem residir na mesma Availability Zone (AZ – Zona de disponibilidade).

Essa é a configuração mínima de VPC necessária para implantar um AWS Elastic Beanstalk ambiente em uma VPC. Nesse cenário, as EC2 instâncias da Amazon que hospedam seu aplicativo residem na sub-rede privada; o balanceador de carga do Elastic Load Balancing, que roteia o tráfego de entrada para seu 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. No nó Amazon VPC no AWS Explorer, abra o VPCsubnó e escolha Create 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 par de chaves é usado para a EC2 instância da Amazon que realiza a conversão de endereços de rede da sub-rede privada para a 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 par de chaves é usado para a EC2 instância da Amazon que realiza a conversão de endereços de rede da sub-rede privada para a 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.

Create VPC

Name: myDeploymentVPC

CIDR Block*: 10.0.0.0/16

Tenancy: default

With Public Subnet

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

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

With Private Subnet

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

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

Configure default security group to allow traffic to NAT

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

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

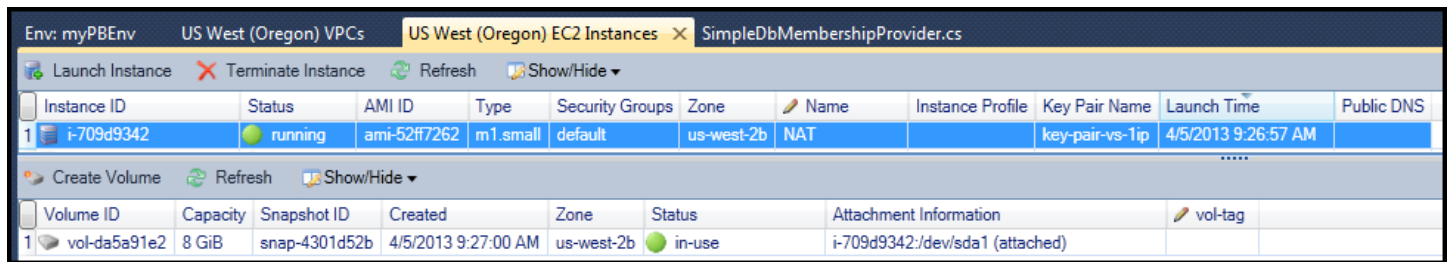
OK Cancel

Você pode ver a nova VPC na VPCs AWS guia do Explorer.

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

A instância NAT pode levar alguns minutos para ser iniciada. Quando estiver disponível, você poderá visualizá-lo expandindo o EC2 nó da Amazon no AWS Explorer e abrindo o subnó Instâncias.

Um volume do Amazon Elastic Block Store (Amazon EBS) é criado para a instância NAT automaticamente. Para obter mais informações sobre o Amazon EBS, consulte o [tópico Amazon Elastic Block Store \(EBS\) no Guia do EC2](#) usuário da Amazon para instâncias Linux.



The screenshot shows the AWS Management Console interface. At the top, there are tabs for 'Env: myPBEEnv', 'US West (Oregon) VPCs', 'US West (Oregon) EC2 Instances', and 'SimpleDbMembershipProvider.cs'. Below the tabs, there are buttons for 'Launch Instance', 'Terminate Instance', 'Refresh', and 'Show/Hide'. The main content area displays a table of EC2 instances and a table of EBS volumes.

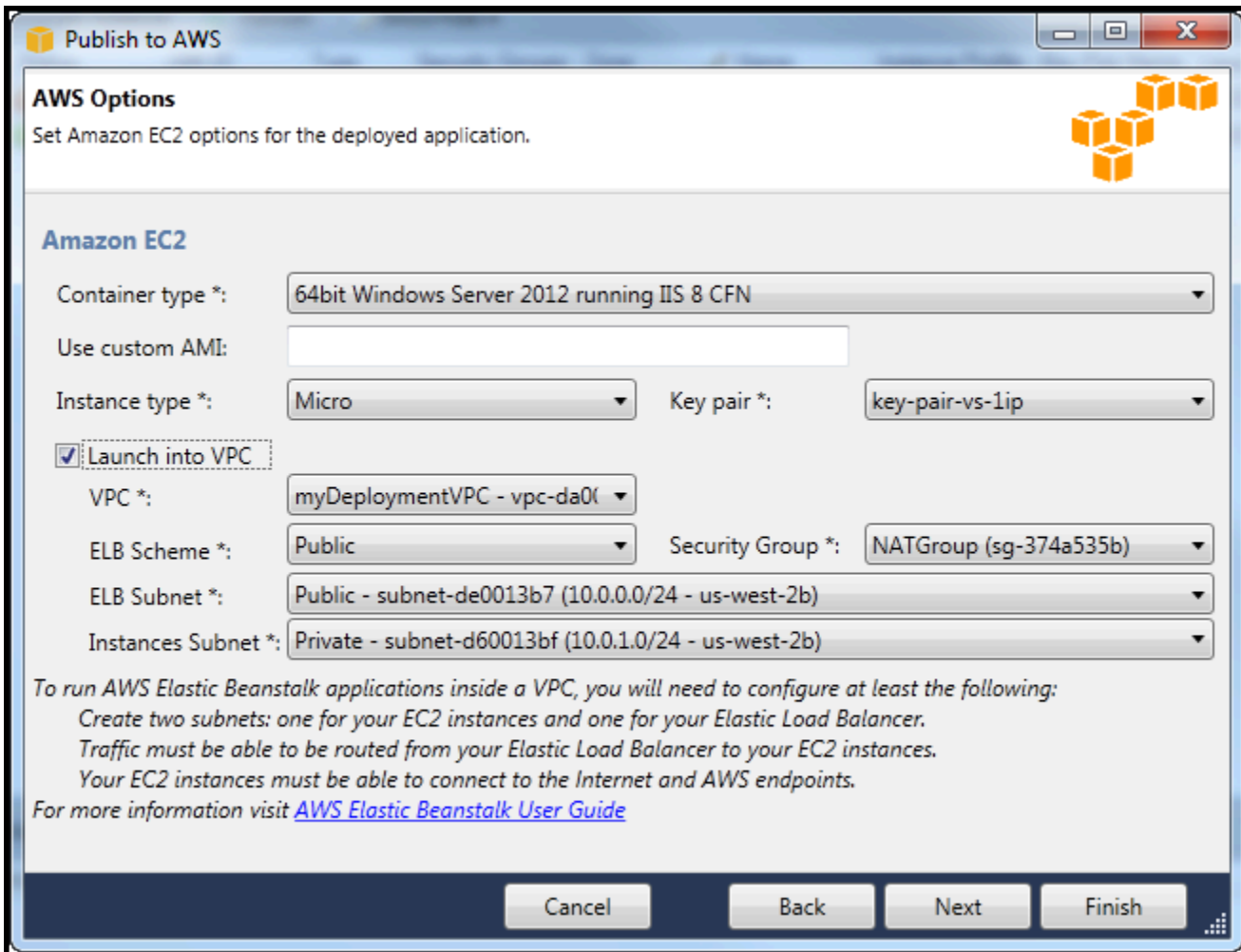
Instance ID	Status	AMI ID	Type	Security Groups	Zone	Name	Instance Profile	Key Pair Name	Launch Time	Public DNS
1 i-709d9342	running	ami-52ff7262	m1.small	default	us-west-2b	NAT		key-pair-vs-1ip	4/5/2013 9:26:57 AM	

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

Se você [implantar um aplicativo em um AWS Elastic Beanstalk ambiente](#) e optar por iniciar o ambiente em uma VPC, o kit de ferramentas preencherá a caixa de Amazon Web Services diálogo Publish to com as informações de configuração da sua VPC.

O Toolkit preenche a caixa de diálogo com informações somente das VPCs que foram criadas no Toolkit, não das VPCs criadas usando o Console de gerenciamento da AWS. 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.



Publish to AWS

AWS Options
Set Amazon EC2 options for the deployed application.

Amazon EC2

Container type *: 64bit Windows Server 2012 running IIS 8 CFN

Use custom AMI:

Instance type *: Micro Key pair *: key-pair-vs-1ip

Launch into VPC

VPC *: myDeploymentVPC - vpc-da0(

ELB Scheme *: Public Security Group *: NATGroup (sg-374a535b)

ELB Subnet *: Public - subnet-de0013b7 (10.0.0.0/24 - us-west-2b)

Instances Subnet *: Private - subnet-d60013bf (10.0.1.0/24 - us-west-2b)

To run AWS Elastic Beanstalk applications inside a VPC, you will need to configure at least the following:
Create two subnets: one for your EC2 instances and one for your Elastic Load Balancer.
Traffic must be able to be routed from your Elastic Load Balancer to your EC2 instances.
Your EC2 instances must be able to connect to the Internet and AWS endpoints.
For more information visit [AWS Elastic Beanstalk User Guide](#)

Cancel Back Next Finish

Para excluir uma VPC

Para excluir a VPC, você deve primeiro encerrar todas as EC2 instâncias da Amazon na VPC.

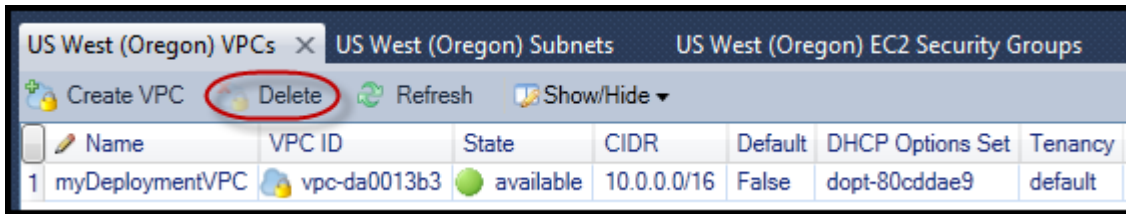
1. Se você implantou um aplicativo em um AWS Elastic Beanstalk ambiente na VPC, exclua o ambiente. Isso encerrará todas as EC2 instâncias da Amazon que hospedam seu aplicativo junto com o balanceador de carga do Elastic Load Balancing.

Se você tentar encerrar diretamente as instâncias que hospedam a aplicação sem excluir o ambiente, o serviço Auto Scaling criará instâncias automaticamente para substituir as excluídas. Para obter mais informações, acesse o [Guia do desenvolvedor do Auto Scaling](#).

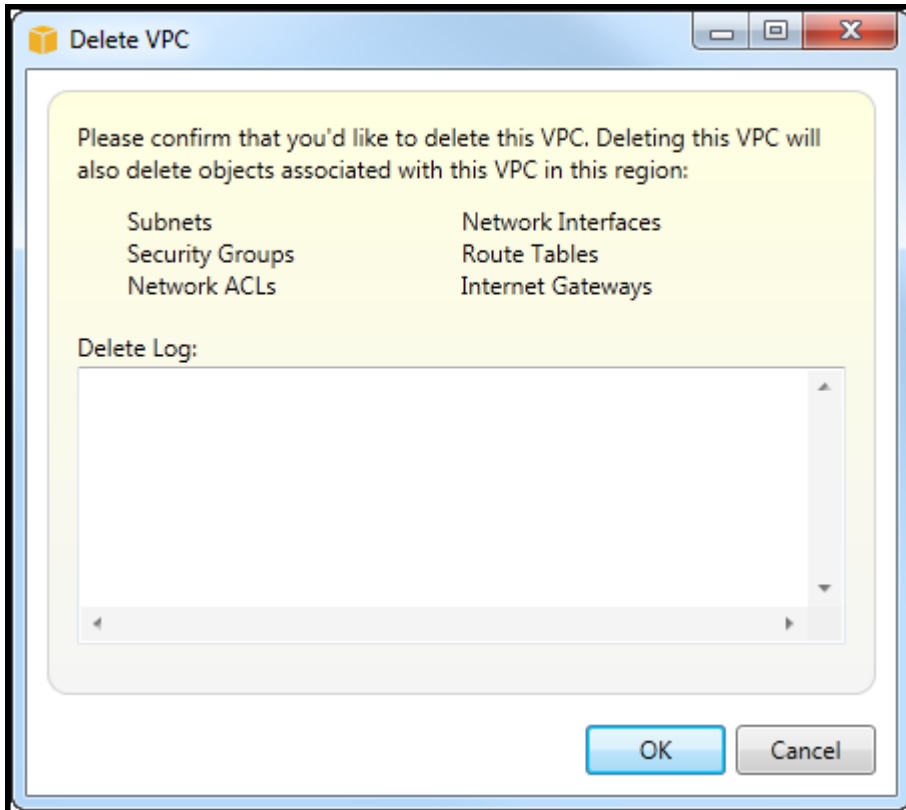
2. Exclua a instância NAT da VPC.

Não é necessário 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.



Usar o Editor de modelos do CloudFormation para Visual Studio

O kit de ferramentas para Visual Studio inclui um editor de modelos do CloudFormation e projetos de modelo do CloudFormation para o Visual Studio. Entre os recursos compatíveis estão:

- Criar novos modelos (vazios ou copiados de uma stack existente ou de um modelo de exemplo) usando o tipo de projeto do modelo do CloudFormation 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 um modelo do Visual Studio.

Tópicos

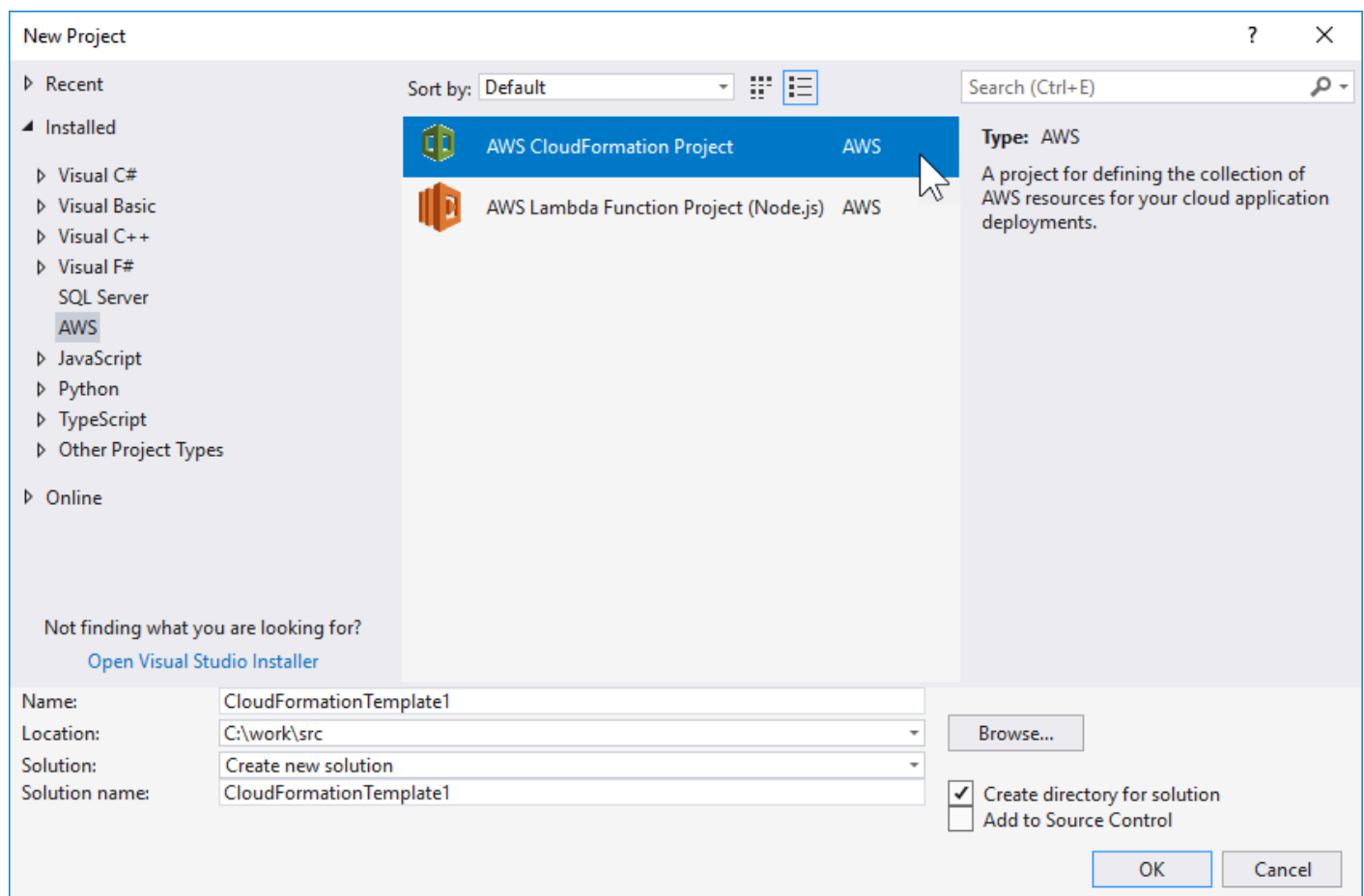
- [Criando um projeto CloudFormation modelo no Visual Studio](#)
- [Implantar um modelo do CloudFormation no Visual Studio](#)
- [Formatar um modelo do CloudFormation no Visual Studio](#)

Criando um projeto CloudFormation modelo no Visual Studio

Para criar um projeto de modelo

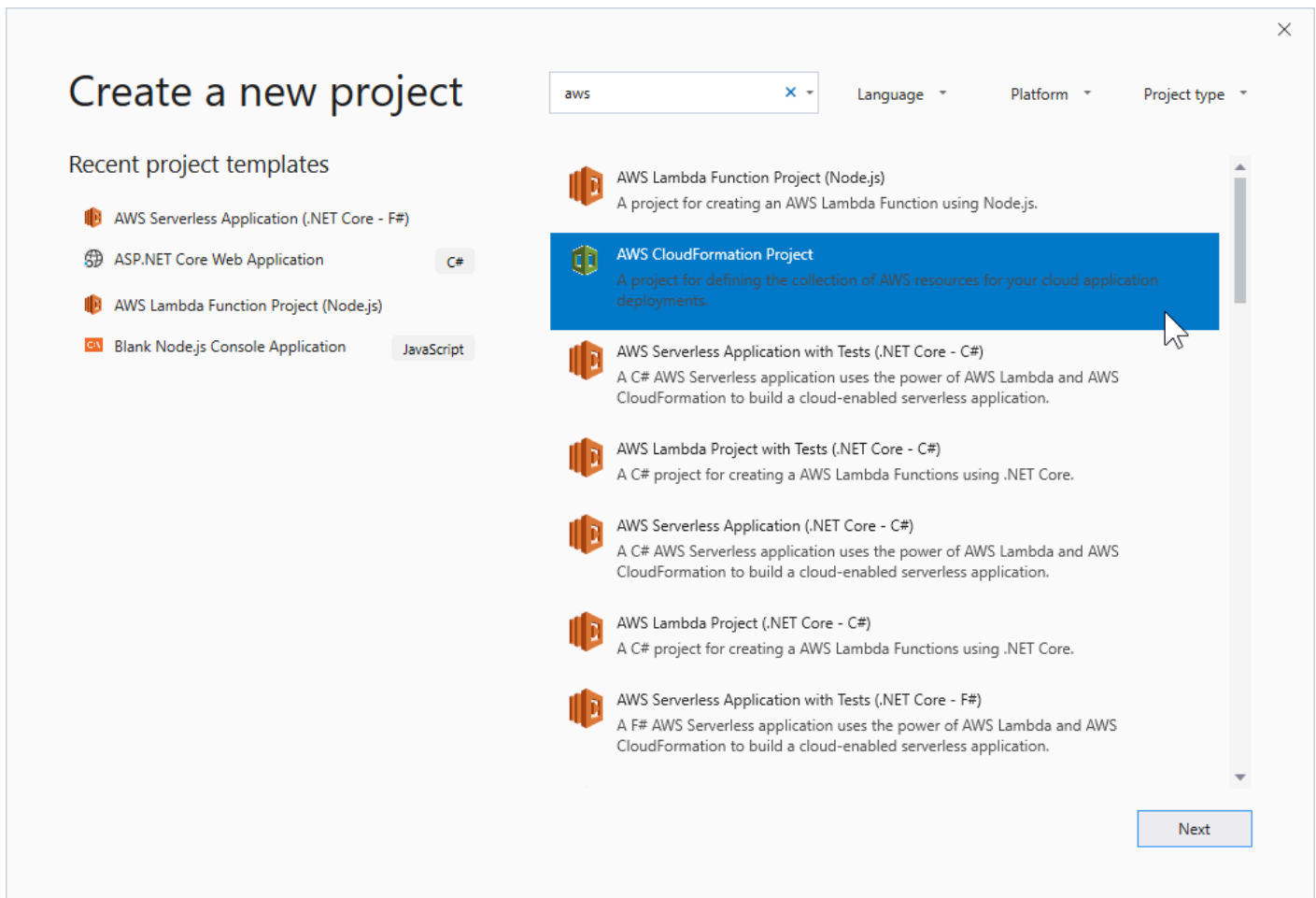
1. No Visual Studio, escolha File (Arquivo), New (Novo) e Project (Projeto).
2. No Visual Studio 2017:

Na caixa de diálogo No projeto, expanda Instalado e selecione AWS.



No Visual Studio 2019:

Na caixa de diálogo Novo projeto, verifique se as caixas suspensas Idioma, Plataforma e Tipo de projeto estão definidas como “Todos...” e digite aws no campo Pesquisar.



3. Selecione o modelo AWS CloudFormation do projeto.

4. No Visual Studio 2017:

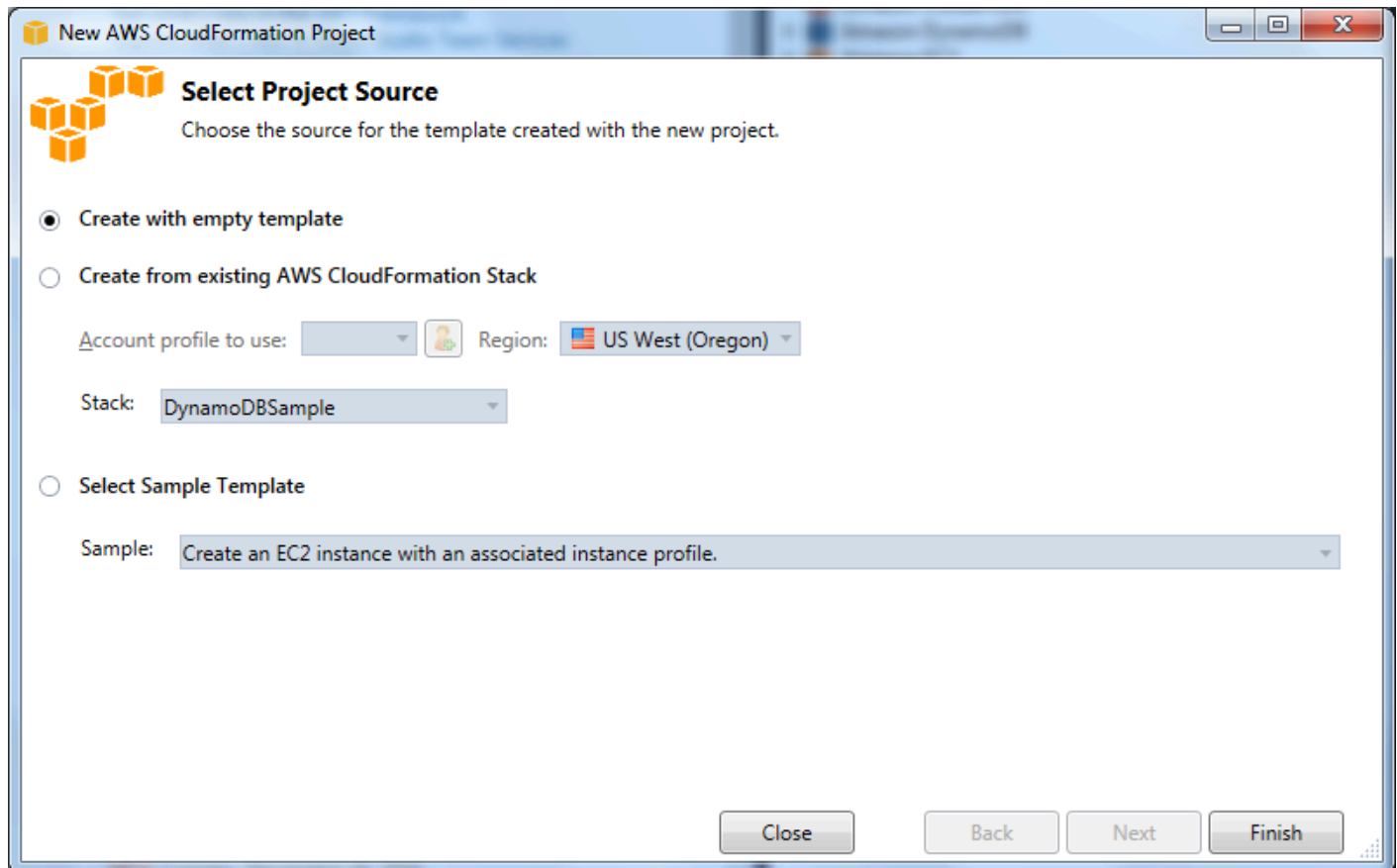
Digite o Name (Nome), o Location (Local) etc. para o seu projeto de modelo e, depois, clique em OK.

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 CloudFormation vazio.
- Criar a partir da pilha AWS |CFN| existente gera um modelo a partir de uma pilha existente em sua conta. AWS (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 CloudFormation .

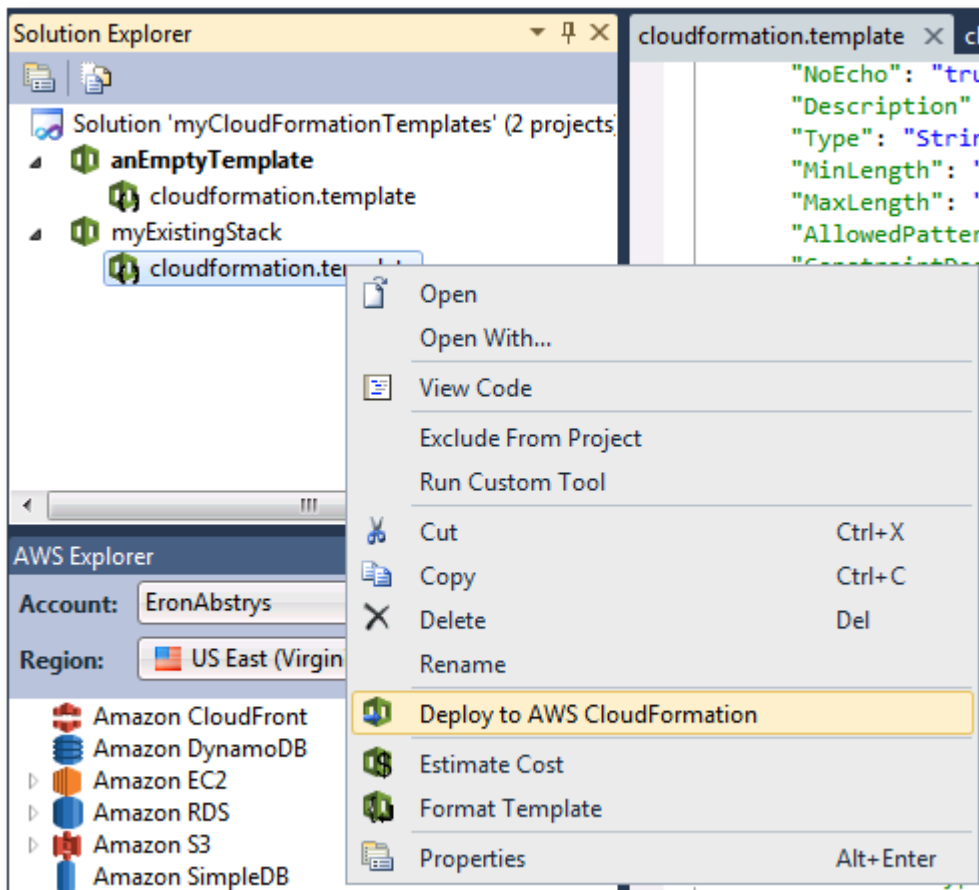


6. Para concluir a criação do seu projeto CloudFormation modelo, escolha Concluir.

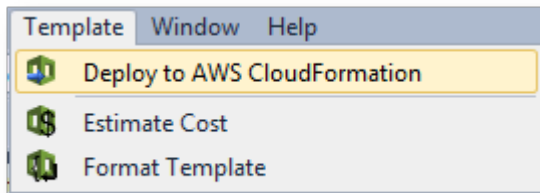
Implantar um modelo do CloudFormation no Visual Studio

Para implantar um modelo do CFN

1. No Solution Explorer, abra o menu de contexto (clique com o botão direito) do modelo que você deseja implantar e escolha Implantar no AWS CloudFormation.



Como alternativa, para implantar o modelo que você está editando no momento, no menu Modelo, escolha Implantar no AWS CloudFormation.



2. Na página Implantar modelo, escolha a Conta da AWS a ser usada para executar a pilha e a região onde ele será executado.

Deploy Template

Select Template

To create a stack, fill in the name for your stack and select a template. You may choose one of the sample templates to get started quickly or on your local hard drive.

Account to use: EronAbstrys Region: US East (Virginia)

Create New Stack

SNS Topic (Optional):

Creation Timeout: None

Rollback on failure

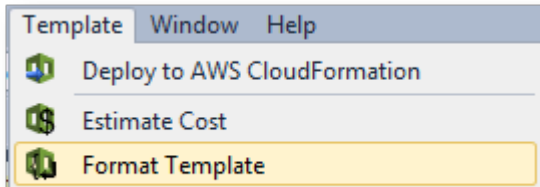
Update Existing Stack

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 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 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.

Note

Para usar essa ferramenta, a política do IAM deve conceder permissões para as ações `s3:GetBucketAcl`, `s3:GetBucket` e `s3:ListBucket`. Para obter mais informações, consulte [Visão geral das políticas AWS 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

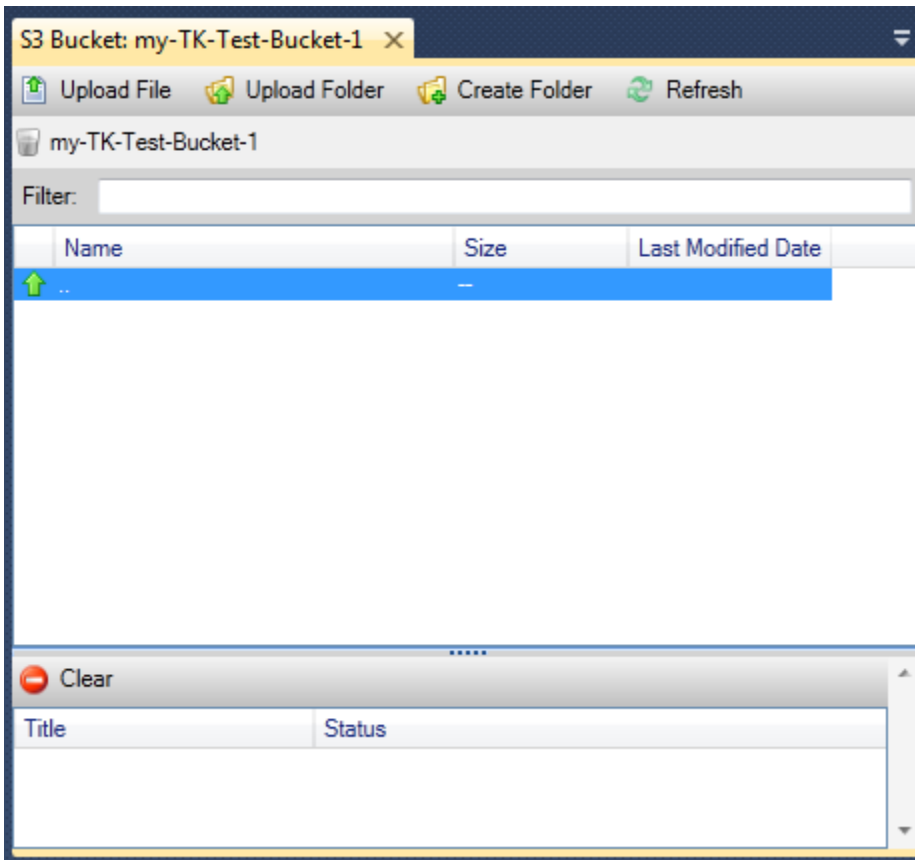
1. No AWS Explorer, abra o menu de contexto (clique com o botão direito do mouse) do nó Amazon S3 e escolha Create Bucket.
2. Na caixa de diálogo Create Bucket (Criar bucket), digite um nome para o bucket. Os nomes de bucket devem ser exclusivos em toda a AWS. Para obter informações sobre outras restrições, acesse a [documentação do Amazon S3](#).
3. Escolha OK.

Gerenciando buckets do Amazon S3 a partir do Explorer AWS

No AWS Explorer, as seguintes operações estão disponíveis quando você abre um menu de contexto (clique com o botão direito do mouse) para 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 no AWS Explorer.



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 na AWS.
 - todos com acesso à Internet.
- Ative o registro em log para o bucket.
- Configure uma notificação usando o Amazon Simple Notification Service (Amazon SNS) para que, se estiver usando o Reduced Redundancy Storage (RRS), receba uma notificação em caso de perda de dados. O RRS é uma opção de armazenamento do Amazon S3 que oferece menor durabilidade do que o armazenamento padrão, mas por um custo reduzido. Para obter mais informações, consulte [S3 FAQs](#).
- Crie um site estático usando os dados no bucket.

Política

Permite que você configure políticas AWS Identity and Access Management (IAM) para seu 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 carregamentos fracionados. O Amazon S3 permite dividir grandes carregamentos 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 usar o AWS Explorer para transferir arquivos ou pastas inteiras do seu computador local para qualquer um dos seus buckets.

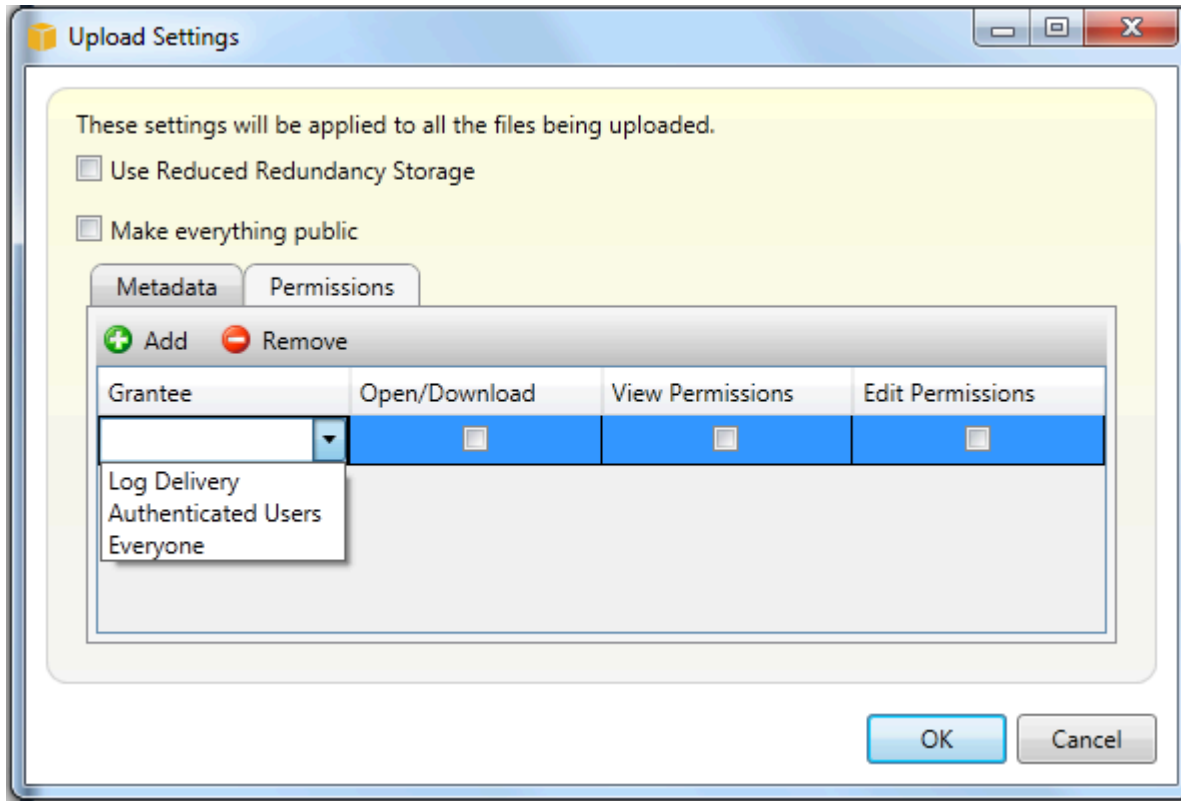
Note

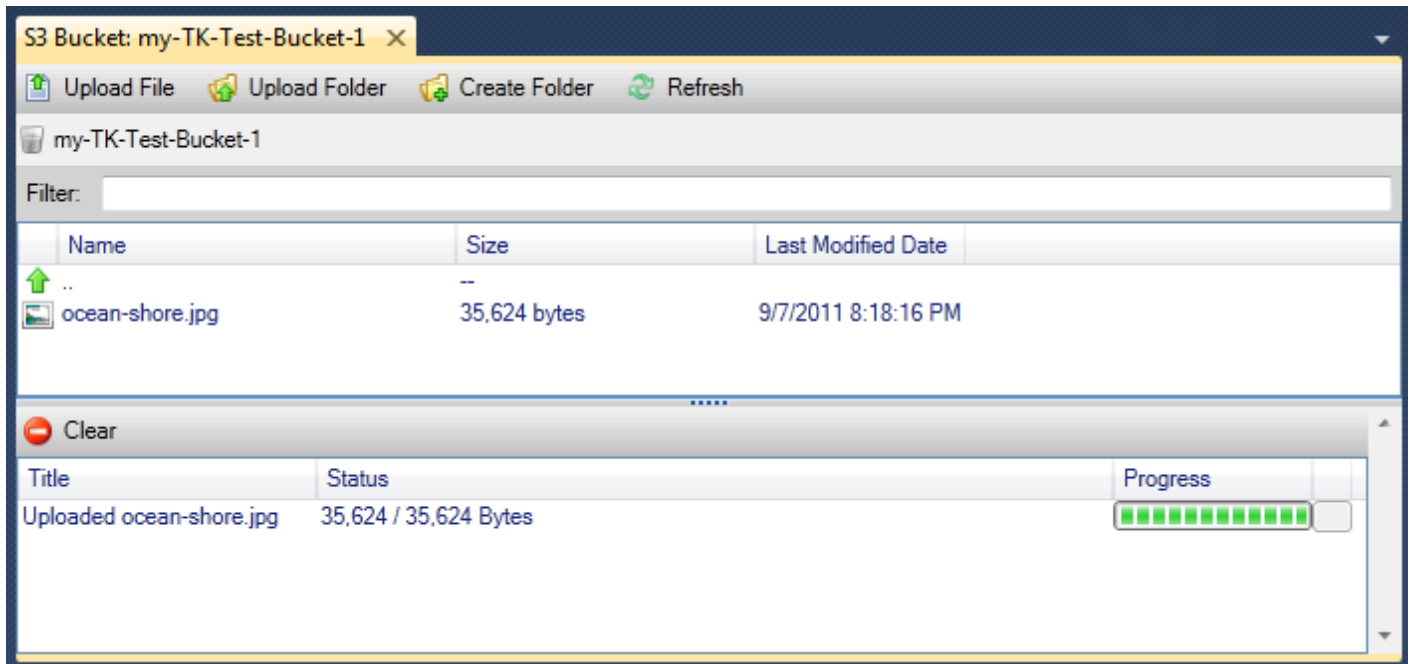
Se você carregar arquivos ou pastas que tenham o mesmo nome de arquivos ou pastas existentes no bucket do Amazon S3, os arquivos carregados substituirão os existentes sem avisar.

Para fazer upload de um arquivo no S3

1. No AWS Explorer, expanda o nó do Amazon S3 e clique duas vezes em um bucket ou abra o menu de contexto (clique com o botão direito do mouse) do bucket e escolha Browse.
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).

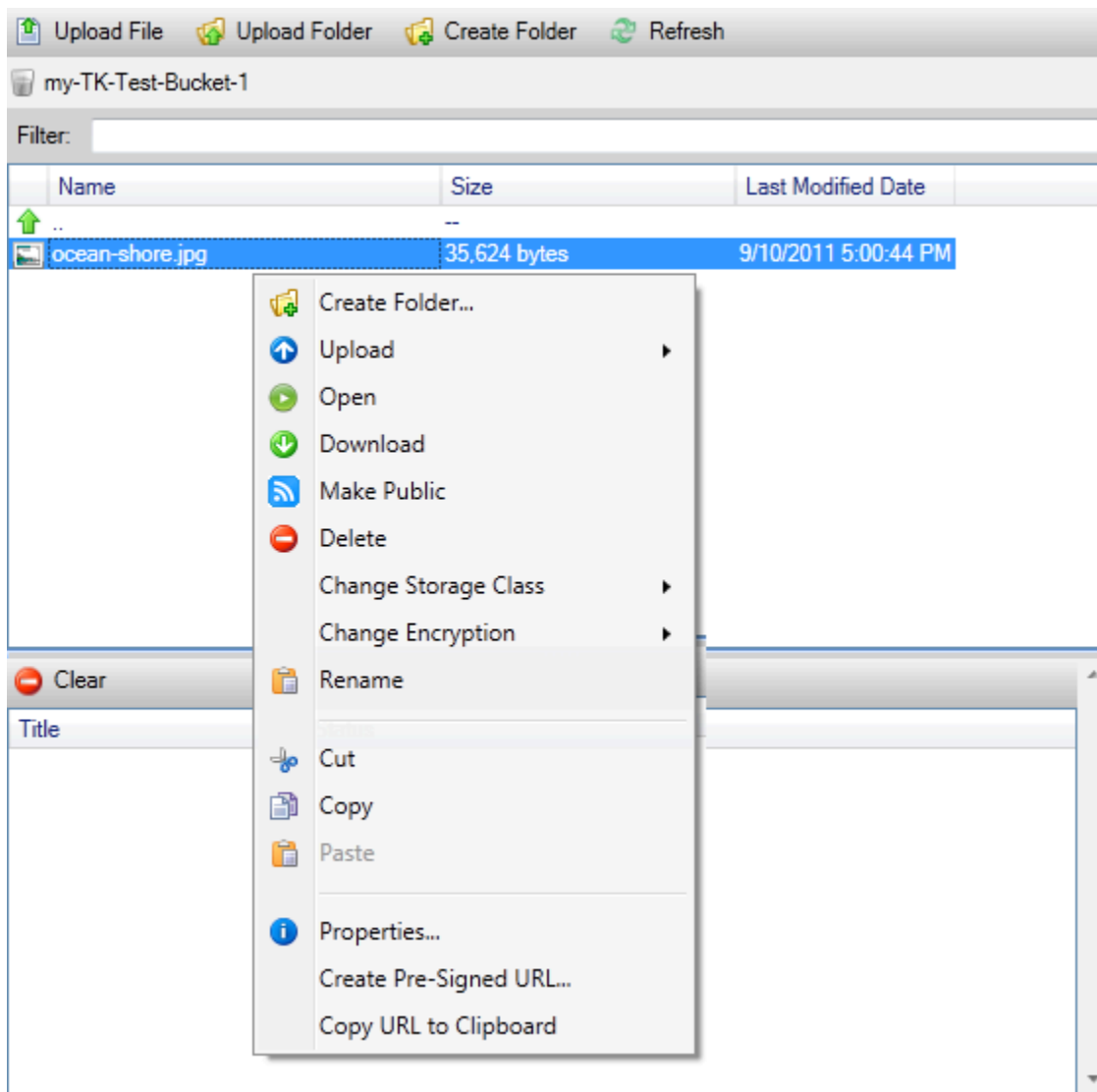
A caixa de diálogo Upload Settings (Configurações de upload) permite definir metadados e permissões nos arquivos ou na pasta que você está fazendo upload. Marcar a caixa de seleção Make everything public (Tornar tudo público) equivale a configurar as permissões Open/Download (Abrir/fazer download) para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





Operações de arquivos do Amazon S3 a partir do AWS Toolkit for Visual Studio

Se escolher um arquivo na visualização do Amazon S3 e abrir o menu de contexto (clizando com o botão direito), 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) para permitir o download do arquivo selecionado.

Tornar público

Define permissões no arquivo selecionado para Abrir/baixar e 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).

Alterar 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.

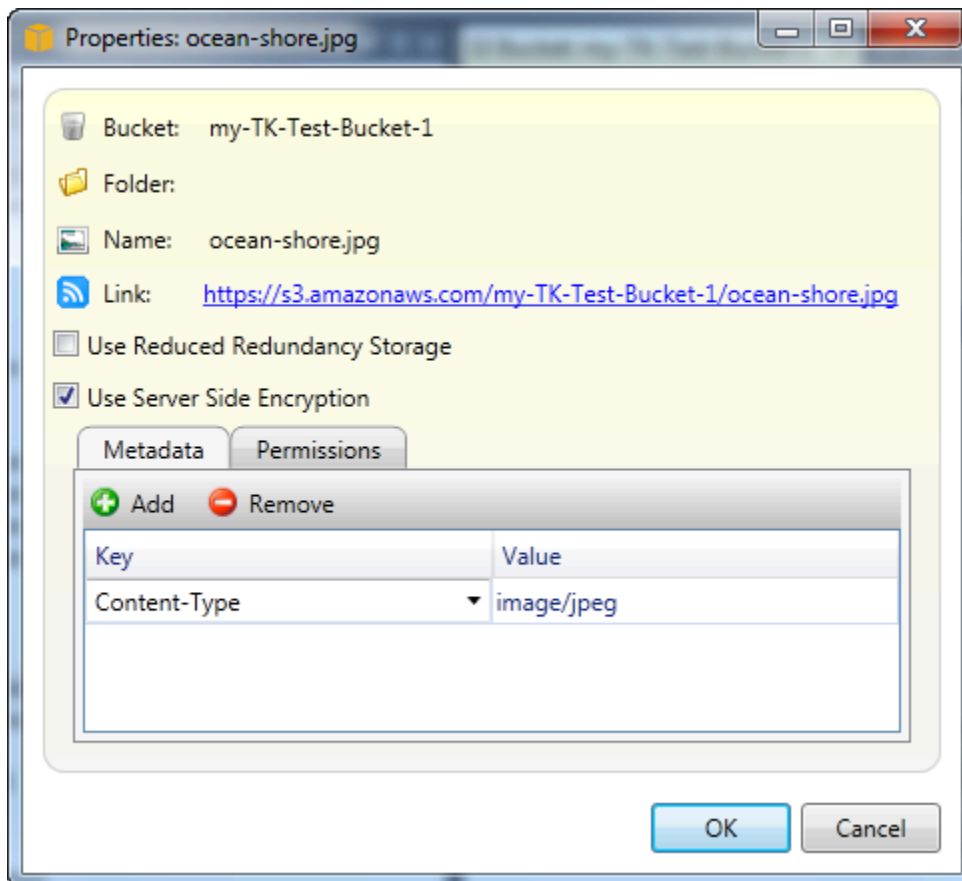
Cortar | Copiar | Colar

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 kit de ferramentas para 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 que você crie e distribua URLs pré-assinado.



Criar Pre-Signed URL

Permite criar um URL pré-assinado com tempo limitado que você pode distribuir para possibilitar que outras pessoas acessem o conteúdo armazenado no Amazon S3.

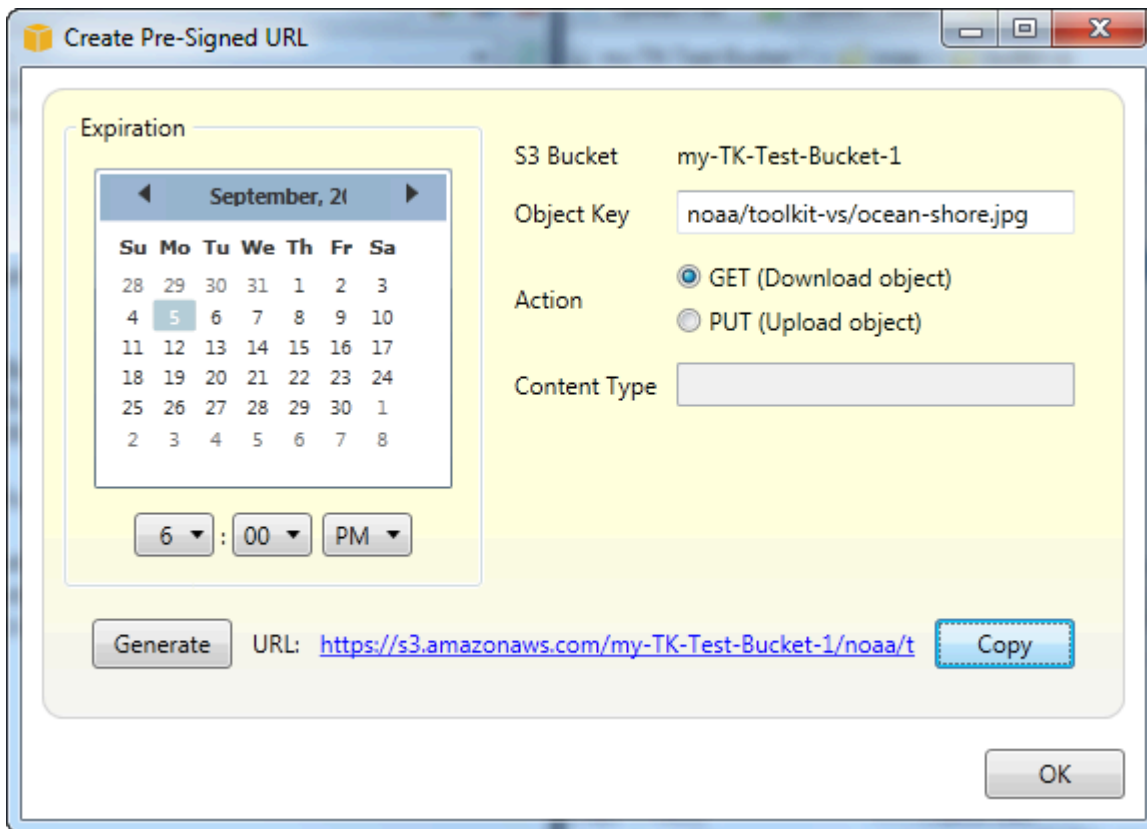
Como criar um pre-signed URL

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.

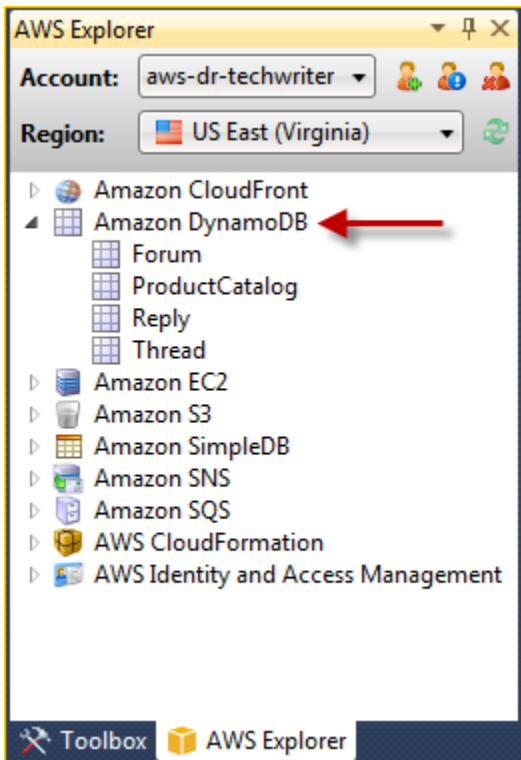
2. Escolha o botão Generate (Gerar).
3. Para copiar o URL para a área de transferência, escolha Copy (Copiar).



AWSUsar o DynamoDB no Explorer

O Amazon DynamoDB é um serviço de banco de dados rápido, altamente dimensionável, altamente disponível, 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 kit de ferramentas para Visual Studio oferece a funcionalidade para trabalhar com o DynamoDB em um contexto de desenvolvimento. Para obter mais informações sobre o DynamoDB, consulte [DynamoDB](#) no site da Amazon Web Services.

No kit de ferramentas para Visual Studio, o AWS Explorer exibe todas as tabelas do DynamoDB associadas à Conta da AWS ativa.



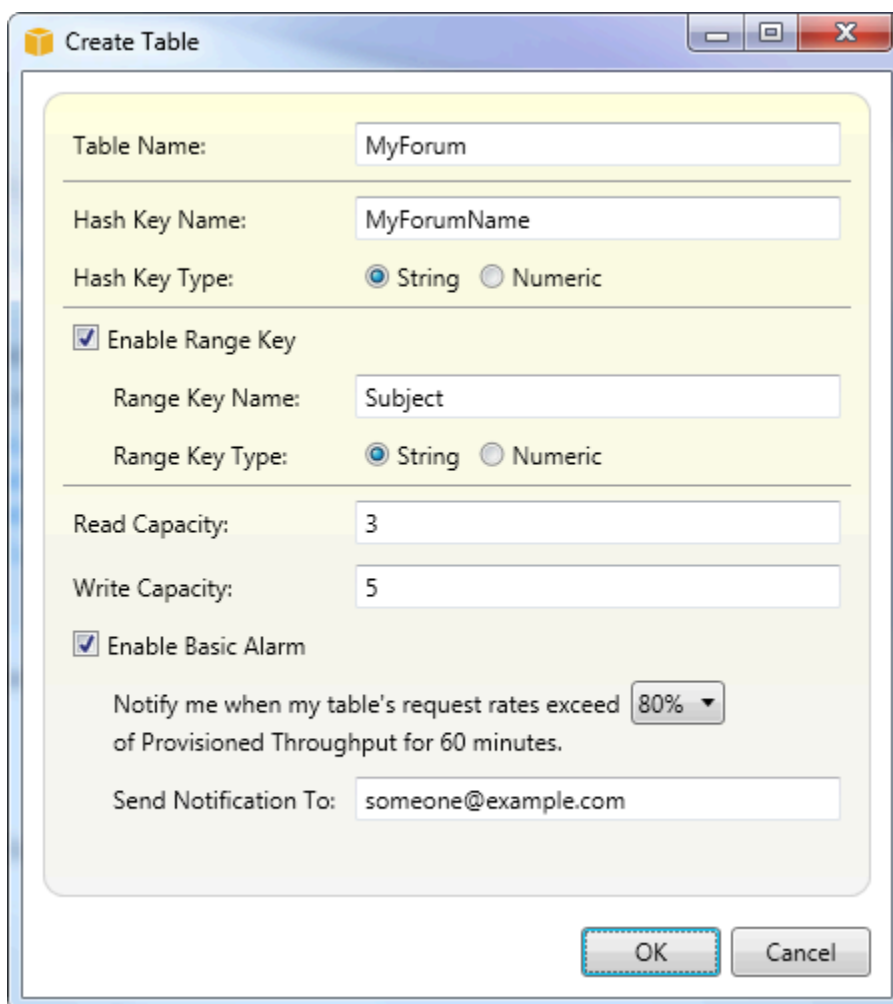
Criar uma tabela do DynamoDB

Você pode usar o kit de ferramentas para Visual Studio para criar uma tabela do DynamoDB.

Como criar uma tabela no AWS Explorer

1. No AWS Explorer, abra o menu de contexto (clique com o botão direito) do Amazon DynamoDB e escolha Criar tabela.
2. No assistente Create Table (Criar tabela), em Table Name (Nome da tabela), digite um nome para a tabela.
3. No campo Nome da chave de hash, digite um atributo de chave de hash primária e, nos botões Tipo de chave de hash, 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, acesse a seção [Chave primária](#) no Guia 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.



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

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

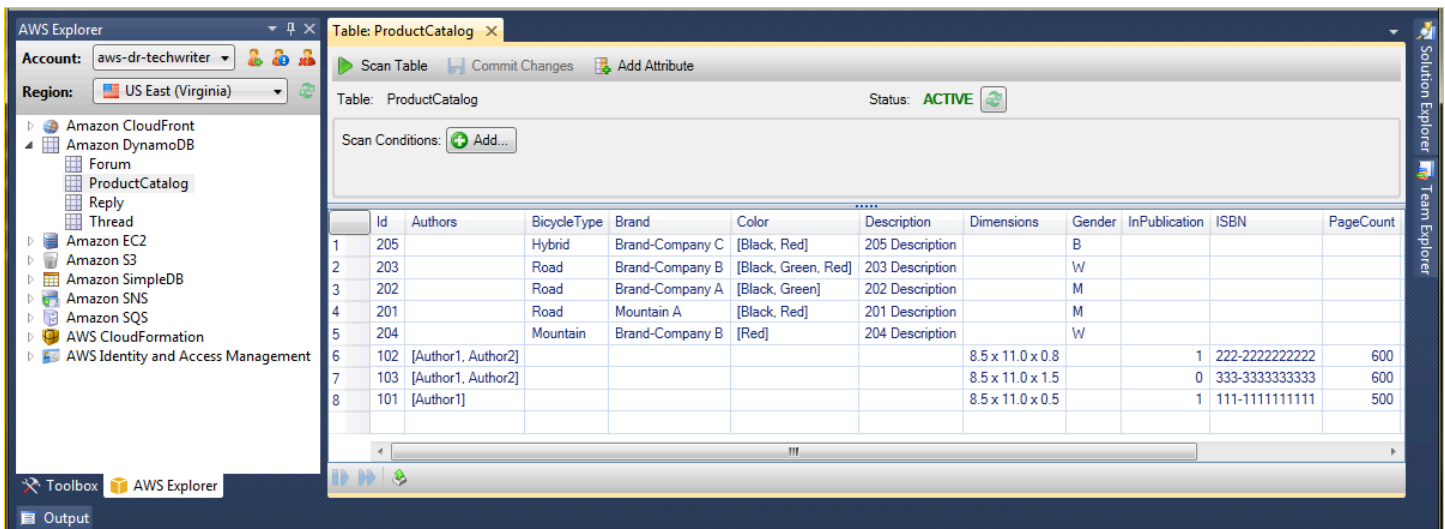
Buttons: OK, Cancel

Para obter mais informações sobre tabelas do DynamoDB, acesse [Tabelas, itens e atributos](#).

Visualizar uma tabela do DynamoDB como uma grade

Para abrir uma visualização em grade das tabelas do DynamoDB, no AWS Explorer, 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	222-222222222	600
7	103	[Author1, Author2]					8.5 x 11.0 x 1.5		0	333-333333333	600
8	101	[Author1]					8.5 x 11.0 x 0.5		1	111-111111111	500

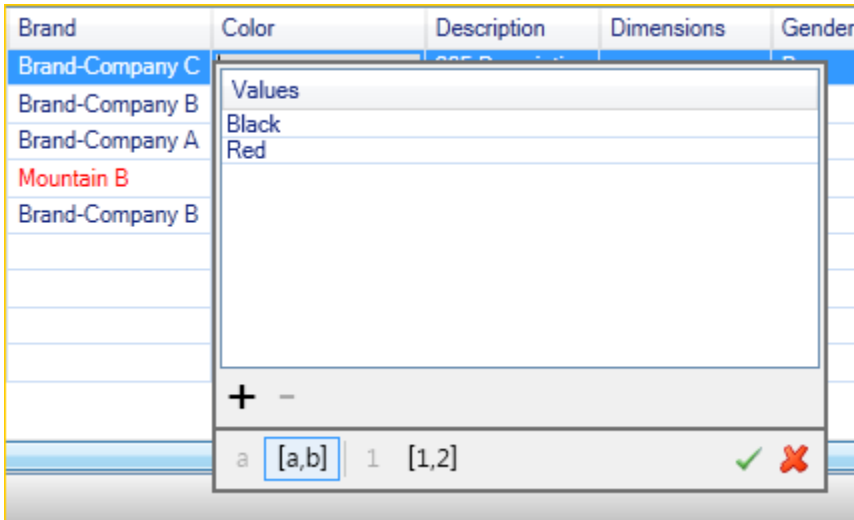
Editar e adicionar atributos e valores

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.

Brand	Color
Brand-Company C	[Black, Red]
Brand-Company B	[Black, Green, Red]
Brand-Company A	[Black, Green]
a	[a,b] 1 [1,2] ✓ ✗

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.

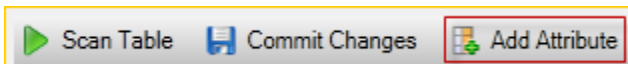


Depois de editar o valor do atributo, escolha a marca de seleção verde para confirmar as alterações. Se você quiser descartar as alterações, escolha o X vermelho.

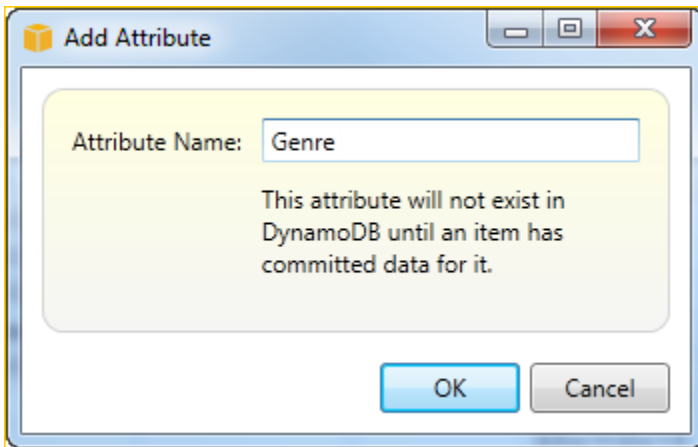
Depois que você tiver confirmado as alterações, o valor do atributo será exibido em vermelho. Isso indica que o atributo foi atualizado e que o novo valor não foi regravado no banco de dados do DynamoDB. Para regravar as alterações no DynamoDB, escolha Confirmar alterações. Para descartar as alterações, 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

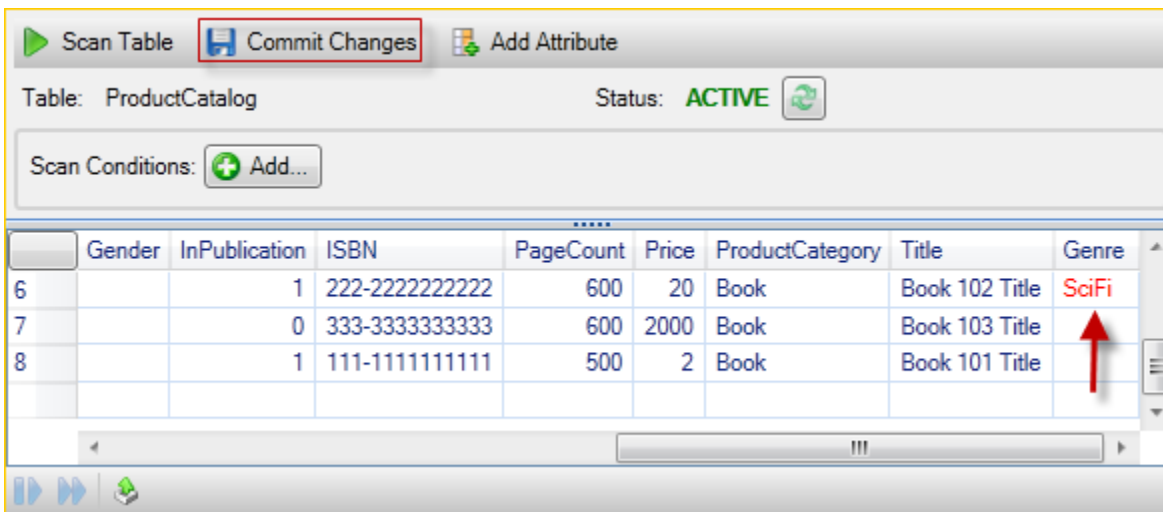
Na visualização em grade, você também pode adicionar atributos à tabela. Para adicionar um novo atributo, escolha Add Attribute (Adicionar atributo).



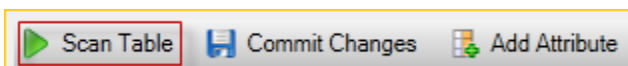
Na caixa de diálogo Add Attribute (Adicionar atributo), digite um nome para o atributo e escolha OK.



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).



Realizar verificações em uma tabela do DynamoDB



Você pode realizar verificações nas tabelas do DynamoDB usando o kit de ferramentas. 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 verificação, consulte o Guia do desenvolvedor do Amazon DynamoDB.

Como realizar uma verificação em uma tabela do DynamoDB no AWS Explorer

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.

Scan Table Commit Changes Add Attribute

Table: ProductCatalog Status: ACTIVE

Scan Conditions: Add...

Match: Brand as: String if: Contain: A

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

Para 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.

Usar o AWS CodeCommit com o Visual Studio Team Explorer

Você pode usar as contas de usuário do AWS Identity and Access Management (IAM) para criar credenciais do Git e utilizá-las para criar e clonar repositórios dentro do Team Explorer.

Tipos de credencial do AWS CodeCommit

A maioria dos usuários do AWS Toolkit for Visual Studio está ciente da configuração de perfis de credencial da AWS que contêm as respectivas chaves de acesso e secretas. Esses perfis de credenciais são usados no kit de ferramentas para Visual Studio para permitir as chamadas de APIs de serviço; por exemplo, para listar buckets do Amazon S3 no AWS Explorer ou executa 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 mais sobre essas credenciais (um nome de usuário e senha) em [Configuração para usuários de HTTPS usando credenciais do Git](#) no Guia do usuário do AWS CodeCommit.

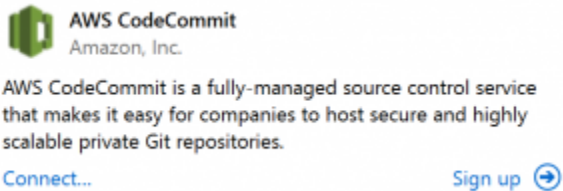
Você pode criar as credenciais do Git para o AWS CodeCommit apenas para contas de usuário do IAM. Você não pode criá-las para uma conta raiz. Você pode criar até dois conjuntos dessas credenciais para o serviço e, embora possa marcar um conjunto de credenciais como inativo, os conjuntos inativos continuam contando para o limite de dois conjuntos. Você pode excluir e recriar credenciais a qualquer momento. Quando você usa o AWS CodeCommit dentro do Visual Studio, as credenciais da AWS tradicionais são utilizadas 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 para o AWS CodeCommit, o kit de ferramentas para Visual Studio cria e gerencia automaticamente essas credenciais do Git para você e as associa ao perfil de credencial da

AWS. Você não precisa se preocupar em ter conjunto certo de credenciais à disposição para realizar operações do Git dentro do Team Explorer. Assim que você se conecta ao Team Explorer com o perfil de credencial da AWS, as credenciais do Git associadas são usadas automaticamente sempre que você trabalha com um Git remoto.

Como se conectar à AWS CodeCommit

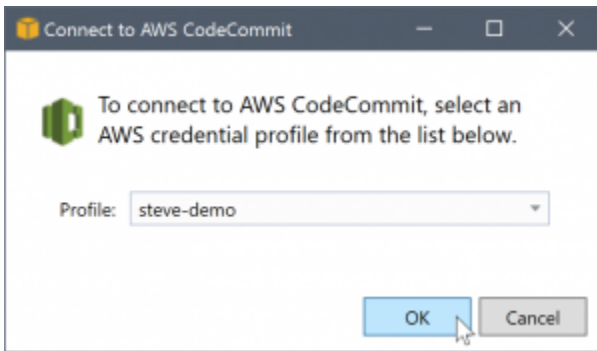
Ao abrir a janela Team Explorer no Visual Studio de 2015 ou posterior, você verá uma entrada do AWS CodeCommit na seção Hosted Service Providers de Manage Connections.



Escolher Cadastre-se abre a página inicial da Amazon Web Services em uma janela do navegador. O que acontece quando você escolhe Conectar depende de o kit de ferramentas para Visual Studio conseguir encontrar um perfil de credencial com chaves de acesso e secreta da AWS para fazer chamadas à AWS em seu nome. É possível configurar um perfil de credencial usando a nova página Conceitos básicos exibida no IDE quando o kit de ferramentas para Visual Studio não consegue encontrar credenciais armazenadas localmente. Ou talvez você esteja usando o kit de ferramentas para Visual Studio, o AWS Tools for Windows PowerShell ou a AWS CLI e já tenha perfis de credencial da AWS disponíveis para o kit de ferramentas para Visual Studio usar.

Ao escolher Conectar, o kit de ferramentas para Visual Studio inicia o processo para encontrar um perfil de credencial a ser usado na conexão. Se o kit de ferramentas para Visual Studio não conseguir encontrar um perfil de credencial, ele abrirá uma caixa de diálogo solicitando que você insira as chaves de acesso e secretas para a Conta 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 kit de ferramentas para Visual Studio encontrar mais de um perfil de credencial da AWS, você deverá selecionar a conta que deseja usar dentro do Team Explorer.



Se você tiver apenas um perfil de credencial, o kit de ferramentas para Visual Studio ignorará a caixa de diálogo de seleção do perfil e a conexão será estabelecida 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.

Manage Connections ▾

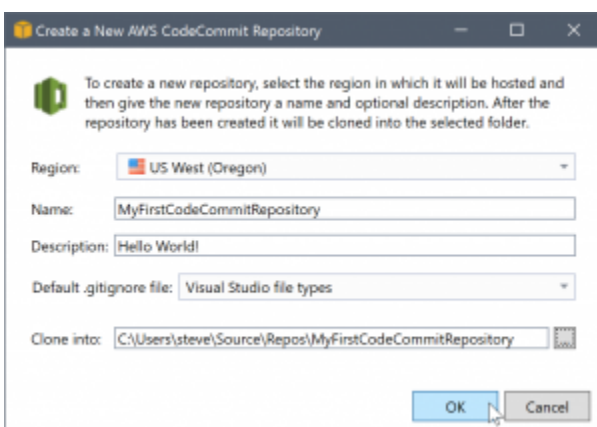
▲ AWS CodeCommit
Clone | Create | Sign out steve-demo

Como você não tem repositórios clonados localmente, o painel mostra apenas as operações que você pode realizar: Clone (Clonar), Create (Criar) e Sign out (Sair). Assim como outros provedores, o AWS CodeCommit no Team Explorer só pode ser vinculado a um perfil de credencial da AWS em um dado 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

Ao clicar no link Criar, a caixa de diálogo Criar um repositório do AWS CodeCommit 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 kit de ferramentas para Visual Studio solicita que o serviço crie o repositório e clone 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 e que o kit de ferramentas para Visual Studio requer acesso às credenciais do Git descritos anteriormente.

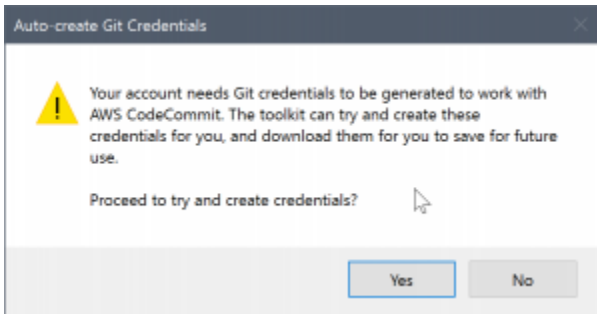
Configurar credenciais do Git

Até esse ponto, você usou chaves de acesso e secretas da AWS para solicitar que o serviço criasse o repositório. Agora você precisa trabalhar com o Git propriamente dito para fazer a operação de clonagem real, mas o Git não reconhece chaves de acesso e secretas da AWS. 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.

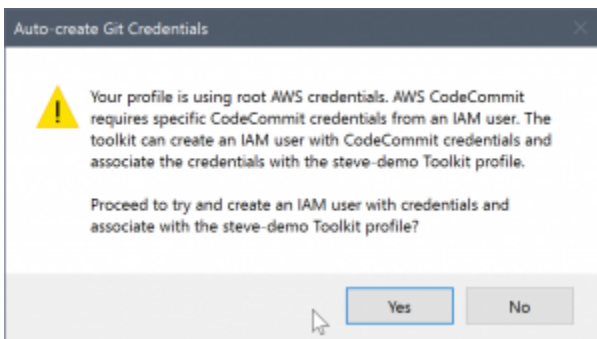
Conforme observado em [Configurar credenciais do Git](#), as credenciais do Git que você usará devem ser associadas a um usuário do IAM. Você não pode gerá-las para credenciais raiz. Você deve sempre configurar os perfis de credencial da AWS para conter chaves de acesso e secretas de usuário do IAM, e não as chaves raiz. O kit de ferramentas para Visual Studio pode tentar configurar credenciais do Git para o AWS CodeCommit em seu nome e associá-las ao perfil de credencial da AWS que você usou para se conectar ao Team Explorer anteriormente.

Ao escolher OK na caixa de diálogo Criar um repositório do AWS CodeCommit e criar com êxito o repositório, o kit de ferramentas para Visual Studio verifica o perfil de credencial da AWS conectado

ao Team Explorer para determinar se as credenciais do Git para o AWS CodeCommit existem e estão associadas localmente ao perfil. Em caso positivo, o kit de ferramentas para 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 kit de ferramentas para Visual Studio verificará o tipo das 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.

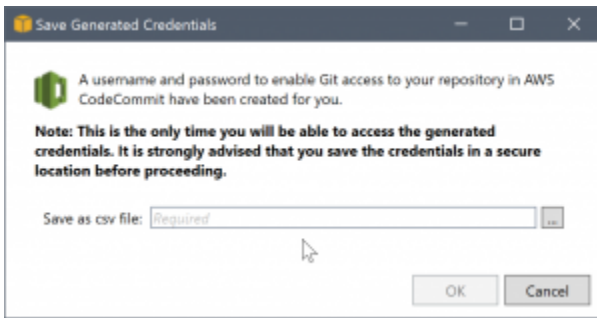


Se as credenciais forem credenciais raiz, a mensagem a seguir será mostrada em seu lugar.



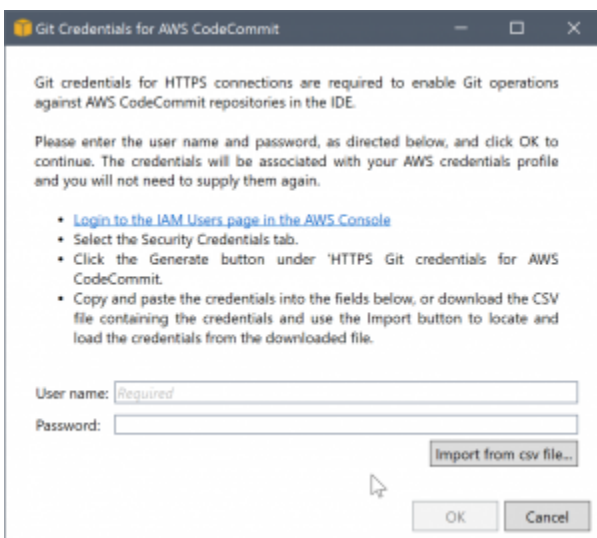
Em ambos os casos, o kit de ferramentas para Visual Studio se oferece para tentar criar as credenciais do Git necessárias em seu nome. No primeiro cenário, tudo o que precisa ser feito é criar um conjunto de credenciais do Git para o usuário do IAM. Quando uma conta raiz estiver em uso, o kit de ferramentas para Visual Studio primeiro tentará criar um usuário do IAM e, em seguida, criar credenciais do Git para esse novo usuário. Se o kit de ferramentas para Visual Studio precisar criar um usuário, ele aplicará a política gerenciada de usuário avançado do AWS CodeCommit a 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. Por isso, o kit de ferramentas para Visual Studio solicita que você salve as credenciais recém-criadas como um arquivo `.csv` 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 kit de ferramentas para Visual Studio não consiga criar automaticamente as credenciais. Por exemplo, talvez você já tenha criado o número máximo de conjuntos de credenciais do Git (dois) para o AWS CodeCommit ou não tenha direitos programáticos suficientes para o kit de ferramentas para Visual Studio fazer esse trabalho (se tiver feito login como um usuário do IAM). Nesses casos, você pode fazer login no Console de gerenciamento da AWS para gerenciar as credenciais ou obtê-las junto ao administrador. Você pode inseri-las na caixa de diálogo Credenciais do Git para o AWS CodeCommit exibida pelo kit de ferramentas para Visual Studio.

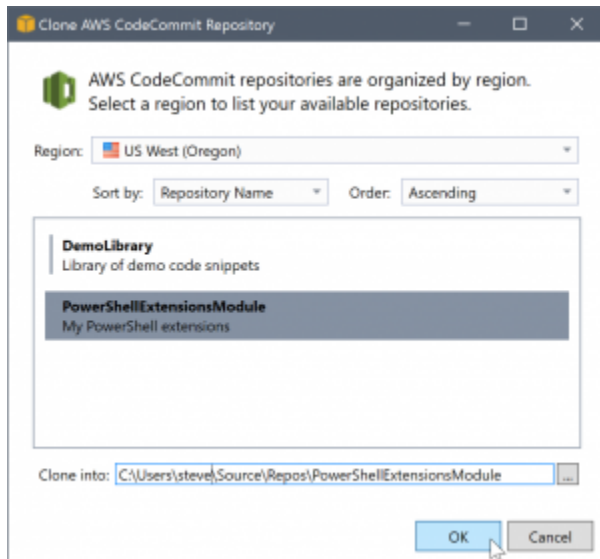


Agora que as credenciais do Git estão disponíveis, a operação de clonagem do novo repositório continua (consulte a indicação do progresso da operação dentro do Team Explorer). Se você tiver optado por aplicar um arquivo `.gitignore` padrão, ele será confirmado para o repositório com um comentário 'Initial 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 repositórios no futuro será a própria caixa de diálogo Criar um repositório do AWS CodeCommit.

Clonar um repositório

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



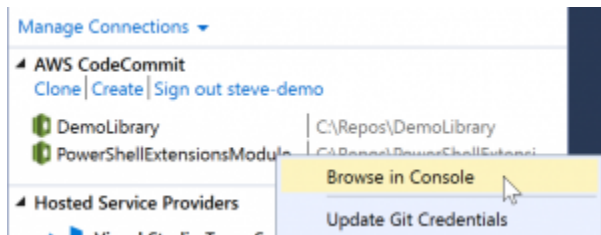
Assim que você escolher a região, o kit de ferramentas para Visual Studio consultará o serviço para descobrir os repositórios disponíveis na região e exibi-los na parte central da lista da caixa de diálogo. O nome e a descrição opcional de cada repositório também são exibidos. Você pode reorganizar a 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.

Trabalho com repositórios

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 a caixa de diálogo Credenciais do Git para o AWS CodeCommit, na qual 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. Como as credenciais do Git já estão armazenadas localmente e associadas ao perfil de credencial da AWS conectado, não deveremos fornecê-las novamente para operações em relação ao AWS CodeCommit remoto.

Usar o CodeArtifact no Visual Studio

O AWS CodeArtifact é um serviço de repositório de artefatos totalmente gerenciado que possibilita que as organizações armazenem e compartilhem com facilidade e segurança pacotes de software usados para desenvolvimento de aplicações. É possível usar o CodeArtifact com ferramentas de compilação e gerenciadores de pacotes conhecidos, como as CLIs NuGet e .NET Core e o Visual Studio. Também é possível configurar o CodeArtifact para extrair pacotes de um repositório público externo, como o [NuGet.org](https://www.nuget.org).

No CodeArtifact, os pacotes são armazenados em repositórios que são então armazenados em um domínio. O AWS Toolkit for Visual Studio simplifica a configuração do Visual Studio com repositórios CodeArtifact, facilitando o consumo de pacotes no Visual Studio diretamente do CodeArtifact e do NuGet.org.

Adicione seu repositório do CodeArtifact como uma fonte de pacotes no Visual Studio.

Para consumir pacotes do CodeArtifact, você precisará adicionar o repositório como uma fonte de pacotes no Gerenciador de Pacotes NuGet no Visual Studio.

Como adicionar o repositório como fonte de pacotes

1. No AWS Explorer, navegue até seu repositório no nó AWS CodeArtifact.
2. Abra o menu de contexto (clique com o botão direito) do repositório que você deseja adicionar e selecione Copiar endpoint de origem do NuGet.
3. Navegue até Fontes de pacotes abaixo do nó Gerenciador de Pacotes NuGet no menu Ferramentas > Opções.
4. Em Fontes de pacotes, selecione o sinal de adição (+), edite o nome e cole o URL do endpoint de origem do NuGet que você copiou anteriormente no campo Fonte.
5. Marque a caixa de seleção ao lado da fonte de pacotes recém-adicionada para habilitá-la.

Note

Recomendamos adicionar uma conexão externa com o NuGet.org ao seu CodeArtifact e desabilitar a fonte de pacotes nuget.org no Visual Studio. Ao usar uma conexão externa, todas as dependências extraídas do NuGet.org são armazenadas no CodeArtifact. Se o NuGet.org for desconectado por algum motivo, os pacotes de que você precisa ainda estarão disponíveis. Para obter mais informações sobre conexões externas, consulte [Add an external connection](#) no Guia do usuário do AWS CodeArtifact.

6. Escolha OK para fechar o menu.

Para obter mais informações sobre como usar o CodeArtifact com o Visual Studio, consulte [Usar o CodeArtifact com o Visual Studio](#) no Guia do Usuário do AWS CodeArtifact.

Amazon RDS no AWS Explorer

O Amazon Relational Database Service (Amazon RDS) é um serviço que permite provisionar e gerenciar sistemas de banco de dados relacional SQL na nuvem. O Amazon RDS comporta três tipos de sistema 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 do [Console de Gerenciamento da AWS](#) para o Amazon RDS.

Tópicos

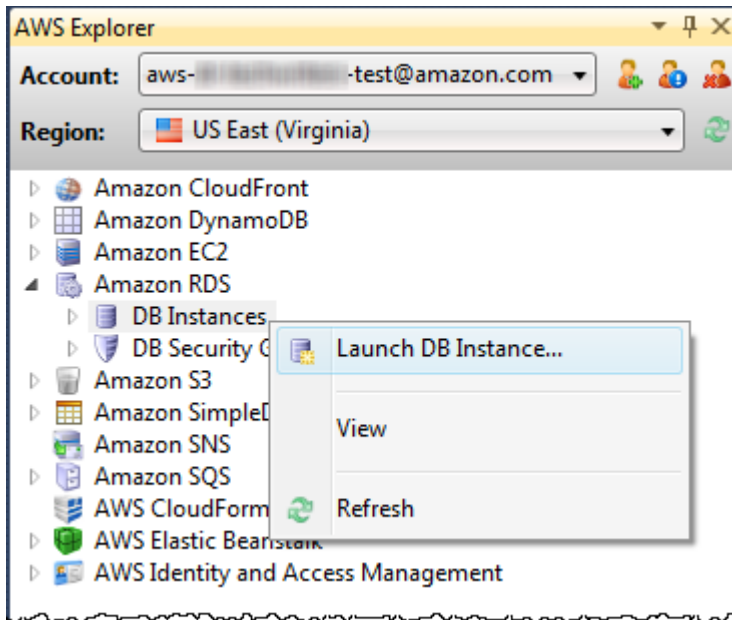
- [Executar uma instância do banco de dados do Amazon RDS](#)
- [Criar um banco de dados do Microsoft SQL Server em uma instância do RDS](#)
- [Grupos de segurança do Amazon RDS](#)

Executar uma instância do banco de dados do Amazon RDS

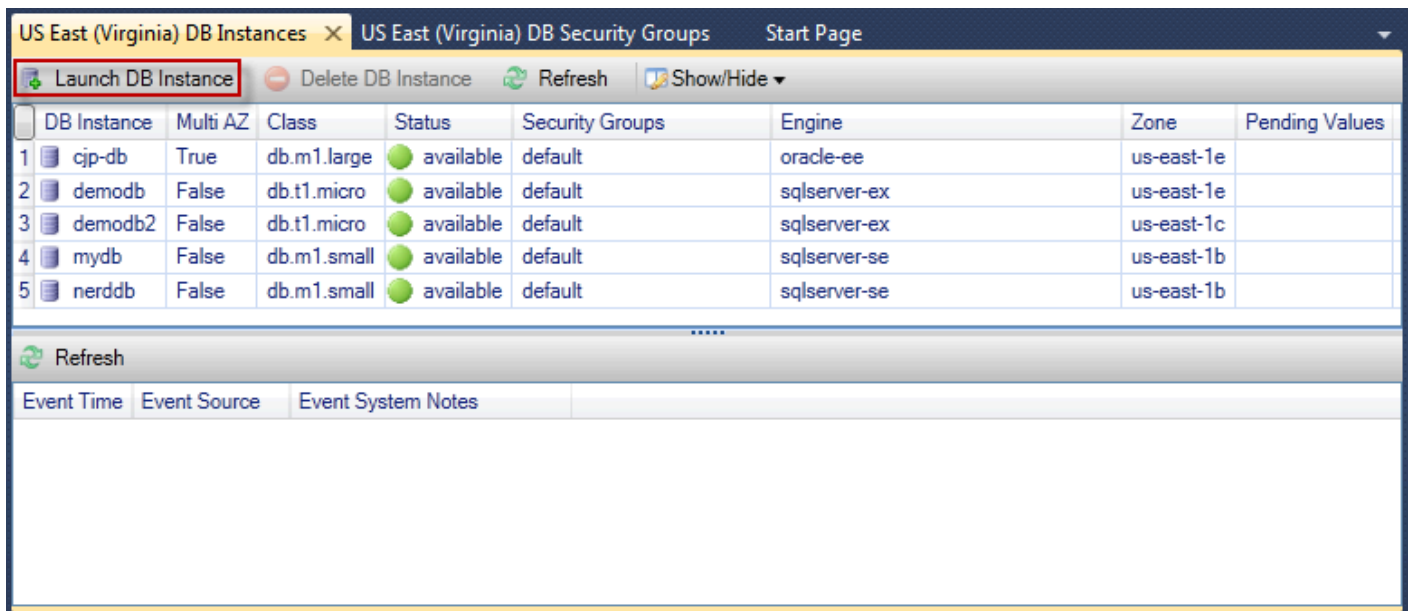
Com o AWS Explorer, você pode executar uma instância de qualquer um dos mecanismos de banco de dados compatíveis com o Amazon RDS. A descrição a seguir mostra a experiência do usuário para executar uma instância do Microsoft SQL Server Standard Edition, mas a experiência do usuário é semelhante em todos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

Para executar uma instância do Amazon RDS

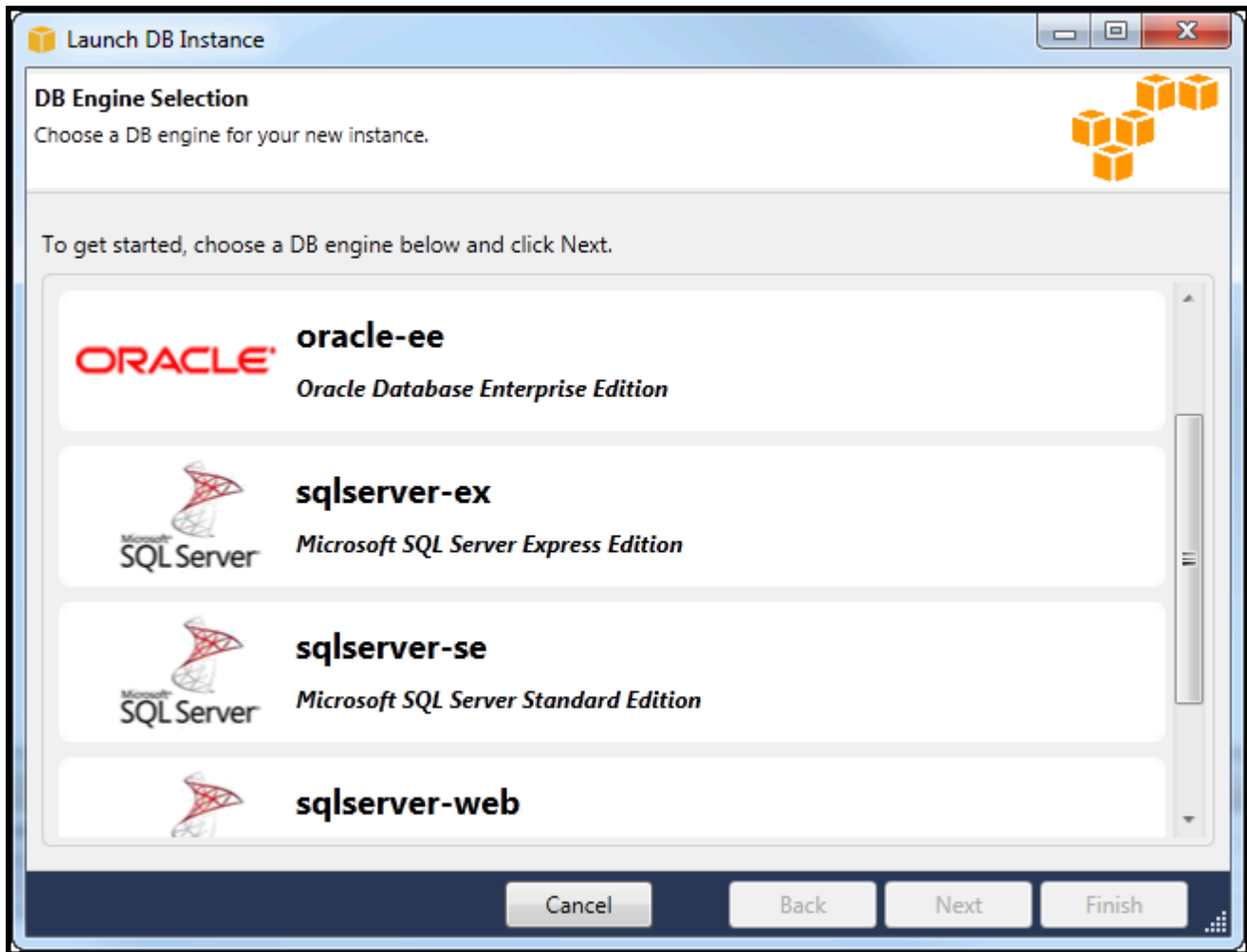
1. No AWS Explorer, abra o menu de contexto (clique com o botão direito) do nó Amazon RDS e escolha Executar instância de banco de dados.



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	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 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 interrupção 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 essa opção para a AWS realizar 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 no AWS Explorer.

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.

Launch DB Instance

DB Engine Instance Options
Configure your DB engine instance.

DB Instance Engine and Class

License Model: *license-included*

DB Engine Version: 10.50.2789.0.v1 (SQL Server 2008 R2 Standard Edition)

DB Instance Class: Small

Perform a multi AZ deployment

Upgrade minor versions automatically

RDS Database Instance

Allocated Storage: 250 GB (Minimum: 250 GB, Maximum 1024 GB)

DB Instance Identifier*: myDB

Master User Name*: myDBAdmin

Master User Password*: ●●●●●●●●

Confirm Password*: ●●●●●●●●

Cancel Back Next Finish

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.

Zona de disponibilidade

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.

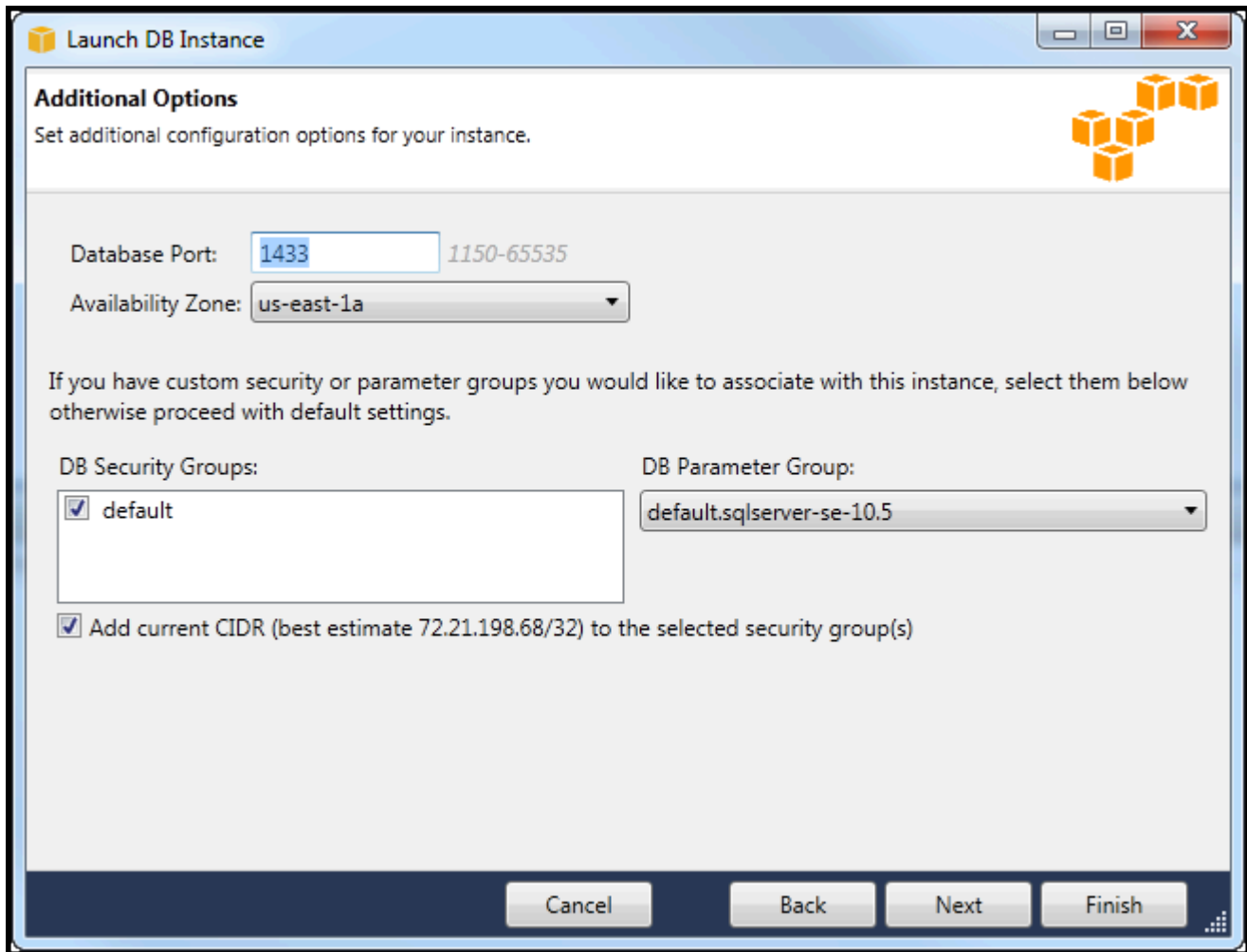
Grupo de segurança do RDS

Selecione um security group (ou grupos) do RDS associado à instância. Os grupos de segurança do RDS especificam o endereço IP, as instâncias do Amazon EC2 e as Contas da AWS com permissão para acessar a instância. Para obter mais informações sobre grupos de segurança do RDS, consulte [Grupos de segurança do Amazon RDS](#). O kit de ferramentas para Visual Studio tenta determinar o endereço IP atual e oferece a opção de adicionar esse endereço aos grupos de segurança 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).

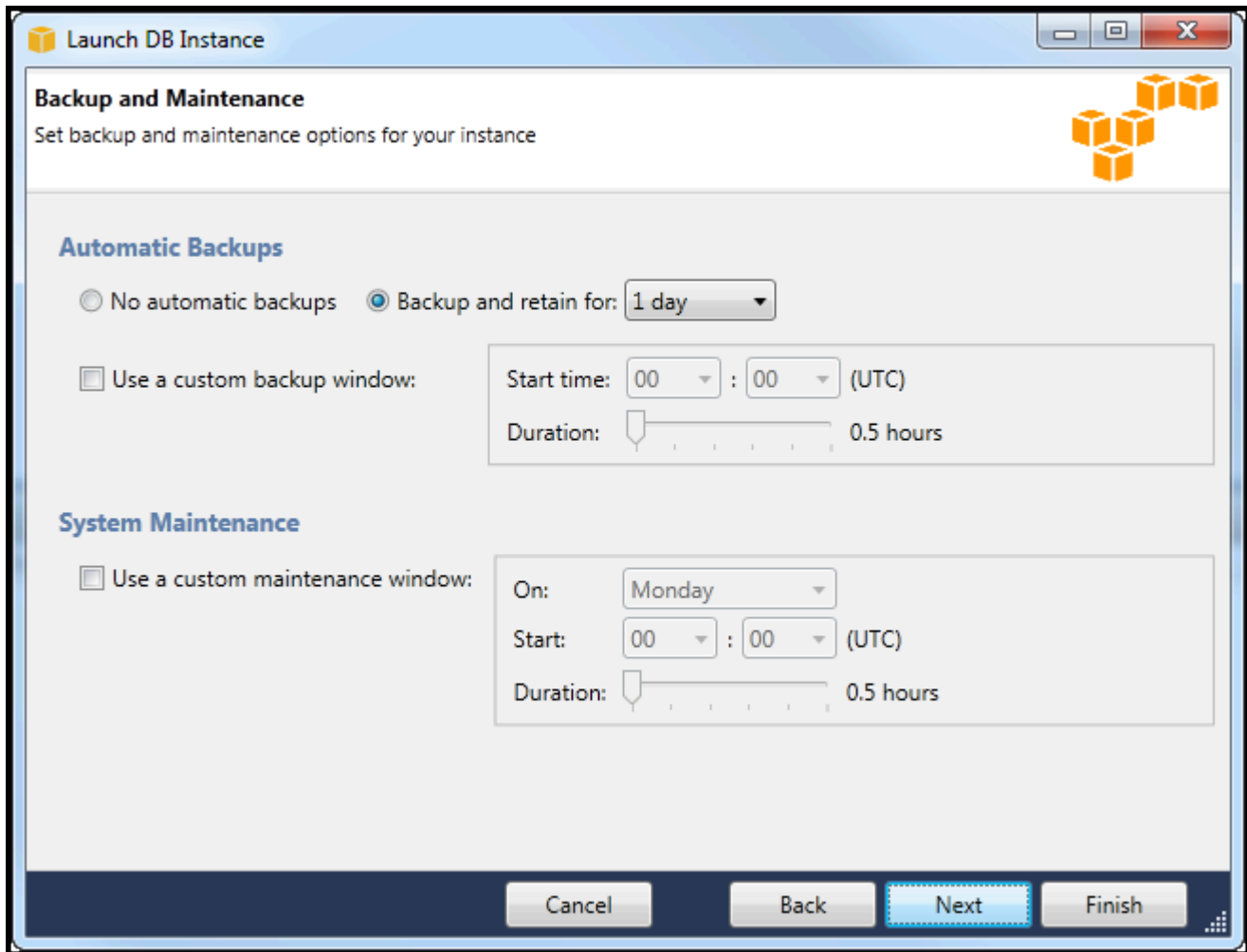


2. A caixa de diálogo Backup e manutenção permite especificar se o Amazon RDS deve fazer backup da instância e, em caso positivo, por quanto tempo o backup deve ser mantido. Você também pode especificar uma janela de tempo durante a qual os backups devem ocorrer.

Essa caixa de diálogo também permite especificar se você deseja que o Amazon RDS realize 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 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).

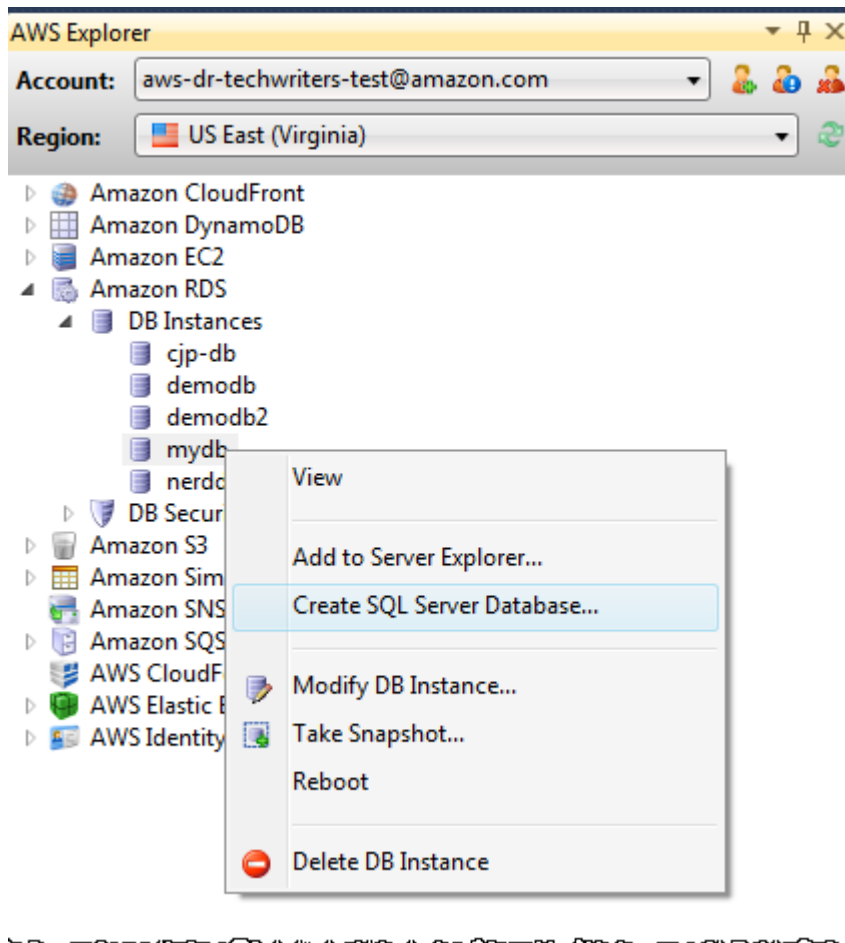
Criar um banco de dados do Microsoft SQL Server em uma instância do RDS

Devido à forma como Microsoft SQL Server foi projetado, depois que você inicia uma instância do Amazon RDS, é necessário criar um banco de dados do SQL Server na instância do RDS.

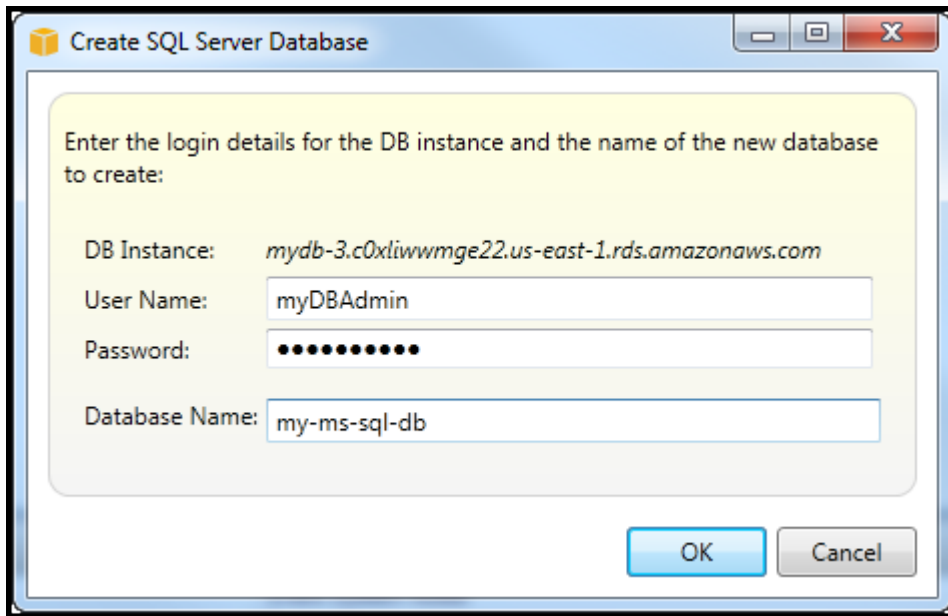
Para obter mais informações sobre como criar uma instância do Amazon RDS, consulte [Iniciar uma instância do banco de dados do Amazon RDS](#).

Para criar um banco de dados do Microsoft SQL Server

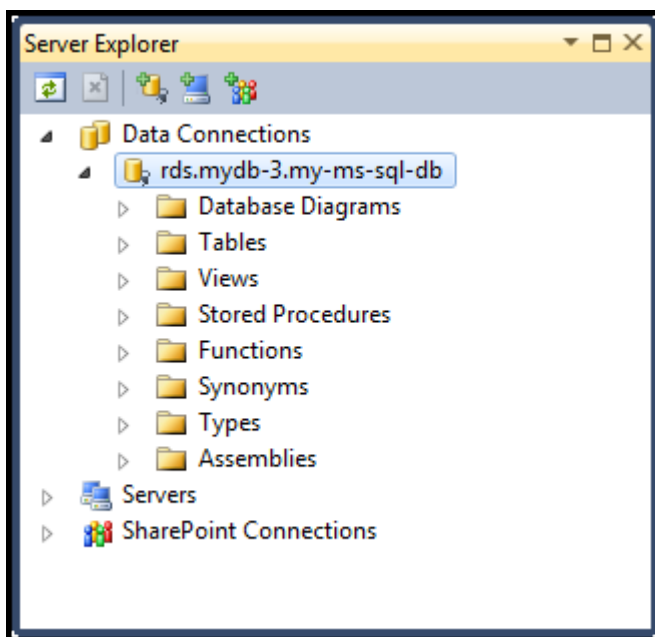
1. No AWS Explorer, abra o menu de contexto (clique com o botão direito) do nó correspondente à instância do RDS do Microsoft SQL Server e escolha Criar um banco de dados do SQL Server.



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 kit de ferramentas para Visual Studio cria o banco de dados do Microsoft SQL Server e o adiciona ao Server Explorer do Visual Studio.



Grupos de segurança do Amazon RDS

Os grupos de segurança do Amazon RDS permitem gerenciar o acesso à rede para as instâncias do Amazon RDS. Com os grupos de segurança, você especifica conjuntos de endereços IP usando a notação Encaminhamento Entre Domínios Sem Classificação (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 grupos de segurança 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.

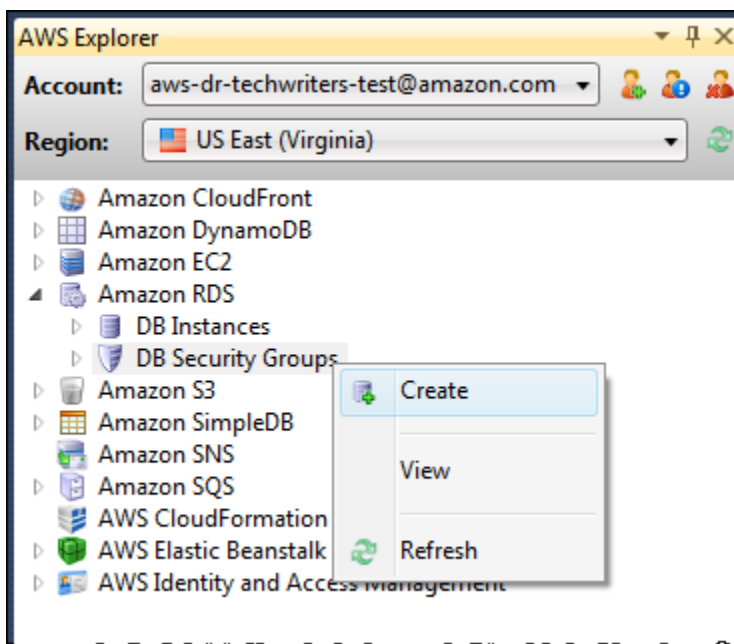
Para obter mais informações sobre grupos de segurança do Amazon RDS, acesse [RDS Security Groups](#). Para obter mais informações sobre grupos de segurança do Amazon EC2, acesse o [Guia do usuário do EC2](#).

Criar um grupo de segurança do Amazon RDS

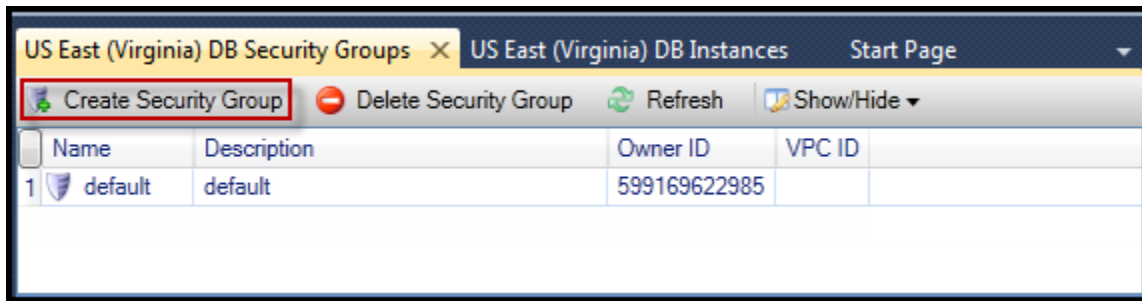
Você pode usar o kit de ferramentas para Visual Studio para criar um grupo de segurança do RDS. Se você usar o kit de ferramentas da AWS para iniciar uma instância do RDS, o assistente permitirá especificar um grupo de segurança do RDS a ser usado com a instância. Você pode usar o procedimento a seguir para criar esse security group antes de iniciar o assistente.

Para criar um security group do Amazon RDS

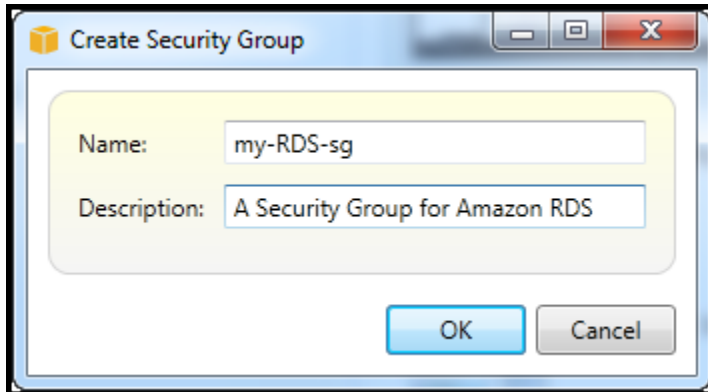
1. No AWS Explorer, expanda o nó Amazon RDS, abra o menu de contexto (clique com o botão direito) do subnó Grupo de segurança de banco de dados e escolha Criar.



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 grupo de segurança do Amazon RDS

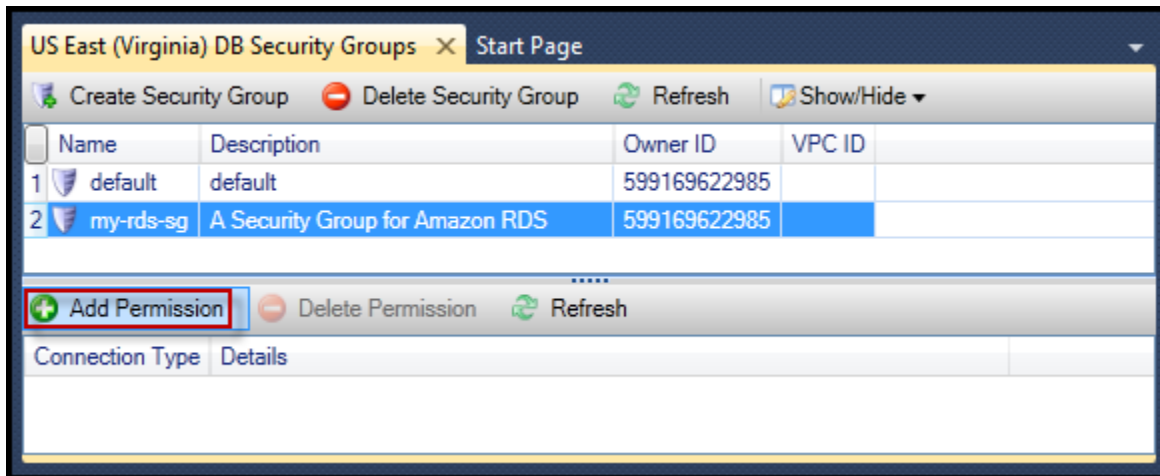
Por padrão, um novo grupo de segurança do Amazon RDS não dá acesso à rede. Para permitir acesso a instâncias do Amazon RDS que usem o grupo de segurança, use o procedimento a seguir para definir as permissões de acesso.

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 grupo de segurança ainda não for exibido na lista, verifique se você está visualizando a lista da região da AWS correta. As guias Grupo de segurança no kit de ferramentas da AWS são específicas de cada região.

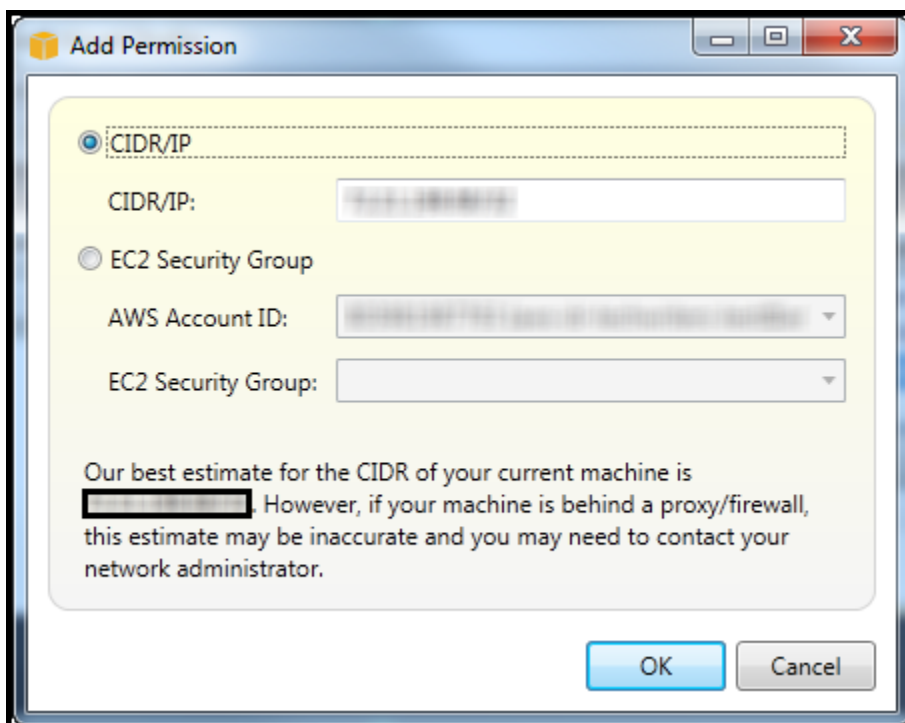
Se nenhuma guia Grupo de segurança for exibida, no AWS Explorer, abra o menu de contexto (clique com o botão direito) do subnó Grupos de segurança de banco de dados e escolha Visualizar.

2. Escolha Add Permission.



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

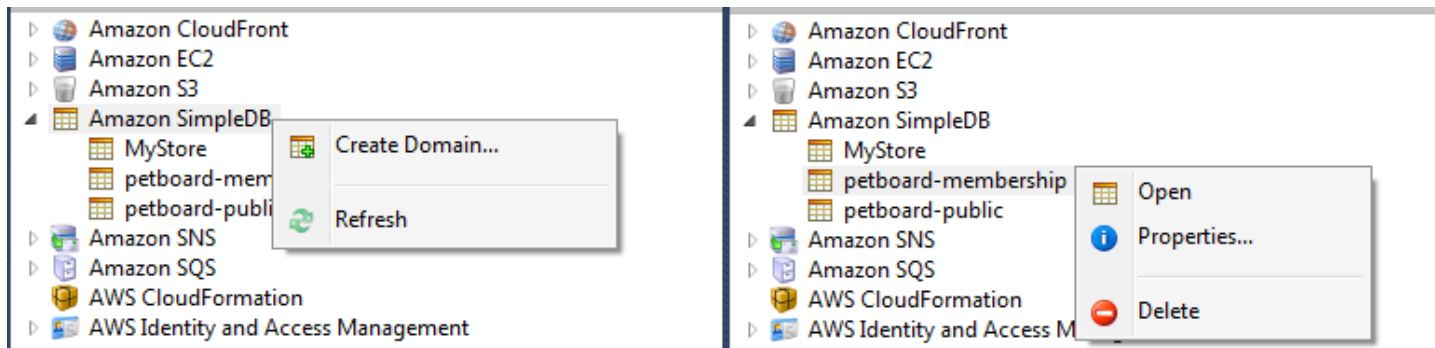
3. Na caixa de diálogo Add Permission (Adicionar permissão), você pode usar a notação CIDR para especificar quais endereços IP podem acessar a instância do RDS ou especificar quais grupos de segurança do EC2 podem acessar a instância do RDS. Ao escolher Grupo de segurança do EC2, você pode especificar o acesso para todas as instâncias do EC2 associadas a uma Conta da AWS com acesso ou escolher um grupo de segurança do EC2 na lista suspensa.



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

Usar o Amazon SimpleDB no AWS Explorer

O AWS Explorer exibe todos os domínios do Amazon SimpleDB associados à conta da AWS ativa. No AWS Explorer, 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

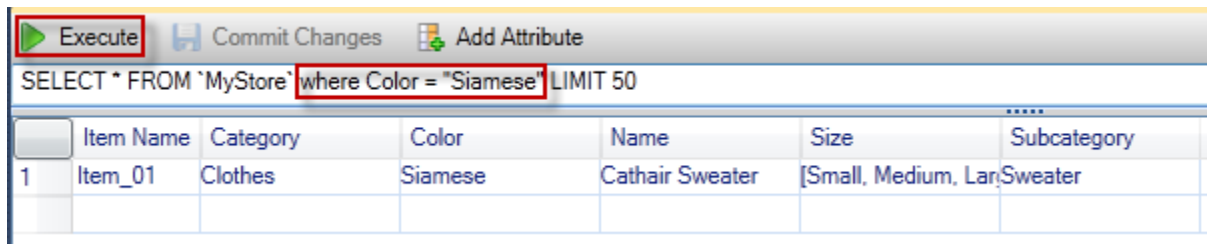
O AWS Explorer também pode exibir uma visualização em grade de um domínio do Amazon SimpleDB na qual você pode ver os itens, atributos e valores nesse domínio. Você pode executar consultas de maneira que somente um subconjunto dos itens do domínio seja exibido. Clicando duas vezes em uma célula, você 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 o AWS SDK para .NET.

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

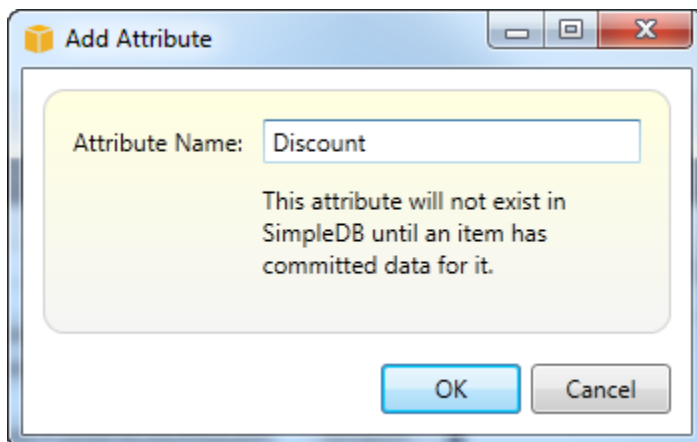


Execute query from AWS Explorer

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

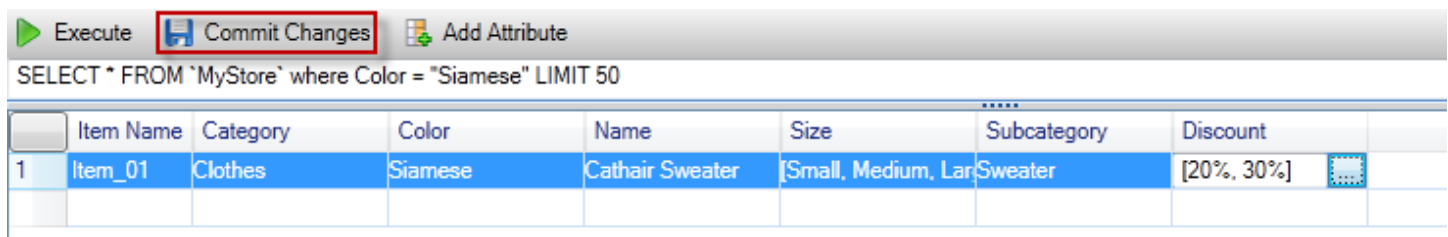
Como adicionar um atributo

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.

Usar o Amazon SQS no AWS Explorer

O Amazon Simple Queue Service (Amazon SQS) é um serviço de fila flexível que permite a passagem da mensagem entre diferentes processos de execução em uma aplicação de software. As filas do Amazon SQS estão localizadas na infraestrutura da AWS, mas os processos que estão passando mensagens podem no local, em instâncias do Amazon EC2 ou em uma combinação de ambos. O Amazon SQS é ideal para coordenar a distribuição de trabalho em vários computadores.

O kit de ferramentas para Visual Studio permite visualizar filas do Amazon SQS associadas à conta ativa, criar e excluir filas, bem como enviar mensagens por meio de filas. (Conta ativa é a conta selecionada no AWS Explorer.)

Para obter mais informações sobre o Amazon SQS, acesse [Conceitos básico do Amazon SQS](#) na documentação da AWS.

Criação de uma fila

Você pode criar uma fila do Amazon SQS no AWS Explorer. 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. No AWS Explorer, abra o menu de contexto (clique com o botão direito) do nó Amazon SQS e escolha Criar 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 no AWS Explorer. Se você excluir uma fila, todas as mensagens associadas à fila deixarão de estar disponíveis.

Para excluir uma fila

1. No AWS Explorer, abra os menus de contexto (clique com o botão direito) da fila que você deseja excluir e escolha Excluir.

Gerenciar propriedades da fila

Você pode visualizar e editar as propriedades de qualquer uma das filas exibidas no AWS Explorer. Você também pode enviar mensagens para a fila nessa visualização de propriedades.

Para gerenciar propriedades da fila

- No AWS Explorer, abra o menu de contexto (clique com o botão direito) da fila cujas propriedades você deseja gerenciar e escolha Visualizar 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.

Save Send Refresh

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

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

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


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

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

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

Message Sampling

Message Id	Message Body	Sender Id	Sent
------------	--------------	-----------	------

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

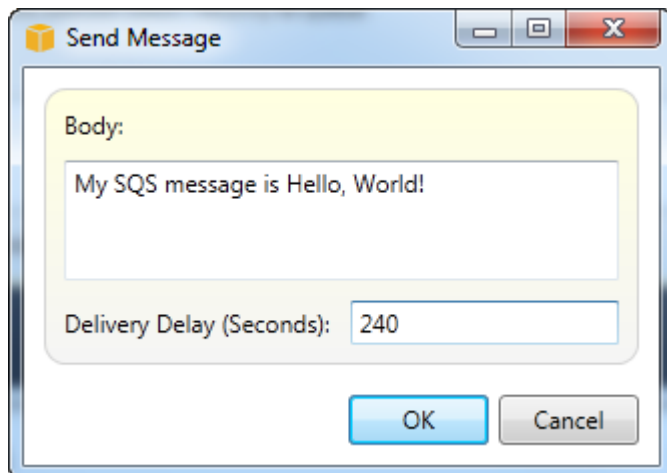
SQS queue properties view

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 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.

The screenshot displays the AWS Management Console interface for an SQS queue. At the top, there are buttons for 'Save', 'Send', and 'Refresh'. Below these are several property fields:

- Visibility timeout (Seconds): 30
- Maximum message size (Bytes): 65536
- Message retention period (Seconds): 345600
- Default Delivery Delay (Seconds): 120
- Created timestamp: 10/20/2011 1:34:49 PM
- Last modified timestamp: 10/20/2011 1:34:49 PM
- Number of messages: 1
- Number of messages not visible: 0

Below the properties, the Queue ARN and Queue URL are shown. A section titled 'Message Sampling' contains a table with the following data:

Message Id	Message Body	Sender Id	Sent
d58475df-2f92-49ec-a400-957bafcc5daf	My SQS message is Hello, World!	arn:aws:iam::111111111111:user:tk	10/20/2011 2:33:02 PM

At the bottom of the console, a warning icon and text state: 'Changes can take up to 60 seconds to propagate throughout the SQS system.'

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.

Gerenciamento de Identidade e Acesso

AWS Identity and Access Management (IAM) permite que você gerencie com mais segurança o acesso aos seus recursos Contas da AWS e aos seus recursos. Com o IAM, você pode criar vários usuários em sua conta primária (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.

É possível 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 concede ao usuário acesso ao serviço Amazon S3 e aos recursos relacionados na conta, mas que não dá acesso a nenhum outro serviço ou recurso.

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

Além de gerenciar permissões nos níveis de usuário e grupo, o IAM também adota o conceito de perfis do IAM. Assim como usuários e grupos, você pode anexar políticas aos perfis do IAM. Em seguida, você pode associar a função do IAM a uma EC2 instância da Amazon. Os aplicativos executados na EC2 instância podem ser acessados AWS usando 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, acesse o [Guia do usuário do IAM](#).

Criar e configurar um usuário do IAM

Os usuários do IAM permitem que você conceda a outras pessoas acesso ao seu Conta 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 a Conta da AWS devem fazê-lo como usuários do IAM, até mesmo o proprietário da conta. Isso garante que, se as credenciais de um dos usuários do IAM forem comprometidas, apenas essas credenciais possam ser desativadas. Não há necessidade de desativar nem alterar as credenciais raiz da conta.

No kit de ferramentas para 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 extraem suas 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 AWS gerar credenciais (ID da chave de acesso e chave secreta) para o usuário do IAM. Para obter mais informações, consulte [Gerar credenciais para um usuário do IAM](#)

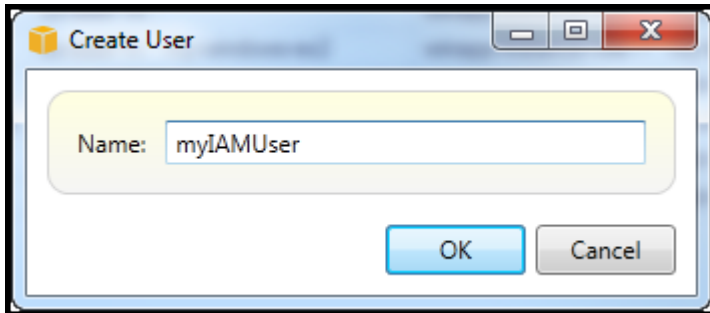


O Toolkit for Visual Studio oferece suporte à especificação de credenciais de usuário do IAM para acessar serviços por meio do Explorer. Como os usuários do IAM normalmente não têm acesso total a todos os Amazon Web Services, algumas das funcionalidades do AWS Explorer podem não estar disponíveis. Se você usar o AWS Explorer para alterar recursos enquanto a conta ativa for um usuário do IAM e depois mudar a conta ativa para a conta raiz, as alterações podem não ficar visíveis até que você atualize a exibição no AWS Explorer. Para atualizar a exibição, escolha o botão refresh (↻).

Para obter informações sobre como configurar usuários do IAM a partir do Console de gerenciamento da AWS, acesse [Trabalho com usuários e grupos](#) no Guia do usuário do IAM.

Para criar um usuário do IAM

1. No AWS Explorer, expanda o AWS Identity and Access Management, abra o menu de contexto (clique com o botão direito do mouse) para Usuários e escolha Criar usuário.
2. Na caixa de diálogo Criar usuário, digite um nome para o usuário do IAM e escolha OK. Esse nome do IAM deve ser um [nome amigável](#). Para obter informações sobre restrições quanto a nomes de usuários do IAM, acesse o [Guia do usuário do IAM](#).



Create an IAM user

O novo usuário aparecerá como um subnó em Usuários, abaixo do nó AWS Identity and Access Management.

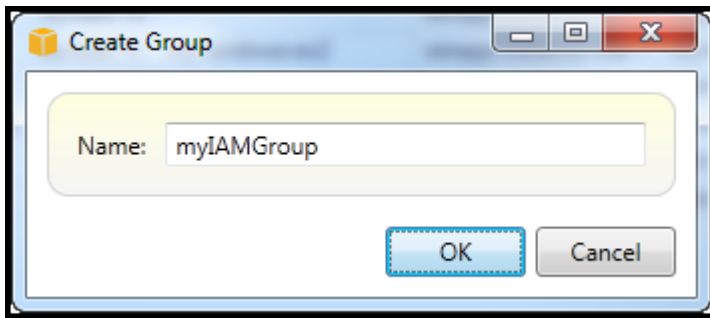
Para obter informações sobre como criar uma política e anexá-la ao usuário, consulte [Criar uma política do IAM](#).

Criar um grupo do IAM

Os grupos são usados para aplicar políticas do IAM a um conjunto de usuários. Para obter informações sobre como gerenciar grupos e usuários do IAM, acesse [Working with Users and Groups](#) no Guia do usuário do IAM.

Para criar um grupo do IAM

1. No AWS Explorer, em Identity and Access Management, abra o menu de contexto (clique com o botão direito do mouse) para Grupos e escolha Criar grupo.
2. Na caixa de diálogo Criar grupo, digite um nome para o grupo do IAM e escolha OK.



Create IAM group

O novo grupo do IAM será exibido no subnó Grupos de Identity and Access Management.

Para obter informações sobre como criar uma política e anexá-la ao grupo do IAM, consulte [Create an IAM Policy](#).

Adicionar um usuário do IAM a um grupo do IAM

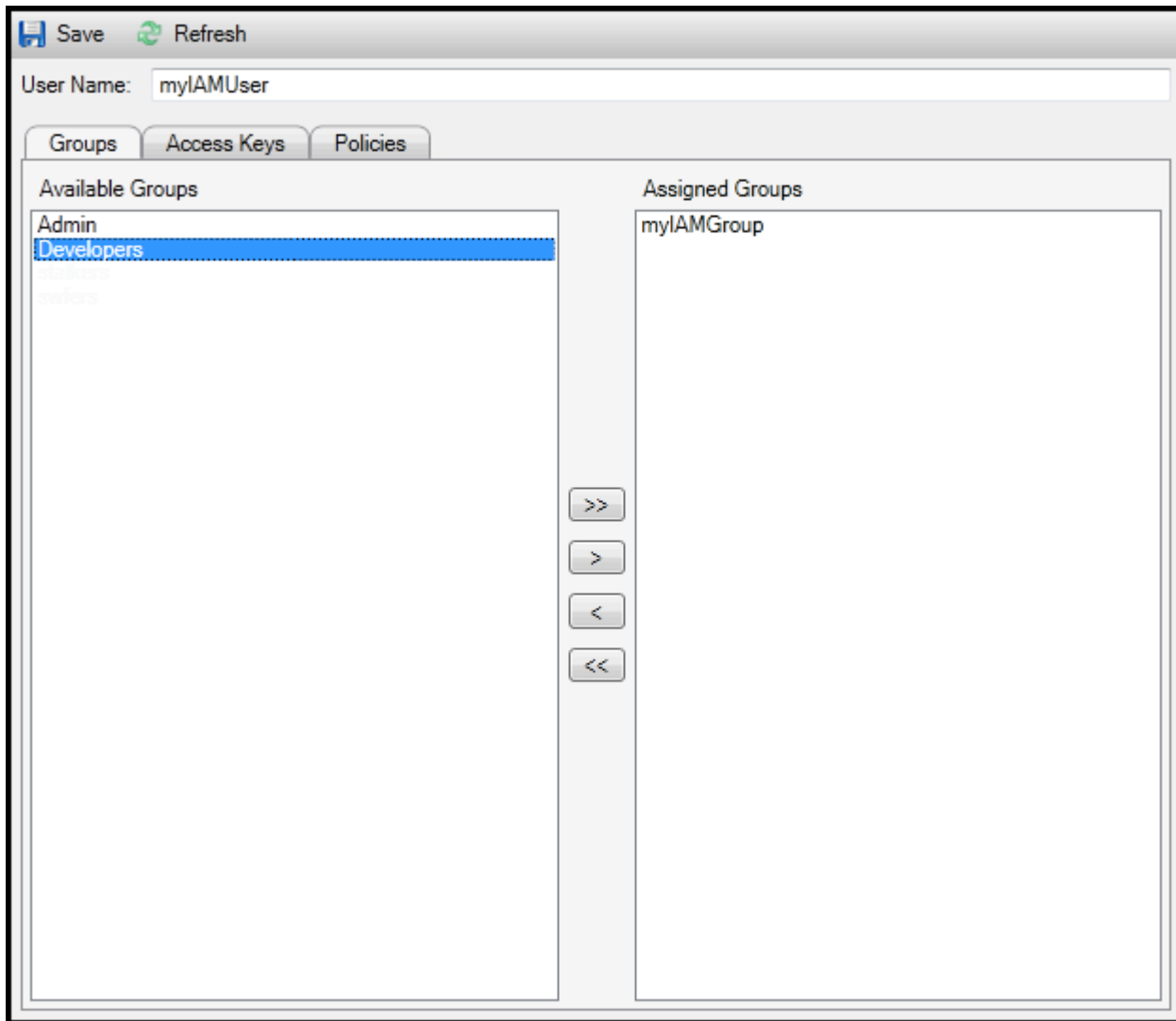
Os usuários do IAM que são membros de um grupo do IAM extraem permissões de acesso das políticas anexadas ao grupo. A finalidade de um grupo do IAM é facilitar o gerenciamento de permissões em um conjunto de usuários do IAM.

Para obter informações sobre como as políticas anexadas a um grupo do IAM interagem com as políticas anexadas a usuários do IAM que são membros desse grupo do IAM, acesse [Gerenciamento de políticas do IAM](#) no Guia do usuário do IAM.

No AWS Explorer, você adiciona usuários do IAM aos grupos do IAM a partir do subnó Usuários, não do subnó Grupos.

Para adicionar um usuário do IAM a um grupo do IAM

1. No AWS Explorer, em Identity and Access Management, abra o menu de contexto (clique com o botão direito do mouse) para Usuários e escolha Editar.



Assign an IAM user to a IAM group

2. O painel esquerdo da guia Grupos exibe 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 o botão >.

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

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

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. Quando você tiver terminado de atribuir o usuário do IAM a grupos do IAM, escolha Salvar.

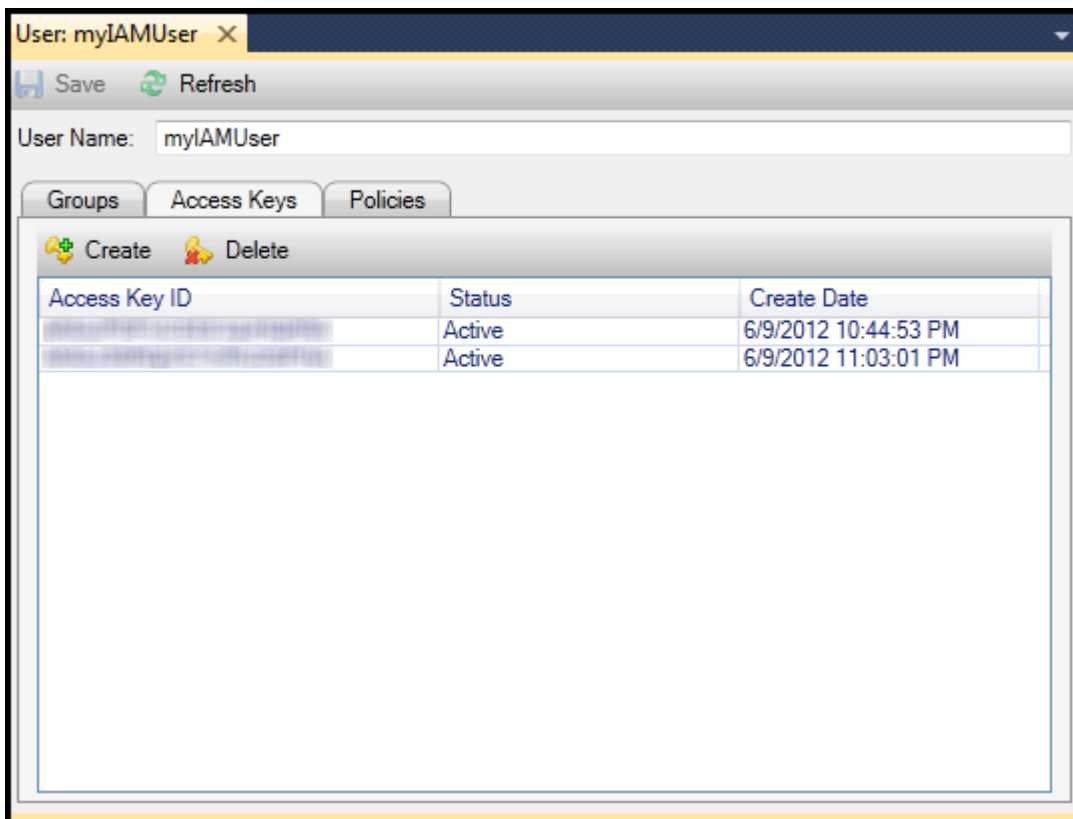
Gerar credenciais para um usuário do IAM

Com o kit de ferramentas para Visual Studio, você pode gerar o ID de chave de acesso e a chave secreta usados para fazer chamadas de API para a AWS. Essas chaves também podem ser especificadas para acessar serviços da Amazon Web Services por meio do kit de ferramentas. 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, consulte [Melhores práticas para gerenciar chaves de AWS acesso](#).

O kit de ferramentas não pode ser usado para gerar uma senha para um usuário do IAM.

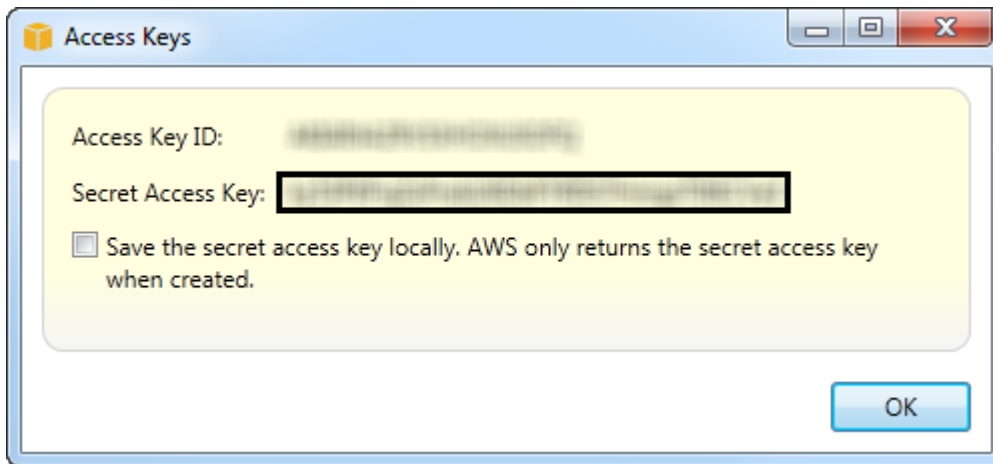
Para gerar credenciais de um usuário do IAM

1. No AWS Explorer, abra o menu de contexto (clique com o botão direito do mouse) para um usuário do IAM e escolha Editar.



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.

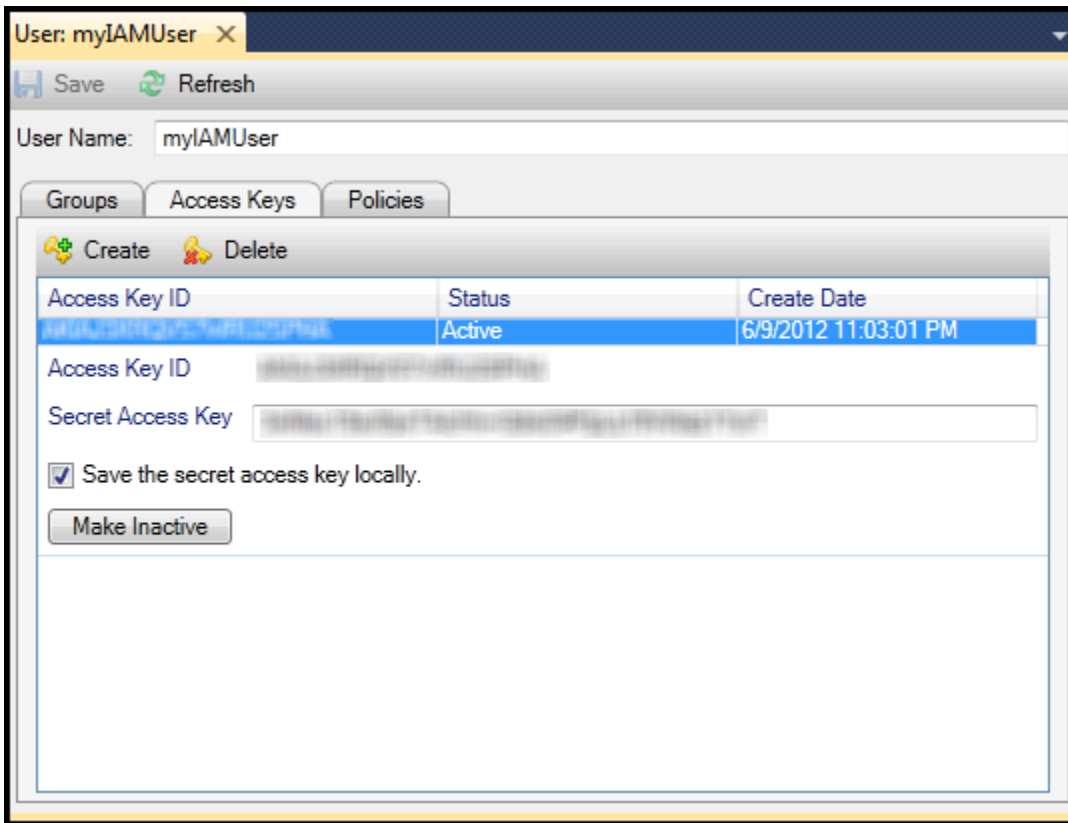


reate credentials for IAM user

Se você quiser que o Toolkit salve uma cópia criptografada da sua chave de acesso secreta em sua unidade local, selecione Salvar a chave de acesso secreta localmente. AWS só 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). (É possível fazer isso se você suspeitar que as credenciais foram comprometidas. Você pode reativar as credenciais se receber a garantia de que elas estão seguras.)

Criar um perfil do IAM

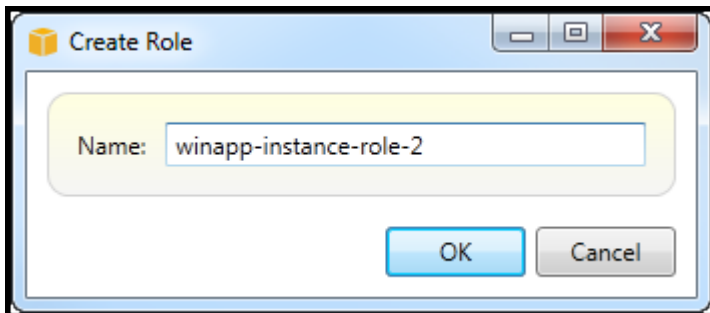
O kit de ferramentas para Visual Studio comporta a criação e configuração de perfis do IAM. Assim como ocorre com usuários e grupos, você pode anexar políticas a perfis do IAM. Em seguida, você pode associar a função do IAM a uma EC2 instância da Amazon. A associação com a EC2 instância é feita por meio de um perfil de instância, que é um contêiner lógico para a função. Os aplicativos executados na EC2 instância recebem automaticamente o nível de acesso especificado pela política associada à função do IAM. Isso é verdade mesmo quando o aplicativo não especificou outras AWS credenciais.

Por exemplo, é possível criar um perfil e anexar uma política a esse perfil que limita o acesso apenas ao Amazon S3. Depois de associar essa função a uma EC2 instância, você pode executar um aplicativo nessa instância e o aplicativo terá acesso ao Amazon S3, mas não a quaisquer outros serviços ou recursos. A vantagem dessa abordagem é que você não precisa se preocupar em transferir e armazenar AWS credenciais com segurança na instância. EC2

Para obter mais informações sobre os perfis do IAM, acesse [Working with IAM Roles](#) no Guia do usuário do IAM. Para ver exemplos de programas acessados AWS usando a função do IAM associada a uma EC2 instância da Amazon, acesse os guias do AWS desenvolvedor para [Java](#), [.NET](#), [PHP](#) e Ruby ([definir credenciais usando o IAM](#), [criar uma função do IAM](#) e [trabalhar com políticas do IAM](#)).

Para criar uma função do IAM

1. No AWS Explorer, em Identity and Access Management, abra o menu de contexto (clique com o botão direito do mouse) para Roles e escolha Create Roles.
2. Na caixa de diálogo Criar perfil, digite um nome para o perfil do IAM e escolha OK.



Create IAM role

O novo perfil do IAM será exibido em Perfis em Identity 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

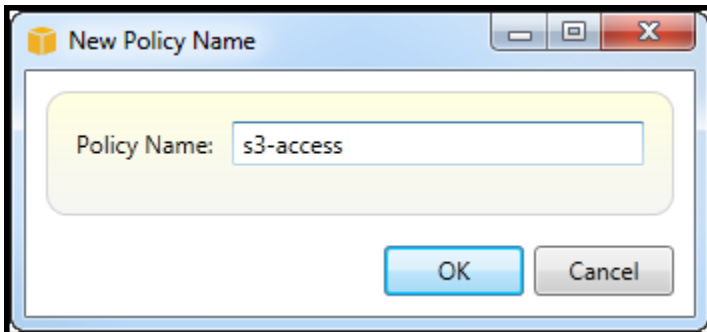
As políticas são fundamentais para o IAM. Elas podem ser associadas a entidades do IAM, como usuários, grupos ou perfis. As políticas especificam o nível de acesso habilitado para um usuário, grupo ou função.

Para criar uma política do IAM

No AWS Explorer, expanda o AWS Identity and Access Management nó e, em seguida, expanda o nó para o tipo de entidade (grupos, funções ou usuários) à qual você anexará a política. Por exemplo, abra um menu de contexto de um perfil do IAM e escolha Editar.

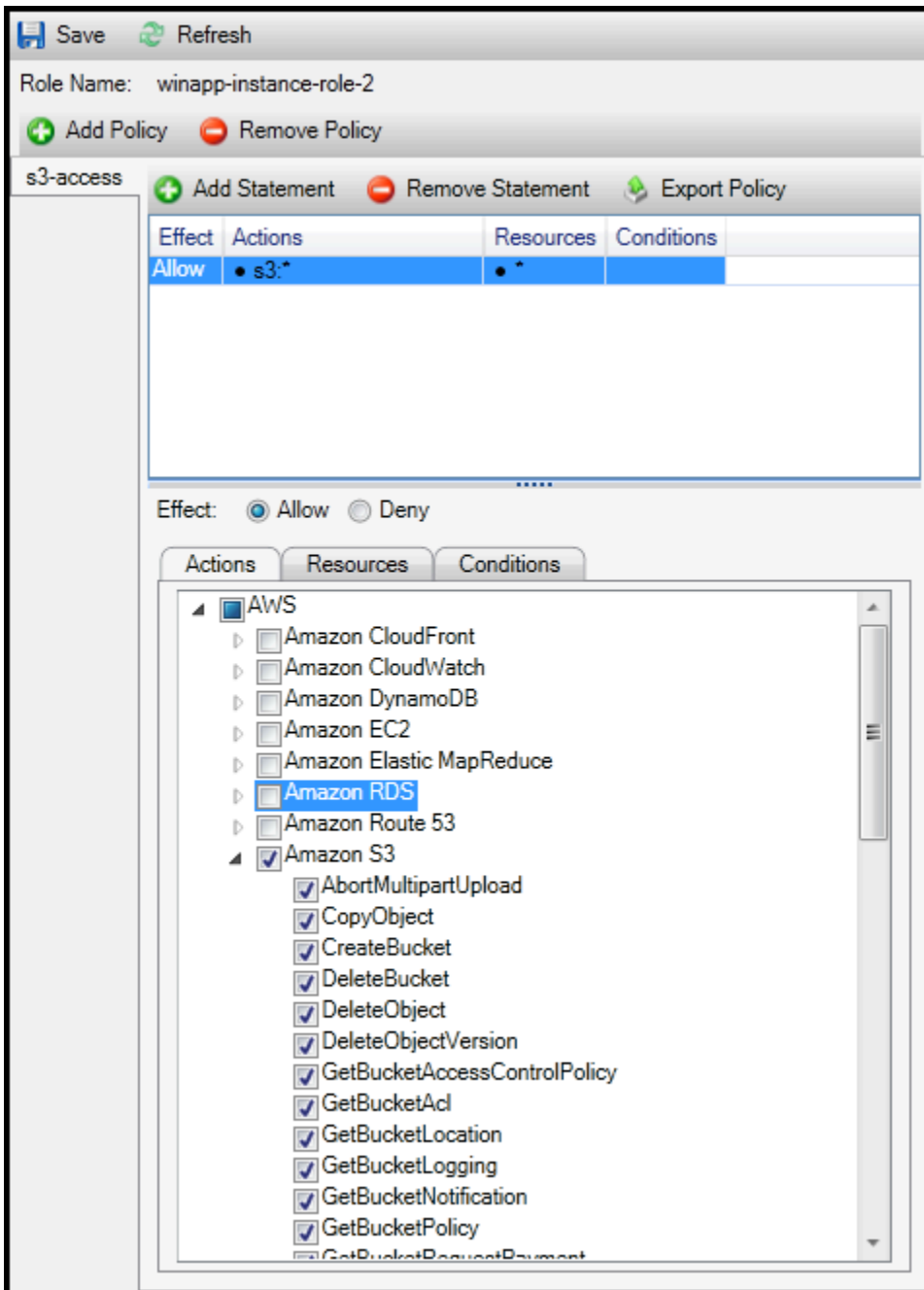
Uma guia associada à função aparecerá no AWS Explorer. Escolha o link Add Policy (Adicionar política).

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 fornecido à função (neste exemplo, winapp-instance-role -2) associada à política. Neste exemplo, uma política concede acesso total ao Amazon S3, mas não a nenhum outro recurso.



Specify IAM policy

Para um controle de acesso mais preciso, você pode expandir os subnós no editor de políticas a fim de permitir ou não ações associadas a serviços da 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. 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 usando o Toolkit for Visual Studio.

Tópicos

- [AWS Lambda Projeto básico](#)
- [AWS Lambda Projeto básico de criação de imagem Docker](#)
- [Tutorial: Crie e teste um aplicativo sem servidor com AWS Lambda](#)
- [Tutorial: Creating an Amazon Rekognition Lambda Application](#)
- [Tutorial: Usando o Amazon Logging Frameworks AWS Lambda para criar registros de aplicativos](#)

AWS Lambda Projeto básico

Você pode criar uma função do 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 no Visual Studio para ajudar a acelerar a inicialização do seu projeto. Os esquemas do Lambda contêm funções pré-escritas que simplificam a criação de uma base de projeto flexível.

Note

O serviço Lambda tem limites de dados para diferentes tipos de pacotes. Para obter informações detalhadas sobre os limites de dados, consulte o tópico [Cotas do Lambda](#) no Guia do usuário do AWS Lambda.

Como criar um projeto do Lambda no Visual Studio

1. No Visual Studio, expanda o menu Arquivo, expanda Novo e selecione Projeto.
2. Na caixa de diálogo Novo projeto, defina as caixas suspensas Idioma, Plataforma e Tipo de projeto como "Todos" e digite aws lambda no campo Pesquisar. Escolha o modelo Projeto do AWS Lambda (.NET Core - C#).
3. No campo Nome, insira **AWSLambdaSample**, especifique o Local do arquivo desejado e clique em Criar para prosseguir.
4. Na página Selecionar esquema, selecione o esquema Função vazia e clique em Concluir 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 arquivo `aws-lambda-tools-defaults.json`, criado automaticamente como parte do projeto. É possível definir as opções de compilação usando os campos nesse arquivo.

Note

Os modelos de projeto no Visual Studio contêm muitos campos diferentes. Observe o seguinte:

- `function-handler`: especifica o método executado quando a função do Lambda é executada.
- A especificação de um valor no campo `function-handler` preenche previamente esse valor no assistente de publicação.
- Se você renomear a função, a classe ou o conjunto, precisará atualizar o campo correspondente no arquivo `aws-lambda-tools-defaults.json`.

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

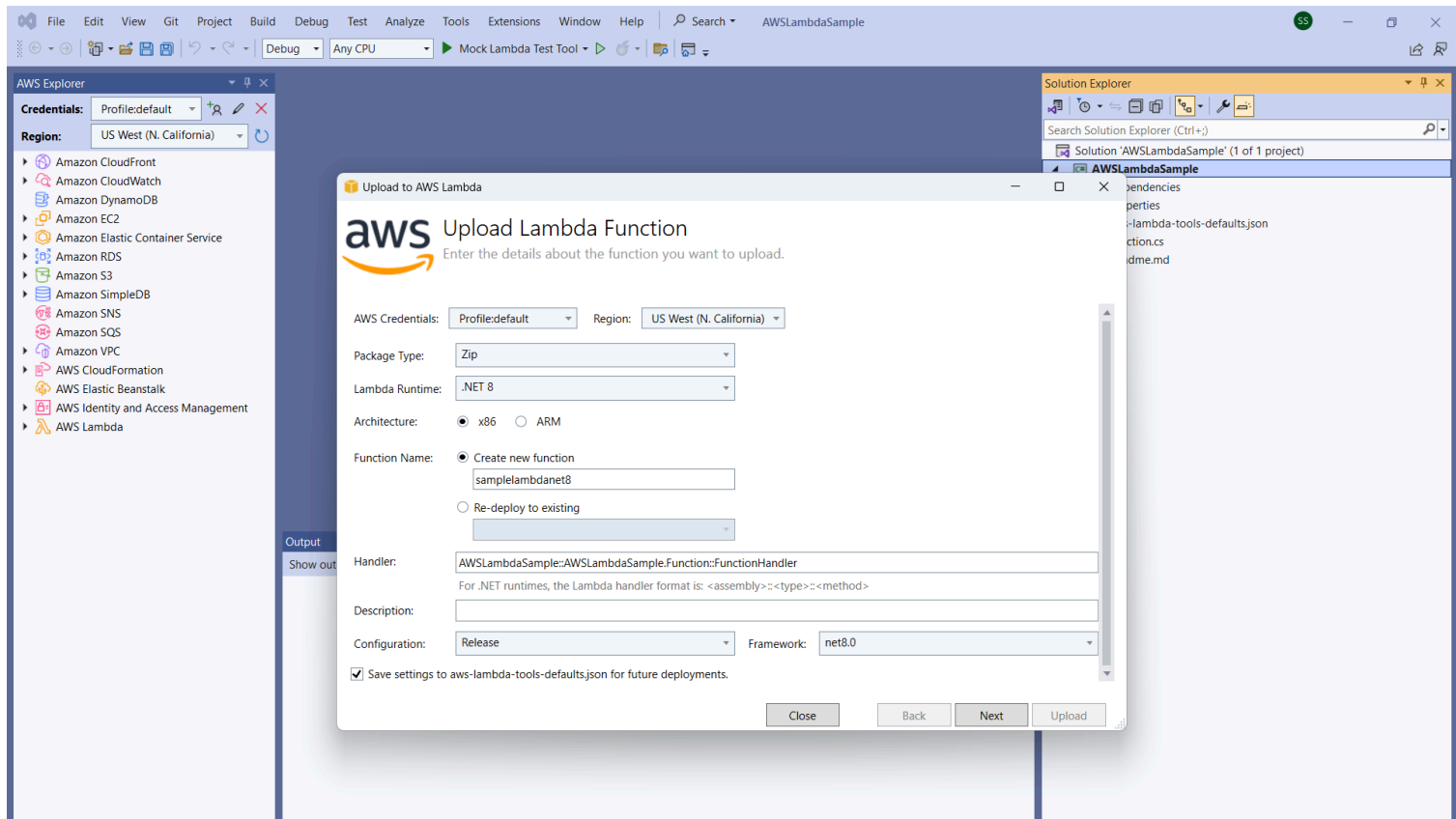
```
"dotnet lambda help",
  "All the command line options for the Lambda command can be specified in this
  file."
],
"profile": "default",
"region": "us-west-2",
"configuration": "Release",
"function-architecture": "x86_64",
"function-runtime": "dotnet8",
"function-memory-size": 512,
"function-timeout":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

Examine 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.

Publicar no Lambda


O procedimento e a imagem a seguir demonstram como fazer upload de uma função no Lambda usando o AWS Toolkit for Visual Studio.



Publicar uma 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 Fazer upload de função do Lambda, preencha os seguintes campos:
 - a. Tipo de pacote: escolha **Zip**. Um arquivo ZIP será criado como resultado do processo de compilação e será carregado no Lambda. Você também pode escolher **Image** como Tipo de pacote. O [Tutorial: Projeto básico do Lambda para criação de imagens do Docker](#) descreve como publicar usando o Tipo de pacote **Image**.
 - b. Runtime do Lambda: escolha o runtime do Lambda no menu suspenso.
 - c. Arquitetura: selecione sua opção de arquitetura preferida.
 - d. Nome da função: selecione a opção Criar nova função, depois insira um nome de exibição para a instância do Lambda. Esse nome é referenciado tanto pelo AWS Explorer quanto pelas Console de gerenciamento da AWS telas.


- e. Manipulador: use este campo para especificar um manipulador de funções. Por exemplo: **AWSLambdaSample::AWSLambdaSample.Function::FunctionHandler**.
 - f. (Opcional) Descrição: insira um texto descritivo que será exibido com a instância no Console de gerenciamento da AWS.
 - g. Configuração: escolha a configuração desejada no menu suspenso.
 - h. Framework: escolha o framework desejado no menu suspenso.
 - i. Salvar configurações: selecione essa caixa para salvar as configurações atuais em `aws-lambda-tools-defaults.json` como padrão para implantações futuras.
 - j. Clique em Próximo 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 a função do Lambda acessar recursos em uma Amazon VPC, selecione as sub-redes e os grupos de segurança.
- c. (Opcional) Defina todas as variáveis de ambiente das quais a função do 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. Selecione Fazer upload para abrir a janela Upload da função 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 `hello lambda!` no campo de entrada de texto e selecione Invocar para invocar manualmente a função do Lambda. O texto aparece na guia Resposta, convertido para 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.

The screenshot displays the AWS Explorer interface within Visual Studio Code. On the left, the 'AWS Explorer' sidebar shows the 'AWS Lambda' section expanded, with 'samplelambdanet8' selected. The main pane shows the configuration for 'Function: samplelambdanet8'. The function is in an 'Active' state, with a 'dotnet8' runtime and a code size of 32,875 bytes. The 'Test Function' tab is active, showing a 'Sample Input' of 'hello lambda!' and a 'Response' of 'HELLO LAMBDA!'. Below the test results, the 'Log output' section shows the following details:

```
START RequestId: 5d597bf6-733e-4cdd-8ca4-71d9255f855d Version: $LATEST
END RequestId: 5d597bf6-733e-4cdd-8ca4-71d9255f855d
REPORT RequestId: 5d597bf6-733e-4cdd-8ca4-71d9255f855d  Duration: 176.47 ms    Billed Duration: 177 ms
Memory Size: 512 MB    Max Memory Used: 68 MB    Init Duration: 330.57 ms
```

The 'Error List' at the bottom shows 0 errors, 0 warnings, and 0 messages. The status bar at the bottom indicates 'Ready'.

7. (Opcional) Para confirmar que você publicou com sucesso sua função Lambda, faça login no Console de gerenciamento da AWS 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 nó AWS Lambda.
2. Clique com o botão direito do mouse na instância implantada e selecione Excluir.

AWS Lambda Projeto básico de criação de imagem 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 maior controle sobre o runtime. Por exemplo, é possível escolher runtimes 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

É possível usar modelos e esquemas do Lambda no Visual Studio para ajudar a acelerar a inicialização do seu projeto. Os esquemas 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 selecione Projeto.
2. Na caixa de diálogo Novo projeto, defina as caixas suspensas Idioma, Plataforma e Tipo de projeto como “Todos” e digite **aws lambda** no campo Pesquisar. Escolha o modelo Projeto do AWS Lambda (.NET Core - C#).
3. No campo Nome do projeto, insira **AWSLambdaDocker**, especifique o Local do arquivo e clique em 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.

Revisar os arquivos de projeto

As seções a seguir examinam os três arquivos de projeto criados pelo esquema .NET 8 (imagem de contêiner):

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

1. `Dockerfile`

O `Dockerfile` executa três ações principais:

- **FROM:** estabelece a imagem básica 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:** os arquivos gerados no processo de compilação local serão copiados para o diretório de trabalho da imagem.

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

- **ENTRYPOINT:** a imagem básica 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 esquema .NET 8 (imagem de contêiner).

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

- **profile:** define seu AWS perfil.

- `region`: define a AWS região em que seus recursos são armazenados.
- `configuration`: define a configuração usada para publicar a função.
- `package-type`: define o tipo de pacote de implantação como uma imagem de contêiner ou arquivamento de arquivos `.zip`.
- `function-memory-size`: define a alocação de memória para a função em MB.
- `function-timeout`: o tempo limite é o período máximo, em segundos, durante o qual uma função do Lambda pode ser executada. Você pode ajustá-lo em incrementos de 1 segundo até um máximo de 15 minutos.
- `docker-host-build-output-dir`: define o diretório de saída do processo de compilação 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 do 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 arquivo `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, `FunctionHandler` chama `ToUpper()` no 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 Explorador de soluções, abra o menu de contexto do projeto (clique com o botão direito do mouse) e escolha **Publicar no AWS Lambda** para abrir a janela **Fazer upload de função do Lambda**.
2. Na página **Fazer upload de função do Lambda**, faça o seguinte:

Upload to AWS Lambda

aws Upload Lambda Function

Enter the details about the function you want to upload.

AWS Credentials: Profile:Default Region: US West (Oregon)

Package Type: Image

Lambda Runtime: Not Applicable to Image based Functions

Architecture: x86 ARM

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

Description:

Image Command: AWSLambdaDocker::AWSLambdaDocker.Function::FunctionHandler

Image Repo: awslambdadocker Image Tag: latest

Close Back Next Upload

- Em Tipo de pacote, **Image** foi selecionado automaticamente como seu Tipo de pacote porque o assistente de publicação detectou um `Dockerfile` em seu projeto.
- 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 Console de gerenciamento da AWS.
- Em Descrição, insira o texto a ser exibido com sua instância no Console de gerenciamento da AWS.
- 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. Escolha 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. Selecione Fazer upload 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.

Function: La...unctionDocker Dockerfile

Apply Changes Refresh

Function: LambdafunctionDocker

State: Active Last Update Status: Successful

Image URI: [x86_64] Last Modified: 3/19/2024 3:25:47 PM Code Size: Not Applicable

Test Function Configuration Event Sources AWS X-Ray Logs

Sample Input Invoke

Example Requests: hello image based lambda

Response JSON Pretty Print

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

Log output

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

Output

Show output from: Package Manager

- 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.

Próximas etapas

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 novo projeto de aplicativo AWS sem servidor](#)

- [Revisar os arquivos da aplicação de tecnologia sem servidor](#)
- [Implantar o aplicativo sem servidor](#)
- [Testar o aplicativo sem servidores](#)

Criar um novo projeto de aplicativo AWS sem servidor

AWS Projetos de aplicativos sem servidor criam funções Lambda com um modelo sem servidor. CloudFormation 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 projeto de aplicação sem servidor da AWS .

1. No Visual Studio, expanda o menu Arquivo, expanda Novo e selecione Projeto.
2. Na caixa de diálogo Novo projeto, verifique se as caixas suspensas Idioma, Plataforma e Tipo de projeto estão definidas como “Todos...” 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 Aplicação de tecnologia sem servidor da AWS com testes (.NET Core - C#) não seja preenchido no topo dos resultados.

4. Clique em Avançar para abrir a caixa de diálogo Configurar novo projeto.
5. Na caixa de diálogo Configurar novo projeto, insira **ServerlessPowertools** em Nome e preencha os campos restantes de acordo com sua preferência. Clique no botão Criar para prosseguir até a caixa de diálogo Selecionar esquema.
6. Na página Selecionar esquema, escolha o esquema Powertools para AWS Lambda e selecione Concluir para criar o projeto do Visual Studio.

Revisar os arquivos da aplicação de tecnologia sem servidor

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

1. serverless.template

2. Functions.cs

3. aws-lambda-tools-defaults.json

1. serverless.template

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 do Lambda que será exposta por meio do Amazon API Gateway como uma operação HTTP `*Get*`. É possível editar esse modelo para personalizar a função existente ou adicionar mais funções e outros recursos exigidos pela sua aplicação.

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 declaração `...AWS:: Serverless::Function...` são semelhantes aos campos de uma implantação de projeto do Lambda. O registro em log, as métricas e o rastreamento do Powertools são configurados por meio das seguintes variáveis de ambiente:

- `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`

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

```
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 arquivo `aws-lambda-tools-defaults.json` incluído no projeto:

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

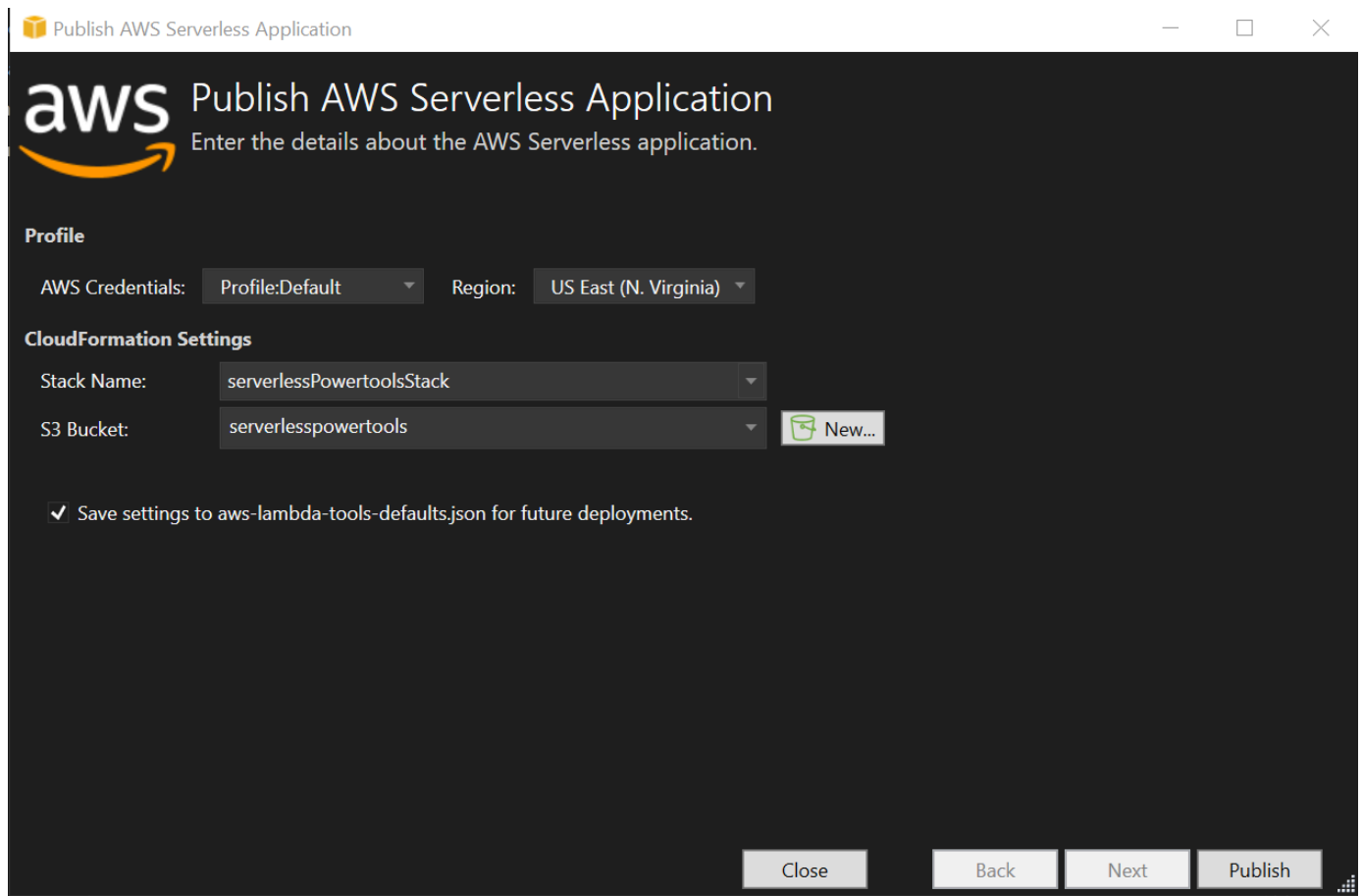
Implantar o aplicativo sem servidor

Para implantar a aplicação sem servidor, execute as seguintes etapas:

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 CloudFormation pilha no campo Nome da pilha.
3. No campo Bucket do S3, escolha um bucket do Amazon S3 para o qual o pacote da aplicação será carregado ou clique no botão Novo... e insira o nome de um novo bucket do Amazon S3. Depois, selecione Publicar para implantar a aplicação.

Note

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



4. A janela de visualização Pilha é aberta durante o processo de publicação. Quando a implantação é concluída, o campo Status exibe: CREATE_COMPLETE.

Resources	Time	Type	Logical ID	Physical ID	Status	Reason
Monitoring	3/29/2024 12:45:26 PM	AWS::CloudFormation::Stack	serverlessPowertoolsStack	arn:aws:cloudformation:us-east-1:50k...	CREATE_COMPLETE	
Template	3/29/2024 12:45:25 PM	AWS::ApiGateway::Stage	ServerlessRestApiProdStage	Prod	CREATE_COMPLETE	
Parameters	3/29/2024 12:45:25 PM	AWS::ApiGateway::Stage	ServerlessRestApiProdStage	Prod	CREATE_IN_PROGRESS	Resource not yet created.
Outputs	3/29/2024 12:45:24 PM	AWS::ApiGateway::Stage	ServerlessRestApiProdStage		CREATE_IN_PROGRESS	
	3/29/2024 12:45:23 PM	AWS::Lambda::Function	Get	serverlessPowertoolsStack-Get-Lgaks	CREATE_COMPLETE	
	3/29/2024 12:45:23 PM	AWS::ApiGateway::Deployment	ServerlessRestApiDeployment9d78fb6c57	qpdttli	CREATE_COMPLETE	
	3/29/2024 12:45:23 PM	AWS::ApiGateway::Deployment	ServerlessRestApiDeployment9d78fb6c57	qpdttli	CREATE_IN_PROGRESS	Resource not yet created.
	3/29/2024 12:45:22 PM	AWS::Lambda::Permission	GetRootGetPermissionProd	serverlessPowertoolsStack-GetRootGi	CREATE_COMPLETE	
	3/29/2024 12:45:22 PM	AWS::Lambda::Permission	GetRootGetPermissionProd	serverlessPowertoolsStack-GetRootGi	CREATE_IN_PROGRESS	Resource not yet created.
	3/29/2024 12:45:21 PM	AWS::ApiGateway::Deployment	ServerlessRestApiDeployment9d78fb6c57		CREATE_IN_PROGRESS	
	3/29/2024 12:45:21 PM	AWS::Lambda::Permission	GetRootGetPermissionProd		CREATE_IN_PROGRESS	
	3/29/2024 12:45:21 PM	AWS::ApiGateway::RestApi	ServerlessRestApi	bhntmpmjoj	CREATE_COMPLETE	
	3/29/2024 12:45:20 PM	AWS::ApiGateway::RestApi	ServerlessRestApi	bhntmpmjoj	CREATE_IN_PROGRESS	Resource not yet created.
	3/29/2024 12:45:19 PM	AWS::ApiGateway::RestApi	ServerlessRestApi		CREATE_IN_PROGRESS	
	3/29/2024 12:45:18 PM	AWS::Lambda::Function	Get	serverlessPowertoolsStack-Get-Lgaks	CREATE_IN_PROGRESS	Event not yet created.
	3/29/2024 12:45:17 PM	AWS::Lambda::Function	Get	serverlessPowertoolsStack-Get-Lgaks	CREATE_IN_PROGRESS	Resource not yet created.
	3/29/2024 12:45:16 PM	AWS::Lambda::Function	Get		CREATE_IN_PROGRESS	
	3/29/2024 12:45:15 PM	AWS::IAM::Role	GetRole	serverlessPowertoolsStack-GetRole-D	CREATE_COMPLETE	
	3/29/2024 12:44:59 PM	AWS::IAM::Role	GetRole	serverlessPowertoolsStack-GetRole-D	CREATE_IN_PROGRESS	Resource not yet created.
	3/29/2024 12:44:58 PM	AWS::IAM::Role	GetRole		CREATE_IN_PROGRESS	
	3/29/2024 12:44:55 PM	AWS::CloudFormation::Stack	serverlessPowertoolsStack	arn:aws:cloudformation:us-east-1:50k...	CREATE_IN_PROGRESS	User In Progress
	3/29/2024 12:44:49 PM	AWS::CloudFormation::Stack	serverlessPowertoolsStack	arn:aws:cloudformation:us-east-1:50k...	REVIEW_IN_PROGRESS	User In Progress

Testar o aplicativo sem servidores

Quando a criação da pilha estiver concluída, você poderá visualizar a aplicação usando o URL sem servidor da AWS . 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 uma aplicação do Lambda do Amazon Rekognition por meio do AWS Toolkit for Visual Studio.

Note

Após a criação, sua aplicação terá uma solução com dois projetos: o projeto de origem, que contém o código da função do Lambda a ser implantado no Lambda, e um projeto de teste que usa o xUnit para testar a 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 selecione Projeto.
2. Na caixa de diálogo Novo projeto, verifique se as caixas suspensas Idioma, Plataforma e Tipo de projeto estão definidas como "Todos..." 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 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. Clique no botão Criar para prosseguir até a caixa de diálogo Selecionar esquema.
6. Na caixa de diálogo Selecionar esquema, selecione o esquema Detectar rótulos de imagens e clique em 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.

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

Veja a seguir um exemplo do atributo de conjunto:

```
// 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 dos serviços Amazon S3 e Amazon Rekognition. O construtor também recupera as credenciais desses clientes da função do IAM que você atribuiu à função ao implantá-la. A região dos clientes é definida como a região em que sua função Lambda está sendo executada. Nesse esquema, você só deseja adicionar tags ao objeto do Amazon S3 caso o serviço Amazon Rekognition tenha 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.IsNullOrEmpty(environmentMinConfidence))
    {
        float value;
```

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

O exemplo a seguir demonstra como é possível utilizar o segundo construtor para testes. O projeto de teste configura os próprios clientes do S3 e do Rekognition e os passa:

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

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

```
public async Task FunctionHandler(S3Event input, ILambdaContext context)
{
    foreach(var record in input.Records)
    {
        if(!SupportedImageTypes.Contains(Path.GetExtension(record.S3.Object.Key)))
        {
            Console.WriteLine($"Object {record.S3.Bucket.Name}:{record.S3.Object.Key}
is not a supported image type");
            continue;
        }

        Console.WriteLine($"Looking for labels in image {record.S3.Bucket.Name}:
{record.S3.Object.Key}");
    }
}
```

```
    var detectResponses = await this.RekognitionClient.DetectLabelsAsync(new
DetectLabelsRequest
    {
        MinConfidence = MinConfidence,
        Image = new Image
        {
            S3Object = new Amazon.Rekognition.Model.S3Object
            {
                Bucket = record.S3.Bucket.Name,
                Name = record.S3.Object.Key
            }
        }
    });

    var tags = new List();
    foreach(var label in detectResponses.Labels)
    {
        if(tags.Count < 10)
        {
            Console.WriteLine($"\\tFound Label {label.Name} with confidence
{label.Confidence}");
            tags.Add(new Tag { Key = label.Name, Value =
label.Confidence.ToString() });
        }
        else
        {
            Console.WriteLine($"\\tSkipped label {label.Name} with confidence
{label.Confidence} because maximum number of tags reached");
        }
    }

    await this.S3Client.PutObjectTaggingAsync(new PutObjectTaggingRequest
    {
        BucketName = record.S3.Bucket.Name,
        Key = record.S3.Object.Key,
        Tagging = new Tagging
        {
            TagSet = tags
        }
    });
}
return;
}
```

`FunctionHandler` 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 em execução no Lambda, todas as chamadas são `Console.WriteLine()` redirecionadas para o Amazon Logs. CloudWatch

2. aws-lambda-tools-defaults.json

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

Para acessar a integração da CLI do .NET Core, acesse 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 a função do 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 arquivo `aws-lambda-tools-defaults.json`.

- Na janela Fazer upload no AWS Lambda, insira um nome no campo Nome da função e clique no botão Próximo para avançar até a janela Detalhes avançados da função.

Note

Este exemplo usa o Nome da função **ImageRekognition**.

Upload to AWS Lambda

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

Package Type: Zip

Lambda Runtime: .NET 8

Architecture: x86 ARM

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

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

Description:

Configuration: Release Framework: net8.0

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

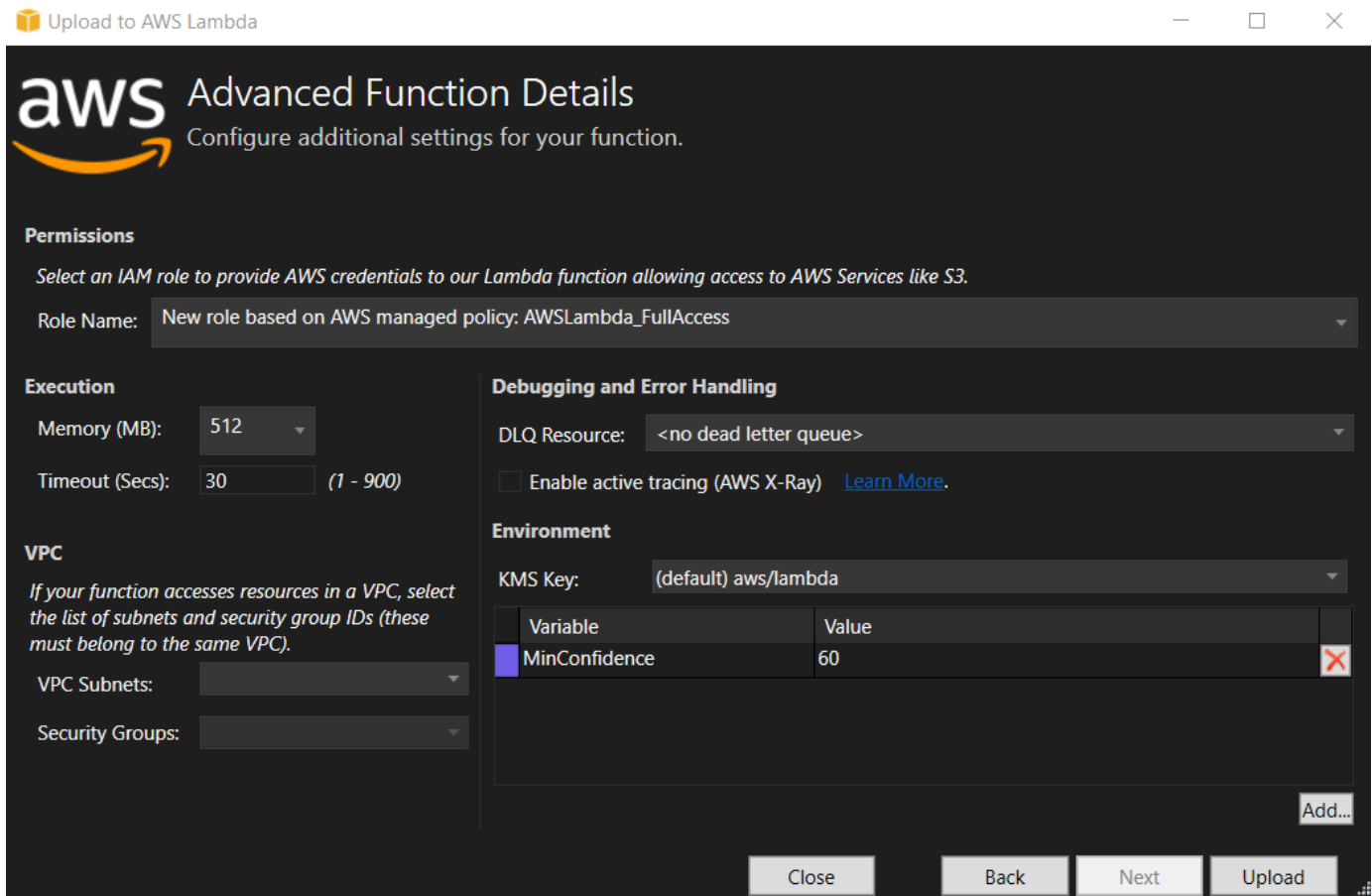
Close Back Next Upload

- Na janela Detalhes avançados da função, selecione um perfil do IAM que conceda permissão ao seu código para acessar seus recursos do Amazon S3 e do Amazon Rekognition.

Note

Se você estiver seguindo este exemplo, selecione o perfil `AWSLambda_FullAccess`.

- Defina a variável de ambiente `MinConfidence` como 60 e selecione Fazer upload para iniciar o processo de implantação. O processo de publicação é concluído quando a visualização da Função é exibida no AWS Explorer.



- Após a implantação bem-sucedida, configure o Amazon S3 a fim de enviar os eventos para a nova função. Para isso, acesse a guia Origens de eventos.
- Na guia Origens de eventos, clique no botão Adicionar e selecione o bucket do Amazon S3 para conectar à sua função do Lambda.

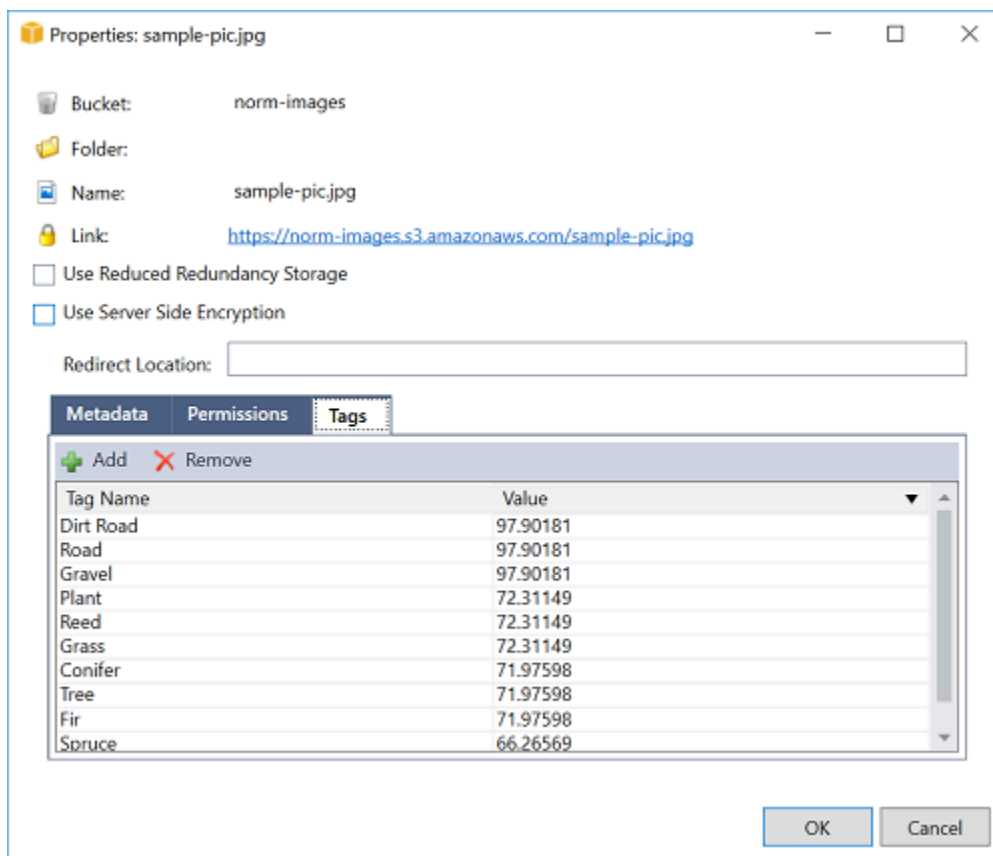
Note

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.

Os frameworks de registro em log do .NET compatíveis incluem:

- NLog: Para ver, consulte o pacote [nuget.org NLog](https://nuget.org/packages/NLog).
- Log4net: para ver, consulte o [pacote Log4net do nuget.org](https://nuget.org/packages/log4net).
- Framework de registro em log ASP.NET Core: para ver, consulte o [pacote do framework de registro em log ASP.NET Core do nuget.org](https://nuget.org/packages/Microsoft.Extensions.Logging).

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 emNLog.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 para .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 [GitHub repositório.NET do AWS Logging](#).

JSON

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

Implantar no AWS

O kit de ferramentas para Visual Studio comporta a implantação de aplicação em contêineres do AWS Elastic Beanstalk ou pilhas do CloudFormation.

Note

Se você estiver usando o Visual Studio Express Edition:

- É possível usar a [CLI do Docker](#) para implantar aplicações em contêineres do Amazon ECS.
- Você pode usar o [Console de Gerenciamento da AWS](#) para implantar aplicações em contêineres do Elastic Beanstalk.

Em implantações do Elastic Beanstalk, você deve primeiramente criar um pacote de implantação da web. Para obter mais informações, consulte [Como criar um pacote de implantação web no Visual Studio](#). Para a implantação do Amazon ECS, é preciso ter uma imagem do Docker. Para obter mais informações, consulte [Ferramentas do Visual Studio para Docker](#).

Tópicos

- [Trabalhar com o Publicar na AWS no Visual Studio](#)
- [Implantando um AWS Lambda projeto com a CLI do.NET Core](#)
- [Implantação AWS Elastic Beanstalk no Visual Studio usando o AWS Toolkit for Visual Studio com o Amazon Q](#)
- [Implantar no Amazon EC2 Container Service](#)

Trabalhar com o Publicar na AWS no Visual Studio

Publicar na AWS é uma experiência de implantação interativa que ajuda você a publicar aplicações .NET em destinos de implantação da AWS, oferecendo compatibilidade para aplicações direcionadas ao o.NET Core 3.1 e versões posteriores. O Publicar na AWS mantém seu fluxo de trabalho dentro do Visual Studio ao disponibilizar estes recursos de implantação diretamente do IDE:

- Capacidade de implantar a aplicação com um único clique.
- Recomendações de implantação com base na aplicação.
- Criação automática do Dockerfile, conforme relevante e exigido pelo ambiente do destino de implantação.
- Configurações otimizadas para criar e empacotar aplicações, conforme exigido pelo seu destino de implantação.

Note

Para obter informações adicionais sobre a publicação de aplicações .NET Framework, consulte [Criar e implantar aplicações .NET no Elastic Beanstalk](#), neste guia.

Também é possível acessar Publicar na AWS pela CLI do .NET. Para obter mais informações, consulte o guia [Deploy .NET applications on AWS](#).

Tópicos

- [Pré-requisitos](#)
- [Tipos de aplicação compatíveis](#)
- [Publicar aplicações em destinos da AWS](#)

Pré-requisitos

Para publicar com êxito aplicações .NET em um serviço da AWS, instale o seguinte em seu dispositivo local:

- .NET Core 3.1+ (que inclui .NET5 e .NET6): para obter informações adicionais sobre esses produtos e download, acesse o [site de download da Microsoft](#).
- Node.js 14.x ou versão posterior: o Node.js é necessário para executar o AWS Cloud Development Kit (AWS CDK). Para baixar ou obter mais informações sobre o Node.js, acesse o [site de download do Node.js](#).

Note

Publicar na AWS utiliza o AWS CDK para implantar a aplicação e toda a infraestrutura de implantação como um único projeto. Para obter mais informações sobre o AWS CDK, consulte o guia do [Cloud Development Kit](#).

- (Opcional) O Docker é usado na implantação em um serviço baseado em contêiner, como o Amazon ECS. Para obter mais informações e baixar o Docker, consulte o site de [download do Docker](#).

Tipos de aplicação compatíveis

Antes de publicar em um destino novo ou existente, primeiro crie ou abra um dos seguintes tipos de projeto no Visual Studio:

- Aplicações ASP.NET Core
- Aplicação do console do .NET
- Aplicação Blazor WebAssembly

Publicar aplicações em destinos da AWS

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

Note

Integração dos kits de ferramentas com o servidor da CLI do .NET:
A publicação inicializa um processo do servidor do .NET no host local para realizar o processo de publicação.

Publicar em um novo destino

A seguir, descrevemos como configurar suas preferências de implantação do Publicar na AWS quando você estiver publicando em um novo destino.

1. No AWS Explorer, expanda o menu suspenso Credenciais e escolha o perfil da AWS que corresponde à região e aos serviços da AWS necessários para a implantação.
2. Expanda o menu suspenso Região e escolha a região da AWS que contém os serviços da AWS necessários para a implantação.
3. No painel Solutions Explorer do Visual Studio, abra o menu de contexto (clique com o botão direito) do nome do projeto e escolha Publicar na AWS. Isso abrirá o Publicar na AWS.
4. No Publicar na AWS, escolha Publicar no novo destino para configurar uma nova implantação.

Note

Para modificar suas credenciais de implantação padrão, escolha ou clique no link Editar localizado ao lado da seção Credenciais, em Publicar na AWS.

Para ignorar o processo de configuração de destino, escolha Publicar no destino existente e selecione a configuração de sua preferência na lista de destinos de implantação anteriores.

5. No painel Destinos de publicação, escolha um serviço da AWS para gerenciar a implantação da aplicação.
6. Quando a configuração estiver adequada para você, escolha Publicar para iniciar o processo de implantação.

Note

Depois de iniciar uma implantação, o Publicar na AWS exibe as seguintes atualizações de status:

- Durante o processo de implantação, o Publicar na AWS exibe informações sobre o progresso da implantação.
- Após o processo de implantação, o Publicar na AWS indica se a implantação foi bem-sucedida ou malsucedida.

- Após a implantação bem-sucedida, o painel Recursos oferece informações adicionais sobre o recurso que foi criado. Essas informações variarão dependendo do tipo de aplicação e da configuração de implantação.

Publicar em um destino existente

A seguir, descrevemos como republicar uma aplicação .NET em um destino da AWS existente.

1. No AWS Explorer, expanda o menu suspenso Credenciais e escolha o perfil da AWS que corresponde à região e aos serviços da AWS necessários para a implantação.
2. Expanda o menu suspenso Região e escolha a região da AWS que contém os serviços da AWS necessários para a implantação.
3. No painel Solutions Explorer do Visual Studio, clique com o botão direito no nome do projeto e escolha Publicar na AWS para abrir o Publicar na AWS.
4. No Publicar na AWS, escolha Publicar no destino existente para selecionar o ambiente de implantação em uma lista de destinos existentes.

Note

Se você publicou recentemente quaisquer aplicações na Nuvem AWS, elas estarão exibidas no Publicar na AWS.

5. Selecione o destino de publicação no qual você deseja implantar seu a aplicação e clique em Publicar para iniciar o processo de implantação.

Implantando um AWS Lambda projeto com a CLI do.NET Core

AWS Toolkit for Visual Studio Isso inclui modelos de projeto AWS Lambda do.NET Core para Visual Studio. Você pode implantar funções do Lambda incorporadas no Visual Studio usando a interface de linha de comandos (CLI) do .NET Core.

Tópicos

- [Pré-requisitos](#)
- [Tópicos relacionados](#)
- [Listar os comandos do Lambda disponibilizados por meio da 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 pré-requisitos a seguir:

- Garanta que o Visual Studio 2015 Update 3 esteja instalado.
- Instale o [.NET Core para Windows](#).
- Configure a CLI do .NET Core para trabalhar com o Lambda. Para obter mais informações, consulte o tópico sobre a [CLI do .NET Core](#) no Guia do desenvolvedor do AWS Lambda .
- Instale o kit de ferramentas para Visual Studio. Para obter mais informações, consulte [Instalando o AWS Toolkit for Visual Studio](#).

Tópicos relacionados

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

- Para obter mais informações sobre as funções do Lambda, consulte [O que é o AWS Lambda?](#) no Guia do AWS Lambda desenvolvedor.
- Para obter informações sobre como criar funções do Lambda no Visual Studio, consulte [AWS Lambda](#).
- Para obter mais informações sobre o Microsoft .NET Core, consulte [.NET Core](#) na documentação on-line da Microsoft.

Listar os comandos do Lambda disponibilizados por meio da CLI do .NET Core

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

1. Abra uma janela de prompt de comando e navegue até a pasta que contém um projeto do Lambda do Visual Studio .NET Core.
2. Insira `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 AWS Lambda do.NET Core no Visual Studio.

1. Abra uma janela de prompt de comando e navegue até a pasta que contém o projeto do Lambda do Visual Studio .NET Core.
2. Insira `dotnet lambda deploy-function`.
3. Quando solicitado, insira o nome da função a ser implantada. Ele pode ser um nome novo ou o nome de uma função existente.

4. Quando solicitado, insira a AWS Região (a região na qual sua função Lambda será implantada).
5. Quando solicitado, selecione ou crie o perfil do IAM que o Lambda assumirá ao executar o perfil.

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 um perfil existente, a função de implantação só solicitará a região da AWS .

```
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, consulte [exemplos de como usar o AWS Lambda](#).

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 Lambda, [consulte Solução de problemas e monitoramento de funções AWS Lambda](#) com a Amazon. CloudWatch

Implantação AWS Elastic Beanstalk no Visual Studio usando o AWS Toolkit for Visual Studio com o Amazon Q

AWS Elastic Beanstalk é um serviço que simplifica o processo de provisionamento de AWS recursos para seu aplicativo. O Elastic Beanstalk fornece toda AWS a infraestrutura necessária para implantar seu aplicativo. Essa infraestrutura inclui:

- As instâncias do Amazon EC2 que hospedam os executáveis e o conteúdo da aplicação.
- Um grupo do Auto Scaling para manter o número apropriado de instâncias do Amazon EC2 para atender à aplicação.
- Um balanceador de carga do Elastic Load Balancing que roteia o tráfego recebido para a instância do Amazon EC2 com a maior largura de banda.

Este tópico do guia do usuário descreve como trabalhar com o assistente do Elastic Beanstalk no kit de ferramentas com o Amazon Q. Para obter informações detalhadas específicas sobre AWS

o Elastic Beanstalk, consulte o Guia do desenvolvedor. [AWS Elastic Beanstalk](#) O assistente do Elastic Beanstalk para AWS o kit de ferramentas com o Amazon Q é descrito nas seções de tópicos a seguir.

Tópicos

- [Implantar uma aplicação no Elastic Beanstalk tradicional](#)
- [Implantar uma aplicação ASP.NET Core no Elastic Beanstalk \(herdado\)](#)
- [Como especificar as credenciais AWS de segurança para seu aplicativo](#)
- [Como republicar a aplicação em um ambiente do Elastic Beanstalk \(herdado\)](#)
- [Implantações de aplicativo Elastic Beanstalk personalizadas](#)
- [Implantações personalizadas do ASP.NET Core com o Elastic Beanstalk](#)
- [Suporte a várias aplicações para o .NET e o Elastic Beanstalk](#)

Implantar uma aplicação no Elastic Beanstalk tradicional

Esta seção descreve como usar o assistente Publicar no Elastic Beanstalk, fornecido como parte do kit de ferramentas para Visual Studio, para implantar uma aplicação 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

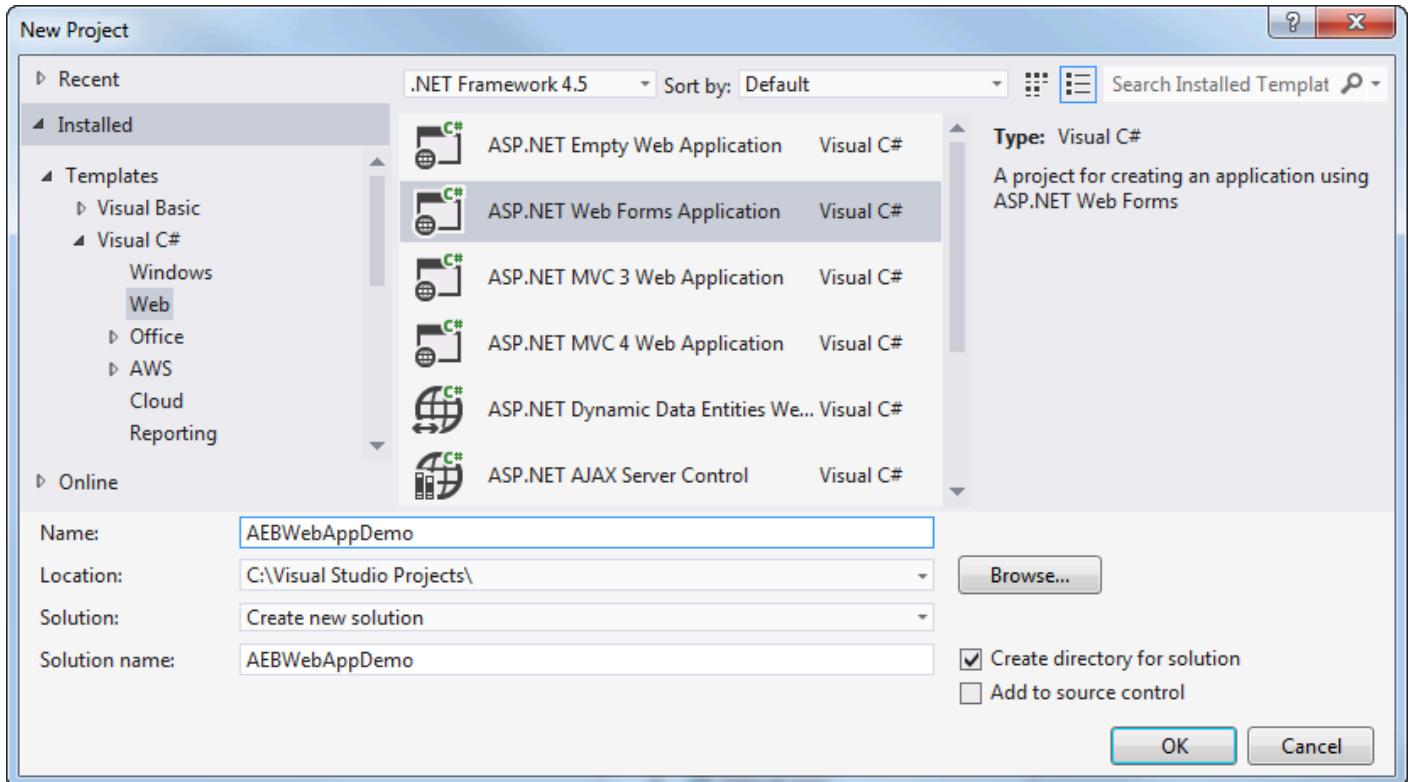
O assistente também dá suporte à implantação de aplicativos do ASP.NET Core. Para obter informações sobre o ASP.NET Core, consulte o guia [AWS .NET deployment tool](#) e o sumário atualizado de [Deploying to AWS](#).

Note

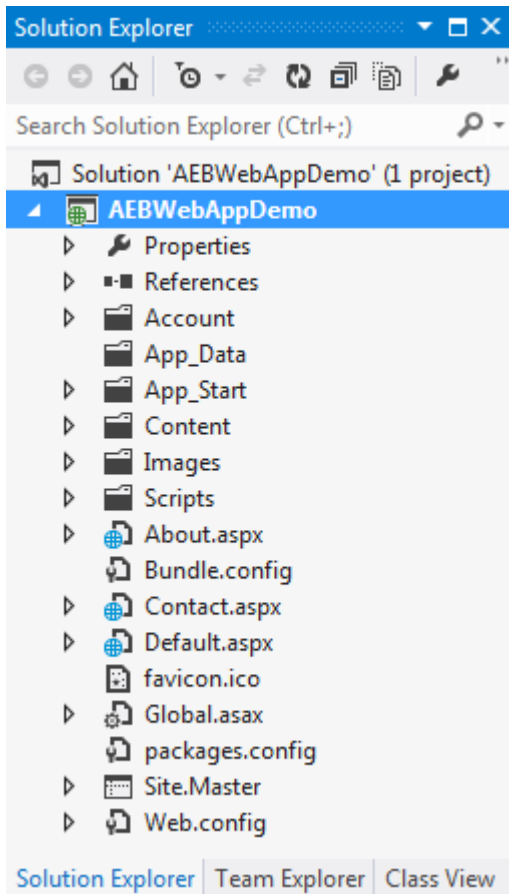
Antes de usar o assistente Publish to Elastic Beanstalk (Publicar no Elastic Beanstalk), é necessário fazer download e instalar [Web Deploy](#). O assistente depende do Web Deploy para implantar aplicativos web e sites aos servidores web do Internet Information Services (IIS).

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).

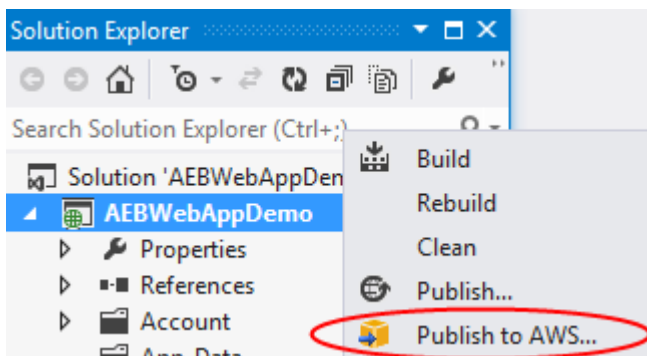


4. Na caixa Name (Nome), digite AEBWebAppDemo.
5. Na caixa Location (Local), digite o caminho para uma pasta de solução na máquina de desenvolvimento ou escolha Browse (Navegar) e navegue até e escolha uma pasta de solução e escolha Select Folder (Selecionar pasta).
6. Confirme se a caixa Criar diretório 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.

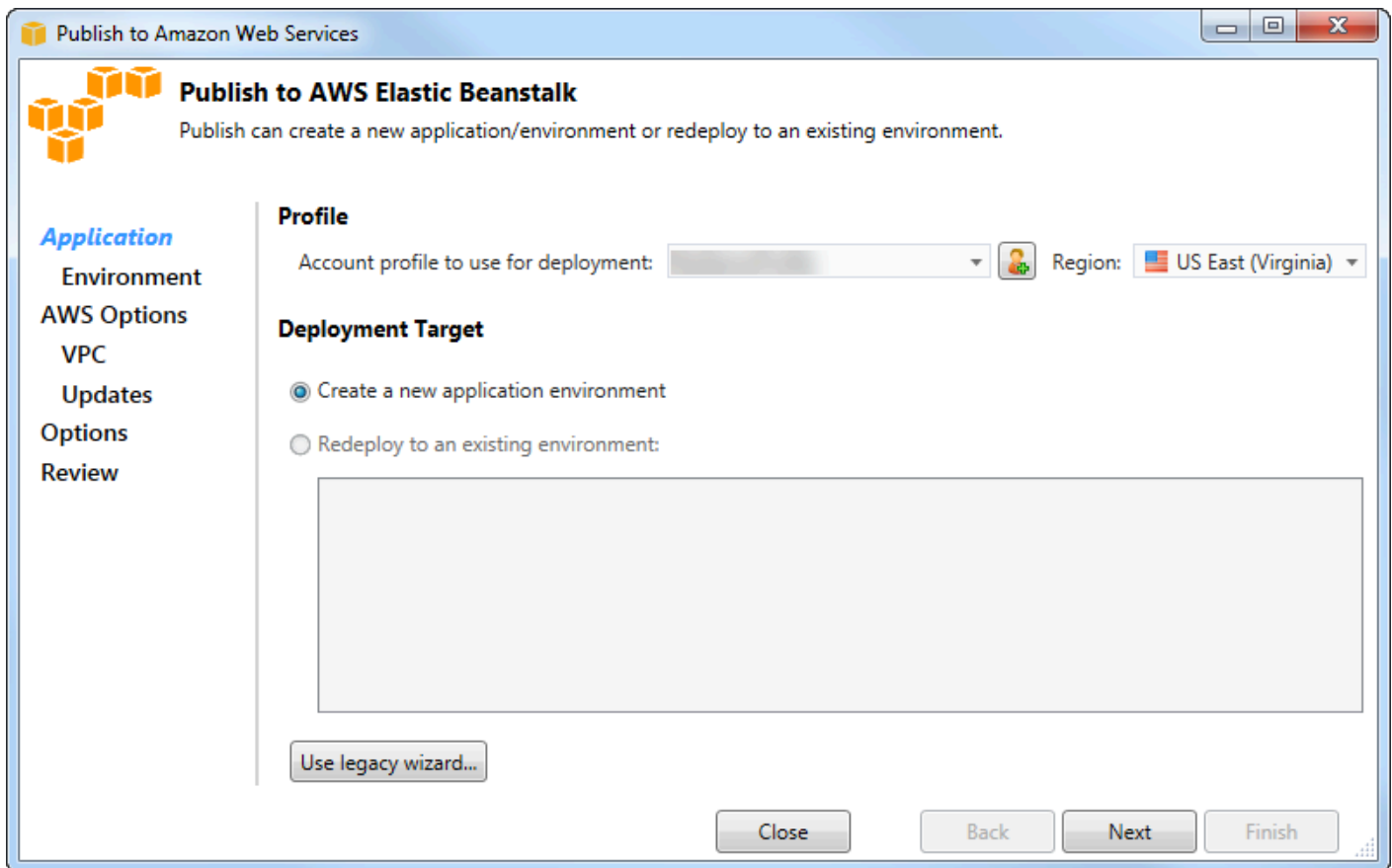


Para implantar um aplicativo usando o assistente Publish to Elastic Beanstalk

1. No Solution Explorer, abra o menu de contexto (clique com o botão direito do mouse) da pasta do projeto que você criou na seção anterior ou abra o menu de contexto da pasta do projeto do seu próprio aplicativo e escolha Publicar no AWS 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 da AWS conta que você deseja usar para a implantação.

Opcionalmente, se você tem uma AWS conta que deseja usar, mas ainda não criou um perfil de AWS conta para ela, você pode escolher o botão com o símbolo de adição (+) para adicionar um perfil de AWS conta.

3. Na lista suspensa Região, escolha a região na qual você deseja que o Elastic Beanstalk implante a aplicação.
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 a ferramenta de implantação autônoma descontinuada.) 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 Próximo.

The screenshot shows a window titled "Publish to Amazon Web Services" with a sub-header "Application Environment". Below the sub-header is the instruction: "Enter the details for your new application environment. To create a new new environment for an existing application, select the appropriate application." On the left is a navigation sidebar with "Application Environment" selected. The main area contains three sections: "Application" with a dropdown menu showing "AEBWebAppDemo"; "Environment" with an empty dropdown menu; and "URL" with a text input field containing "http:" followed by a blurred domain, ".elasticbeanstalk.com", and a "Check availability..." button. Below the URL field is a green checkmark and the text "The requested URL is available". At the bottom are buttons for "Close", "Back", "Next", and "Finish".

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 o ambiente do Elastic Beanstalk. Neste contexto, o termo ambiente se refere às provisões de infraestrutura do Elastic Beanstalk para a aplicação. 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.
- 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.
 - Escolha Check availability (Verificar disponibilidade) para verificar se o URL do aplicativo web ainda não está em uso.
 - Se o URL do aplicativo da web puder ser usado, escolha Next (Próximo).

Publish to Amazon Web Services

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

Application
Environment
AWS Options
VPC
Updates
Options
Review

Amazon EC2 Launch Configuration

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

Instance type *: Micro Key pair *: MyKeyPair

Use custom AMI:

Use a VPC Single instance environment Enable Rolling Deployments

Deployed Application Permissions

Role: aws-elasticbeanstalk-ec2-role

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

Relational Database Access

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

default

Close Back Next Finish

- Na página Opções da AWS , em Configuração de inicialização do Amazon EC2, na lista suspensa Tipo de contêiner, escolha um tipo de imagem de máquina da Amazon (AMI) a ser usado na aplicação.
- Na lista suspensa Tipo de instância, especifique um tipo de instância do Amazon EC2 a ser usado. Para este exemplo, recomendamos usar Micro. Isso minimizará o custo associado à

execução da instância. Para obter mais informações sobre os custos do Amazon EC2, acesse a página [Preço do Amazon EC2](#).

3. Na lista suspensa Par de chaves, escolha um par de chaves da instância do Amazon EC2 a ser usado para fazer login nas instâncias que serão usadas na aplicação.
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 [Como usar a personalização AMIs](#) no Guia do desenvolvedor do [AWS Elastic Beanstalk e Criar 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 executar uma única instância do Amazon EC2 e implantar a aplicação nela, marque a caixa Ambiente de instância única.

Se você marcar essa caixa, o Elastic Beanstalk continuará a criar um grupo do Auto Scaling, mas não o configurará. Se quiser configurar o grupo do Auto Scaling posteriormente, você poderá usar o Console de gerenciamento da AWS.

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 usa AWS serviços como Amazon S3 e DynamoDB, a melhor maneira de fornecer credenciais é usar uma função do IAM. Na área Permissões da aplicação implantada, você pode escolher um perfil do IAM ou criar um que o assistente usará para iniciar o ambiente. Os aplicativos que usam o AWS SDK para .NET usarão automaticamente as credenciais fornecidas por essa função do IAM ao fazer uma solicitação a um AWS serviço.
9. Se a aplicação acessar um banco de dados do Amazon RDS, na lista suspensa na área Acesso ao banco de dados relacional, marque as caixas ao lado de todos os grupos de segurança do Amazon RDS que o assistente atualizará, para que as instâncias do Amazon EC2 possam acessar esse banco de dados.

10 Escolha 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.

AWS Elastic Beanstalk Developer Guide'. At the bottom, there are four buttons: 'Close', 'Back', 'Next', and 'Finish'."/>

Publish to Amazon Web Services

VPC Options

Set Amazon VPC options for the deployed application.

Application

Environment

AWS Options

VPC

Updates

Options

Review

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

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

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

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

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

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

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

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

Close Back Next Finish

A VPC já deve ter sido criada. Se tiver criado a VPC no kit de ferramentas para Visual Studio, este preencherá essa página para você. Se você tiver criado a VPC no [Console de Gerenciamento da AWS](#), digite informações sobre a VPC nessa 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 kit de ferramentas para Visual Studio implanta o balanceador de carga do Elastic Load Balancing para a aplicação 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 criadas por você usando o kit de ferramentas para 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 kit de ferramentas para Visual Studio implanta as instâncias do Amazon EC2 da aplicação na sub-rede privada.
- As instâncias do Amazon EC2 da aplicação comunicam-se pela sub-rede privada com a internet por meio de uma instância do Amazon EC2 na sub-rede pública que realiza 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 uma aplicação do Elastic Beanstalk em uma VPC acesse o [Guia do desenvolvedor do AWS 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.

Publish to Amazon Web Services

Rolling Deployments

Configure rolling deployments for application and environment configuration changes to avoid downtime during redeployments.

Application

Application Versions

Percentage

Update application versions: % of instances updated at a time.

Fixed

Update application versions: instance(s) at a time.

Environment Configuration

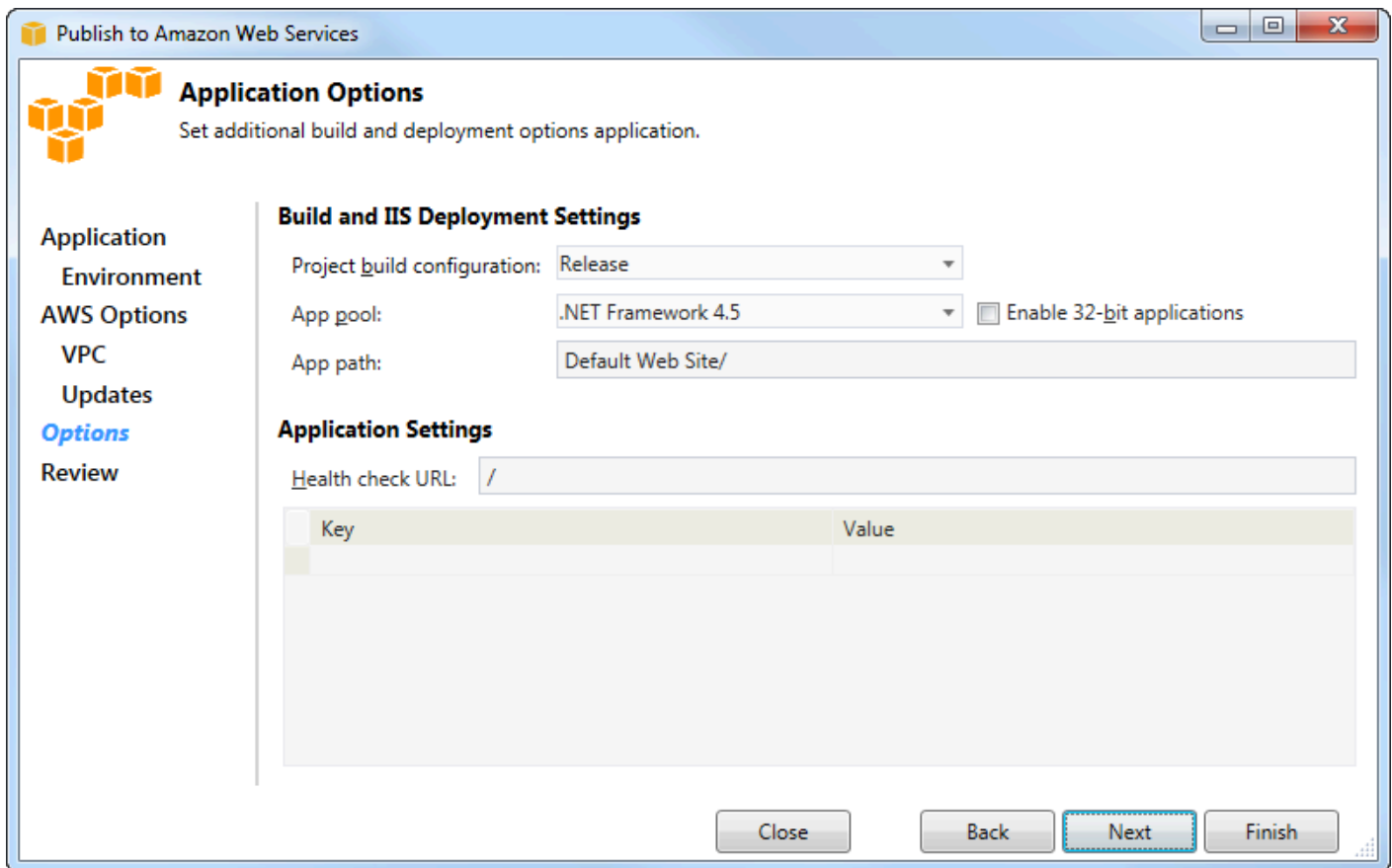
Enables you to specify the number of instances that remain in service during environment configuration updates.

Maximum Batch Size: The maximum number of instances that should be modified at any given time.

Minimum instance in service: The minimum number of instances that should be in service at any given time.

Close Back Next Finish

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 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.



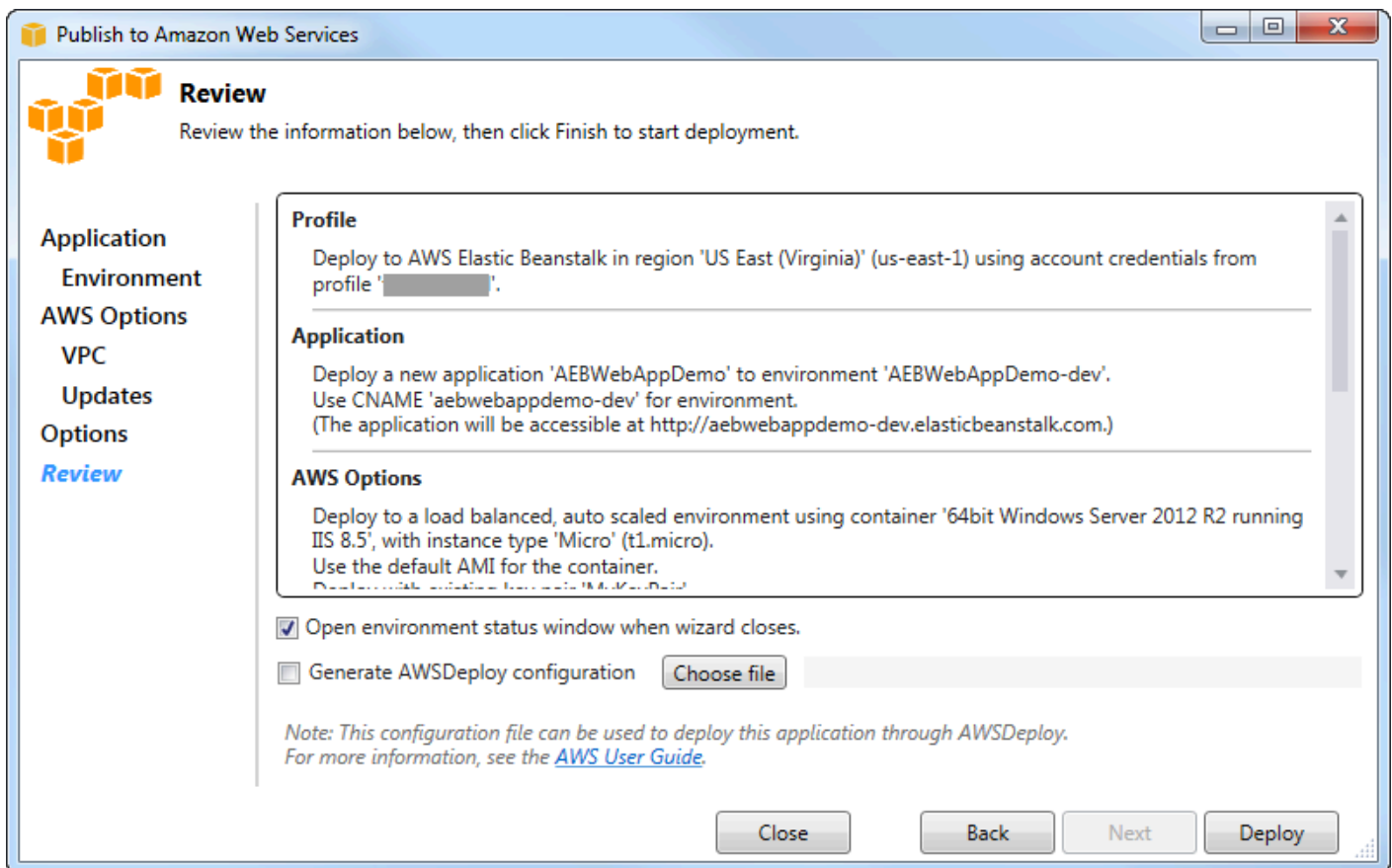
7. Na área Build and IIS Deployment Settings (Configurações de compilação e implantação IIS), na lista suspensa Project build configuration (Configuração de compilação do projeto), escolha a configuração da compilação de destino. Se o assistente conseguir encontrá-la, Release (Liberar) será exibida, 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 de aplicação, na caixa URL de verificação de integridade, digite um URL para o Elastic Beanstalk a fim de verificar se a aplicação web ainda responde. 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 AWS as credenciais sob as quais seu aplicativo deve ser executado. A abordagem preferida é especificar um perfil do IAM na lista suspensa Perfil do Identity and Access Management da página Opções da AWS. No entanto, se você precisar usar AWS credenciais em vez de uma função do IAM para executar seu aplicativo, na linha Chave, escolha `AWSAccessChave`. Na linha Value (Valor), digite a chave de acesso. Repita essas etapas para `AWSecretKey`.

13 Escolha 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 implantar a aplicação, a conta ativa incorrerá em cobranças pelos recursos da AWS usados pela aplicação.

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, no AWS Explorer, expanda o nó do Elastic Beanstalk, abra o menu de contexto (clique com o botão direito do mouse) do subnó da implantação e escolha Excluir. O processo de exclusão pode demorar alguns minutos.

Implantar uma aplicação ASP.NET Core no Elastic Beanstalk (herdado)

Important

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](#).

AWS Elastic Beanstalk é um serviço que simplifica o processo de provisionamento de AWS recursos para seu aplicativo. AWS Elastic Beanstalk fornece toda a AWS infraestrutura necessária para implantar seu aplicativo.

O Toolkit for Visual Studio oferece suporte à implantação de aplicativos ASP.NET Core usando AWS 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 Beanstalk facilita a implantação de aplicativos em uma variedade de idiomas diferentes para AWS. O Elastic Beanstalk é compatível com aplicações tradicionais do ASP.NET e 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 kit de ferramentas para 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 você nunca usou o kit de ferramentas antes, a primeira coisa que você precisará fazer depois de instalar o kit de ferramentas é registrar suas AWS credenciais no kit de ferramentas. Consulte [Como especificar as credenciais AWS 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 em... AWS

Na primeira página do assistente Publish to AWS Elastic Beanstalk deployment, escolha criar um novo aplicativo do 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 os AWS 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, AWS Opções, permite que você configure o tipo de AWS 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 atribuir AWS credenciais às instâncias do EC2 que executam seu aplicativo. Isso é importante se seu aplicativo usa o AWS SDK para .NET para acessar outros

AWS 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 carregado AWS, você pode verificar o status do ambiente do Elastic Beanstalk abrindo a visualização AWS de status do ambiente no 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. Ali também é possível extrair os logs do ambiente ou da área de trabalho remota para as instâncias do Amazon EC2 que fazem parte do ambiente do Elastic Beanstalk.

A primeira implantação de qualquer aplicativo demorará um pouco mais do que as reimplementações subsequentes, pois cria novos AWS 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.

Republicar pacotes da aplicação usando as configurações da execução anterior por meio do assistente de implantação e carregue o pacote de aplicações no ambiente do Elastic Beanstalk existente.

Como especificar as credenciais AWS de segurança para seu aplicativo

A AWS conta que você especifica no assistente Publicar no Elastic Beanstalk AWS é a conta que o assistente usará para implantação no Elastic Beanstalk.

Embora não seja recomendado, talvez você também precise especificar as credenciais da AWS conta que seu aplicativo usará para acessar AWS os serviços após a implantação. A abordagem preferida é especificar um perfil do IAM. No assistente Publicar no Elastic Beanstalk, você pode fazer

isso por meio da lista suspensa Perfil do Identity and Access Management na página Opções da AWS . No assistente herdado Publicar na Amazon Web Services, você pode fazer isso por meio da lista suspensa Perfil do IAM na página AWS Opções da AWS.

Se precisar usar credenciais de AWS conta em vez de uma função do IAM, você pode especificar as credenciais da AWS conta para seu aplicativo de uma das seguintes formas:

- Faça referência a um perfil correspondente às credenciais da AWS conta no appSettings elemento do Web.config arquivo do projeto. (Para criar um perfil, consulte [Configuração de AWS credenciais](#).) 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 o assistente Publish to Elastic Beanstalk, na página Opções do aplicativo, na linha Chave da área Chave e Valor, escolha. AWS AccessKey Na linha Value (Valor), digite a chave de acesso. Repita essas etapas para AWS SecretKey.
- Se estiver usando o assistente Publicar na Amazon Web Services legado, na área Credenciais da aplicação da página Opções de aplicação, selecione Usar estas credenciais e digite a chave de acesso e a chave de acesso secreta nas caixas Chave de acesso e Chave secreta.

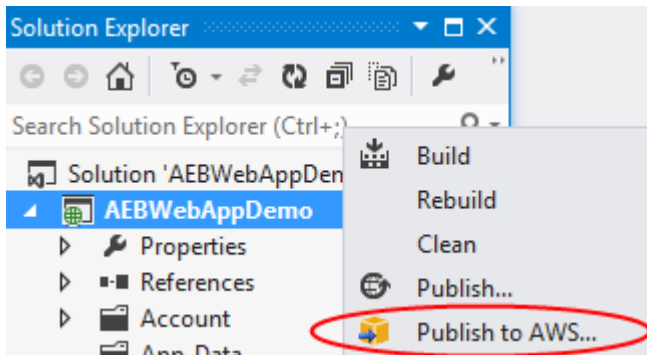
Como republicar a aplicação em um ambiente do Elastic Beanstalk (herdado)

Important

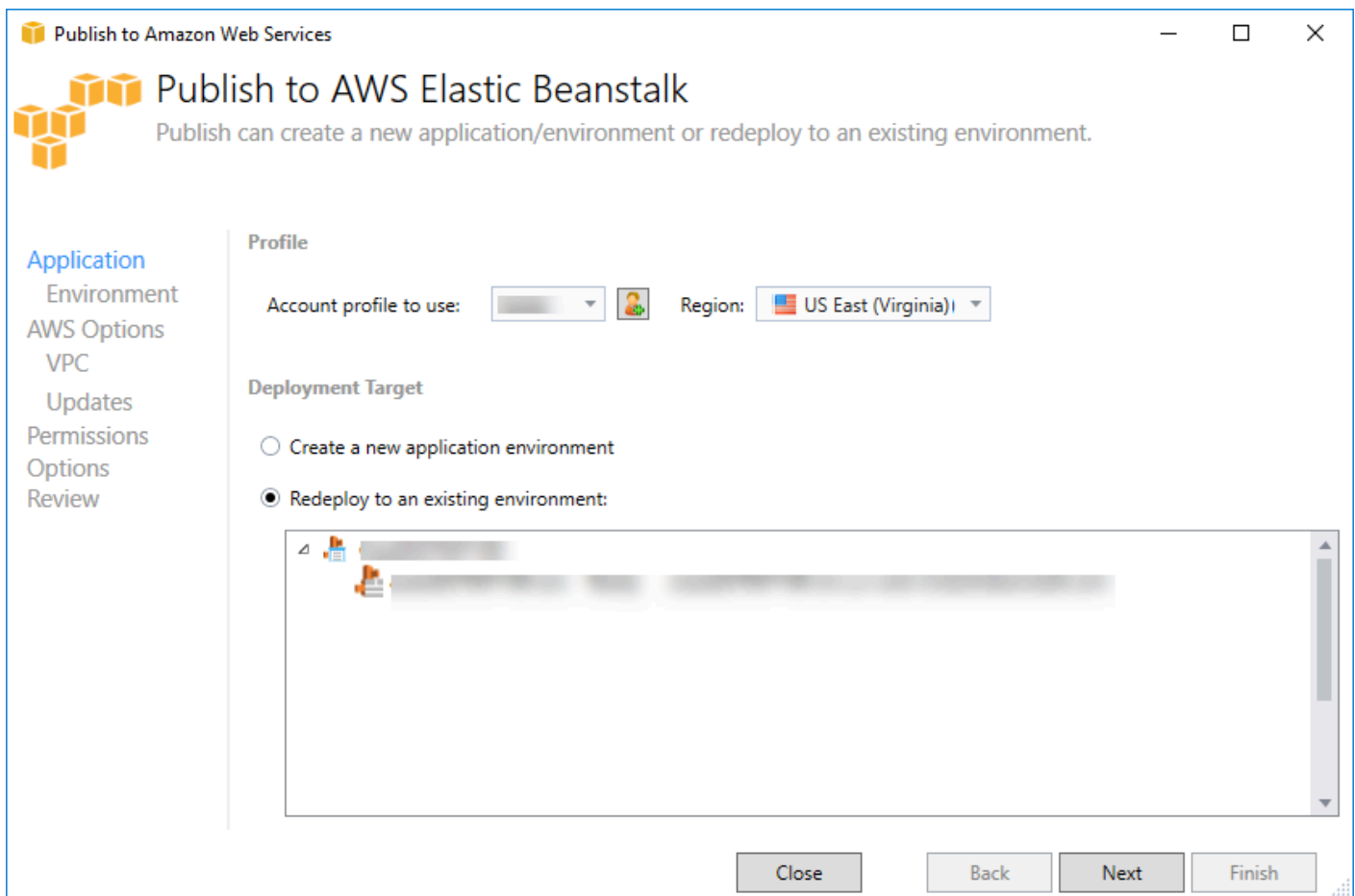
Esta documentação refere-se a serviços e recursos herdados. Para obter guias e conteúdos atualizados, consulte o guia da [ferramenta de implantação de .NET da AWS](#).

É possível iterar na aplicação fazendo alterações discretas e publicando novamente uma nova versão no ambiente do Elastic Beanstalk já iniciado.

1. No Solution Explorer, abra o menu de contexto (clique com o AEBWebAppDemobotão direito do mouse) da pasta do projeto publicado na seção anterior e escolha Publicar AWS Elastic Beanstalk em.

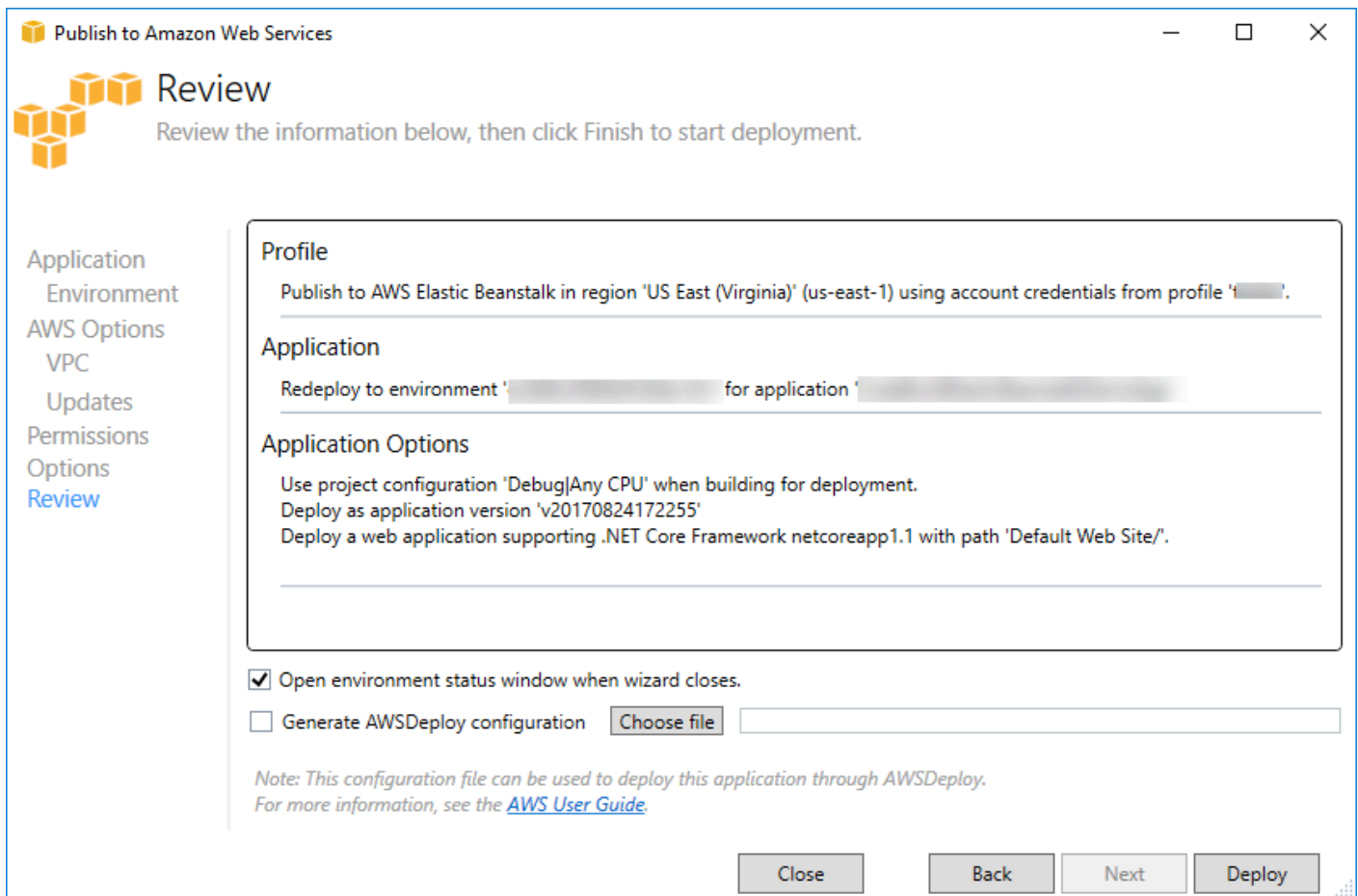


O assistente Publish to Elastic Beanstalk (Publicar no Elastic Beanstalk) é exibido.



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 em que sentido o manifesto de implantação do contêiner do Microsoft Windows do Elastic Beanstalk é compatível com as implantações de aplicação personalizadas.

As implantações de aplicação personalizadas são um recurso de ponta para usuários avançados que desejam aproveitar a eficiência do Elastic Beanstalk para criar e gerenciar os recursos da AWS e querem controle completo sobre a maneira como a aplicação é implantada. Para uma implantação de aplicação personalizada, você pode criar scripts do Windows PowerShell para as três diferentes ações 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 em 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 caso básico que implanta um site estático simples. No entanto, com a implantação de aplicação personalizada, você pode implantar qualquer tipo de aplicação e permitir que o Elastic Beanstalk gerencie os recursos da AWS para ela.

Implantações personalizadas do ASP.NET Core com o Elastic Beanstalk

Este tópico descreve como a implantação funciona e o que você pode fazer para personalizar implantações ao criar aplicações ASP.NET Core com o Elastic Beanstalk e o kit de ferramentas para Visual Studio.

Depois que você concluir o assistente de implantação no kit de ferramentas para Visual Studio, o kit empacotará a aplicação e a enviará ao 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 chamado `aws-windows-deployment-manifest.json`, que o contêiner do Elastic Beanstalk Windows (versão 1.2 ou posterior) lê para determinar como implantar a aplicação. 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, invoca 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 um arquivo msdeploy.

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 `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 acima do que o assistente de implantação comporta. Como a AWS definiu um esquema JSON para o arquivo `aws-windows-deployment-manifest.json`, quando você instalou o kit de ferramentas para 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?

Os arquivos de configuração .ebextensions do Elastic Beanstalk são compatíveis com 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 publishOptions no arquivo project.json. Para obter mais informações sobre .ebextensions, confira o [Guia do desenvolvedor do Elastic Beanstalk](#).

Suporte a várias aplicações para o .NET e o Elastic Beanstalk

Usando o manifesto de implantação, você pode implantar várias aplicações 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 aplicações e atualizar um ambiente do Elastic Beanstalk 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 o ambiente do Elastic Beanstalk sobre o que fazer com todos essas aplicações, copie o manifesto da solução para o espaço de trabalho 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)
```

Tendo já criado o pacote de aplicações, você pode acessar o console da web e carregar o arquivo em um ambiente do Elastic Beanstalk. Também é possível continuar usando os cmdlets do PowerShell da AWS para atualizar o ambiente do Elastic Beanstalk com o pacote de aplicações. Verifique se você definiu o perfil e a região atuais segundo o perfil e a região que contêm o ambiente do Elastic Beanstalk usando os cmdlets Set-AWSCredentials e Set-DefaultAWSRegion.

```
Write-Host 'Write application bundle to S3'
# Determine S3 bucket to store application bundle
$s3Bucket = New-EBStorageLocation
Write-S3Object -BucketName $s3Bucket -File $appBundle

$applicationName = "ASPNETCoreOnAWS"
$environmentName = "ASPNETCoreOnAWS-dev"
$versionLabel = [System.DateTime]::Now.Ticks.ToString()

Write-Host 'Update Beanstalk environment for new application bundle'
New-EBApplicationVersion -ApplicationName $applicationName -VersionLabel $versionLabel
  -SourceBundle_S3Bucket $s3Bucket -SourceBundle_S3Key app-bundle.zip
Update-EBEnvironment -ApplicationName $applicationName -EnvironmentName
  $environmentName -VersionLabel $versionLabel
```

Agora verifique o status da atualização usando página de status do ambiente do Elastic Beanstalk no kit de ferramentas ou no console da 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 novo recurso Publicar na AWS foi projetado para simplificar a forma como você publica aplicações .NET na AWS. Você pode ter de confirmar se deseja mudar para essa experiência de publicação depois de escolher Publicar contêiner na AWS. Para obter mais informações, consulte [Trabalhar com o Publicar na AWS no Visual Studio](#).

O Amazon Elastic Container Service é um serviço de gerenciamento de contêiner altamente escalável e de alta performance que oferece suporte aos contêineres do Docker e permite que você execute aplicações facilmente em um cluster gerenciado de instâncias do Amazon EC2.

Para implantar aplicações no Amazon Elastic Container Service, os componentes da aplicação 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 kit de ferramentas para Visual Studio fornece um assistente que simplifica a publicação de aplicações por meio do Amazon ECS. Esse assistente é descrito nas seções a seguir.

Para obter mais informações sobre o Amazon ECS, consulte a documentação do [Elastic Container Service](#). Ela inclui uma visão geral dos [conceitos básicos do Docker](#) e da [criação de um cluster](#).

Tópicos

- [Especifique AWS as credenciais para seu aplicativo ASP.NET Core 2](#)
- [Implantar uma aplicação ASP.NET Core 2.0 no Amazon ECS \(Fargate\) \(herdado\)](#)
- [Implantar uma aplicação ASP.NET Core 2.0 no Amazon ECS \(EC2\)](#)

Especifique AWS as credenciais 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 Publish Container como AWS assistente 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 da instância são usadas pela instância (incluindo seu aplicativo) para acessar diferentes AWS serviços. Por exemplo, a aplicação ASP.NET Core 2.0 que lê e grava em objetos do Amazon S3 precisa 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

A AWS conta que você especifica no Publish Container to AWS Wizard é a AWS conta que o assistente usará para implantação no Amazon ECS. O perfil da conta deve ter permissões para Amazon Elastic Compute Cloud, Amazon Elastic Container Service e AWS 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 a aplicação e não o vir na página Cluster do assistente Publicar contêiner na AWS. 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 as `AWSSDK.Extensions.NETCore.NuGet` Pacote de configuração para seu projeto.
2. Adicione AWS configurações a `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 um perfil do IAM para controlar o que a aplicação (e o serviço) pode acessar. Por exemplo, para configurar um perfil do IAM usando o Amazon ECS como serviço principal com permissões para o Amazon Simple Storage Service e o Amazon DynamoDB pelo Console de gerenciamento da AWS:

1. Faça login no Console de gerenciamento da AWS e abra o console do IAM em <https://console.aws.amazon.com/iam/>.
2. No painel de navegação do console do IAM, escolha Perfis e, em seguida, Criar perfil.
3. Escolha o tipo de perfil do serviço da AWS e selecione EC2 Container Service.
4. Escolha o caso de uso EC2 Container Service Task (Tarefa do EC2 Container Service). Os casos de uso são definidos pelo serviço para incluir a política de confiança que o serviço exige. Então, escolha Próximo: permissões.
5. Escolha as políticas de permissões do AmazonS3 FullAccess e do AmazonDynamoDBFullAccess. Marque a caixa de seleção ao lado de cada política e escolha Next: Review (Próximo: Análise).
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 AWS. Eles não são diferenciados por maiúsculas e minúsculas. Por exemplo, não é

possível criar perfis denominados `PRODR0LE` 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 Criar função.

Você pode usar esse perfil como o perfil da tarefa na página Definição de tarefas do ECS do assistente Publicar contêiner na AWS.

Para obter mais informações, consulte [Uso de funções baseadas em serviços](#).

Implantar uma aplicação ASP.NET Core 2.0 no Amazon ECS (Fargate) (herdado)

Important

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](#).

Esta seção descreve como usar o assistente Publicar na AWS, fornecido como parte do kit de ferramentas para Visual Studio, para implantar uma aplicação ASP.NET Core 2.0 em contêiner direcionada para Linux por meio do Amazon ECS usando o tipo de execução do Fargate. Como um aplicativo web é destinado a funcionar continuamente, ele será implantado como um serviço.

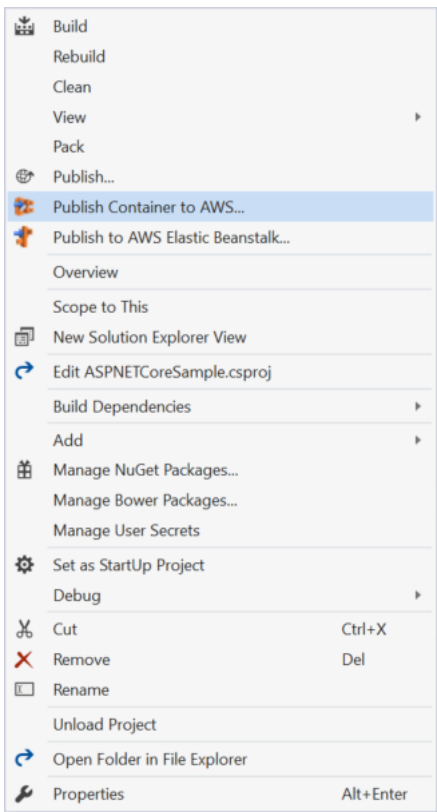
Antes de publicar o contêiner

Antes de usar o assistente Publicar contêiner na AWS para implantar a aplicação ASP.NET Core 2.0:

- [Especifique suas credenciais da AWS](#) e [faça a configuração no 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 uma aplicação ASP.NET Core 2.0 em contêiner direcionada para Linux.

Acessando o contêiner de publicação no AWS assistente

Para implantar uma aplicação ASP.NET Core 2.0 em contêiner direcionada para Linux, clique com o botão direito no projeto no Solution Explorer e selecione Publicar contêiner na AWS.



Você também pode selecionar Publicar contêiner na AWS no menu Compilar do Visual Studio.

Publicar contêiner no AWS assistente

Publish Container to AWS

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

Profile

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

Docker Image Build

Configuration: Release

Docker Repository: aspnetcoresample Tag: latest

Deployment Target

Service on an ECS Cluster

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

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

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

Close Back Next Publish

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.

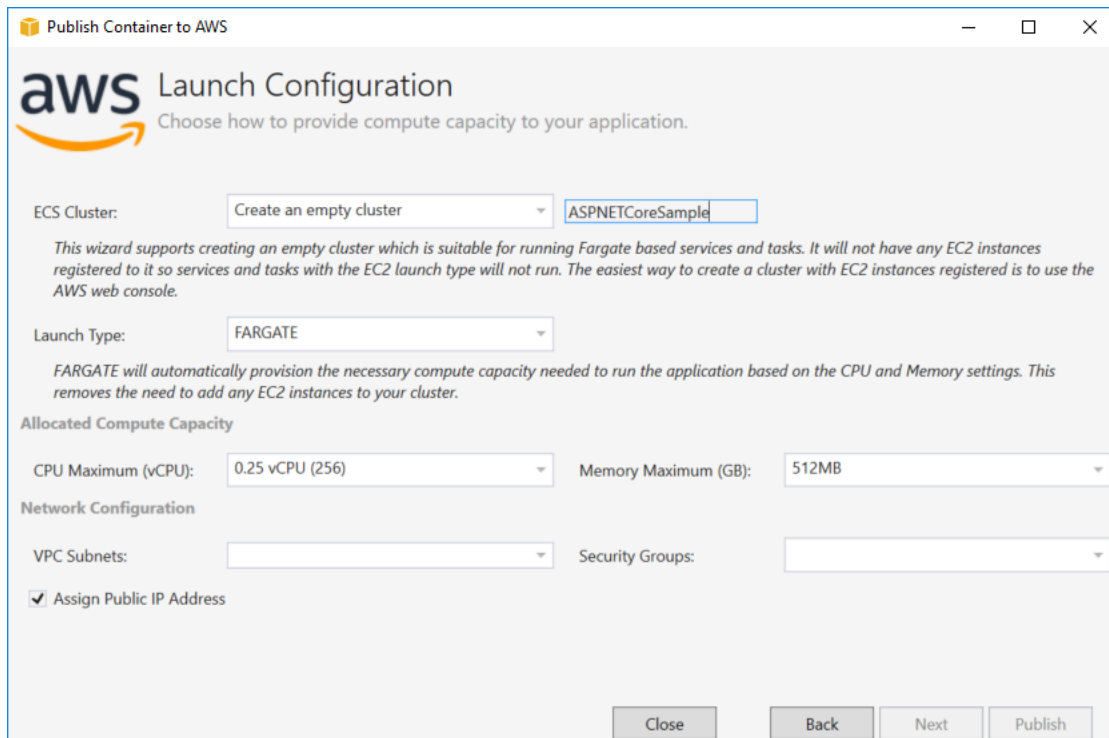
Repositório do Docker — escolha um repositório existente do Docker ou digite o nome de um novo repositório e ele será criado. Este é o repositório para onde o contêiner de compilação é enviado.

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).

Salvar as configurações no **aws-docker-tools-defaults.json** e configurar o projeto para ser implantado pela 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



The screenshot shows the 'Publish Container to AWS' wizard window. The title bar reads 'Publish Container to AWS'. The main content area has the AWS logo and the text 'Launch Configuration Choose how to provide compute capacity to your application.' Below this, there are several configuration sections:

- ECS Cluster:** A dropdown menu set to 'Create an empty cluster' and a text input field containing 'ASPNETCoreSample'. A note below states: 'This wizard supports creating an empty cluster which is suitable for running Fargate based services and tasks. It will not have any EC2 instances registered to it so services and tasks with the EC2 launch type will not run. The easiest way to create a cluster with EC2 instances registered is to use the AWS web console.'
- Launch Type:** A dropdown menu set to 'FARGATE'. A note below states: 'FARGATE will automatically provision the necessary compute capacity needed to run the application based on the CPU and Memory settings. This removes the need to add any EC2 instances to your cluster.'
- Allocated Compute Capacity:** Two dropdown menus: 'CPU Maximum (vCPU):' set to '0.25 vCPU (256)' and 'Memory Maximum (GB):' set to '512MB'.
- Network Configuration:** Two dropdown menus: 'VPC Subnets:' and 'Security Groups:'. A checkbox labeled 'Assign Public IP Address' is checked.

At the bottom right, there are four buttons: 'Close', 'Back', 'Next', and 'Publish'.

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](#).

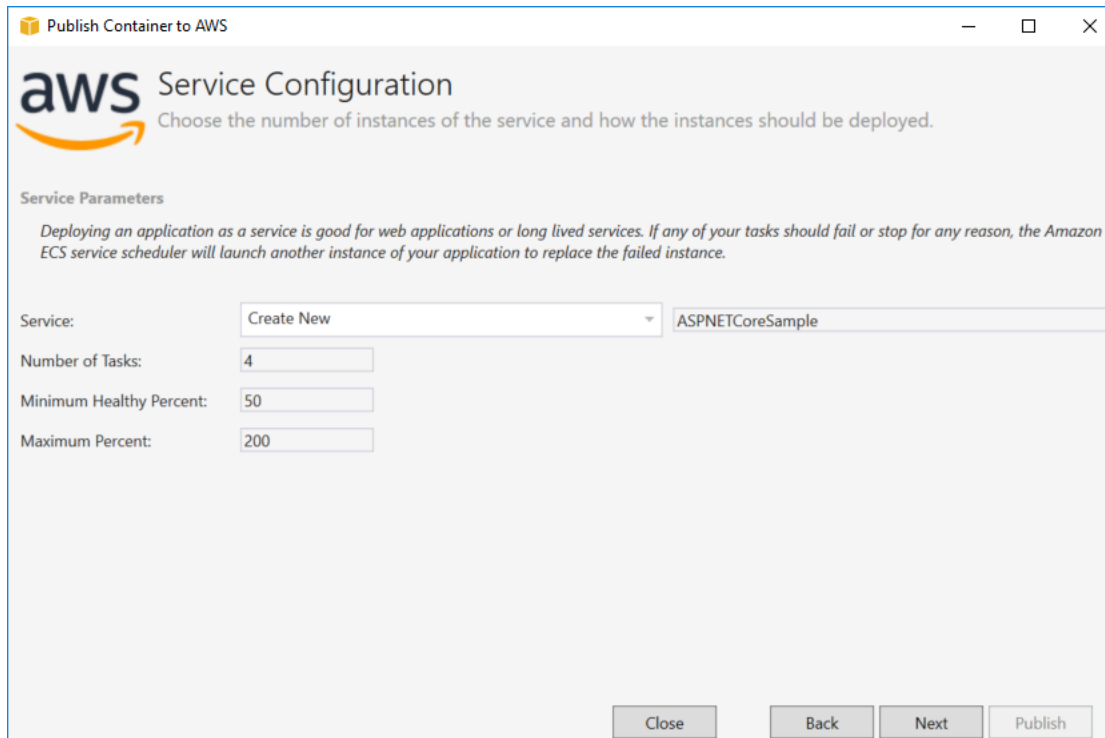
Grupos de segurança — escolha um grupo de segurança.

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.

Os [grupos de segurança padrão](#) são configurados para permitir tráfego de entrada de instâncias atribuídas ao mesmo grupo de segurança e todo o tráfego de saída 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

aws Application Load Balancer Configuration

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

Configure Application Load Balancer

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

Load Balancer:

Listener Port:

Load Balancer Target Group

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

Target Group:

Path Pattern:

Health Check Path:

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 de destino: selecione o grupo de destino no qual o Amazon ECS registrará as tarefas do 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

Task Definition: Create New ASPNETCoreSample

Container: Create New ASPNETCoreSample

Permissions

Task Role: [Empty]

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

Task Execution Role: ecsTaskExecutionRole

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

Port Mapping

Container Port
80

Environment Variables

Variable	Value
ASPNETCORE_ENVIRONMENT	Production

Buttons: Add... Add... Close Back Next Publish

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 da tarefa: selecione uma função do IAM que tenha as credenciais que seu aplicativo precisa para acessar AWS os Serviços. Esta é a forma como as credenciais são passadas para o seu aplicativo. Consulte [Como especificar as credenciais de segurança da AWS para a aplicação](#).

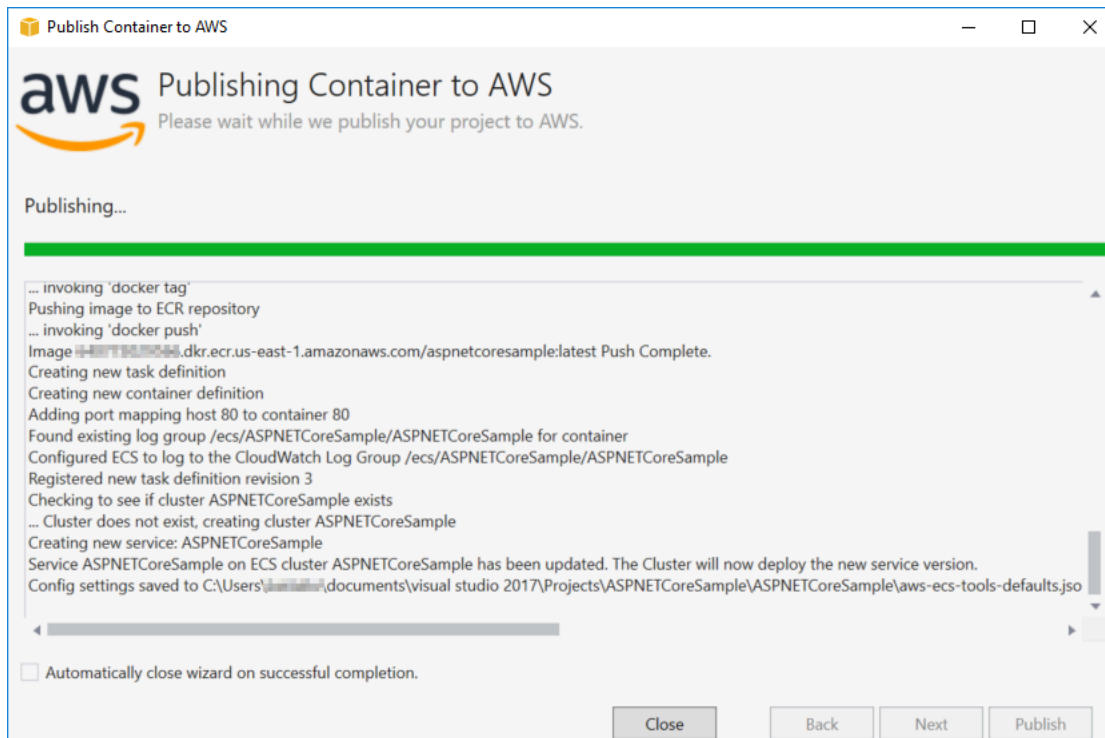
Função de execução de tarefas - Selecione uma função com permissões para extrair imagens privadas e publicar registros. AWS Fargate o usará em seu nome.

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 em AWS



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 das suas novas instâncias no AWS Explorer. Expanda o Amazon ECS e os clusters e, em seguida, clique no seu cluster.

Implantar uma aplicação ASP.NET Core 2.0 no Amazon ECS (EC2)

Esta seção descreve como usar o assistente Publicar contêiner na AWS, fornecido como parte do kit de ferramentas para Visual Studio, para implantar uma aplicação ASP.NET Core 2.0 em contêineres direcionados para Linux por meio do Amazon ECS usando o tipo de execução do EC2. Como uma aplicação web é desenvolvida para funcionar continuamente, ela será implantada como um serviço.

Antes de publicar o contêiner

Antes de usar Publicar contêiner na AWS para implantar sua aplicação ASP.NET Core 2.0:

- [Especifique suas credenciais da AWS](#) e [faça a configuração no 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 uma aplicação ASP.NET Core 2.0 em contêiner direcionada para Linux.

Acessando o contêiner de publicação no AWS assistente

Para implantar uma aplicação ASP.NET Core 2.0 em contêiner direcionada para Linux, clique com o botão direito no projeto no Solution Explorer e selecione Publicar contêiner na AWS.

Você também pode selecionar Publicar contêiner na AWS no menu Compilar do Visual Studio.

Publicar contêiner no AWS assistente

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 as configurações no **aws-docker-tools-defaults.json** e configurar o projeto para ser implantado pela 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 pode [criar um cluster ECS](#) usando o AWS Management Console.

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 - distribua tarefas entre 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 da tarefa - Selecione uma função de tarefa para uma função do IAM que permita ao contêiner chamar as AWS APIs que estão especificadas nas políticas associadas em seu nome. Esta é a forma como as credenciais são passadas para o seu aplicativo. Veja [como especificar credenciais AWS 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.

Contêiner de publicação em AWS

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 das suas novas instâncias no AWS Explorer. 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](#)
- [Visualizar e filtrar as verificações de segurança do Amazon Q](#)
- [O AWS kit de ferramentas não está instalado corretamente](#)
- [Configurações de firewall e proxy](#)

Práticas recomendadas de solução de problemas

As práticas recomendadas a seguir são sugeridas para a solução problemas do AWS Toolkit for Visual Studio .

- Repare o Visual Studio e reinicie o sistema.
- 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.

Reparar o Visual Studio e reiniciar o sistema

1. Feche todas as instâncias em execução do Visual Studio.
2. No menu Iniciar do Windows, execute o instalador do Visual Studio.
3. Execute a ação de reparo nas instalações afetadas do Visual Studio. Isso permitirá que o Visual Studio recompile seu índice de extensões instaladas.
4. Reinicie o Windows antes de reiniciar o Visual Studio.

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.

Visualizar e filtrar as verificações de segurança do Amazon Q

Para ver as verificações de segurança do Amazon Q no Visual Studio, abra a Lista de erros do Visual Studio expandindo o cabeçalho Exibir no menu principal do Visual Studio e selecionando Lista de erros.

Por padrão, a Lista de erros do Visual Studio exibe todos os avisos e erros da sua base de código. Para filtrar as descobertas da verificação de segurança do Amazon Q da Lista de erros do Visual Studio, crie um filtro concluindo o procedimento a seguir.

Note

As descobertas da verificação de segurança do Amazon Q só ficam visíveis após a execução de uma verificação de segurança e a detecção de problemas.

As descobertas da verificação de segurança do Amazon Q aparecem como avisos no Visual Studio. Para visualizar as descobertas da verificação de segurança do Amazon Q na Lista de erros, a opção Avisos no cabeçalho da Lista de erros deve ser selecionada.

1. No menu principal do Visual Studio, expanda o cabeçalho Exibir e selecione Lista de erros para abrir o painel Lista de erros.
2. No painel Lista de erros, clique com o botão direito da linha do cabeçalho e abra o menu de contexto.
3. No menu de contexto, expanda Mostrar colunas e selecione Ferramenta no menu expandido.
4. A coluna Ferramenta é adicionada à sua Lista de erros.
5. No cabeçalho da coluna Ferramenta, selecione o ícone Filtro e escolha Amazon Q para filtrar as descobertas da verificação de segurança do Amazon Q.

O AWS kit de ferramentas não está instalado corretamente

Problema:

Dentro de um minuto após iniciar o Visual Studio, AWS Toolkit for Visual Studio as seguintes mensagens aparecem no painel de saída e na barra de informações, respectivamente:

```
Some Toolkit components could not be initialized. Some functionality may not work during this IDE session.
```

```
The AWS Toolkit is not properly installed.
```

Solução:

É possível que a atualização ou instalação de uma extensão tenha causado o desaparecimento de alguns dos arquivos de cache internos do Visual Studio out-of-sync. O procedimento a seguir descreve como recompilar esses arquivos na próxima vez que você inicializar o Visual Studio.

Note

É possível que essa solução tenha impacto nas suas personalizações do Visual Studio. Depois de concluir esse procedimento, a extensão do AWS Toolkit deve ser listada como instalada e não reportar mais uma mensagem de erro. Se você continuar enfrentando esse problema depois de concluir as etapas a seguir, consulte o [Problema #452](#) no AWS Toolkit for Visual Studio GitHub repositório para obter informações adicionais.

1. Instale a versão mais recente do Visual Studio 2022.

Note

A versão mínima exigida é 17.11.5.

2. Feche todas as instâncias em execução do Visual Studio.
3. No Windows, abra o Prompt de Comando do Desenvolvedor como Administrador.
4. No Prompt de Comando do Desenvolvedor, execute o comando `devenv /updateconfiguration /resetExtensions` e aguarde sua conclusão.
5. Depois que o comando for concluído, reinicie o Visual Studio.
6. No Visual Studio, a AWS extensão agora está listada como instalada e não relata mais as mensagens de erro listadas na parte superior desse problema.

Configurações de firewall e proxy

Solucionar problemas nas configurações de firewall e proxy

O software de verificações de segurança pode interferir na sua capacidade de baixar arquivos dos servidores de linguagens do kit de ferramentas da AWS , removendo arquivos dos downloads ou impedindo completamente os downloads.

Para verificar suas configurações de firewall e proxy, navegue até <https://aws-toolkit-language-servers.amazonaws.com/codewhisperer/0/manifest.json> em um navegador da Internet instalado no mesmo sistema da sua instância do Visual Studio. Se houver um erro ou se a página não carregar, poderá haver um firewall ou filtro de proxy impedindo que você acesse `aws-toolkit-language-servers.amazonaws.com`.

Certificados personalizados

O AWS Toolkit for Visual Studio utiliza um servidor de linguagem que é executado no tempo de execução do Node.js. Para obter informações detalhadas sobre como verificar se a sua rede usa um certificado personalizado, consulte o tópico [Definições de configuração e arquivo de credenciais na AWS CLI](#) no Guia do usuário da AWS Command Line Interface versão 1.

Para definir configurações de proxy e um certificado, configure a variável de ambiente `HTTPS_PROXY` e crie variáveis de ambiente do Windows para as chaves `NODE_OPTIONS` e `NODE_EXTRA_CA_CERTS`.

Para configurar a variável de ambiente `HTTPS_PROXY`, conclua as etapas a seguir.

1. No menu principal do Visual Studio, selecione Ferramentas e Opções.
2. No menu Opções, expanda Kit de ferramentas da AWS e escolha Proxy.
3. No menu Proxy, defina o Host e a Porta.

Note

Para obter informações sobre como configurar o `HTTPS_PROXY` partir do AWS CLI, consulte o AWS CLI tópico [Usando um proxy HTTP](#) no Guia do AWS Command Line Interface Usuário.

Crie variáveis de ambiente do Windows para as chaves a seguir.

- `NODE_OPTIONS = --use-openssl-ca`
- `NODE_EXTRA_CA_CERTS = Path/To/Corporate/Certs`

Note

Para saber mais sobre como extrair certificados-raiz corporativos, consulte o artigo [Exportar um certificado com sua chave privada](#) em learn.microsoft.com. Para obter informações detalhadas sobre as chaves de variáveis de ambiente do Windows, consulte a [documentação do Node.js v23.3.0](#) em nodejs.org.

Permitir listagem e etapas adicionais

Além de interferir nos servidores de linguagem do AWS Toolkit, as configurações do firewall podem impedir que o Amazon Q faça o upload para o Amazon S3 e chame a API do serviço. Para minimizar o potencial desses erros, recomendamos permitir o acesso de saída à internet na porta 443 (HTTPS) para os seguintes endpoints:

- `https://codewhisperer.us-east-1.amazonaws.com/`
- `https://amazonq-code-transformation-us-east-1-c6160f047e0.s3.amazonaws.com/`

- <https://aws-toolkit-language-servers.amazonaws.com/>
- <https://q.us-east-1.amazonaws.com>
- <https://client-telemetry.us-east-1.amazonaws.com>
- <https://cognito-identity.us-east-1.amazonaws.com>
- <https://oidc.us-east-1.amazonaws.com>

Para obter uma lista detalhada dos endpoints, consulte o tópico [Atualizar firewalls e gateways para permitir o acesso](#) neste Guia do usuário. Para obter informações detalhadas sobre como configurar um proxy corporativo para o Amazon Q, consulte o tópico [Configurar um proxy corporativo no Amazon Q](#) no Guia do usuário do Amazon Q Developer. Se você continuar enfrentando problemas de firewall e proxy, colete os registros do AWS kit de ferramentas e entre em contato com a AWS Toolkit for Visual Studio equipe por meio da seção de [AWS Toolkit for Visual Studio problemas](#) do AWS Toolkit for Visual Studio GitHub repositório. Para obter detalhes sobre como coletar os registros do AWS kit de ferramentas, consulte as informações na seção de melhores práticas de solução de problemas deste tópico do Guia do usuário.

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](#)
- [Gerenciamento de Identidade e Acesso](#)
- [Validação de conformidade para este AWS produto ou serviço](#)
- [Resiliência para este AWS produto ou serviço](#)
- [Segurança da infraestrutura para este AWS produto ou serviço](#)
- [Análise de configuração e vulnerabilidade em AWS Toolkit for Visual Studio](#)

Proteção de dados em AWS Toolkit for Visual Studio

O [modelo de responsabilidade AWS compartilhada](#) de se aplica à proteção de dados no AWS Toolkit for Visual Studio com o Amazon Q. 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 o conteúdo hospedado nessa infraestrutura. Você também é responsável pelas tarefas de configuração e gerenciamento de segurança dos Serviços da AWS que usa. Para saber mais sobre a privacidade de dados, consulte as [Data Privacy FAQ](#). Para saber mais sobre a proteção de dados na Europa, consulte a postagem do blog [AWS Shared Responsibility Model and RGPD](#) no Blog de segurança da AWS .

Para fins de proteção de dados, recomendamos que você proteja Conta da AWS as credenciais e configure usuários individuais com Centro de Identidade do AWS IAM 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 AWS os recursos. Exigimos TLS 1.2 e recomendamos TLS 1.3.
- Configure a API e o registro de atividades do usuário com AWS CloudTrail. Para obter informações sobre o uso de CloudTrail trilhas para capturar AWS atividades, consulte Como [trabalhar com CloudTrail trilhas](#) no Guia AWS CloudTrail do usuário.
- 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 sensíveis armazenados no Amazon S3.
- Se você precisar de módulos criptográficos validados pelo FIPS 140-3 ao acessar AWS por meio de uma interface de linha de comando ou de uma API, use um endpoint FIPS. Para saber mais sobre os endpoints FIPS disponíveis, consulte [Federal Information Processing Standard \(FIPS\) 140-3](#).

É altamente recomendável que nunca sejam colocadas informações confidenciais ou sensíveis, como endereços de e-mail de clientes, em tags ou campos de formato livre, como um campo Nome. Isso inclui quando você trabalha com o AWS Toolkit com o Amazon Q ou outro Serviços da AWS usando o console, a API ou AWS SDKs. AWS CLI Quaisquer dados inseridos em tags ou em 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, é fortemente recomendável que não sejam incluídas informações de credenciais no URL para validar a solicitação nesse servidor.

Gerenciamento de Identidade e Acesso

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](#)
- [Autenticação com identidades](#)
- [Gerenciar o acesso usando políticas](#)
- [Como Serviços da AWS trabalhar com o IAM](#)
- [Solução de problemas AWS de identidade e acesso](#)

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 a solicitar as permissões corretas ao administrador. Se você não conseguir acessar um recurso no AWS, consulte [Solução de problemas AWS de identidade e acesso](#) 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. Envie as solicitações ao administrador do IAM para alterar as permissões dos usuários de serviço. Revise as informações nesta página para compreender os conceitos básicos do 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 o 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.

Autenticação com identidades

A autenticação é a forma como você faz login AWS usando suas credenciais de identidade. Você deve estar autenticado como usuário do IAM ou assumindo uma função do IAM. Usuário raiz da conta da AWS

Você pode fazer login como uma identidade federada usando credenciais de uma fonte de identidade como Centro de Identidade do AWS IAM (IAM Identity Center), autenticação de login único ou credenciais. Google/Facebook Para ter mais informações sobre como fazer login, consulte [Como fazer login em sua Conta da AWS](#) no Guia do usuário do Início de Sessão da AWS .

Para acesso programático, AWS fornece um SDK e uma CLI para assinar solicitações criptograficamente. Para ter mais informações, consulte [AWS Signature Version 4 para solicitações de API](#) no Guia do usuário do IAM.

Conta da AWS usuário root

Ao criar um Conta da AWS, você começa com uma identidade de login chamada usuário Conta da AWS raiz que tem acesso completo a todos Serviços da AWS os recursos. É altamente recomendável não usar o usuário-raiz em tarefas diárias. Consulte as tarefas que exigem credenciais de usuário-raiz em [Tarefas que exigem credenciais de usuário-raiz](#) no Guia do usuário do IAM.

Identidade federada

Como prática recomendada, exija que os usuários humanos 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 corporativo, provedor de identidade da web ou Directory Service que acessa Serviços da AWS usando credenciais de uma fonte de identidade. As identidades federadas assumem funções que oferecem credenciais temporárias.

Para o gerenciamento de acesso centralizado, recomendamos Centro de Identidade do AWS IAM. Para saber mais, consulte [O que é o IAM Identity Center?](#) no Guia do usuário do Centro de Identidade do AWS IAM .

Usuários e grupos do IAM

Um [usuário do IAM](#) é uma identidade com permissões específicas para uma única pessoa ou aplicação. É recomendável usar credenciais temporárias, em vez de usuários do IAM com credenciais de longo prazo. Para obter mais informações, consulte [Exigir que usuários humanos usem a federação com um provedor de identidade para acessar AWS usando credenciais temporárias](#) no Guia do usuário do IAM.

Um [grupo do IAM](#) especifica um conjunto de usuários do IAM e facilita o gerenciamento de permissões para grandes conjuntos de usuários. Para ter mais informações, consulte [Casos de uso de usuários do IAM](#) no Guia do usuário do IAM.

Perfis do IAM

Uma [perfil do IAM](#) é uma identidade com permissões específicas que oferece credenciais temporárias. Você pode assumir uma função [mudando de um usuário para uma função do IAM \(console\)](#) ou chamando uma operação de AWS API AWS CLI ou. Para saber mais, consulte [Métodos para assumir um perfil](#) no Manual do usuário do IAM.

Os perfis do IAM são úteis para acesso de usuário federado, permissões de usuário do IAM temporárias, acesso entre contas, acesso entre serviços e aplicações em execução no Amazon EC2. Consulte mais informações em [Acesso a recursos entre contas no IAM](#) no Guia do usuário do IAM.

Gerenciar o acesso usando políticas

Você controla o acesso AWS criando políticas e anexando-as a AWS identidades ou recursos. Uma política define permissões quando associada a uma identidade ou recurso. AWS avalia essas políticas quando um diretor faz uma solicitação. A maioria das políticas é armazenada AWS como documentos JSON. Para ter mais informações sobre documentos de política JSON, consulte [Visão geral das políticas JSON](#) no Guia do usuário do IAM.

Por meio de políticas, os administradores especificam quem tem acesso a que, definindo qual entidade principal pode realizar ações em quais recursos e sob quais condições.

Por padrão, usuários e perfis não têm permissões. Um administrador do IAM cria políticas do IAM e as adiciona aos perfis, os quais os usuários podem então assumir. As políticas do IAM definem permissões, independentemente do método usado para realizar a operação.

Políticas baseadas em identidade

As políticas baseadas em identidade são documentos de políticas de permissão JSON que você anexa a uma identidade (usuário, grupo ou perfil). Essas políticas controlam quais ações as identidades podem realizar, em quais recursos e sob quais condições. Para saber como criar uma política baseada em identidade, consulte [Definir permissões personalizadas do IAM com as políticas gerenciadas pelo cliente](#) no Guia do Usuário do IAM.

As políticas baseadas em identidade podem ser políticas em linha (incorporadas diretamente em uma única identidade) ou políticas gerenciadas (políticas autônomas anexadas a várias identidades). Para saber como escolher entre uma política gerenciada e políticas em linha, consulte [Escolher 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. Entre os exemplos estão políticas de confiança de perfil do IAM e políticas de bucket do Amazon S3. Em serviços compatíveis com políticas baseadas em recursos, os administradores de serviço podem usá-las para controlar o acesso a um recurso específico. É necessário [especificar uma entidade principal](#) em uma política baseada em recursos.

Políticas baseadas em recursos são políticas em linha 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 diretores (membros da conta, usuários ou funções) têm permissões para acessar um recurso. ACLs são semelhantes às políticas baseadas em recursos, embora não usem o formato de documento de política JSON.

O Amazon S3 e o AWS WAF Amazon VPC são exemplos de serviços que oferecem suporte. ACLs Para saber mais ACLs, consulte a [visão geral 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 que podem definir o máximo de permissões concedidas por tipos de políticas mais comuns:

- Limites de permissões: definem o número máximo de permissões que uma política baseada em identidade pode conceder a uma entidade do IAM. Para saber mais sobre limites de permissões, consulte [Limites de permissões para identidades do IAM](#) no Guia do usuário do IAM.
- Políticas de controle de serviço (SCPs) — Especifique as permissões máximas para uma organização ou unidade organizacional em AWS Organizations. Para saber mais, consulte [Políticas de controle de serviço](#) no Guia do usuário do AWS Organizations .
- Políticas de controle de recursos (RCPs) — Defina o máximo de permissões disponíveis para recursos em suas contas. Para obter mais informações, consulte [Políticas de controle de recursos \(RCPs\)](#) no Guia AWS Organizations do usuário.
- Políticas de sessão: políticas avançadas transmitidas como um parâmetro durante a criação de uma sessão temporária para um perfil ou um usuário federado. Para saber mais, 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 `aws:GetWidget` fictícias.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
aws: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 `aws: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

É possível criar um perfil que os usuários de outras contas ou pessoas fora da organização podem usar para acessar seus recursos. É possível 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 essas políticas para conceder às pessoas acesso aos seus recursos.

Para saber mais, consulte:

- Para saber se é AWS compatível com esses recursos, consulte [Como Serviços da AWS trabalhar com o IAM](#).
- Para saber como fornecer acesso aos seus recursos em todas as Contas da AWS que você possui, consulte Como [fornecer acesso a um usuário do IAM em outra 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.
- Para saber como conceder acesso por meio da federação de identidades, consulte [Conceder acesso a usuários autenticados externamente \(federação de identidades\)](#) no Guia do usuário do IAM.
- Para saber a diferença entre perfis e políticas baseadas em recurso para acesso entre contas, consulte [Acesso a recursos entre contas no IAM](#) 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. Para obter mais informações sobre sua responsabilidade de conformidade ao usar Serviços da AWS, consulte a [documentação AWS de segurança](#).

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 altamente disponíveis, tolerantes a falhas e escaláveis que uma ou várias infraestruturas de data center 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 oferecer compatibilidade 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, comporta esses modos.

Além disso, as solicitações devem ser assinadas usando 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. Às vezes, essas atualizações incluem atualizações de segurança, por isso é importante manter o AWS Toolkit com o Amazon Q atualizado.

Para verificar se as atualizações automáticas para extensões estão habilitadas

1. Abra o gerenciador de extensões selecionando 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 as atualizações automáticas para extensões, verifique se há atualizações do kit de ferramentas da AWS com Amazon Q com a frequência adequada para o seu ambiente.

Histórico do documento do Guia do usuário do AWS Toolkit for Visual Studio

Histórico do documentos

A tabela a seguir descreve as alterações recentes importantes do Guia do usuário do AWS Toolkit for Visual Studio. Para receber notificações sobre atualizações dessa documentação, inscreva-se em um [feed RSS](#).

Alteração	Descrição	Data
Atualizações no conteúdo da seção Conceitos básicos	Atualizações no conteúdo das seções Conceitos básicos e Conectar-se à AWS para refletir as alterações feitas na interface do usuário.	24 de abril de 2025
Atualizar firewalls e gateways para permitir o acesso	Listas de endpoints e recursos que devem ser incluídos na lista de permissões para acesso a todos os serviços e recursos do AWS Toolkit for Visual Studio com Amazon Q para extensões.	20 de março de 2025
Solucionar problemas nas configurações de firewall e proxy	Adição de um novo tópico de solução de problemas que aborda as configurações de firewall e proxy para o AWS Toolkit for Visual Studio e o Amazon Q.	15 de dezembro de 2024
Atualização da solução de problemas de instalação	Atualização do conteúdo sobre problemas de instalação para considerar uma atualização da Microsoft.	20 de novembro de 2024

Atualizações no conteúdo da seção Conceitos básicos	Atualizações no conteúdo das seções Conceitos básicos e Conectar-se à AWS para refletir as alterações feitas na interface do usuário.	24 de outubro de 2024
Atualizações na seção Conectar-se à AWS	Atualizações no conteúdo da seção Conectar-se à AWS.	26 de setembro de 2024
Atualizações no conteúdo sobre AMIs do Amazon EC2	Atualizações de conteúdo para documentar as alterações no processo e nos procedimentos de AMIs do Amazon EC2.	13 de setembro de 2024
Não era possível inicializar os componentes do kit de ferramentas da AWS	Adição de um tópico de solução de problemas para resolver problemas em componentes do AWS Toolkit for Visual Studio que não eram inicializados.	13 de setembro de 2024
Visualizar e filtrar as verificações de segurança do Amazon Q	Adição de tópico de solução de problemas para ajudar na visualização e filtragem das verificações de segurança do Amazon Q.	31 de julho de 2024
Amazon Q para AWS Toolkit for Visual Studio	O Amazon Q já está disponível para o AWS Toolkit for Visual Studio.	30 de junho de 2024
Atualizações e manutenção de conteúdo	Atualização do conteúdo para alterações na interface do usuário e nas diretrizes de estilo da AWS.	6 de março de 2024

Atualizações e manutenção de conteúdo	Atualização do conteúdo para alterações na interface do usuário e nas diretrizes de estilo da AWS.	6 de março de 2024
Atualizações e manutenção de conteúdo	Atualização do conteúdo para alterações na interface do usuário e nas diretrizes de estilo da AWS.	6 de março de 2024
Atualizações e manutenção de conteúdo	Atualização do conteúdo para alterações na interface do usuário e nas diretrizes de estilo da AWS.	6 de março de 2024
Atualizações e manutenção de conteúdo	Atualização do conteúdo para alterações na interface do usuário e nas diretrizes de estilo da AWS.	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 acesso para ver as alterações.	22 de junho de 2023
Autenticação e acesso	Fornecer credenciais da AWS agora é intitulada Autenticação e acesso. Refatoração do sumário e dos subtópicos para atender aos requisitos de estilo e segurança da AWS.	4 de maio 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
Foram adicionadas informações do AWS Toolkit for Visual Studio 2022	Compatibilidade adicionada ao AWS Toolkit for Visual Studio para o Visual Studio 2022.	20 de dezembro de 2022
Atualizações do guia Publicar na AWS	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. Agora o guia encontra-se no guia Publicar na AWS.	6 de julho de 2022

[Implantar na AWS: atualizações de título e conteúdo](#)

A seção do guia formalmente intitulada “Deployment Using the AWS Toolkit” tem um sumário atualizado e agora é intitulada “Implantar na AWS”. Os seguintes guias foram descontinuados e não estão mais acessíveis: Implantar no Elastic Beanstalk (herdado) e Implantar no AWS CloudFormation (herdado). O conteúdo atualizado sobre a implantação no Elastic Beanstalk e no Cloudformation 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: Trabalhar com o CloudWatch Logs no Visual Studio	Criação do tópico Integração do Amazon CloudWatch Logs para Visual Studio neste guia.	29 de junho de 2022
Novo tópico do guia: Configurar a integração do CloudWatch Logs para o Visual Studio	Criação de uma seção de configuração da integração do Amazon CloudWatch Logs no Visual Studio neste guia.	29 de junho de 2022
Integração do CloudWatch Logs para o Visual Studio	Criação de um guia para a integração do Amazon CloudWatch Logs no Visual Studio, incluindo os seguintes tópicos: Configurar o CloudWatch Logs para o Visual Studio e Trabalhar com o CloudWatch Logs no Visual Studio .	29 de junho de 2022
Publicar no AWS	Publicar na AWS não está mais em visualização prévia. Atualizações para refletir as mudanças na interface de usuário e as melhorias nas sugestões de publicação.	1º de junho de 2022

Novo Publicar na AWS disponível para visualização prévia	Experiência de implantação aprimorada que fornece orientação sobre qual serviço da AWS é adequado para a aplicação.	21 de outubro de 2021
Compatibilidade com SSO e MFA para credenciais da AWS	Atualizado para documentar o novo suporte para o AWS Single Sign-On (Centro de Identidade do IAM) e autenticação multifator em credenciais da AWS.	21 de abril de 2021
Projeto básico do AWS Lambda de criação de imagem do 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
Fornecer credenciais da AWS	Atualizado com informações sobre como criar perfis de credenciais no arquivo compartilhado de credenciais da AWS.	20 de junho de 2019
Usar o projeto do AWS Lambda no kit de ferramentas da AWS para Visual Studio	O suporte para o Visual Studio 2019 foi adicionado ao kit de ferramentas da AWS para Visual Studio.	28 de março de 2019
Tutorial: Creating an Amazon Rekognition Lambda Application	O suporte para o Visual Studio 2019 foi adicionado ao kit de ferramentas da AWS para Visual Studio.	28 de março de 2019

Tutorial: Compilar e testar uma aplicação sem servidor com o AWS Lambda	O suporte para o Visual Studio 2019 foi adicionado ao kit de ferramentas da AWS para Visual Studio.	28 de março de 2019
Configurar o AWS Toolkit for Visual Studio	Compatibilidade adicionada ao AWS Toolkit for Visual Studio para o Visual Studio 2019.	28 de março de 2019
Implantar uma aplicação ASP.NET Core 2.0 (Fargate)	O suporte para o Visual Studio 2019 foi adicionado ao kit de ferramentas da AWS para 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 kit de ferramentas da AWS para Visual Studio.	28 de março de 2019
Criar um projeto de modelo do AWS CloudFormation no Visual Studio	O suporte para o Visual Studio 2019 foi adicionado ao kit de ferramentas da AWS para Visual Studio.	28 de março de 2019
Visualizações detalhadas do Container Service	Foram adicionadas informações sobre as exibições detalhadas dos clusters do Amazon Elastic Container Service e repositórios de contêineres fornecidos pelo AWS Explorer.	16 de fevereiro de 2018
Implantar no Amazon EC2 Container Service	Foram adicionadas informações 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 direcionado ao Linux por meio do Amazon ECS usando o tipo de execução do EC2.

16 de fevereiro de 2018

[Credenciais para implantação 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.