Guide de l'utilisateur

AWS Boîte à outils pour Visual Studio

AWS Boîte à outils pour Visual Studio: Guide de l'utilisateur

Table of Contents

AWS Toolkit for Visual Studio

Il s'agit du guide de l'utilisateur pour AWS Toolkit for Visual Studio. Si vous recherchez le AWS Toolkit pour VS Code for VS Code, consultez le guide de l'utilisateur du AWS Toolkit for Visual Studio Code.

Qu'est-ce que le Toolkit for Visual Studio

Il AWS Toolkit for Visual Studio s'agit d'un plugin pour l'IDE Visual Studio qui facilite le développement, le débogage et le déploiement d'applications .NET utilisant Amazon Web Services. Le Toolkit for Visual Studio est pris en charge pour les versions 2019 et ultérieures de Visual Studio. Pour plus d'informations sur le téléchargement et l'installation du kit, consultez la rubrique Installation et configuration du présent guide de l'utilisateur.

> **Note**
>
> Le Toolkit for Visual Studio a également été publié pour les versions de Visual Studio 2008, 2010, 2012, 2013, 2015 et 2017. Toutefois, ces versions ne sont plus prises en charge. Pour plus d'informations, consultez la rubrique Installation et configuration de ce guide de l'utilisateur.

Le Toolkit for Visual Studio contient les fonctionnalités suivantes pour améliorer votre expérience de développement.

AWS Explorateur

La fenêtre de l'outil AWS Explorer, disponible dans le menu Affichage de l'IDE, vous permet d'interagir avec de nombreux AWS services depuis l'IDE Visual Studio. Les services de données pris en charge incluent Amazon Simple Storage Service (Amazon S3), Amazon SimpleDB, Amazon Simple Notification Service (Amazon SNS), Amazon Simple Queue Service (Amazon SQS) et Amazon. CloudFront AWS Explorer permet également d'accéder à la gestion d'Amazon Elastic Compute Cloud (Amazon EC2) AWS Identity and Access Management , à la gestion des utilisateurs et des politiques (IAM), au déploiement d'applications et de fonctions sans serveur et au déploiement d'applications AWS Lambda Web vers et. AWS Elastic Beanstalk AWS CloudFormation

Gestion des informations d'identification et des régions

AWS Explorer prend en charge plusieurs AWS comptes (y compris les comptes utilisateur IAM) et régions, et vous permet de modifier facilement l'affichage d'un compte à l'autre ou de consulter et de gérer les ressources et les services dans différentes régions.

Amazon EC2

Dans AWS Explorer, vous pouvez afficher les Amazon Machine Images (AMI) disponibles, créer des instances Amazon EC2 à partir de ces AMI, puis vous connecter à ces instances à l'aide de Windows Remote Desktop. AWS Explorer permet également des fonctionnalités de support, telles que la capacité de créer et de gérer des paires de clés et des groupes de sécurité.

AWS Lambda

Vous pouvez utiliser Lambda pour héberger vos fonctions .NET Core C# sans serveur et vos applications sans serveur. Utilisez des plans pour créer rapidement de nouveaux projets sans serveur et prendre une longueur d'avance sur le développement de votre application sans serveur.

AWS CodeCommit

CodeCommit est intégré à Visual Studio Team Explorer. Cela facilite le clonage et la création de référentiels conservés CodeCommit, ainsi que l'utilisation des modifications du code source depuis l'IDE.

Amazon DynamoDB

DynamoDB est un service de base de données non relationnel rapide, hautement évolutif, hautement disponible et économique. Le Toolkit for Visual Studio fournit des fonctionnalités permettant d'utiliser Amazon DynamoDB dans un contexte de développement. Avec le Toolkit for Visual Studio, vous pouvez créer et modifier des attributs dans les tables DynamoDB et exécuter des opérations de numérisation sur les tables.

Amazon S3

Vous pouvez rapidement et facilement charger du contenu dans des compartiments Amazon S3 par glisser-déposer, ou télécharger du contenu depuis Amazon S3. Vous pouvez également définir des autorisations, des métadonnées et des balises facilement sur des objets dans des compartiments.

Amazon RDS

AWS Explorer peut vous aider à créer et à gérer des actifs Amazon RDS dans Visual Studio. Les instances Amazon RDS qui utilisent Microsoft SQL Server peuvent également être ajoutées à l'explorateur de serveurs de Visual Studio.

AWS Elastic Beanstalk

Vous pouvez utiliser Elastic Beanstalk pour déployer vos projets d'applications Web .NET sur. AWS Vous pouvez déployer votre application sur un environnement d'instance unique ou un environnement à charge équilibrée et dimensionnement automatique depuis l'IDE. Vous pouvez également déployer rapidement et facilement de nouvelles versions de votre application sans quitter Visual Studio. Si votre application utilise SQL Server dans Amazon RDS, l'assistant de déploiement peut également configurer la connectivité entre votre environnement d'application dans Elastic Beanstalk et l'instance de base de données dans Amazon RDS. Le Toolkit for Visual Studio inclut également l'outil de déploiement autonome en ligne de commande. Utilisez l'outil de déploiement pour faire du déploiement une étape automatique de votre processus de construction, ou pour l'inclure dans d'autres scénarios de script à l'extérieur de Visual Studio.

AWS CloudFormation

Vous pouvez utiliser le Toolkit for Visual Studio pour modifier des modèles au AWS CloudFormation format JSON en prenant en charge l'éditeur IntelliSense et le surlignage syntaxique. À l'aide d'un AWS CloudFormation modèle, vous décrivez les ressources que vous souhaitez instancier pour héberger votre application. Depuis l'IDE, vous déployez ensuite le modèle sur AWS CloudFormation. Les ressources décrites dans le modèle vous sont allouées, ce qui vous permet de vous concentrer sur le développement de l'application.

AWS Identity and Access Management (JE SUIS)

Dans AWS Explorer, vous pouvez créer des utilisateurs, des rôles et des politiques IAM, et associer des politiques aux utilisateurs.

Informations connexes

Pour ouvrir un numéro ou consulter les problèmes actuellement ouverts, rendez-vous sur https://github.com/aws/ aws-toolkit-visual-studio /issues.

Pour en savoir plus sur Visual Studio, rendez-vous sur https://visualstudio.microsoft.com/vs/.

Amazon Q et Amazon CodeWhisperer

Qu'est-ce qu'Amazon Q

Depuis le 30 avril 2024, Amazon CodeWhisperer fait désormais partie d'Amazon Q Developer, ce qui inclut les suggestions de code intégrées et les scans de sécurité.

Pour en savoir plus sur l'utilisation d'Amazon Q Developer dans le AWS Toolkit for Visual Studio, consultez la rubrique Amazon Q Developer in IDE dans le manuel Amazon Q Developer User Guide. Pour obtenir des informations détaillées sur les forfaits et les tarifs d'Amazon Q, consultez le guide de tarification d'Amazon Q.

Téléchargement du Toolkit pour Visual Studio

Vous pouvez télécharger, installer et configurer le Toolkit for Visual Studio via Visual Studio Marketplace dans votre IDE. Pour obtenir des instructions détaillées, consultez la section Installation du AWS Toolkit for Visual Studio dans la rubrique Getting started de ce guide de l'utilisateur.

Téléchargement du kit d'outils depuis Visual Studio Marketplace

Téléchargez les fichiers d'installation du Toolkit for Visual Studio en accédant au site de téléchargement de AWS Visual Studio dans votre navigateur Web.

Kits d'outils IDE supplémentaires de AWS

Outre le Toolkit pour Visual Studio, propose AWS également des boîtes à outils IDE pour VS Code et JetBrains.

AWS Toolkit for Visual Studio Codeliens

- Suivez ce lien pour le télécharger AWS Toolkit for Visual Studio Code depuis VS Code Marketplace.
- Pour en savoir plusAWS Toolkit for Visual Studio Code, consultez le guide de l'AWS Toolkit for Visual Studio Codeutilisateur.

AWS Toolkit for JetBrainsliens

- Suivez ce lien pour le télécharger AWS Toolkit for JetBrains depuis le JetBrains Marketplace.
- Pour en savoir plusAWS Toolkit for JetBrains, consultez le guide de l'AWS Toolkit for JetBrainsutilisateur.

Commencer

AWS Toolkit for Visual Studiomet vos AWS services et ressources à disposition à partir de l'environnement de développement intégré (IDE) Visual Studio.

Pour vous aider à démarrer, les rubriques suivantes décrivent comment installer, configurer et configurer leAWS Toolkit for Visual Studio.

Rubriques

Installation et configuration du AWS Toolkit for Visual Studio

Les rubriques suivantes décrivent comment télécharger, installer, configurer et désinstaller le AWS Toolkit for Visual Studio.

Rubriques

Prérequis

Les conditions suivantes sont requises pour configurer les versions prises en charge du AWS Toolkit for Visual Studio.

- Visual Studio 19 ou version ultérieure
- Windows 10 ou version ultérieure de Windows
- Accès administrateur à Windows et Visual Studio
- Informations d' AWS identification IAM actives

> **Note**
>
> Des versions non prises en charge AWS Toolkit for Visual Studio sont disponibles pour Visual Studio 2008, 2010, 2012, 2013, 2015 et 2017. Pour télécharger une version non prise en charge, accédez à la page AWS Toolkit for Visual Studiod'accueil et choisissez la version souhaitée dans la liste des liens de téléchargement.
> Pour en savoir plus sur les informations d'identification IAM ou créer un compte, visitez la passerelle de AWS console.

Installation du AWS Toolkit for Visual Studio

Pour installer le AWS Toolkit for Visual Studio, recherchez votre version de Visual Studio à l'aide des procédures suivantes et effectuez les étapes nécessaires. Les liens de téléchargement pour toutes les versions du se AWS Toolkit for Visual Studio trouvent sur la page AWS Toolkit for Visual Studiod'accueil.

> **Note**
>
> Si vous rencontrez des problèmes lors de l'installation du AWS Toolkit for Visual Studio, consultez la rubrique Résolution des problèmes d'installation dans ce guide.

Installation du AWS Toolkit for Visual Studio pour Visual Studio 2022

Pour installer AWS Toolkit for Visual Studio 2022 à partir de Visual Studio, procédez comme suit :

1. Dans le menu principal, accédez à Extensions, puis sélectionnez Gérer les extensions.
2. Dans le champ de recherche, recherchez AWS.
3. Cliquez sur le bouton Télécharger pour la version appropriée de Visual Studio 2022 et suivez les instructions d'installation.

   > **Note**
   >
   > Vous devrez peut-être fermer et redémarrer Visual Studio manuellement pour terminer le processus d'installation.

4. Lorsque le téléchargement et l'installation sont terminés, vous pouvez ouvrir le AWS Toolkit for Visual Studio en choisissant AWS Explorer dans le menu Afficher.

Installation du AWS Toolkit for Visual Studio pour Visual Studio 2019

Pour installer AWS Toolkit for Visual Studio 2019 à partir de Visual Studio, procédez comme suit :

1. Dans le menu principal, accédez à Extensions, puis sélectionnez Gérer les extensions.
2. Dans le champ de recherche, recherchez AWS.
3. Cliquez sur le bouton Télécharger pour Visual Studio 2017 et 2019 et suivez les instructions.

> **Note**
>
> Vous devrez peut-être fermer et redémarrer Visual Studio manuellement pour terminer le processus d'installation.

4. Lorsque le téléchargement et l'installation sont terminés, vous pouvez ouvrir le AWS Toolkit for Visual Studio en choisissant AWS Explorer dans le menu Afficher.

Désinstallation du AWS Toolkit for Visual Studio

Pour désinstaller le AWS Toolkit for Visual Studio, recherchez votre version de Visual Studio à l'aide des procédures suivantes et effectuez les étapes nécessaires.

Désinstaller le AWS Toolkit for Visual Studio pour Visual Studio 2022

Pour désinstaller AWS Toolkit for Visual Studio 2022 de Visual Studio, procédez comme suit :

1. Dans le menu principal, accédez à Extensions, puis sélectionnez Gérer les extensions.
2. Dans le menu de navigation Gérer les extensions, développez le titre Installés.
3. Localisez l'extension AWS Toolkit for Visual Studio 2022 et cliquez sur le bouton Désinstaller.

> **Note**
>
> Si le AWS Toolkit for Visual Studio n'est pas visible dans la section Installé du menu de navigation, vous devrez peut-être redémarrer Visual Studio.

4. Suivez les instructions à l'écran pour terminer le processus de désinstallation.

Désinstaller le AWS Toolkit for Visual Studio pour Visual Studio 2019

Pour désinstaller AWS Toolkit for Visual Studio 2019 de Visual Studio, procédez comme suit :

1. Dans le menu principal, accédez à Outils, puis sélectionnez Gérer les extensions.
2. Dans le menu de navigation Gérer les extensions, développez le titre Installés.
3. Localisez l'extension AWS Toolkit for Visual Studio 2019 et cliquez sur le bouton Désinstaller.
4. Suivez les instructions à l'écran pour terminer le processus de désinstallation.

Désinstaller le AWS Toolkit for Visual Studio pour Visual Studio 2017

Pour désinstaller AWS Toolkit for Visual Studio 2017 dans Visual Studio, procédez comme suit :

1. Dans le menu principal, accédez à Outils, puis sélectionnez Extensions et mises à jour.
2. Dans le menu de navigation Extensions et mises à jour, développez le titre Installés.
3. Localisez l'extension AWS Toolkit for Visual Studio 2017 et cliquez sur le bouton Désinstaller.
4. Suivez les instructions à l'écran pour terminer le processus de désinstallation.

Désinstaller le AWS Toolkit for Visual Studio pour Visual Studio 2013 ou 2015

Pour désinstaller AWS Toolkit for Visual Studio 2013 ou 2015, procédez comme suit :

1. Dans le panneau de configuration Windows, ouvrez Programmes et fonctionnalités.

   > **Note**
   >
   > Vous pouvez ouvrir les programmes et fonctionnalités immédiatement en les exécutant `appwiz.cpl` à partir d'une invite de commande Windows ou de la boîte de dialogue Windows Run.

2. Dans la liste des programmes installés, ouvrez le menu contextuel des AWS Outils pour Windows (cliquez avec le bouton droit de la souris).
3. Choisissez Désinstaller et suivez les instructions pour terminer le processus de désinstallation.

> **Note**
>
> Votre répertoire Samples n'est pas supprimé pendant le processus de désinstallation. Ce répertoire est conservé au cas où vous auriez modifié des échantillons. Ce répertoire doit être supprimé manuellement.

Connexion à AWS

La plupart des services et ressources Amazon Web Services (AWS) sont gérés via un AWS compte. Un AWS compte n'est pas nécessaire pour utiliser le AWS Toolkit for Visual Studio, mais les fonctions du Toolkit sont limitées sans connexion.

Si vous avez déjà configuré un AWS compte et une authentification via un autre AWS service (tel que le AWS Command Line Interface), le Toolkit for Visual Studio détecte automatiquement vos informations d'identification.

Prérequis

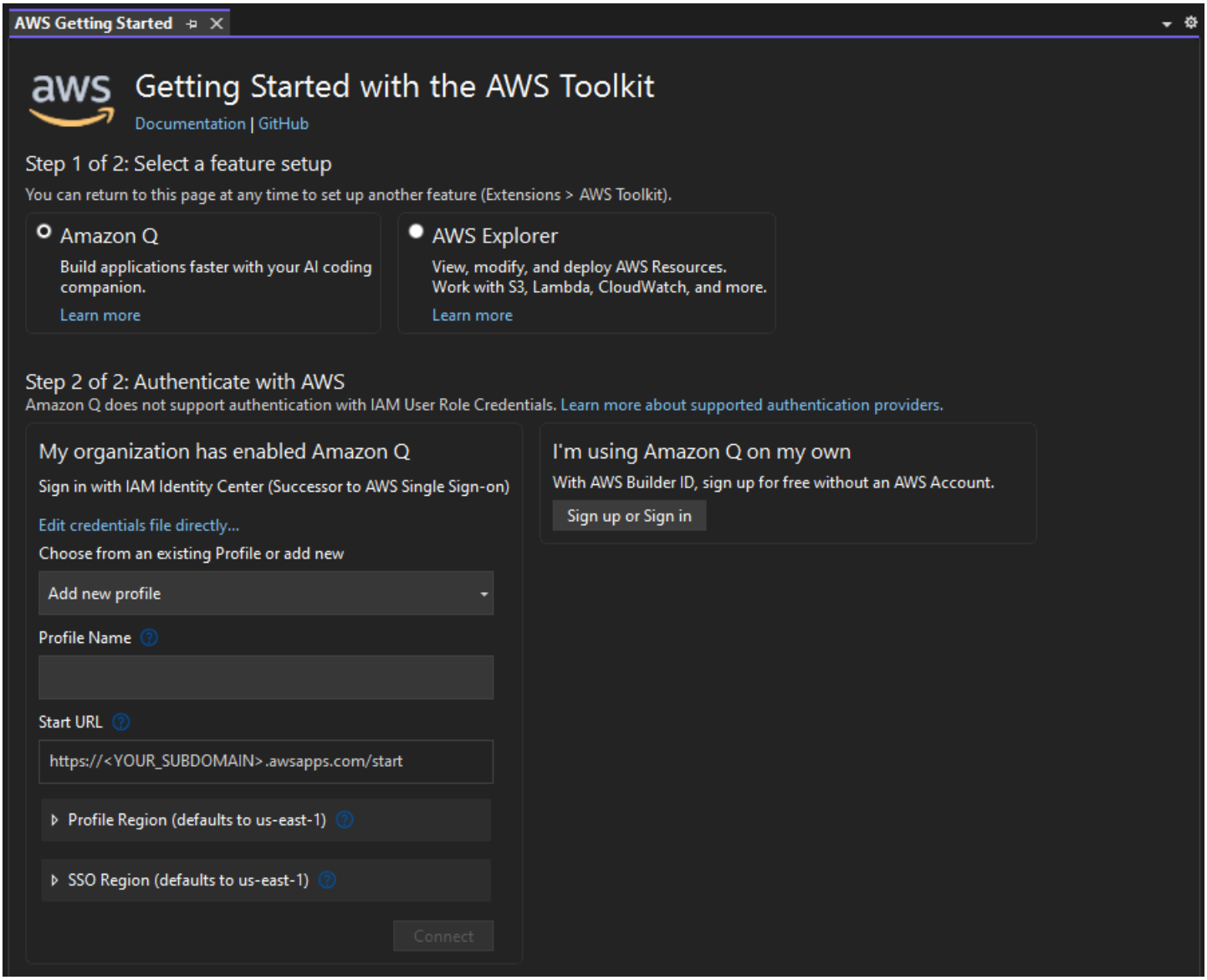
Si vous êtes nouveau AWS ou si vous n'avez pas créé de compte, vous devez suivre 3 étapes principales pour connecter le Toolkit for Visual Studio à votre AWS compte :

1. Création d'un AWS compte : vous pouvez créer un AWS compte depuis le portail d'AWS inscription. Pour obtenir des informations détaillées sur la configuration d'un nouveau AWS compte, consultez la rubrique Présentation du Guide de l'utilisateur de AWS configuration.
2. Configuration de l'authentification : il existe 3 méthodes principales pour vous authentifier avec votre AWS compte à partir du Toolkit for Visual Studio. Pour en savoir plus sur chacune de ces méthodes, consultez la rubrique Authentification et accès de ce guide de l'utilisateur.
3. Authentification AWS depuis le kit d'outils : vous pouvez vous connecter à votre AWS compte depuis le kit d'outils en suivant les procédures décrites dans les sections suivantes de ce guide de l'utilisateur.

Connexion AWS depuis le kit d'outils

Pour vous connecter à vos AWS comptes depuis le Toolkit for Visual Studio, ouvrez l'interface utilisateur Getting Started with the AWS Toolkit (interface utilisateur de connexion) en effectuant la procédure suivante.

1. Dans le menu principal de Visual Studio, développez Extensions, puis développez le AWS Toolkit.
2. Dans les options du menu du AWS kit d'outils, choisissez Getting Started.
3. L'interface utilisateur de connexion Getting Started with the AWS Toolkit s'ouvre dans Visual Studio.



Le tableau suivant décrit les méthodes d'authentification compatibles avec chaque fonctionnalité. Pour en savoir plus sur chacune des 3 méthodes d'authentification AWS IAM Identity Center, les AWS Identity and Access Management informations d'identification et l'ID du AWS constructeur, consultez la table des matières Authentification et accès de ce guide de l'utilisateur.

> **Note**
>
> À l'heure actuelle, lorsque vous travaillez avec CodeCatalyst le Toolkit for Visual Studio, vous devez uniquement autoriser avec votre AWS Builder ID lors du clonage d'un référentiel tiers.

Développeur Amazon Q	AWS Explorateur	Amazon CodeCatalyst
☑ ID du AWS constructeur	☒ ID du AWS constructeur	☑ ID du AWS constructeur
☑ Centre d'identité IAM	☑ Centre d'identité IAM	☒ Centre d'identité IAM
☒ Informations AWS d'identification IAM	☑ Informations AWS d'identification IAM	☒ Informations AWS d'identification IAM

Authentification pour Amazon Q Developer

Pour commencer à utiliser Amazon Q Developer, authentifiez-vous et connectez-vous à l'aide de vos informations d'identification AWS IAM Identity Center ou de celles du AWS Builder ID.

Les procédures suivantes décrivent comment authentifier et connecter le Toolkit à votre AWS compte.

Authentifiez-vous et connectez-vous à IAM Identity Center

1. Dans l'interface utilisateur de connexion Getting Started with the AWS Toolkit, sélectionnez le radial Amazon Q Developer pour étendre les options d'authentification Amazon Q Developer.

   > **Note**
   >
   > Si aucune information d'identification n'est enregistrée, passez à l'étape 3 pour ajouter ou mettre à jour vos informations d'identification IAM Identity Center.

2. Dans la section Mon organisation a activé Amazon Q Developer, élargissez le menu Choisir parmi un profil existant ou ajoutez un nouveau menu déroulant pour choisir parmi votre liste d'informations d'identification enregistrées.
3. Dans le menu déroulant Type de profil, sélectionnez AWS IAM Identity Center

4. Dans le champ de texte Nom du profil, entrez le **`Profile Name`** profil IAM Identity Center avec lequel vous souhaitez vous authentifier.
5. Dans le champ de texte URL de démarrage, entrez le **`Start URL`** nom joint à vos informations d'identification IAM Identity Center.
6. Dans le menu déroulant Profile Region (par défaut us-east-1), choisissez la Profile Region définie par le profil utilisateur IAM Identity Center auprès duquel vous vous authentifiez.
7. Dans le menu déroulant Région SSO (par défaut us-east-1), choisissez la région SSO définie par vos informations d'identification IAM Identity Center, puis cliquez sur le bouton Connect pour ouvrir la boîte de dialogue Log in with IAM Identity Center. AWS
8. Dans la boîte de dialogue Connexion avec AWS IAM Identity Center, cliquez sur le bouton Passer au navigateur pour ouvrir le site de demande d' AWS autorisation dans votre navigateur Web par défaut.
9. Vérifiez que le code de sécurité de votre IDE correspond au code de confirmation de demande d' AWS autorisation affiché dans votre navigateur Web et cliquez sur le bouton Soumettre et continuer pour continuer.
10. Suivez les instructions de votre navigateur Web par défaut, vous êtes averti lorsque le processus d'autorisation est terminé, vous pouvez fermer votre navigateur en toute sécurité et retourner dans Visual Studio.

Authentifiez-vous et connectez-vous avec un AWS Builder ID

1. Dans l'interface utilisateur de connexion Getting Started with the AWS Toolkit, sélectionnez le radial Amazon Q Developer pour étendre les options d'authentification Amazon Q Developer.
2. Dans la section J'utilise Amazon Q Developer sur mon propre compte, cliquez sur le bouton S'inscrire ou Se connecter pour ouvrir la boîte de dialogue Se connecter avec AWS Builder ID.
3. Cliquez sur le bouton Passer au navigateur pour ouvrir le site de demande d' AWS autorisation dans votre navigateur Web par défaut.
4. Vérifiez que le code de sécurité de votre IDE correspond au code de confirmation de demande d' AWS autorisation affiché dans votre navigateur Web et cliquez sur le bouton Soumettre et continuer pour continuer.
5. Suivez les instructions de votre navigateur Web par défaut, vous êtes averti lorsque le processus d'autorisation est terminé, vous pouvez fermer votre navigateur en toute sécurité et retourner dans Visual Studio.

Authentification pour l' AWS explorateur

Pour commencer à utiliser l' AWS explorateur à partir du kit d'outils, authentifiez-vous et connectez-vous à l'aide de vos informations d'identification IAM Identity Center ou de vos informations d'identification IAM.

Les procédures suivantes décrivent comment authentifier et connecter le Toolkit à votre AWS compte.

Authentifiez-vous et connectez-vous à IAM Identity Center

1. Dans l'interface utilisateur de connexion Getting Started with the AWS Toolkit, sélectionnez le radial AWS Explorer pour étendre les options d'authentification Amazon Q Developer.
2. Dans le menu déroulant **`Profile Type`**, choisissez AWS IAM Identity Center.
3. Dans le champ de texte Nom du profil, entrez le **`Profile Name`** profil IAM Identity Center que vous souhaitez utiliser.
4. Dans le champ de texte URL de démarrage, entrez le **`Start URL`** nom joint à vos informations d'identification IAM Identity Center.
5. Dans le menu déroulant Profile Region (par défaut us-east-1), choisissez la Profile Region définie par le profil utilisateur IAM Identity Center auprès duquel vous vous authentifiez.
6. Dans le menu déroulant Région SSO (par défaut us-east-1), choisissez la région SSO définie par vos informations d'identification IAM Identity Center.
7. Cliquez sur le bouton Passer au navigateur pour ouvrir le site de demande d'AWS autorisation dans votre navigateur Web par défaut.
8. Vérifiez que le code de sécurité de votre IDE correspond au code de confirmation de demande d'AWS autorisation affiché dans votre navigateur Web et cliquez sur le bouton Soumettre et continuer pour continuer.
9. Suivez les instructions de votre navigateur Web par défaut, vous êtes averti lorsque le processus d'autorisation est terminé, vous pouvez fermer votre navigateur en toute sécurité et retourner dans Visual Studio.

Authentifiez-vous et connectez-vous avec les informations d'identification IAM

1. Dans l'interface utilisateur de connexion Getting Started with the AWS Toolkit, sélectionnez le radial AWS Explorer pour étendre les options d'authentification Amazon Q Developer.
2. **`Profile Type`**Dans le menu déroulant, sélectionnez IAM User Role.

3. Dans le champ de texte Nom du profil, entrez le **`Profile Name`** profil avec lequel vous souhaitez vous authentifier.
4. Dans le champ de texte ID de clé d'accès, entrez **`Access Key ID`** le profil avec lequel vous souhaitez vous authentifier.
5. Dans le champ de texte Clé secrète, entrez **`Secret Key`** le profil avec lequel vous souhaitez vous authentifier.
6. Dans le menu déroulant Emplacement de stockage (par défaut, fichier d'informations d'identification partagé), indiquez si vous souhaitez stocker vos informations d'identification dans un fichier d'informations d'identification partagé ou dans .NET Encrypted Stored Stored.
7. Dans le menu déroulant Région du profil (par défaut us-east-1), choisissez la région du profil associée au profil auprès duquel vous souhaitez vous authentifier.

Résolution des problèmes d'installation du AWS Toolkit for Visual Studio

Les informations suivantes sont connues pour résoudre les problèmes d'installation courants lors de l'installation duAWS Toolkit for Visual Studio.

Si vous rencontrez une erreur lors de l'installation du AWS Toolkit for Visual Studio ou si vous ne savez pas si l'installation est terminée, consultez les informations de chacune des sections suivantes.

Autorisations d'administrateur pour Visual Studio

L'AWS Toolkit for Visual Studioextension nécessite des autorisations d'administrateur pour garantir l'accessibilité de tous les AWS services et fonctionnalités.

Si vous disposez d'autorisations d'administrateur local, il est possible que vos autorisations d'administrateur ne s'étendent pas directement à votre instance de Visual Studio.

Pour lancer Visual Studio avec des autorisations d'administrateur localement :

1. Dans Windows, localisez le lanceur d'applications Visual Studio (icône).
2. Ouvrez le menu contextuel (cliquez avec le bouton droit) sur l'icône Visual Studio pour ouvrir le menu contextuel.
3. Sélectionnez Exécuter en tant qu'administrateur dans le menu contextuel.

Pour lancer Visual Studio à distance avec des autorisations d'administrateur :

1. Dans Windows, localisez le lanceur d'applications correspondant à l'application que vous utilisez pour vous connecter à votre instance distante de Visual Studio.
2. Ouvrez le menu contextuel (cliquez avec le bouton droit) de l'application pour ouvrir le menu contextuel.
3. Sélectionnez Exécuter en tant qu'administrateur dans le menu contextuel.

> **Note**
>
> Que vous lanciez le programme localement ou que vous vous connectiez à distance, Windows peut vous demander de confirmer vos informations d'identification administratives.

Obtenir un journal d'installation

Si vous avez suivi les étapes décrites dans la section précédente sur les autorisations d'administrateur située ci-dessus et qu'il est confirmé que vous exécutez Visual Studio ou que vous vous y connectez avec des autorisations d'administrateur, l'obtention d'un fichier journal d'installation peut vous aider à diagnostiquer d'autres problèmes.

Pour installer manuellement le AWS Toolkit for Visual Studio à partir d'un `.vsix` fichier et générer un fichier journal d'installation, procédez comme suit.

1. Sur la page AWS Toolkit for Visual Studiod'accueil, cliquez sur le lien Télécharger et enregistrez le `.vsix` fichier de la AWS Toolkit for Visual Studio version que vous souhaitez installer.
2. Dans le menu principal de Visual Studio, développez l'en-tête Outils, développez le sous-menu Command Line, puis choisissez Visual Studio Developer Command Prompt.
3. À partir de l'invite de commande du développeur de Visual Studio, entrez la `vsixinstaller` commande au format suivant :

   ```
   vsixinstaller /logFile:[file path to log file] [file path to Toolkit installation file]
   ```
4. `[file path to log file]`Remplacez-le par le nom de fichier et le chemin complet du répertoire dans lequel vous souhaitez créer le journal d'installation. Un exemple de `vsixinstaller` commande avec le chemin de fichier et le nom de fichier que vous avez spécifiés ressemble au suivant :

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

5. `[file path to Toolkit installation file]`Remplacez-le par le chemin complet du fichier du répertoire dans lequel se `AWSToolkitPackage.vsix` trouve le.

   Un exemple de `vsixinstaller` commande avec le chemin d'accès complet au fichier d'installation de Toolkit doit ressembler à ce qui suit :

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

6. Vérifiez que le nom et les chemins de votre fichier sont corrects, puis exécutez la `vsixinstaller` commande.

   Un exemple de `vsixinstaller` commande complète ressemble à ce qui suit :

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

Installation de différentes extensions de Visual Studio

Si vous avez obtenu un fichier journal d'installation et que vous ne parvenez toujours pas à déterminer pourquoi le processus d'installation échoue, vérifiez si vous êtes en mesure d'installer d'autres extensions Visual Studio. L'installation de différentes extensions de Visual Studio peut fournir des informations supplémentaires sur vos problèmes d'installation. Si vous ne parvenez pas à installer d'extensions Visual Studio, il peut être nécessaire de résoudre les problèmes liés à Visual Studio, au lieu deAWS Toolkit for Visual Studio.

Contacter l'assistance

Si vous avez consulté toutes les sections de ce guide et avez besoin de ressources ou d'assistance supplémentaires, vous pouvez consulter les anciens numéros ou en ouvrir un nouveau depuis le site AWS Toolkit for Visual StudioGithub Issues.

Pour vous aider à trouver rapidement une solution à votre problème :

- Vérifiez les problèmes passés et actuels pour voir si d'autres personnes ont rencontré une situation similaire.
- Conservez des notes détaillées sur chaque étape que vous avez prise pour résoudre le problème.

- Enregistrez tous les fichiers journaux que vous avez obtenus lors de l'installation de l'extension AWS Toolkit for Visual Studio ou d'autres extensions.
- Joignez vos fichiers journaux AWS Toolkit for Visual Studio d'installation au nouveau problème.

Profilés et reliure de fenêtre

Profils et Toolkit for Visual Studio

Lorsque vous utilisez les outils de publication, les assistants et les autres fonctionnalités de la Toolkit for Visual Studio, tenez compte des points suivants :

- La fenêtre de l'AWSExplorateur est liée à un seul profil et à une seule région à la fois. Fenêtres ouvertes à partir de l'AWSexplorateur par défaut vers ce profil et cette région liés.
- Après l'ouverture d'une nouvelle fenêtre, vous pouvez utiliser cette instance de l'AWSExplorateur pour passer à un autre profil ou à une autre région.
- Le Toolkit pour les outils et fonctionnalités de publication de Visual Studio utilise automatiquement par défaut le profil et la région définis dans l'AWSExplorateur.
- Si un nouveau profil ou une nouvelle région est spécifié dans un outil de publication, un assistant ou une fonctionnalité, toutes les ressources créées ultérieurement continueront à utiliser les nouveaux paramètres de profil et de région.
- Si plusieurs instances de Visual Studio sont ouvertes, chaque instance peut être liée à un profil et à une région différents.
- L'AWSexplorateur enregistre le dernier profil et la dernière région spécifiés et les valeurs de la toute dernière instance de Visual Studio fermée seront conservées.

Authentification et accès

Vous n'avez pas besoin de vous authentifier AWS pour commencer à utiliser le AWS Toolkit for Visual Studio. Cependant, la plupart des AWS ressources sont gérées par le biais d'un AWS compte. Pour accéder à tous les services et fonctionnalités du AWS Toolkit for Visual Studio, vous aurez besoin d'au moins deux types d'authentification de compte :

1. Soit AWS Identity and Access Management (IAM), soit AWS IAM Identity Centerl'authentification de vos AWS comptes. La plupart AWS des services et ressources sont gérés via IAM et IAM Identity Center.
2. Un AWS Builder ID est facultatif pour certains autres AWS services.

Les rubriques suivantes contiennent des détails supplémentaires et des instructions de configuration pour chaque type d'informations d'identification et méthode d'authentification.

Rubriques

- AWS Informations d'identification IAM Identity Center dans AWS Toolkit for Visual Studio
- AWS Informations d'identification IAM
- AWS ID du constructeur
- Authentification multifactorielle (MFA) dans Toolkit for Visual Studio
- Configuration des informations d'identification externes

AWS Informations d'identification IAM Identity Center dans AWS Toolkit for Visual Studio

AWS IAM Identity Center est la meilleure pratique recommandée pour gérer l'authentification de votre AWS compte.

Pour obtenir des instructions détaillées sur la configuration d'IAM Identity Center pour les kits de développement logiciel (SDK) et le AWS Toolkit for Visual Studio, consultez la section sur l'authentification IAM Identity Center du guide de référence des AWS SDK et outils.

Authentification auprès d'IAM Identity Center à partir du AWS Toolkit for Visual Studio

Pour vous authentifier auprès d'IAM Identity Center à partir du en AWS Toolkit for Visual Studio ajoutant un profil IAM Identity Center à votre `config` fichier `credentials` or, procédez comme suit.

1. Dans votre éditeur de texte préféré, ouvrez les informations AWS d'identification enregistrées dans le `<hone-directory>\.aws\credentials` fichier.
2. `credentials file`Dans la section inférieure`[default]`, ajoutez un modèle pour un profil IAM Identity Center nommé. Voici un exemple de modèle :

   > **Important**
   >
   > N'utilisez pas le mot profil lors de la création d'une entrée dans le `credential` fichier, car cela crée un conflit avec les conventions de dénomination des `credential` fichiers. N'incluez le mot préfixe `profile_` que lors de la configuration d'un profil nommé dans le `config` fichier.

```
[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`**: URL qui pointe vers le portail utilisateur IAM Identity Center de votre organisation.
- **`sso_region`**: AWS région qui contient l'hôte de votre portail IAM Identity Center. Cela peut être différent de la AWS région spécifiée ultérieurement dans le `region` paramètre par défaut.
- **`sso_account_id`**: ID de AWS compte contenant le rôle IAM avec l'autorisation que vous souhaitez accorder à cet utilisateur du IAM Identity Center.
- **`sso_role_name`**: nom du rôle IAM qui définit les autorisations de l'utilisateur lorsqu'il utilise ce profil pour obtenir des informations d'identification via IAM Identity Center.
- **`region`**: AWS région par défaut à laquelle cet utilisateur du IAM Identity Center se connecte.

> **Note**
>
> Vous pouvez également ajouter un profil activé par IAM Identity Center à votre profil AWS CLI en exécutant la `aws configure sso` commande. Après avoir exécuté cette commande, vous fournissez des valeurs pour l'URL de démarrage du centre d'identité IAM (`sso_start_url`) et pour la AWS région (`region`) qui héberge le répertoire du centre d'identité IAM.
> Pour plus d'informations, consultez la section Configuration de la AWS CLI pour utiliser l'authentification AWS unique dans le guide de l'AWS Command Line Interface utilisateur.

Connexion avec IAM Identity Center

Lorsque vous vous connectez avec un profil IAM Identity Center, le navigateur par défaut est lancé sur le navigateur `sso_start_url` spécifié dans votre`credential file`. Vous devez vérifier votre identifiant IAM Identity Center avant de pouvoir accéder à vos AWS ressources dans AWS Toolkit for Visual Studio. Si vos informations d'identification expirent, vous devrez répéter le processus de connexion pour obtenir de nouvelles informations d'identification temporaires.

AWS Informations d'identification IAM

AWS Les informations d'identification IAM s'authentifient auprès de votre AWS compte grâce à des clés d'accès stockées localement.

Les sections suivantes décrivent comment configurer les informations d'identification IAM pour vous authentifier auprès de votre AWS compte depuis le. AWS Toolkit for Visual Studio

> **Important**
>
> Avant de configurer les informations d'identification IAM pour vous authentifier auprès de votre AWS compte, notez que :
>
> - Si vous avez déjà défini les informations d'identification IAM par le biais d'un autre AWS service (tel que le AWS AWS CLI), ces informations d'identification sont AWS Toolkit for Visual Studio automatiquement détectées.
> - AWS recommande d'utiliser AWS IAM Identity Center l'authentification. Pour plus d'informations sur les meilleures pratiques en matière d' AWS IAM, consultez la section

Bonnes pratiques de sécurité en matière d'IAM du guide de l'utilisateur AWS d'Identity and Access Management.

- Afin d'éviter les risques de sécurité, n'employez pas les utilisateurs IAM pour l'authentification lorsque vous développez des logiciels spécialisés ou lorsque vous travaillez avec des données réelles. Utilisez plutôt la fédération avec un fournisseur d'identité tel que AWS IAM Identity Center. Pour plus d'informations, consultez le document Qu'est-ce qu'IAM Identity Center ? dans le guide de AWS IAM Identity Center l'utilisateur.

Création d'un utilisateur IAM

Avant de configurer l' AWS Toolkit for Visual Studio authentification avec votre AWS compte, vous devez suivre l'étape 1 : créer votre utilisateur IAM et l'étape 2 : obtenir vos clés d'accès dans la rubrique Authentifier à l'aide d'informations d'identification à long terme du guide de référence des AWS SDK et des outils.

> **Note**
>
> Étape 3 : La mise à jour des informations d'identification partagées est facultative.
> Si vous terminez l'étape 3, le détecte AWS Toolkit for Visual Studio automatiquement vos informations d'identification à partir du`credentials file`.
> Si vous n'avez pas terminé l'étape 3, AWS Toolkit for Visual Studio vous pouvez suivre le processus de création d'un, `credentials file` comme décrit dans la AWS Toolkit for Visual Studio section Création d'un fichier d'informations d'identification située ci-dessous.

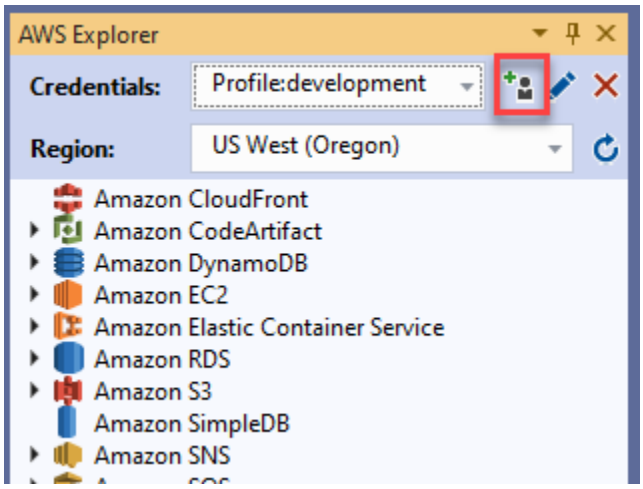
Création d'un fichier d'informations d'identification

Pour ajouter un utilisateur ou en créer un `credentials file` à partir du AWS Toolkit for Visual Studio :

> **Note**
>
> Lorsqu'un nouveau profil utilisateur est ajouté à partir de la boîte à outils :
>
> - S'il en existe `credentials file` déjà un, les nouvelles informations utilisateur sont ajoutées au fichier existant.

- Si un `credentials file` n'existe pas, un nouveau fichier est créé.

1. Dans l' AWS explorateur, choisissez l'icône Nouveau profil de compte pour ouvrir la boîte de dialogue Nouveau profil de compte.



2. Renseignez les champs obligatoires dans la boîte de dialogue Nouveau profil de compte et cliquez sur le bouton OK pour créer l'utilisateur IAM.

Modification des informations d'identification des utilisateurs IAM à partir de la boîte à outils

Pour modifier les informations d'identification de l'utilisateur IAM à partir du kit d'outils, procédez comme suit :

1. Dans le menu déroulant Informations d'identification de l' AWS explorateur, choisissez les informations d'identification de l'utilisateur IAM que vous souhaitez modifier.
2. Cliquez sur l'icône Modifier le profil pour ouvrir la boîte de dialogue Modifier le profil.
3. Dans la boîte de dialogue Modifier le profil, terminez vos mises à jour et cliquez sur le bouton OK pour enregistrer vos modifications.

Pour supprimer les informations d'identification de l'utilisateur IAM du kit d'outils, procédez comme suit :

1. Dans le menu déroulant Informations d'identification de l' AWS explorateur, choisissez les informations d'identification de l'utilisateur IAM que vous souhaitez supprimer.

2. Cliquez sur l'icône Supprimer le profil pour ouvrir l'invite de suppression du profil.
3. Confirmez que vous souhaitez supprimer le profil pour le supprimer de votre`Credentials file`.

> **Important**
>
> Les profils qui prennent en charge les fonctionnalités d'accès avancées, telles que le centre d'identité IAM ou l'authentification multifactorielle (MFA) dans la boîte de dialogue Modifier le profil, ne peuvent pas être modifiés à partir du. AWS Toolkit for Visual Studio Pour apporter des modifications à ces types de profils, vous devez les modifier à l'`credentials file`aide d'un éditeur de texte.

Modification des informations d'identification d'un utilisateur IAM à partir d'un éditeur de texte

Outre la gestion des utilisateurs IAM avec le AWS Toolkit for Visual Studio, vous pouvez effectuer des modifications `credential files` à partir de votre éditeur de texte préféré. L'emplacement par défaut du `credential file` dans Windows est`C:\Users\`*`USERNAME`*`\.aws\credentials`.

Pour plus de détails sur l'emplacement et la structure de`credential files`, consultez la section Fichiers de configuration et d'informations d'identification partagés du guide de référence AWS des SDK et des outils.

Création d'utilisateurs IAM à partir du AWS Command Line Interface ()AWS CLI

AWS CLI Il s'agit d'un autre outil que vous pouvez utiliser pour créer un utilisateur IAM dans le`credentials file`, à l'aide de la commande`aws configure`.

Pour obtenir des informations détaillées sur la création d'utilisateurs IAM à partir de la AWS CLI section Configuration des AWS CLI rubriques du Guide de l'AWS CLI utilisateur.

Le Toolkit for Visual Studio prend en charge les propriétés de configuration suivantes :

```
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 du constructeur

AWS Le Builder ID est une méthode AWS d'authentification supplémentaire qui peut être requise pour utiliser certains services ou fonctionnalités, tels que le clonage d'un référentiel tiers avec Amazon CodeCatalyst.

Pour obtenir des informations détaillées sur la méthode d'authentification AWS Builder ID, consultez la rubrique Se connecter avec AWS Builder ID dans le Guide de l'utilisateur de AWS connexion.

Pour plus d'informations sur le clonage d'un référentiel pour CodeCatalyst from AWS Toolkit for Visual Studio, consultez la CodeCatalyst rubrique Travailler avec Amazon dans ce guide de l'utilisateur.

Authentification multifactorielle (MFA) dans Toolkit for Visual Studio

L'authentification multifactorielle (MFA) renforce la sécurité de vos comptes. AWS La MFA oblige les utilisateurs à fournir des informations de connexion et une authentification unique à l'aide d'un mécanisme AWS MFA compatible lorsqu'ils accèdent à des sites Web ou à des services. AWS

AWS prend en charge une gamme de périphériques virtuels et matériels pour l'authentification MFA. Voici un exemple de dispositif MFA virtuel activé via une application pour smartphone. Pour plus d'informations sur les options des appareils MFA, consultez la section Utilisation de l'authentification multifactorielle (MFA) AWS dans le guide de l'utilisateur IAM.

Étape 1 : Création d'un rôle IAM pour déléguer l'accès aux utilisateurs IAM

La procédure suivante décrit comment configurer la délégation de rôles pour attribuer des autorisations à un utilisateur IAM. Pour des informations détaillées sur la délégation de rôles,

consultez la rubrique Création d'un rôle pour déléguer des autorisations à un utilisateur IAM dans le Guide de l'AWS Identity and Access Management utilisateur.

1. Accédez à la console IAM à l'adresse https://console.aws.amazon.com/iam.
2. Choisissez Rôles dans la barre de navigation, puis choisissez Créer un rôle.
3. Sur la page Créer un rôle, choisissez Un autre AWS compte.
4. Entrez le numéro de compte requis et cochez la case Exiger le MFA.

   > **Note**
   >
   > Pour trouver votre numéro de compte (ID) à 12 chiffres, accédez à la barre de navigation de la console, puis choisissez Support, Support Center.

5. Sélectionnez Next: Permissions (Étape suivante : autorisations).
6. Associez des politiques existantes à votre rôle ou créez-en une nouvelle pour celui-ci. Les politiques que vous choisissez sur cette page déterminent les AWS services auxquels l'utilisateur IAM peut accéder avec le Toolkit.
7. Après avoir joint des politiques, choisissez Next : Tags pour pouvoir ajouter des balises IAM à votre rôle. Choisissez ensuite Next : Review pour continuer.
8. Sur la page Révision, entrez le nom de rôle requis (toolkit-role, par exemple). Vous pouvez également ajouter une description de rôle facultative.
9. Sélectionnez Créer un rôle.
10. Lorsque le message de confirmation s'affiche (« Le rôle de la boîte à outils a été créé », par exemple), choisissez le nom du rôle dans le message.
11. Sur la page Résumé, cliquez sur l'icône de copie pour copier l'ARN du rôle et le coller dans un fichier. (Vous avez besoin de cet ARN lorsque vous configurez l'utilisateur IAM pour qu'il assume le rôle.)

Étape 2 : Création d'un utilisateur IAM qui assume les autorisations du rôle

Cette étape crée un utilisateur IAM sans autorisation afin qu'une politique en ligne puisse être ajoutée.

1. Accédez à la console IAM à l'adresse https://console.aws.amazon.com/iam.
2. Choisissez Utilisateurs dans la barre de navigation, puis sélectionnez Ajouter un utilisateur.

3. Sur la page Ajouter un utilisateur, entrez le nom d'utilisateur requis (toolkit-user, par exemple) et cochez la case Accès par programmation.
4. Choisissez Suivant : Autorisations, Suivant : Balises et Suivant : Révision pour passer aux pages suivantes. Vous n'ajoutez pas d'autorisations à ce stade, car l'utilisateur va assumer les autorisations du rôle.
5. Sur la page d'évaluation, vous êtes informé que cet utilisateur n'a aucune autorisation. Choisissez Create user (Créer un utilisateur).
6. Sur la page Réussite, choisissez Télécharger le fichier .csv pour télécharger le fichier contenant l'ID de clé d'accès et la clé d'accès secrète. (Vous avez besoin des deux pour définir le profil de l'utilisateur dans le fichier d'informations d'identification.)
7. Choisissez Fermer.

Étape 3 : ajout d'une politique permettant à l'utilisateur IAM d'assumer le rôle

La procédure suivante crée une politique en ligne qui permet à l'utilisateur d'assumer le rôle (et les autorisations associées à ce rôle).

1. Sur la page Utilisateurs de la console IAM, choisissez l'utilisateur IAM que vous venez de créer (toolkit-user, par exemple).
2. Dans l'onglet Autorisations de la page Résumé, choisissez Ajouter une politique intégrée.
3. Sur la page Créer une politique, choisissez Choisir un service, entrez STS dans Rechercher un service, puis sélectionnez STS dans les résultats.
4. Pour Actions, commencez à saisir le terme AssumeRole. AssumeRoleCochez la case lorsqu'elle apparaît.
5. Dans la section Ressource, assurez-vous que Spécifique est sélectionné, puis cliquez sur Ajouter un ARN pour restreindre l'accès.
6. Dans la boîte de dialogue Ajouter un ou plusieurs ARN, pour le rôle Spécifier l'ARN, ajoutez l'ARN du rôle que vous avez créé à l'étape 1.

   Une fois que vous avez ajouté l'ARN du rôle, le compte fiable et le nom du rôle associés à ce rôle sont affichés dans Nom du compte et du rôle avec chemin.
7. Choisissez Ajouter.

8. De retour sur la page Créer une politique, choisissez Spécifier les conditions de demande (facultatif), cochez la case MFA requise, puis cliquez sur Fermer pour confirmer.
9. Choisissez Review policy (Examiner la politique)
10. Dans la page Révision de la politique, entrez le nom de la politique, puis choisissez Créer une politique.

    L'onglet Autorisations affiche la nouvelle politique intégrée attachée directement à l'utilisateur IAM.

Étape 4 : Gestion d'un périphérique MFA virtuel pour l'utilisateur IAM

1. Téléchargez et installez une application MFA virtuelle sur votre smartphone.

   Pour obtenir la liste des applications prises en charge, consultez la page de ressources sur l'authentification multifactorielle.
2. Dans la console IAM, choisissez Utilisateurs dans la barre de navigation, puis choisissez l'utilisateur qui assume un rôle (toolkit-user, dans ce cas).
3. Sur la page Résumé, choisissez l'onglet Informations d'identification de sécurité, et pour le périphérique MFA attribué, choisissez Gérer.
4. Dans le volet Gérer le périphérique MFA, choisissez le périphérique MFA virtuel, puis choisissez Continuer.
5. Dans le volet Configurer un appareil MFA virtuel, choisissez Afficher le code QR, puis scannez le code à l'aide de l'application MFA virtuelle que vous avez installée sur votre smartphone.
6. Après avoir scanné le code QR, l'application MFA virtuelle génère des codes MFA à usage unique. Entrez deux codes MFA consécutifs dans le code MFA 1 et le code MFA 2.
7. Choisissez Assign MFA (Affecter le MFA).
8. De retour dans l'onglet Informations d'identification de sécurité de l'utilisateur, copiez l'ARN du nouveau périphérique MFA attribué.

   L'ARN inclut votre identifiant de compte à 12 chiffres et le format est similaire au suivant :`arn:aws:iam::123456789012:mfa/toolkit-user`. Vous aurez besoin de cet ARN pour définir le profil MFA à l'étape suivante.

Étape 5 : Création de profils pour autoriser le MFA

La procédure suivante crée les profils autorisant le MFA lors de l'accès aux AWS services depuis le Toolkit for Visual Studio.

Les profils que vous créez incluent trois informations que vous avez copiées et stockées au cours des étapes précédentes :

- Clés d'accès (ID de clé d'accès et clé d'accès secrète) pour l'utilisateur IAM
- ARN du rôle qui délègue les autorisations à l'utilisateur IAM
- ARN du périphérique MFA virtuel attribué à l'utilisateur IAM

Dans le fichier d'informations d'identification AWS partagé ou dans le magasin du SDK qui contient vos AWS informations d'identification, ajoutez les entrées suivantes :

```
[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
```

Deux profils sont définis dans l'exemple fourni :

- `[toolkit-user]`le profil inclut la clé d'accès et la clé d'accès secrète qui ont été générées et enregistrées lorsque vous avez créé l'utilisateur IAM à l'étape 2.
- `[mfa]`le profil définit le mode de prise en charge de l'authentification multifactorielle. Il y a trois entrées :

  ◦ `source_profile` : Spécifie le profil dont les informations d'identification sont utilisées pour assumer le rôle spécifié par ce `role_arn` paramètre dans ce profil. Dans ce cas, il s'agit du `toolkit-user` profil.

  ◦ `role_arn` : Spécifie le nom de ressource Amazon (ARN) du rôle IAM que vous souhaitez utiliser pour effectuer les opérations demandées à l'aide de ce profil. Dans ce cas, il s'agit de l'ARN du rôle que vous avez créé à l'étape 1.

- `mfa_serial` : Spécifie l'identification ou le numéro de série du dispositif MFA que l'utilisateur doit utiliser lorsqu'il assume un rôle. Dans ce cas, il s'agit de l'ARN du périphérique virtuel que vous avez configuré à l'étape 3.

Configuration des informations d'identification externes

Si vous disposez d'une méthode pour générer ou rechercher des informations d'identification qui n'est pas directement prise en charge AWS, vous pouvez ajouter au fichier d'informations d'identification partagé un profil contenant le `credential_process` paramètre. Ce paramètre spécifie une commande externe exécutée pour générer ou récupérer les informations d'authentification à utiliser. Par exemple, vous pouvez inclure une entrée similaire à la suivante dans le `config` fichier :

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

Pour plus d'informations sur l'utilisation des informations d'identification externes et les risques de sécurité associés, consultez la section Obtenir des informations d'identification par le biais d'un processus externe dans le guide de AWS Command Line Interface l'utilisateur.

Travailler avec les AWS services

Les rubriques suivantes décrivent comment commencer à utiliser les AWS services du AWS Toolkit for Visual Studio.

Rubriques

Amazon CodeCatalyst pour la AWS boîte à outils pour Visual Studio

Qu'est-ce qu'Amazon CodeCatalyst ?

Amazon CodeCatalyst est un espace de collaboration basé sur le cloud pour les équipes de développement de logiciels. À l'aide du AWS Toolkit pour Visual Studio, vous pouvez afficher et

gérer les CodeCatalyst ressources directement depuis AWS Toolkit for Visual Studio. Pour plus d'informations à ce sujetCodeCatalyst, consultez le Guide de CodeCatalyst l'utilisateur Amazon.

Les rubriques suivantes décrivent comment connecter le AWS Toolkit pour Visual Studio CodeCatalyst et comment l'utiliser CodeCatalyst via le AWS Toolkit pour Visual Studio.

Rubriques

Démarrez avec Amazon CodeCatalyst et la AWS boîte à outils pour Visual Studio

Pour commencer à travailler avec Amazon CodeCatalyst à partir du AWS Toolkit pour Visual Studio, procédez comme suit.

Rubriques

Installation du AWS kit d'outils pour Visual Studio

Avant d'intégrer le AWS Toolkit for Visual Studio à vos CodeCatalyst comptes, assurez-vous que vous utilisez une version actuelle de AWS Toolkit for Visual Studio. Pour plus d'informations sur l'installation et la configuration de la dernière version de AWS Toolkit for Visual Studio, consultez la section Configuration du AWS Toolkit pour Visual Studio de ce guide de l'utilisateur.

Création d'un CodeCatalyst compte et d'un AWS Builder ID

Outre l'installation de la dernière version du AWS Toolkit for Visual Studio, vous devez disposer d'un AWS Builder ID et d'un CodeCatalyst compte actifs pour vous connecter à AWS Toolkit for Visual Studio. Si vous ne possédez pas d'identifiant ou de CodeCatalyst compte AWS Builder actif, consultez la CodeCatalyst section Configuration avec du Guide de l'CodeCatalystutilisateur.

> **Note**
>
> Un AWS Builder ID est différent de vos AWS informations d'identification. Pour savoir comment s'inscrire et s'authentifier à l'aide d'un AWS Builder ID, consultez la rubrique Authentification et accès : AWS Builder ID de ce guide de l'utilisateur.
> Pour obtenir des informations détaillées sur les AWS Builder ID, consultez la rubrique AWSBuilder ID du AWSGeneral Reference User Guide.

Connexion de AWS Toolkit pour Visual Studio avec CodeCatalyst

Pour connecter AWS Toolkit for Visual Studio à votre CodeCatalyst compte, procédez comme suit.

1. Dans l'élément de menu Git de Visual Studio, choisissez Clone Repository... .
2. Dans la section Parcourir un référentiel, sélectionnez Amazon CodeCatalyst comme fournisseur.
3. Dans la section Connexion, choisissez Se connecter avec AWS Builder ID pour ouvrir la CodeCatalyst console dans votre navigateur Web préféré.
4. Dans votre navigateur, saisissez votre AWS Builder ID dans le champ prévu à cet effet et suivez les instructions pour continuer.
5. Lorsque vous y êtes invité, choisissez Autoriser pour confirmer la connexion entre AWS Toolkit for Visual Studio et votre CodeCatalyst compte. Lorsque le processus de connexion est terminé, CodeCatalyst affiche une confirmation indiquant que vous pouvez fermer votre navigateur en toute sécurité.

Utilisation des CodeCatalyst ressources Amazon issues de la AWS boîte à outils pour Visual Studio

Les sections suivantes fournissent une vue d'ensemble des fonctionnalités de gestion CodeCatalyst des ressources d'Amazon Amazon disponibles pour le AWS Toolkit pour Visual Studio.

Rubriques

- Cloner un référentiel

Cloner un référentiel

CodeCatalystest un service basé sur le cloud qui nécessite que vous soyez connecté au cloud pour travailler sur CodeCatalyst des projets. Pour travailler sur un projet localement, vous pouvez cloner CodeCatalyst des référentiels sur votre machine locale et les synchroniser avec votre CodeCatalyst projet lors de votre prochaine connexion au cloud.

Pour cloner un référentiel sur votre machine locale, procédez comme suit.

1. Dans l'élément de menu Git de Visual Studio, choisissez Clone Repository... .
2. Dans la section Parcourir un référentiel, sélectionnez Amazon CodeCatalyst comme fournisseur.

> **Note**
>
> Si la section Connexion affiche un `Not Connected` message, suivez les étapes décrites dans la section Authentification et accès : AWS Builder ID du présent guide de l'utilisateur avant de poursuivre.

3. Choisissez l'espace et le projet à partir desquels vous souhaitez cloner un référentiel.
4. Dans la section Référentiels, choisissez le référentiel que vous souhaitez cloner.
5. Dans la section Chemin, choisissez le dossier dans lequel vous souhaitez cloner votre référentiel.

> **Note**
>
> Ce dossier doit initialement être vide pour que le clonage soit réussi.

6. Sélectionnez Cloner pour commencer à cloner le référentiel.
7. Une fois le référentiel cloné, Visual Studio chargera votre solution clonée

> **Note**
>
> Si Visual Studio n'ouvre pas la solution dans le référentiel cloné, vos options de Visual Studio peuvent être ajustées à partir du paramètre Charger automatiquement la solution lors de l'ouverture d'un référentiel Git, situé dans les paramètres généraux de Git, du menu Contrôle de source.

Résolution des problèmes

Vous trouverez ci-dessous des rubriques de résolution des problèmes connus lors de l'utilisation d'Amazon CodeCatalyst à partir du AWS Toolkit pour Visual Studio.

Rubriques

Informations d'identification

Si une boîte de dialogue vous demandant des informations d'identification s'affiche lorsque vous tentez de cloner un référentiel basé sur gitCodeCatalyst, votre assistant AWS CodeCommit d'identification est peut-être configuré globalement, ce qui peut provoquer des interférences avec. CodeCatalyst Pour plus d'informations sur l'assistant AWS CodeCommit d'identification, consultez la section relative à la configuration des connexions HTTPS aux AWS CodeCommit référentiels sous Windows à l'aide de l'assistant d'identification AWS CLI du Guide de l'utilisateur. AWSCodeCommit

Pour limiter l'assistant AWS CodeCommit d'identification à la gestion des CodeCommit URL uniquement, procédez comme suit.

1. ouvrez le fichier de configuration git global dans : `%userprofile%\.gitconfig`
2. Repérez la section suivante dans votre fichier :

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

3. Modifiez cette section comme suit :

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

4. Enregistrez vos modifications, puis suivez les étapes pour cloner votre référentiel.

Amazon CloudWatch Intégration des journaux pour Visual Studio

L'Amazonie CloudWatch Intégration des journaux depuisAWSToolkit for Visual Studio vous permet de surveiller, de stocker et d'accéder CloudWatch Consigne les ressources, sans avoir à quitter votre IDE. En savoir plus sur la configuration d' CloudWatch service et comment utiliser CloudWatch Fonctionnalités des journaux, choisissez parmi les rubriques suivantes.

Rubriques

Configuration d' CloudWatch Intégration de journaux pour Visual Studio

Avant de pouvoir utiliser Amazon CloudWatch Intégration des journaux avec l'Toolkit for Visual Studio, vous avez besoin d'unAWS. Vous pouvez créer un nouveauAWSdepuis leAWSConnexionsite. La plupart des CloudWatch Les fonctionnalités de journaux disponibles dans le Toolkit for Visual Studio sont accessibles avec activeAWSInformations d'identification . Si une fonctionnalité particulière nécessite une configuration supplémentaire, les exigences sont incluses dans les sections pertinentes duUtilisation d' CloudWatch Journauxguide.

Pour plus d'informations et pour connaître les options de configuration CloudWatch Logs, consultez leConfigurationsection de l'Amazon CloudWatch Guide des journaux.

Utilisation d' CloudWatch Journaux dans Visual Studio

Amazon CloudWatch L'intégration de journaux vous permet de surveiller, de stocker et d'accéder CloudWatch Journaux à partir deAWSToolkit for Visual Studio. Avoir accès à CloudWatch Les fonctionnalités de journalisation, sans qu'il soit nécessaire de quitter votre IDE, améliorent l'efficacité en simplifiant CloudWatch Enregistre le processus de développement et réduit les perturbations de votre flux de travail. Les rubriques suivantes décrivent comment travailler avec les fonctionnalités de base de CloudWatch Intégration des journaux.

Rubriques

CloudWatch Groupes de journaux

UN`log group`est un groupe de`log streams`qui partagent les mêmes paramètres de rétention, de surveillance et de contrôle d'accès. Le nombre de flux de journaux pouvant appartenir à un groupe de journaux est illimité.

Affichage des groupes de journaux

Le`View Log Groups`affiche une liste de groupes de journaux dans CloudWatchExplorateur de groupes de journaux

Pour accéder à la fonctionnalité Afficher les groupes de journaux et ouvrir le CloudWatch Explorateur de groupes de journaux, effectuez les étapes suivantes.

1. À partir deAWSExplorateur, développerAmazon CloudWatch.
2. Double cliquezGroupes de journauxou ouvrez le menu contextuel (clic droit) et sélectionnezAfficher, pour ouvrirCloudWatch Explorateur de journaux.

> **Note**
>
> Le CloudWatch L'Explorateur des groupes de journaux s'ouvre dans la même fenêtre que l'Explorateur de solutions.

Filtrage de groupes

Votre compte individuel peut contenir des milliers de groupes de journaux différents. Pour simplifier la recherche de groupes spécifiques, utilisez le`filtering`fonctionnalité décrite ci-dessous.

1. À partir deCloudWatch Explorateur de groupes, placez le curseur dans la barre de recherche située en haut de la fenêtre.
2. Commencez à saisir un préfixe lié aux groupes de journaux que vous recherchez.
3. CloudWatch Explorateur de groupesest automatiquement mis à jour pour afficher les résultats correspondant aux termes de recherche que vous avez spécifiés à l'étape précédente.

Suppression des groupes

Pour supprimer un groupe de journaux spécifique, consultez la procédure suivante.

1. À partir deCloudWatch Explorateur de groupes, cliquez avec le bouton droit sur le groupe de journaux que vous souhaitez supprimer.
2. Lorsque vous y êtes invité, confirmez que vous souhaitez supprimer le groupe de journaux actuellement sélectionné.
3. Choix duOuisupprime le groupe de journaux sélectionné, puis rafraîchit leCloudWatch Explorateur de groupes.

Groupes de journaux

Pour actualiser la liste actuelle des groupes de journaux affichés dans leCloudWatch Explorateur de journaux, choisissez leIcône d'actualisationsitué dans lebarre d'outils.

Copier l'ARN du groupe de journaux

Pour copier l'ARN d'un groupe de journaux spécifique, procédez comme suit.

1. À partir deCloudWatch Explorateur de groupes, cliquez avec le bouton droit sur le groupe de journaux à partir duquel vous souhaitez copier un ARN.
2. Cliquez sur l'ongletCopier l'ARNdans le menu.
3. L'ARN est maintenant copié dans votre presse-papiers local et prêt à être collé.

CloudWatch Flux de journaux

Un flux de journal est une séquence d'événements du journaux qui partagent la même source.

> **Note**
>
> Lorsque vous consultez des flux de journaux, vous devez être conscient des propriétés suivantes :
>
> - Par défaut, les flux de journaux sont triés en fonction de l'horodatage de l'événement le plus récent.
> - Les colonnes associées à un flux de journaux peuvent être triées par ordre croissant ou décroissant, en activant l'optioncaretsitué dans les en-têtes de colonne.
> - Les entrées filtrées ne peuvent être triées que parLog Stream Name (Nom du flux de journaux).

Affichage de flux de journaux

1. À partir deCloudWatch Explorateur de groupesdouble-cliquez avec le bouton droit de la souris sur un groupe de journaux et sélectionnezFlux de journauxdans le menu contextuel.
2. Un nouvel onglet s'ouvre dansdocument, qui contient la liste des flux de journaux associés à votre groupe de journaux.

Filtrage de flux de

1. À partir deFlux de journauxonglet, dans ledocument, placez le curseur dans la barre de recherche.
2. Commencez à saisir un préfixe lié au flux de journaux que vous recherchez.
3. Au fur et à mesure que vous tapez, l'affichage actuel se met automatiquement à jour pour filtrer vos flux de journaux en fonction de vos entrées

Flux de journaux

Pour actualiser la liste actuelle des flux de journaux affichés dans ledocument, choisissezIcône d'actualisation, situé dans lebarre d'outils, à partir debarre de recherche.

ARN de flux de journaux

Pour copier l'ARN d'un flux de journaux spécifique, procédez comme suit.

1. À partir deFlux de journauxonglet, dans ledocument, cliquez avec le bouton droit sur le flux de journaux à partir duquel vous souhaitez copier un ARN.
2. Cliquez sur l'ongletCopier l'ARNdans le menu.
3. L'ARN est maintenant copié dans votre presse-papiers local et prêt à être collé.

Diffusion de journaux

LeFlux de journauxtélécharge et stocke le flux de journaux sélectionné localement, où il est accessible par des outils et des logiciels personnalisés pour un traitement supplémentaire.

1. À partir deFlux de journauxonglet, dans ledocument, cliquez avec le bouton droit sur le flux de journaux que vous souhaitez télécharger.
2. ChoisissezFlux de journauxpour ouvrirExporter vers un fichier textedialogue.

3. Choisissez l'emplacement où vous souhaitez stocker le fichier localement et spécifiez un nom dans le champ de texte fourni.
4. Confirmez le téléchargement en sélectionnantOK.. L'état du téléchargement est affiché dans leCentre d'état des tâches Visual Studio

CloudWatch Événements de journaux

Les événements de journaux sont des enregistrements de l'activité enregistrée par l'application ou la ressource contrôlée par CloudWatch.

Actions de journaux

Les événements de journal sont affichés sous forme de tableau. Par défaut, les événements sont triés du plus ancien au plus récent.

Les actions suivantes sont associées aux événements de journal dans Visual Studio :

- Mode texte encadré : Vous pouvez activer le texte ajusté en cliquant sur un événement.
- Bouton d'habillage de texte : situé dans le`document window` **`toolbar`**, ce bouton active et désactive le retour à la ligne, pour toutes les entrées.
- Copier les messages dans le presse-papiers : sélectionnez les messages que vous souhaitez copier, puis cliquez avec le bouton droit sur la sélection et choisissezCopier(raccourci clavier)`Ctrl + C`).

Affichage des événements de journaux

1. À partir dedocument, choisissez un onglet contenant la liste des flux de journaux.
2. Double-cliquez sur un flux de journaux ou cliquez avec le bouton droit sur un flux de journauxFlux de journauxà partir du menu.
3. A new Événements de journauxs'ouvre dans l'ongletdocument, qui contient un tableau des événements de journaux associés au flux de journaux que vous avez choisi.

Filtrage de journaux

Vous pouvez filtrer les événements de journaux de trois manières : par contenu, par plage horaire ou les deux. Pour filtrer les événements de vos journaux à la fois par contenu et par plage horaire,

commencez par filtrer vos messages par contenu ou par plage horaire, puis filtrez ces résultats par l'autre méthode.

Pour filtrer les événements de vos journaux par contenu :

1. À partir deÉvénements de journauxonglet, dans ledocument, placez le curseur dans la barre de recherche située en haut de la fenêtre.
2. Commencez à saisir un terme ou une phrase en rapport avec les événements de journal que vous recherchez.
3. Au fur et à mesure que vous tapez, l'affichage actuel commence automatiquement à filtrer les événements de vos journaux.

> **Note**
>
> Les modèles de filtre sont sensibles à la casse. Vous pouvez améliorer les résultats de recherche en mettant les termes exacts et les phrases entre des caractères non alphanumériques entre des guillemets doubles (*""*). Pour en savoir plus sur les modèles de filtre, consultez leSyntaxe de filtre et de modèlesujet dans Amazon CloudWatch guide.

Pour afficher les événements de journaux générés pendant une période spécifique :

1. À partir deÉvénements de journauxonglet, dans ledocument, choisissezIcône de calendrier, situé dans lebarre d'outils.
2. À l'aide des champs fournis, spécifiez la période dans laquelle rechercher.
3. Les résultats filtrés sont automatiquement mis à jour lorsque vous spécifiez les contraintes de date et d'heure.

> **Note**
>
> LeEffacer le filtreefface tous vos paramètres actuels date-and-time Sélections de filtre.

Événements de journaux

Pour actualiser la liste actuelle des événements de journaux affichés dans leÉvénements de journaux, choisissezIcône d'actualisation, situé dans lebarre d'outils.

Accès supplémentaire à CloudWatchJournaux

Vous pouvez accéder à CloudWatch Journaux associés à d'autresAWSservices et ressources directement à partir duAWSToolkit dans Visual Studio.

Lambda

Pour afficher les flux de journaux associés à une fonction Lambda :

> **Note**
>
> Votre rôle d'exécution Lambda doit avoir les autorisations appropriées pour envoyer des journaux à CloudWatchBûches. Pour plus d'informations sur les autorisations Lambda requises pour CloudWatch Logs, consultez lehttps://docs.aws.amazon.com/lambda/latest/dg/monitoring-cloudwatchlogs.html#monitoring-cloudwatchlogs-prereqs

1. À partir deAWSToolkit Explorer, développezLambda.
2. cliquez avec le bouton droit de la souris sur la fonction à afficher, puis choisissezAfficher les journauxpour ouvrir les flux de journaux associés dansdocumentfenêtre.

Pour afficher les flux de journaux à l'aide de l'Lambda`function view` :

1. À partir deAWSToolkit Explorer, développezLambda.
2. cliquez avec le bouton droit de la souris sur la fonction à afficher, puis choisissezFonction Viewpour ouvrir la vue des fonctions dans ledocumentfenêtre.
3. À partir de`function view`, surJournaux, les flux de journaux associés à la fonction Lambda sélectionnée s'affichent.

ECS

Pour afficher les ressources de journaux associées à un conteneur de tâches ECS, procédez comme suit.

> **Note**
>
> Pour que le service Amazon ECS envoie des journaux à CloudWatch, chaque conteneur pour une tâche Amazon ECS donnée doit répondre à la configuration requise. Pour plus

d'informations sur la configuration et les configurations requises, veuillez consulter le guideUtilisation deAWSPilote de journal.

1. À partir deAWSToolkit Explorer, développezAmazon ECS.
2. Sélectionnez le cluster Amazon ECS que vous souhaitez afficher pour ouvrir un nouveauCluster ECSonglet, dans ledocumentfenêtre.
3. Dans le menu de navigation, situé sur la gauche de laCluster ECS, choisissezTâchespour afficher toutes les tâches associées au cluster.
4. À partir deTâchesafficher, sélectionnez une tâche et choisissezAfficher les journaux, situé dans le coin inférieur gauche.

   > **Note**
   >
   > Cet affichage répertorie toutes les tâches contenues dans le cluster, le`View Logs`n'est visible que pour chaque tâche qui répond à la configuration requise des journaux.
   >
   > - Si une tâche n'est associée qu'à un seul conteneur,Afficher les journauxouvre le flux de journaux de ce conteneur.
   > - Si une tâche est associée à plusieurs conteneurs,Afficher les journauxouvre leAfficher CloudWatch Journaux pour la tâche ECS, utilisez la boîte de dialogueConteneur :menu déroulant pour choisir le conteneur pour lequel vous souhaitez afficher les journaux, puis choisissezOK..

5. Un nouvel onglet s'ouvre dans ledocumentqui affiche les flux de journaux associés à votre sélection de conteneur.

Gestion des instances Amazon EC2

AWSExplorer fournit une vue détaillée des Amazon Machine Images (AMI) et des instances Amazon Elastic Compute Cloud (Amazon EC2). Dans ces vues, vous pouvez lancer une instance Amazon EC2 à partir d'une AMI, vous y connecter et arrêter ou résilier l'instance, depuis l'intérieur de l'environnement de développement Visual Studio. Vous pouvez utiliser la vue des instances pour créer des AMI depuis vos instances. Pour plus d'informations, consultez Créer une AMI à partir d'une instance Amazon EC2.

Les vues des images machine Amazon et des instances Amazon EC2

DeAWSExplorer, vous pouvez afficher les vues des Amazon Machine Images (AMI) et des instances Amazon EC2. DansAWSExplorer, développez leAmazon EC2nœud.

Pour afficher la vue AMI, sur le premier sous-nœud, AMI, ouvrez le menu contextuel (clic droit) et choisissez Afficher.

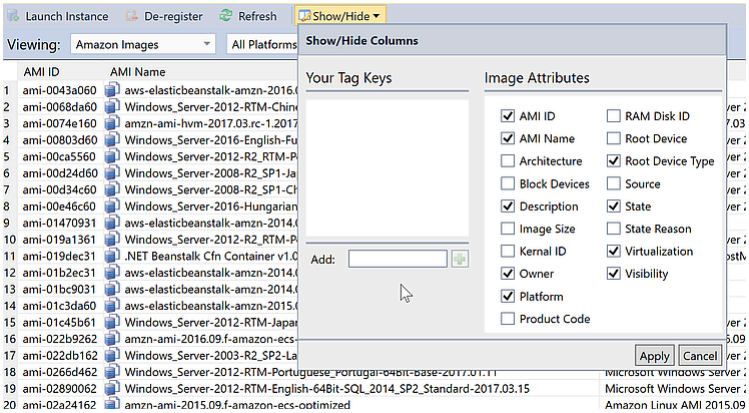
Pour afficher la vue des instances Amazon EC2, sur le nœud Instances, ouvrez le menu contextuel (clic droit) et choisissez Afficher.

Vous pouvez également afficher ces vues en cliquant deux fois sur le nœud approprié.

- Les vues sont étendues à la région spécifiée dansAWSExplorer (par exemple, la région USA Ouest (Californie du Nord))).
- Vous pouvez réorganiser les colonnes par glisser-déposer. Pour trier les valeurs d'une colonne, cliquez sur l'en-tête de cette dernière.
- Vous pouvez utiliser les listes déroulantes et la zone de filtre dans Affichage pour configurer les vues. La vue initiale affiche les AMI de tous les types de plate-forme (Windows ou Linux) détenus par le compte spécifié dansAWSExplorer.

Afficher / Masquer les colonnes

Vous pouvez également choisir l'option déroulante Afficher/Masquer en haut de la vue pour configurer l'affichage des colonnes. Votre choix de colonnes est conservé si vous fermez la vue et la rouvrez.



L'interface Afficher / Masquer les colonnes pour les vues des AMI et des instances

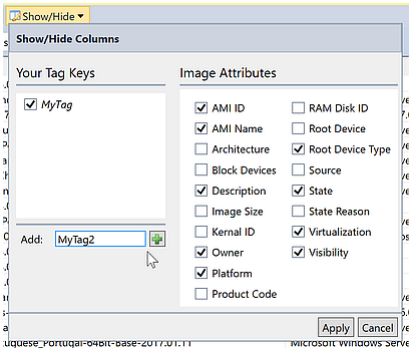
Balisage des AMI, des instances et des volumes

Vous pouvez également utiliser l'Show/Hide HideListe déroulante pour ajouter des balises pour les AMI, les instances Amazon EC2 ou les volumes que vous possédez. Les balises sont des paires nom-valeur qui vous permettent d'attacher des métadonnées à vos AMI, vos instances et vos volumes. Les noms de balise sont limités à votre compte et sont séparés de vos AMI et de vos instances. Par exemple, il n'y a aucun conflit si vous avez utilisé le même nom de balise pour vos AMI et vos instances. Les noms de balise ne sont pas sensibles à la casse.

Pour en savoir plus sur les balises, consultezUtilisation de balisesdans leGuide de l'utilisateur Amazon EC2 pour les instances Linux.

Pour ajouter une balise

1. Dans la zone Ajouter, saisissez le nom de la balise. Choisissez le bouton vert avec le signe plus (+), puis choisissez Appliquer.



   Ajouter une balise à une AMI ou une instance Amazon EC2

   La nouvelle balise est affichée en italique, ce qui indique qu'aucune valeur ne lui a encore été associée.

   Dans la liste, le nom de la balise apparaît sous forme de nouvelle colonne. Lorsque au moins une valeur a été associée à la balise, cette dernière devient visible dans l'AWS Management Console.

2. Pour ajouter une valeur à la balise, cliquez deux fois sur une cellule de la colonne de cette balise, puis saisissez une valeur. Pour supprimer la valeur de la balise, cliquez deux fois sur la cellule et supprimez le texte.

   Si vous supprimez la balise de la liste déroulante Afficher/Masquer, la colonne correspondante disparaît de la vue. La balise est préservée, ainsi que les valeurs de la balise associées aux AMI, aux instances ou aux volumes.

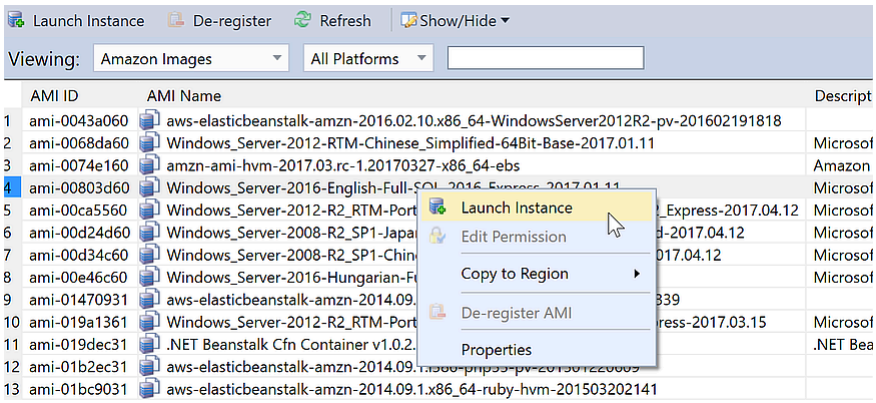
> **Note**
>
> Si vous effacez une balise dans leShow/Hide Hideliste déroulante qui n'a pas de valeurs associées, la liste déroulanteAWSToolkit supprimera entièrement la balise. Elle n'apparaîtra plus dans la vue liste ou dans la liste déroulante Afficher/Masquer. Pour utiliser de nouveau cette balise, utilisez la boîte de dialogue Afficher/Masquer pour la recréer.

Lancement d'une instance Amazon EC2

AWSExplorer fournit toutes les fonctionnalités requises pour lancer une instance Amazon EC2. Dans cette section, nous allons sélectionner une image machine Amazon (AMI), configurez-la et démarrez-la en tant qu'instance Amazon EC2.

Pour lancer une instance Windows Server Amazon EC2

1. En haut de la vue AMI, dans la liste déroulante de gauche, choisissez Images Amazon. Dans la liste déroulante de droite, choisissez Windows. Dans la zone de filtre, saisissez `ebs` pour Elastic Block Storage. L'actualisation de la vue peut prendre quelques minutes.
2. Choisissez une AMI dans la liste, ouvrez le menu contextuel (clic droit) et choisissez Lancer une instance.



Liste AMI

3. Dans la boîte de dialogue Launch New Amazon EC2 Instance (Lancer une nouvelle instance Amazon EC2), configurez l'AMI de votre application.

Type d'instance

Choisissez le type d'instance EC2 à lancer. Pour obtenir la liste des types d'instances et la tarification correspondante, consultez la page Tarification EC2.

Nom

Saisissez un nom pour votre instance. Ce nom ne peut pas dépasser 256 caractères.

Key Pair (Paire de clés)

Une paire de clés est utilisée pour obtenir le mot de passe Windows permettant de se connecter à l'instance EC2 à l'aide du protocole RDP (Remote Desktop Protocol). Choisissez une paire de clés pour laquelle vous disposez d'un accès à la clé privée, ou choisissez l'option pour créer une paire de clés. Si vous créez la paire de clés dans la boîte à outils, cette dernière peut stocker la clé privée pour vous.

Les paires de clés stockées dans la boîte à outils sont chiffrées. Elles sont accessibles sur`%LOCALAPPDATA%\AWSToolkit\keypairs`(généralement : `C:\Users\<user>\AppData\Local\AWSToolkit\keypairs`). Vous pouvez exporter la key pair chiffrée dans une`.pem`dans le fichier.

a. Dans Visual Studio, sélectionnezAfficherpuis cliquez surAWSExplorateur.

b. Cliquez sur Amazon EC2 et sélectionnez Paires de clés.

c. Les paires de clés sont répertoriées et celles créées/gérées par la boîte à outils marquées comme Stored in AWSToolkit (Stockées dans AWSToolkit).

d. Cliquez avec le bouton droit sur la paire de clés que vous avez créée et sélectionnez Export Private Key (Exporter la clé privée). La clé privée est non chiffrée et stockée dans l'emplacement spécifié.

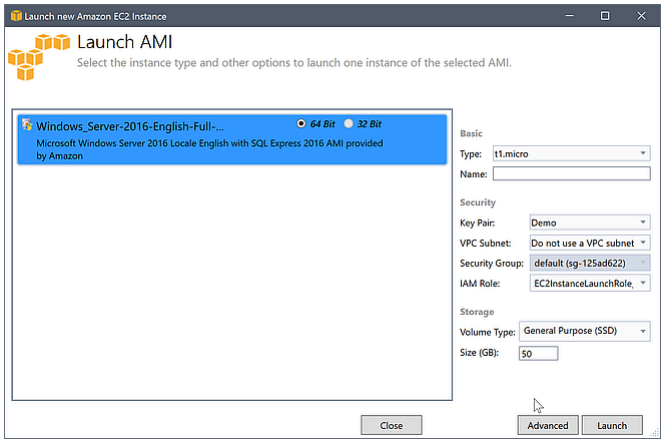
Security Group

Le groupe de sécurité contrôle le type de trafic réseau accepté par l'instance EC2. Choisissez un groupe de sécurité qui autorise le trafic entrant sur le port 3389, c'est-à-dire le port utilisé par RDP, afin que vous puissiez vous connecter à l'instance EC2. Pour plus d'informations sur l'utilisation de la boîte à outils pour créer des groupes de sécurité, consultezGestion des groupes de sécurité à partir deAWSExplorateur.

Profil d'instance

Le profil d'instance est un conteneur logique de rôle IAM. Lorsque vous choisissez un profil d'instance, vous associez le rôle IAM à l'instance EC2. Les rôles IAM sont configurés avec

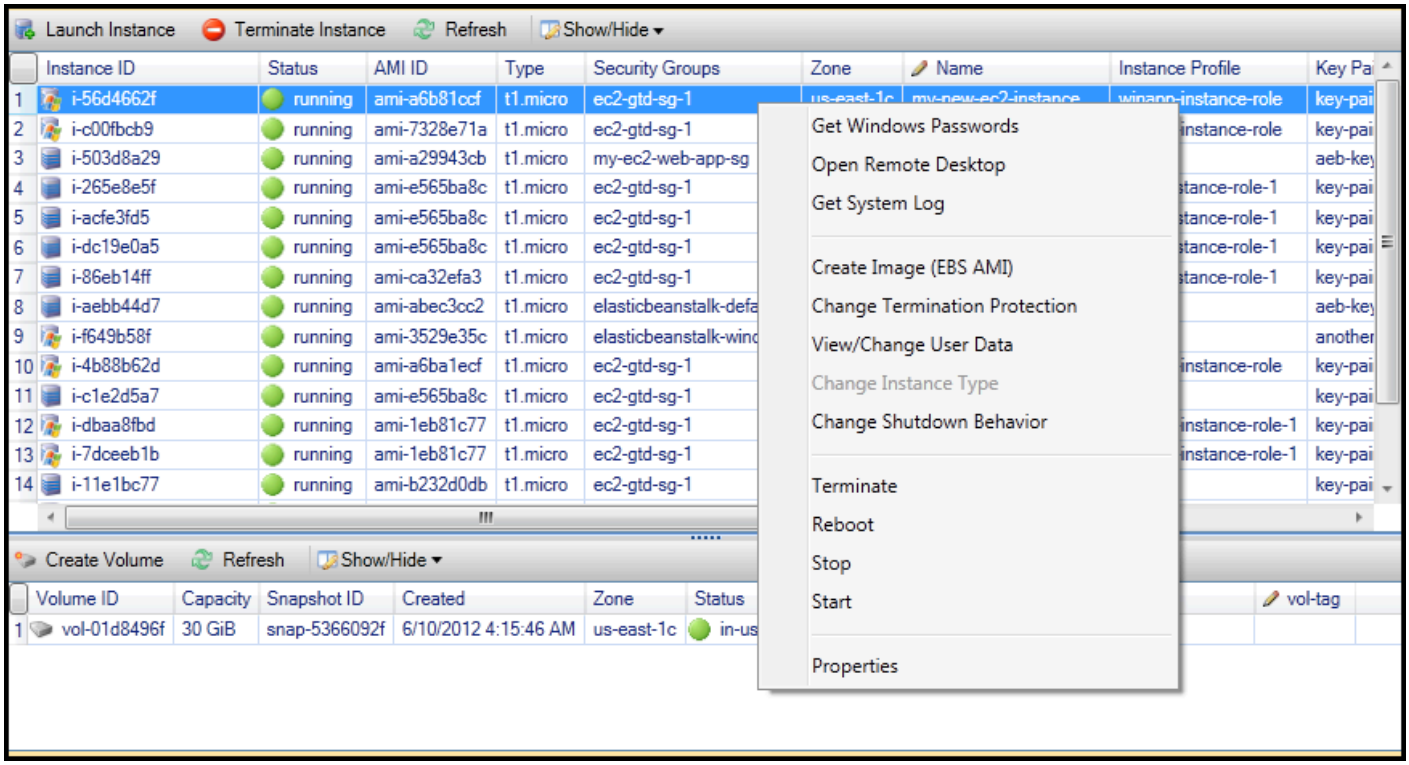
des stratégies qui spécifient l'accès aux Amazon Web Services et aux ressources de compte Amazon Web. Lorsqu'une instance EC2 est associée à un rôle IAM, le logiciel d'application exécuté sur l'instance s'exécute avec les autorisations spécifiées par le rôle IAM. Ainsi, le logiciel d'application peut être exécuté sans avoir à spécifier deAWSinformations d'identification spécifiques, ce qui le rend plus sûr. Pour plus d'informations sur les rôles IAM, accédez au Guide de l'utilisateur IAM.



Boîte de dialogue Launch AMI (Lancer une AMI) EC2

4. Choisissez Launch.

DansAWSExplorer, sur leInstancessous-nœud deAmazon EC2, ouvrez le menu contextuel (clic droit) et choisissez.Afficher. LeAWSToolkit affiche la liste des instances Amazon EC2 associées au compte actif. Vous devrez peut-être choisir Actualiser pour afficher votre nouvelle instance. Lorsque l'instance s'affiche d'abord, elle peut passer par l'état en attente, mais après quelques instants, elle passe à l'état en cours.



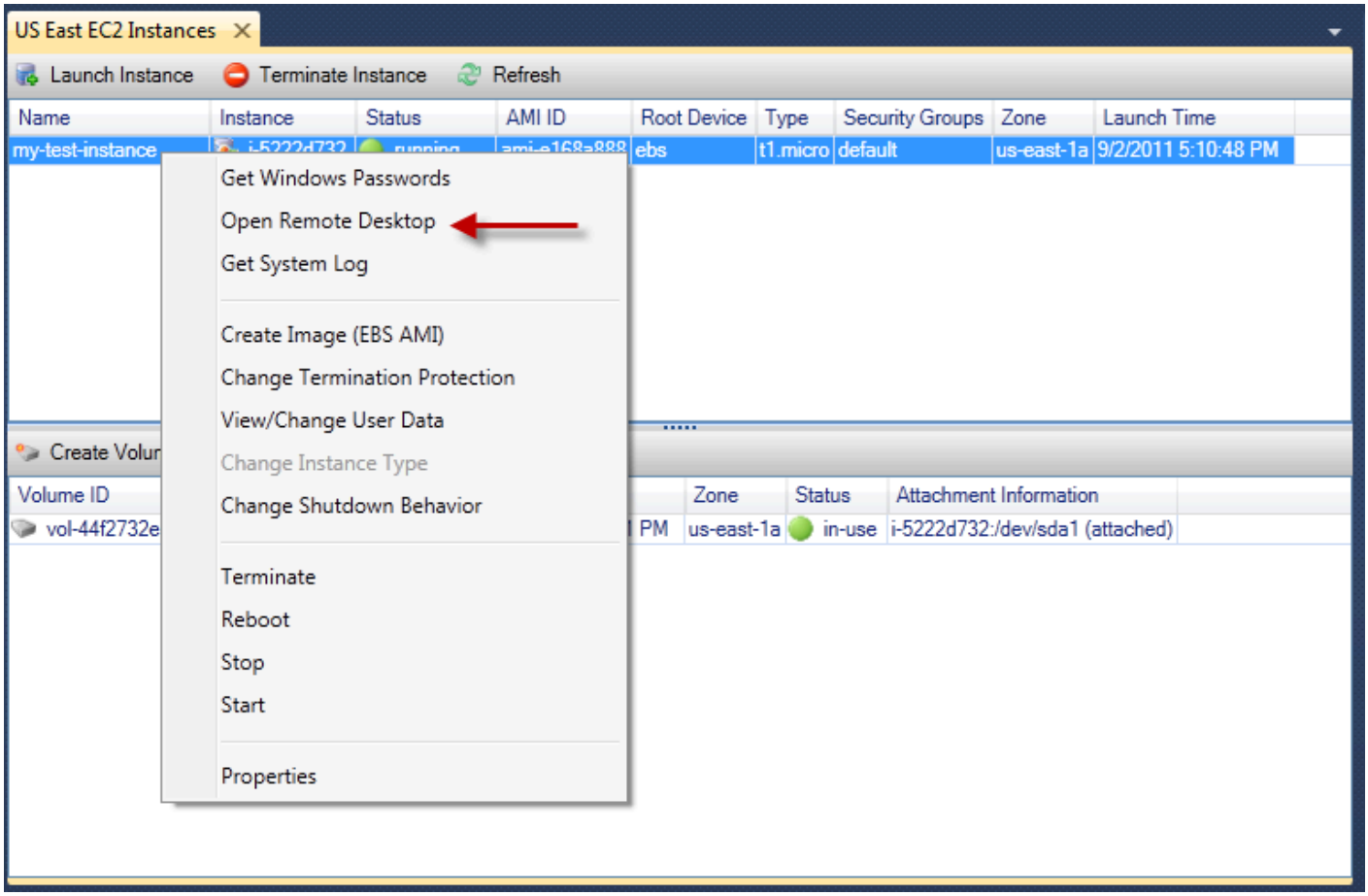
Connexion à une instance Amazon EC2

Vous pouvez utiliser le Bureau à distance Windows pour vous connecter à une instance Windows Server. Pour l'authentification, leAWSToolkit vous permet de récupérer le mot de passe administrateur de l'instance, ou de simplement utiliser la key pair stockée associée à l'instance. Dans la procédure suivante, nous allons utiliser la paire de clés stockée.

Pour se connecter à une instance Windows Server à l'aide du Bureau à distance Windows

1. Dans la liste d'instance EC2, cliquez avec le bouton droit sur l'instance Windows Server à laquelle vous souhaitez vous connecter. Dans le menu contextuel, choisissez Open Remote Desktop (Ouvrir le bureau à distance).

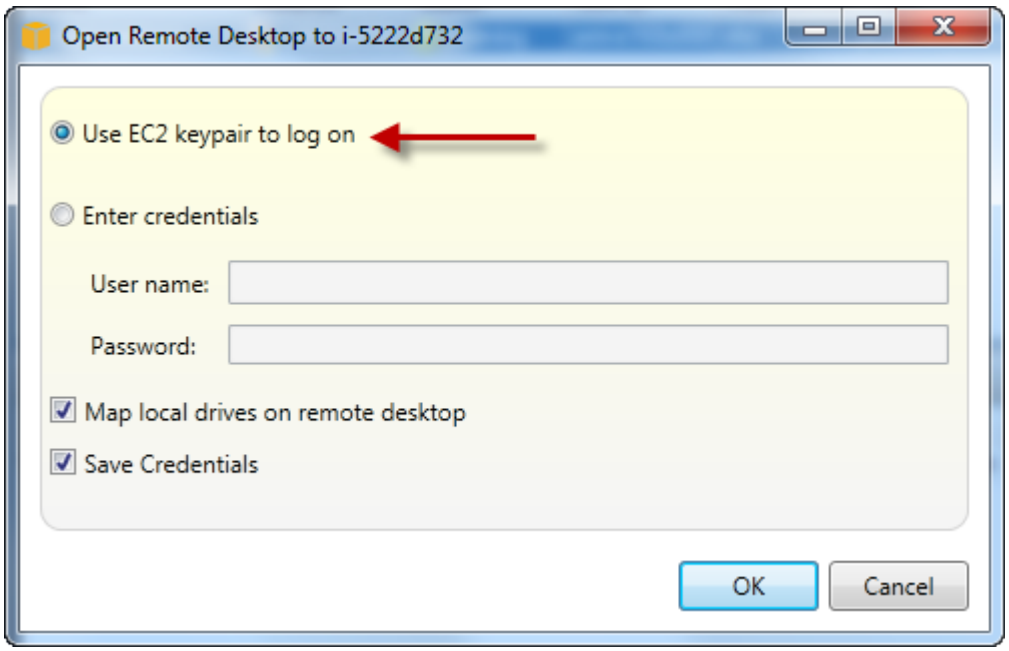
   Si vous souhaitez vous authentifier à l'aide du mot de passe administrateur, choisissez Get Windows Passwords (Obtenir des mots de passe Windows).



Menu contextuel d'instance EC2

2. Dans la boîte de dialogue Open Remote Desktop (Ouvrir le bureau à distance), choisissez Use EC2 keypair to log on (Utiliser la paire de clés EC2 pour vous connecter), puis choisissez OK.

   Si vous n'avez pas stocker une key pair avec l'AWSBoîte à outils, spécifiez le fichier PEM contenant la clé privée.

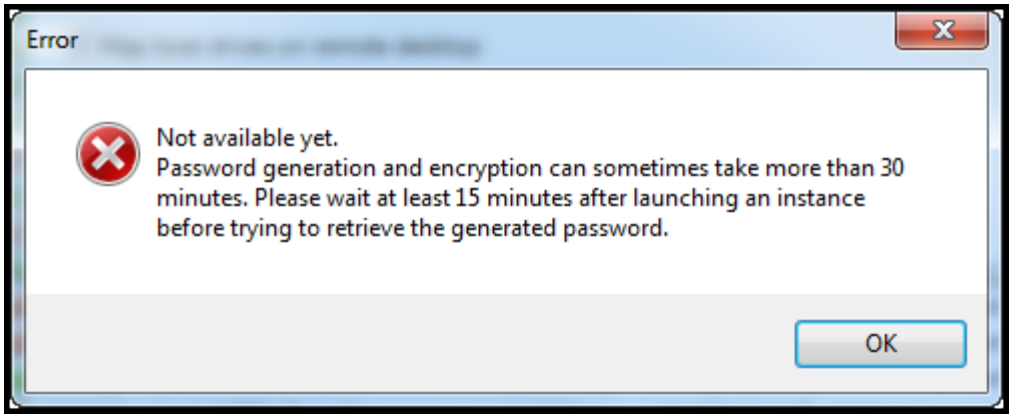


Boîte de dialogue Open Remote Desktop (Ouvrir le bureau à distance)

3. La fenêtre Remote Desktop (Bureau à distance) s'ouvre. Vous n'avez pas besoin de vous connecter car l'authentification s'est faite avec la paire de clés. Vous agirez en tant qu'administrateur sur l'instance Amazon EC2.

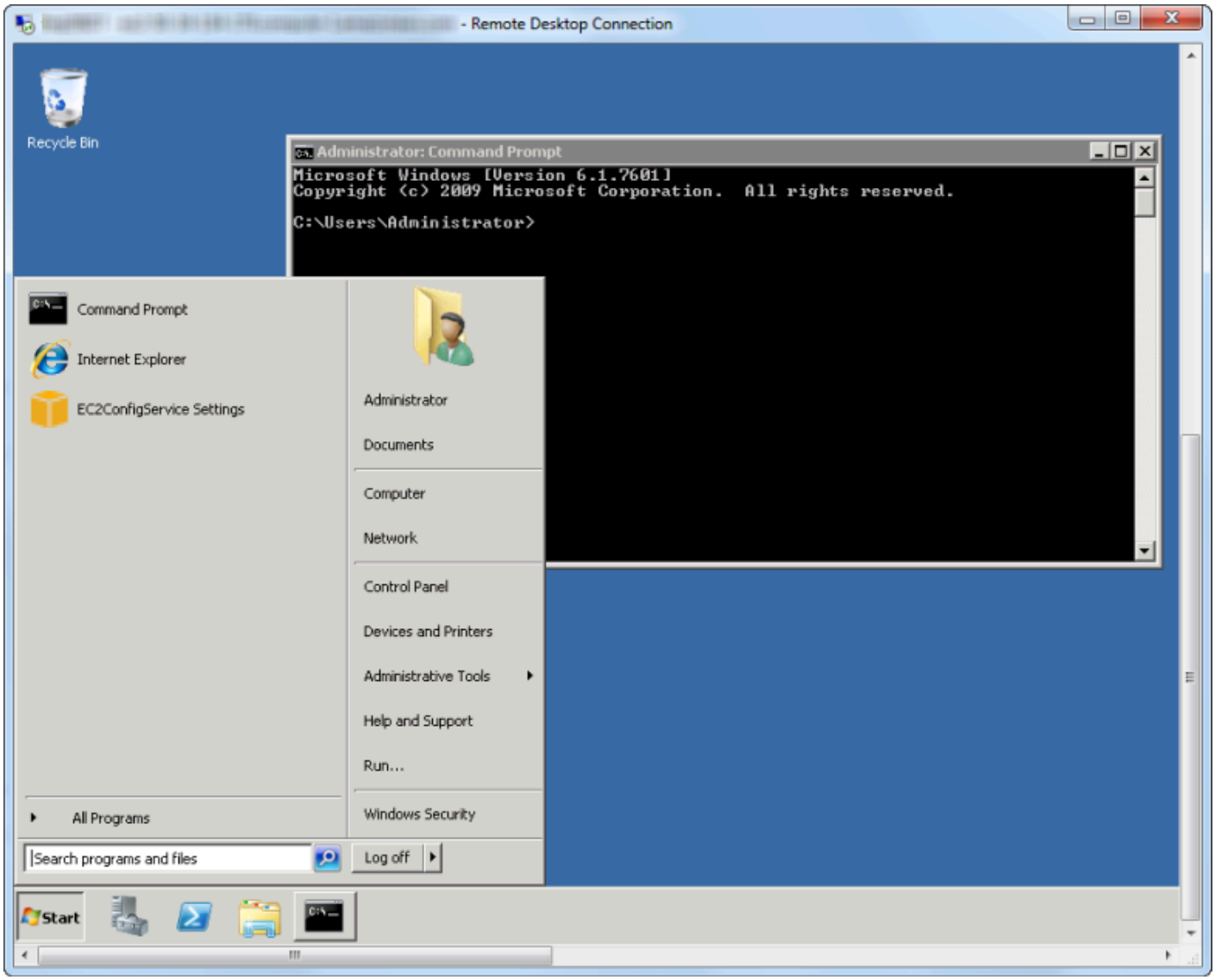
   Si l'instance EC2 vient seulement d'être lancée, vous ne pourrez peut-être pas vous connecter pour deux raisons :

   - Le service Bureau à distance peut ne pas être encore opérationnel. Patientez quelques minutes et réessayez.
   - Les informations de mot de passe peuvent ne pas avoir été transmises à l'instance. Dans ce cas, une zone de message semblable à ce qui suit apparaîtra.



Mot de passe pas encore disponible

La capture d'écran suivante illustre un utilisateur connecté en tant qu'administrateur via le Bureau à distance.



Bureau à distance

Mise hors service d'une instance Amazon EC2

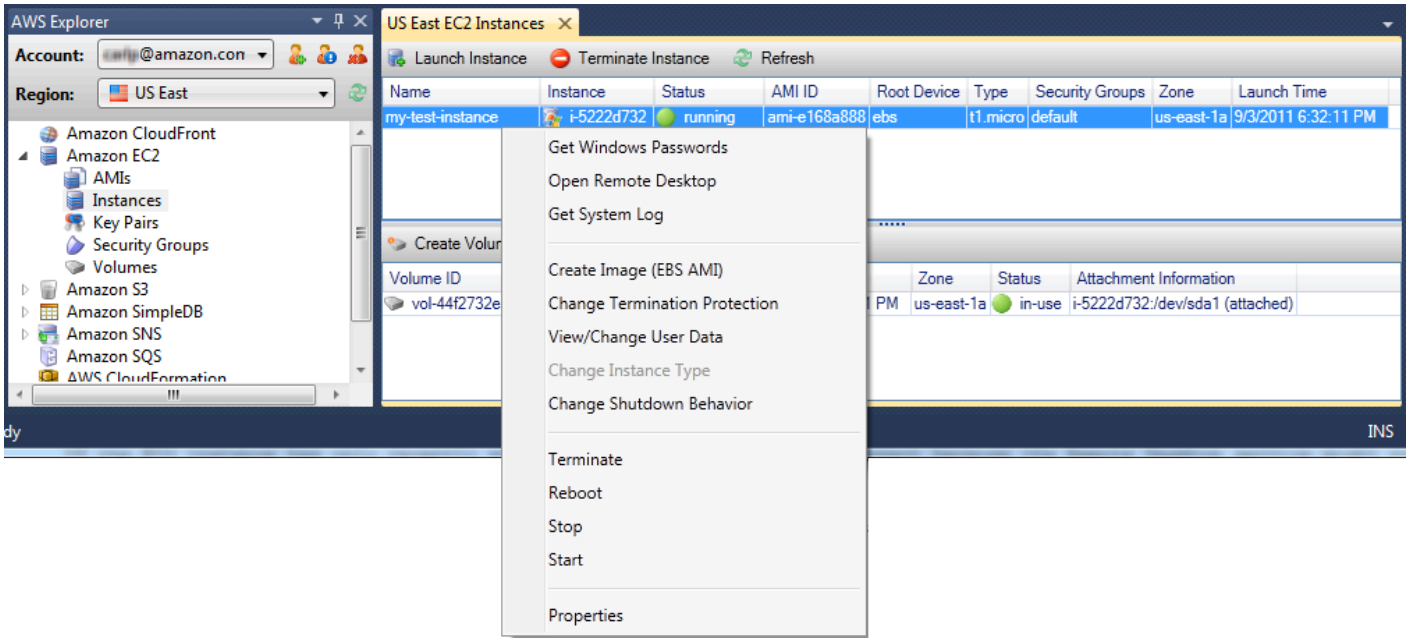
Utilisation deAWSToolkit, vous pouvez arrêter ou résilier une instance Amazon EC2 en cours d'exécution depuis Visual Studio. Pour être arrêtée, l'instance EC2 doit utiliser un volume Amazon EBS. Si l'instance EC2 n'utilise pas de volume Amazon EBS, vous n'avez pas d'autre choix que de la résilier.

Si vous arrêtez l'instance, les données stockées sur le volume EBS sont conservées. Si vous résiliez l'instance, toutes les données stockées sur l'appareil de stockage local de l'instance sont perdues. Dans les deux cas, que vous l'arrêtiez ou la résiliez, vous ne serez plus facturé pour l'instance EC2. Cependant, si vous arrêtez une instance, vous continuerez à être facturé pour le stockage EBS qui persiste après son arrêt.

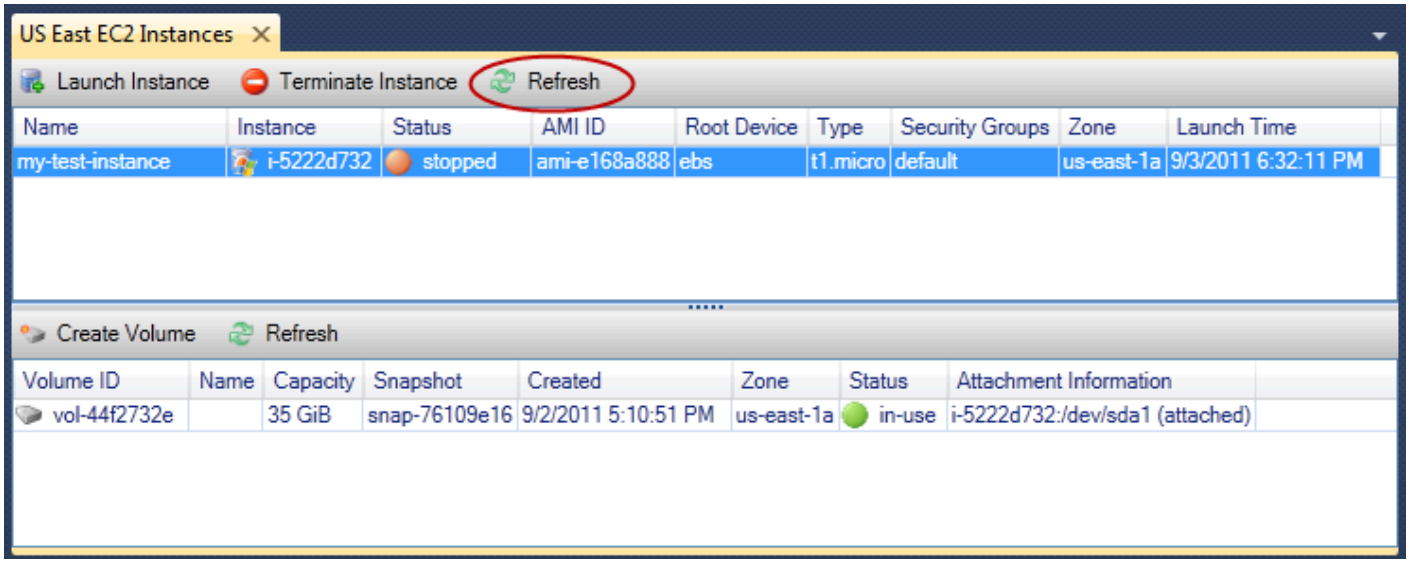
L'autre moyen de mettre fin à une instance consiste à utiliser le Bureau à distance pour vous connecter à l'instance, puis dans le menu Windows Début, utilisez Fermeture. Dans ce scénario, vous pouvez configurer l'instance pour qu'elle s'arrête ou soit résiliée.

Pour arrêter une instance Amazon EC2

1. DansAWSExplorer, développez leAmazon EC2Ouvrez le menu contextuel (clic droit) correspondant àInstancespuis choisissezAfficher. Dans la liste Instances, cliquez avec le bouton droit sur l'instance que vous souhaitez arrêter et choisissez Arrêter dans le menu contextuel. Choisissez Oui pour confirmer que vous souhaitez arrêter l'instance.

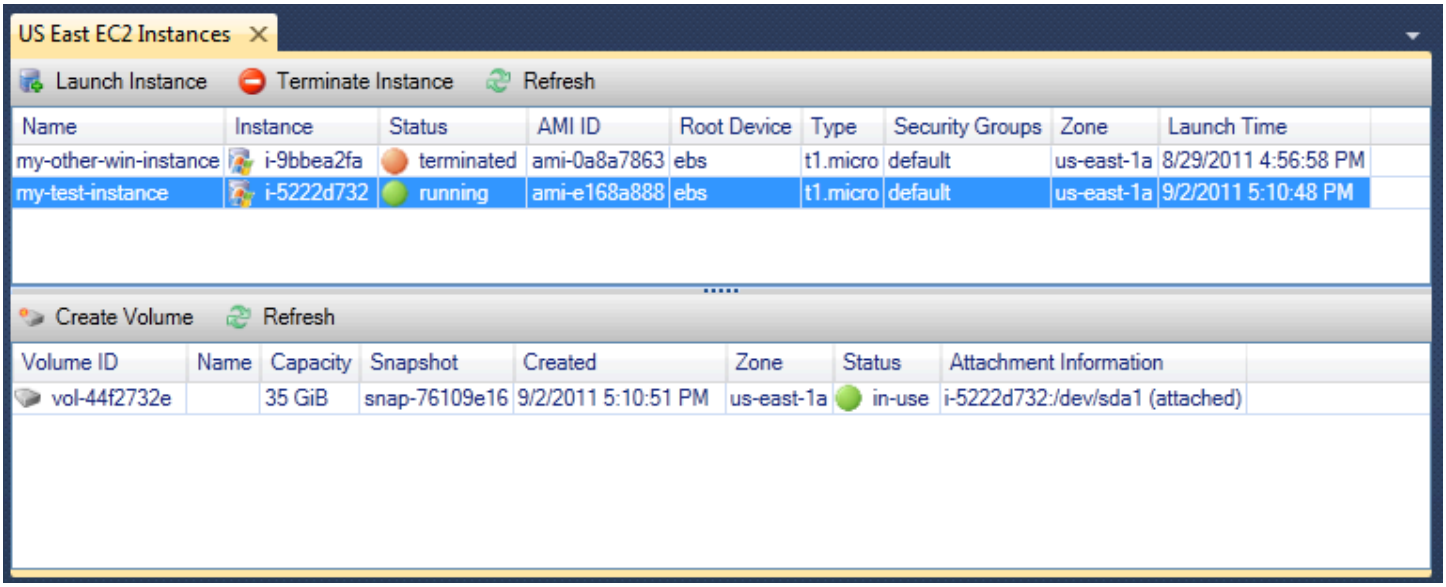


2. En haut de la liste Instances, choisissez Actualiser pour constater la modification de l'état de l'instance Amazon EC2. Le volume EBS associé à l'instance est toujours actif car nous avons arrêté l'instance plutôt que de la résilier.



Instances résiliées qui restent visibles

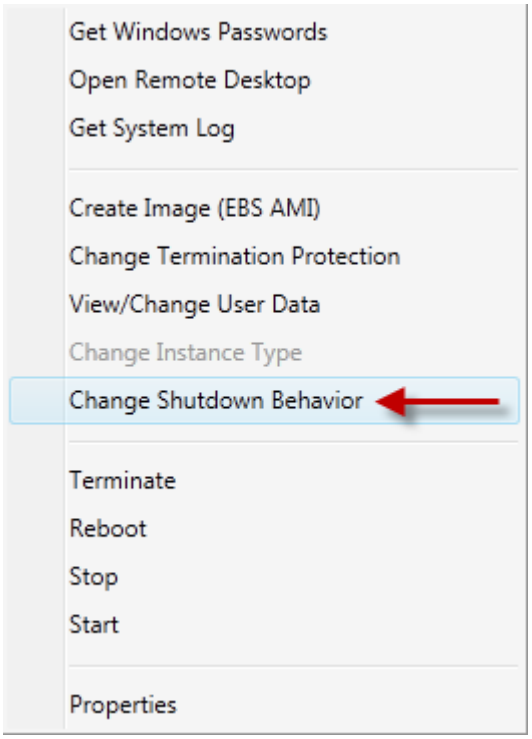
Si vous résiliez une instance, elle apparaît toujours dans la liste Instance avec les instances en cours ou arrêtées. Finalement,AWSrécupère ces instances et elles disparaissent de la liste. Vous n'êtes pas facturé pour les instances résiliées.



Pour spécifier le comportement d'une instance EC2 à l'arrêt

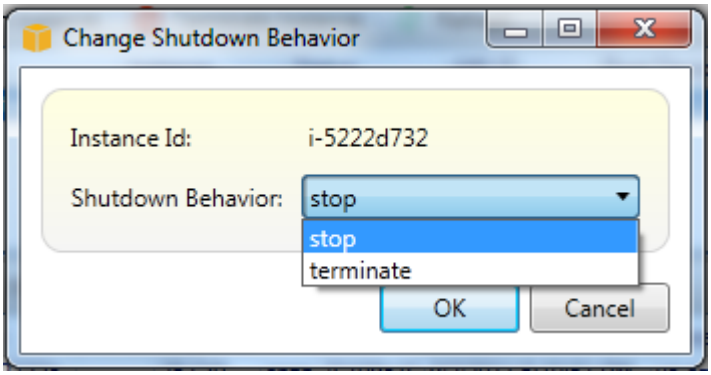
LeAWSToolkit vous permet de spécifier si une instance Amazon EC2 sera arrêtée ou résiliée siFermetureest sélectionné à partir duDémarrermenu.

1. Dans la liste Instances, cliquez avec le bouton droit sur une instance Amazon EC2, puis choisissez Changer le comportement d'arrêt.



Élément du menu Changer le comportement d'arrêt

2. Dans la boîte de dialogue Changer le comportement d'arrêt, dans la liste déroulante Comportement d'arrêt, choisissez Arrêter ou Terminer.



Gestion des instances Amazon ECS

AWSAmazon Explorer fournit des vues détaillées des clusters Amazon Elastic Container Service (Amazon ECS) et des référentiels de conteneur. Vous pouvez créer, supprimer et gérer les détails des clusters et des conteneurs à partir de l'environnement de développement Visual Studio.

Modification des propriétés du service

Vous pouvez consulter les détails, les événements et les propriétés du service à partir de l'affichage du cluster.

1. DansAWSOuvrez le menu contextuel (clic droit) du cluster à gérer, puis choisissezAfficher.
2. Dans la vue Cluster ECS, cliquez sur Services sur la gauche, puis sur l'onglet Détails dans la vue des détails. Vous pouvez cliquer sur Événements pour voir les messages d'événement et sur Déploiements pour afficher le statut du déploiement.
3. Cliquez sur Modifier. Vous pouvez modifier le nombre de tâches souhaitées, ainsi que le pourcentage minimal et maximal de tâches saines.
4. Cliquez sur Enregistrer pour accepter les modifications ou sur Annuler pour rétablir les valeurs existantes.

Arrêt d'une tâche

Vous pouvez voir le statut actuel des tâches et arrêter une ou plusieurs tâches dans l'affichage du cluster.

Pour arrêter une tâche

1. DansAWSOuvrez le menu contextuel (clic droit) du cluster contenant les tâches que vous souhaitez arrêter, puis choisissezAfficher.
2. Dans la vue Cluster ECS, cliquez sur Tâches sur la gauche.
3. Vérifiez que l'option Desired Task Status (Statut de tâche souhaité) est définie sur `Running`. Choisissez les tâches individuelles à arrêter, puis cliquez sur Arrêter ou sur Tout arrêter pour sélectionner et arrêter toutes les tâches en cours d'exécution.
4. Dans la boîte de dialogue Arrêter les tâches, choisissez Oui.

Suppression d'un service

Vous pouvez supprimer des services à partir d'un cluster dans l'affichage du cluster.

Pour supprimer un service de cluster

1. DansAWSOuvrez le menu contextuel (clic droit) du cluster contenant un service à supprimer, puis choisissezAfficher.

2. Dans la vue Cluster ECS, cliquez sur Services sur la gauche, puis sur Supprimer.
3. Dans la boîte de dialogue Supprimer un cluster, si votre cluster contient un équilibreur de charge et un groupe cible, vous pouvez choisir de les supprimer avec le cluster. Ils ne seront pas utilisés lors de la suppression du service.
4. Dans la boîte de dialogue Supprimer un cluster, choisissez OK. Lorsque le cluster est supprimé, il est supprimé duAWSExplorer.

Suppression d'un cluster

Vous pouvez supprimer un cluster Amazon Elastic Container Service à partir deAWSExplorer.

Pour supprimer un cluster

1. DansAWSOuvrez le menu contextuel (clic droit) du cluster que vous souhaitez supprimer sous le bouton droit de la sourisClustersNœud deAmazon ECSChoisissez, puisSupprimer.
2. Dans la boîte de dialogue Supprimer un cluster, choisissez OK. Lorsque le cluster est supprimé, il est supprimé duAWSExplorer.

Création d'un référentiel

Vous pouvez créer un référentiel Amazon Elastic Container Registry à partir deAWSExplorer.

Pour créer un référentiel

1. DansAWSOuvrez le menu contextuel (clic droit) du menuRéférentielsnoeud sousAmazon ECSChoisissez, puisCréation d'un référentiel.
2. Dans la boîte de dialogue Créer un référentiel, indiquez un nom de référentiel, puis cliquez sur OK.

Suppression d'un référentiel

Vous pouvez supprimer un référentiel Amazon Elastic Container Registry à partir deAWSExplorer.

Pour supprimer un référentiel

1. DansAWSOuvrez le menu contextuel (clic droit) du menuRéférentielsnoeud sousAmazon ECSChoisissez, puisSuppression d'un référentiel.

2. Dans la boîte de dialogue Supprimer le référentiel, vous pouvez choisir de supprimer le référentiel, même s'il contient des images. Sinon, il ne sera supprimé que s'il est vide. Cliquez Oui.

Gestion des groupes de sécurité depuisAWSExplorateur

La Toolkit for Visual Studio vous permet de créer et de configurer des groupes de sécurité à utiliser avec des instances Amazon Elastic Compute Cloud (Amazon EC2) ouAWS CloudFormation. Lorsque vous lancez des instances Amazon EC2 ou déployez une application surAWS CloudFormation, vous spécifiez un groupe de sécurité à associer aux instances Amazon EC2. (Deployment versAWS CloudFormationcrée des instances Amazon EC2.)

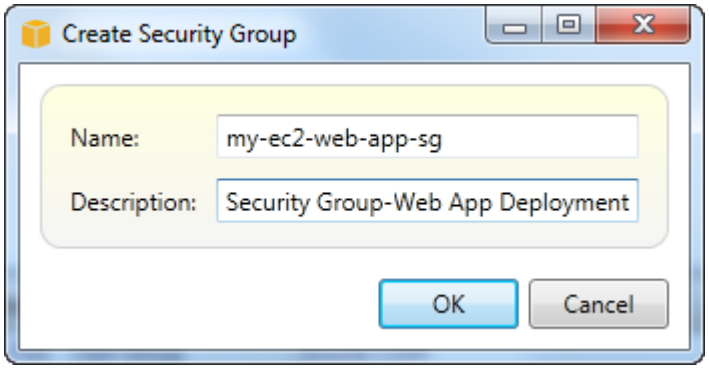
Le groupe de sécurité agit comme un pare-feu sur le trafic réseau entrant. Le groupe de sécurité spécifie les types de trafic réseau autorisés sur une instance Amazon EC2. Il peut également indiquer que le trafic entrant sera accepté uniquement depuis certaines adresses IP ou d'autres utilisateurs ou groupes de sécurité spécifiés.

Création d'un groupe de sécurité

Dans cette section, nous allons créer un groupe de sécurité. Une fois créé, le groupe de sécurité ne dispose d'aucune autorisation configurée. La configuration des autorisations est effectuée par le biais d'une opération supplémentaire.

Pour créer un groupe de sécurité

1. DansAWSExplorer, sous leAmazon EC2, ouvrez le menu contextuel (clic droit) sur laGroupes de sécurité, puis choisissezAfficher.
2. Dans l'onglet Groupes de sécurité EC2, choisissez Créer un groupe de sécurité.
3. Dans la boîte de dialogue Créer un groupe de sécurité, saisissez le nom et la description du groupe de sécurité, puis choisissez OK.

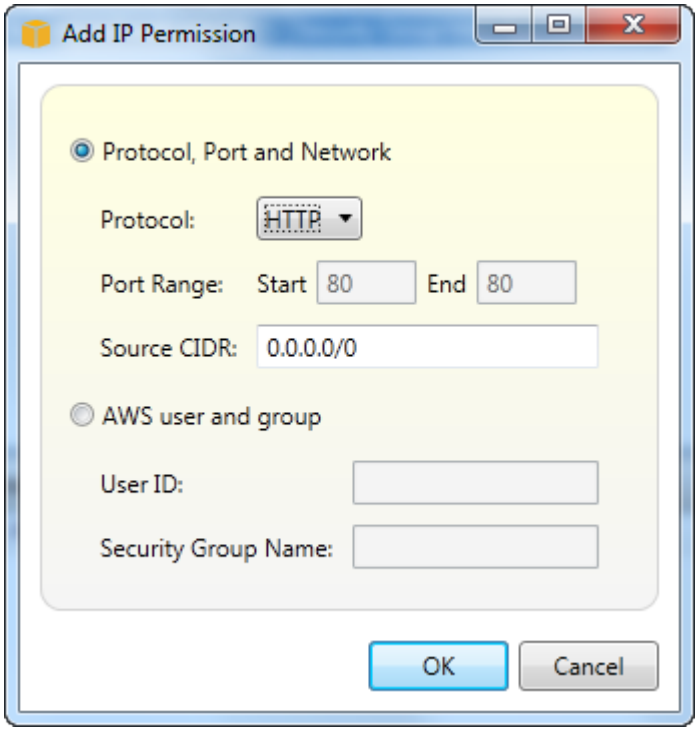


Ajout d'autorisations aux groupes de sécurité

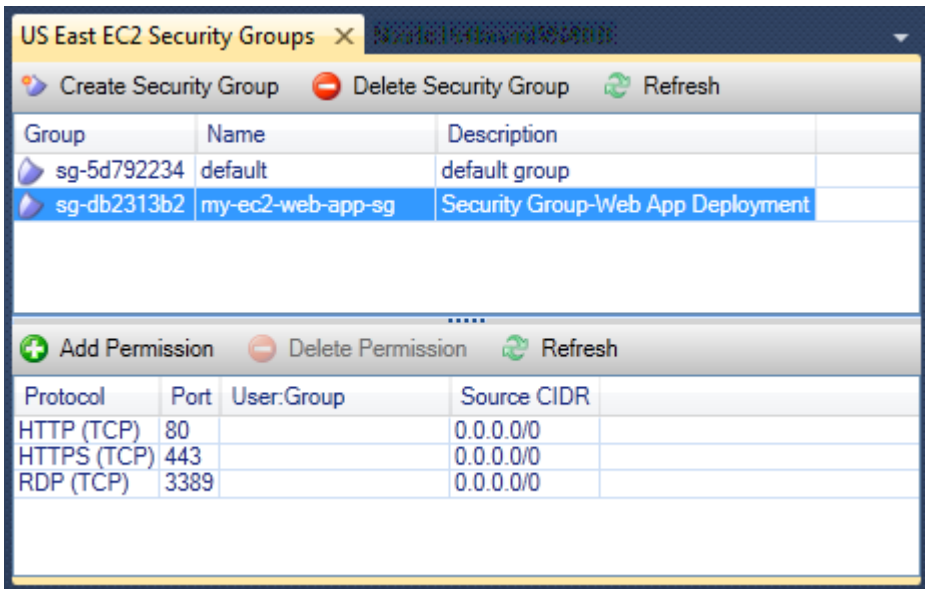
Dans cette section, nous allons ajouter des autorisations au groupe de sécurité pour autoriser le trafic web via les protocoles HTTP et HTTPS. Nous allons également autoriser d'autres ordinateurs de se connecter à l'aide du protocole RDP (Remote Desktop Protocol).

Pour ajouter des autorisations à un groupe de sécurité

1. Dans l'onglet Groupes de sécurité EC2, choisissez un groupe de sécurité, puis choisissez le bouton Ajouter autorisation.
2. Dans la boîte de dialogue Add IP Permission (Ajouter une autorisation IP), choisissez la case d'option Protocol, Port and Network (Protocole, port et réseau), puis dans la liste déroulante Protocole, choisissez HTTP. La plage de ports s'ajuste automatiquement au port 80, le port par défaut pour HTTP. Le champ Source CIDR (CIDR source) est défini par défaut sur 0.0.0.0/0, qui spécifie que le trafic réseau HTTP sera accepté depuis n'importe quelle adresse IP externe. Choisissez OK.



   Ouvrez le port 80 (HTTP) de ce groupe de sécurité
3. Répétez cette procédure pour HTTPS et RDP. Les autorisations de vos groupes de sécurité doivent à présent ressembler à celles-ci.



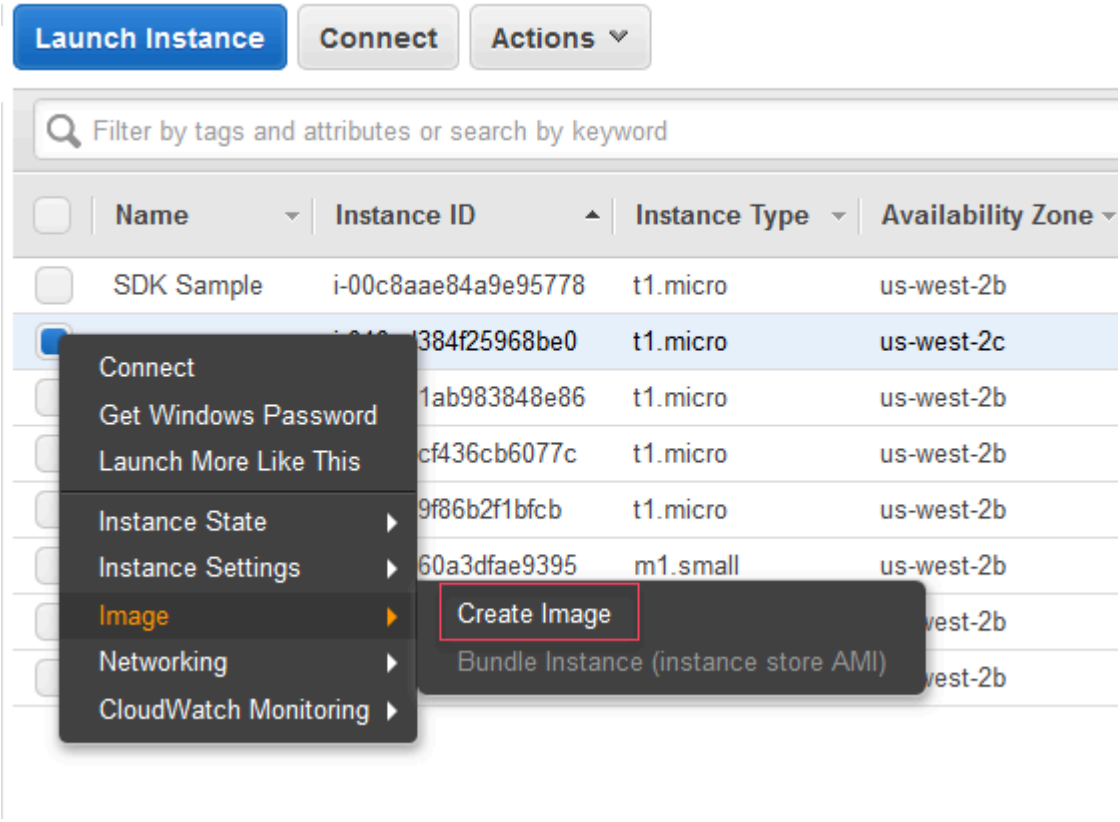
Vous pouvez également définir des autorisations dans le groupe de sécurité en spécifiant un ID utilisateur et un nom de groupe de sécurité. Dans ce cas, les instances Amazon EC2 de ce groupe de sécurité doivent accepter l'ensemble du trafic réseau entrant provenant des instances Amazon EC2 du groupe de sécurité spécifié. Vous devez également spécifier l'ID utilisateur pour désambiguïser le nom du groupe de sécurité. Les noms de groupe de sécurité ne doivent pas obligatoirement être uniques dans l'ensemble des servicesAWS. Pour plus d'informations sur les groupes de sécurité, consultez la documentation EC2.

Créer une AMI à partir d'une instance Amazon EC2

Sur la page Instances Amazon EC2, vous pouvez créer des images machine Amazon (AMI) depuis des instances en cours ou arrêtées. Pour plus d'informations sur les AMI, consultez la rubrique Amazon Machine Images (AMI) dans le Guide de l'utilisateur Amazon Elastic Compute Cloud pour les instances Windows.

Pour créer une AMI à partir d'une instance

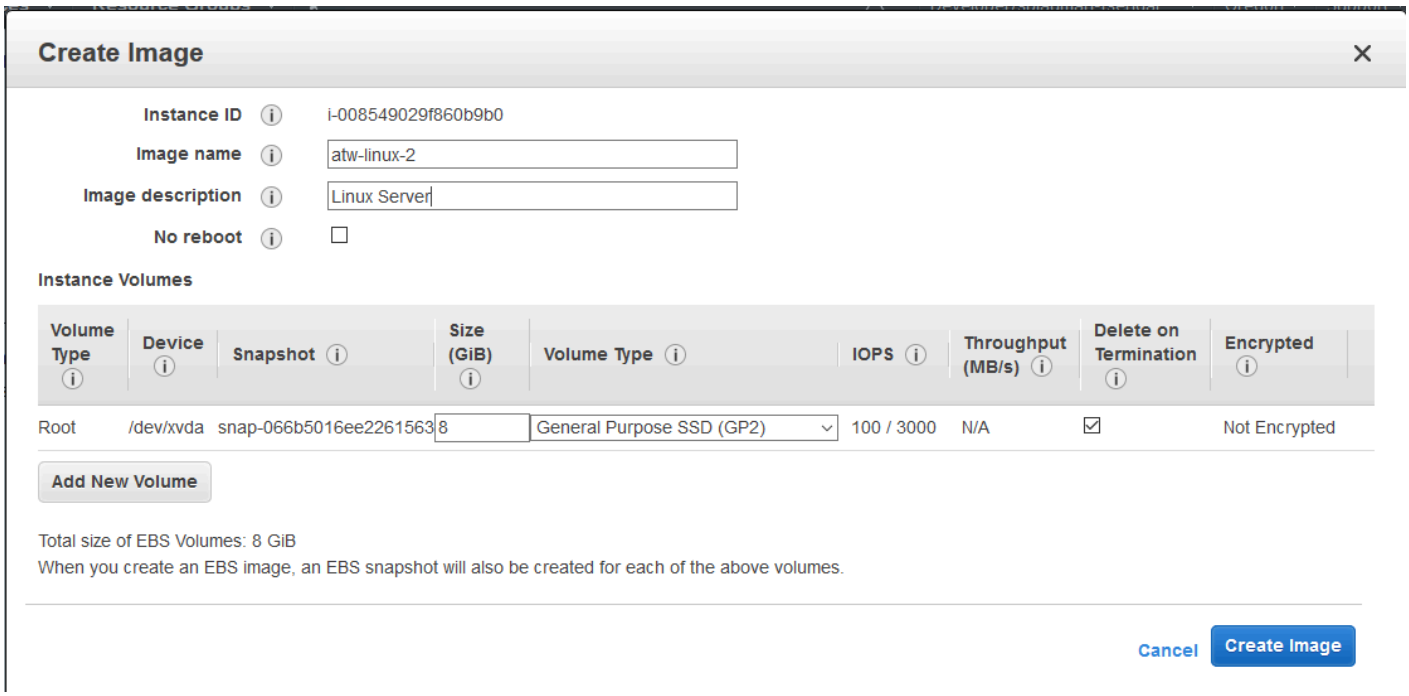
1. Cliquez avec le bouton droit sur l'instance que vous souhaitez utiliser comme base pour votre AMI, et choisissez Créer une image dans le menu contextuel.



Menu contextuel Créer une image

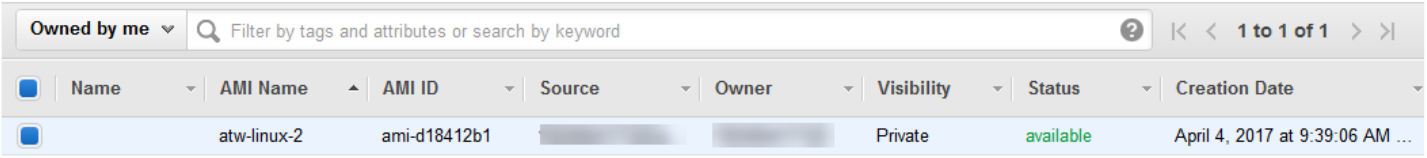
2. Dans la boîte de dialogue Créer une image, saisissez un nom unique et une description, puis choisissez Créer une image. Par défaut, Amazon EC2 met hors tension l'instance, effectue des instantanés de n'importe quel volume attaché, crée et enregistre l'AMI, puis redémarre l'instance. Sélectionnez No reboot si vous ne voulez pas que votre instance soit mise hors tension.

> **Warning**
>
> Si vous sélectionnez No reboot, nous ne pouvons pas garantir l'intégrité du système de fichiers de l'image créée.



Boîte de dialogue Créer une image

La création de l'AMI peut prendre quelques minutes. Une fois créé, il apparaîtra dans la vue AMIs de l'AWSExplorateur. Pour afficher cette vue, double-cliquez sur le nœud Amazon EC2 | AMIs dans l'AWSExplorateur. Pour consulter vos AMI, dans la liste déroulante Afficher, choisissez M'appartenant. Vous devrez peut-être choisir Actualiser pour consulter votre AMI. Lorsque l'AMI s'affiche d'abord, elle peut passer par l'état en attente, mais après quelques instants, elle passe à l'état disponible.



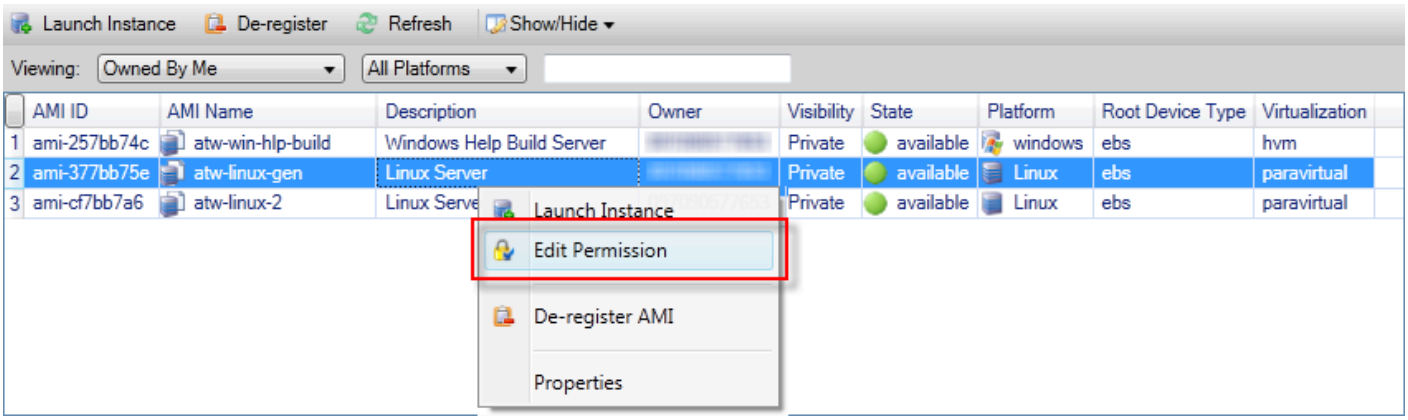
Liste des AMI créées

Définition des autorisations de lancement sur une Amazon Machine Image

Vous pouvez définir des autorisations de lancement sur vos images machine Amazon (AMI) depuis leAMIAfficher dansAWSExplorer. Vous pouvez utiliser la boîte de dialogue Set AMI Permissions (Définir des autorisations d'AMI) pour copier des autorisations à partir d'AMI.

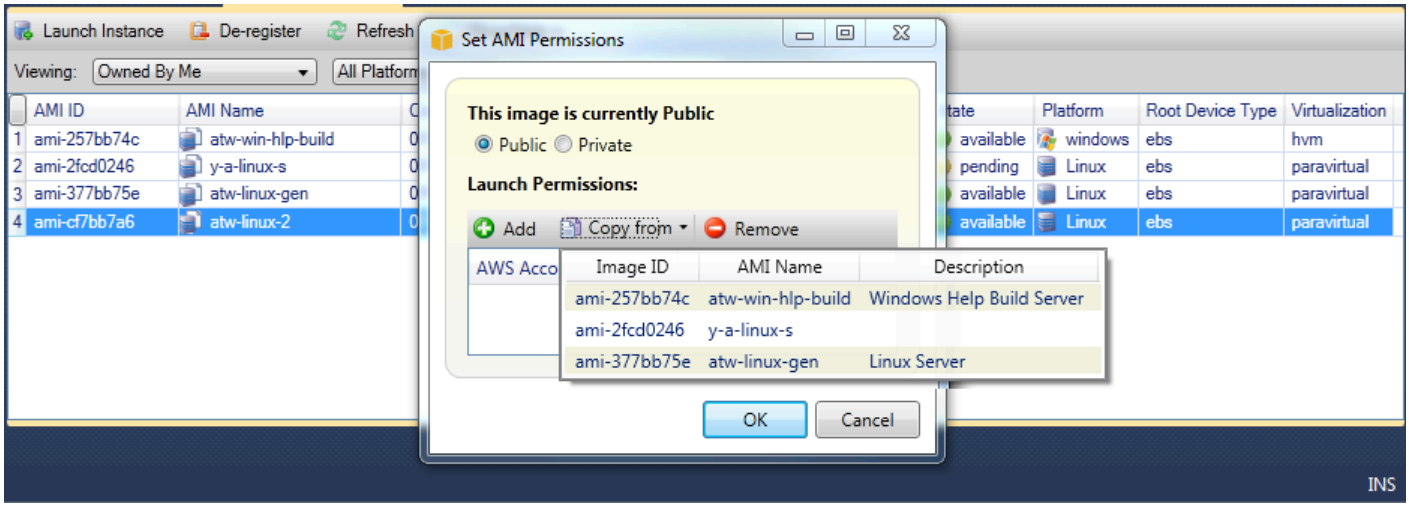
Pour définir des autorisations sur une AMI

1. DansAMIAfficher dansAWSExplorer, ouvrez le menu contextuel (clic droit) sur une AMI, puis choisissezModifier une autorisation.



2. Il existe trois options disponibles dans la boîte de dialogue Set AMI Permissions (Définir des autorisations d'AMI) :
   - Pour accorder une autorisation de lancement, choisissezAddition, et saisissez le numéro de compte duAWSutilisateur auquel vous donnez l'autorisation de lancement.
   - Pour supprimer une autorisation de lancement, choisissez le numéro de compte duAWSutilisateur à qui vous souhaitez retirer une autorisation de lancement, et choisissezSupprimez.
   - Pour copier des autorisations d'une AMI vers une autre, choisissez-en une dans la liste, puis choisissez Copy from (Copier depuis). Les utilisateurs qui disposent d'autorisations de lancement sur l'AMI que vous avez choisie se verront accorder des autorisations de lancement sur l'AMI actuelle. Vous pouvez répéter ce processus avec d'autres AMI dans la liste Copy from (Copier depuis) pour copier des autorisations à partir de plusieurs AMI dans l'AMI cible.

     LeExécution de la commande COcontient uniquement les AMI appartenant au compte qui était actif lorsqueAMIla vue a été affichée depuisAWSExplorer. Par conséquent, la liste Copy from (Copier depuis) peut n'afficher aucune AMI si aucune autre n'appartient au compte actif.



Boîte de dialogue Copy AMI permissions (Copier des autorisations d'AMI)

Amazon Virtual Private Cloud (VPC)

Amazon Virtual Private Cloud (Amazon VPC) vous permet de lancer des ressources Amazon Web Services (Amazon Web Services) dans un réseau virtuel défini par vos soins. Ce réseau virtuel ressemble beaucoup à un réseau traditionnel que vous pourriez exécuter dans votre propre data center, et présente l'avantage d'utiliser l'infrastructure évolutive deAWS. Pour plus d'informations, consultez le Guide de l'utilisateur Amazon VPC.

Toolkit for Visual Studio permet à un développeur d'accéder à des fonctionnalités VPC similaires à celles exposées par leAWS Management Consolemais depuis l'environnement de développement Visual Studio. LeAmazon VPCNœud deAWSExplorer inclut des sous-nœuds pour les domaines suivants.

- VPC
- Sous-réseaux
- Adresses IP Elastic
- Passerelles Internet
- Listes ACL réseau
- Tables de routage
- Groupes de sécurité

Création d'un VPC public-privé pour le déploiement avecAWS Elastic Beanstalk

Cette section décrit comment créer un VPC Amazon qui contient à la fois des sous-réseaux publics et privés. Le sous-réseau public contient une instance Amazon EC2 qui exécute une NAT (Network Address Translation, traduction d'adresses réseau) pour permettre aux instances du sous-réseau privé de communiquer avec le sous-réseau public. Les deux sous-réseaux doivent résider dans la même zone de disponibilité (AZ).

Cette configuration est la configuration de VPC minimale requise pour déployer un environnement AWS Elastic Beanstalk dans un VPC. Dans ce scénario, les instances Amazon EC2 qui hébergent votre application résident dans le sous-réseau privé. L'équilibreur de charge Elastic Load Balancing qui achemine le trafic entrant vers votre application réside dans le sous-réseau public.

Pour plus d'informations sur la traduction d'adresses réseau (NAT), consultez NAT Instances (Instances NAT) dans le Guide de l'utilisateur Amazon Virtual Private Cloud. Pour obtenir un exemple de la manière de configurer votre déploiement pour utiliser un VPC, consultez Déploiement dans Elastic Beanstalk.

Pour créer un sous-réseau public-privé VPC

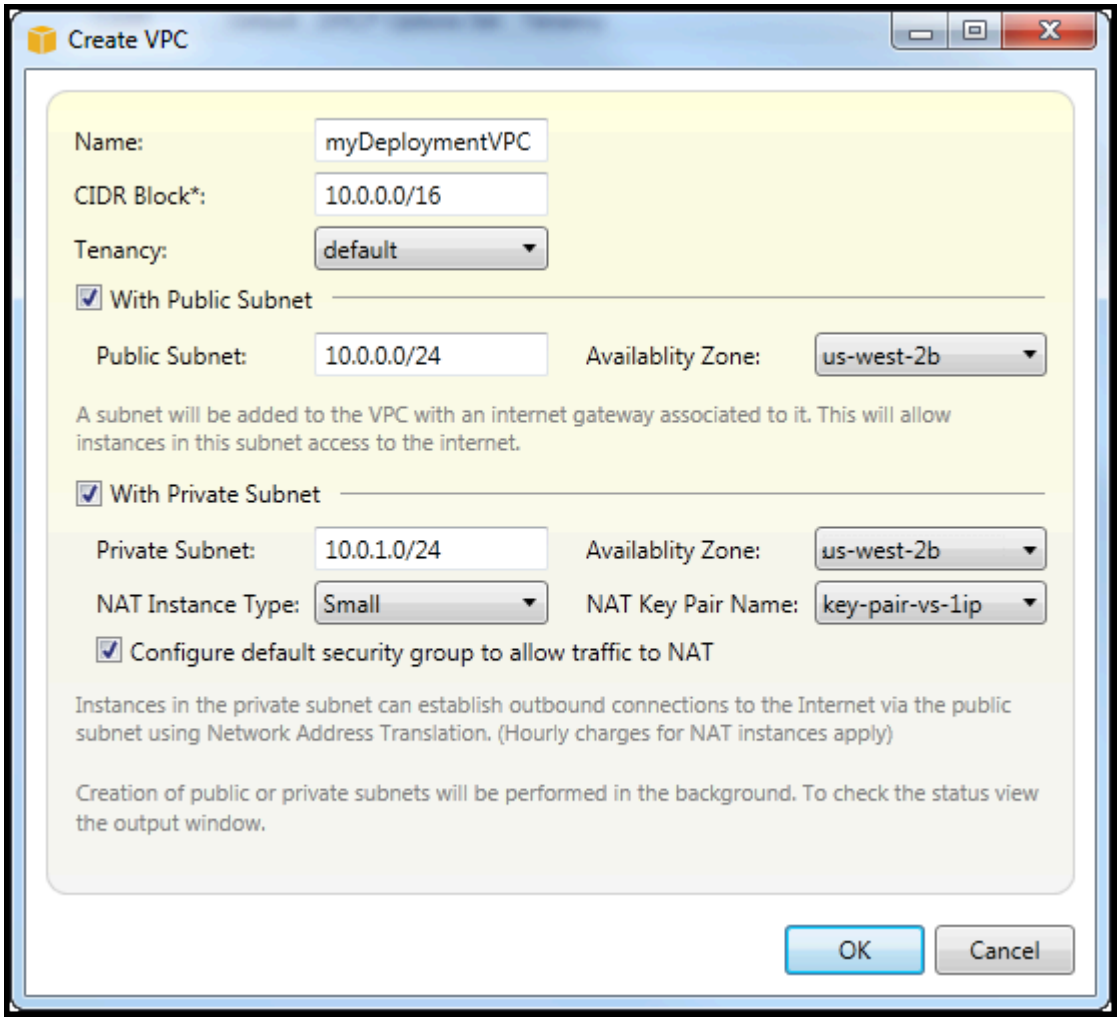
1. DansAmazon VPCNœud dansAWSExplorer, ouvrez leVPC, puis, choisissezCréation d'un VPC.

2. Configurez le VPC en procédant comme suit :
   - Indiquez un nom pour votre VPC.
   - Cochez les cases With Public Subnet (Avec un sous-réseau public) et With Private Subnet (Avec un sous-réseau privé).

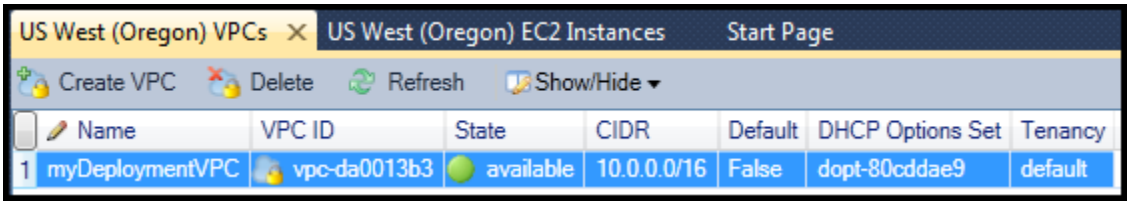
- Dans la zone de liste déroulante Zone de disponibilité pour chaque sous-réseau, choisissez une zone de disponibilité. Veillez à utiliser la même zone de disponibilité pour les deux sous-réseaux.
- Pour le sous-réseau privé, indiquez une paire de clés dans NAT Key Pair Name (Nom de la paire de clés NAT). Cette key pair est utilisée pour l'instance Amazon EC2 qui exécute la traduction des adresses réseau du sous-réseau privé en adresses réseau de l'Internet public.
- Cochez la case Configure default security group to allow traffic to NAT (Configurer un groupe de sécurité par défaut pour autoriser le trafic vers NAT).

Indiquez un nom pour votre VPC. Cochez les cases With Public Subnet (Avec un sous-réseau public) et With Private Subnet (Avec un sous-réseau privé). Dans la zone de liste déroulante Zone de disponibilité pour chaque sous-réseau, choisissez une zone de disponibilité. Veillez à utiliser la même zone de disponibilité pour les deux sous-réseaux. Pour le sous-réseau privé, indiquez une paire de clés dans NAT Key Pair Name (Nom de la paire de clés NAT). Cette key pair est utilisée pour l'instance Amazon EC2 qui exécute la traduction des adresses réseau du sous-réseau privé en adresses réseau de l'Internet public. Cochez la case Configure default security group to allow traffic to NAT (Configurer un groupe de sécurité par défaut pour autoriser le trafic vers NAT).

Choisissez OK.

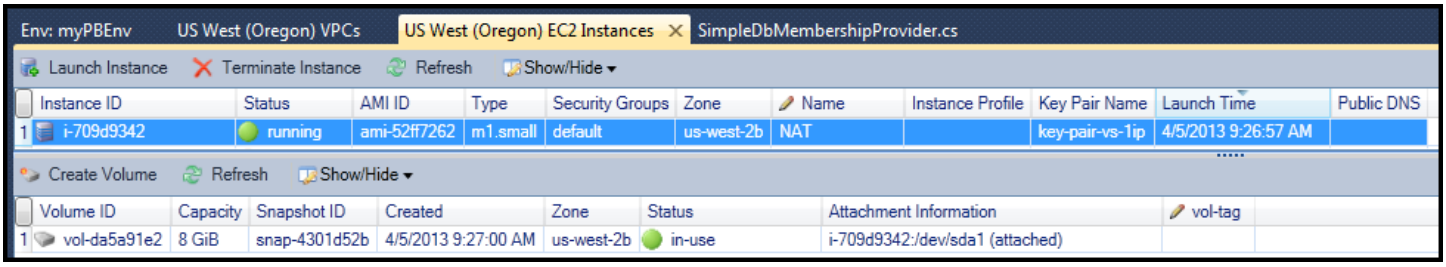


Vous pouvez afficher le nouveau VPC dans le manuelVPCOnglet dansAWSExplorer.



Le lancement de l'instance NAT peut prendre quelques minutes. Lorsqu'elle est disponible, vous pouvez l'afficher en développant le manuelAmazon EC2Nœud dansAWSExplorateur, puis ouvrez leInstancessous-nœud.

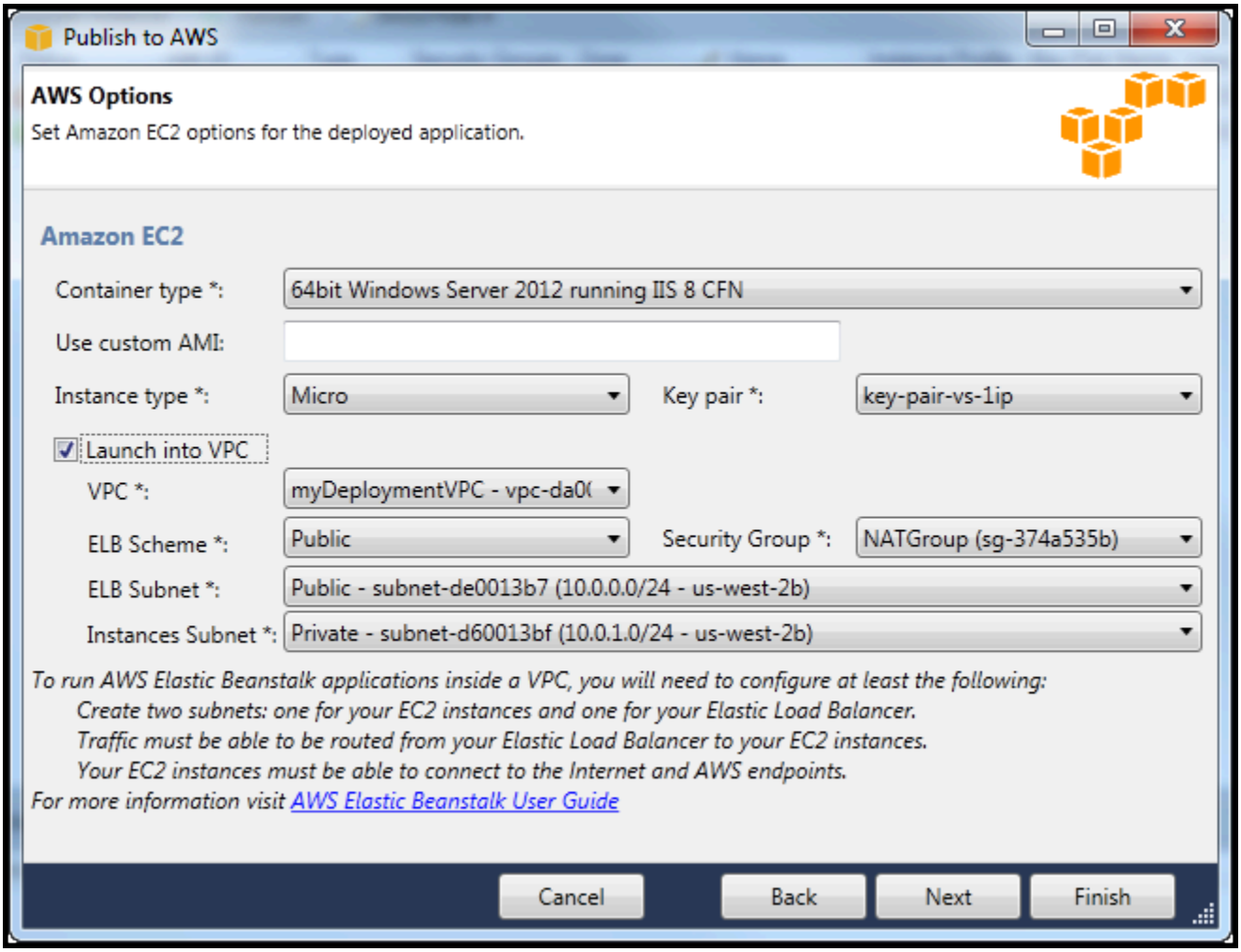
UnAWS Elastic BeanstalkLe volume (Amazon EBS) est créé automatiquement pour l'instance NAT. Pour plus d'informations sur Elastic Beanstalk, accédez au manuelAWS Elastic Beanstalk(EBS)dans leGuide de l'utilisateur Amazon EC2 pour les instances Linux.



Si vousdéployer une application sur unAWS Elastic Beanstalkenvironnementet choisissez de lancer l'environnement dans un VPC, la boîte à outils remplit lePublier dansAmazon Web Servicescontenant les informations de configuration de votre VPC.

Toolkit ne renseigne la boîte de dialogue avec les informations qu'à partir des VPC qui ont été créés dans Toolkit et pas à partir de ceux qui ont été créés à l'aide du manuelAWS Management Console. Cela provient du fait que lorsque la boîte à outils crée un VPC, elle étiquète les composants du VPC de façon à pouvoir accéder à leurs informations.

La capture d'écran suivante de l'assistant de déploiement montre un exemple de boîte de dialogue renseignée avec les valeurs issues d'un VPC créé dans la boîte à outils.



Pour supprimer un VPC

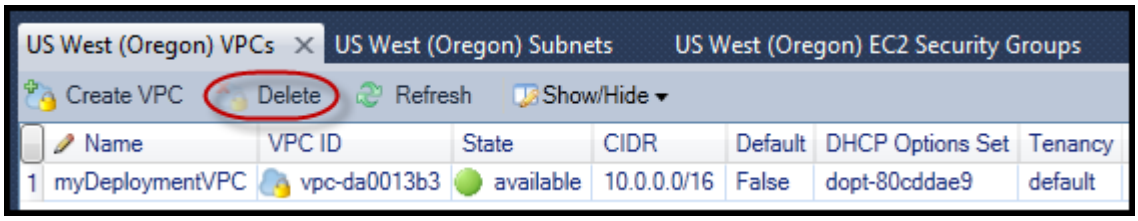
Pour supprimer le VPC, vous devez commencer par suspendre les instances Amazon EC2 du VPC.

1. Si vous avez déployé une application dans un environnement AWS Elastic Beanstalk du VPC, supprimez cet environnement. Ainsi, les instances Amazon EC2 hébergeant votre application seront supprimées, ainsi que l'équilibreur de charge Elastic Load Balancing.

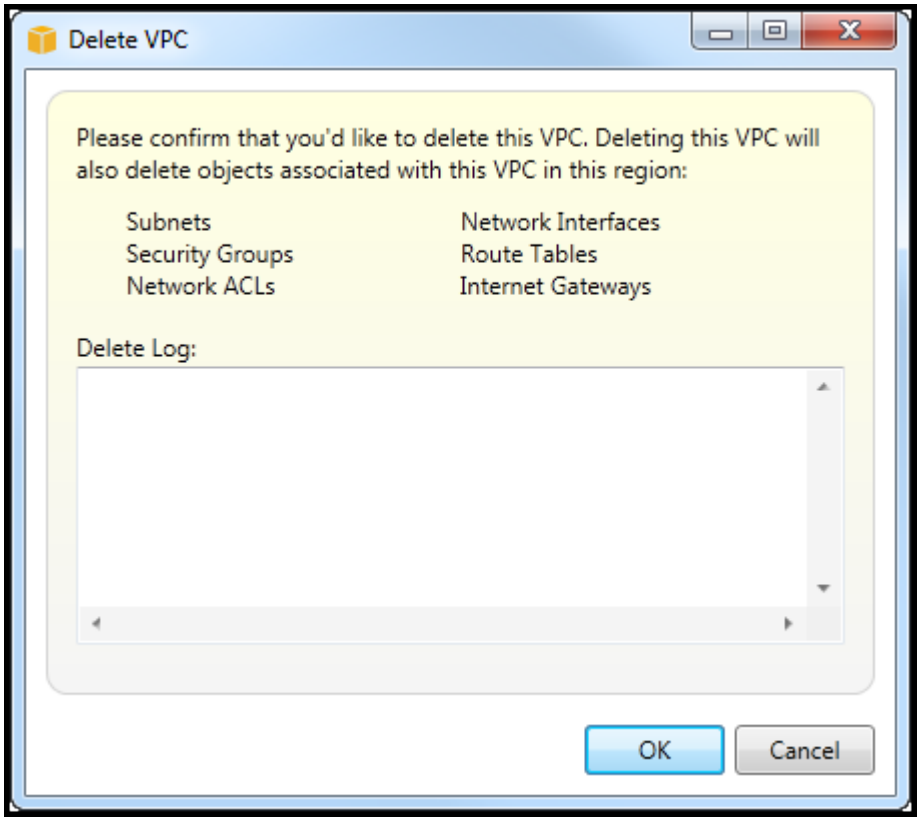
   Si vous essayez de suspendre directement les instances hébergeant votre application sans supprimer l'environnement, le service Auto Scaling créera automatiquement de nouvelles instances pour remplacer les instances supprimées. Pour plus d'informations, accédez au Manuel du développeur Auto Scaling.
2. Supprimez l'instance NAT du VPC.

Pour supprimer le VPC, vous n'avez pas besoin de supprimer le volume Amazon EBS associé à l'instance NAT. Cependant, si vous ne supprimez pas le volume, vous continuerez à être facturé même si vous avez supprimé l'instance NAT et le VPC.

3. Dans l'onglet VPC, choisissez le lien Supprimer pour supprimer le VPC.



4. Dans la boîte de dialogue Delete VPC (Supprimer le VPC), choisissez OK.



Utilisation de l'éditeur de AWS CloudFormation modèles pour Visual Studio

Le Toolkit for Visual Studio inclut un éditeur de AWS CloudFormation AWS CloudFormation modèles et des projets de modèles pour Visual Studio. Les fonctionnalités prises en charge sont les suivantes :

- Création de nouveaux modèles (vides ou copiés à partir d'une pile existante ou d'un exemple de modèle) à l'aide du type de projet AWS CloudFormation modèle fourni.
- Modification de modèles avec validation JSON automatique, saisie semi-automatique, pliage de code et mise en évidence de la syntaxe.
- Suggestion automatique des fonctions intrinsèques et des paramètres de référence des ressources pour les valeurs de champ de votre modèle.
- Éléments de menu permettant d'effectuer des actions courantes pour votre modèle à partir de Visual Studio.

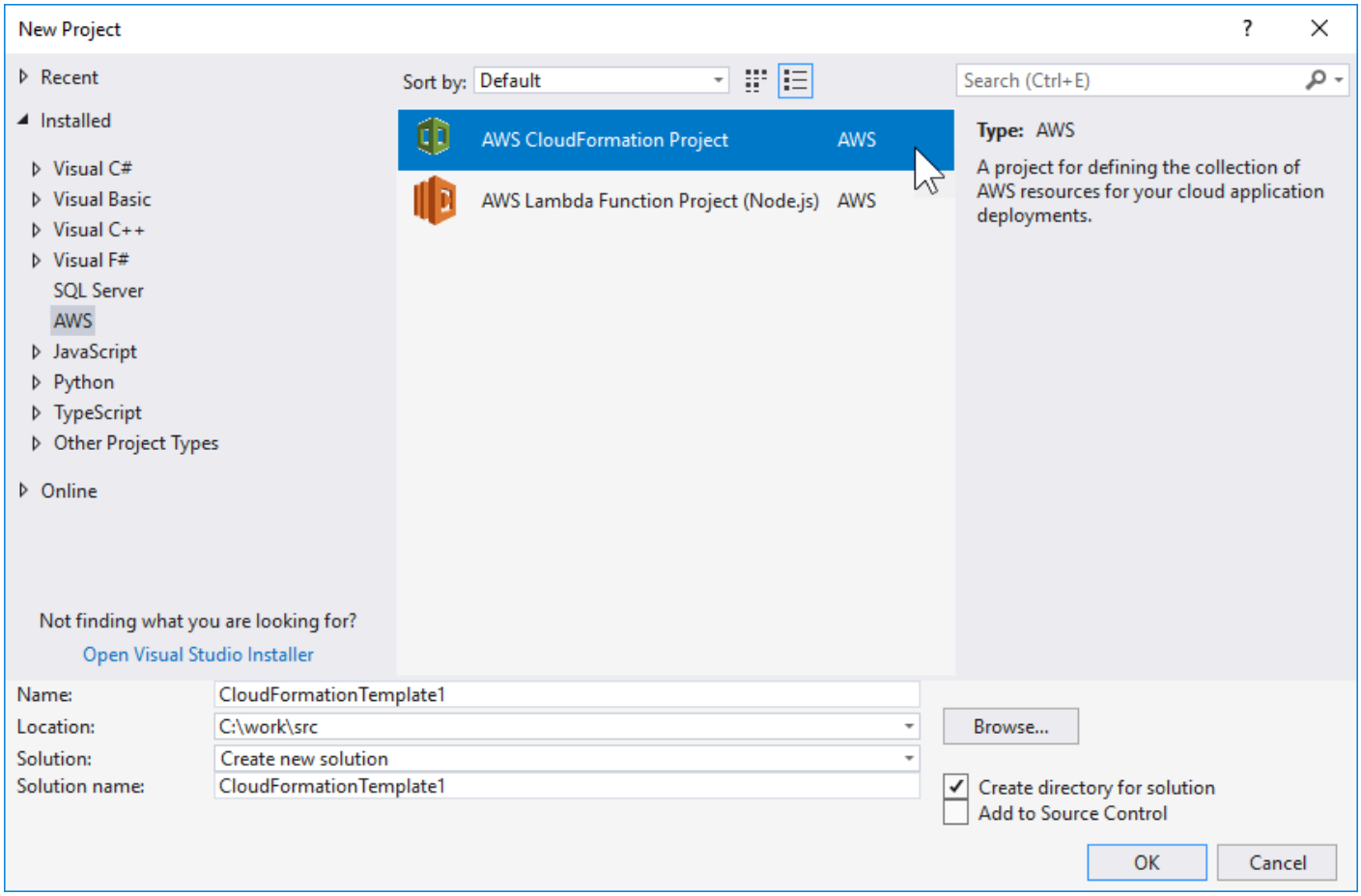
Rubriques

Création d'un projet de modèle AWS CloudFormation dans Visual Studio

Pour créer un projet de modèle

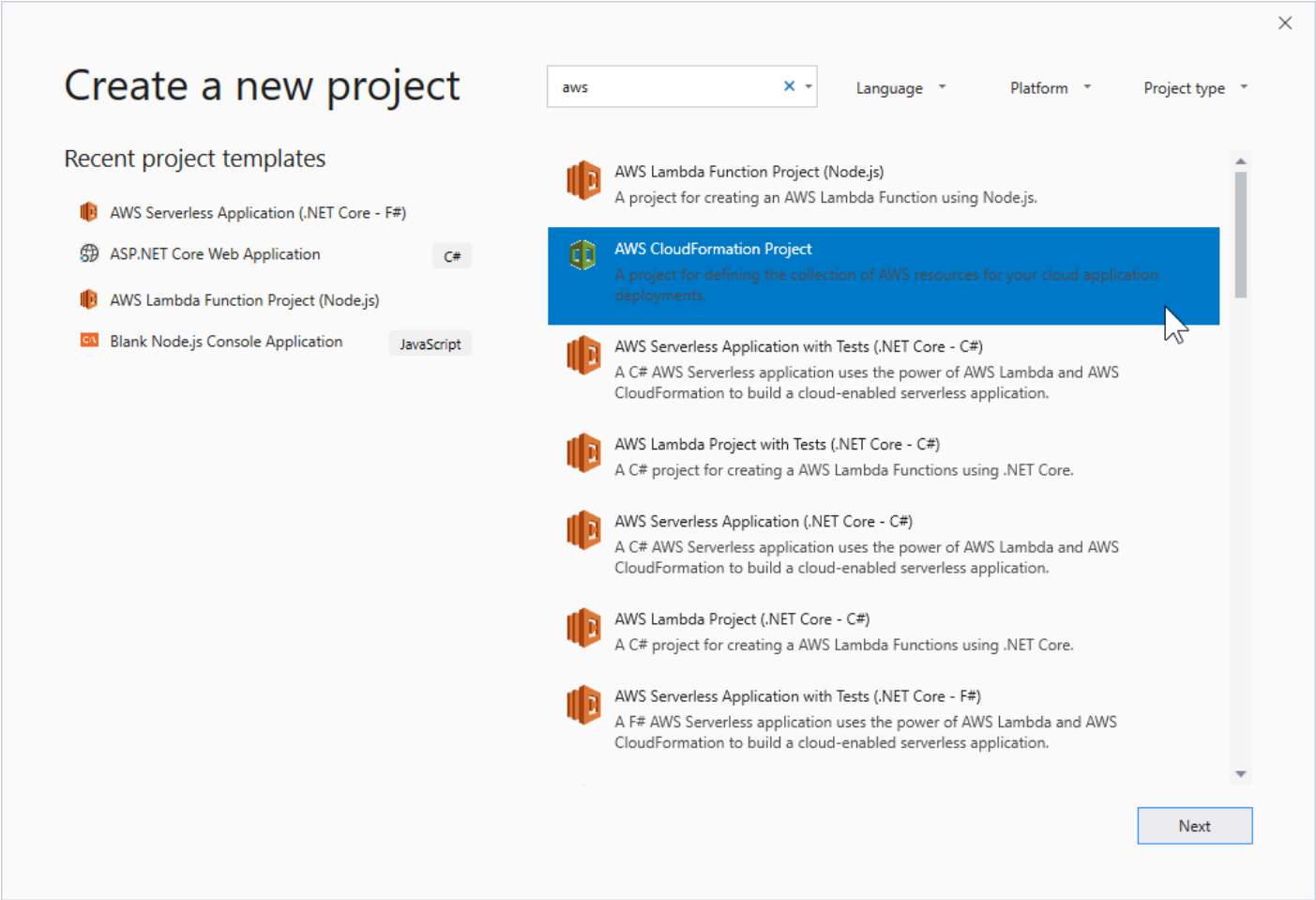
1. Dans Visual Studio, choisissez Fichier, choisissez Nouveau, puis choisissez Projet.
2. Pour Visual Studio 2017 :

   DansNouveau projetboîte de dialogue, développezInstallation deet sélectionnezAWS.



Pour Visual Studio 2019 :

Dans la boîte de dialogue New Project (Nouveau projet) assurez-vous que les listes déroulantes Language (Langue), Platform (Plateforme), et Project type (Type de projet) sont définies sur « Tous... » et tapez aws dans le champ Search (Rechercher).



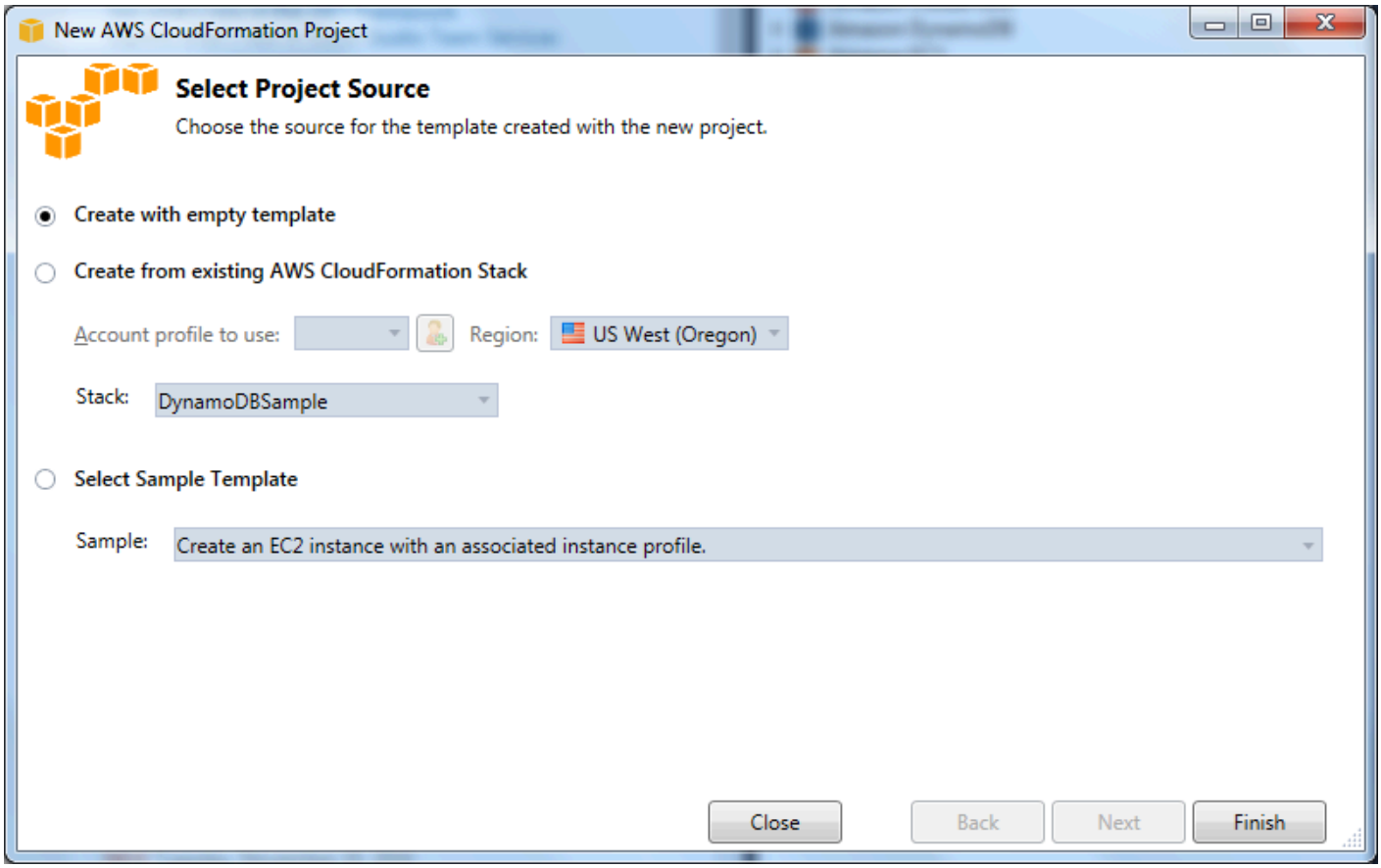
3. Select theAWSProjet CloudFormationmodèle.
4. Pour Visual Studio 2017 :

   Saisissez le Name (Nom), Location (Emplacement), etc. souhaités de votre projet de modèle, puis cliquez sur OK.

   Pour Visual Studio 2019 :

   Cliquez sur Next (Suivant). Dans la boîte de dialogue suivante, saisissez le Name (Nom), Location (Emplacement), etc. de votre projet de modèle, puis cliquez sur Create (Créer).
5. Sur la page Select Project Source (Sélectionner la source du projet), choisissez la source du modèle que vous allez créer :
   - Create with empty template (Créer avec un modèle vide) génère un nouveau modèle AWS CloudFormation vide.
   - Création à partir d'une créationAWS|CFN| pilegénère un modèle à partir d'une pile existante dans votreAWS. (La pile n'a pas besoin d'avoir un état `CREATE_COMPLETE`.)

- Select sample template (Sélectionner un exemple de modèle) génère un modèle à partir de l'un des exemples de modèles AWS CloudFormation.

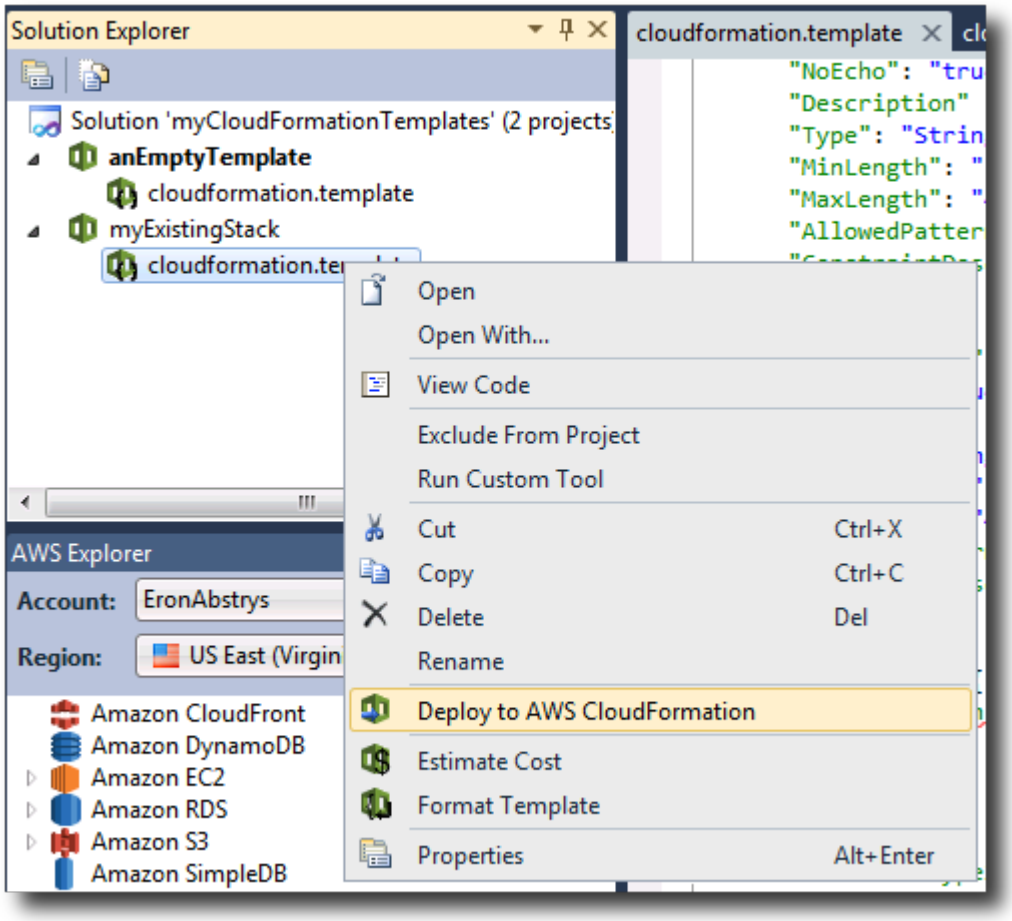


6. Pour finaliser la création de votre projet de modèle AWS CloudFormation, choisissez Terminer.

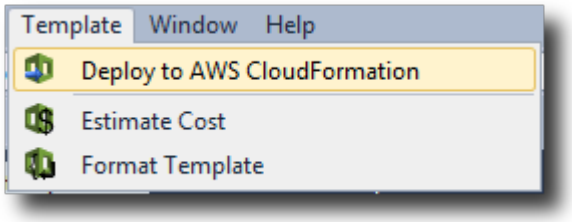
Déploiement d'un modèle AWS CloudFormation dans Visual Studio

Pour déployer un modèle CFN

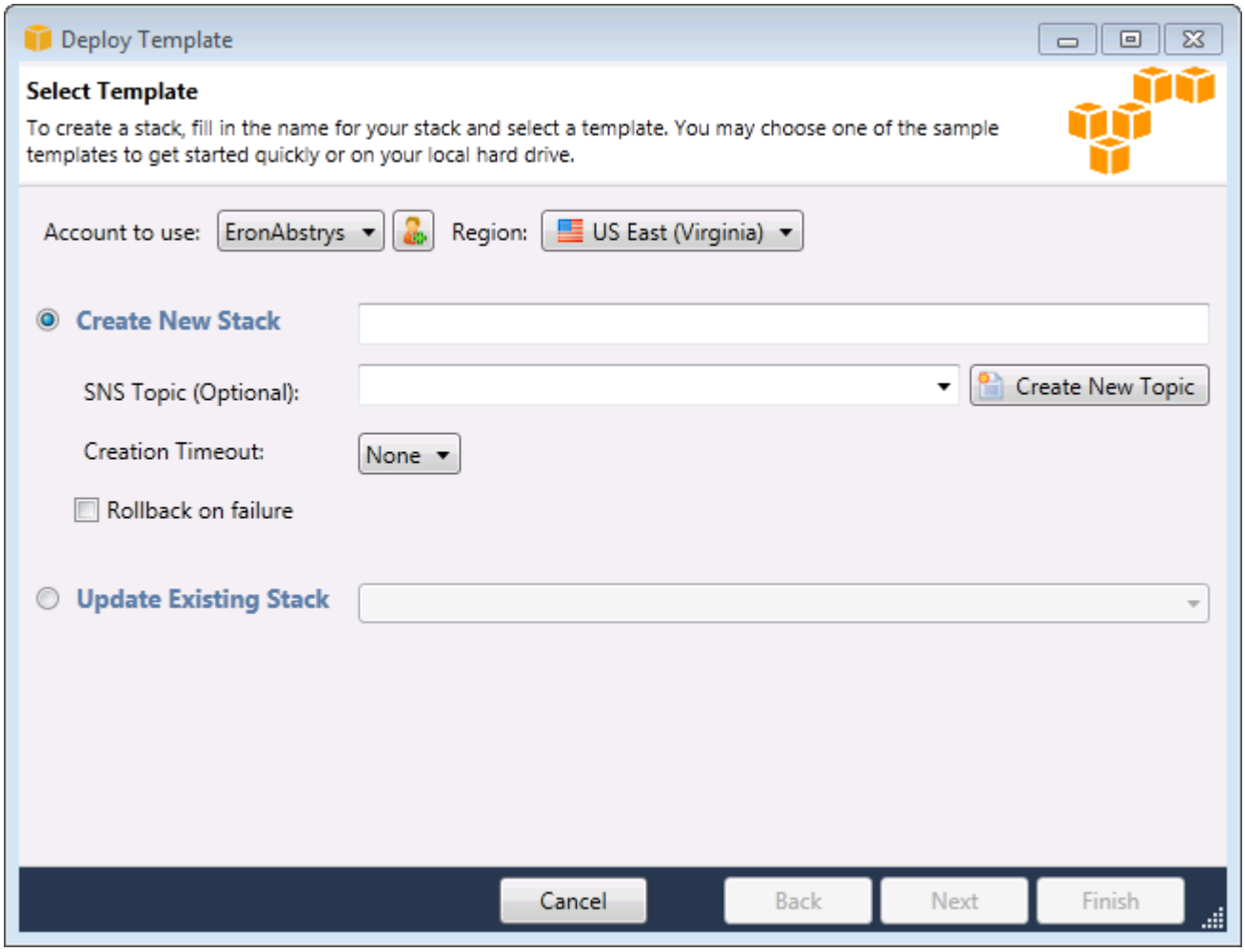
1. Dans l'Explorateur de solutions, ouvrez le menu contextuel du modèle à déployer en cliquant avec le bouton droit de la souris, puis choisissezDéploiement surAWS CloudFormation.



Vous pouvez également déployer le modèle que vous êtes sur le point de modifier en choisissant leTemplate (Modèle), choisissezDéploiement surAWS CloudFormation.



2. Dans la pageModèle de déploiement, choisissez la pageCompte AWSà utiliser pour lancer la pile et la région où la pile sera lancée.

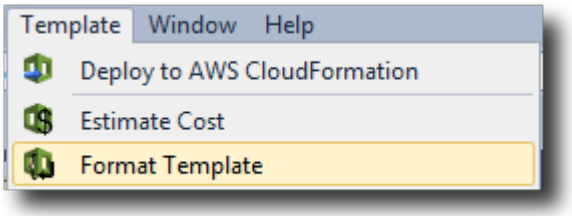


3. Cliquez sur Créer une nouvelle pile et tapez un nom pour votre pile.
4. Choisissez une ou aucune des options suivantes :
   - Pour recevoir des notifications sur la progression de la pile, choisissez une rubrique SNS dans la liste déroulante Rubrique SNS. Vous pouvez également créer une rubrique SNS en choisissant Créer une rubrique et en tapant une adresse e-mail dans la zone.
   - Utilisez Creation Timeout (Délai de création) pour spécifier le délai pendant lequel AWS CloudFormation doit attendre que la pile soit créée avant que l'échec de création de la pile ne soit déclaré, (et que la pile soit annulée, sauf si l'option Restauration en cas d'échec est décochée).
   - Utilisez Restauration en cas d'échec si vous voulez que la pile s'annule (c'est-à-dire se supprime) en cas d'échec. Ne cochez pas cette option si vous voulez que la pile reste active en vue du débogage même si son lancement a échoué.
5. Choisissez Terminer pour lancer la pile.

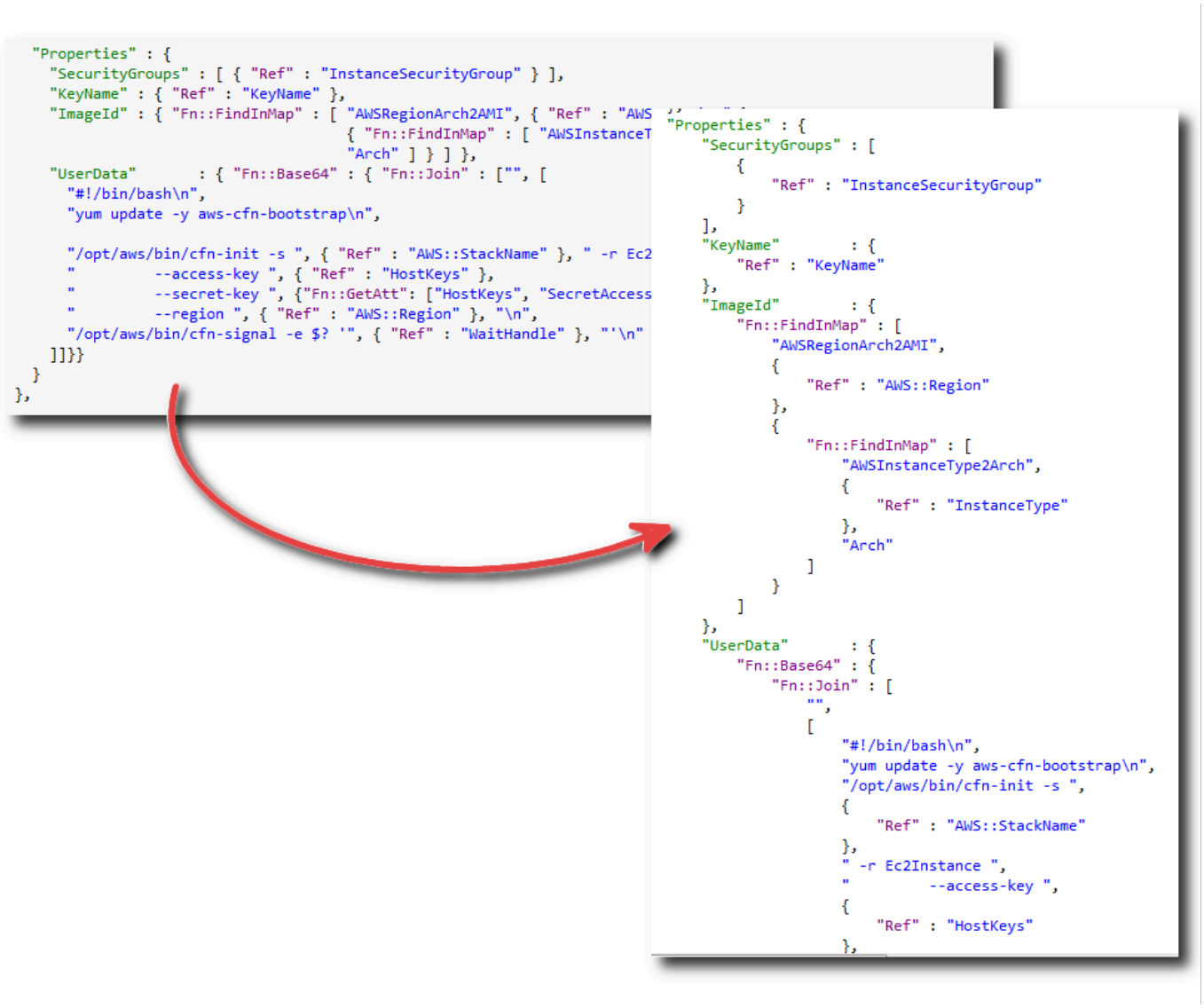
Formatage d'un modèle AWS CloudFormation dans Visual Studio

- Dans Solution Explorer, ouvrez le menu contextuel du modèle en cliquant sur le bouton droit de la souris et choisissez Format Template (Formater un modèle).

  Vous pouvez également formater le modèle que vous êtes sur le point de modifier en choisissant Format Template dans le menu Modèles.

  Votre code JSON est formaté de manière à présenter clairement sa structure.



Utilisation d'Amazon S3 dansAWSExplorateur

Amazon Simple Storage Service (Amazon S3) vous permet de stocker et d'extraire des données depuis n'importe quelle connexion à Internet. Toutes les données que vous stockez sur Amazon S3 sont associées à votre compte et, par défaut, sont uniquement accessibles par vous. Toolkit for Visual Studio vous permet de stocker des données sur Amazon S3 et d'afficher, de gérer, d'extraire et de distribuer ces données.

Amazon S3 utilise le concept de compartiments, lesquels peuvent être considérés comme similaires aux systèmes de fichiers ou aux lecteurs logiques. Les compartiments peuvent contenir des dossiers, qui sont semblables aux répertoires et aux objets, lesquels sont similaires aux fichiers. Dans cette

section, nous allons utiliser ces concepts en parcourant les fonctionnalités Amazon S3 exposées par Toolkit for Visual Studio.

> **Note**
>
> Pour utiliser cet outil, votre stratégie IAM doit accorder des autorisations pour le modules`s3:GetBucketAcl`,`s3:GetBucket`, et`s3:ListBucket`actions. Pour de plus amples informations, veuillez consulterPrésentation d'AWSStratégies IAM.

Création d’un compartiment Amazon S3

Dans Amazon S3, le compartiment est l'unité de stockage la plus fondamentale.

Pour créer un compartiment S3

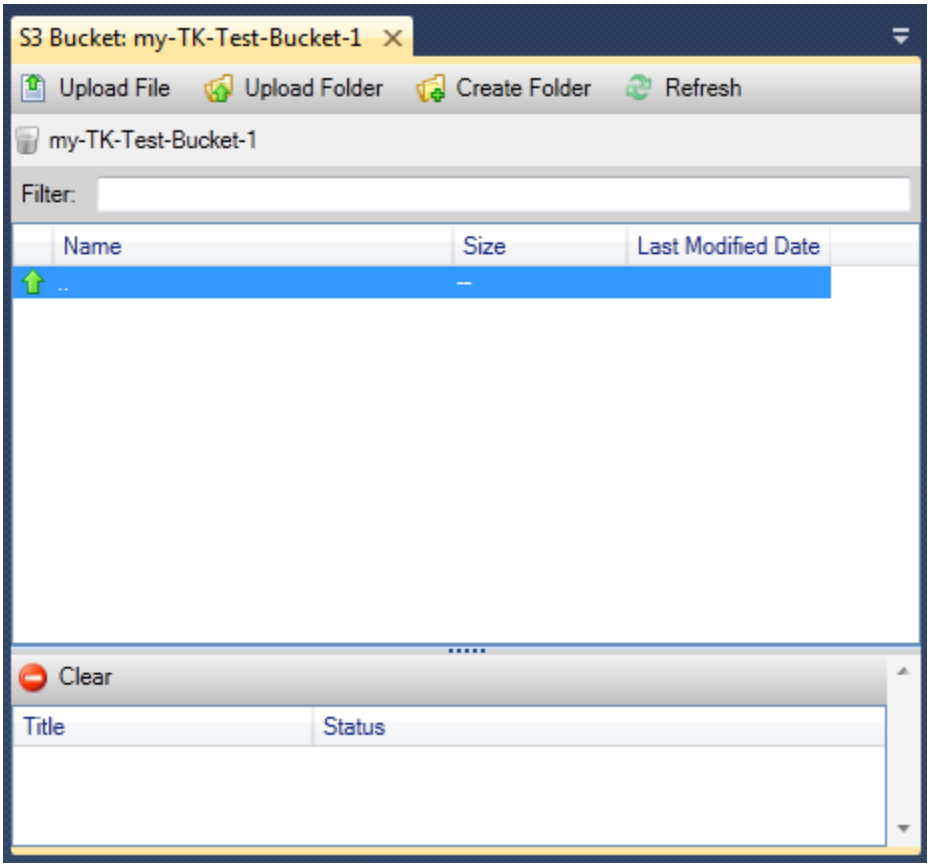
1. DansAWSOuvrez le menu contextuel en cliquant avec le bouton droit de la souris sur le bouton droit de la sourisAmazon S3noeud, puis choisissezcréer un compartiment.
2. Dans la boîte de dialogue Créer un compartiment, tapez un nom pour le compartiment. Les noms de compartiment doivent être uniques dansAWS. Pour plus d'informations sur les autres contraintes, consultez la documentation Amazon S3.
3. Choisissez OK.

Gestion des compartiments Amazon S3 à partir deAWSExplorateur

DansAWSExplorer, les opérations suivantes sont disponibles lorsque vous cliquez avec le bouton droit de la souris sur un compartiment Amazon S3 pour ouvrir un menu contextuel.

Parcourir

Permet de visualiser les objets contenus dans le compartiment. À partir d'ici, vous pouvez créer des dossiers ou charger des fichiers ou des répertoires et dossiers entiers à partir de votre ordinateur local. Le volet inférieur affiche les messages d'état concernant le processus de chargement. Pour effacer ces messages, choisissez l'icône Effacer. Vous pouvez également accéder à cette vue du compartiment en double-cliquant sur le nom du compartiment dansAWSExplorer.



Propriétés

Affiche une boîte de dialogue dans laquelle vous pouvez effectuer les actions suivantes :

- Définir les autorisations Amazon S3 qui couvrent :
  - vous en tant que propriétaire du compartiment.
  - tous les utilisateurs qui ont été authentifiés surAWS.
  - toute personne ayant un accès à Internet.
- Activer la journalisation pour le compartiment.
- Configurer une notification à l'aide d'Amazon Simple Notification Service (Amazon SNS), pour que vous soyez informé en cas de perte de données si vous utilisez le stockage à redondance réduite (RRS). RRS est une option de stockage Amazon S3 qui offre moins de durabilité que le stockage standard, mais à moindre coût. Pour plus d'informations, consultez FAQ sur S3.
- Créer un site web statique avec les données du compartiment.

Stratégie

Vous permet de configurer des stratégies AWS Identity and Access Management (IAM) pour votre compartiment. Pour plus d'informations, consultez la Documentation IAM et les cas d'utilisation pour IAM et S3.

Create Pre-Signed URL (Créer une URL pré-signée)

Vous permet de générer une URL limitée dans le temps que vous pouvez distribuer pour fournir l'accès au contenu du compartiment. Pour plus d'informations, consultez Comment créer une URL pré-signée.

View Multi-Part Uploads (Afficher des chargements partitionnés)

Vous permet d'afficher vos chargements partitionnés. Amazon S3 prend en charge la division des objets volumineux en plusieurs parties pour améliorer l'efficacité du processus de chargement. Pour plus d'informations, accédez à la présentation des chargements partitionnés dans la documentation S3.

Suppression

Permet de supprimer le compartiment. Vous ne pouvez supprimer que des compartiments vides.

Chargement de fichiers et de dossiers sur Amazon S3

Vous pouvez utiliserAWSExplorer pour transférer des fichiers ou des dossiers entiers à partir de votre ordinateur local vers un de vos compartiments.

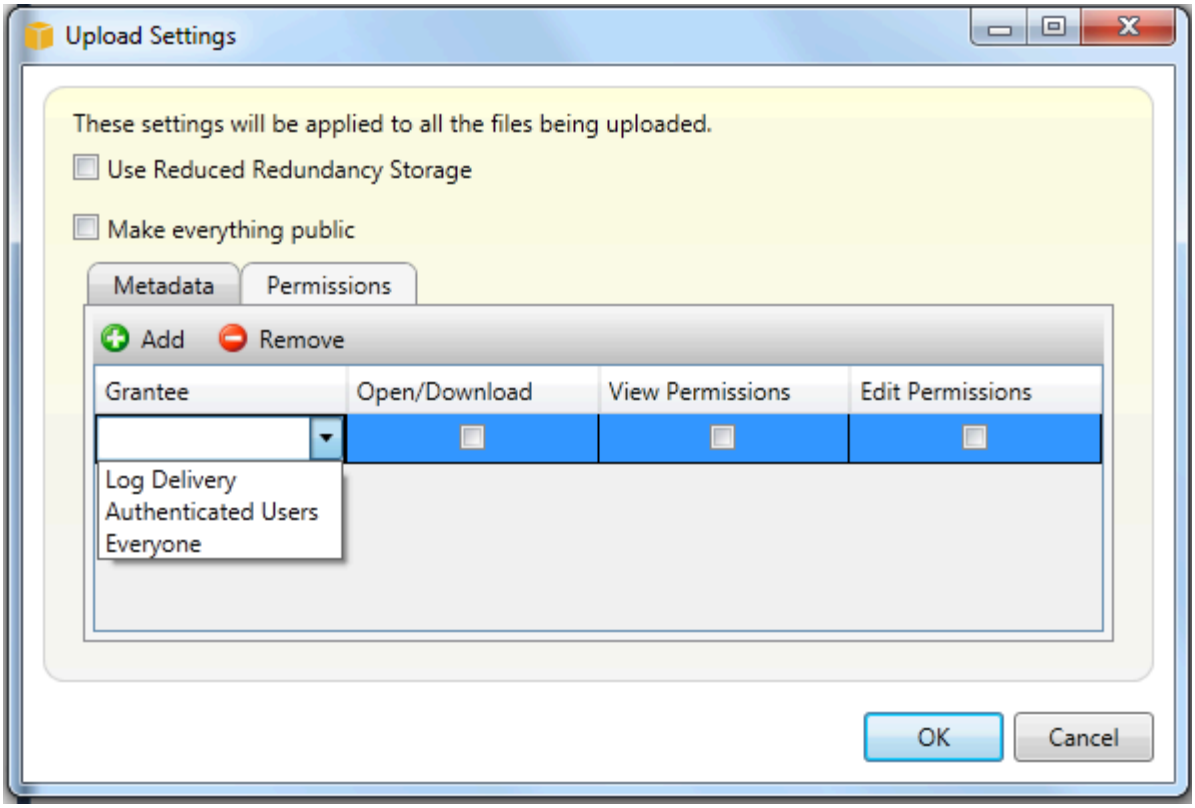
> **Note**
>
> Si vous chargez des fichiers ou des dossiers ayant le même nom que des fichiers ou des dossiers déjà présents dans le compartiment Amazon S3, vos fichiers chargés remplacent les fichiers existants sans avertissement.

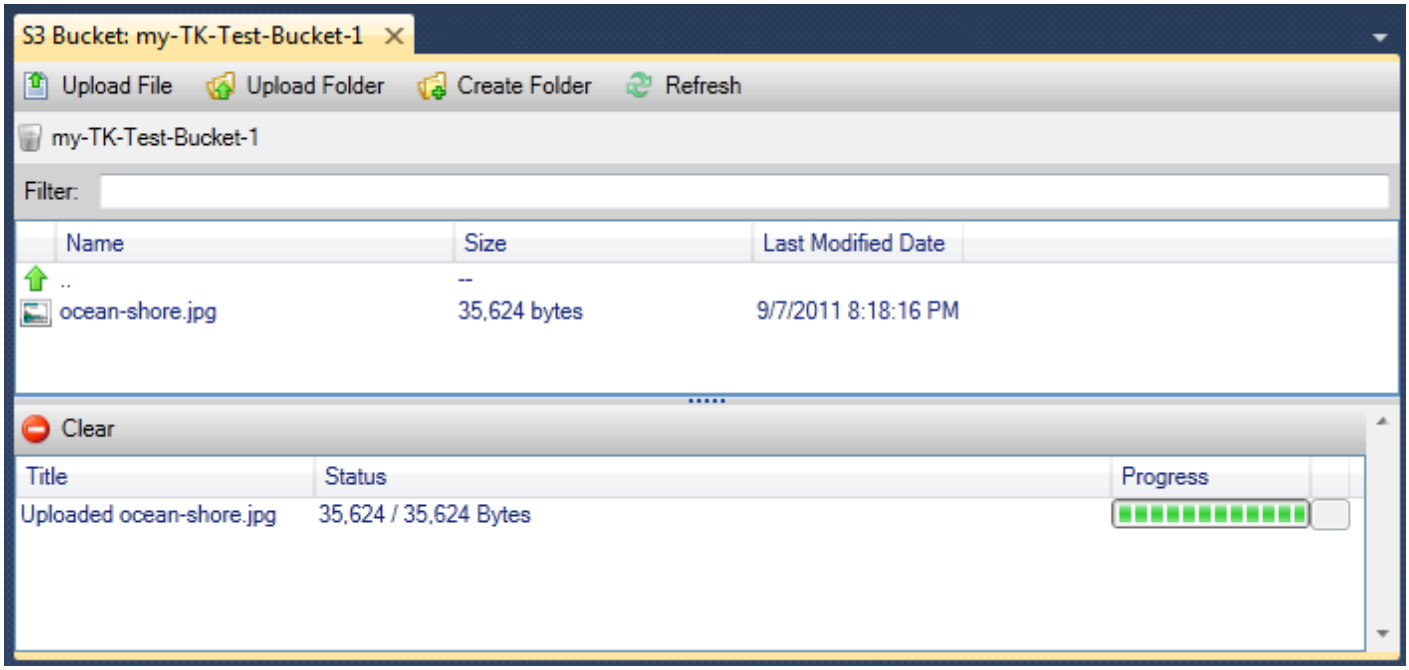
Pour charger un fichier dans S3

1. DansAWSExplorer, développez leAmazon S3, puis double-cliquez sur un compartiment ou bien ouvrez le menu contextuel en cliquant avec le bouton droit de la souris sur un compartiment et choisissezParcourir.
2. Dans la vue Parcourir de votre compartiment, choisissez Charger le fichier ou Upload Folder (Charger le dossier).

3. Dans la boîte de dialogue File-Open (Fichier-ouvrir), recherchez les fichiers à charger, sélectionnez-les, puis cliquez sur Ouvrir. Si vous chargez un dossier, recherchez-le, sélectionnez-le, puis cliquez sur Ouvrir.

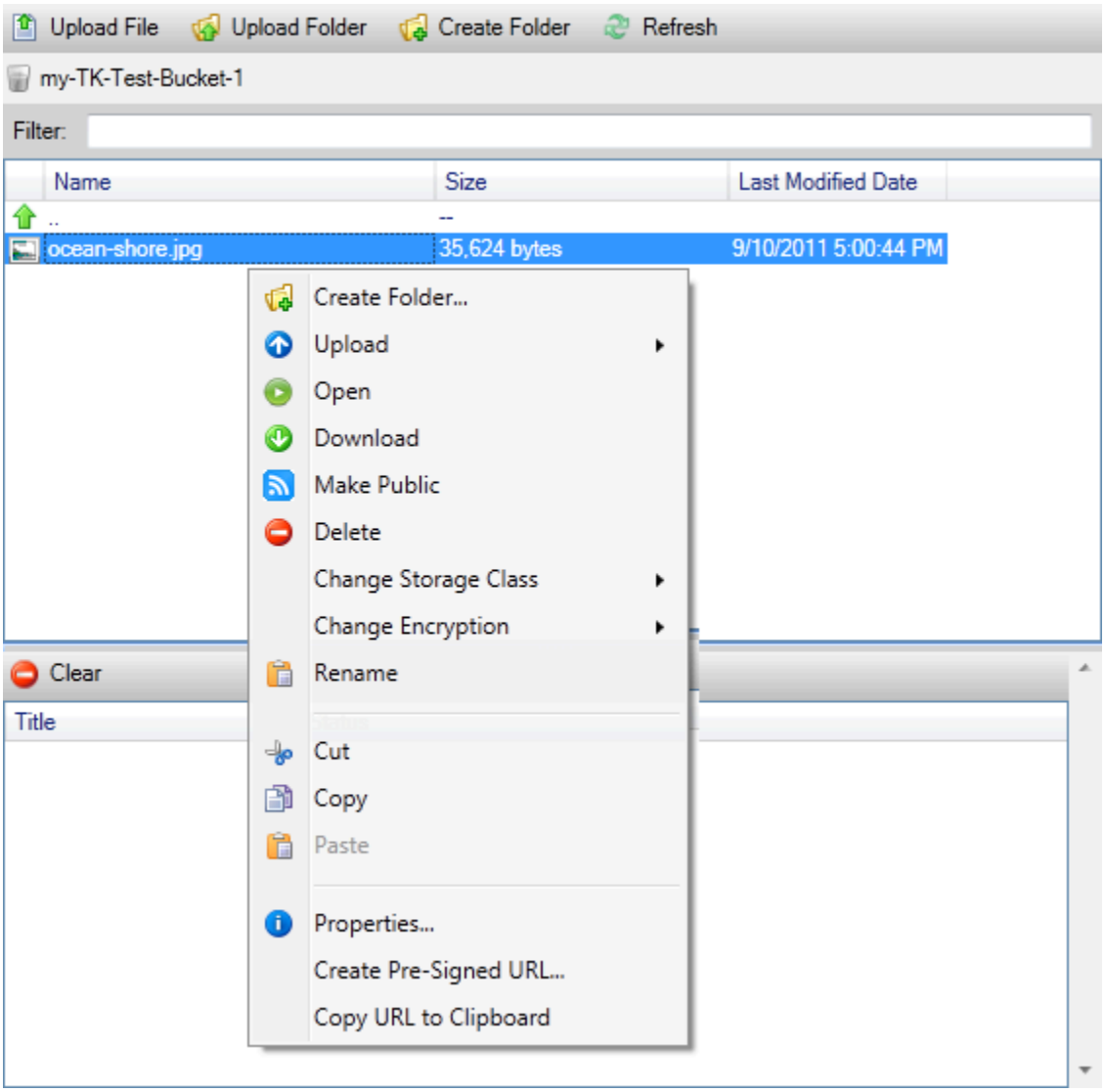
   La boîte de dialogue Upload Settings (Paramètres de téléchargement) vous permet de définir des métadonnées et des autorisations sur les fichiers ou dossiers que vous chargez. Cocher la case Make everything public (Rendre tout public) équivaut à définir les autorisations Open/Download (Ouvrir/Télécharger) sur Tout le monde. Vous pouvez choisir d'utiliser le Reduced Redundancy Storage (Stockage à redondance réduite) pour les fichiers téléchargés.





Opérations de fichier Amazon S3 à partir deAWSToolkit pour Visual Studio

Si vous choisissez un fichier dans la vue Amazon S3 et que vous cliquez sur le bouton droit de la souris pour ouvrir le menu contextuel de ce fichier, vous pouvez exécuter différentes opérations sur ce fichier.



Créer un dossier

Vous permet de créer un dossier dans le compartiment actif. (Équivaut à cliquer sur le lien Créer un dossier.)

Charger

Vous permet de charger des fichiers ou des dossiers. (Équivaut à cliquer sur le lien Charger le fichier ou Upload Folder (Charger le dossier).)

Ouvert

Tente d'ouvrir le fichier sélectionné dans votre navigateur par défaut. Selon le type de fichier et les fonctionnalités de votre navigateur par défaut, le fichier peut ne pas être affiché. Au lieu de cela, il peut simplement être téléchargé par votre navigateur.

Download

Ouvre une boîte de dialogue Folder-Tree (Dossier-arborescence) pour vous permettre de télécharger le fichier sélectionné.

Rendre public

Définit les autorisations sur le fichier sélectionné sur Open/Download (Ouvrir/Télécharger) et Tout le monde. (Équivaut à cocher la case Make everything public (Rendre tout public) dans la boîte de dialogue Upload Settings (Paramètres de téléchargement).)

Suppression

Supprime les fichiers ou dossiers sélectionnés. Vous pouvez également supprimer des fichiers ou des dossiers en les sélectionnant et en appuyant sur `Delete`.

Changer de classe de stockage

Définit la classe de stockage sur Standard ou Reduced Redundancy Storage (RRS). Pour afficher le paramètre de la classe de stockage actuelle, choisissez Propriétés.

Modifier le chiffrement

Vous permet de définir un chiffrement côté serveur sur le fichier. Pour afficher le paramètre de chiffrement actuel, choisissez Propriétés.

Renommer

Vous permet de renommer un fichier. Vous ne pouvez pas renommer un dossier.

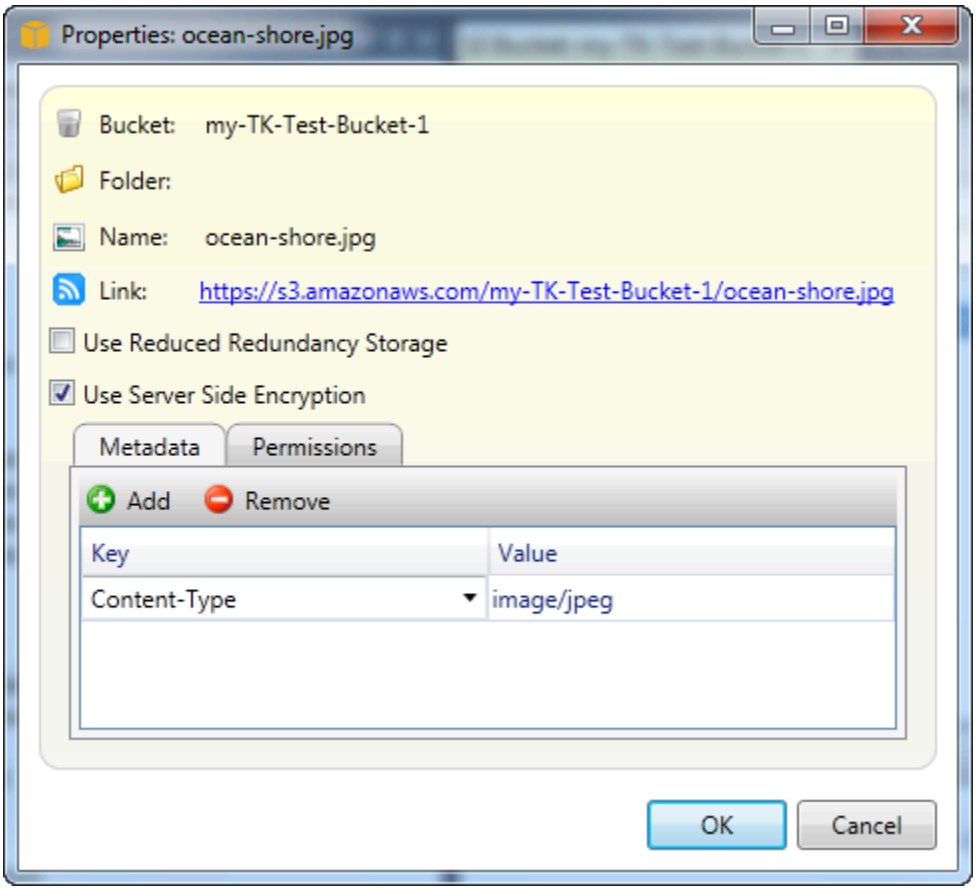
Cut | Copy | Paste (Couper | Copier| Coller)

Vous permet de couper, copier et coller des fichiers ou des dossiers entre les dossiers ou les compartiments.

Propriétés

Affiche une boîte de dialogue qui vous permet de définir des métadonnées et des autorisations pour le fichier, ainsi que de basculer le stockage du fichier entre Reduced Redundancy Storage (RRS) et Standard, et de définir le chiffrement côté serveur du fichier. Cette boîte de dialogue affiche également un lien https vers le fichier. Si vous choisissez ce lien, Toolkit for Visual Studio ouvre le

fichier dans votre navigateur par défaut. Si vous avez des autorisations sur le fichier définies sur Open/Download (Ouvrir/Télécharger) et Tout le monde, d'autres personnes peuvent accéder au fichier en cliquant sur ce lien. Nous vous recommandons de créer et distribuer des URL pré-signées au lieu de distribuer ce lien.



Create Pre-Signed URL (Créer une URL pré-signée)

Vous permet de créer une URL pré-signée limitée dans le temps que vous pouvez distribuer pour permettre à d'autres personnes d'accéder au contenu que vous avez stocké sur Amazon S3.

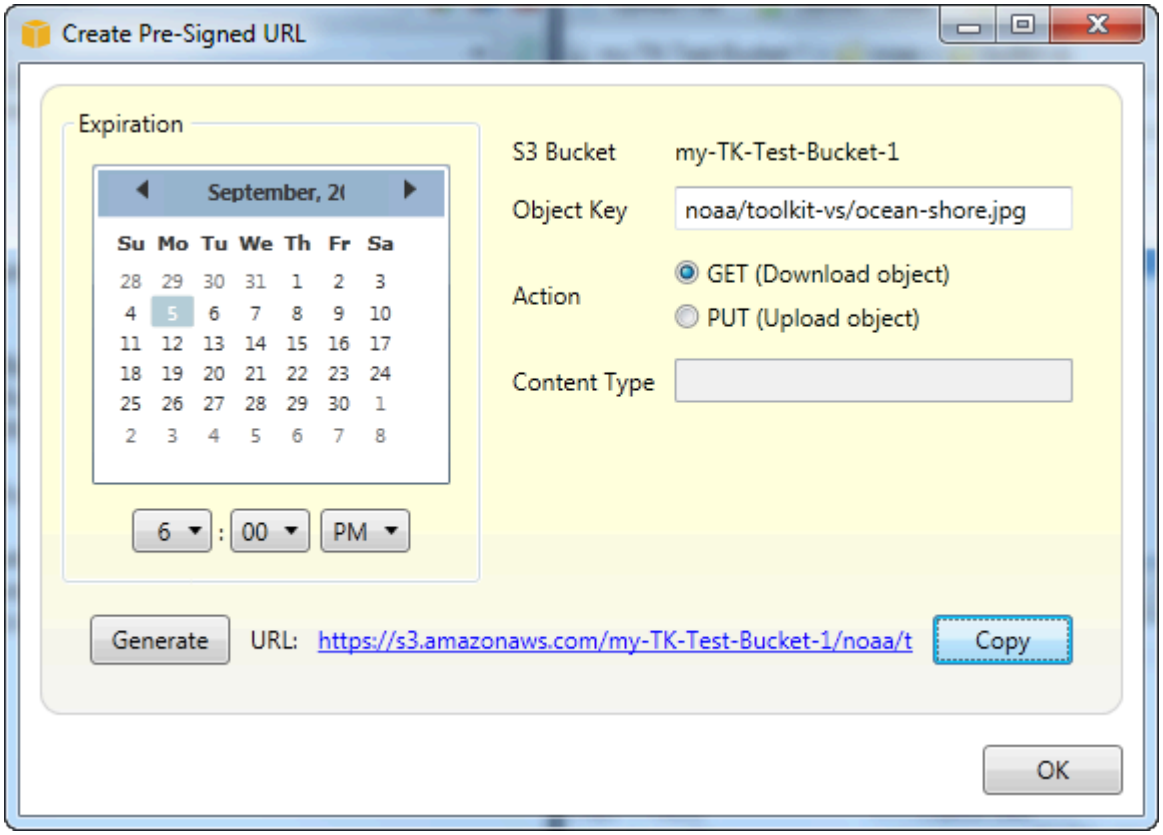
Comment créer une URL pré-signée

Vous pouvez créer une URL pré-signée pour un compartiment ou des fichiers d'un compartiment. D'autres personnes peuvent ensuite utiliser cette URL pour accéder au compartiment ou au fichier. L'URL expire au bout de la période que vous spécifiez lorsque vous créez l'URL.

Pour créer une URL pré-signée

1. Dans la boîte de dialogue Create Pre-Signed URL (Créer une URL pré-signée), définissez la date et l'heure d'expiration de l'URL. Le paramètre par défaut est une heure après l'heure actuelle.

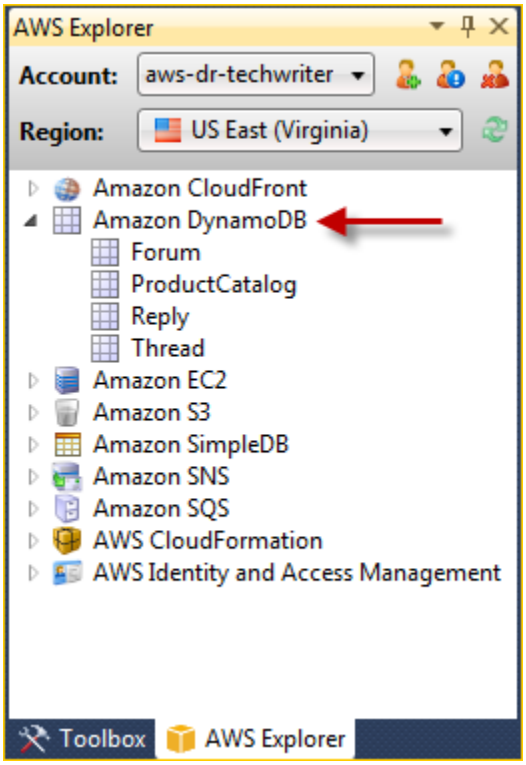
2. Cliquez sur le bouton Générer.
3. Pour copier l'URL dans le presse-papiers, choisissez Copier.



Utilisation de DynamoDB depuisAWSExplorateur

Amazon DynamoDB est un service de base de données non relationnelle rapide, économique, très évolutif et hautement disponible. DynamoDB permet de s'affranchir des limites habituelles du dimensionnement de stockage de données, tout en conservant une faible latence et des performances prévisibles. Toolkit for Visual Studio fournit des fonctionnalités pour utiliser DynamoDB dans un contexte de développement. Pour plus d'informations sur DynamoDB, consultez.DynamoDBsur le site Web Amazon Web Services.

Dans Toolkit for Visual Studio,AWSL'explorateur affiche toutes les tables DynamoDB associées à l'actif.Compte AWS.



Création d'une table DynamoDB

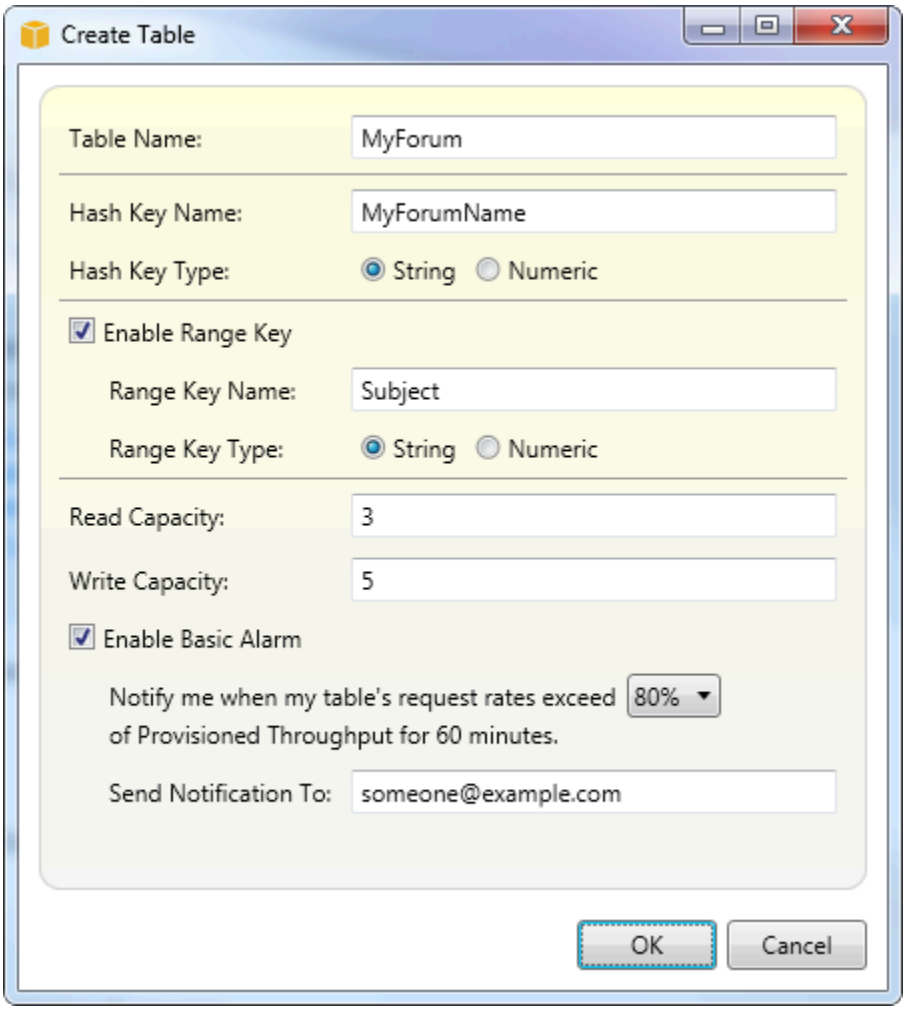
Vous pouvez utiliser Toolkit for Visual Studio pour créer une table DynamoDB.

Pour créer une table dansAWSExplorateur

1. DansAWSExplorateur, ouvrez le menu contextuel (clic droit) pourAmazon DynamoDB, puis choisissezCréer une table.
2. Dans l'assistant Créer une table dans Nom de la table, saisissez le nom de la table.
3. DansNom de la clé de hachage, saisissez un attribut de clé de hachage primaire et dans le champType de clé de hachage, choisissez le type de clé de hachage. DynamoDB crée un index de hachage non ordonné à l'aide de l'attribut de clé primaire et d'un index de plage trié à l'aide de l'attribut de clé primaire de plage. Pour plus d'informations sur l'attribut de clé de hachage primaire, accédez au manuelClé primairedans la sectionAmazon DynamoDB Developer Guide.
4. (Facultatif) Sélectionnez Enable Range Key (Activer la clé de plage). Dans le champ Hash Key Name (Nom de clé de hachage), saisissez un attribut de clé de plage, puis cochez le type de clé de plage dans Hash Key Type (Type de clé de hachage).
5. Dans le champ Capacité de lecture, saisissez le nombre d'unités de lecture. Dans le champ Capacité d'écriture, saisissez le nombre d'unités d'écriture. Vous devez spécifier au minimum

trois unités de lecture et cinq unités d'écriture. Pour plus d'informations sur les unités de lecture et d'écriture, consultez Provisioned Throughput in DynamoDB (Débit alloué dans DynamoDB).

6. (Facultatif) Sélectionnez Enable Basic Alarm (Activer une alarme de base) pour être averti lorsque les débits de demandes de votre table sont trop élevés. Choisissez le pourcentage de débit alloué toutes les 60 minutes devant être dépassé avant que l'alerte soit envoyée. Dans Envoyez des notifications à, saisissez une adresse e-mail.
7. Cliquez sur OK pour créer la table.

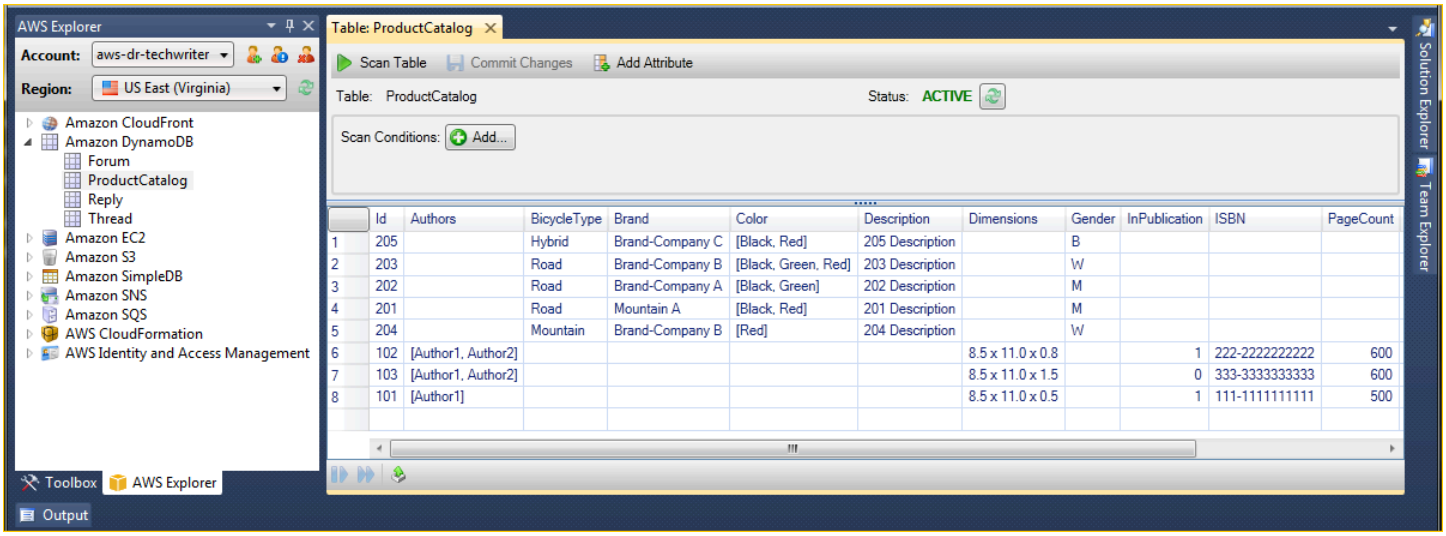


Pour plus d'informations sur les tables DynamoDB, accédez au manuelConcepts de modèle de données : tables, éléments et attributs.

Affichage d'une table DynamoDB sous forme de grille

Pour afficher l'une de vos tables DynamoDB sous forme de grille, dansAWSCliquez deux fois sur le sous-nœud correspondant à la table. Dans la vue grille, vous pouvez afficher les éléments, les attributs et les valeurs stockés dans la table. Chaque ligne correspond à un élément de la table. Les colonnes de la table correspondent aux attributs. Chaque cellule de la table contient les valeurs associées à l'attribut de cet élément.

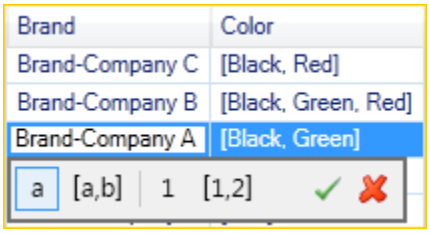
La valeur d'un attribut peut être une chaîne ou un nombre. Certains attributs disposent d'une valeur composée d'un ensemble de chaînes ou de nombres. L'ensemble de valeurs est affiché sous forme de liste séparée par des virgules délimitée par des crochets.



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

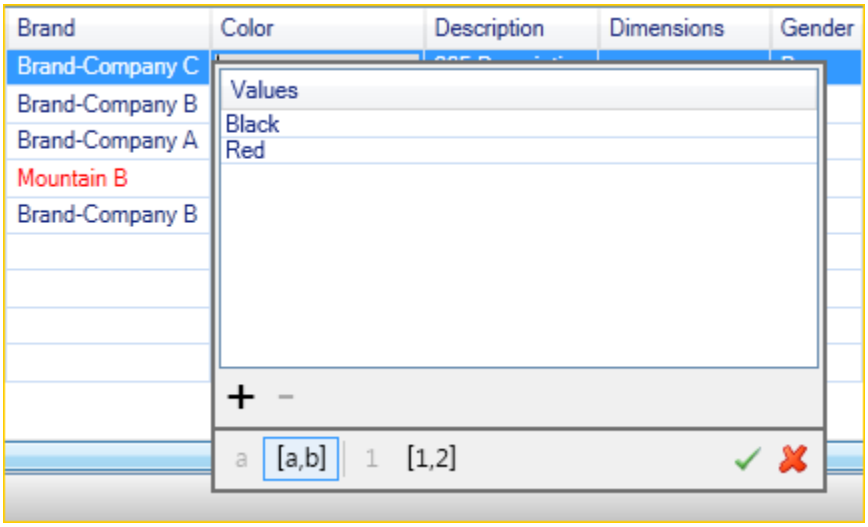
Modification et ajout d'attributs et de valeurs

En cliquant deux fois sur une cellule, vous pouvez modifier les valeurs de l'attribut correspondant à l'élément. Pour les attributs de l'ensemble de valeurs, vous pouvez également ajouter ou supprimer des valeurs individuelles à partir de l'ensemble.



Outre la modification de la valeur d'un attribut, vous pouvez également modifier le format de la valeur d'un attribut (avec certaines restrictions). Par exemple, toute valeur numérique peut être convertie en une valeur de chaîne. Si vous disposez d'une valeur de chaîne dont le contenu est un

nombre, comme 125, l'éditeur de cellule vous permet de convertir le format de la valeur d'une chaîne en un nombre. Vous pouvez également convertir une valeur unique en un ensemble de valeurs. Cependant, vous ne pouvez généralement pas convertir un ensemble de valeurs en une valeur unique ; sauf lorsque l'ensemble de valeurs ne dispose que d'un seul élément dans l'ensemble.

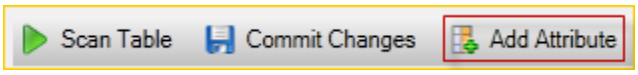


Après avoir modifié la valeur d'attribut, choisissez la coche verte pour confirmer vos modifications. Si vous voulez annuler vos modifications, choisissez la X rouge.

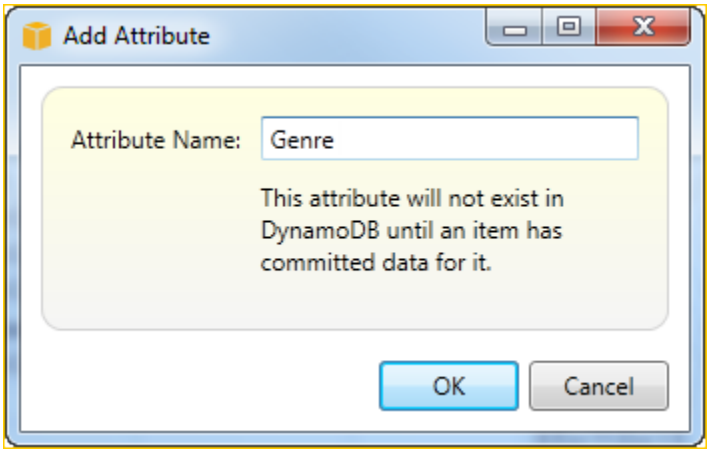
Après avoir confirmé vos modifications, la valeur d'attribut s'affiche en rouge. Cela indique que l'attribut a été mis à jour, mais que la nouvelle valeur n'a pas été répercutée dans la base de données DynamoDB. Pour répercuter vos modifications dans DynamoDB, choisissezCommettre des modifications. Pour annuler vos modifications, choisissez Scan Table (Analyser la table) et lorsque la boîte à outils vous demande si vous souhaitez valider vos modifications avant l'analyse, choisissez Non.

Ajout d'un attribut

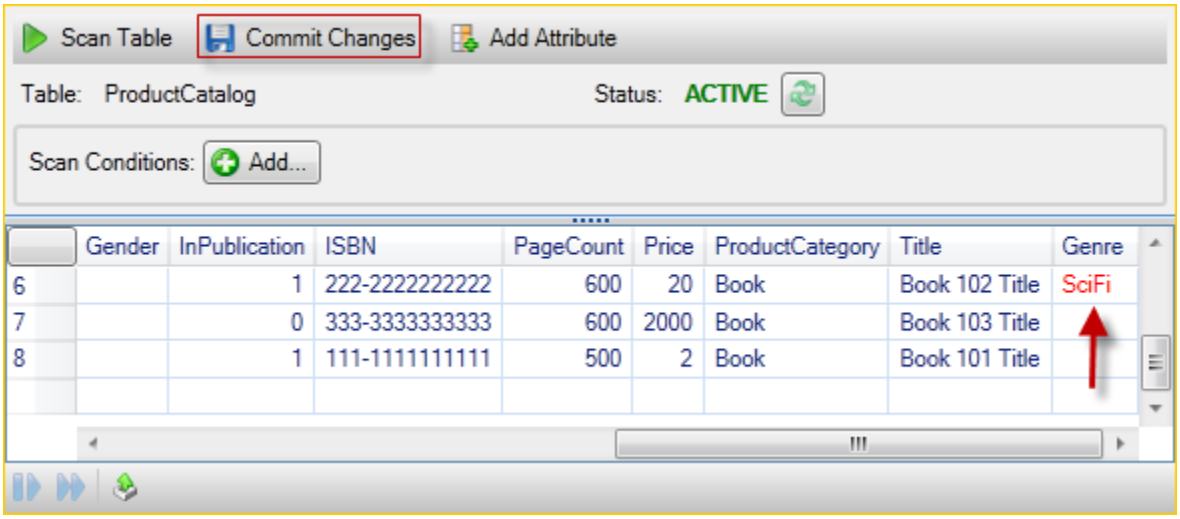
Dans la vue grille, vous pouvez également ajouter des attributs à la table. Pour ajouter un nouvel attribut, choisissez Ajouter un attribut.



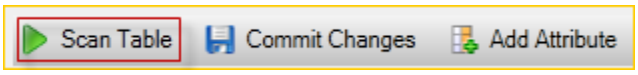
Dans la boîte de dialogue Ajouter un attribut, saisissez le nom de votre attribut, puis choisissez OK.



Pour que le nouvel attribut fasse partie de la table, vous devez y ajouter une valeur pour au moins un élément et choisir le bouton Valider les modifications. Pour annuler le nouvel attribut, fermez la vue grille de la table sans choisir Valider les modifications.



Analyse d'une table DynamoDB

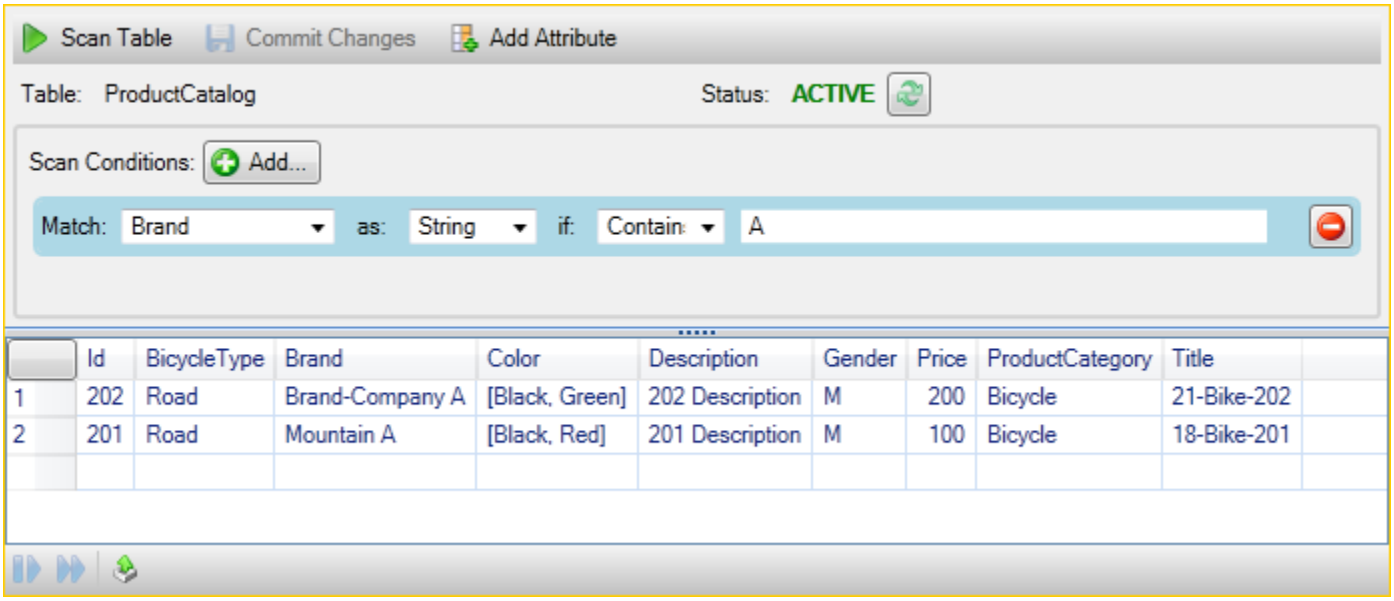


Vous pouvez effectuer des analyses sur vos tables DynamoDB depuis le Toolkit. Dans une analyse, vous définissez un ensemble de critères et l'analyse renvoie tous les éléments correspondant à vos critères depuis la table. Les analyses constituent une opération coûteuse qui doit être utilisée avec précaution pour éviter de perturber un trafic de production de priorité plus élevée sur la table. Pour plus d'informations sur l'utilisation de l'analyse, accédez au manuelAmazon DynamoDB Developer Guide.

Pour réaliser l'analyse d'une table DynamoDB depuisAWSExplorateur

1. Dans la vue grille, choisissez le bouton scan conditions: add (.conditions d’analyse : ajouter).
2. Dans l'éditeur de clause d'analyse, choisissez l'attribut à associer, l'interprétation de la valeur d'attribut (chaîne, nombre, ensemble de valeurs), la façon dont il doit être associé (par exemple, Commence par ou Contient), et la valeur littérale à laquelle il doit être associé.
3. Ajoutez plusieurs clauses d'analyse, si nécessaire, pour votre recherche. L'analyse renvoie uniquement les éléments correspondant aux critères de l'ensemble des clauses d'analyse. L'analyse réalise une comparaison sensible à la casse en cas d'association à des valeurs de chaîne.
4. Sur la barre de boutons en haut de la vue grille, choisissez Scan Table (Analyser la table).

Pour supprimer une clause d'analyse, choisissez le bouton rouge avec la ligne blanche à droite de chaque clause.



Pour revenir à la vue de la table qui inclut tous les éléments, supprimez toutes les clauses d'analyse et choisissez de nouveau Scan Table (Analyser la table).

Pagination des résultats de l'analyse

Trois boutons sont situés en bas de la page.

Les deux premiers boutons bleus fournissent la pagination des résultats de l'analyse. Le premier bouton affiche une autre page de résultats. Le deuxième bouton affiche dix autres pages de résultats. Dans ce contexte, une page équivaut à 1 Mo de contenu.

Exporter les résultats de l'analyse au format CSV

Le troisième bouton exporte les résultats de l'analyse actuelle dans un fichier CSV.

A l'aide deAWS CodeCommitavec Visual Studio Team Explorer

Vous pouvez utiliserAWS Identity and Access Management(IAM) pour créer des informations d'identification Git et les utiliser pour créer et cloner des référentiels dans Team Explorer.

Types d'informations d'identification pour AWS CodeCommit

MostAWS Toolkit for Visual Studioles utilisateurs sont au courant de la configurationAWSprofils d'informations d'identification qui contiennent leurs clés d'accès et leurs clés secrètes. Ces profils d'informations d'identification sont utilisés dans Toolkit for Visual Studio pour activer les appels d'API de service, par exemple, pour répertorier les compartiments Amazon S3 dansAWSExplorer ou pour lancer une instance Amazon EC2. L'intégration d'AWS CodeCommit avec Team Explorer utilise également ces profils d'informations d'identification. Cependant, pour utiliser Git lui-même, vous avez besoin d'autres informations d'identification, plus précisément des informations d'identification Git pour les connexions HTTPS. Pour obtenir des informations sur ces informations d'identification (un nom d'utilisateur et un mot de passe), consultez l'Configuration pour les utilisateurs en HTTPS avec informations d'identification Gitdans leAWS CodeCommitGuide de l'utilisateur.

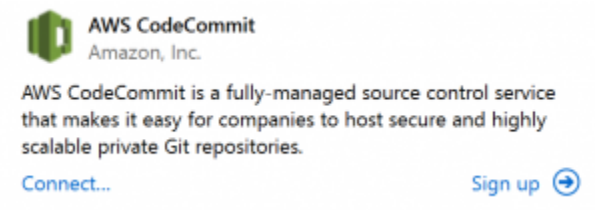
Vous pouvez créer les informations d'identification Git pourAWS CodeCommituniquement pour les comptes utilisateur IAM. Vous ne pouvez pas les créer pour un compte racine. Vous pouvez créer jusqu'à deux ensembles de ces informations d'identification pour le service et, bien que vous puissiez marquer un ensemble d'informations d'identification comme inactif, ces ensembles inactifs sont comptabilisés dans le nombre limite de deux jeux. Notez que vous pouvez supprimer et recréer ces informations d'identification à tout moment. Lorsque vous utilisezAWS CodeCommitdepuis Visual Studio, votre système traditionnelAWSLes informations d'identification sont utilisées pour travailler avec le service lui-même, par exemple lorsque vous créez et répertoriez des référentiels. Lorsque vous utilisez les référentiels Git réels hébergés dans AWS CodeCommit, vous utilisez les informations d'identification Git.

Dans le cadre de l'appui àAWS CodeCommit, Toolkit for Visual Studio crée et gère automatiquement ces informations d'identification Git pour vous et les associe à votreAWSprofil d'informations

d'identification. Vous n'avez pas besoin de vous occuper de savoir si vous avez un ensemble d'informations d'identification approprié à portée de main pour effectuer les opérations Git dans Team Explorer. Une fois que vous vous êtes connecté à Team Explorer avec votreAWS, les informations d'identification Git associées sont utilisées automatiquement chaque fois que vous utilisez une télécommande Git.

Connexion à AWS CodeCommit

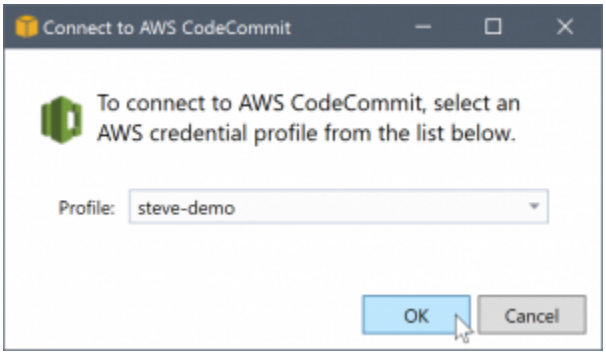
Lorsque vous ouvrez la fenêtre Team Explorer dans Visual Studio 2015 ou une version ultérieure, vous voyez une entrée AWS CodeCommit dans la section Hosted Service Providers de Manage Connections.



ChoixS'inscrireouvre la page d'accueil Amazon Web Services dans une fenêtre de navigateur. Ce qui se passe lorsque vous choisissezConnexiondépend si Toolkit for Visual Studio peut trouver un profil d'informations d'identification avecAWSclés d'accès et secrètes pour lui permettre de passer des appels àAWSen votre nom. Vous avez peut-être configuré un profil d'informations d'identification à l'aide de la nouvelle page de mise en route qui s'affiche dans l'IDE lorsque Toolkit for Visual Studio ne trouve pas d'informations d'identification stockées localement. Ou vous avez peut-être utilisé Toolkit for Visual Studio, leAWS Tools for Windows PowerShell, ou leAWS CLIet ont déjàAWSProfils d'informations d'identification disponibles pour Toolkit for Visual Studio à utiliser.

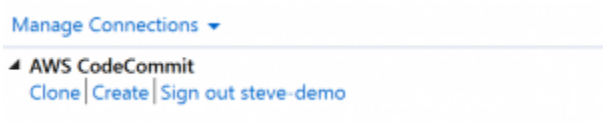
Lorsque vous choisissezConnexion, Toolkit for Visual Studio démarre le processus de recherche d'un profil d'informations d'identification à utiliser dans la connexion. Si Toolkit for Visual Studio ne trouve pas de profil d'informations d'identification, il ouvre une boîte de dialogue qui vous invite à saisir les clés d'accès et secrètes associées à votreCompte AWS. Nous vous recommandons vivement d'utiliser un compte d'utilisateur IAM au lieu de vos informations d'identification racine. En outre, comme indiqué précédemment, les informations d'identification Git dont vous avez inévitablement besoin ne peuvent être créées que pour les utilisateurs IAM. Lorsque les clés d'accès et les clés secrètes ont été fournies et que le profil d'informations d'identification a été créé, la connexion entre Team Explorer et AWS CodeCommit est prête à être utilisée.

Si Toolkit for Visual Studio en trouve plusieursAWSProfil d'informations d'identification, vous êtes invité à sélectionner le compte que vous souhaitez utiliser dans Team Explorer.



Si vous avez un seul profil d'informations d'identification, Toolkit for Visual Studio contourne la boîte de dialogue de sélection de profil et vous êtes connecté immédiatement :

Lorsqu'une connexion est établie entre Team Explorer et AWS CodeCommit via vos profils d'informations d'identification, la boîte de dialogue d'invitation se ferme et le panneau de connexion s'affiche.

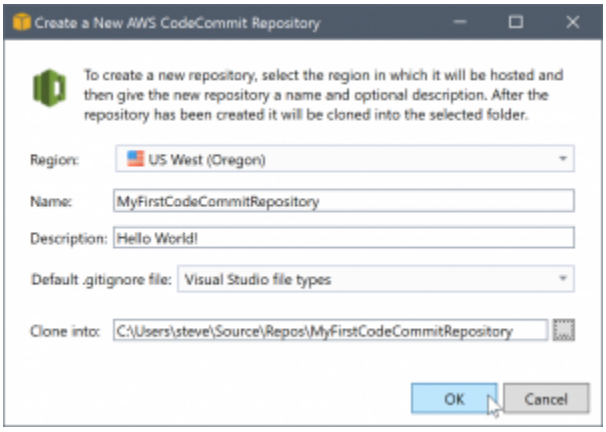


Etant donné que vous n'avez pas de référentiels clonés localement, le panneau n'affiche que les opérations que vous pouvez effectuer : Clone,Créer, etDéconnecter. Comme les autres fournisseurs,AWS CodeCommitdans Team Explorer ne peut être lié qu'à un seulAWSprofil d'informations d'identification à un moment donné. Pour passer d'un compte à un autre, vous utilisez Déconnexion pour supprimer la connexion et démarrer une nouvelle connexion avec un autre compte.

Maintenant que vous avez établi une connexion, vous pouvez créer un référentiel en cliquant sur le lien Créer.

Création d'un référentiel

Lorsque vous cliquez sur le boutonCréer, leCréer uneAWS CodeCommitRéférentiel.s'ouvre.



Les référentiels AWS CodeCommit sont organisés par région. Ainsi, dans Région, vous pouvez sélectionner la région dans laquelle héberger le référentiel. La liste contient toutes les régions dans lesquelles AWS CodeCommit est pris en charge. Vous fournissez le nom (obligatoire) et une description (facultative) pour votre nouveau référentiel.

Le comportement par défaut de la boîte de dialogue consiste à ajouter à l'emplacement du dossier du nouveau référentiel le nom du référentiel (lorsque vous indiquez le nom, l'emplacement du dossier se met à jour). Pour utiliser un autre nom de dossier, modifiez le chemin d'accès du dossier Clone into (Cloner en) après avoir indiqué le nom du référentiel.

Vous pouvez également choisir de créer automatiquement un fichier `.gitignore` initial pour le référentiel. AWS Toolkit for Visual Studio fournit une valeur par défaut intégrée pour les types de fichiers Visual Studio. Vous pouvez également choisir de n'avoir aucun fichier ou d'utiliser un fichier existant personnalisé et de le réutiliser dans tous les référentiels. Il vous suffit de sélectionner Use custom (Utiliser une version personnalisée) dans la liste et d'accéder au fichier personnalisé à utiliser.

Une fois que vous avez un nom de référentiel et un emplacement, vous êtes prêt à cliquer sur OK et à commencer à créer le référentiel. Toolkit for Visual Studio demande que le service crée le référentiel, puis clone le nouveau référentiel localement et ajoute une validation initiale pour le fichier .gitignore si vous en utilisez un. C'est à ce stade que vous commencez à utiliser le git distant.Toolkit for Visual Studio a donc maintenant besoin d'accéder aux informations d'identification Git décrites précédemment.

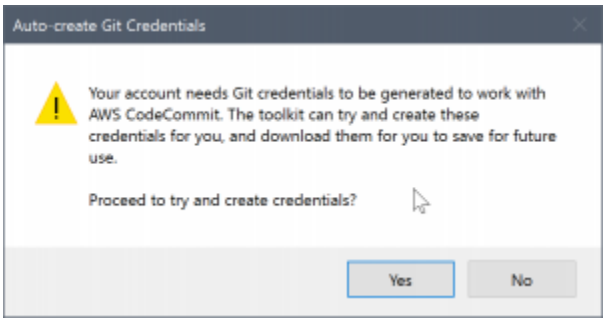
Configuration des informations d'identification Git

À ce stade, vous avez utiliséAWSclés d'accès et secrètes pour demander que le service crée votre référentiel. Maintenant, vous devez travailler avec Git lui-même pour effectuer l'opération de clonage réelle, et Git ne comprend pas.AWSclés d'accès et secrètes. À la place, vous devez fournir les

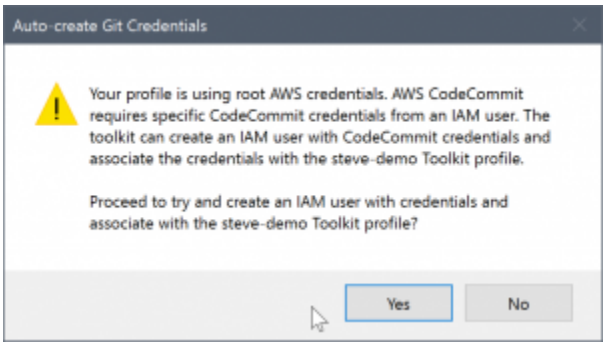
informations d'identification (nom d'utilisateur et mot de passe) que Git doit utiliser pour établir une connexion HTTPS avec le référentiel distant.

Comme indiqué dans Configuration des informations d'identification Git, les informations d'identification Git que vous allez utiliser doivent être associées à un utilisateur IAM. Vous ne pouvez pas les générer pour des informations d'identification racine. Vous devez toujours configurer votreAWSpour contenir des clés d'informations d'identification pour contenir des clés d'accès et secrètes IAM, et non des clés racine. Toolkit for Visual Studio peut tenter de configurer des informations d'identification Git pourAWS CodeCommitpour vous, et associez-les à laAWSprofil d'informations d'identification que vous avez utilisé pour vous connecter dans Team Explorer plus tôt.

Lorsque vous choisissezOK.dans leCréer uneAWS CodeCommitRéférentiel.et permet de créer le référentiel avec succès, Toolkit for Visual Studio vérifie laAWSprofil d'informations d'identification connecté dans Team Explorer pour déterminer si les informations d'identification Git pourAWS CodeCommitexistent et sont associés localement au profil. Si tel est le cas, Toolkit for Visual Studio indique à Team Explorer de lancer l'opération de clonage sur le nouveau référentiel. Si les informations d'identification Git ne sont pas disponibles localement, Toolkit for Visual Studio vérifie le type d'informations d'identification de compte qui ont été utilisées lors de la connexion dans Team Explorer. Si ces informations d'identification sont associées à un utilisateur IAM, comme nous le recommandons, le message suivant s'affiche.

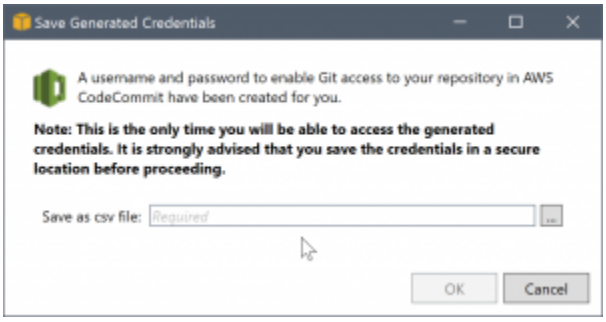


Si les informations d'identification sont des informations d'identification racine, le message suivant s'affiche à la place.



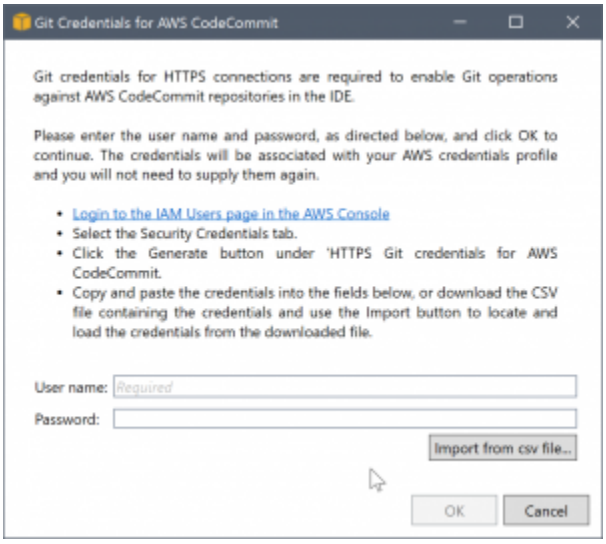
Dans les deux cas, Toolkit for Visual Studio propose d'essayer d'effectuer le travail pour créer les informations d'identification Git nécessaires pour vous. Dans le premier scénario, il lui suffit de créer un ensemble d'informations d'identification Git pour l'utilisateur IAM. Lorsqu'un compte racine est utilisé, Toolkit for Visual Studio commence par créer un utilisateur IAM, puis se met à créer des informations d'identification Git pour ce nouvel utilisateur. Si Toolkit for Visual Studio doit créer un nouvel utilisateur, il applique l'optionAWS CodeCommitStratégie gérée par Power User sur ce nouveau compte utilisateur. Cette stratégie permet d'accéder uniquement à AWS CodeCommit et autorise l'exécution de toutes les opérations avec AWS CodeCommit, sauf pour la suppression du référentiel.

Lorsque vous créez des informations d'identification, vous ne pouvez les afficher qu'une seule fois. Par conséquent, Toolkit for Visual Studio vous invite à enregistrer les informations d'identification nouvellement créées sous forme d'un `.csv`avant de continuer.



Nous vous recommandons vivement d'enregistrer les informations d'identification AWS CodeCommit. Veillez à les enregistrer dans un emplacement sûr !

Dans certains cas, Toolkit for Visual Studio ne peut pas créer automatiquement d'informations d'identification. Par exemple, vous avez peut-être déjà créé le nombre maximal d'ensembles d'informations d'identification Git pourAWS CodeCommit(deux), ou vous n'avez peut-être pas de droits de programmation suffisants pour que Toolkit for Visual Studio effectue le travail à votre place (si vous êtes connecté en tant qu'utilisateur IAM). Dans ces cas-là, vous pouvez vous connecter à l'AWS Management Consolepour gérer les informations d'identification ou les obtenir auprès de votre administrateur. Vous pouvez ensuite les entrer dans leInformations d'identification Git pourAWS CodeCommit, que s'affiche dans Toolkit for Visual Studio.

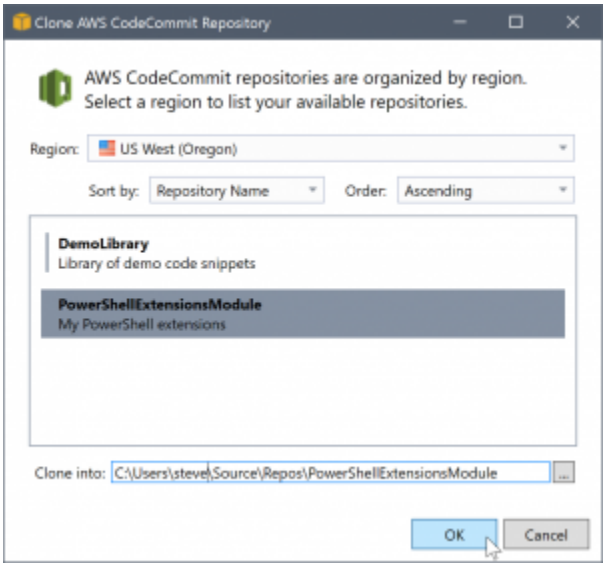


Maintenant que les informations d'identification pour Git sont disponibles, l'opération de clonage du nouveau référentiel continue (voir l'avancement de l'opération dans Team Explorer). Si vous avez choisi d'appliquer un fichier `.gitignore` par défaut, celui-ci est validé dans le référentiel avec le commentaire « Initial Commit ».

C'est tout ce qu'il faut pour configurer des informations d'identification et créer un référentiel dans Team Explorer. Une fois que les informations d'identification requises sont en place, seule la seule chose que vous voyez lors de la création ultérieure de référentiels, seule laCréer uneAWS CodeCommitRéférentiel.boîte de dialogue elle-même.

Clonage d'un référentiel

Pour cloner un référentiel existant, revenez au panneau de connexion pour AWS CodeCommit dans Team Explorer. Cliquez surClonelien pour ouvrir leCloneAWS CodeCommitRéférentiel., puis sélectionnez le référentiel à cloner et l'emplacement où vous voulez le placer sur le disque.



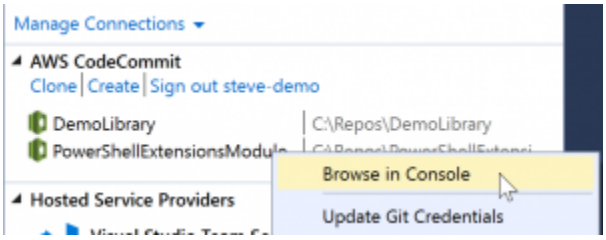
Une fois que vous avez choisi la région, Toolkit for Visual Studio interroge le service pour connaître les référentiels qui sont disponibles dans cette région et les affiche dans la partie centrale de la boîte de dialogue. Le nom et la description facultative de chaque référentiel sont également affichés. Vous pouvez réorganiser la liste en la triant par nom de référentiel ou selon la date de la dernière modification, et par ordre croissant ou décroissant.

Après avoir sélectionné le référentiel, vous pouvez choisir l'emplacement où le cloner. Par défaut, il s'agit du même emplacement de référentiel utilisé dans d'autres modules d'extension de Team Explorer, mais vous pouvez rechercher ou saisir un autre emplacement. Par défaut, le nom du référentiel est ajouté comme suffixe au chemin sélectionné. Cependant, si vous voulez un chemin spécifique, il vous suffit de modifier la zone de texte après avoir sélectionné le dossier. Quel que soit le texte figurant dans la zone, lorsque vous cliquez sur OK, vous obtenez le dossier dans lequel se trouve le référentiel cloné.

Après avoir sélectionné le référentiel et un emplacement de dossier, vous cliquez ensuite sur OK pour continuer l'opération de clonage. Vous voyez la progression de l'opération de clonage dans Team Explorer, comme lorsque vous créez un référentiel.

Utilisation des référentiels

Lorsque vous clonerez ou créerez des référentiels, vous remarquerez que les référentiels locaux correspondant à la connexion sont répertoriés dans le panneau des connexions de Team Explorer sous les liens d'opération. Ces entrées vous permettent d'accéder commodément au référentiel pour en consulter le contenu. Pour cela, cliquez avec le bouton droit de la souris sur le référentiel et choisissez Browse in Console (Parcourir dans la console).



Vous pouvez également utiliser Update Git Credentials (Mettre à jour les informations d'identification Git) pour mettre à jour les informations d'identification Git associées au profil d'informations d'identification. Cela est très utile si vous avez modifié les informations d'identification. La commande ouvre la commandeInformations d'identification Git pourAWS CodeCommitdans laquelle vous pouvez entrer ou importer les nouvelles informations d'identification.

Les opérations Git sur les référentiels fonctionnent comme prévu. Vous pouvez effectuer des validations locales et, lorsque vous êtes prêt à partager, vous utilisez l'option Sync dans Team Explorer. Parce que les informations d'identification Git sont déjà stockées localement et associées à notre connexionAWS, nous ne serons pas invités à les fournir à nouveau pour les opérations sur le référentielAWS CodeCommitdistante.

Utilisation de CodeArtifact dans Visual Studio

AWS CodeArtifactest un service de référentiel d'artefacts intégralement géré, qui permet aux entreprises de stocker et partager en toute sécurité les packages logiciels utilisés pour le développement d'applications. Vous pouvez utiliser CodeArtifact avec des outils de génération et des gestionnaires de packages populaires tels que NuGet et .NET Core CLI et Visual Studio. Vous pouvez également configurer CodeArtifact pour extraire des packages à partir d'un référentiel public externe tel queNuget.org.

Dans CodeArtifact, vos packages sont stockés dans des référentiels qui sont ensuite stockés dans un domaine. LeAWS Toolkit for Visual Studiosimplifie la configuration de Visual Studio avec vos référentiels CodeArtifact, ce qui facilite la consommation de paquets dans Visual Studio à partir de CodeArtifact directement et de Nuget.org.

Ajoutez votre référentiel CodeArtifact en tant que source de package NuGet

Pour consommer des paquets de votre CodeArtifact, vous devez ajouter votre référentiel en tant que source de paquets dans leGestionnaire de packages NuGetdans Visual Studio

Pour ajouter votre référentiel en tant que source de package

1. DansAWSExplorer, accédez à votre référentiel dans leAWS CodeArtifactnœud.
2. Ouvrez le menu contextuel (clic droit) du référentiel que vous souhaitez ajouter, puis choisissezCopier le point de terminaison source NuGet.
3. Accédez àSources de packagessous leGestionnaire de packages NuGetdans le nœudOutils > Optionsmenu.
4. DansSources de packages, sélectionnez le signe plus (+), modifiez le nom et collez l'URL du point de terminaison source NuGet que vous avez copiée précédemment dans leSource.
5. Activez la case à cocher en regard de la source de package que vous venez d'ajouter pour l'activer.

> **Note**
>
> Nous vous recommandons d'ajouter une connexion externe àNuget.orgsur votre CodeArtifact et désactivation dunuget.orgsource du package dans Visual Studio. Lorsque vous utilisez une connexion externe, toutes les dépendances extraites deNuget.orgsont stockés dans CodeArtifact. SiNuget.orgtombe en panne pour n'importe quelle raison, les paquets dont vous avez besoin seront toujours disponibles. Pour plus d'informations sur les connexions externes, consultezAjouter une connexion externedans leAWS CodeArtifactGuide de l'utilisateur.

6. ChoisissezOK.pour fermer le menu.

Pour plus d'informations sur l'utilisation de CodeArtifact avec Visual Studio, consultezUtiliser CodeArtifact avec Visual Studiodans leAWS CodeArtifactGuide de l'utilisateur.

Amazon RDS à partir deAWSExplorateur

Amazon Relational Database Service (Amazon RDS) est un service qui vous permet d'allouer et de gérer des systèmes de base de données relationnelle SQL dans le cloud. Amazon RDS prend en charge trois types de systèmes de base de données :

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

Pour plus d'informations, consultez le Guide d'utilisateur Amazon RDS.

Un certain nombre de fonctionnalités présentées ici sont également disponibles via l'AWSManagement Consolepour Amazon RDS.

Rubriques

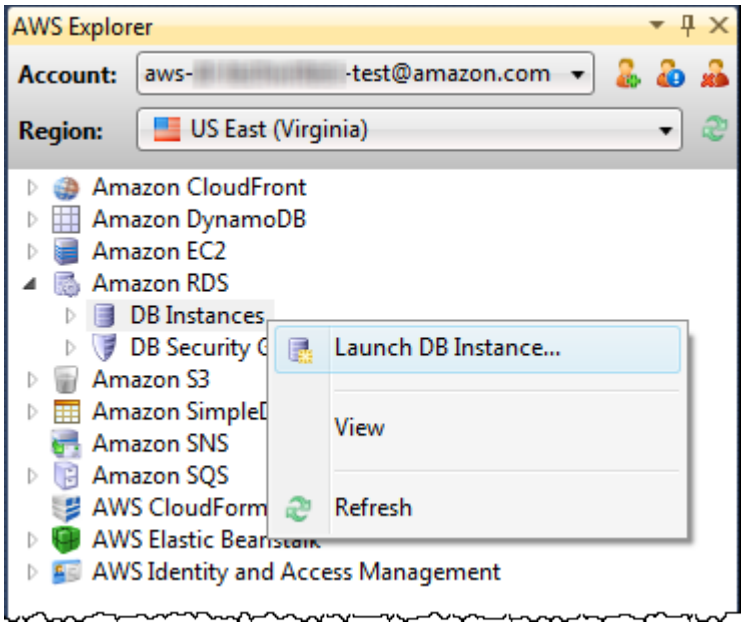
- Lancer une instance de base de données Amazon RDS
- Créer une base de données Microsoft SQL Server dans une instance RDS
- Groupes de sécurité Amazon RDS

Lancer une instance de base de données Amazon RDS

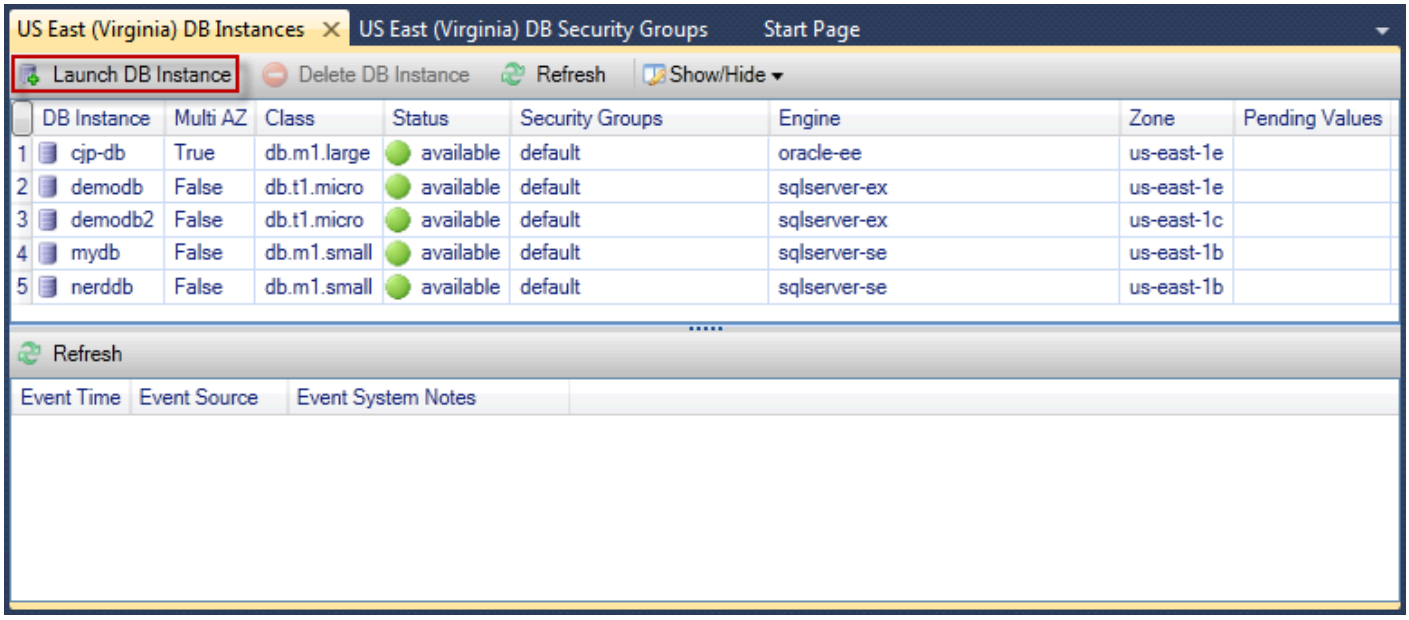
avecAWSExplorer, vous pouvez lancer une instance de tous les moteurs de base de données pris en charge par Amazon RDS. La procédure suivante montre l'expérience utilisateur pour lancer une instance de Microsoft SQL Server Standard Edition, mais l'expérience utilisateur est semblable pour tous les moteurs pris en charge.

Pour lancer une instance Amazon RDS

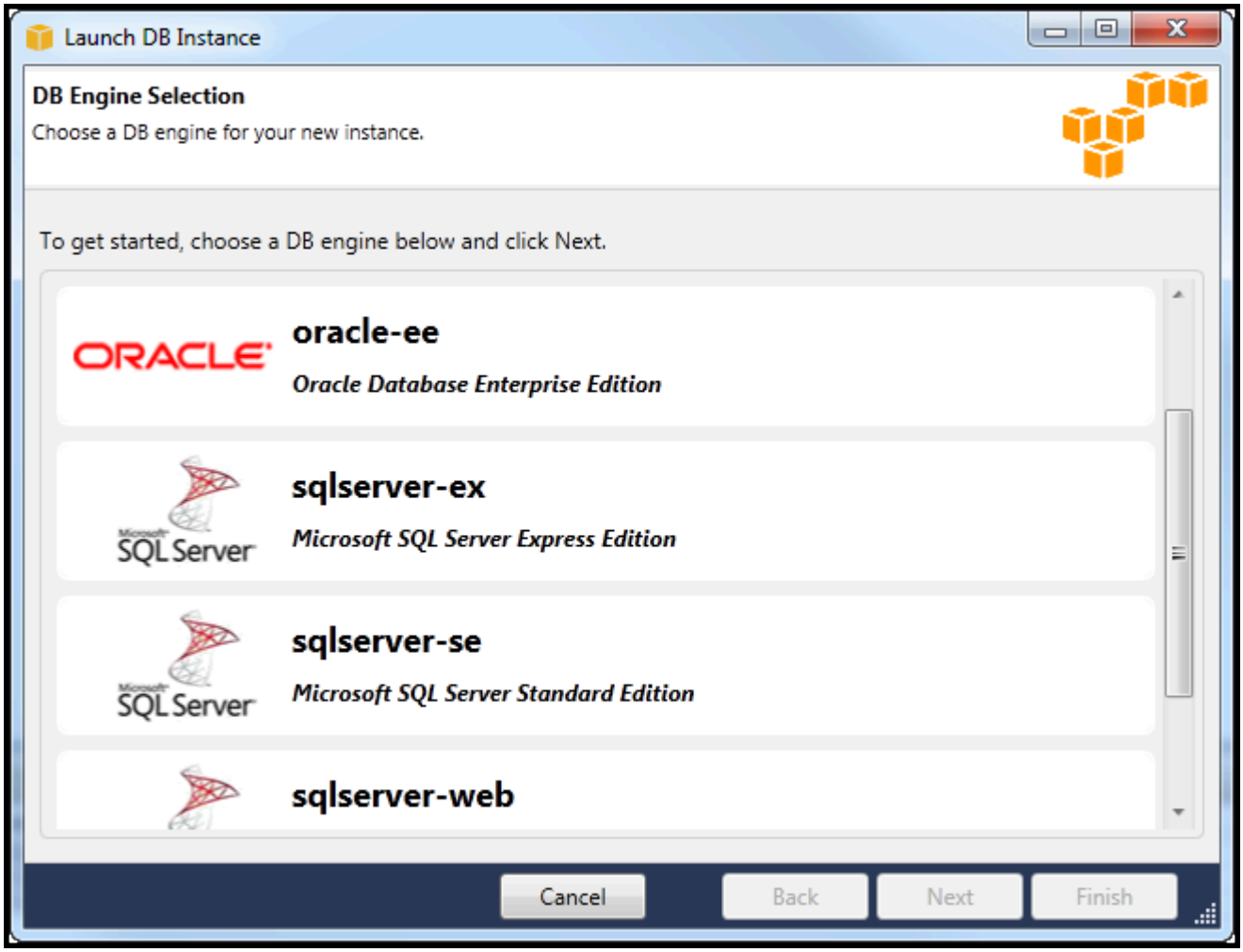
1. DansAWSOuvrez le menu contextuel (clic droit) correspondant à laAmazon RDSnoeud et choisissezLancement d'une instance DB.



   Sinon, dans l'onglet Instances DB, choisissez Lancement d'une instance DB.



2. Dans la boîte de dialogue DB Engine Selection (Sélection du moteur de la base de données), choisissez le type de moteur de base de données à lancer. Pour cette procédure, choisissez Microsoft SQL Server Standard Edition (sqlserver-se), puis choisissez Suivant.



3. Dans la boîte de dialogue DB Engine Instance Options (Options d'instance du moteur de la base de données), choisissez les options de configuration.

   Dans la section DB Engine Instance Options and Class (Options et classe d'instance du moteur de la base de données), vous pouvez spécifier les paramètres suivants.

   License Model

Type de moteur	Licence
Microsoft SQL Server	license-included
MySql	general-public-license
Oracle	bring-your-own-license

Le modèle de licence varie en fonction du type de moteur de base de données. Type de moteur Licence Microsoft SQL Server license-included MySql general-public-license Oracle bring-your-own-license

DB Instance Version (Version de l'instance de base de données)

Choisissez la version du moteur de base de données que vous souhaitez utiliser. Si une seule version est prise en charge, elle est sélectionnée pour vous.

Classe d'instance de base de données

Choisissez la classe d'instance pour le moteur de base de données. La tarification des classes d'instances varie. Pour en savoir plus, consultez la page Tarification Amazon RDS.

Perform a multi AZ deployment (Exécuter un déploiement multi-AZ)

Sélectionnez cette option pour créer un déploiement multi-AZ pour une durabilité et une disponibilité des données améliorées. Amazon RDS attribue et conserve une copie de secours de votre base de données dans une autre zone de disponibilité pour le basculement automatique en cas de panne planifiée ou non planifiée. Pour plus d'informations sur la tarification des déploiements multi-AZ, consultez la section tarification de la page de détails Amazon RDS. Cette option n'est pas prise en charge pour Microsoft SQL Server.

Upgrade minor versions automatically (Mettre à niveau automatiquement les versions)

Sélectionnez cette option pour avoirAWSexécute automatiquement des mises à jour de version mineure sur vos instances RDS pour vous.

Dans la section RDS Database Instance (Instance de la base de données RDS), vous pouvez spécifier les paramètres suivants.

Stockage alloué

Engine	Minimum (Go)	Maximum (Go)
MySQL	5	1 024
Oracle Enterprise Edition	10	1 024

Engine	Minimum (Go)	Maximum (Go)
Microsoft SQL Server Express Edition	30	1 024
Microsoft SQL Server Standard Edition	250	1 024
Microsoft SQL Server Web Edition	30	1 024

Les valeurs minimale et maximale pour le stockage alloué dépendent du type de moteur de base de données. Moteur Minimum (Go) Maximum (Go) 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

Identifiant d'instance de base de données

Spécifiez un nom pour l'instance de base de données. Ce nom n'est pas sensible à la casse. Il sera affiché en minuscules dansAWSExplorer.

Identifiant principal

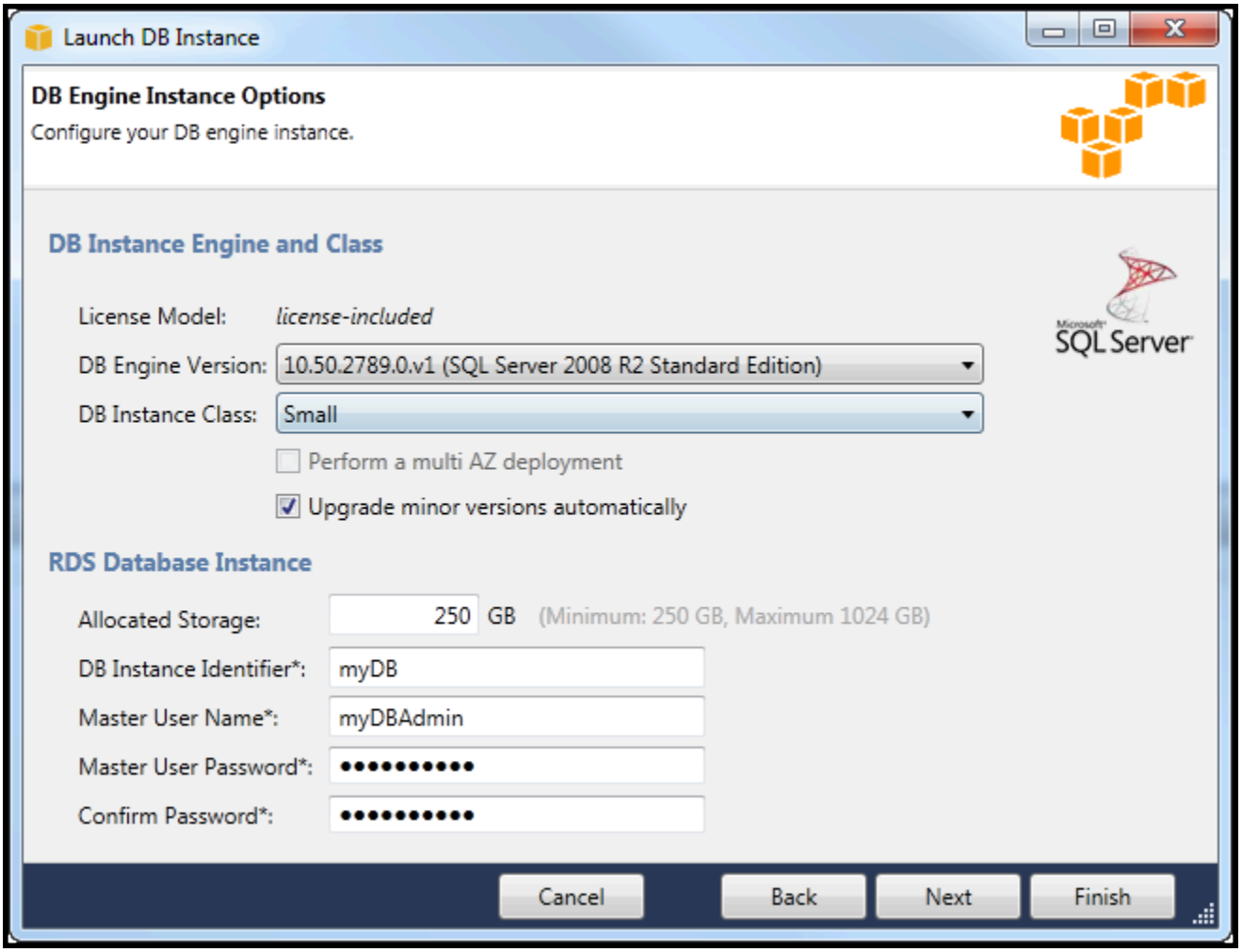
Saisissez un nom pour l'administrateur de l'instance de base de données.

Mot de passe de l'utilisateur principal

Saisissez un mot de passe pour l'administrateur de l'instance de base de données.

Confirm Password

Saisissez de nouveau le mot de passe pour le confirmer.



1. Dans la boîte de dialogue Additional Options (Options supplémentaires), vous pouvez spécifier les paramètres suivants.

   Database Port

   Il s'agit du port TCP que l'instance utilisera pour communiquer sur le réseau. Si votre ordinateur accède à Internet via un pare-feu, définissez cette valeur sur un port via lequel votre pare-feu autorise le trafic.

   Zone de disponibilité

   Utilisez cette option si vous souhaitez que l'instance soit lancée dans une zone de disponibilité particulière de votre région. L'instance de base de données que vous avez spécifiée pourrait ne pas être disponible dans toutes les zones de disponibilité d'une région donnée.

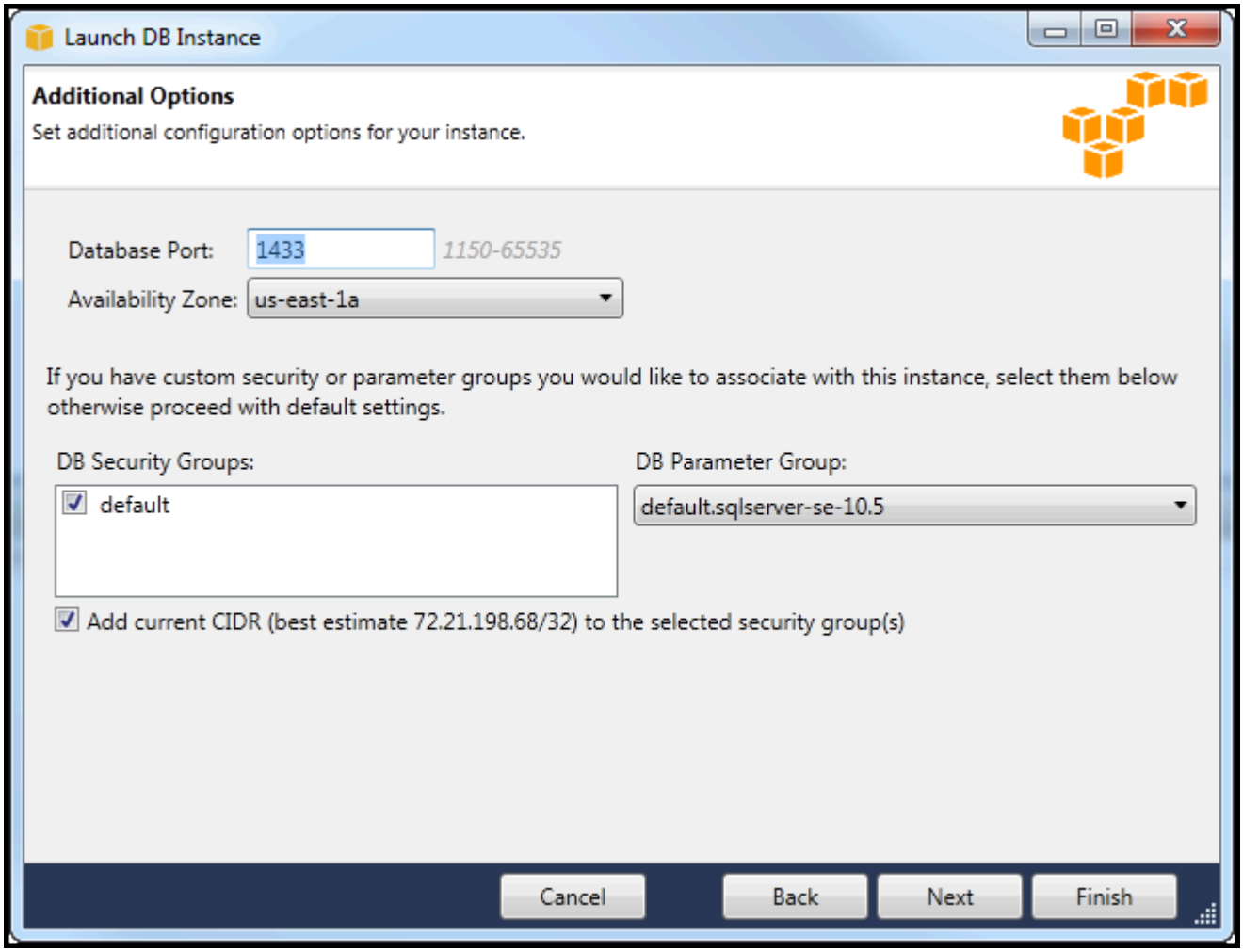
RDS Security Group (Groupe de sécurité RDS)

Sélectionnez un ou plusieurs groupes de sécurité RDS à associer à votre instance. Les groupes de sécurité RDS spécifient l'adresse IP, les instances Amazon EC2 etComptes AWSqui sont autorisés à accéder à votre instance. Pour plus d'informations sur les groupes de sécurité RDS, consultez Groupes de sécurité Amazon RDS. Toolkit for Visual Studio tente de déterminer votre adresse IP actuelle et offre la possibilité d'ajouter cette adresse aux groupes de sécurité associés à votre instance. Toutefois, si votre ordinateur accède à Internet via un pare-feu, l'adresse IP générée par la boîte à outils peut être inexacte. Pour déterminer l'adresse IP à utiliser, contactez votre administrateur système.

Groupe de paramètres DB

(Facultatif) Dans cette liste déroulante, choisissez un groupe de paramètres DB à associer à votre instance. Les groupes de paramètres DB vous permettent de modifier la configuration par défaut de l'instance. Pour plus d'informations, consultez le Manuel de l’utilisateur Amazon Relational Database Serviceet cet article.

Lorsque vous avez spécifié les paramètres de cette boîte de dialogue, choisissez Suivant.

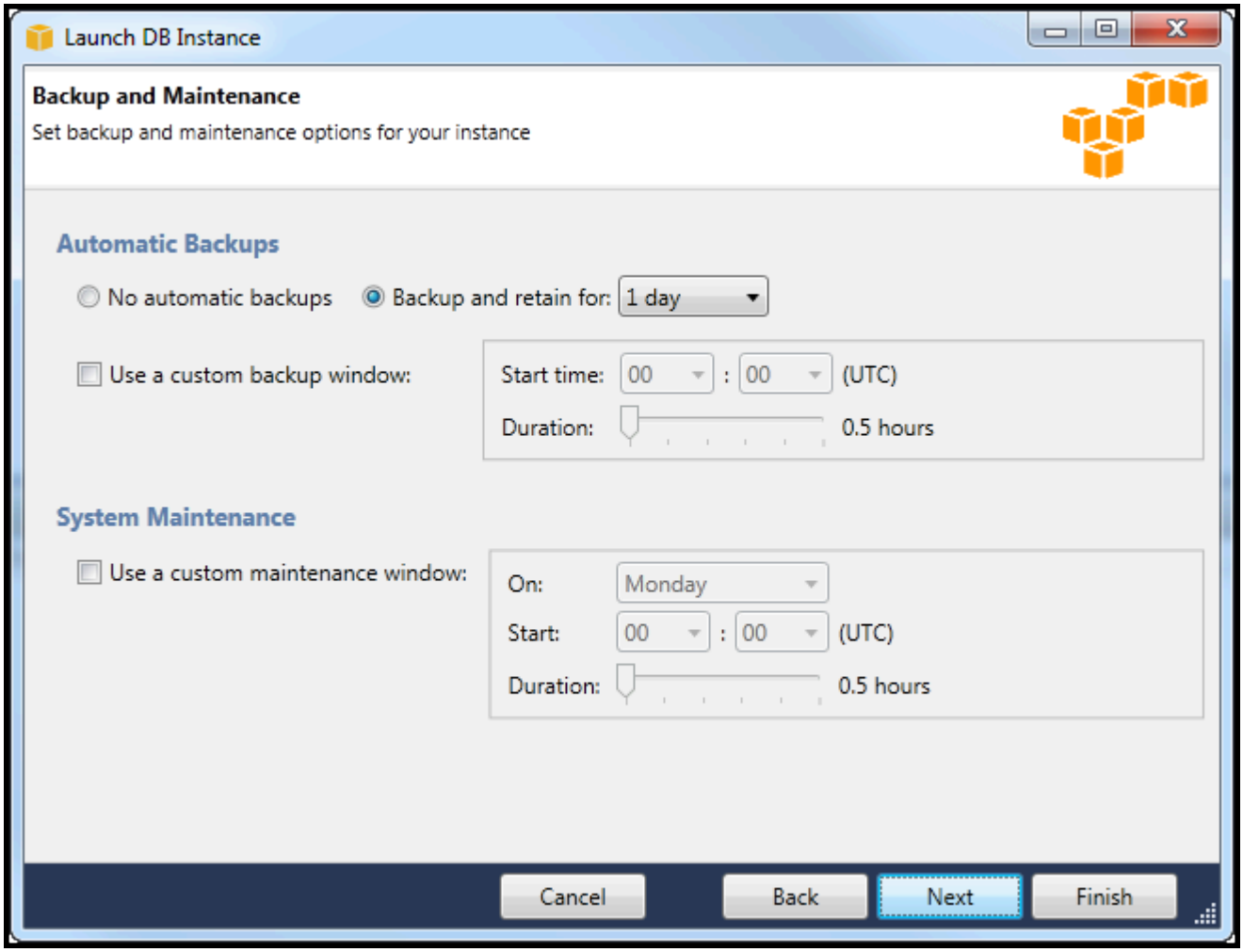


2. LeBackup et maintenancevous permet de spécifier si Amazon RDS doit sauvegarder votre instance et si oui, la durée de conservation des données sauvegardées. Vous pouvez également spécifier une fenêtre horaire pendant laquelle les sauvegardes doivent être exécutées.

   Cette boîte de dialogue vous permet également de spécifier si vous souhaitez qu'Amazon RDS exécute une maintenance du système sur votre instance. La maintenance inclut des correctifs de routine et des mises à niveau de version mineure.

   La fenêtre horaire que vous spécifiez pour la maintenance du système ne peut pas chevaucher la fenêtre spécifiée pour les sauvegardes.

   Choisissez Next (Suivant).



3. La boîte de dialogue finale de l'assistant vous permet d'examiner les paramètres de votre instance. Si vous avez besoin de modifier les paramètres, utilisez le bouton Retour. Si tous les paramètres sont corrects, choisissez Lancer.

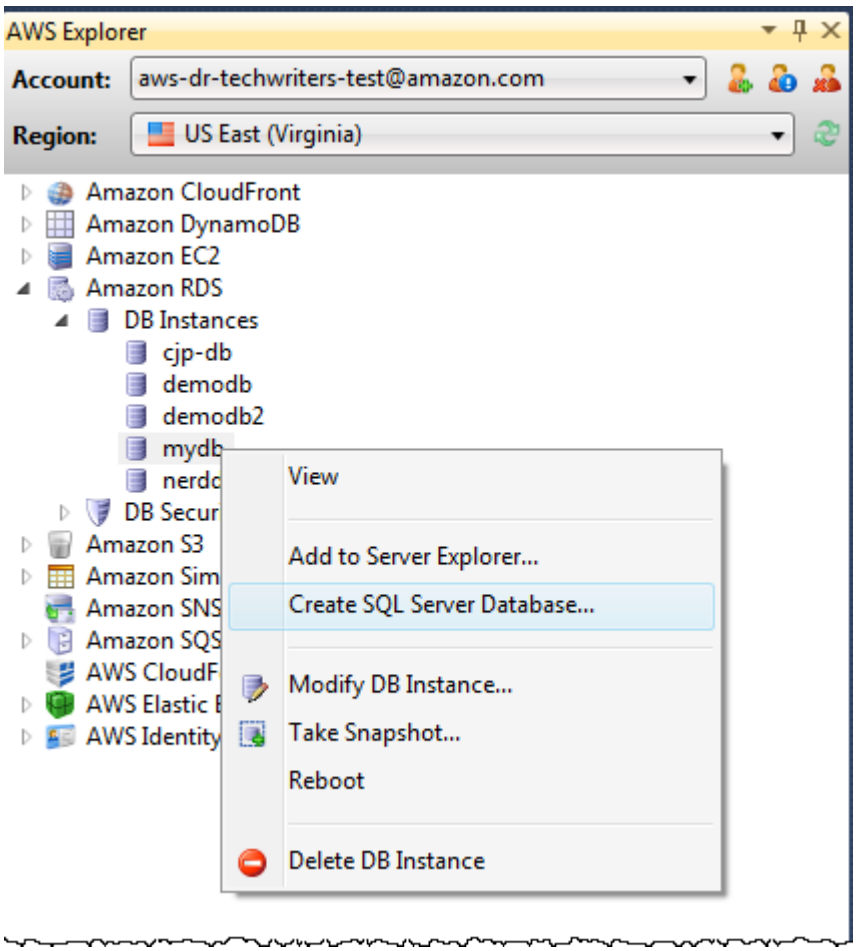
Créer une base de données Microsoft SQL Server dans une instance RDS

Microsoft SQL Server est conçu de manière à ce qu'après le lancement d'une instance Amazon RDS, vous deviez créer une base de données SQL Server dans l'instance RDS.

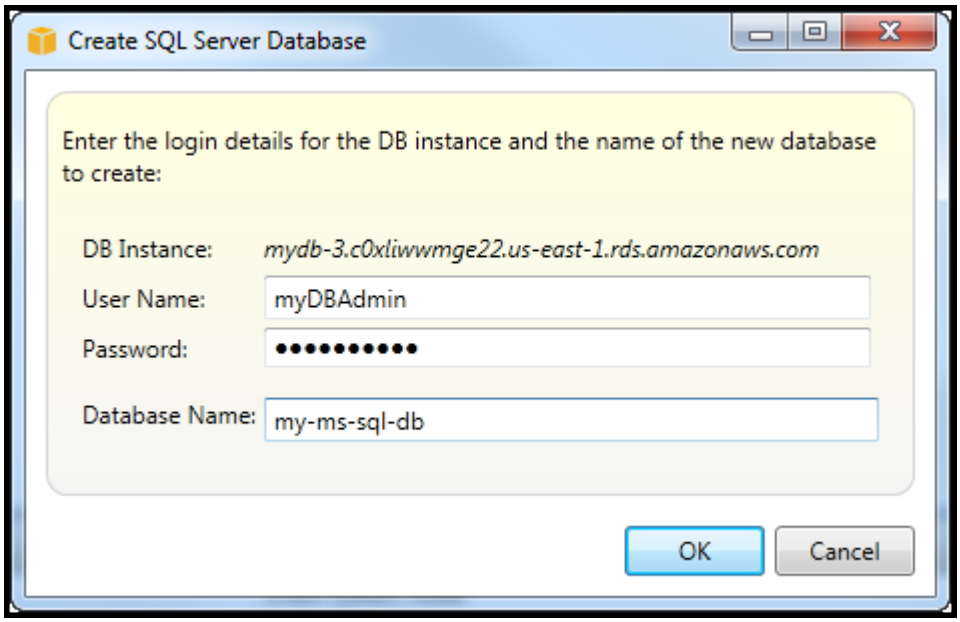
Pour plus d'informations sur la création d'une instance Amazon RDS, consultezLancer une instance de base de données Amazon RDS.

Pour créer une base de données Microsoft SQL Server

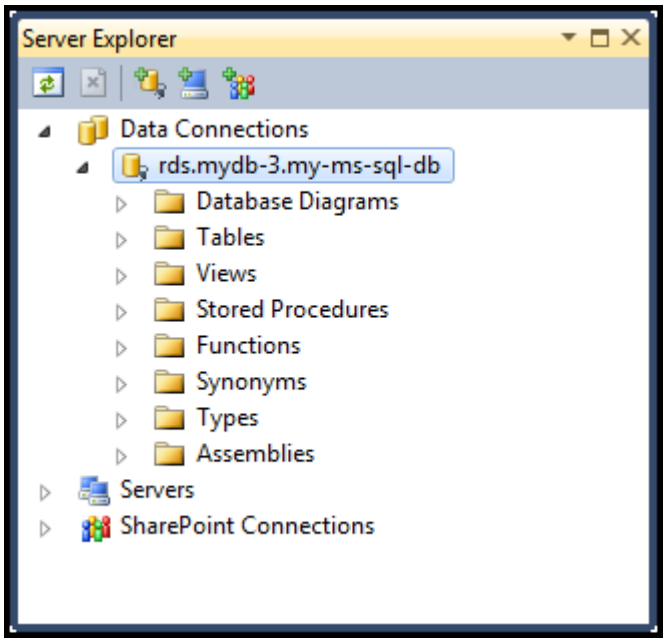
1. DansAWSExplorer, ouvrez le menu contextuel (clic droit) du nœud correspondant à votre instance RDS pour Microsoft SQL Server, et choisissezCréer une base de données SQL Server.



2. Dans la boîte de dialogue Create SQL Server Database (Créer une base de données SQL Server), saisissez le mot de passe spécifié lors de la création de l'instance RDS, saisissez le nom de la base de données Microsoft SQL Server, puis choisissez OK.



3. Toolkit for Visual Studio crée la base de données Microsoft SQL Server et l'ajoute au Visual Studio Server Explorer.



Groupes de sécurité Amazon RDS

Les groupes de sécurité Amazon RDS vous permettent de gérer l'accès réseau à vos instances Amazon RDS. Avec les groupes de sécurité, vous spécifiez des ensembles d'adresses IP à l'aide de la notation CIDR, et seul le trafic réseau provenant de ces adresses est reconnu par votre instance Amazon RDS.

Bien qu'ils fonctionnent de la même manière, les groupes de sécurité Amazon RDS sont différents des groupes de sécurité Amazon EC2. Il est possible d'ajouter un groupe de sécurité EC2 à votre groupe de sécurité RDS. Toutes les instances EC2 qui sont membres du groupe de sécurité EC2 sont ensuite en mesure d'accéder aux instances RDS qui sont membres du groupe de sécurité RDS.

Pour plus d'informations sur les groupes de sécurité Amazon RDS, consultez la pageGroupes de sécurité RDS. Pour plus d'informations sur les groupes de sécurité Amazon EC2, consultez la pageGuide de l'utilisateur EC2.

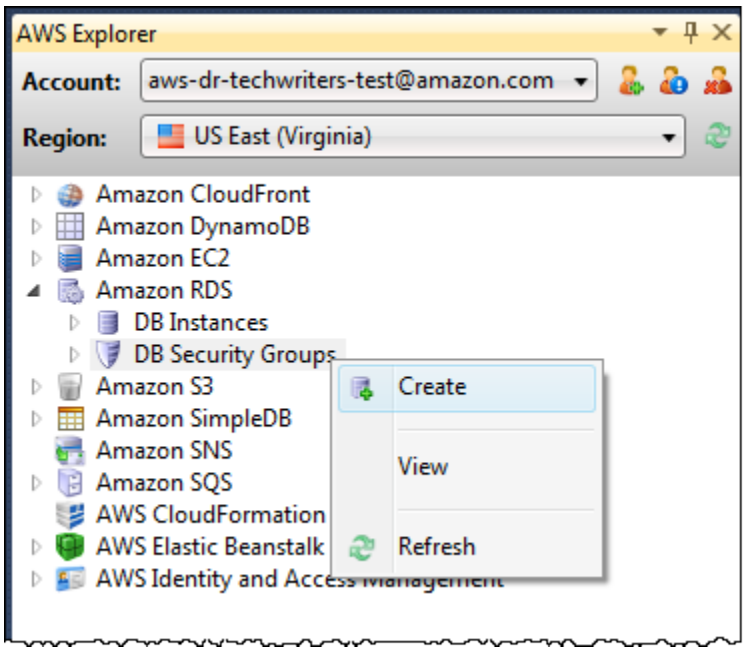
Créer un groupe de sécurité Amazon RDS

Vous pouvez utiliser Toolkit for Visual Studio pour créer un groupe de sécurité RDS. Si vous utilisez le pluginAWSToolkit pour lancer une instance RDS, l'assistant vous autorise à spécifier un groupe de

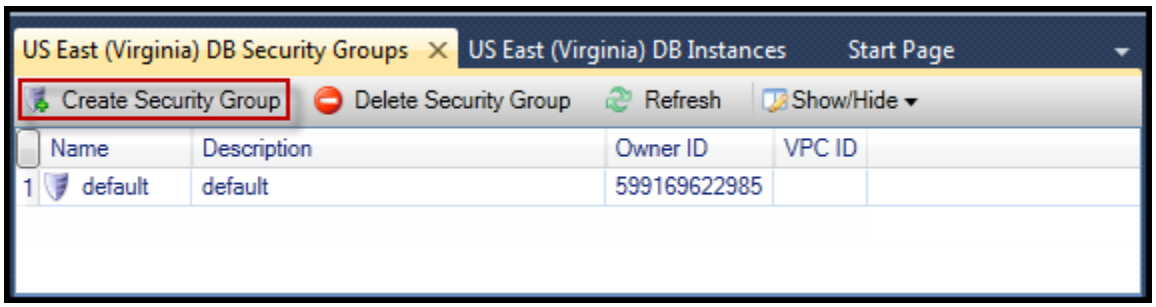
sécurité RDS pour utiliser avec votre instance. Vous pouvez utiliser la procédure suivante pour créer ce groupe de sécurité avant de lancer l'assistant.

Pour créer un groupe de sécurité Amazon RDS

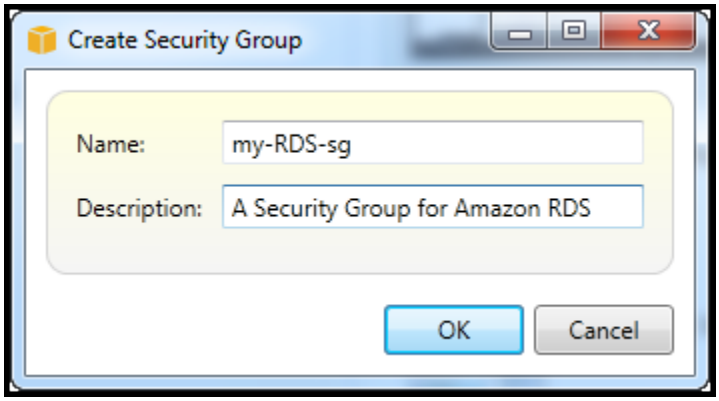
1. DansAWSExplorer, développez leAmazon RDS, ouvrez le menu contextuel (clic droit) correspondant àGroupes de sécurité DBsous-nœud et choisissezCréer.



   Sinon, dans l'onglet Groupes de sécurité, choisissez Créer un groupe de sécurité. Si cet onglet n'est pas affiché, ouvrez le menu contextuel (clic droit) du sous-nœud Groupes de sécurité DB et choisissez Afficher.



2. Dans la boîte de dialogue Créer un groupe de sécurité, saisissez le nom et la description du groupe de sécurité, puis choisissez OK.



Définir des autorisations d'accès pour un groupe de sécurité Amazon RDS

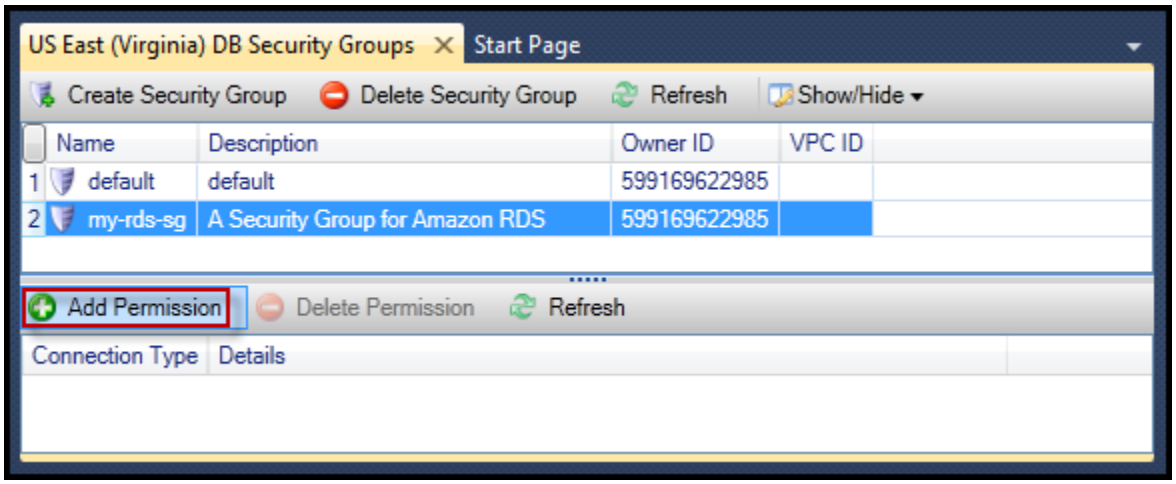
Par défaut, un nouveau groupe de sécurité Amazon RDS ne fournit aucun accès réseau. Pour activer l'accès aux instances Amazon RDS qui utilisent le groupe de sécurité, utilisez la procédure suivante pour définir ses autorisations d'accès.

Pour définir un accès au groupe de sécurité Amazon RDS

1. Dans l'onglet Groupes de sécurité, choisissez le groupe de sécurité dans la liste. Si votre groupe de sécurité n'apparaît pas dans la liste, choisissez Actualiser. Si votre groupe de sécurité n'apparaît toujours pas dans la liste, vérifiez que vous consultez la liste correspondant à la bonneAWSregion. Security Grouponglets dans leAWSLes outils sont propres à chaque région.

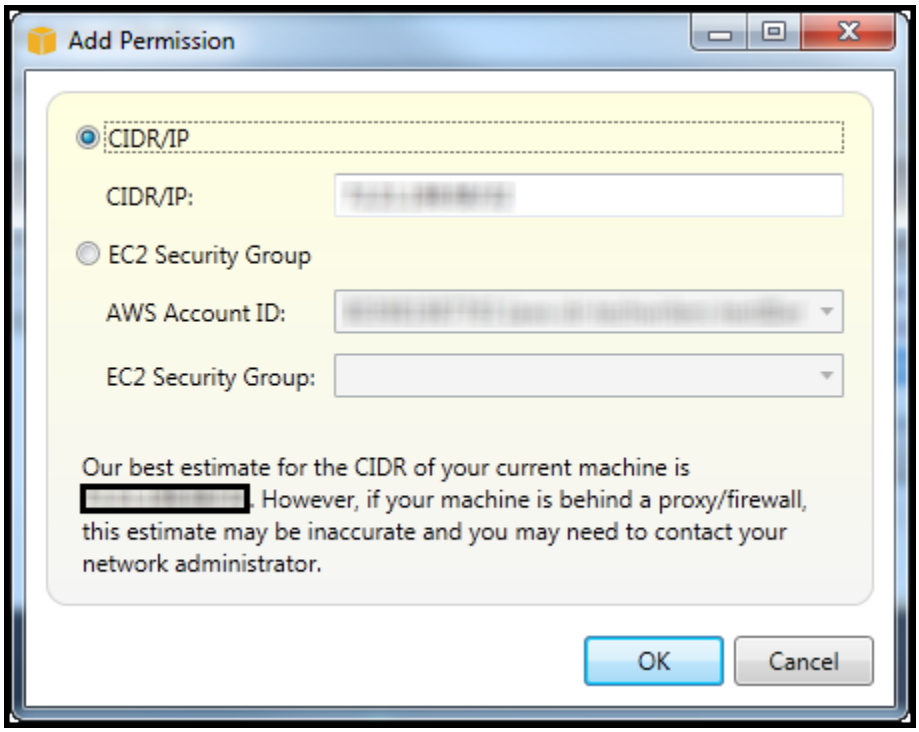
   Si nonSecurity Grouples onglets apparaissent, dansAWSExplorateur, ouvrez le menu contextuel (clic droit) correspondant à l'ongletGroupes de sécurité DBsous-nœud et choisissezAfficher.

2. Choisissez Ajouter autorisation.



Bouton Ajouter autorisation dans l'onglet Groupes de sécurité

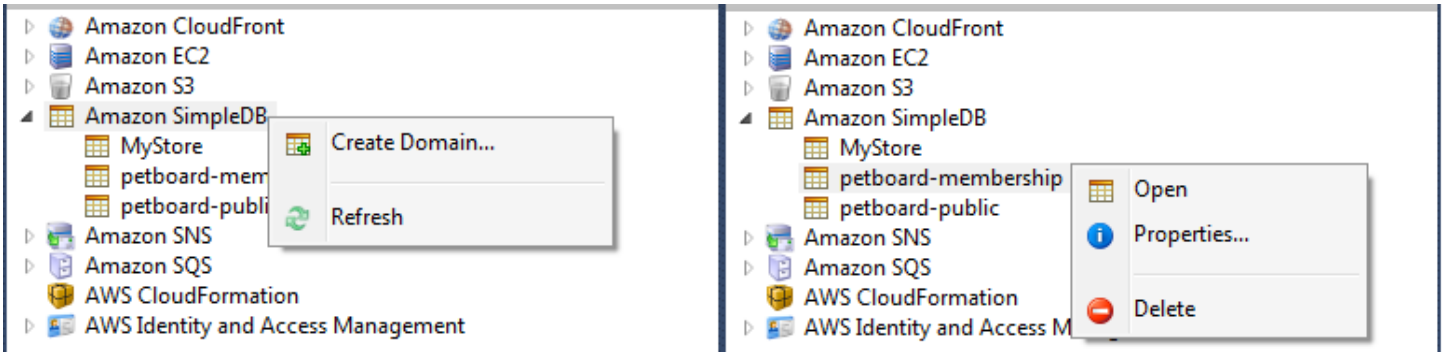
3. Dans la boîte de dialogue Ajouter autorisation, vous pouvez utiliser la notation CIDR pour spécifier les adresses IP qui peuvent accéder à votre instance RDS, ou spécifier les groupes de sécurité EC2 qui peuvent accéder à votre instance RDS. Lorsque vous choisissezGroupe de sécurité EC2, vous pouvez spécifier l'accès à toutes les instances EC2 associées à unCompte AWSavez accès ou vous pouvez choisir un groupe de sécurité EC2 dans la liste déroulante.



LeAWSToolkit tente de déterminer votre adresse IP et renseigne automatiquement la boîte de dialogue avec la spécification CIDR appropriée. Toutefois, si votre ordinateur accède à Internet via un pare-feu, l'adresse CIDR déterminée par la boîte à outils peut être inexacte.

Utiliser Amazon SimpleDB à partir deAWSExplorateur

AWSAmazon SimpleDB affiche tous les domaines Amazon SimpleDB associés à l'actifAWS. DeAWSDans Explorer, vous pouvez créer ou supprimer des domaines Amazon SimpleDB.

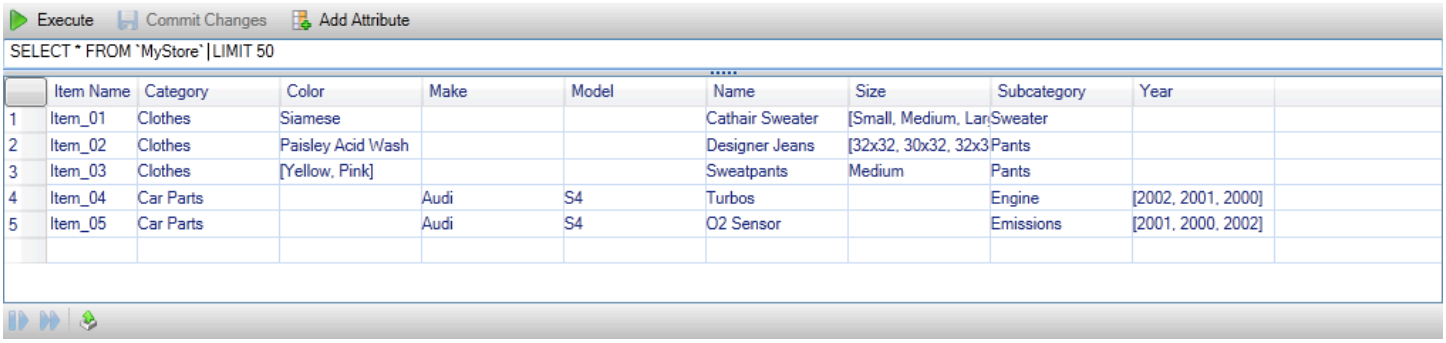


Create, delete, or open Amazon SimpleDB domains associated with your account

Exécution de requêtes et modification des résultats

AWSAmazon SimpleDB peuvent également afficher la grille d'un domaine Amazon SimpleDB de laquelle vous pouvez consulter les éléments, les attributs et les valeurs de ce dernier. Vous pouvez exécuter des requêtes afin que seul un sous-ensemble des éléments du domaine s'affiche. En cliquant deux fois sur une cellule, vous pouvez modifier les valeurs de l'attribut correspondant à cet élément. Vous pouvez également ajouter de nouveaux attributs au domaine.

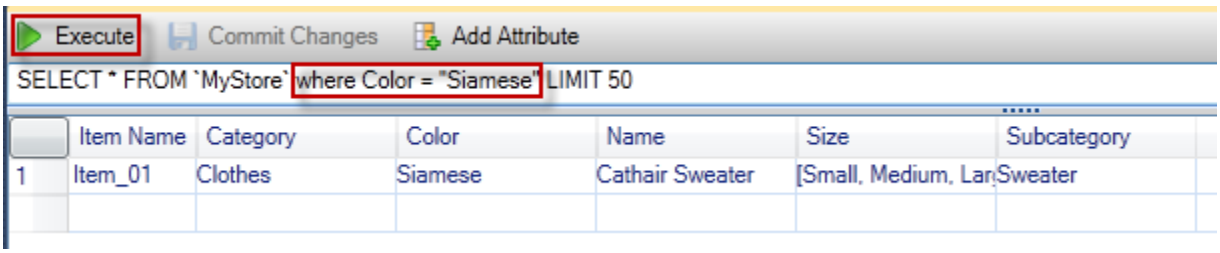
Le domaine affiché ici provient de l'exemple Amazon SimpleDB inclus avecAWS SDK for .NET.



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

Amazon SimpleDB grid view

Pour exécuter une requête, modifiez-la dans la zone de texte en haut de la vue tableau, puis choisissez Exécuter. L'affichage est filtré pour montrer uniquement les éléments correspondant à la requête.



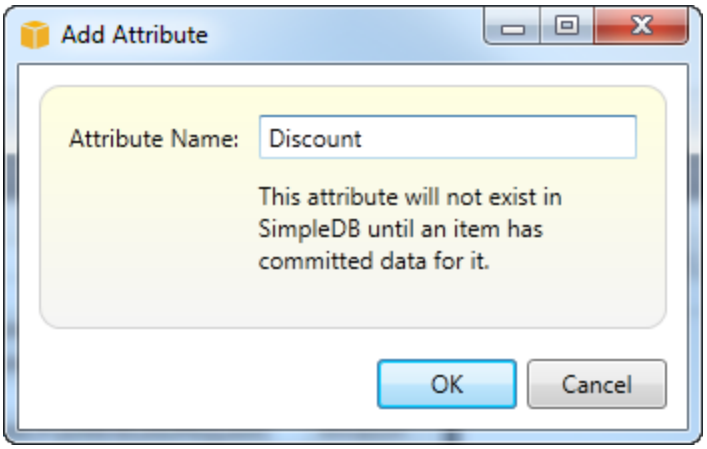
	Item Name	Category	Color	Name	Size	Subcategory
1	Item_01	Clothes	Siamese	Cathair Sweater	[Small, Medium, Lar	Sweater

Execute query from AWS Explorer

Pour modifier les valeurs associées à un attribut, cliquez deux fois sur la cellule correspondante, modifiez les valeurs, puis choisissez Valider les modifications.

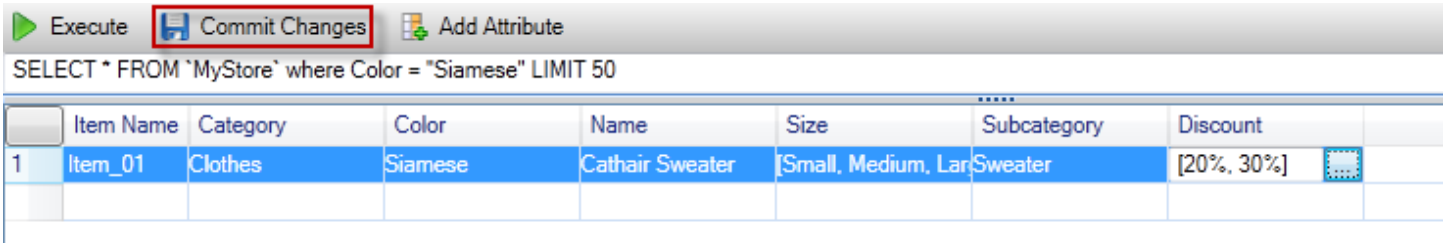
Ajout d'un attribut

Pour ajouter un attribut, en haut de la page, choisissez Ajouter un attribut.



Add Attribut dialog box

Pour que l'attribut fasse partie du domaine, vous devez ajouter une valeur à au moins un élément, puis choisir Valider les modifications.



Commit changes for a new attribute

Pagination des résultats de la requête

Trois boutons sont situés en bas de la page.

Paginate and export buttons

Les deux premiers boutons fournissent la pagination des résultats de la requête. Pour afficher une autre page de résultats, choisissez le premier bouton. Pour afficher dix autres pages de résultats, choisissez le second bouton. Dans ce contexte, une page équivaut à 100 lignes ou au nombre de résultats spécifiés par la valeur LIMIT, si elle est incluse dans la requête.

Exporter vers CSV

Le dernier bouton exporte les résultats actuels vers un fichier CSV.

Utilisation d'Amazon SQS à partir deAWSExplorateur

Amazon Simple Queue Service (Amazon SQS) est un service de file d'attente flexible qui permet de transmettre des messages entre les différents processus d'exécution dans une application logicielle. Les files d'attente Amazon SQS se trouvent dans leAWSmais les processus qui transmettent des messages peuvent être situés localement, sur des instances Amazon EC2, ou sur une combinaison d'entre elles. Amazon SQS est idéal pour coordonner la distribution du travail sur plusieurs ordinateurs.

Toolkit for Visual Studio vous permet de consulter les files d'attente Amazon SQS associées au compte actif, de créer et de supprimer des files d'attente, ainsi que d'envoyer des messages via les files d'attente. (Le compte actif correspond au compte sélectionné dansAWSExplorer.)

Pour plus d'informations, consultez la présentation d'Amazon SQS.Présentation des instances dedans leAWS.

Création d'une file d'attente

Vous pouvez créer une file d'attente Amazon SQS à partir deAWSExplorer. L'ARN et l'URL pour la file d'attente reposent sur le numéro de compte du compte actif et le nom de la file d'attente spécifié lors de la création.

Pour créer une file d'attente

1. DansAWSExplorer, ouvrez le menu contextuel (clic droit) correspondant à l'Amazon SQSnoeud, puis choisissezCréation d'une file.
2. Dans la boîte de dialogue Créer une file d'attente, spécifiez le nom de la file d'attente par défaut, le délai de visibilité par défaut et le retard de diffusion par défaut. Le délai de visibilité et le retard de diffusion par défaut sont spécifiés en quelques secondes. Le délai de visibilité par défaut correspond à la durée pendant laquelle un message est invisible pour les processus de réception potentiels, après l'acquisition du message par un processus donné. Le retard de diffusion par défaut correspond à la durée entre le moment où le message est envoyé et celui où il devient visible pour les processus de réception potentiels.
3. Choisissez OK. La nouvelle file d'attente apparaît en tant que sous-nœud sous le nœud Amazon SQS.

Suppression d'une file d'attente

Vous pouvez supprimer des files d'attente existantes à partir deAWSExplorer. Si vous supprimez une file d'attente, tous les messages associés à cette dernière ne sont plus disponibles.

Pour supprimer une file d'attente

1. DansAWSExplorer, ouvrez le menu contextuel (clic droit) de la file d'attente que vous souhaitez supprimer, puis choisissezSupprimer.

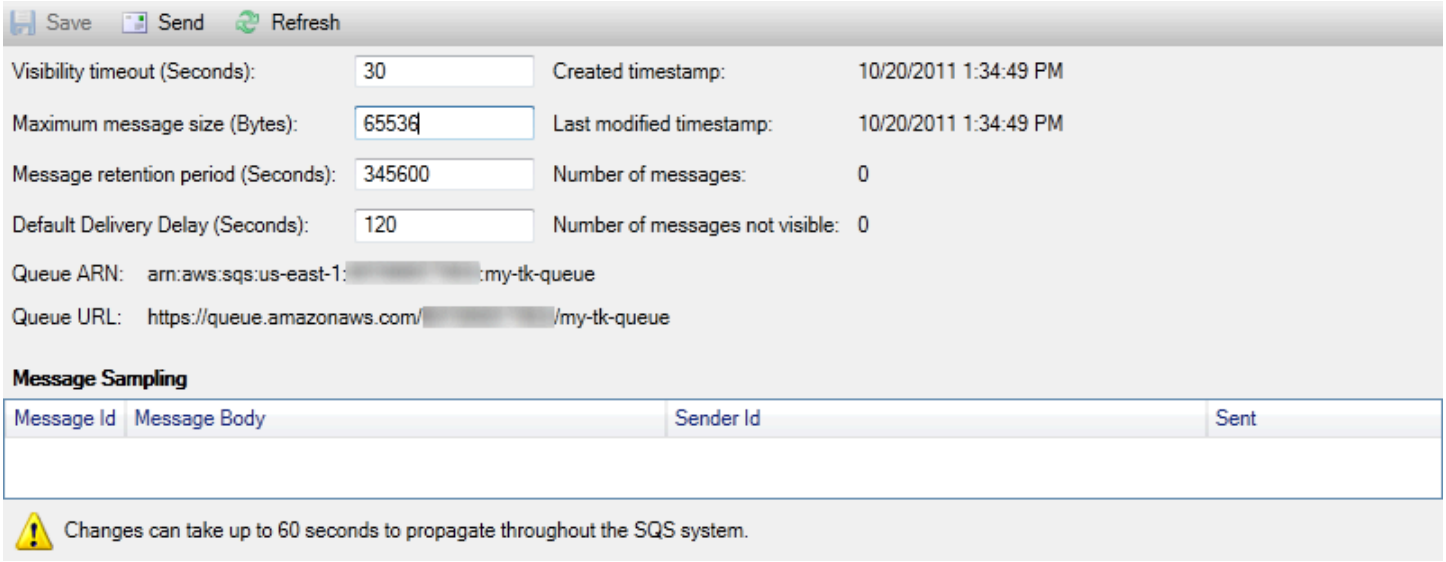
Gestion des propriétés de file d'attente

Vous pouvez afficher et modifier les propriétés de toutes les files d'attente affichées dansAWSExplorer. Dans l'affichage des propriétés, vous pouvez également envoyer des messages à la file d'attente.

Pour gérer des propriétés de file d'attente

- DansAWSExplorer, ouvrez le menu contextuel (clic droit) correspondant à la file d'attente dont vous souhaitez gérer les propriétés, puis choisissezAffichage de la file.

  Dans l'affichage des propriétés, vous pouvez modifier le délai de visibilité, la taille maximum des messages, la durée de rétention des messages et retard de diffusion par défaut. Le retard de diffusion par défaut peut être remplacé lorsque vous envoyez un message. Dans la capture d'écran suivante, le texte masqué correspond au composant du numéro de compte de l'ARN et de l'URL de la file d'attente.



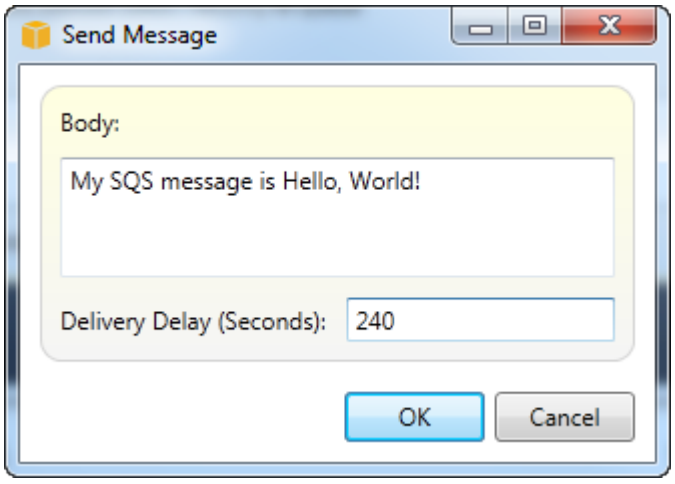
SQS queue properties view

Envoi d'un message à une file d'attente

Dans l'affichage des propriétés de la file d'attente, vous pouvez envoyer un message à cette dernière.

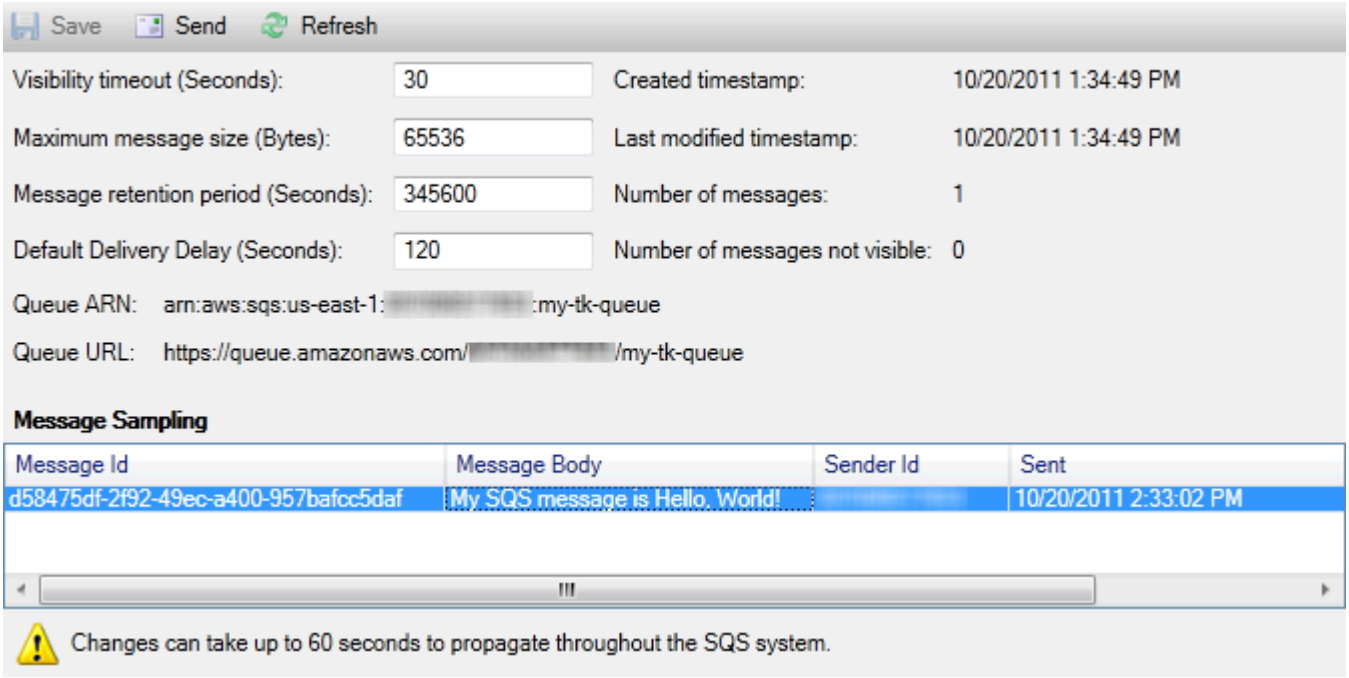
Pour envoyer un message

1. Dans la partie supérieure de l'affichage des propriétés de la file d'attente, choisissez le bouton Envoyer.
2. Saisissez le message. (Facultatif) Saisissez un retard de diffusion qui remplacera celui par défaut pour la file d'attente. Dans l'exemple suivant, nous avons remplacé le retard par une valeur de 240 secondes. Choisissez OK.



Envoyer un message dialog box

3. Patientez pendant environ 240 secondes (quatre minutes). Le message apparaît dans la section Message Sampling (Échantillonnage de message) de l'affichage des propriétés de la file d'attente.



SQS properties view with sent message

L'horodatage dans l'affichage des propriétés de la file d'attente correspond à l'heure à laquelle vous avez choisi le bouton Envoyer. Il ne tient pas compte du retard. Par conséquent, l'heure à laquelle le message apparaît dans la file d'attente et est disponible pour les destinataires peut être postérieure à cet horodatage. L'horodatage est affiché dans l'heure locale de votre ordinateur.

Identity and Access Management

AWS Identity and Access Management(IAM) vous permet de gérer l'accès à votreComptes AWSet ressources. Avec IAM, vous pouvez créer plusieurs utilisateurs dans votre principal (racine)Compte AWS. Ces utilisateurs peuvent avoir leurs propres informations d'identification : mot de passe, ID de clé d'accès et clé secrète, mais tous les utilisateurs IAM partagent un seul et même numéro de compte.

Vous pouvez gérer chaque niveau d'accès aux ressources de l'utilisateur IAM en associant des stratégies IAM à l'utilisateur. Par exemple, vous pouvez associer une stratégie à un utilisateur IAM, qui permet à celui-ci d'accéder dans votre compte au service Amazon S3 et aux ressources associées, mais pas aux autres services ou ressources.

Pour gérer les accès plus efficacement, vous pouvez créer des groupes IAM, lesquels sont des ensembles d'utilisateurs. Lorsque vous associez une stratégie à un groupe, elle s'applique à tous les utilisateurs qui appartiennent à ce groupe.

En plus de gérer les autorisations au niveau de l'utilisateur et du groupe, IAM prend également en charge le concept des rôles IAM. En plus des utilisateurs et des groupes, vous pouvez associer des stratégies aux rôles IAM. Vous pouvez ensuite associer le rôle IAM à une instance Amazon EC2. Les applications qui sont exécutées sur l'instance EC2 peuvent accéder àAWSen utilisant les autorisations fournies par le rôle IAM. Pour plus d'informations sur l'utilisation des rôles IAM avec la boîte à outils, consultez Création d'un rôle IAM. Pour plus d'informations sur IAM, accédez au manuelIAM User Guide.

Création et configuration d'un utilisateur IAM

Les utilisateurs IAM vous permettent d'accorder l'accès à votreCompte AWS. En associant des stratégies aux utilisateurs IAM, vous pouvez limiter avec précision les ressources auxquelles un utilisateur IAM peut accéder et les opérations qu'il peut effectuer sur ces ressources.

Comme il est recommandé, tous les utilisateurs qui accèdent à unCompte AWSdoivent le faire en tant qu'utilisateurs IAM, même le propriétaire du compte. Ainsi, lorsque les informations d'identification sont mises en danger pour l'un des utilisateurs IAM, il vous suffit de les désactiver. Il n'est pas nécessaire de désactiver ou modifier les informations d'identification racine du compte.

Dans Toolkit for Visual Studio, vous pouvez attribuer des autorisations à un utilisateur IAM en lui associant une stratégie IAM ou en affectant cet utilisateur à un groupe. Les utilisateurs IAM qui sont affectés à un groupe tirent leurs autorisations des stratégies associées à ce groupe. Pour plus d'informations, consultez Création d'un groupe IAM et Ajout d'un utilisateur IAM à un groupe IAM.

Toolkit for Visual Studio permet également de générer des résultatsAWSinformations d'identification (ID de clé d'accès et clé secrète) pour l'utilisateur IAM. Pour plus d'informations, consultez Génération d'informations d'identification pour un utilisateur IAM

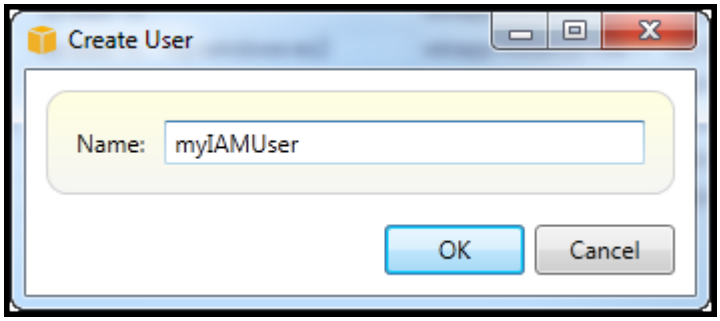
Toolkit for Visual Studio prend en charge la spécification des informations d'identification IAM pour l'accès aux services viaAWSExplorer. Etant donné que les utilisateurs IAM n'ont pas un accès total à tous les Amazon Web Services, certaines des fonctionnalités deAWSExplorer n'est peut-être pas disponible. Si vous utilisezAWSPour modifier les ressources alors que le compte actif est un utilisateur IAM, puis passer au compte racine comme compte actif, les modifications ne seront peut-

être pas visibles tant que vous n'aurez pas actualiser la vue dansAWSExplorer. Pour actualiser la vue, cliquez sur le bouton d'actualisation ().

Pour plus d'informations sur la configuration des utilisateurs IAM à partir du moduleAWS Management Console, accédez àUtilisation des utilisateurs et des groupesdans le guide de l'utilisateur d'IAM.

Pour créer un utilisateur IAM

1. DansAWSExplorer, développez leAWS Identity and Access Management, ouvrez le menu contextuel (clic droit) correspondant àUserspuis choisissezCréer un utilisateur.
2. DansCréer un utilisateur, tapez un nom pour l'utilisateur IAM et cliquez surOK.. C'est l'IAM.nom convivial. Pour plus d'informations sur les contraintes associées aux noms des utilisateurs IAM, consultez leIAM User Guide.



Create an IAM user

Le nouvel utilisateur apparaîtra en tant que sous-nœud sousUserssousAWS Identity and Access Managementnœud.

Pour plus d'informations sur la manière de créer une stratégie et de l'associer à l'utilisateur, consultez Création d'une stratégie IAM.

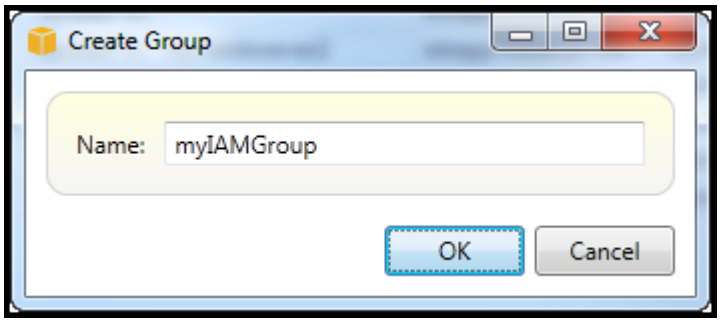
Création d'un groupe IAM

Les groupes permettent d'appliquer des stratégies IAM à un ensemble d'utilisateurs. Pour plus d'informations sur la gestion des utilisateurs et groupes IAM, accédez àUtilisation des utilisateurs et des groupesdans le guide de l'utilisateur d'IAM.

Pour créer un groupe IAM

1. DansAWSExplorer, sousIdentity and Access Management, ouvrez le menu contextuel (clic droit) correspondant àGroups (Groupes)et choisissezCréation d'un groupe.

2. DansCréation d'un groupe, tapez un nom pour le groupe IAM et cliquez surOK..



Create IAM group

Le nouveau groupe IAM apparaîtra sous leGroups (Groupes)sous-nœud deIdentity and Access Management.

Pour plus d'informations sur la manière de créer une stratégie et de l'associer au groupe IAM, consultezCréation d'une stratégie IAM.

Ajout d'un utilisateur IAM à un groupe IAM

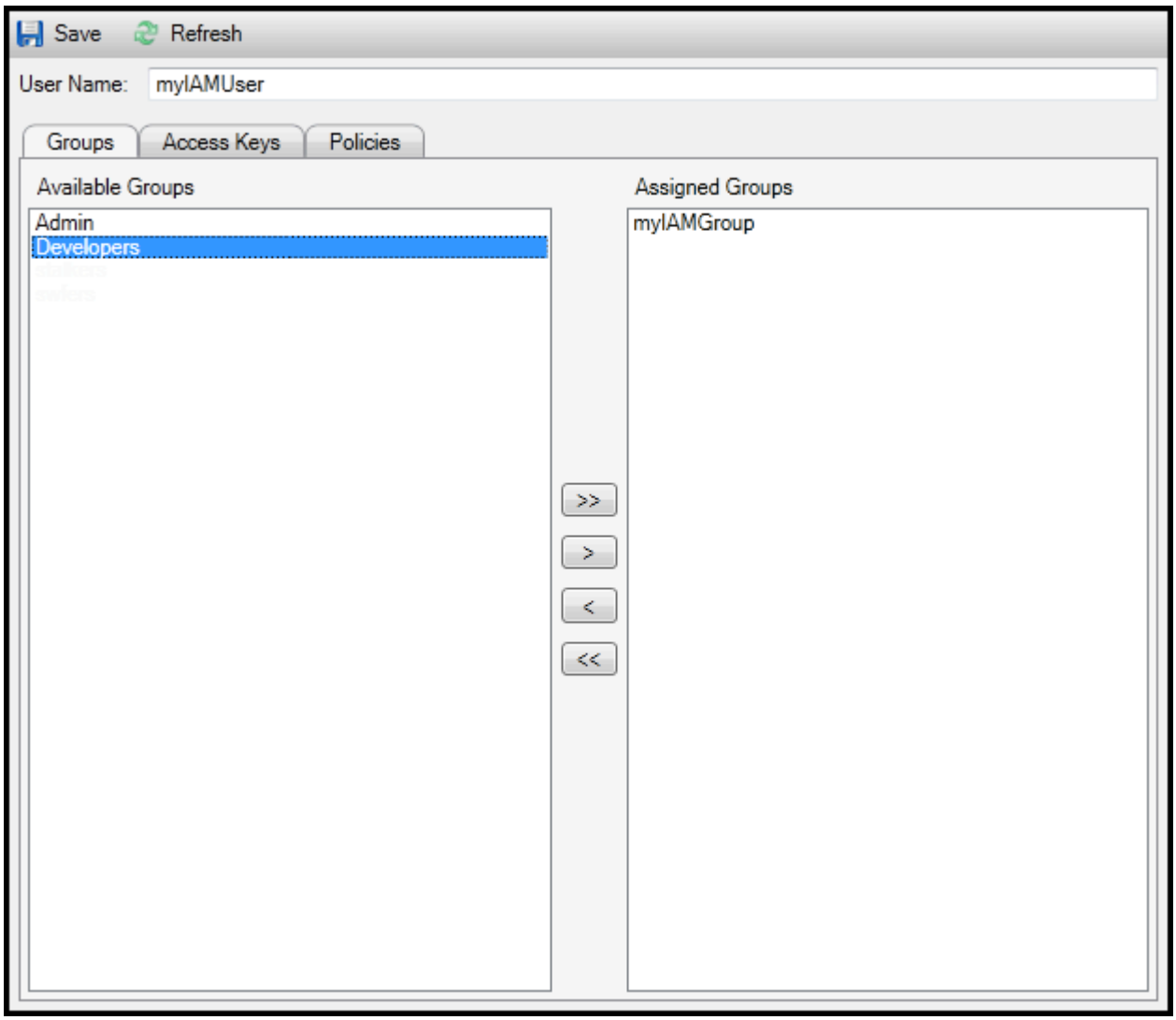
Les utilisateurs IAM qui appartiennent à un groupe IAM tirent leurs autorisations d'accès des stratégies associées à ce groupe. L'objectif d'un groupe IAM est de faciliter la gestion des autorisations pour un ensemble d'utilisateurs IAM.

Pour plus d'informations sur la manière dont les stratégies associées à un groupe IAM interagissent avec les stratégies associées aux utilisateurs IAM de ce groupe IAM, consultezGestion des stratégies IAM dans le Guide de l'utilisateur IAM.

DansAWSExplorer, vous ajoutez des utilisateurs IAM aux groupes IAM à partir du moduleUserssous-nœud, pas le sous-nœudGroups (Groupes)sous-nœud.

Pour ajouter un utilisateur IAM à un groupe IAM

1. DansAWSExplorer, sousIdentity and Access Management, ouvrez le menu contextuel (clic droit) correspondant àUserset choisissezModifier.



Assign an IAM user to a IAM group

2. Volet de gauche de laGroups (Groupes)affiche les groupes IAM disponibles. Le volet droit affiche les groupes auxquels l'utilisateur IAM spécifié appartient déjà.

   Pour ajouter l'utilisateur IAM à un groupe, choisissez le groupe IAM dans le volet gauche, puis cliquez sur le bouton**>**.

   Pour supprimer l'utilisateur IAM dans un groupe, choisissez le groupe IAM dans le volet droit, puis cliquez sur le bouton**<**.

   Pour ajouter l'utilisateur IAM à tous les groupes IAM, cliquez sur le bouton**>>**. De même, pour supprimer l'utilisateur IAM dans tous les groupes, choisissez le**<<**.

Pour sélectionner plusieurs groupes, sélectionnez-les en séquence. Vous n'avez pas besoin de maintenir la touche Ctrl enfoncée. Pour effacer un groupe dans votre sélection, sélectionnez-le une deuxième fois.

3. Lorsque vous avez terminé d'affecter l'utilisateur IAM à des groupes IAM, choisissezEnregistrer.

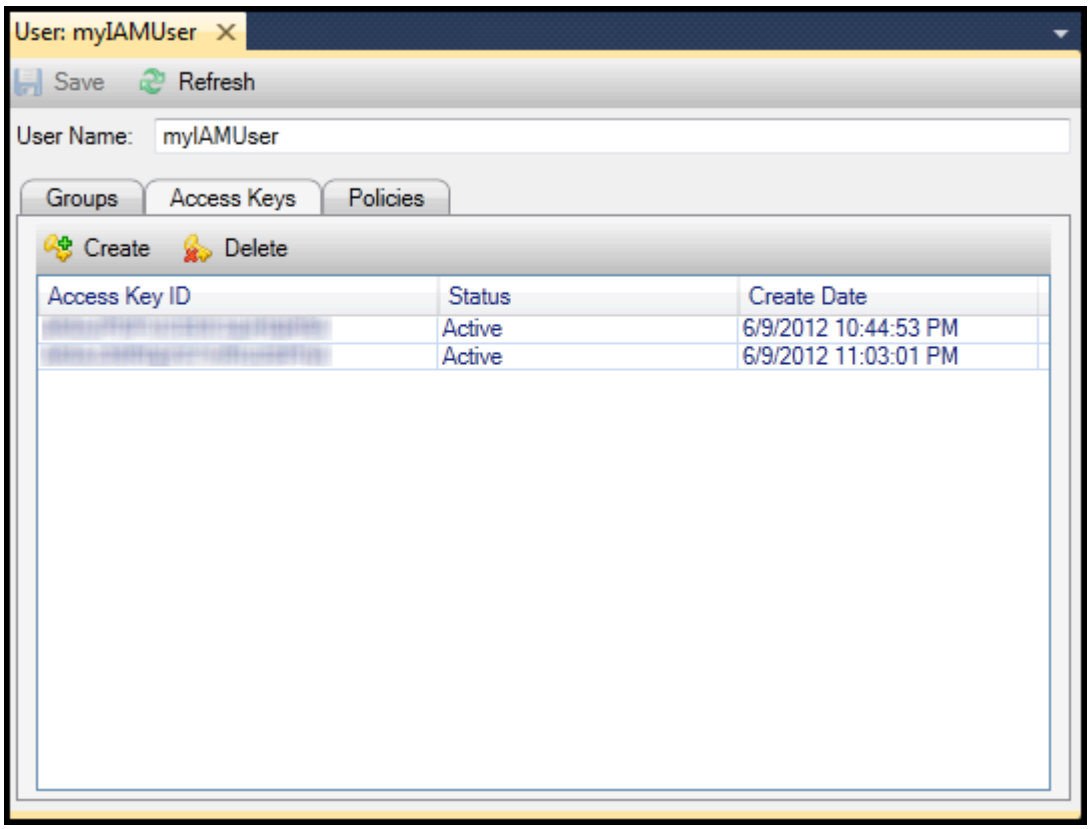
Génération d'informations d'identification pour un utilisateur IAM

Avec Toolkit for Visual Studio, vous pouvez générer l'ID de clé d'accès et la clé secrète utilisés pour effectuer des appels d'API versAWS. Ces clés peuvent également être spécifiées pour accéder à Amazon Web Services via Toolkit. Pour en savoir plus sur la spécification des informations d'identification à utiliser avec la boîte à outils, consultez les informations d'identification. Pour plus d'informations sur la manière de gérer les informations d'identification en toute sécurité, consultezBonnes pratiques pour la gestionAWSClés d'accès.

Toolkit ne peut pas être utilisé pour générer un mot de passe pour un utilisateur IAM.

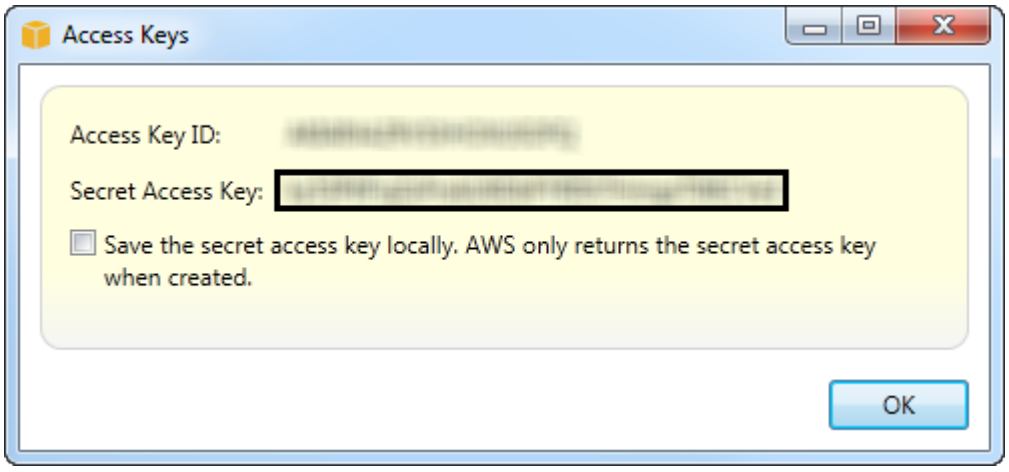
Pour générer des informations d'identification pour un utilisateur IAM

1. DansAWSExplorer, ouvrez le menu contextuel d'un utilisateur IAM en cliquant sur le bouton droit de la souris et choisissezModifier.



2. Pour générer des informations d'identification, choisissez Créer dans l'onglet Clés d'accès.

   Vous ne pouvez générer que deux jeux d'informations d'identification par utilisateur IAM. Si vous avez déjà deux jeux d'informations d'identification et que vous avez besoin de créer un jeu supplémentaire, vous devez supprimer l'un des jeux existants.



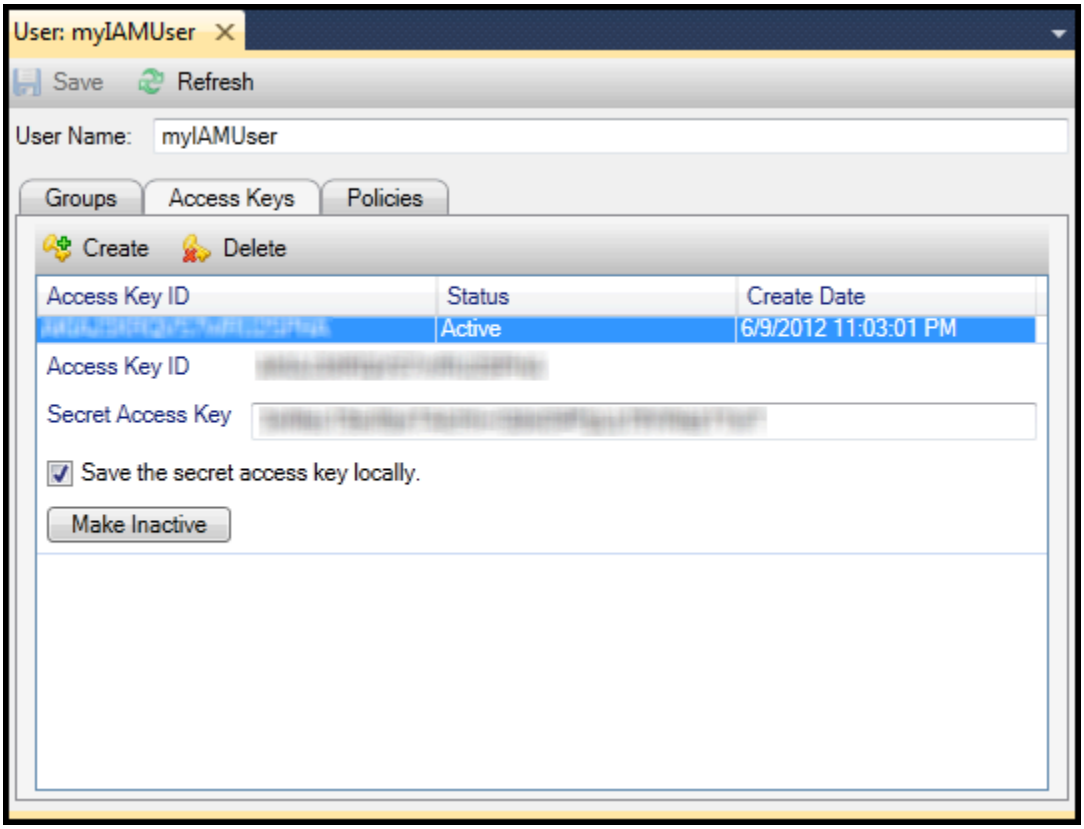
   reate credentials for IAM user

   Si vous souhaitez que Toolkit enregistre une copie chiffrée de votre clé d'accès secrète sur votre disque local, sélectionnezEnregistrez la clé d'accès secrète localement.AWSrenvoie la clé d'accès

secrète uniquement lorsqu'elle est créée.. Vous pouvez également copier la clé d'accès secrète à partir de la boîte de dialogue et l'enregistrer dans un emplacement sûr.

3. Choisissez OK.

Une fois que vous avez généré les informations d'identification, vous pouvez les afficher dans l'onglet Clés d'accès. Si vous avez choisi que la boîte à outils enregistre la clé secrète localement, elle sera affichée ici.



Create credentials for IAM user

Si vous avez enregistré la clé secrète vous-même et que vous souhaitez aussi que la boîte à outils l'enregistre, tapez la clé d'accès secrète dans la zone Clé d'accès secrète, puis sélectionnez Save the secret access key locally (Enregistrer la clé d’accès secrète localement).

Pour désactiver les informations d'identification, choisissez Rendre inactif. (Vous pouvez le faire si vous pensez que les informations d'identification ont été mises en danger. Vous pouvez réactiver les informations d'identification si vous recevez la confirmation qu'ils sont sécurisés.)

Créer un rôle IAM

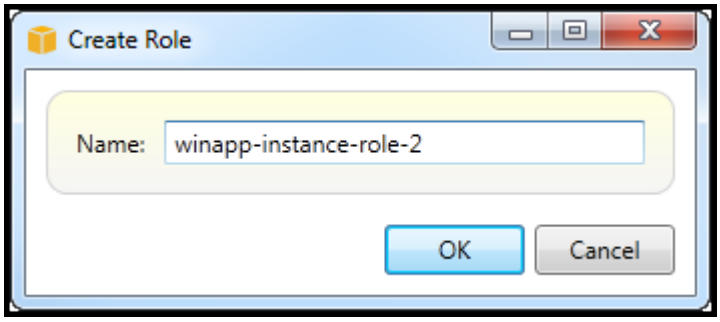
Toolkit for Visual Studio prend en charge la création et la configuration des rôles IAM. Tout comme avec les utilisateurs et les groupes, vous pouvez associer des stratégies aux rôles IAM. Vous pouvez ensuite associer le rôle IAM à une instance Amazon EC2. L'association avec l'instance EC2 est gérée par le biais d'un profil d'instance, qui est un conteneur logique du rôle. Les applications qui s'exécutent sur l'instance EC2 reçoivent automatiquement le niveau d'accès spécifié par la stratégie associée au rôle IAM. Cela est vrai même lorsque l'application n'a pas spécifié d'autres élémentsAWSInformations d'identification .

Par exemple, vous pouvez créer un rôle et associer une stratégie à ce rôle qui ne limite l'accès qu'à Amazon S3. Après avoir associé ce rôle à une instance EC2, vous pouvez ensuite exécuter une application sur cette instance et celle-ci pourra accéder à Amazon S3, mais pas aux autres services ou ressources. L'avantage de cette approche est que vous n'avez pas besoin de vous soucier de transférer et stocker de manière sécurisée.AWSinformations d'identification sur l'instance EC2.

Pour plus d'informations sur les rôles IAM, accédez àUtilisation des rôles IAM dans le Guide de l'utilisateur IAM. Pour des exemples de programmes accédant àAWSà l'aide du rôle IAM associé à une instance Amazon EC2, accédez auAWSguides de développement pourJava,.NET,PHP, et Ruby (Définition d'informations d'identification avec IAM,Création d'un rôle IAM, etUtilisation des stratégies IAM).

Pour créer un rôle IAM

1. DansAWSExplorer, sousIdentity and Access Management, ouvrez le menu contextuel (clic droit) correspondant àRôlespuis choisissezCréation de rôles.
2. DansCréation d'un rôle, tapez un nom pour le rôle IAM et cliquez surOK..



Create IAM role

Le nouveau rôle IAM apparaîtra sousRôlesdansIdentity and Access Management.

Pour plus d'informations sur la manière de créer une stratégie et de l'associer au rôle, consultez Create an IAM Policy (Créer une stratégie IAM).

Création d'une stratégie IAM

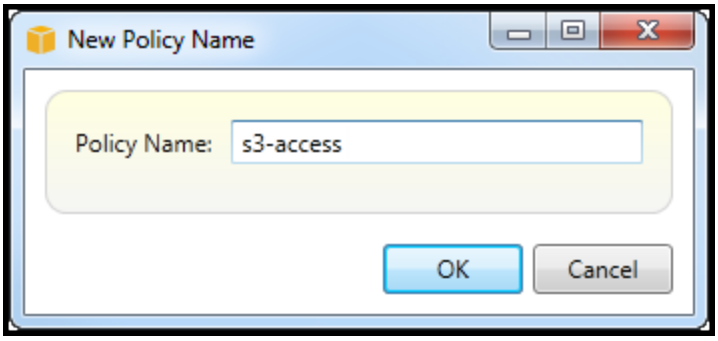
Les stratégies sont essentielles à l'IAM. Les stratégies peuvent être associées à IAMentitéstels que les utilisateurs, les groupes ou les rôles. Ces stratégies spécifient le niveau d'accès autorisé pour un utilisateur, un groupe ou un rôle.

Pour créer une stratégie IAM

DansAWSExplorer, développez leAWS Identity and Access Management, puis développez le nœud correspondant au type d'entité (Groups (Groupes),Rôles, ouUsers) auquel vous allez attacher la politique. Par exemple, ouvrez le menu contextuel d'un rôle IAM et cliquez surModifier.

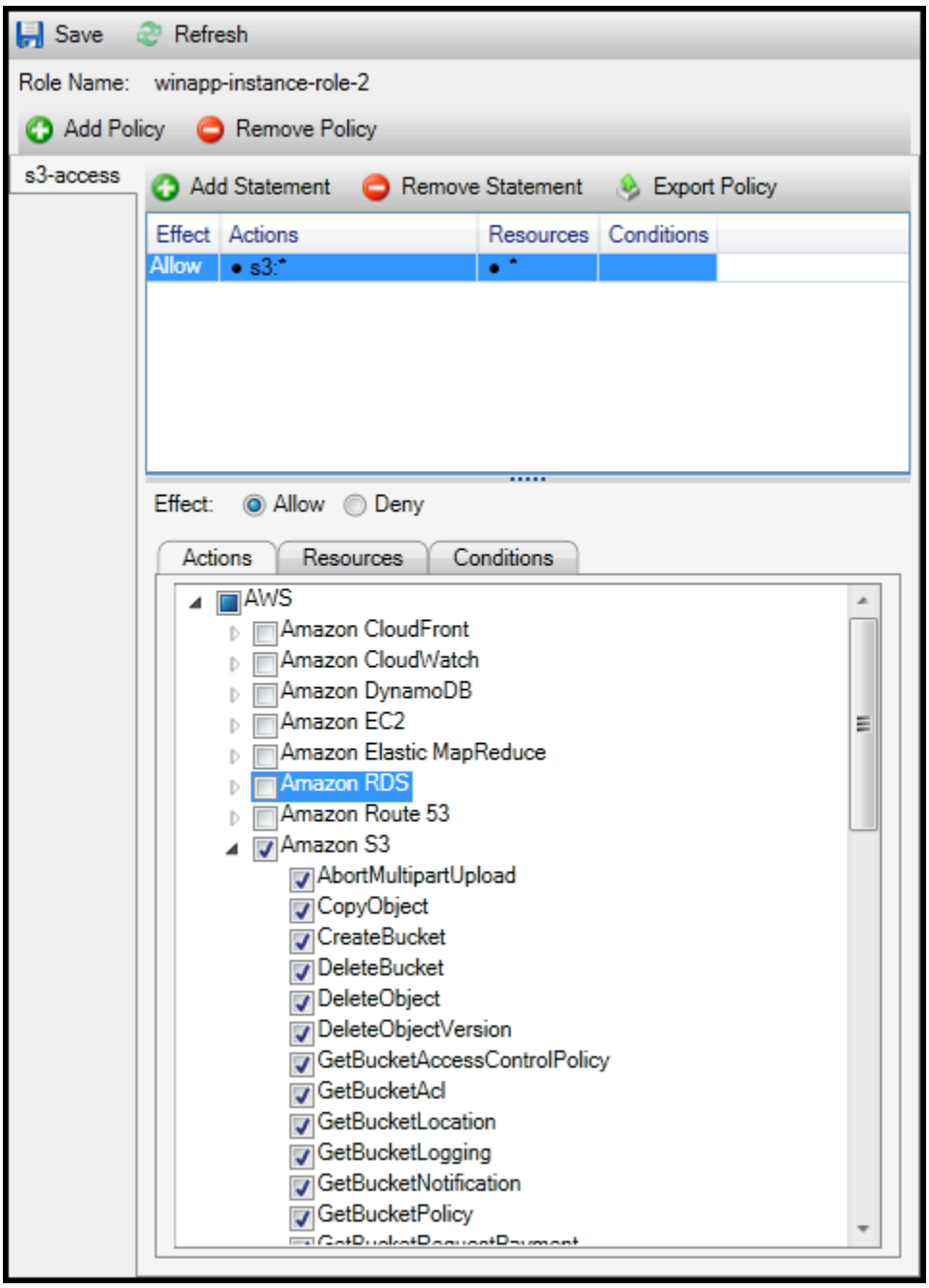
Un onglet associé au rôle apparaît alors dans le menuAWSExplorer. Cliquez sur le lien Ajouter une stratégie.

Dans la boîte de dialogue New Policy Name (Nouveau nom de la stratégie), saisissez un nom pour la stratégie (par exemple, s3-access).



New Policy Name dialog box

Dans l'éditeur de stratégie, ajoutez les déclarations de stratégie afin de spécifier le niveau d'accès à attribuer au rôle (dans l'exemple ci-dessous, le nom de rôle winapp-instance-role-2 est associé à la stratégie). Dans cet exemple, une stratégie fournit un accès complet à Amazon S3, mais aucun accès aux autres ressources.



Specify IAM policy

Pour affiner le contrôle d'accès, vous pouvez étendre les sous-nœuds dans l'éditeur de stratégie afin d'autoriser ou d'interdire les actions associées à Amazon Web Services.

Après avoir modifié la stratégie, cliquez sur le lien Enregistrer.

AWS Lambda

Développez et déployez vos fonctions Lambda C# basées sur .NET Core avec le. AWS Toolkit for Visual Studio AWS Lambda est un service de calcul qui vous permet d'exécuter du code sans provisionner ni gérer de serveurs. Le Toolkit for Visual Studio inclut des modèles de projet AWS Lambda .NET Core pour Visual Studio.

Pour plus d'informations AWS Lambda, consultez le guide du développeur AWS Lambda.

Pour plus d'informations sur .NET Core, consultez le guide Microsoft .NET Core. Pour obtenir les prérequis et les instructions d'installations de .NET Core concernant les plateformes Windows, macOS et Linux, consultez Téléchargements .NET Core.

Les rubriques suivantes décrivent comment AWS Lambda utiliser le Toolkit for Visual Studio.

Rubriques

AWS Lambda Projet de base

Vous pouvez créer une fonction Lambda à l'aide de modèles de projet Microsoft .NET Core, dans le. AWS Toolkit for Visual Studio

Création d'un projet Lambda Visual Studio .NET Core

Vous pouvez utiliser les modèles et les plans Lambda-Visual Studio pour accélérer l'initialisation de votre projet. Les plans Lambda contiennent des fonctions prédéfinies qui simplifient la création d'une base de projet flexible.

> **Note**
>
> Le service Lambda impose des limites de données pour différents types de packages. Pour des informations détaillées sur les limites de données, consultez la rubrique Quotas Lambda dans le Guide de l'utilisateur AWS Lambda.

Pour créer un projet Lambda dans Visual Studio

1. Dans Visual Studio, développez le menu Fichier, développez Nouveau, puis choisissez Projet.
2. Dans la boîte de dialogue Nouveau projet, définissez les listes déroulantes Langue, plate-forme et type de projet sur « Tous », puis saisissez le aws lambda texte dans le champ Rechercher. Choisissez le modèle AWS Lambda Project (.NET Core - C#).
3. Dans le champ Nom, entrez**`AWSLambdaSample`**, spécifiez l'emplacement du fichier souhaité, puis choisissez Créer pour continuer.
4. Sur la page Sélectionner un plan, sélectionnez le plan de fonction vide, puis choisissez Terminer pour créer le projet Visual Studio.

Vérification des fichiers du projet

Il y a deux dossiers de projet à examiner : `aws-lambda-tools-defaults.json` et`Function.cs`.

L'exemple suivant montre le `aws-lambda-tools-defaults.json` fichier, qui est automatiquement créé dans le cadre de votre projet. Vous pouvez définir les options de construction à l'aide des champs de ce fichier.

> **Note**
>
> Les modèles de projet dans Visual Studio contiennent de nombreux champs différents, prenez note des points suivants :
>
> - function-handler : spécifie la méthode qui s'exécute lorsque la fonction Lambda s'exécute
> - La spécification d'une valeur dans le champ du gestionnaire de fonctions préremplit cette valeur dans l'assistant de publication.
> - Si vous renommez la fonction, la classe ou l'assemblage, vous devez également mettre à jour le champ correspondant dans le `aws-lambda-tools-defaults.json` fichier.

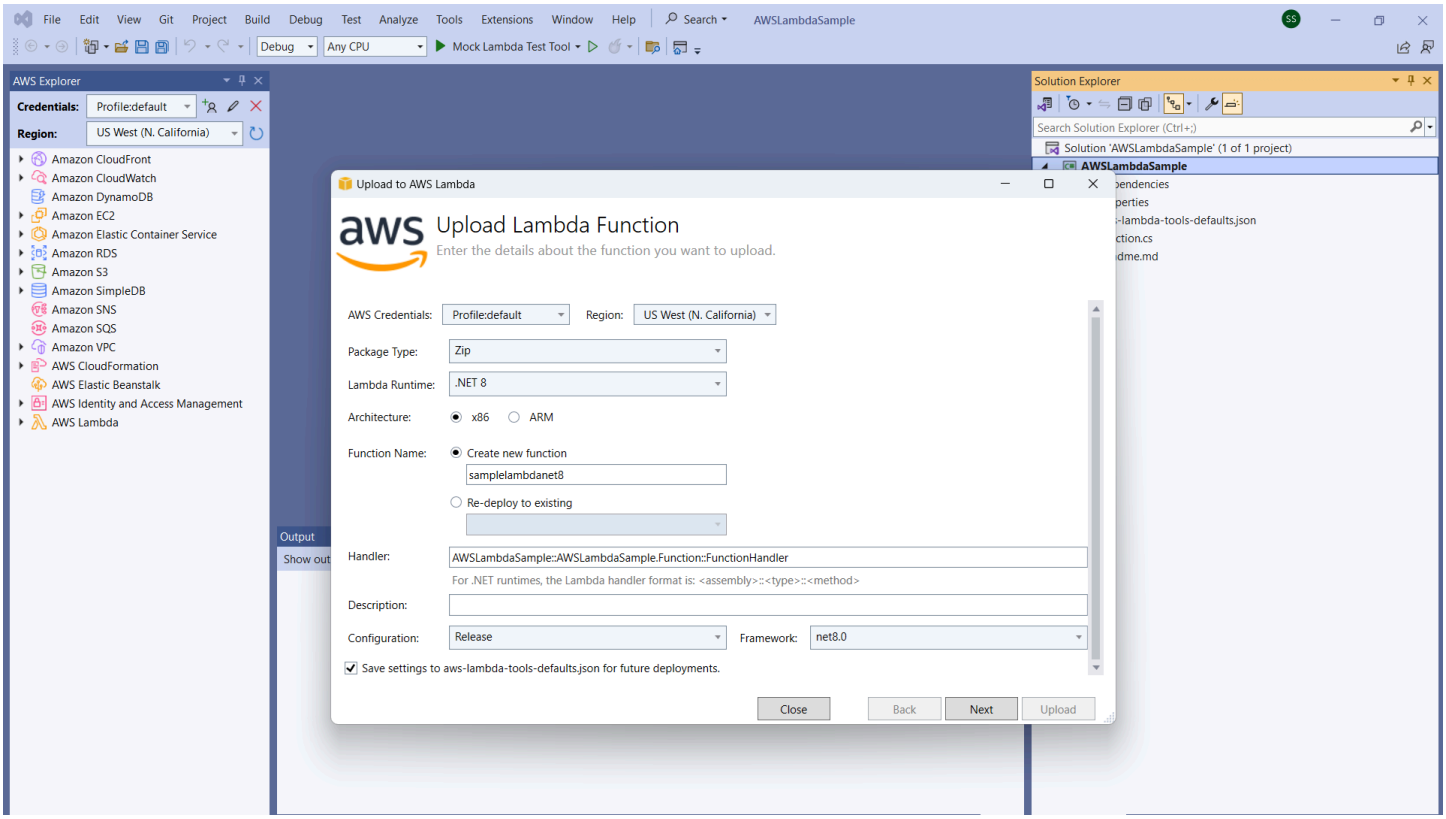
```
{
  "Information": [
    "This file provides default values for the deployment wizard inside Visual Studio
 and the AWS Lambda commands added to the .NET Core CLI.",
    "To learn more about the Lambda commands with the .NET Core CLI execute the
 following command at the command line in the project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

Examinez le `Function.cs` fichier. `Function.cs`définit les fonctions c# à exposer en tant que fonctions Lambda. Il s'`FunctionHandler`agit de la fonctionnalité Lambda qui s'exécute lorsque la fonction Lambda est exécutée. Dans ce projet, une fonction est définie :`FunctionHandler`, qui fait appel `ToUpper()` au texte saisi.

Votre projet est maintenant prêt à être publié sur Lambda.

Publier sur Lambda

La procédure et l'image suivantes montrent comment télécharger votre fonction sur Lambda à l'aide du. AWS Toolkit for Visual Studio



Publication de votre fonction sur Lambda

1. Accédez à l' AWS explorateur en développant View et en choisissant AWS Explorer.
2. Dans l'explorateur de solutions, ouvrez le menu contextuel (cliquez avec le bouton droit) du projet que vous souhaitez publier, puis choisissez Publier sur AWS Lambda pour ouvrir la fenêtre Upload Lambda Function.
3. Dans la fenêtre Upload Lambda Function, renseignez les champs suivants :

    a. Type de package : Choisissez**`Zip`**. Un fichier ZIP sera créé à la suite du processus de construction et sera téléchargé sur Lambda. Vous pouvez également choisir le type de package**`Image`**. Le didacticiel : Basic Lambda Project Creating Docker Image décrit comment publier à l'aide du type de package. **`Image`**

    b. Lambda Runtime : Choisissez votre Lambda Runtime dans le menu déroulant.

    c. Architecture : sélectionnez le radial correspondant à votre architecture préférée.

    d. Nom de la fonction : sélectionnez le radial pour Créer une nouvelle fonction, puis entrez un nom d'affichage pour votre instance Lambda. Ce nom est référencé à la fois par l' AWS explorateur et par AWS Management Console les écrans.

e. Gestionnaire : utilisez ce champ pour spécifier un gestionnaire de fonctions. Par exemple : **`AWSLambdaSample::AWSLambdaSample.Function::FunctionHandler`**.

f. (Facultatif) Description : entrez le texte descriptif à afficher avec votre instance, depuis le AWS Management Console.

g. Configuration : Choisissez votre configuration préférée dans le menu déroulant.

h. Cadre : choisissez votre cadre préféré dans le menu déroulant.

i. Enregistrer les paramètres : cochez cette case pour enregistrer vos paramètres actuels `aws-lambda-tools-defaults.json` comme paramètres par défaut pour les futurs déploiements.

j. Choisissez Suivant pour accéder à la fenêtre Détails des fonctions avancées.

4. Dans la fenêtre Détails des fonctions avancées, renseignez les champs suivants :

a. Nom du rôle : Choisissez un rôle associé à votre compte. Le rôle fournit des informations d'identification temporaires pour tous les appels de AWS service effectués par le code de la fonction. Si vous n'avez pas de rôle, faites défiler la page jusqu'à trouver Nouveau rôle basé sur la politique AWS gérée dans le sélecteur déroulant, puis choisissez AWSLambdaBasicExecutionRole. Ce rôle dispose d'autorisations d'accès minimales.

> **Note**
>
> Votre compte doit être autorisé à exécuter l' ListPolicies action IAM, sinon la liste des noms de rôle sera vide et vous ne pourrez pas continuer.

b. (Facultatif) Si votre fonction Lambda accède aux ressources d'un Amazon VPC, sélectionnez les sous-réseaux et les groupes de sécurité.

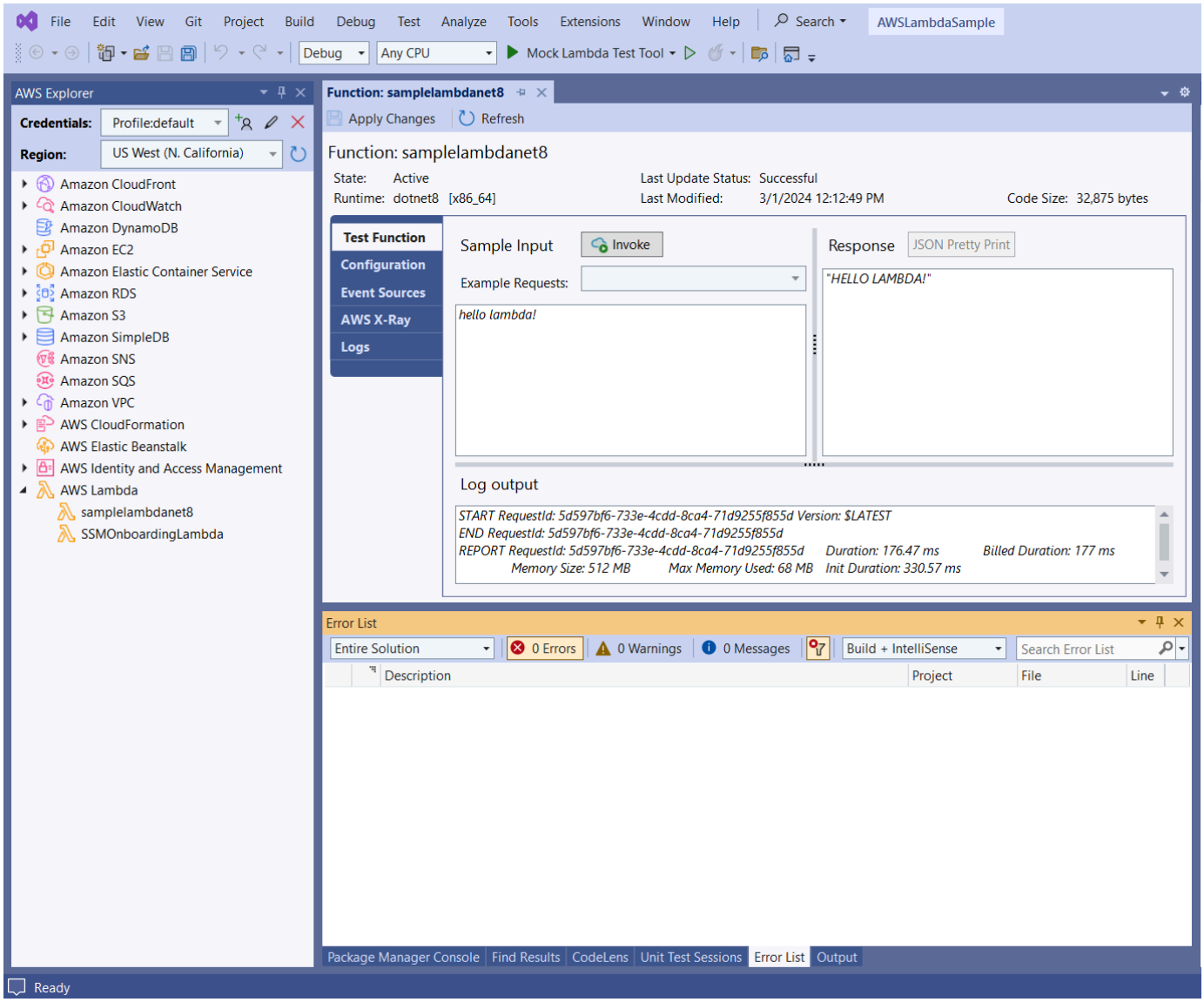
c. (Facultatif) Définissez les variables d'environnement dont votre fonction Lambda a besoin. Les clés sont automatiquement cryptées par la clé de service par défaut qui est gratuite. Vous pouvez également spécifier une AWS KMS clé payante. KMS est un service géré qui permet de créer et contrôler les clés de chiffrement utilisées pour chiffrer vos données. Si vous avez une AWS KMS clé, vous pouvez la sélectionner dans la liste.

5. Choisissez Upload pour ouvrir la fenêtre de la fonction de téléchargement et commencer le processus de téléchargement.

> **Note**
>
> La page Fonction de téléchargement s'affiche lorsque la fonction est en cours de téléchargement vers. AWS Pour que l'assistant reste ouvert après le téléchargement afin que vous puissiez consulter le rapport, décochez la case Fermer automatiquement l'assistant en cas de réussite au bas du formulaire avant la fin du téléchargement.
> Une fois la fonction téléchargée, votre fonction Lambda est active. La page Function : view s'ouvre et affiche la configuration de votre nouvelle fonction Lambda.

6. Dans l'onglet Fonction de test, entrez `hello lambda!` dans le champ de saisie de texte, puis choisissez Invoke pour appeler manuellement votre fonction Lambda. Votre texte apparaît dans l'onglet Réponse, converti en majuscules.

> **Note**
>
> Vous pouvez rouvrir la vue Function : à tout moment en double-cliquant sur votre instance déployée située dans l'AWS explorateur sous le AWS Lambdanœud.



7. (Facultatif) Pour vérifier que vous avez correctement publié votre fonction Lambda, connectez-vous au, AWS Management Console puis choisissez Lambda. La console affiche toutes les fonctions Lambda que vous avez publiées, y compris celle que vous venez de créer.

Nettoyage

Si vous ne comptez pas poursuivre le développement avec cet exemple, supprimez la fonction que vous avez déployée afin de ne pas être facturée pour les ressources inutilisées de votre compte.

> **Note**
>
> Lambda surveille automatiquement les fonctions Lambda pour vous, en fournissant des statistiques via Amazon. CloudWatch Pour surveiller et résoudre les problèmes liés à votre fonction, consultez la rubrique Dépannage et surveillance des fonctions AWS Lambda avec CloudWatch Amazon dans AWS Lambda le Guide du développeur.

Pour supprimer votre fonction

1. À partir de l'AWS explorateur, développez le AWS Lambdanœud.
2. Cliquez avec le bouton droit sur votre instance déployée, puis choisissez Supprimer.

AWS Lambda Projet de base : création d'une image Docker

Vous pouvez utiliser le Toolkit for Visual Studio pour déployer votre AWS Lambda fonction sous forme d'image Docker. Avec Docker, vous avez plus de contrôle sur votre environnement d'exécution. Par exemple, vous pouvez choisir des environnements d'exécution personnalisés tels que .NET 8.0. Vous déployez votre image Docker de la même manière que n'importe quelle autre image de conteneur. Ce didacticiel est très similaire à Tutorial : Basic Lambda Project, à deux différences près :

- Un Dockerfile est inclus dans le projet.
- Une autre configuration de publication est choisie.

Pour plus d'informations sur les images de conteneurs Lambda, consultez la section Packages de déploiement Lambda dans le guide du développeur.AWS Lambda

Pour plus d'informations sur l'utilisation de Lambda AWS Toolkit for Visual Studio, consultez la section Utilisation des AWS Lambda modèles dans la AWS Toolkit for Visual Studio rubrique de ce guide de l'utilisateur.

Création d'un projet Lambda Visual Studio .NET Core

Vous pouvez utiliser les modèles et les plans Lambda Visual Studio pour accélérer l'initialisation de votre projet. Les plans Lambda contiennent des fonctions prédéfinies qui simplifient la création d'une base de projet flexible.

Pour créer un projet Lambda Visual Studio .NET Core

1. Dans Visual Studio, développez le menu Fichier, développez Nouveau, puis choisissez Projet.
2. Dans la boîte de dialogue Nouveau projet, définissez les listes déroulantes Langue, plate-forme et type de projet sur « Tous », puis saisissez le **`aws lambda`** texte dans le champ Rechercher. Choisissez le modèle de projet AWS Lambda (.NET Core - C#).
3. Dans le champ Nom du projet, entrez**`AWSLambdaDocker`**, spécifiez l'emplacement de votre fichier, puis choisissez Créer.
4. Sur la page Sélectionner un plan, choisissez le plan .NET 8 (image conteneur), puis choisissez Terminer pour créer le projet Visual Studio. Vous pouvez maintenant vérifier la structure et le code du projet.

Révision des fichiers de projet

Les sections suivantes examinent les trois fichiers de projet créés par le plan .NET 8 (Container Image) :

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

1. Dockerfile

A `Dockerfile` exécute trois actions principales :

- `FROM`: définit l'image de base à utiliser pour cette image. Cette image de base fournit le .NET Runtime, le runtime Lambda et un script shell qui fournit un point d'entrée pour le processus Lambda .NET.
- `WORKDIR`: définit le répertoire de travail interne de l'image sous la forme`/var/task`.
- `COPY`: copiera les fichiers générés par le processus de construction depuis leur emplacement local dans le répertoire de travail de l'image.

Les `Dockerfile` actions facultatives que vous pouvez spécifier sont les suivantes :

- `ENTRYPOINT`: L'image de base inclut déjà un`ENTRYPOINT`, qui est le processus de démarrage exécuté au démarrage de l'image. Si vous souhaitez spécifier le vôtre, vous remplacez ce point d'entrée de base.
- `CMD`: indique le code personnalisé AWS que vous souhaitez exécuter. Il attend un nom complet pour votre méthode personnalisée. Cette ligne doit être incluse directement dans le Dockerfile ou peut être spécifiée lors du processus de publication.

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

Voici un exemple de Dockerfile créé par le plan .NET 8 (Container Image).

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

WORKDIR /var/task

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

2. aws-lambda-tools-defaults.json

Le `aws-lambda-tools-defaults.json` fichier est utilisé pour spécifier les valeurs par défaut de l'assistant de déploiement de Toolkit for Visual Studio et de la CLI .NET Core. La liste suivante décrit les champs que vous pouvez définir dans votre `aws-lambda-tools-defaults.json` fichier.

- `profile`: définit votre AWS profil.
- `region`: définit la AWS région dans laquelle vos ressources sont stockées.

- `configuration`: définit la configuration utilisée pour publier votre fonction.
- `package-type`: définit le type de package de déploiement sur une image de conteneur ou une archive de fichier .zip.
- `function-memory-size`: définit l'allocation de mémoire pour votre fonction en Mo.
- `function-timeout`: Le délai d'expiration est la durée maximale en secondes pendant laquelle une fonction Lambda peut être exécutée. Vous pouvez l'ajuster par incréments d'une seconde jusqu'à une valeur maximale de 15 minutes.
- `docker-host-build-output-dir`: définit le répertoire de sortie du processus de construction qui est en corrélation avec les instructions du`Dockerfile`.
- `image-command`: est le nom complet de votre méthode, le code que vous souhaitez faire exécuter par la fonction Lambda. La syntaxe est la suivante :`{Assembly}::{Namespace}.{ClassName}::{MethodName}`. Pour plus d'informations, consultez la section Signatures du gestionnaire. Cette valeur est préremplie ultérieurement dans l'assistant de publication de Visual Studio. `image-command`

Voici un exemple de aws-lambda-tools-defaults fichier .json créé par le plan .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

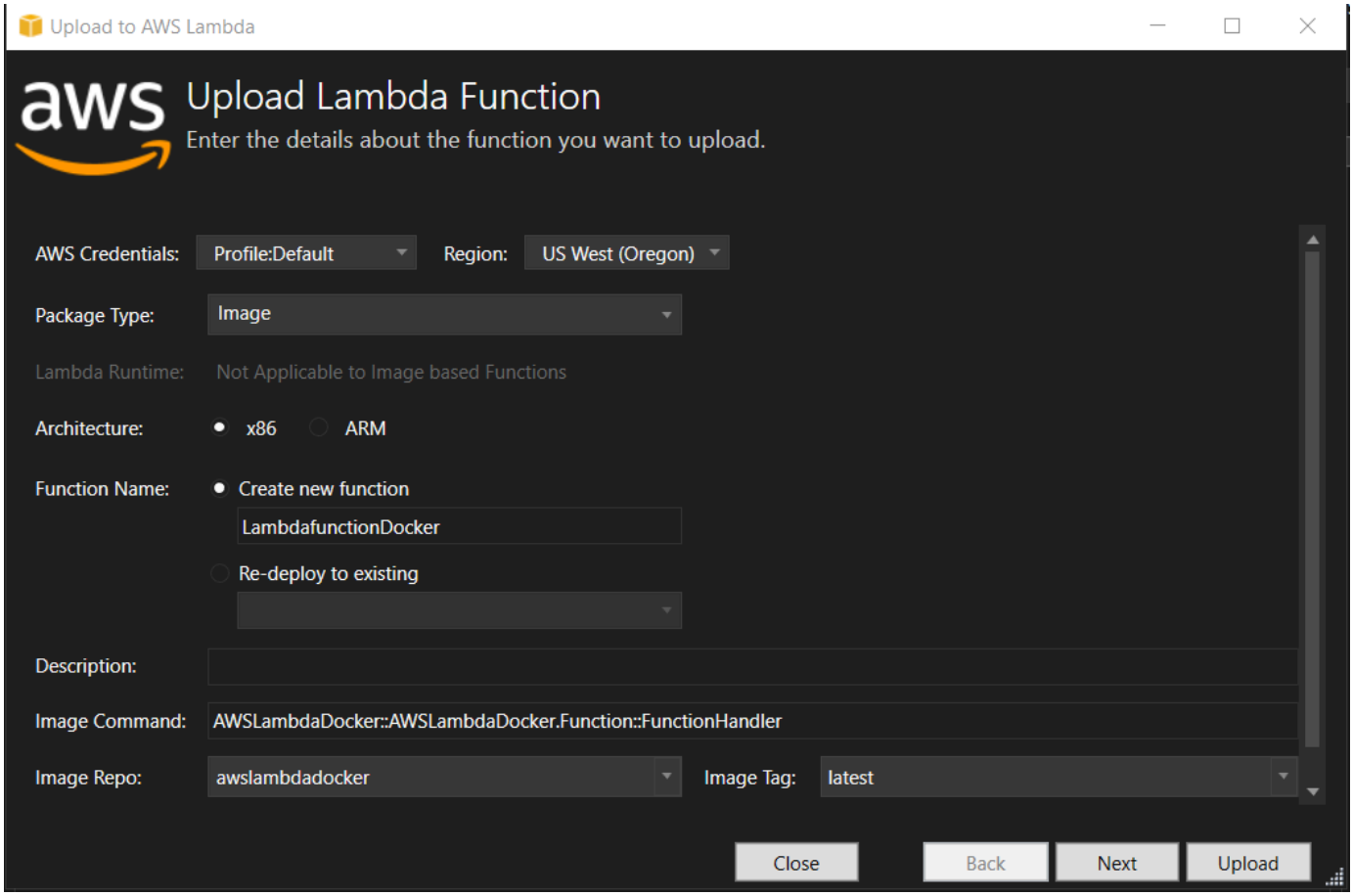
Le `Function.cs` fichier définit les fonctions c# à exposer en tant que fonctions Lambda. `FunctionHandler`Il s'agit de la fonctionnalité Lambda qui s'exécute lorsque la fonction Lambda s'exécute. Dans ce projet, `FunctionHandler` fait `ToUpper()` appel au texte saisi.

Publier sur Lambda

Les images Docker générées par le processus de création sont chargées sur Amazon Elastic Container Registry (Amazon ECR). Amazon ECR est un registre de conteneurs Docker entièrement géré que vous utilisez pour stocker, gérer et déployer des images de conteneurs Docker. Amazon ECR héberge l'image, à laquelle Lambda fait ensuite référence pour fournir la fonctionnalité Lambda programmée lorsqu'elle est invoquée.

Pour publier votre fonction sur Lambda

1. Dans l'explorateur de solutions, ouvrez le menu contextuel du projet (cliquez avec le bouton droit de la souris), puis choisissez Publier pour AWS Lambda ouvrir la fenêtre Upload Lambda Function.
2. Sur la page Upload Lambda Function, procédez comme suit :



a. Pour le type de package, **`Image`** il a été automatiquement sélectionné comme type de package car l'assistant de publication en a détecté un `Dockerfile` dans votre projet.

b. Dans Nom de la fonction, entrez un nom d'affichage pour votre instance Lambda. Ce nom est le nom de référence affiché à la fois dans l' AWS explorateur de Visual Studio et dans le AWS Management Console.

c. Pour Description, entrez le texte à afficher avec votre instance dans le AWS Management Console.

d. Pour Image Command, entrez un chemin complet vers la méthode que vous souhaitez exécuter par la fonction Lambda : **`AWSLambdaDocker::AWSLambdaDocker.Function::FunctionHandler`**

> **Note**
>
> Tout nom de méthode saisi ici remplacera toute instruction CMD dans le Dockerfile. La saisie de la commande Image n'est facultative que SI vous `Dockerfile` incluez un `CMD` pour indiquer comment lancer la fonction Lambda.

e. Pour Image Repo, entrez le nom d'un Amazon Elastic Container Registry nouveau ou existant. L'image Docker créée par le processus de génération est téléchargée dans ce registre. La définition Lambda publiée fera référence à cette image Amazon ECR.

f. Pour Image Tag, entrez une balise Docker à associer à votre image dans le référentiel.

g. Choisissez Suivant.

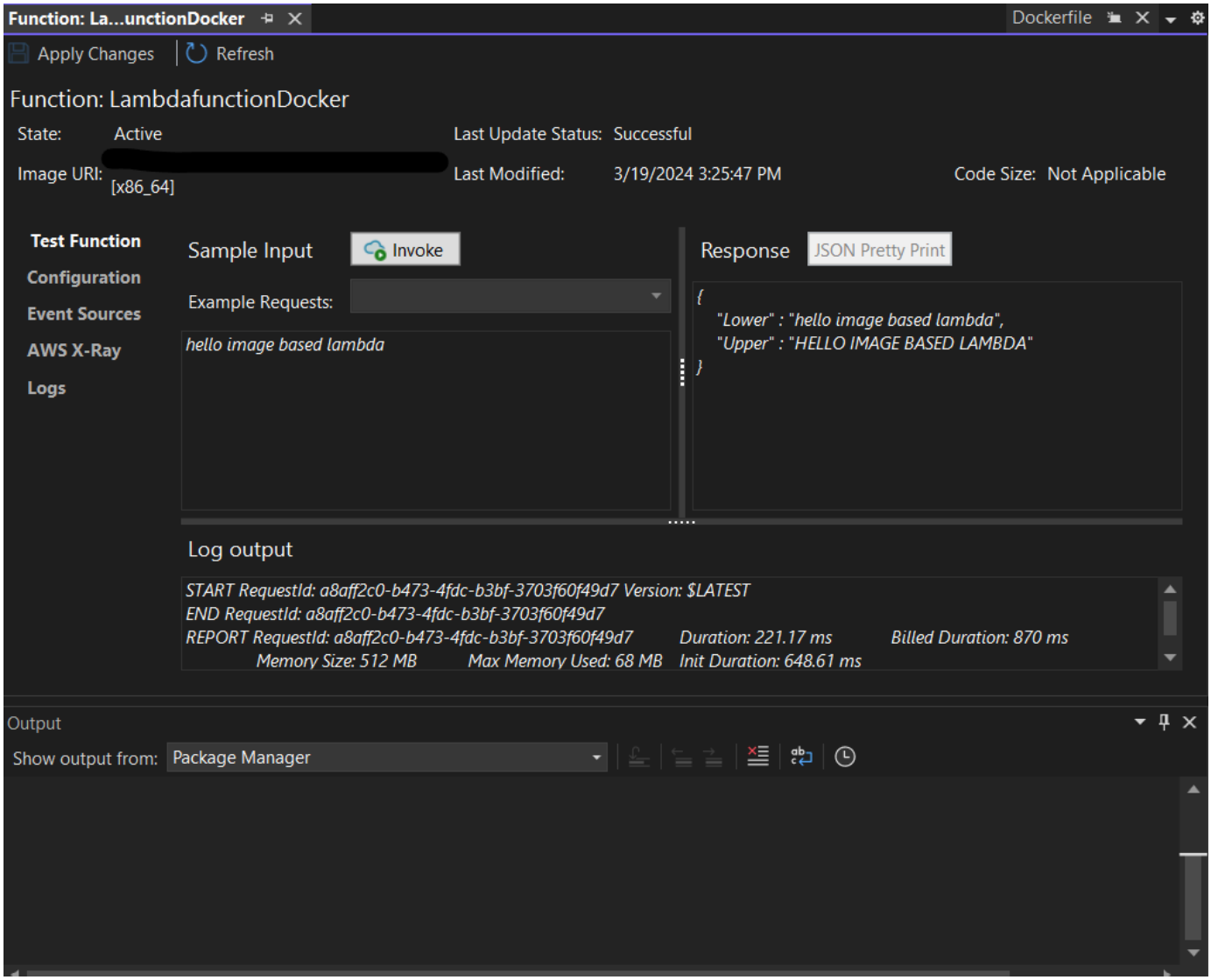
3. Sur la page Détails des fonctions avancées, dans Nom du rôle, choisissez un rôle associé à votre compte. Le rôle est utilisé pour fournir des informations d'identification temporaires pour tous les appels Amazon Web Services effectués par le code de la fonction. Si vous n'avez pas de rôle, choisissez Nouveau rôle basé sur la politique AWS gérée, puis choisissez AWSLambdaBasicExecutionRole.

> **Note**
>
> Votre compte doit être autorisé à exécuter l' ListPolicies action IAM, sinon la liste des noms de rôle sera vide.

4. Choisissez Upload pour démarrer les processus de téléchargement et de publication.

> **Note**
>
> La page de la fonction de téléchargement s'affiche pendant le téléchargement de la fonction. Le processus de publication crée ensuite l'image en fonction des paramètres de configuration, crée le référentiel Amazon ECR si nécessaire, télécharge l'image dans le référentiel et crée le Lambda référençant ce dépôt avec cette image.
> Une fois la fonction chargée, la page Function s'ouvre et affiche la configuration de votre nouvelle fonction Lambda.

5. Pour appeler manuellement la fonction Lambda, dans l'onglet Fonction de test, entrez **`hello image based lambda`** dans le champ de saisie en texte libre de la demande, puis choisissez Invoke. Votre texte, converti en majuscules, apparaîtra dans Réponse.



6. Pour afficher le référentiel, dans l'AWS explorateur, sous Amazon Elastic Container Service, sélectionnez Repositories.

   Vous pouvez rouvrir la vue Function : à tout moment en double-cliquant sur votre instance déployée située dans l'AWS explorateur sous le AWS Lambdanœud.

   > **Note**
   >
   > Si la fenêtre de votre AWS explorateur n'est pas ouverte, vous pouvez l'ancrer via Affichage -> AWS Explorateur

7. Notez les options de configuration supplémentaires spécifiques à l'image dans l'onglet Configuration. Cet onglet permet de remplacer le `ENTRYPOINTCMD`, et `WORKDIR` qui peut avoir

été spécifié dans le Dockerfile. La description est la description que vous avez saisie (le cas échéant) lors du chargement/de la publication.

Nettoyage

Si vous ne comptez pas poursuivre le développement avec cet exemple, pensez à supprimer la fonction et l'image ECR déployées afin de ne pas être facturée pour les ressources inutilisées de votre compte.

- Les fonctions peuvent être supprimées en cliquant avec le bouton droit sur votre instance déployée située dans l'AWS explorateur sous le AWS Lambdanœud.
- Les référentiels peuvent être supprimés dans l'AWS explorateur sous Amazon Elastic Container Service -> Référentiels.

Étapes suivantes

Pour plus d'informations sur la création et le test d'images Lambda, consultez la section Utilisation d'images de conteneurs avec Lambda.

Pour plus d'informations sur le déploiement d'images de conteneurs, les autorisations et le remplacement des paramètres de configuration, consultez la section Configuration des fonctions.

Tutoriel : Création et test d'une application sans serveur avec AWS Lambda

Vous pouvez créer une application Lambda sans serveur à l'aide AWS Toolkit for Visual Studio d'un modèle. Les modèles de projet Lambda incluent un modèle pour une application AWS sans serveur, qui est l' AWS Toolkit for Visual Studio implémentation du modèle d'application AWS sans serveur (SAM).AWS Ce type de projet vous permet de développer un ensemble de AWS Lambda fonctions et de les déployer avec toutes les AWS ressources nécessaires en tant qu'application complète, AWS CloudFormation afin d'orchestrer le déploiement.

Pour les prérequis et les informations relatives à la configuration du AWS Toolkit for Visual Studio, consultez la section Utilisation des modèles AWS Lambda dans AWS le Toolkit for Visual Studio.

Rubriques

- Création d'un nouveau projet d'application AWS sans serveur
- Révision des fichiers de l'application sans serveur
- Déploiement de l'application sans serveur

- Testez l'application sans serveur

Création d'un nouveau projet d'application AWS sans serveur

AWS Les projets d'applications sans serveur créent des fonctions Lambda à l'aide d'un AWS CloudFormation modèle sans serveur. AWS CloudFormation les modèles vous permettent de définir des ressources supplémentaires telles que des bases de données, d'ajouter des rôles IAM et de déployer plusieurs fonctions à la fois. Cela diffère des projets AWS Lambda, qui se concentrent sur le développement et le déploiement d'une fonction Lambda unique.

La procédure suivante décrit comment créer un nouveau projet d'application AWS sans serveur.

1. Dans Visual Studio, développez le menu Fichier, développez Nouveau, puis choisissez Projet.
2. Dans la boîte de dialogue Nouveau projet, assurez-vous que les listes déroulantes Langue, Plateforme et Type de projet sont définies sur « Tout... » et entrez **`aws lambda`** dans le champ Rechercher.
3. Sélectionnez le modèle AWS Serverless Application with Tests (.NET Core - C#).

   > **Note**
   >
   > Il est possible que le modèle AWS Serverless Application with Tests (.NET Core - C#) ne soit pas renseigné en haut des résultats.

4. Cliquez sur Suivant pour ouvrir la boîte de dialogue Configurer votre nouveau projet.
5. Dans la boîte de dialogue Configurer votre nouveau projet, saisissez **`ServerlessPowertools`** le nom, puis complétez les champs restants selon vos préférences. Cliquez sur le bouton Créer pour accéder à la boîte de dialogue Sélectionner le plan.
6. Dans la boîte de dialogue Select Blueprint, choisissez les Powertools for AWS Lambda Blueprint, puis cliquez sur Terminer pour créer le projet Visual Studio.

Révision des fichiers de l'application sans serveur

Les sections suivantes fournissent un aperçu détaillé de trois fichiers d'application sans serveur créés pour votre projet :

1. serverless.template
2. Functions.cs

3. aws-lambda-tools-defaults.json

1. serverless.template

Un `serverless.template` fichier est un AWS CloudFormation modèle pour déclarer vos fonctions Serverless et autres AWS ressources. Le fichier inclus dans ce projet contient une déclaration pour une seule fonction Lambda qui sera exposée via Amazon API Gateway en tant `HTTP *Get*` qu'opération. Vous pouvez modifier ce modèle pour personnaliser la fonction existante ou ajouter d'autres fonctions et autres ressources requises par votre application.

Voici un exemple de fichier `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/"
       }
     }
   }
}
```

Notez que de nombreux champs de `...AWS:: Serverless::Function...` déclaration sont similaires aux champs d'un déploiement de projet Lambda. La journalisation, les métriques et le suivi de Powertools sont configurés via les variables d'environnement suivantes :

- POWERTOOLS_SERVICE_NAME= ServerlessGreeting
- PowerTools_Log_Level=Informations
- POWERTOOLS_LOGGER_CASE= PascalCase
- PowerTools_Tracer_Capture_Response=vrai
- PowerTools_Tracer_Capture_Error=vrai
- ESPACE DE NOMS POWERTOOLS_METRICS_= ServerlessGreeting

Pour obtenir des définitions et des informations supplémentaires sur les variables d'environnement, consultez le site Web Powertools for AWS Lambda references.

2. Functions.cs

`Functions.cs`est un fichier de classe contenant une méthode C# mappée à une seule fonction déclarée dans le fichier modèle. La fonction Lambda répond aux `HTTP Get` méthodes d'API Gateway. Voici un exemple de `Functions.cs` fichier :

```
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`fournit les valeurs par défaut pour l'assistant de AWS déploiement dans Visual Studio et les AWS Lambda commandes ajoutées à la CLI .NET Core. Voici un exemple du `aws-lambda-tools-defaults.json` fichier inclus dans ce projet :

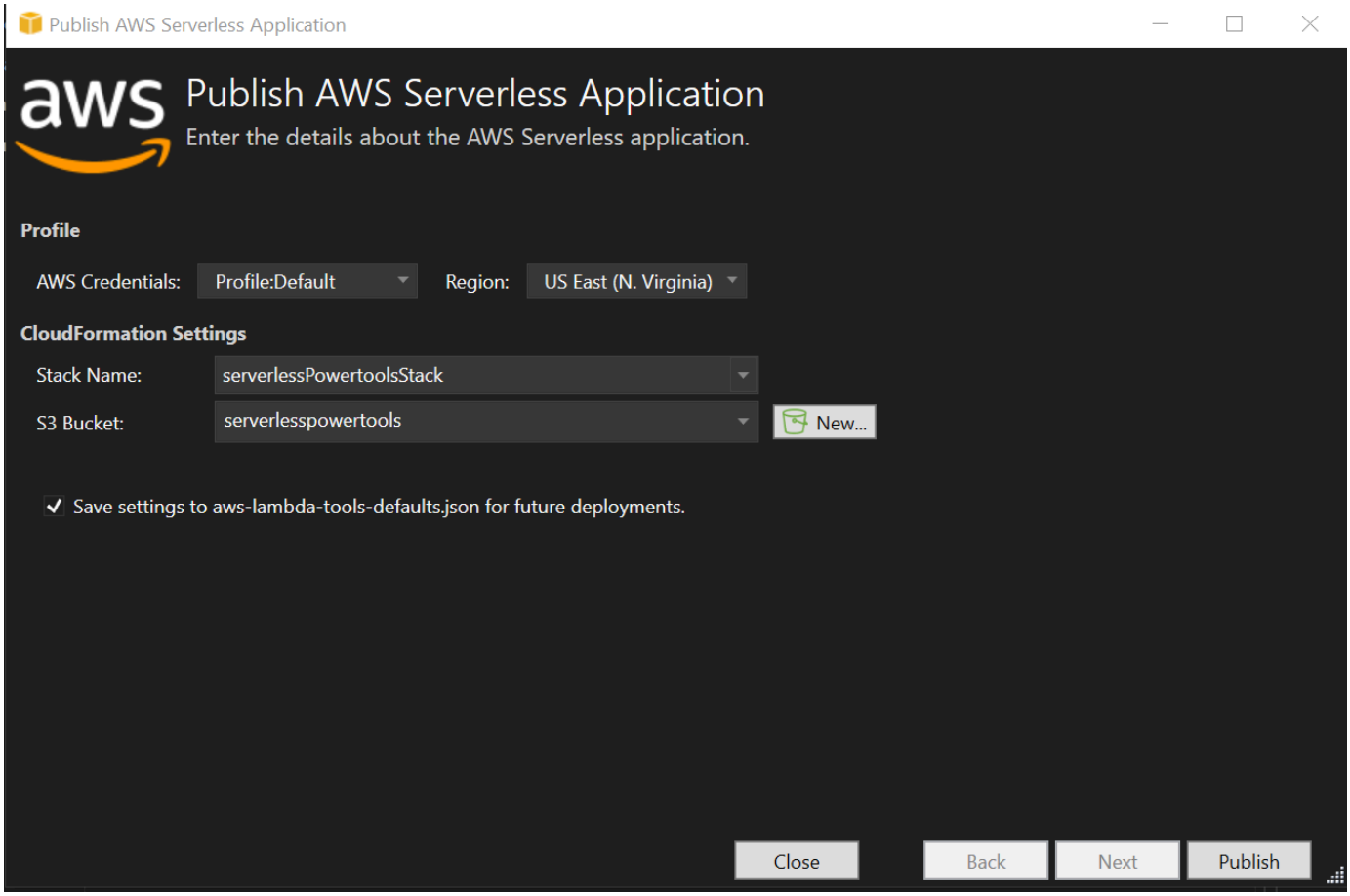
```
{
  "profile": "Default",
  "region": "us-east-1",
  "configuration": "Release",
  "s3-prefix": "ServerlessPowertools/",
  "template": "serverless.template",
  "template-parameters": ""
}
```

Déploiement de l'application sans serveur

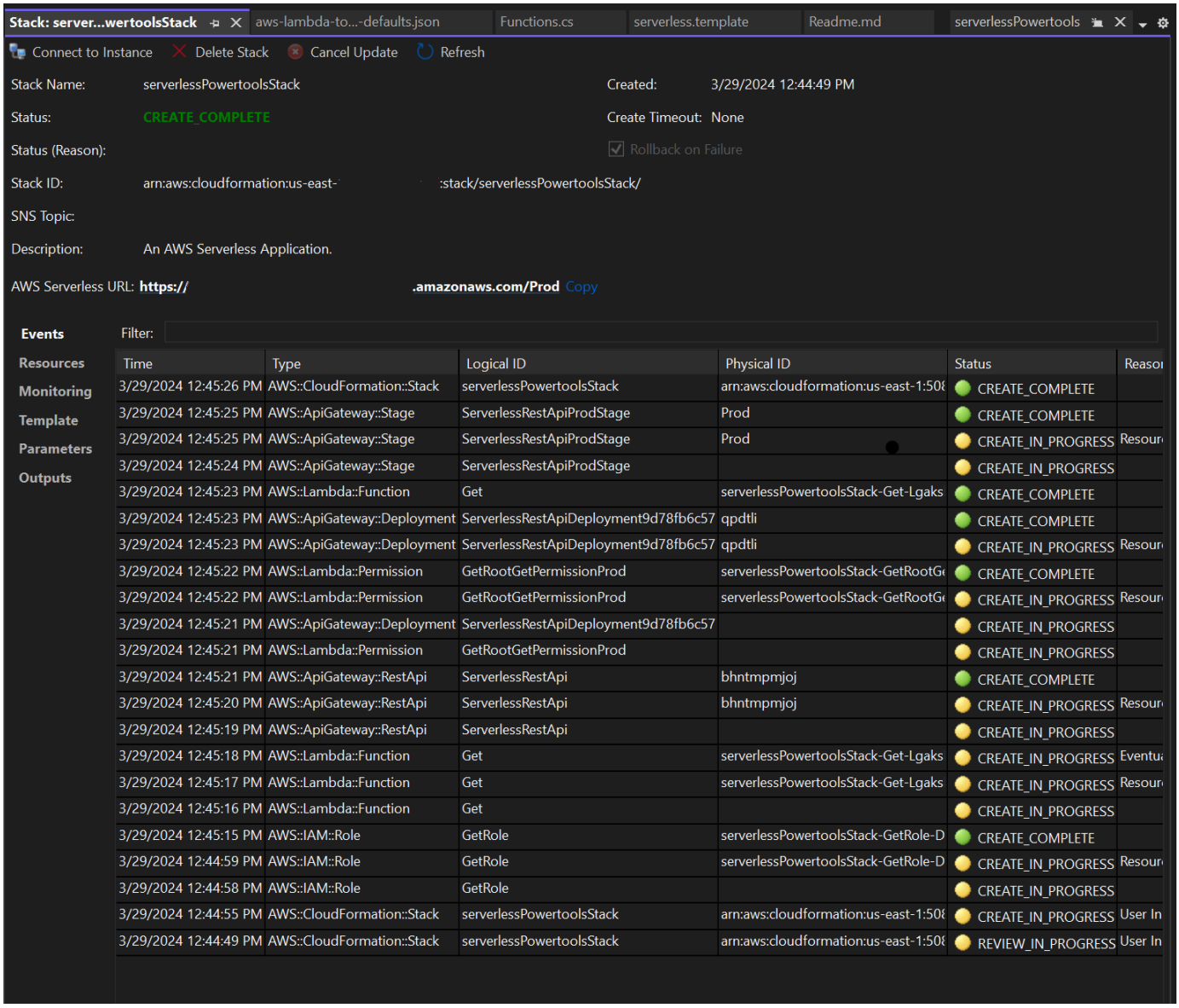
Pour déployer votre application sans serveur, procédez comme suit :

1. Dans l'explorateur de solutions, ouvrez le menu contextuel de votre projet (cliquez avec le bouton droit de la souris) et choisissez Publier sur AWS Lambda pour ouvrir la boîte de dialogue Publier une application AWS sans serveur.
2. Dans la boîte de dialogue Publier une application AWS sans serveur, entrez le nom du conteneur de AWS CloudFormation pile dans le champ Stack Name.
3. Dans le champ Compartiment S3, choisissez un compartiment Amazon S3 vers lequel votre bundle d'applications sera chargé ou choisissez le Nouveau... bouton et entrez le nom d'un nouveau compartiment Amazon S3. Choisissez ensuite Publier pour publier afin de déployer votre application.

> **Note**
>
> Votre AWS CloudFormation stack et votre compartiment Amazon S3 doivent se trouver dans la même AWS région. Les autres paramètres de votre projet sont définis dans le `serverless.template` fichier.



4. La fenêtre Stack View s'ouvre pendant le processus de publication. Lorsque le déploiement est terminé, le champ État affiche :`CREATE_COMPLETE`.



Testez l'application sans serveur

Lorsque la création de la pile est terminée, vous pouvez consulter votre application à l'aide de l'URL AWS sans serveur. Si vous avez terminé ce didacticiel sans ajouter de fonctions ou de paramètres supplémentaires, l'accès à votre URL AWS sans serveur affiche la phrase suivante dans votre navigateur Web :`Hello Powertools for AWS Lambda (.NET)`.

Didacticiel : Création d'une application Lambda Amazon Rekognition

Ce didacticiel explique comment créer une application Lambda qui utilise Amazon Rekognition pour étiqueter des objets Amazon S3 avec des étiquettes détectées.

Pour les prérequis et les informations relatives à la configuration du AWS Toolkit for Visual Studio, consultez la section Utilisation des modèles AWS Lambda dans AWS le Toolkit for Visual Studio.

Création d'un projet de rekognition d'images Lambda Visual Studio .NET Core

La procédure suivante explique comment créer une application Amazon Rekognition Lambda à partir du. AWS Toolkit for Visual Studio

> **Note**
>
> Lors de sa création, votre application dispose d'une solution composée de deux projets : le projet source qui contient le code de votre fonction Lambda à déployer sur Lambda, et un projet de test utilisant xUnit pour tester votre fonction localement.
> Il arrive que Visual Studio ne trouve pas toutes les NuGet références de vos projets. Cela est dû au fait que les plans nécessitent des dépendances qui doivent être NuGet extraites. Lorsque de nouveaux projets sont créés, Visual Studio extrait uniquement des références locales et non des références distantes NuGet. Pour corriger les NuGet erreurs : cliquez avec le bouton droit sur vos références et choisissez Restaurer les packages.

1. Dans Visual Studio, développez le menu Fichier, développez Nouveau, puis choisissez Projet.
2. Dans la boîte de dialogue Nouveau projet, assurez-vous que les listes déroulantes Langue, Plateforme et Type de projet sont définies sur « Tout... » et entrez **`aws lambda`** dans le champ Rechercher.
3. Sélectionnez le modèle AWS Lambda with Tests (.NET Core - C#).
4. Cliquez sur Suivant pour ouvrir la boîte de dialogue Configurer votre nouveau projet.
5. Dans la boîte de dialogue Configurer votre nouveau projet, saisissez ImageRekognition « » pour le nom, puis complétez les champs restants selon vos préférences. Cliquez sur le bouton Créer pour accéder à la boîte de dialogue Sélectionner le plan.
6. Dans la boîte de dialogue Sélectionner un plan, choisissez le plan Detect Image Labels, puis choisissez Terminer pour créer le projet Visual Studio.

   > **Note**
   >
   > Ce plan fournit du code pour écouter les événements Amazon S3 et utilise Amazon Rekognition pour détecter les étiquettes et les ajouter à l'objet S3 sous forme de balises.

Révision des fichiers de projet

Les sections suivantes examinent ces fichiers de projet :

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

1. Function.cs

À l'intérieur du `Function.cs` fichier, le premier segment de code est l'attribut d'assemblage, situé en haut du fichier. Par défaut, Lambda accepte uniquement les paramètres d'entrée et les types de retour. `System.IO.Stream` Vous devez enregistrer un sérialiseur pour utiliser des classes typées pour les paramètres d'entrée et les types de retour. L'attribut assembly enregistre le sérialiseur Lambda JSON, qui permet de `Newtonsoft.Json` convertir les flux en classes typées. Vous pouvez définir le sérialiseur au niveau de l'assemblage ou de la méthode.

Voici un exemple de l'attribut assembly :

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

La classe possède deux constructeurs. Le premier est un constructeur par défaut qui est utilisé lorsque Lambda appelle votre fonction. Ce constructeur crée les clients des services Amazon S3 et Amazon Rekognition. Le constructeur extrait également les AWS informations d'identification de ces clients à partir du rôle IAM que vous attribuez à la fonction lorsque vous la déployez. La AWS région pour les clients est définie sur la région dans laquelle votre fonction Lambda s'exécute. Dans ce plan, vous ne souhaitez ajouter des balises à l'objet Amazon S3 que si le service Amazon Rekognition possède un niveau de confiance minimal quant à l'étiquette. Ce constructeur vérifie la variable d'environnement `MinConfidence` pour déterminer le niveau de confiance acceptable. Vous pouvez définir cette variable d'environnement lorsque vous déployez la fonction Lambda.

Voici un exemple du premier constructeur de classe dans `Function.cs` :

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

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

L'exemple suivant montre comment le second constructeur peut être utilisé pour les tests. Le projet de test configure ses propres clients S3 et Rekognition et les transmet :

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

Voici un exemple de la `FunctionHandler` méthode contenue dans le `Function.cs` fichier.

```
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` est la méthode que lambda appelle après avoir construit l'instance. Notez que le paramètre d'entrée est de type `S3Event` et pas un `Stream`. Vous pouvez effectuer cette action grâce au sérialiseur JSON Lambda enregistré. `S3Event`Il contient toutes les informations relatives à l'événement déclenché dans Amazon S3. La fonction parcourt tous les objets S3 qui faisaient partie de l'événement et indique à Rekognition de détecter les étiquettes. Lorsque les étiquettes ont été détectées, elles sont ajoutées sous forme d'étiquettes à l'objet S3.

> **Note**
>
> Le code contient des appels à`Console.WriteLine()`. Lorsque la fonction est exécutée dans Lambda, tous les appels sont redirigés `Console.WriteLine()` vers Amazon CloudWatch Logs.

2. aws-lambda-tools-defaults.json

Le `aws-lambda-tools-defaults.json` fichier contient les valeurs par défaut définies par le plan pour préremplir certains champs de l'assistant de déploiement. Il est également utile pour définir les options de ligne de commande pour l'intégration à la CLI .NET Core.

Pour accéder à l'intégration de la CLI .NET Core, accédez au répertoire de projet de la fonction et tapez**`dotnet lambda help`**.

> **Note**
>
> Le gestionnaire de fonctions indique la méthode que Lambda doit appeler en réponse à la fonction invoquée. Le format de ce champ est le suivant :`<assembly-name>::<full-type-name>::<method-name>`. L'espace de noms doit être inclus dans le nom du type.

Déploiement de la fonction

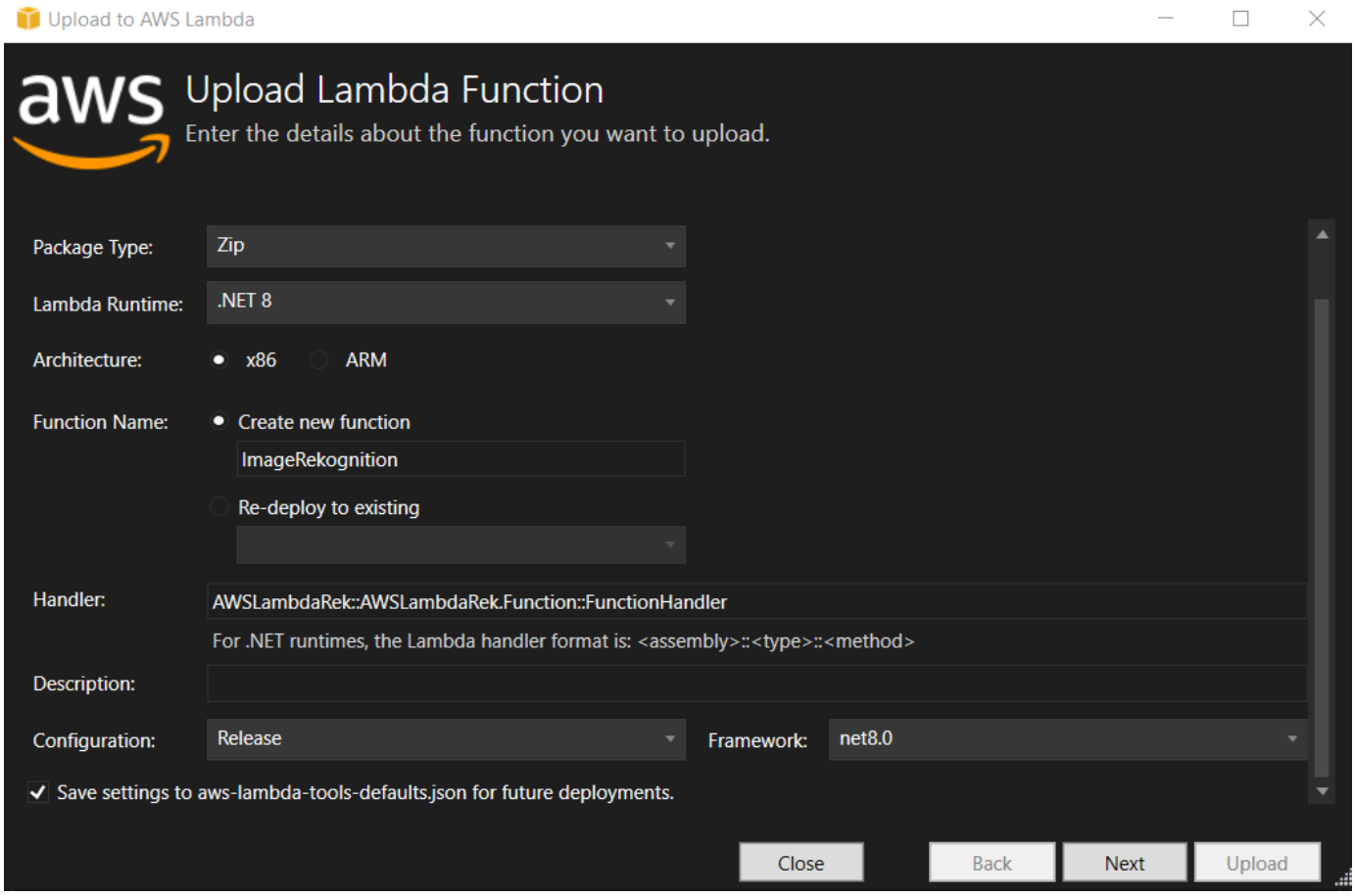
La procédure suivante décrit comment déployer votre fonction Lambda.

1. Dans l'explorateur de solutions, cliquez avec le bouton droit sur le projet Lambda et choisissez Publier sur AWS Lambda pour ouvrir la fenêtre Upload to. AWS Lambda

> **Note**
>
> Les valeurs prédéfinies sont extraites du `aws-lambda-tools-defaults.json` fichier.

2. Dans la AWS Lambda fenêtre Télécharger vers, entrez un nom dans le champ Nom de la fonction, puis cliquez sur le bouton Suivant pour accéder à la fenêtre Détails des fonctions avancées.

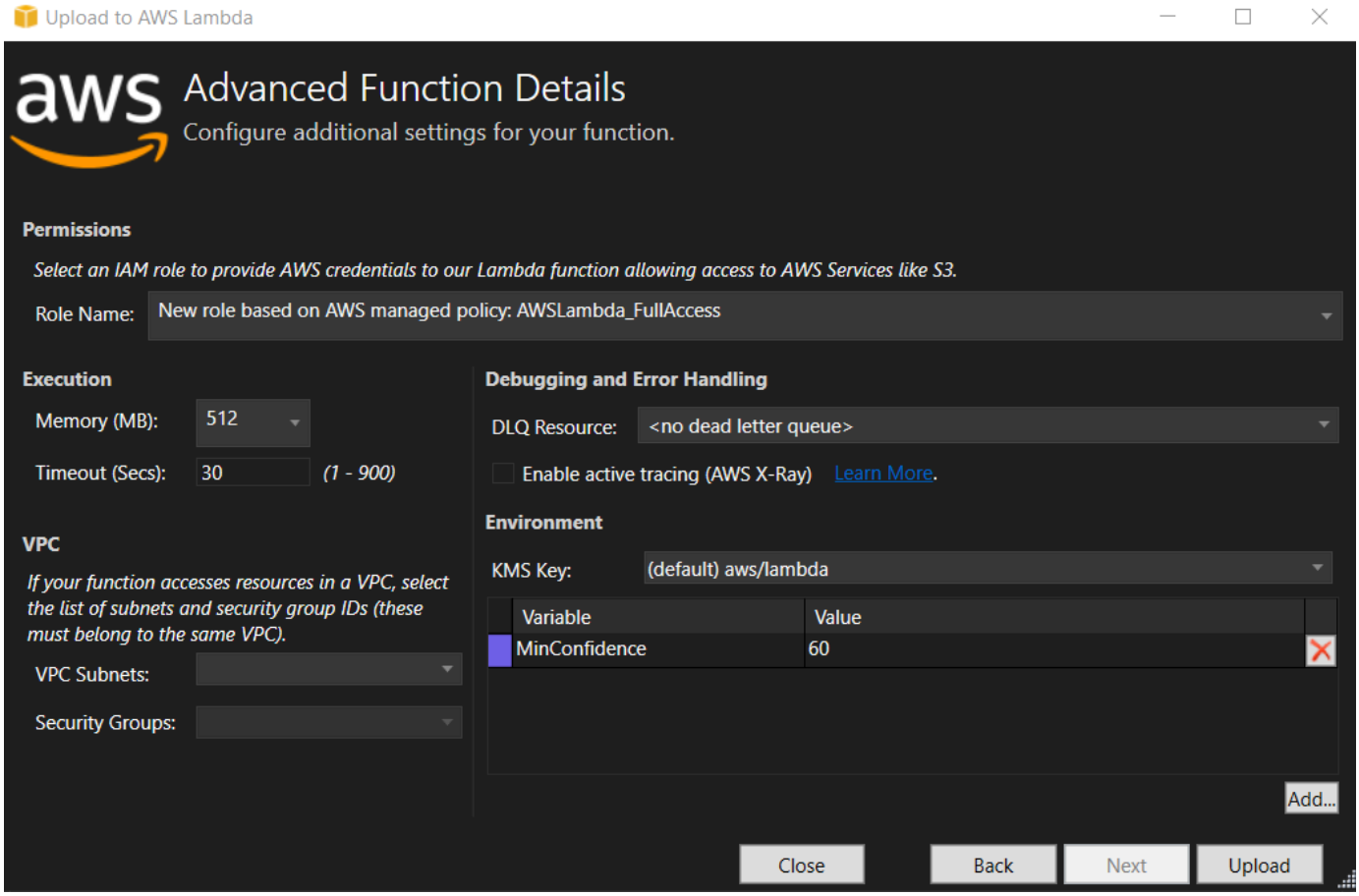
> **Note**
>
> Cet exemple utilise le nom de la fonction**`ImageRekognition`**.



3. Dans la fenêtre Détails des fonctions avancées, sélectionnez un rôle IAM qui autorise votre code à accéder à vos ressources Amazon S3 et Amazon Rekognition.

> **Note**
>
> Si vous suivez cet exemple, sélectionnez le `AWSLambda_FullAccess` rôle.

4. Définissez la variable `MinConfidence` d'environnement sur 60, puis choisissez Upload pour lancer le processus de déploiement. Le processus de publication est terminé lorsque la vue Fonction s'affiche dans l'AWS explorateur.



5. Après un déploiement réussi, configurez Amazon S3 pour qu'il envoie ses événements à votre nouvelle fonction en accédant à l'onglet Sources d'événements.

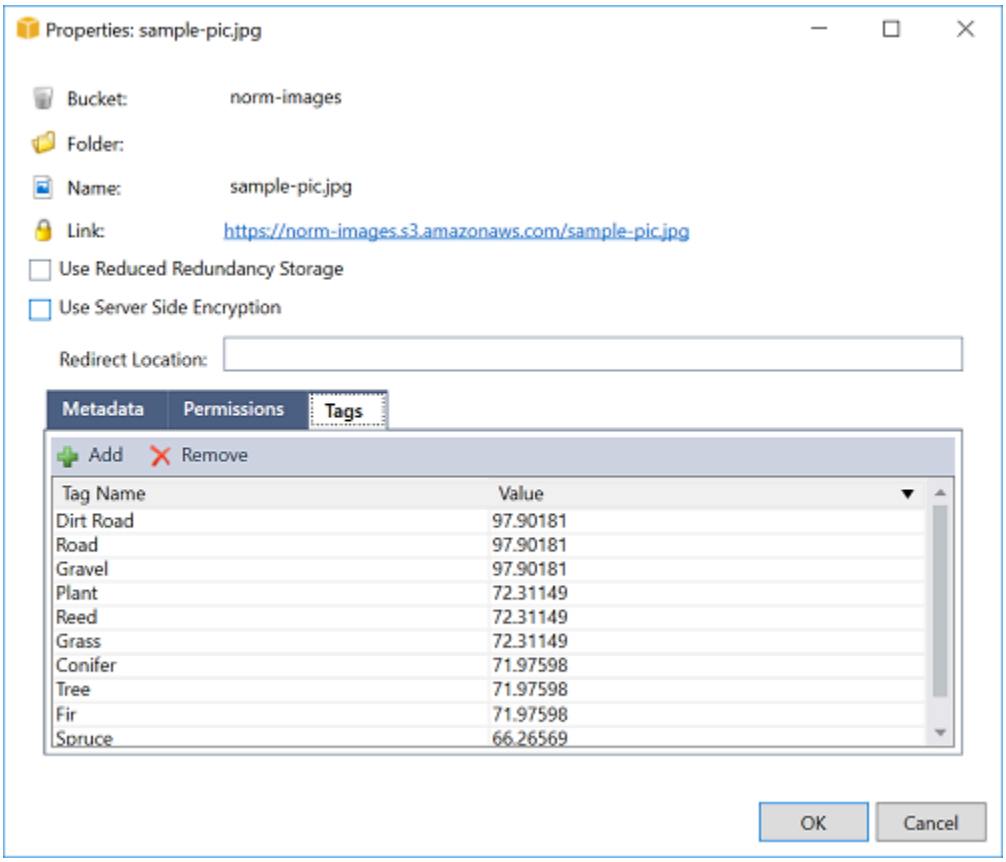
6. Dans l'onglet Sources d'événements, cliquez sur le bouton Ajouter, puis sélectionnez le compartiment Amazon S3 pour vous connecter à votre fonction Lambda.

> **Note**
>
> Le bucket doit se trouver dans la même AWS région que votre fonction Lambda.

Test de la fonction

Maintenant que la fonction est déployée et qu'un compartiment S3 est configuré comme source d'événements pour celle-ci, ouvrez le navigateur de compartiments S3 depuis l'AWS explorateur pour le compartiment que vous avez sélectionné. Chargez ensuite des images.

Lorsque le chargement est terminé, vous pouvez vérifier que votre fonction s'est exécutée en consultant les journaux dans la vue de la fonction. Vous pouvez également cliquer avec le bouton droit de la souris sur les images dans le navigateur de compartiment et choisir Propriétés. Dans l'onglet Balises, vous pouvez afficher les étiquettes qui ont été appliquées à votre objet.



Tutoriel : Utilisation d'Amazon Logging Frameworks AWS Lambda pour créer des journaux d'applications

Vous pouvez utiliser Amazon CloudWatch Logs pour surveiller, stocker et accéder aux journaux de votre application. Pour transférer les données des CloudWatch journaux dans Logs, utilisez un AWS SDK ou installez l'agent CloudWatch Logs pour surveiller certains dossiers de journaux. CloudWatch Logs est intégré à plusieurs frameworks de journalisation .NET populaires, ce qui simplifie les flux de travail.

Pour commencer à travailler avec CloudWatch Logs et les frameworks de journalisation .NET, ajoutez le NuGet package et la source de sortie CloudWatch Logs appropriés à votre application, puis utilisez votre bibliothèque de journalisation comme vous le feriez normalement. Cela permet à votre application de consigner les messages avec votre framework .NET, de les envoyer à CloudWatch Logs, d'afficher les messages de journal de votre application dans la console CloudWatch Logs. Vous pouvez également configurer des métriques et des alarmes à partir de la console CloudWatch Logs, en fonction des messages de journal de votre application.

Les frameworks de journalisation .NET pris en charge incluent :

- NLog : pour le consulter, consultez le package NLog de nuget.org.
- Log4net : Pour le voir, consultez le package Log4net nuget.org.
- Framework de journalisation ASP.NET Core : pour le voir, consultez le package nuget.org ASP.NET Core logging Framework.

Voici un exemple de `NLog.config` fichier qui active à la fois les CloudWatch journaux et la console comme sortie pour les messages de journal en y ajoutant le `AWS.Logger.NLog` NuGet package et la AWS cible`NLog.config`.

```
<?xml version="1.0" encoding="utf-8" ?>
<nlog xmlns="http://www.nlog-project.org/schemas/NLog.xsd"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      throwExceptions="true">
  <targets>
    <target name="aws" type="AWSTarget" logGroup="NLog.ConfigExample" region="us-
east-1"/>
    <target name="logfile" xsi:type="Console" layout="${callsite} ${message}" />
  </targets>
  <rules>
    <logger name="*" minlevel="Info" writeTo="logfile,aws" />
```

```
  </rules>
</nlog>
```

Les plugins de journalisation sont tous basés sur AWS SDK for .NET et authentifient vos AWS informations d'identification selon un processus similaire au SDK. L'exemple suivant détaille les autorisations requises par les informations d'identification du plugin de journalisation pour accéder aux CloudWatch journaux :

> **Note**
>
> Les plugins de journalisation AWS .NET sont un projet open source. Pour obtenir des informations, des exemples et des instructions supplémentaires, consultez les rubriques relatives aux exemples et aux instructions du GitHub référentiel AWS Logging .NET.

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

Déploiement dans AWS

La Toolkit for Visual Studio prend en charge le déploiement d'applicationsAWS Elastic Beanstalk dans des conteneurs ou desAWS CloudFormation piles.

> **Note**
>
> Si vous utilisez Visual Studio Express Edition :
>
> - Vous pouvez utiliser l'interface de ligne de commande Docker pour déployer des applications dans des conteneurs Amazon ECS.
> - Vous pouvez utiliser la consoleAWS de gestion pour déployer des applications dans des conteneurs Elastic Beanstalk.
>
> Pour les déploiements d'Elastic Beanstalk, vous devez d'abord créer un package de déploiement Web. Pour plus d'informations, consultez Comment : créer un Package de déploiement Web dans Visual Studio. Pour le déploiement d'Amazon ECS, vous devez disposer d'une image Docker. Pour en savoir plus, consultez Outils Visual Studio pour Docker.

Rubriques

Utilisation de Publier dansAWSdans Visual Studio

Publier dansAWSest une expérience de déploiement interactive qui vous aide à publier vos applications .NET surAWScibles de déploiement, prenant en charge les applications ciblant .NET Core 3.1 et version ultérieure Utilisation de Publier dansAWSconserve votre flux de travail au sein de Visual Studio en rendant ces fonctionnalités de déploiement disponibles, directement depuis votre IDE :

- La possibilité de déployer votre application en un seul clic.
- Recommandations de déploiement en fonction de votre application.
- Création automatique de Dockerfile, en fonction de la pertinence et des exigences de l'environnement de destination de votre déploiement (cible de déploiement).
- Paramètres optimisés pour la création et la mise en package de vos applications, en fonction de votre objectif de déploiement.

> **Note**
>
> Pour plus d'informations sur la publication d'applications .NET Framework, consultez le guideCréation et déploiement d'applications .NET sur Elastic Beanstalk
> Vous pouvez également accéder à Publier dansAWSà partir de la CLI .NET. Pour plus d'informations, consultez le .Déployer des applications .NETAWSguide.

Rubriques

Prérequis

Pour publier avec succès des applications .NET sur unAWS, installez les éléments suivants sur votre appareil local :

- .NET Core 3.1+ (qui inclut .NET5 et .NET6) : Pour plus d'informations sur ces produits et pour obtenir des informations sur le téléchargement, rendez-vous sur leSite de téléchargement Microsoft.
- Node.js 14.x ou version ultérieure : Node.js est requis pour exécuterAWS Cloud Development Kit (AWS CDK). Pour télécharger ou obtenir plus d'informations sur Node.js, rendez-vous sur leSite de téléchargement Node.js.

> **Note**
>
> Publier dansAWSutiliseAWS CDKpour déployer votre application et l'ensemble de son infrastructure de déploiement en tant que projet unique. Pour plus d'informations surAWS CDKvoirCloud Development Kitguide.

- (Facultatif) Docker est utilisé lors du déploiement vers un service basé sur des conteneurs tel qu'Amazon ECS. Pour plus d'informations et télécharger Docker, consultezDocker télécharger site.

Types d'application pris

Avant de publier sur une nouvelle cible ou de la quitter, commencez par créer ou ouvrir l'un des types de projets suivants dans Visual Studio :

- Application ASP.NET Core
- Application de console .NET
- Blazor WebAssembly candidature

Publier des applications dansAWScibles

Lors de la publication vers une nouvelle cible, Publier versAWSvous guidera tout au long du processus en formulant des recommandations et en utilisant les paramètres courants. Si vous devez publier sur une cible précédemment configurée, vos préférences sont enregistrées et peuvent être ajustées, ou sont immédiatement disponibles pour un déploiement en un clic.

Publier vers une nouvelle cible

Ce qui suit explique comment configurer votre Publier dansAWSpréférences de déploiement, lorsque vous publiez sur une nouvelle cible.

1. À partir deAWSExplorateur, développezInformations d'identificationmenu déroulant, puis sélectionnezAWSprofil qui correspond à la région etAWSles services nécessaires à votre déploiement.
2. DéveloppezRegion (Région)menu déroulant, puis sélectionnezAWSrégion qui contient leAWSles services nécessaires à votre déploiement.

3. À partir de Visual StudioExplorer de solutions, ouvrez le menu contextuel (clic droit) du nom du projet, puis sélectionnezPublier dansAWS. Cela va ouvrirPublier dansAWS.
4. DePublier dansAWS, choisissezPublier dans une nouvelle ciblepour configurer un nouveau déploiement.

> **Note**
>
> Pour modifier vos informations d'identification de déploiement par défaut, choisissez ou cliquez sur le boutonModifierlien situé à côté duInformations d'identificationSection, dansPublier dansAWS.
> Pour contourner le processus de configuration cible, choisissezPublier sur une cible existante, puis sélectionnez votre configuration préférée dans la liste de vos cibles de déploiement précédentes.

5. À partir dePublier des cibles, choisissez uneAWSpour gérer le déploiement de votre application.
6. Lorsque vous êtes satisfait de votre configuration, choisissezPublierpour commencer le processus de déploiement.

> **Note**
>
> Après avoir lancé un déploiement,Publier dansAWSaffiche les mises à jour de statut suivantes :
>
> - Au cours du processus de déploiement,Publier dansAWSaffiche les informations sur la progression du déploiement.
> - À la suite du processus de déploiement,Publier dansAWSindique si le déploiement a réussi ou a échoué.
> - Après un déploiement réussi, leRessourcesfournit des informations supplémentaires sur la ressource qui a été créée. Ces informations varieront en fonction du type d'application et de la configuration du déploiement.

Publier sur une cible existante

La section suivante décrit comment republier votre application .NET sur unAWScible.

1. À partir deAWSExplorateur, développezInformations d'identificationmenu déroulant, puis sélectionnezAWSprofil qui correspond à la région etAWSles services nécessaires à votre déploiement.
2. DéveloppezRegion (Région)menu déroulant, puis sélectionnezAWSrégion qui contient leAWSles services nécessaires à votre déploiement.
3. À partir de Visual StudioExplorer de solutions, cliquez avec le bouton droit sur le nom du projet, puis sélectionnezPublier dansAWSpour ouvrirPublier dansAWS.
4. DePublier dansAWS, choisissezPublier sur une cible existantepour sélectionner votre environnement de déploiement dans une liste de cibles existantes.

   > **Note**
   >
   > Si vous avez récemment publié des applications dans leAWSCloud, ces applications sont affichées dans Publier surAWS.

5. Sélectionnez la cible de publication où vous souhaitez déployer votre application, puis cliquez surPublierpour commencer le processus de déploiement.

DéploiementAWS LambdaProjet avec l'interface de ligne de commande .NET Core

AWS Toolkit for Visual Studio inclut des modèles de projet AWS Lambda .NET Core pour Visual Studio. Vous pouvez déployer les fonctions Lambda intégrées dans Visual Studio grâce à l'interface de ligne de commande (CLI) .NET Core.

Rubriques

Prérequis

Avant d'utiliser l'interface de ligne de commande .NET Core pour déployer les fonctions Lambda, vous devez répondre aux exigences suivantes :

- Assurez-vous que Visual Studio 2015 Update 3 est installé.
- Install.NET Core pour Windows.
- Configurez l'interface de ligne de commande .NET Core pour fonctionner avec Lambda. Pour de plus amples informations, veuillez consulterInterface de ligne de commande .NET Coredans leAWS LambdaManuel du développeur.
- Installation de Toolkit for Visual Studio. Pour plus d'informations, consultez Installation du AWS Toolkit for Visual Studio.

Rubriques en relation

Les rubriques connexes suivantes peuvent vous être utiles lorsque vous utilisez l'interface de ligne de commande .NET Core pour déployer les fonctions Lambda :

- Pour plus d'informations sur les fonctions Lambda, consultezPrésentation d'AWSLambda ?dans leAWS LambdaManuel du développeur.
- Pour plus d'informations sur la création des fonctions Lambda dans Visual Studio, consultezAWS Lambda.
- Pour plus d'informations sur Microsoft .NET Core, consultez.NET Coredans la documentation en ligne de Microsoft.

Liste des commandes Lambda disponibles via l'interface de ligne de commande .NET Core

Pour répertorier les commandes Lambda disponibles via l'interface de ligne de commande .NET Core, procédez comme suit.

1. Ouvrez une fenêtre d'invite de commande et accédez au dossier contenant un projet Visual Studio .NET Core Lambda.
2. Saisissez `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>
```

Publication d'un projet .NET Core Lambda de l'interface de ligne de commande .NET Core

Les instructions suivantes supposent que vous avez créé une fonction AWS Lambda .NET Core dans Visual Studio.

1. Ouvrez une fenêtre d'invite de commande et accédez au dossier contenant votre projet Visual Studio .NET Core Lambda.
2. Saisissez `dotnet lambda deploy-function`.
3. Lorsque vous y êtes invité, saisissez le nom de la fonction à déployer. Il peut s'agit d'un nouveau nom ou de celui d'une fonction existante.
4. Lorsque vous y êtes invité, saisissezAWSRegion (la région sur laquelle votre fonction Lambda sera déployée).

5. Lorsque vous y êtes invité, sélectionnez ou créez le rôle IAM que Lambda assumera lors de l'exécution de la fonction.

En cas d'exécution réussie, le message New Lambda function created (Nouvelle fonction Lambda créée) s'affiche.

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

Si vous déployez une fonction existante, elle demande uniquementAWSRégion .

```
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
```

Une fois que votre fonction Lambda est déployée, elle est prête à l'emploi. Pour de plus amples informations, veuillez consulterExemples d'utilisation deAWSLambda.

Lambda surveille automatiquement les fonctions Lambda pour vous et présente les métriques via Amazon CloudWatch. Pour surveiller et dépanner votre fonction Lambda, consultezRésolution des problèmes et surveillanceAWSFonctions Lambda avec Amazon CloudWatch.

Déploiement sur Elastic Beanstalk

AWS Elastic Beanstalkest un service qui simplifie le processus de provisionnementAWSdes ressources pour votre application. Elastic Beanstalk fournit tous lesAWSl'infrastructure nécessaire pour déployer votre application ; Cette infrastructure comprend :

- des instances Amazon EC2 qui hébergent les fichiers exécutables et le contenu de votre application.
- un groupe Auto Scaling pour maintenir le nombre d'instances Amazon EC2 approprié pour prendre en charge votre application ;
- un équilibreur de charge Elastic Load Balancing qui achemine le trafic entrant vers l'instance Amazon EC2 qui a le plus de bande passante.

Toolkit for Visual Studio comporte un assistant qui simplifie la publication des applications via Elastic Beanstalk. Cet assistant est décrit dans les sections suivantes.

Pour plus d'informations sur Elastic Beanstalk, accédez au manuelDocumentation Elastic Beanstalk.

Rubriques

- Déploiement d'une application ASP.NET traditionnelle sur Elastic Beanstalk
- Déploiement d'une application ASP.NET Core vers Elastic Beanstalk (Legacy)
- Comment spécifierAWSInformations d'identification de sécurité de votre application
- Comment republier votre application dans un environnement Elastic Beanstalk (ancienne version)
- Déploiements personnalisés d'applications Elastic Beanstalk
- Déploiements personnalisés ASP.NET Core Elastic Beanstalk
- Support de plusieurs applications pour .NET et Elastic Beanstalk

Déploiement d'une application ASP.NET traditionnelle sur Elastic Beanstalk

Cette section explique comment utiliser l'assistant Publier sur Elastic Beanstalk, fourni dans le cadre de la Toolkit for Visual Studio, pour déployer une application via Elastic Beanstalk. Pour vous exercer, vous pouvez utiliser le projet de démarrage de l'instance d'une application web intégré à Visual Studio ou votre propre projet.

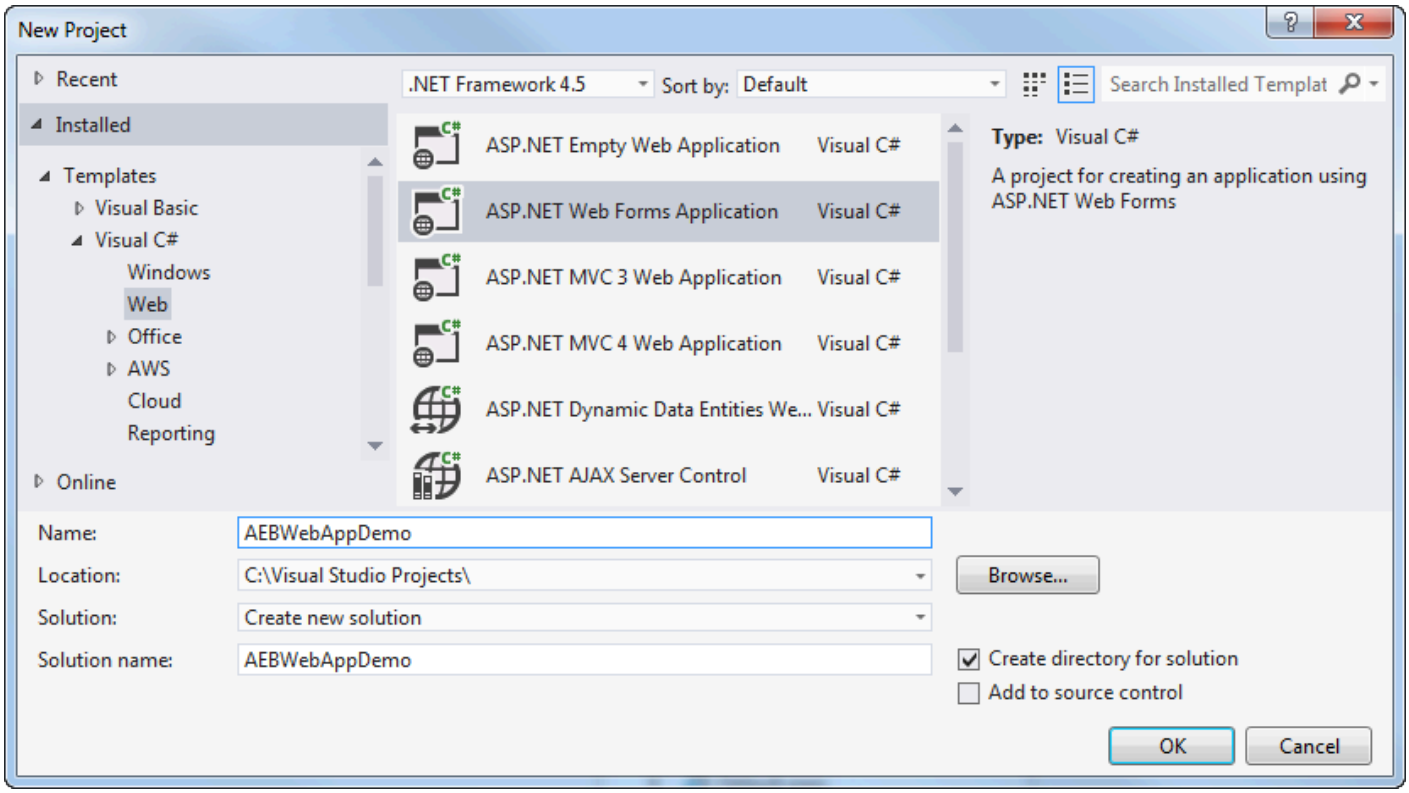
> **Note**
>
> L'assistant prend également en charge le déploiement des applications ASP.NET Core. Pour plus d'informations sur ASP.NET Core, consultez le guide des outils de déploiementAWS .NET et laAWS table des matières mise à jour.

> **Note**
>
> Avant de pouvoir utiliser l'assistant Publish to Elastic Beanstalk (Publier dans Elastic Beanstalk), vous devez télécharger et installer Web Deploy. L'assistant s'appuie sur Web Deploy pour déployer des applications et des sites web sur des serveurs web IIS (Internet Information Services).

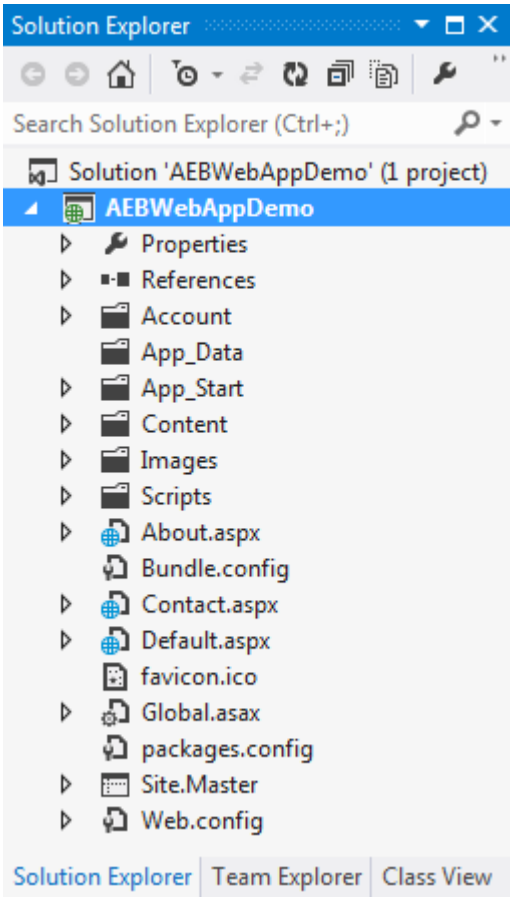
Pour créer un exemple de projet de démarrage d'une application web

1. Dans Visual Studio, dans le menu Fichier, choisissez Nouveau, puis choisissez Projet.

2. Dans le panneau de navigation de la boîte de dialogue New Project (Nouveau projet), développez Installations, développez Modèles, développez Visual C#, puis choisissez Web.
3. Dans la liste des modèles de projet web, choisissez-en un contenant les mots `Web` et `Application` dans sa description. Pour cet exemple, choisissez ASP.NET Web Forms Application (Application de formulaires web ASP.NET).

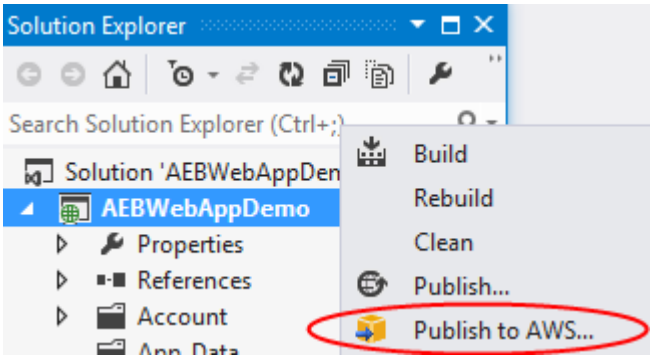


4. Dans la case Nom, tapez `AEBWebAppDemo`.
5. Dans la zone Emplacement, saisissez le chemin vers un dossier de solution sur votre machine de développement ou choisissez Parcourir, puis naviguez jusqu'à un dossier de solution, choisissez-le, et choisissez Select Folder (Sélectionner un dossier).
6. Vérifiez que la case Create directory for solution (Créer un répertoire pour la solution) est cochée. Dans la liste déroulante Solution, vérifiez que la case Create new solution (Créer une nouvelle solution) est cochée, et choisissez OK. Visual Studio crée une solution et un projet basés sur le modèle de projet ASP.NET Web Forms Application. Ensuite, Visual Studio affiche l'Explorateur de solutions dans lequel apparaissent la nouvelle solution et le nouveau projet.

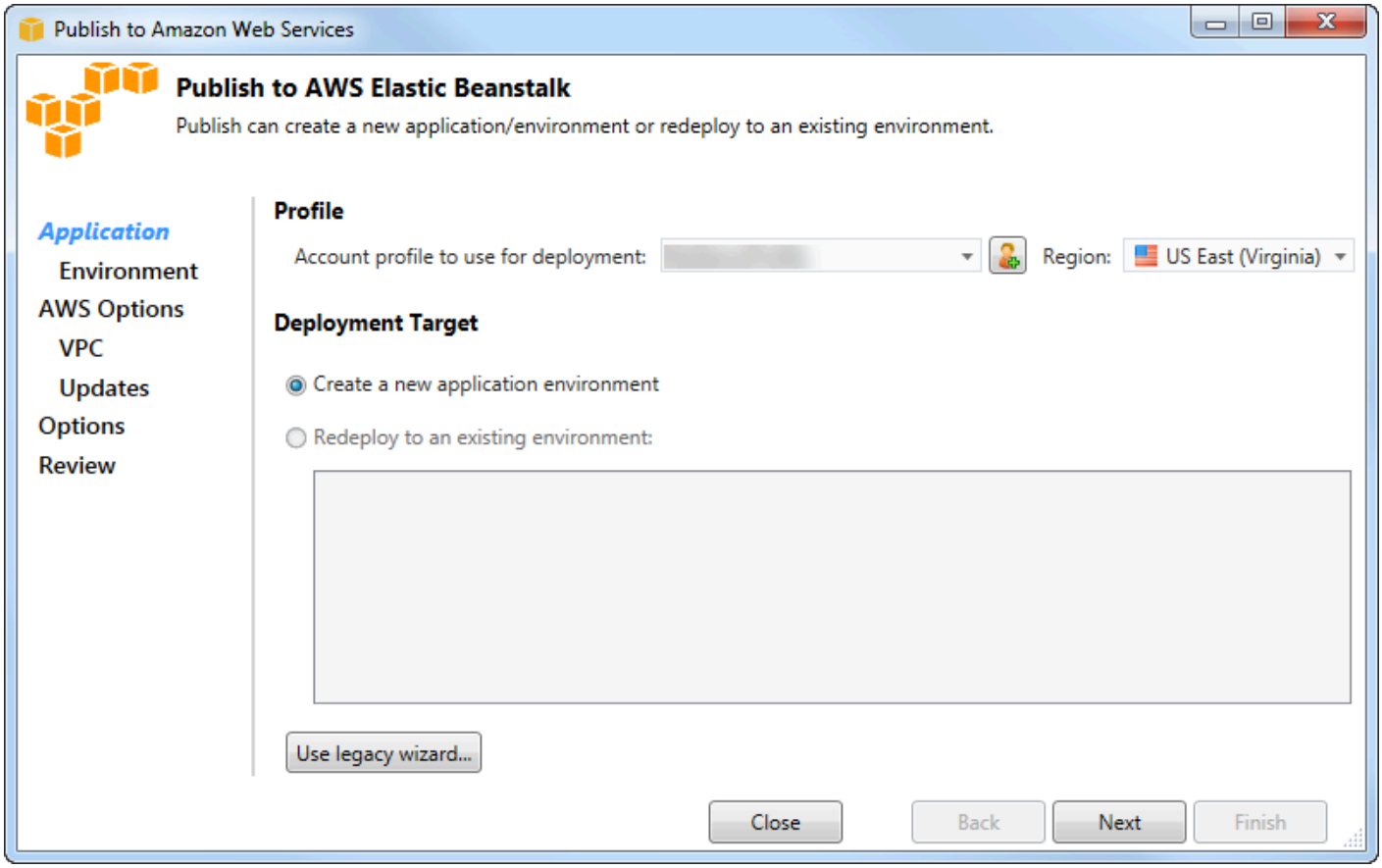


Pour déployer une application à l'aide de l'assistant Publish to Elastic Beanstalk (Publier dans Elastic Beanstalk)

1. Dans l'Explorateur de solutions, ouvrez le menu contextuel (clic droit) du dossier deWebAppDemo projet AEB correspondant au projet que vous avez créé dans la section précédente, ou ouvrez le menu contextuel du dossier de projet de votre propre application, puis choisissez Publier surAWS Elastic Beanstalk.



   L'assistant Publish to Elastic Beanstalk (Publier dans Elastic Beanstalk) s'ouvre.



2. Dans Profil, dans la liste déroulante Profil du compte à utiliser pour le déploiement, choisissez le profil deAWS compte que vous souhaitez utiliser pour le déploiement.

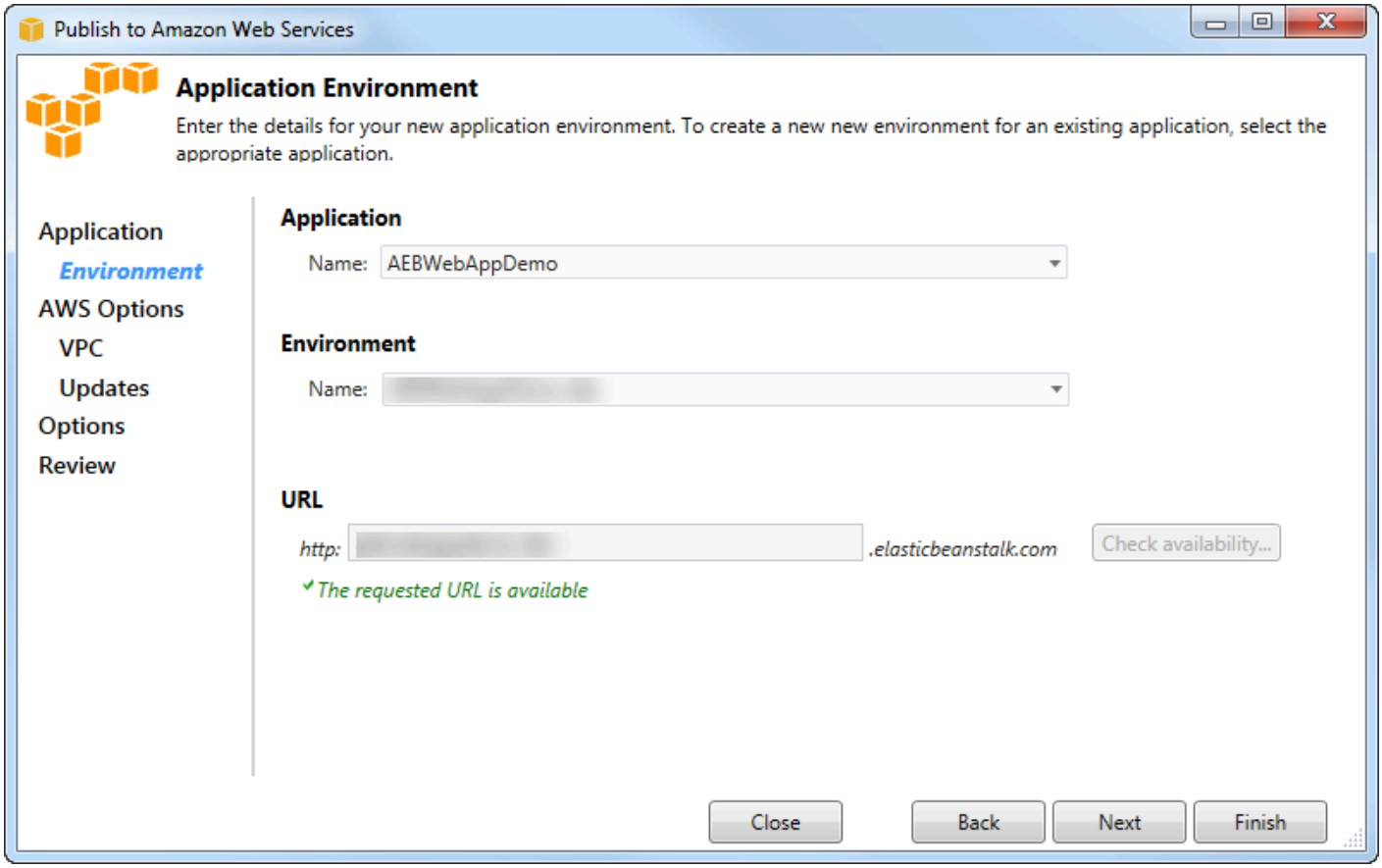
   Si vous avez unAWS compte que vous souhaitez utiliser, mais que vous n'avez pas encore créé de profil deAWS compte pour ce compte, vous pouvez cliquer sur le bouton avec le symbole plus (+) pour ajouter un profil deAWS compte.

3. Dans la liste déroulante Région, choisissez la région dans laquelle vous souhaitez qu'Elastic Beanstalk déploie l'application.

4. Dans Cible de déploiement, vous pouvez choisir Create a new application environment (Créer un nouvel environnement d’application) pour procéder au déploiement initial d'une application ou Redeploy to an existing environment (Redéployer vers un environnement existant) pour redéployer une application précédemment déployée. (Les déploiements précédents ont peut-être été effectués à l'aide de l'assistant ou de l'outil de déploiement autonome obsolète.) Si vous choisissez Redeploy to an existing environment (Redéployer vers un environnement existant), il vous faudra sans doute patienter le temps que l'assistant récupère les informations des déploiements précédents actuellement en cours d'exécution.

> **Note**
>
> Si vous choisissez Redeploy to an existing environment (Redéployer vers un environnement existant), choisissez un environnement dans la liste, puis choisissez Suivant, l'assistant vous amène directement à la page Application Options (Options de l'application). Si vous choisissez cette option, ignorez les instructions fournies ultérieurement dans cette section qui décrivent comment utiliser la page Application Options (Options de l'application).

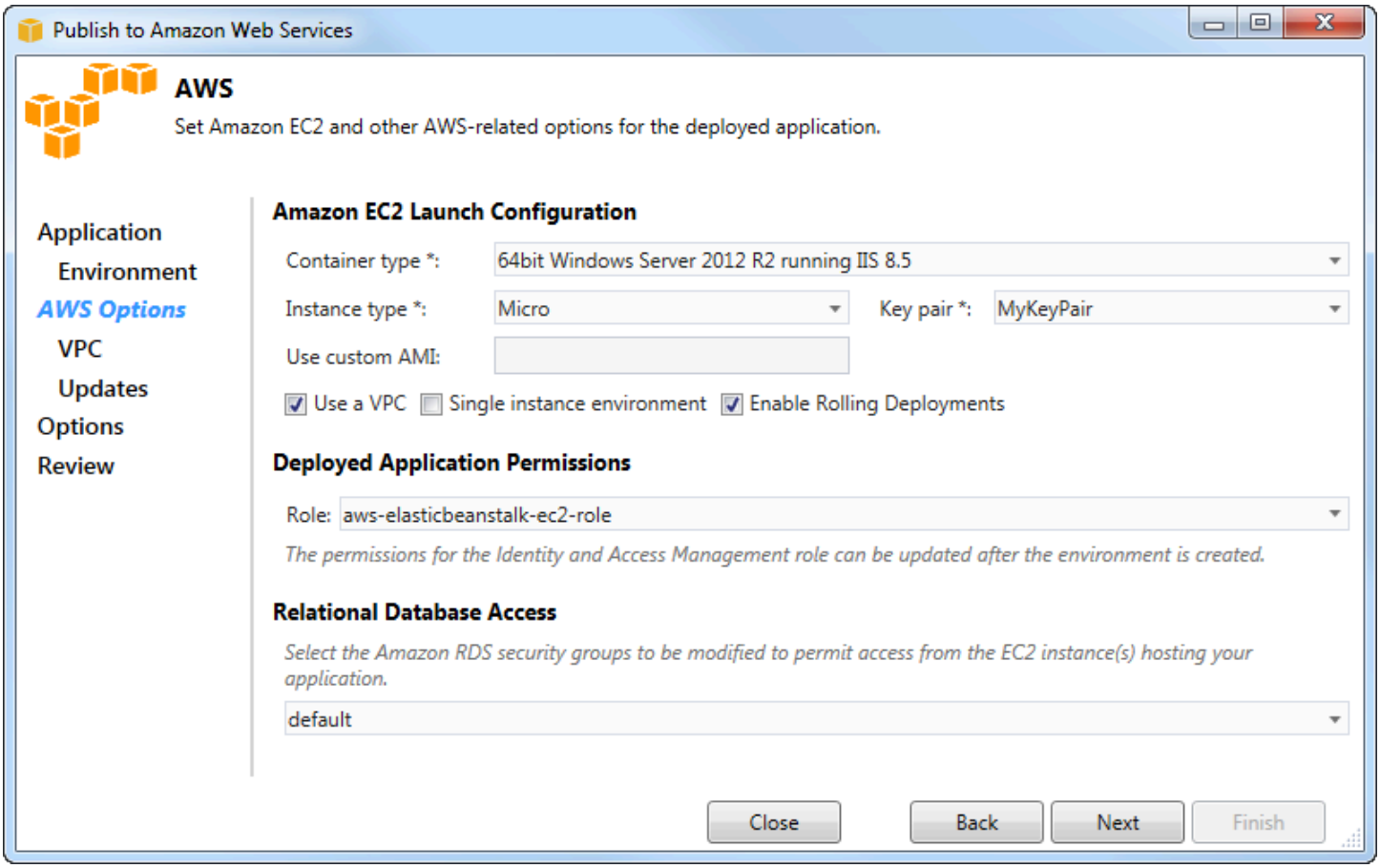
5. Choisissez Next (Suivant).



6. Sur la page Application Environment (Environnement de l'application), dans la zone Application, la liste déroulante Nom propose un nom par défaut pour l'application. Vous pouvez le modifier en en choisissant un différent de celui de la liste déroulante.
7. Dans la zone Environnement, dans la liste déroulante Nom, saisissez le nom de votre environnement Elastic Beanstalk. Dans ce contexte, le terme environnement fait référence à l'infrastructure fournie par Elastic Beanstalk pour votre application. Un nom par défaut peut-être déjà proposé dans cette liste déroulante. Si un nom par défaut n'est pas déjà proposé, vous

pouvez en saisir un ou en choisir un dans la liste déroulante, si des noms supplémentaires sont disponibles. Le nom de l'environnement ne peut pas dépasser 23 caractères.

8. Dans la zone URL, le champ propose un sous-domaine par défaut `.elasticbeanstalk.com` qui correspond à l'URL de votre application web. Vous pouvez modifier le sous-domaine par défaut en en saisissant un nouveau.
9. Choisissez Vérifier la disponibilité pour vous assurer que l'URL de votre application web n'est pas déjà utilisée.
10. Si vous pouvez l'utiliser, choisissez Suivant.



1. Sur la page AWSOptions, dans Configuration de lancement d'Amazon EC2, dans la liste déroulante Type de conteneur, choisissez un type Amazon Machine Image (AMI) qui sera utilisé pour votre application.
2. Dans la liste déroulante Type d'instance, spécifiez le type d'instance Amazon EC2 à utiliser. Pour cet exemple, nous vous conseillons d'utiliser Micro. Cela permettra de minimiser les coûts

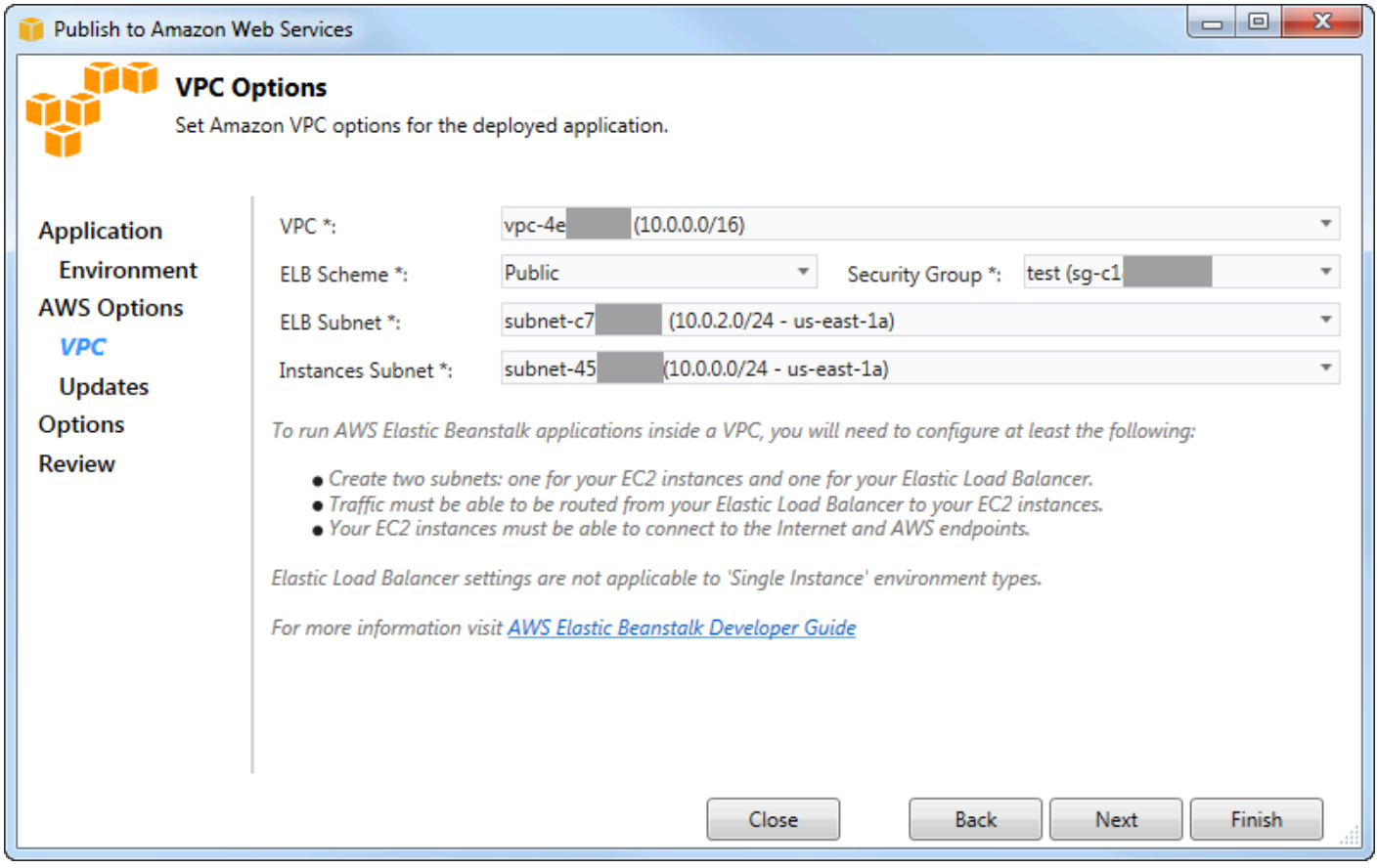
associés à l'exécution de l'instance. Pour plus d'informations sur les coûts Amazon EC2, consultez la page de Tarification EC2.

3. Dans la liste déroulante des paires de clés, choisissez une key pair d'instance Amazon EC2 à utiliser pour vous connecter aux instances qui seront utilisées pour votre application.
4. Dans le champ Use custom AMI (Utiliser une AMI personnalisée), vous pouvez éventuellement spécifier une AMI personnalisée qui remplacera celle indiquée dans la liste déroulante Container type (Type de conteneur). Pour plus d'informations sur la création d'une AMI personnalisée, consultez la section Utilisation d'AMI personnalisées dans le guide du développeurAWS Elastic Beanstalk et la section Création d'une AMI à partir d'une instance Amazon EC2.
5. Si vous souhaitez éventuellement lancer vos instances dans un VPC, cochez la case Use a VPC (Utiliser un VPC).
6. Si vous souhaitez lancer une instance Amazon EC2 unique, puis y déployer votre application, cochez la case Environnement à instance unique.

   Si vous cochez cette case, Elastic Beanstalk créera toujours un groupe Auto Scaling, mais ne le configurera pas. Si vous souhaitez configurer le groupe Auto Scaling ultérieurement, vous pouvez utiliser leAWS Management Console.
7. Si vous souhaitez éventuellement contrôler les conditions de déploiement de votre application sur les instances, cochez la case Enable Rolling Deployments (Autoriser la propagation des déploiements). Vous pouvez cochez cette case uniquement si vous n'avez pas coché la case Single instance environment (Environnement à instance unique).
8. Si votre application utiliseAWS des services tels qu'Amazon S3 et DynamoDB, le meilleur moyen de fournir des informations d'identification est d'utiliser un rôle IAM. Dans la zone Autorisations des applications déployées, vous pouvez choisir un rôle IAM existant ou en créer un que l'assistant utilisera pour lancer votre environnement. Les applications utilisant leAWS SDK for .NET utiliseront automatiquement les informations d'identification fournies par ce rôle IAM lorsqu'elles adressent une demande à unAWS service.
9. Si votre application accède à une base de données Amazon RDS, dans la liste déroulante de la zone Accès à la base de données relationnelle, cochez les cases à côté des groupes de sécurité Amazon RDS que l'assistant mettra à jour afin que vos instances Amazon EC2 puissent accéder à cette base de données.
10. Choisissez Next (Suivant).
    - Si vous avez coché la case Use a VPC (Utiliser un VPC), la page VPC Options (Options du VPC) apparaît.

- Si vous avez coché la case Enable Rolling Deployments (Autoriser la propagation des déploiements), mais pas la case Use a VPC (Utiliser un VPC), la page Rolling Deployments (Propagation des déploiements) apparaît. Ignorez les instructions fournies ultérieurement dans cette section qui décrivent comment utiliser la page Rolling Deployments (Propagation des déploiements).
- Si vous n'avez pas coché la case Use a VPC (Utiliser un VPC) ou Enable Rolling Deployments (Autoriser la propagation des déploiements), la page Application Options (Options de l'application) apparaît. Ignorez les instructions fournies ultérieurement dans cette section qui décrivent comment utiliser la page Application Options (Options de l'application).

11. Si vous avez coché la case Use a VPC (Utiliser un VPC), spécifiez les informations sur la page VPC Options (Options du VPC) pour lancer votre application dans un VPC.



Le VPC doit déjà avoir été créé. Si vous avez créé le VPC dans la Toolkit for Visual Studio, la Toolkit for Visual Studio remplira cette page pour vous. Si vous avez créé le VPC dans la consoleAWS de gestion, saisissez les informations relatives à votre VPC sur cette page.

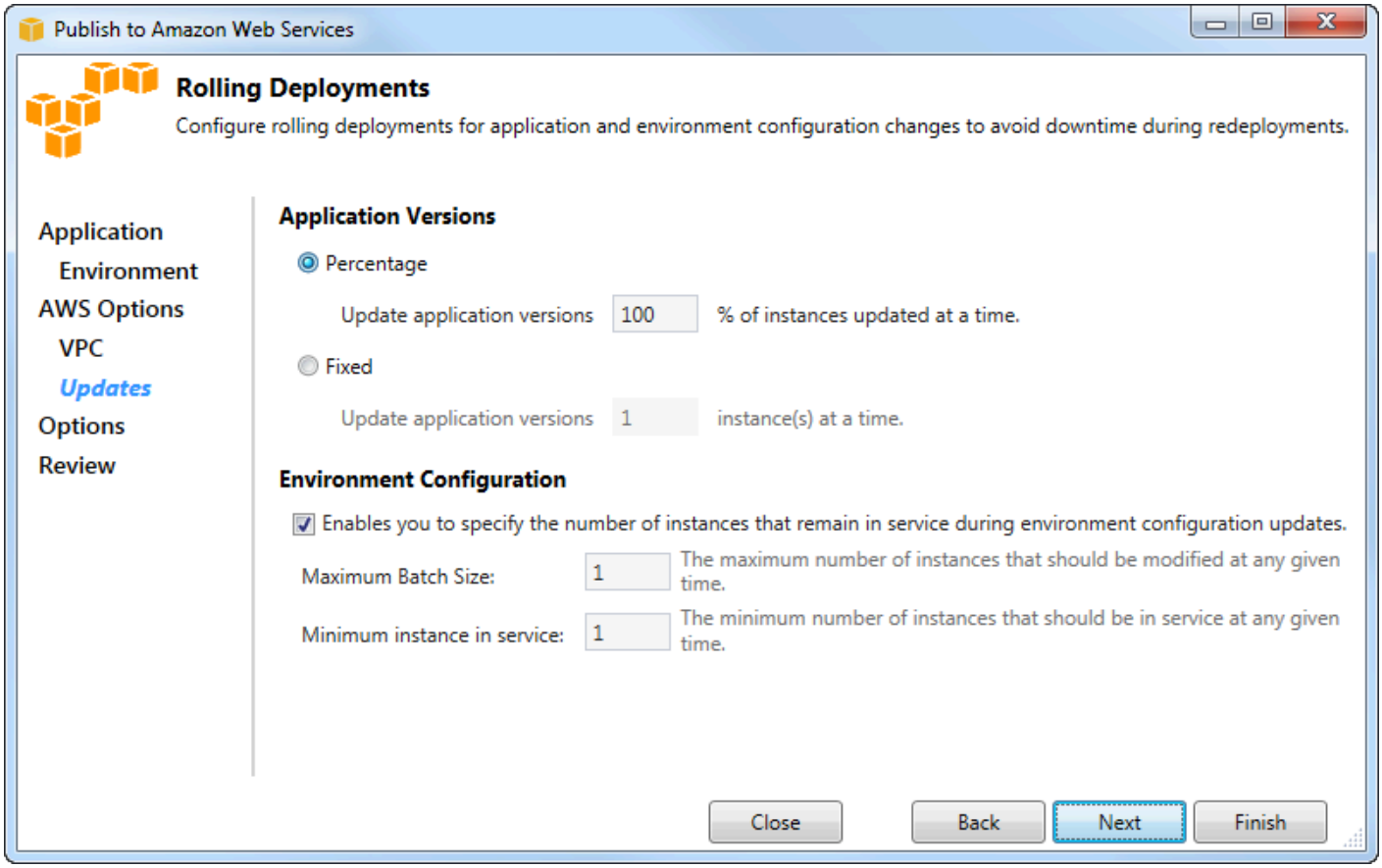
Principaux éléments à prendre en compte pour le déploiement sur un VPC

- Votre VPC a besoin d'au moins un sous-réseau public et un sous-réseau privé.
- Dans la liste déroulante ELB Subnet (Sous-réseau ELB), spécifiez le sous-réseau public. La Toolkit for Visual Studio déploie l'équilibreur de charge Elastic Load Balancing pour votre application sur le sous-réseau public. Le sous-réseau public est associé à une table de routage possédant une entrée qui pointe vers une passerelle Internet. Vous pouvez identifier une passerelle Internet car son ID commence par `igw-` (par exemple, `igw-83cddaex`). Les sous-réseaux publics que vous créez à l'aide de la Toolkit for Visual Studio possèdent des valeurs de balise qui les identifient comme publics.
- Dans la liste déroulante Instances Subnet (Sous-réseau d'instances), spécifiez le sous-réseau privé. La Toolkit for Visual Studio déploie les instances Amazon EC2 de votre application sur le sous-réseau privé.
- Les instances Amazon EC2 de votre application communiquent depuis le sous-réseau privé vers Internet via une instance Amazon EC2 du sous-réseau public qui effectue la traduction d'adresses réseau (NAT). Pour activer cette communication, vous avez besoin d'un groupe de sécurité VPC qui autorise le trafic à circuler du sous-réseau privé vers l'instance NAT. Spécifiez ce groupe de sécurité VPC dans la liste déroulante Groupe de sécurité.

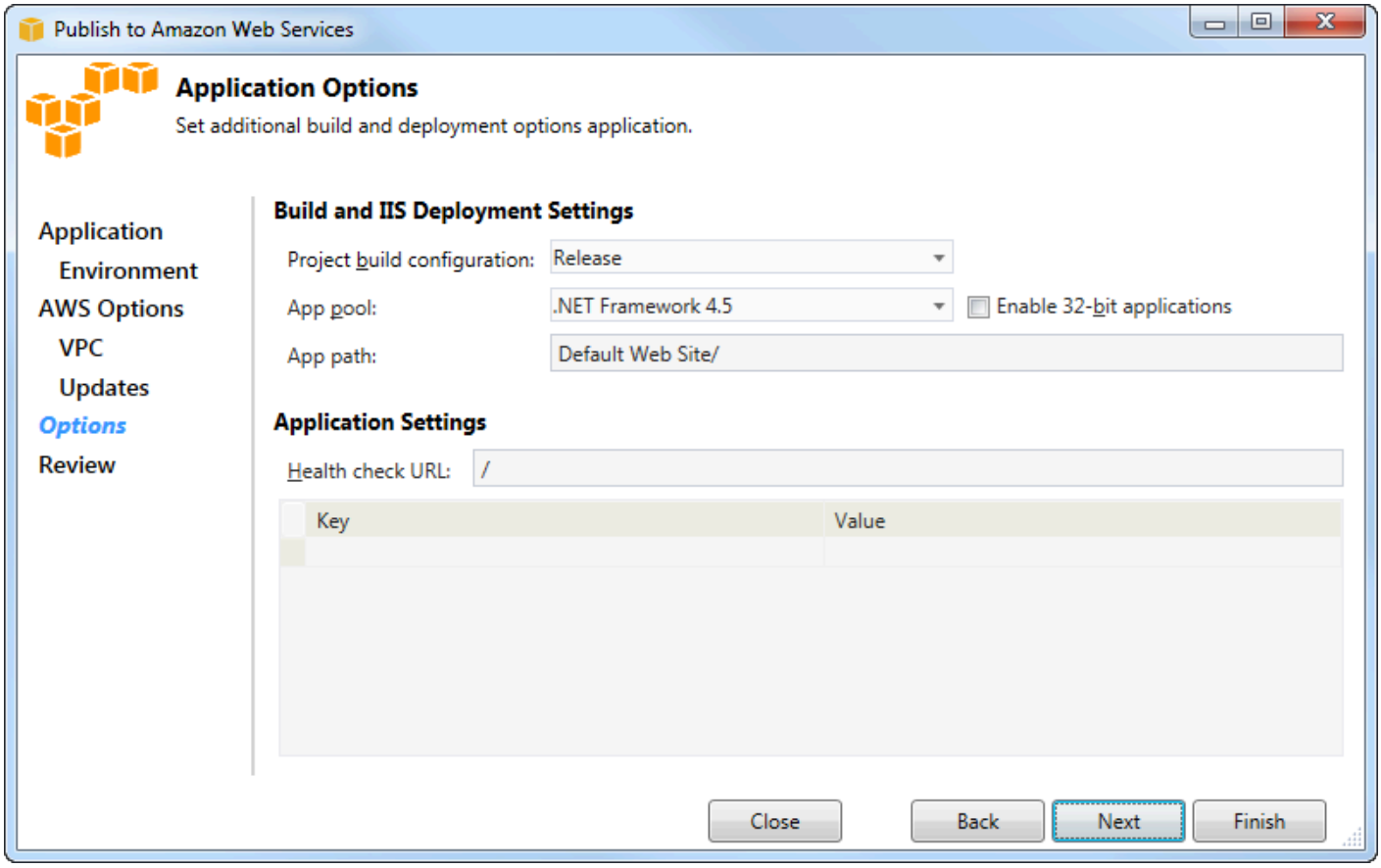
Pour plus d'informations sur la façon de déployer une application Elastic Beanstalk sur un VPC, consultez le guide du développeurAWS Elastic Beanstalk.

1. Une fois que vous avez rempli toutes les informations sur la page VPC Options (Options du VPC), choisissez Suivant.
   - Si vous avez coché la case Enable Rolling Deployments (Autoriser la propagation des déploiements), la page Rolling Deployments (Propagation des déploiements) apparaît.
   - Si vous n'avez pas coché la case Enable Rolling Deployments (Autoriser la propagation des déploiements), la page Application Options (Options de l'application) apparaît. Ignorez les instructions fournies ultérieurement dans cette section qui décrivent comment utiliser la page Application Options (Options de l'application).
2. Si vous avez coché la case Enable Rolling Deployments (Autoriser la propagation des déploiements), vous spécifiez les informations sur la page Rolling Deployments (Propagation des déploiements) pour configurer le déploiement des nouvelles versions de vos applications sur les instances d'un environnement à charge équilibrée. Par exemple, si vous disposez de quatre instances dans votre environnement et que vous souhaitez modifier le type d'instance, vous

pouvez configurer l'environnement pour modifier deux instances à la fois. Ceci permet de veiller à ce que votre application soit toujours en cours d'exécution pendant que vous y apportez des modifications.



3. Dans la zone Versions de l'application, choisissez une option pour contrôler les déploiements sur un pourcentage ou un nombre d'instances à la fois. Spécifiez le pourcentage ou le nombre souhaité.
4. (Facultatif) Dans la zone Configuration de l'environnement, cochez la case si vous souhaitez éventuellement spécifier le nombre d'instances qui restent en service pendant les déploiements. Si vous cochez cette case, spécifiez le nombre maximum d'instances qui doivent être modifiées à la fois, le nombre minimum d'instances qui doivent rester en service à la fois, ou les deux.
5. Choisissez Next (Suivant).
6. Sur la page Application Options (Options de l'application), vous spécifiez les informations sur les paramètres de génération, d'Internet Information Services (IIS) et d'application.

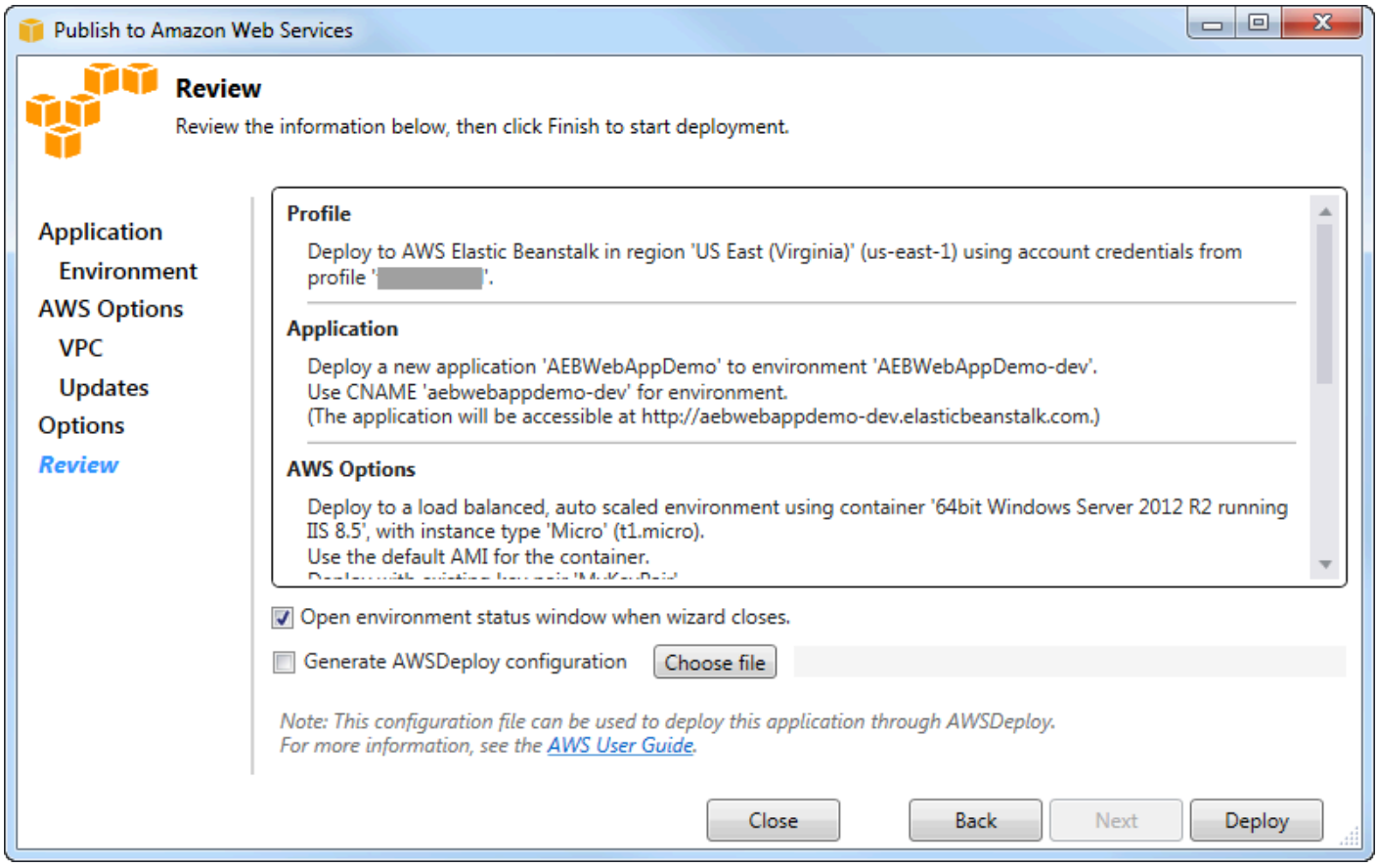


7. Dans la zone Build and IIS Deployment Settings (Paramètres de déploiement build et IIS), dans la liste déroulante Project build configuration (Configuration de la génération de projet), choisissez la configuration de la génération cible. Si l'assistant peut la trouver, Publier apparaît, sinon la configuration active s'affiche dans cette zone.
8. Dans la liste déroulante App pool (Groupe d'applications), choisissez la version .NET Framework requise pour votre application. La version .NET Framework correcte doit déjà être affichée.
9. Si votre application est en 32 bits, cochez la case Activer les applications 32 bits.
10. Dans le champ App path (Chemin d'application), spécifiez le chemin que les IIS utiliseront pour déployer l'application. Par défaut, Default Web Site/(Site Internet par défaut/) est spécifié, ce qui se traduit généralement par le chemin `c:\inetpub\wwwroot`. Si vous spécifiez un chemin différent de Default Web Site/(Site Internet par défaut/), l'assistant place une redirection dans le chemin Default Web Site/(Site Internet par défaut/) qui pointe vers le chemin que vous avez spécifié.
11. Dans la zone Paramètres de l'application, dans la zone URL de vérification de l'Health, saisissez une URL pour qu'Elastic Beanstalk vérifie si votre application Web répond toujours. Cette URL est relative à l'URL du serveur racine. L'URL du serveur racine est spécifiée par défaut. Par exemple, si l'URL complète est `example.com/site-is-up.html`, vous saisirez `/site-is-up.html`.

12. Dans la zone Clé et Valeur, vous pouvez spécifier n'importe quelle paire clé/valeur que vous souhaitez ajouter au fichier `Web.config` de votre application.

> **Note**
>
> Bien que cela ne soit pas recommandé, vous pouvez utiliser la zone Clé et Valeur pour spécifier lesAWS informations d'identification sous lesquelles votre application doit s'exécuter. L'approche préférée consiste à spécifier un rôle IAM dans la liste déroulante Rôle de Identity and Access Management sur la page AWSOptions. Toutefois, si vous devez utiliser desAWS informations d'identification au lieu d'un rôle IAM pour exécuter votre application, dans la ligne Clé, choisissez AWSAccessKey. Sur la ligne Valeur, saisissez la clé d'accès. Répétez ces étapes pour AWSSecretKey.

13. Choisissez Next (Suivant).



14. Sur la page Révision, examinez les options que vous avez configuré, et cochez la case Open environment status window when wizard closes (Ouvrir la fenêtre du statut de l'environnement quand l'assistant ferme).

15. Si tout vous paraît correct, choisissez Déploiement.

> **Note**
>
> Lorsque vous déployez l'application, le compte actif est facturé pour lesAWS ressources utilisées par l'application.

Les informations sur le déploiement apparaissent dans la barre d'état Visual Studio et la fenêtre Sortie. Cette opération peut prendre plusieurs minutes. Lorsque le déploiement est terminé, un message de confirmation s'affiche dans la fenêtre Sortie.

16. Pour supprimer le déploiement, développez le nœud Elastic Beanstalk dansAWS Explorer, ouvrez le menu contextuel (clic droit) pour le sous-nœud pour le déploiement, puis choisissez Supprimer. Le processus de suppression peut prendre quelques minutes.

Déploiement d'une application ASP.NET Core vers Elastic Beanstalk (Legacy)

> **Important**
>
> Cette documentation fait référence aux services et fonctionnalités existants. Pour obtenir des guides et du contenu mis à jour, consultez le guide de l'outil de déploiementAWS .NET et la mise à jour de la table des matières du Déploiement vers laAWS table des matières.

AWS Elastic Beanstalkest un service qui simplifie le processus de provisionnementAWS des ressources pour votre application. AWS Elastic Beanstalkfournit toute l'AWSinfrastructure nécessaire au déploiement de votre application.

La Toolkit for Visual Studio prend en charge le déploiement d'applications ASP.NET Core àAWS l'aide d'Elastic Beanstalk. ASP.NET Core est la nouvelle version d'ASP.NET avec une architecture modularisée qui réduit les frais généraux et rationalise l'exécution de votre application dans le cloud.

AWS Elastic Beanstalkfacilite le déploiement d'applications dans une variété de langues différentes pourAWS. Elastic Beanstalk prend en charge à la fois les applications ASP.NET traditionnelles et les applications ASP.NET Core. Cette rubrique décrit le déploiement des applications ASP.NET Core.

Utilisation de l'assistant de déploiement

Toolkit for Visual Studio est la méthode la plus simple pour déployer des applications ASP.NET Core vers Elastic Beanstalk.

Si vous avez utilisé la boîte à outils avant pour déployer l'ASP traditionnel. applications ASP.NET traditionnelles, vous trouverez l'expérience avec les applications ASP.NET Core assez semblable. Dans les étapes ci-dessous, nous allons examiner l'expérience de déploiement.

Si vous n'avez jamais utilisé la boîte à outils, vous devez l'installer, puis y enregistrer vosAWS informations d'identification. Reportez-vous à la section Comment spécifier les informations d'identification deAWS sécurité pour votre application pour la documentation Visual Studio pour plus de détails sur la procédure à suivre.

Pour déployer une application Web ASP.NET Core, cliquez avec le bouton droit sur le projet dans l'Explorateur de solutions et sélectionnez Publier surAWS...

Sur la première page de l'assistant de publication dans leAWS Elastic Beanstalk déploiement, choisissez de créer une nouvelle application Elastic Beanstalk. Une application Elastic Beanstalk est un ensemble logique de composants Elastic Beanstalk, y compris des environnements, des versions, et des configurations d'environnement. L'assistant de déploiement génère une application qui, en retour, contient un ensemble de versions de l'application et d'environnements. Les environnements contiennent lesAWS ressources réelles qui exécutent une version d'application. Chaque fois que vous déployez une application, une nouvelle version de l'application est créée et l'assistant pointe l'environnement vers cette version. Pour en savoir plus sur ces concepts, consultez Composants Elastic Beanstalk.

Ensuite, définissez les noms de l'application et de son premier environnement. Chaque environnement possède un CNAME unique qui lui est associé et que vous pouvez utiliser pour accéder à l'application à la fin du déploiement.

La page suivante, AWSOptions, vous permet de configurer le type deAWS ressources à utiliser. Dans cet exemple, conservez les valeurs par défaut, sauf pour la section Paire de clés. Les paires de clés vous permettent de récupérer le mot de passe administrateur Windows, afin que vous puissiez vous connecter à la machine. Si vous n'avez pas encore créé de paire de clés, sélectionnez Créer une paire de clés.

Autorisations

La page Autorisations est utilisée pour attribuer desAWS informations d'identification aux instances EC2 qui exécutent votre application. C'est important si votre application les utiliseAWS SDK for .NET pour accéder à d'autresAWS services. Si vous n'utilisez pas d'autres services depuis votre application, conservez les valeurs par défaut sur cette page.

Options de l'application

Les détails sur la page Application Options (Options de l'application) sont différents de ceux spécifiés lors du déploiement d'applications ASP.NET traditionnelles. Ici, vous spécifiez la configuration et l'infrastructure de la génération utilisées pour empaqueter l'application ainsi que le chemin de ressource IIS pour l'application.

Après avoir renseigné la page Application Options (Options de l'application), cliquez sur Suivant pour examiner les paramètres, puis cliquez sur Déploiement pour lancer le processus de déploiement.

Vérification de l'état de l'environnement

Une fois l'application empaquetée et téléchargéeAWS, vous pouvez vérifier l'état de l'environnement Elastic Beanstalk en ouvrant la vue de l'état de l'environnement depuis l'AWSExplorateur dans Visual Studio.

Les événements sont affichés dans la barre d'état à mesure que l'environnement est mis en service. Une fois que tout est terminé, l'environnement passe en état sain. Vous pouvez cliquer sur l'URL pour afficher le site. À partir de là, vous pouvez également extraire les journaux de l'environnement ou du poste de travail distant vers les instances Amazon EC2 qui font partie de votre environnement Elastic Beanstalk.

Le premier déploiement d'une application prendra un peu plus de temps que les redéploiements suivants, car il crée de nouvellesAWS ressources. À mesure que vous itérez sur votre application pendant le développement, vous pouvez rapidement redéployer en réutilisant l'assistant, ou en sélectionnant l'option Republish (Republier) lorsque vous cliquez avec le bouton droit sur le projet.

Republiez les packages de votre application en utilisant les paramètres de l'exécution précédente via l'assistant de déploiement et télécharge le bundle d'applications dans l'environnement Elastic Beanstalk existant.

Comment spécifierAWSInformations d'identification de sécurité de votre application

LeAWScompte que vous spécifiez dans lePublication sur Elastic Beanstalkl'assistant estAWSque l'assistant utilisera pour le déploiement sur Elastic Beanstalk.

Bien que cela ne soit pas recommandé, vous pouvez également spécifierAWSles informations d'identification du compte que votre application utilisera pour accéderAWSservices une fois qu'il a été déployé. L'approche préférée consiste à spécifier un rôle IAM. DansPublication sur Elastic Beanstalk, vous utilisez pour celaIdentity and Access Managementdans laAWSOptions. Dans l'héritéPublier sur Amazon Web Services, vous utilisez pour celaRôle IAMdans laAWSOptions.

Si vous devez utiliserAWSles informations d'identification du compte au lieu d'un rôle IAM, vous pouvez spécifier leAWSInformations d'identification de votre compte pour votre application de l'une des manières suivantes :

- Référencez un profil correspondant àAWSInformations d'identification du compte dans`appSettings`élément du projet`Web.config`dans le fichier. (Pour créer un profil, consultezConfigurationAWSInformations d'identification.) L'exemple suivant spécifie les informations d'identification dont le nom de profil est `myProfile`.

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

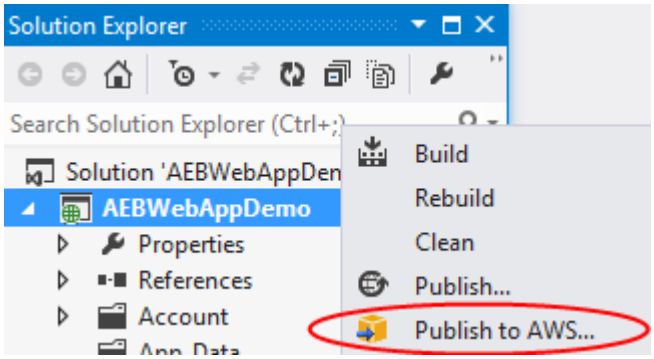
- Si vous utilisezPublication sur Elastic Beanstalkmagicien, sur leOptions de l'application, dans laClé row of the CléetValeur, choisissezAWSAccessKey. Sur la ligne Valeur, saisissez la clé d'accès. Répétez ces étapes pourAWSSecretKey.
- Si vous utilisez l'assistant existant Publish to Amazon Web Services (Publier dans Amazon Web Services), sur la page Application Options (Options de l’application), dans la zone Application Credentials (Informations d’identification de l’application), choisissez Use these credentials (Utiliser ces informations d’identification), puis saisissez la clé d'accès et la clé d'accès secrète dans les zones Clé d'accès et Clé secrète.

Comment republier votre application dans un environnement Elastic Beanstalk (ancienne version)

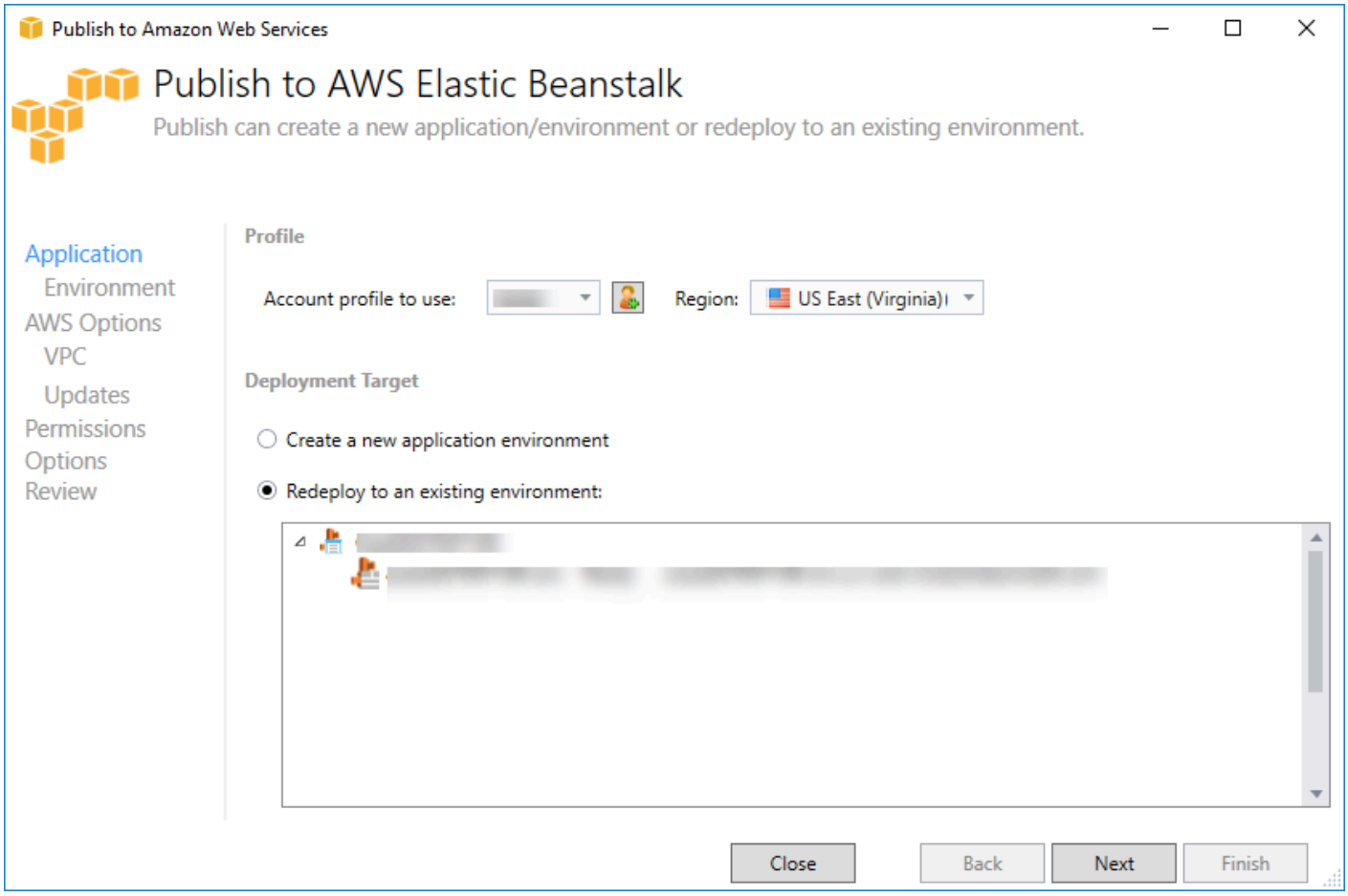
> **Important**
>
> Cette documentation fait référence aux services et fonctionnalités existants. Pour obtenir des guides et du contenu mis à jour, consultez le guide de l'outil de déploiementAWS .NET et la mise à jour de la table des matières du Déploiement vers laAWS table des matières.

Vous pouvez modifier votre application en apportant des modifications discrètes, puis en publiant à nouveau une nouvelle version dans votre environnement Elastic Beanstalk déjà lancé.

1. Dans Solution Explorer (Explorateur de solutions), ouvrez le menu contextuel (clic droit) du dossier deWebAppDemo projet AEB du projet que vous avez publié dans la section précédente, puis sélectionnez Publish to (Publier dans)AWS Elastic Beanstalk.

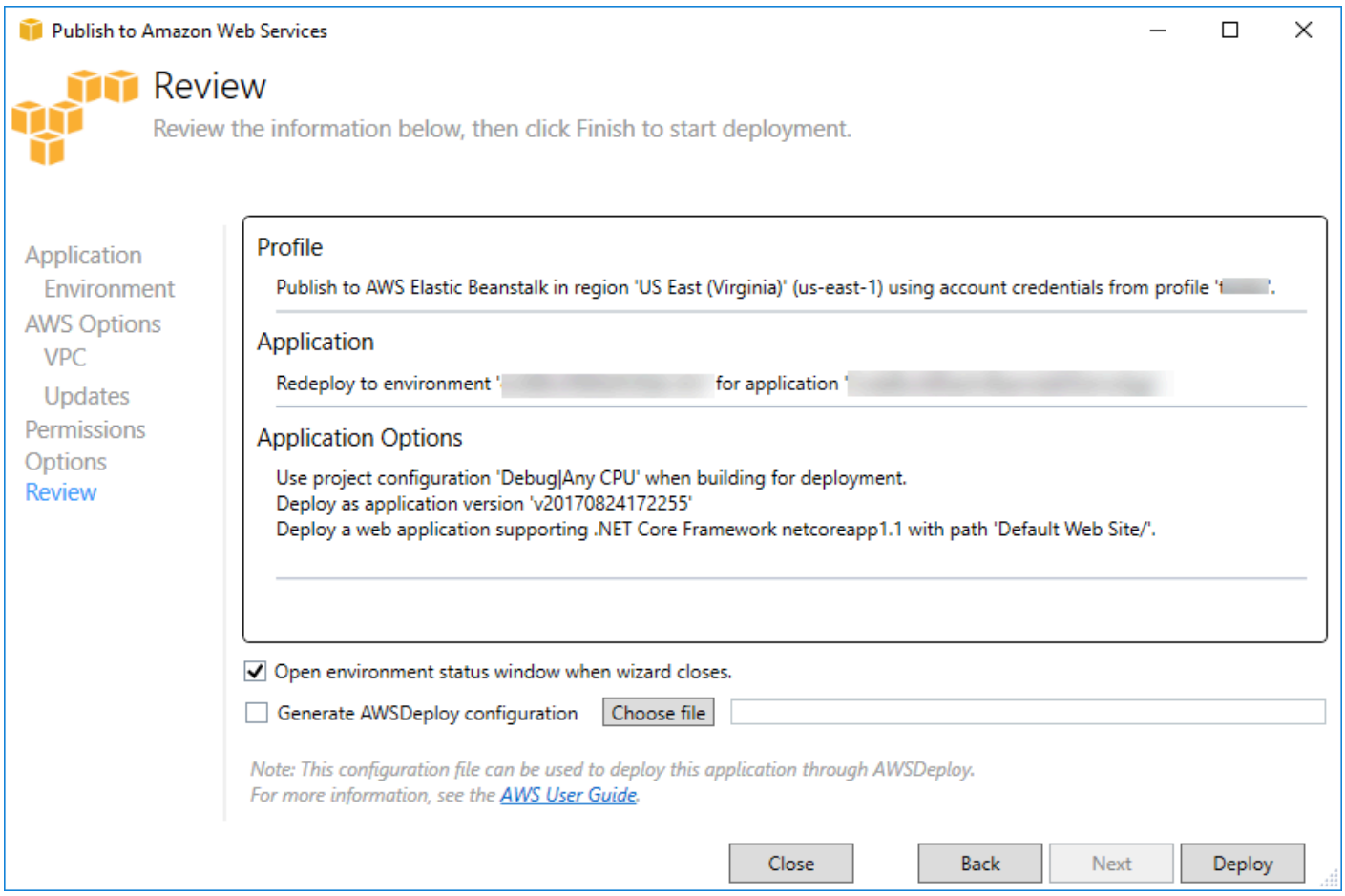


   L'assistant Publish to Elastic Beanstalk (Publier dans Elastic Beanstalk) s'ouvre.



2. Sélectionnez Redeploy to an existing environment (Redéployer dans un environnement existant) et choisissez l'environnement dans lequel vous avez effectué la publication précédemment. Cliquez sur Next (Suivant).

   L'assistant Révision apparaît.



3. Cliquez sur Déploiement. L'application sera redéployée dans le même environnement.

Vous ne pouvez pas republier si votre application est en cours de lancement ou de mise hors service.

Déploiements personnalisés d'applications Elastic Beanstalk

Cette rubrique décrit comment le manifeste de déploiement du conteneur Microsoft Windows d'Elastic Beanstalk prend en charge les déploiements personnalisés d'applications.

Les déploiements personnalisés d'applications sont une fonctionnalité puissante destinée aux utilisateurs expérimentés qui souhaitent exploiter la puissance d'Elastic Beanstalk pour créer et gérer leurAWSmais veulent avoir un contrôle complet sur la façon dont leur application est déployée. Pour un déploiement personnalisé d'applications, vous créez des scripts Windows PowerShell pour les trois actions différentes exécutées par Elastic Beanstalk. L'action d'installation est utilisée lorsqu'un déploiement est lancé, le redémarrage est utilisé lorsque l'API `RestartAppServer` est appelée depuis la boîte à outils ou la console web, et la désinstallation est appelée sur n'importe quel déploiement antérieur à chaque nouveau déploiement.

Par exemple, vous pouvez disposer d'une application ASP.NET que vous souhaitez déployer tandis que votre équipe de documentation écrit un site web statique qu'elle souhaite inclure au déploiement. Pour ce faire, écrivez votre manifeste de déploiement comme suit :

```
{
  "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"
          }
        }
      }
    ]
  }
}
```

Les scripts répertoriés pour chaque action doivent se trouver dans la solution groupée d'applications associée au fichier manifeste de déploiement. Dans cet exemple, la solution groupée d'applications renferme également un fichier documentation.zip qui contient un site web statique créé par votre équipe de documentation.

Le script `install.ps1` extrait le fichier zip et configure le champ 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}
```

Étant donné que votre application s'exécute dans IIS, l'action de redémarrage appellera une réinitialisation d'IIS.

```
iisreset /timeout:1
```

Pour désinstaller des scripts, il est important de nettoyer tous les paramètres et les fichiers utilisés pendant la phase d'installation. De cette façon, lors de la phase d'installation de la nouvelle version, vous pouvez éviter toute collision avec des déploiements précédents. Dans cet exemple, vous devez supprimer l'application IIS pour le site web statique et supprimer les fichiers de ce dernier.

```
powershell.exe -Command {Remove-WebApplication -Name documentation}
Remove-Item -Recurse -Force 'c:\inetpub\wwwroot\documentation'
```

Avec ces fichiers de script et le fichier documentation.zip inclus dans votre solution groupée d'applications, le déploiement crée l'application ASP.NET et déploie le site de la documentation.

Dans cet exemple, nous avons choisi un exemple simple qui déploie un simple site web statique, mais grâce au déploiement personnalisé d'applications, vous pouvez déployer n'importe quel type d'application et laisser Elastic Beanstalk en gérer leAWSressources pour cela.

Déploiements personnalisés ASP.NET Core Elastic Beanstalk

Cette rubrique décrit le mode de fonctionnement et de personnalisation du déploiement lors de la création d'applications ASP.NET Core avec Elastic Beanstalk et Toolkit for Visual Studio.

Après avoir exécuté l'assistant de déploiement dans la Toolkit for Visual Studio, la boîte à outils groupe l'application et l'envoie à Elastic Beanstalk. La première étape de la création d'une solution groupée d'applications consiste à utiliser la nouvelle interface de ligne de commande dotnet afin de préparer l'application pour la publication à l'aide de la commande publish. L'infrastructure et la configuration sont transmises depuis les paramètres de l'assistant vers la commande publish. Ainsi, si vous avez sélectionné Publier pour `configuration` et netcoreapp1.0 pour `framework`, la boîte à outils exécute la commande suivante :

```
dotnet publish --configuration Release --framework netcoreapp1.0
```

Lorsque la commande publish est terminée, la boîte à outils écrit le nouveau manifeste de déploiement dans le dossier de publication. Le manifeste de déploiement est un fichier JSON nomméaws-windows-deployment-manifest.json, que le conteneur Elastic Beanstalk Windows (version 1.2 ou supérieure) lit pour identifier le mode de déploiement de l'application. Par exemple, pour une application ASP.NET Core que vous souhaitez déployer à la racine d'IIS, la boîte à outils génère un fichier manifeste semblable à ce qui suit :

```
{
  "manifestVersion": 1,
  "deployments": {

    "aspNetCoreWeb": [
      {
        "name": "app",
        "parameters": {
          "appBundle": ".",
          "iisPath": "/",
          "iisWebSite": "Default Web Site"
        }
      }
    ]
  }
}
```

La propriété `appBundle` indique l'endroit où les bits de l'application sont en lien avec le fichier manifeste. Cette propriété peut pointer vers un annuaire ou une archive ZIP. Les propriétés `iisPath` et `iisWebSite` indiquent l'endroit où héberger l'application dans IIS.

Personnalisation du manifeste

La boîte à outils écrit uniquement le fichier manifeste s'il n'existe pas déjà dans le dossier de publication. Si le fichier existe, la boîte à outils met à jour les propriétés `appBundle`, `iisPath` et `iisWebSite` dans la première application répertoriée sous la section `aspNetCoreWeb` du manifeste. Cela vous permet d'ajouter aws-windows-deployment-manifest.json à votre projet et de personnaliser le manifeste. Par exemple, pour une application web ASP.NET Core dans Visual Studio, ajoutez un nouveau fichier JSON à la racine du projet et nommez-le aws-windows-deployment-manifest.json.

Le manifeste doit être nommé aws-windows-deployment-manifest.json et il doit se trouver à la racine du projet. Le conteneur Elastic Beanstalk recherche le manifeste dans la racine et s'il le trouve, il appelle les outils de déploiement. Si le fichier n'existe pas, le conteneur Elastic Beanstalk utilise les anciens outils de déploiement, ce qui suppose que l'archive estmsDeployArchive.

Pour veiller à ce que la commande `publish` de l'interface de ligne de commande dotnet inclut le manifeste, mettez à jour le fichier `project.json` pour y inclure le fichier manifeste dans la section inclure sous `include` dans `publishOptions`.

```
{
   "publishOptions": {
     "include": [
       "wwwroot",
       "Views",
       "Areas/**/Views",
       "appsettings.json",
       "web.config",
       "aws-windows-deployment-manifest.json"
     ]
   }
 }
```

Maintenant que vous avez déclaré le manifeste de façon à ce qu'il soit inclus dans la solution groupée d'applications, vous pouvez configurer la façon dont vous souhaitez déployer l'application. Vous pouvez personnaliser le déploiement au-delà de ce que l'assistant de déploiement prend en charge.AWSa défini un schéma JSON pour laaws-windows-deployment-manifest.json, et lorsque vous avez installé Toolkit for Visual Studio, la configuration a enregistré l'URL pour le schéma.

Lorsque vous ouvrez `windows-deployment-manifest.json`, vous voyez l'URL du schéma sélectionnée dans la zone déroulante Schema. Vous pouvez accéder à l'URL pour obtenir une description complète de ce qui peut être défini dans le manifeste. Avec le schéma sélectionné, Visual Studio met à disposition IntelliSense pendant que vous modifiez le manifeste.

Vous pouvez procéder à une personnalisation en configurant le groupe d'applications IIS sous lequel l'application sera exécutée. L'exemple suivant montre comment vous pouvez définir un groupe d'applications IIS (« customPool ») qui recycle le processus toutes les 60 minutes, et l'attribuer à l'application à l'aide de `"appPool": "customPool"`.

```
{
  "manifestVersion": 1,
```

```
  "iisConfig": {
    "appPools": [
      {
        "name": "customPool",
        "recycling": {
          "regularTimeInterval": 60
        }
      }
    ]
  },
  "deployments": {
    "aspNetCoreWeb": [
      {
        "name": "app",
        "parameters": {
          "appPool": "customPool"
        }
      }
    ]
  }
}
```

De plus, le manifeste peut déclarer des scripts Windows PowerShell pour qu'ils s'exécutent avant et après l'installation, redémarrent et désinstallent des actions. Par exemple, le manifeste suivant exécute le script Windows PowerShell `PostInstallSetup.ps1` pour poursuivre la configuration après le déploiement de l'application ASP.NET Core sur IIS. Lorsque vous ajoutez des scripts de ce type, veillez à ce qu'ils soient ajoutés dans la section inclure sous publishOptions dans le fichier `project.json`, comme vous l'aviez fait avec le fichier `aws-windows-deployment-manifest.json`. Sinon, les scripts ne seront pas inclus dans le cadre de la commande publish de l'interface de ligne de commande dotnet.

```
{
  "manifestVersion": 1,
  "deployments": {
    "aspNetCoreWeb": [
      {
        "name": "app",
        "scripts": {
          "postInstall": {
            "file": "SetupScripts/PostInstallSetup.ps1"
          }
        }
```

```
      }
    ]
  }
}
```

Qu'en est-il des .ebextensions ?

Le haricot Elastic Beanstalk.ebextensionsLes fichiers de configuration sont pris en charge comme dans tous les autres conteneurs Elastic Beanstalk. Pour inclure des .ebextensions dans une application ASP.NET Core, ajoutez l'annuaire `.ebextensions` à la section `include` sous `publishOptions` dans le fichier `project.json`. Pour plus d'informations sur les .ebextensions, consultez le Manuel du développeur Elastic Beanstalk.

Support de plusieurs applications pour .NET et Elastic Beanstalk

Grâce au manifeste de déploiement, vous avez la possibilité de déployer plusieurs applications sur le même environnement Elastic Beanstalk.

Le manifeste de déploiement prend en charge les applications web ASP.NET Core ainsi que les archives msdeploy pour les applications ASP.NET traditionnelles. Imaginez un scénario dans lequel vous avez écrit une nouvelle application incroyable en utilisant ASP.NET Core pour le serveur frontal et une API web pour une API d'extension. Vous disposez également d'une application d'administration que vous avez écrite à l'aide d'ASP.NET traditionnel.

L'assistant de déploiement de la boîte à outils se concentre sur le déploiement d'un seul projet. Pour profiter du déploiement de plusieurs applications, vous devez créer manuellement la solution groupée d'applications. Pour commencer, écrivez le manifeste. Dans cet exemple, vous allez écrire le manifeste à la racine de votre solution.

La section de déploiement du manifeste possède deux enfants : un éventail d'applications web ASP.NET Core à déployer et un éventail d'archives msdeploy à déployer. Pour chaque application, vous définissez le chemin IIS et l'emplacement des bits de l'application relatifs au manifeste.

```
{
  "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"
        }
      }
    ]
  }
}
```

Une fois le manifeste écrit, vous utilisez Windows PowerShell pour créer le bundle d'application et mettre à jour un environnement Elastic Beanstalk existant pour l'exécuter. Le script est écrit en supposant qu'il sera exécuté depuis le dossier contenant votre solution Visual Studio.

La première chose à faire dans le script est de configurer un espace de travail dans lequel créer la solution groupée d'applications.

```
$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
}
```

Une fois le dossier créé, il est temps de préparer le serveur frontal. Comme avec l'assistant de déploiement, utilisez l'interface de ligne de commande dotnet pour publier l'application.

```
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
```

Notez que le sous-dossier « serveur frontal » a été utilisé pour le dossier de sortie, qui correspond à celui que vous avez défini dans le manifeste. Maintenant, vous devez faire de même pour le projet d'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
```

Le site d'administration est une application ASP.NET traditionnelle, vous ne pouvez donc pas utiliser l'interface de ligne de commande dotnet. Pour l'application d'administration, vous devez utiliser msbuild, en spécifiant le package de build cible pour créer l'archive msdeploy. Par défaut, le package cible crée l'archive msdeploy sous le dossier `obj\Release\Package`, vous devrez donc la copier dans l'espace de travail de publication.

```
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
```

Pour indiquer à l'environnement Elastic Beanstalk ce qu'il doit faire avec toutes ces applications, copiez le manifeste depuis votre solution sur l'espace de travail de publication et compressez le dossier.

```
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)
```

Maintenant que vous disposez du bundle d'application, vous pouvez accéder à la console web et charger l'archive sur un environnement Elastic Beanstalk. Sinon, vous pouvez continuer à utiliser

le kitAWSAplets de commande PowerShell pour mettre à jour l'environnement Elastic Beanstalk avec le bundle d'application. Veillez à avoir défini le profil et la région actuels sur le profil et la région contenant votre environnement Elastic Beanstalk à l'aide de`Set-AWSCredential`et`Set-DefaultAWSRegion`Applets de commande .

```
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
```

A présent, vérifiez l'état de la mise à jour grâce à la page d'état de l'environnement Elastic Beanstalk dans la boîte à outils ou la console web. Une fois terminé, vous pourrez accéder à chacune des applications que vous avez déployées vers le chemin IIS défini dans le manifeste de déploiement.

Déploiement vers Amazon EC2 Container Service

> **Important**
>
> Le nouveauPublier dansAWSest conçue pour simplifier la façon dont vous publiez des applications .NET surAWS. Vous pouvez être invité à passer à cette expérience de publication après avoir choisiPublier un conteneur dansAWS. Pour plus d'informations, consultez Utilisation de Publier dansAWSdans Visual Studio.

Amazon Elastic Container Service est un service de gestion de conteneurs performant et extrêmement évolutif qui prend en charge les conteneurs Docker et qui vous permet d'exécuter facilement des applications sur un cluster géré d'instances Amazon EC2.

Pour déployer des applications sur Amazon Elastic Container Service, les composants de votre application doivent être développés pour s'exécuter dans un conteneur Docker. Un conteneur Docker est une unité standardisée pour le développement logiciel, contenant tout ce dont votre application logicielle a besoin pour être exécutée : code, exécutable, outils système, bibliothèques système, etc.

Toolkit for Visual Studio comporte un assistant qui simplifie la publication des applications via Amazon ECS. Cet assistant est décrit dans les sections suivantes.

Pour plus d'informations sur Amazon ECS, accédez au manuelDocumentation Elastic Container Service. Elle inclut une présentation des principes de base de Docker et de la création d'un cluster.

Rubriques

- SpécifiezAWSInformations d'identification de votre application ASP.NET Core 2
- Déploiement d'une application ASP.NET Core 2.0 sur Amazon ECS (Fargate) (ancienne version)
- Déploiement d'une application ASP.NET Core 2.0 sur Amazon ECS (EC2)

SpécifiezAWSInformations d'identification de votre application ASP.NET Core 2

Il existe deux types d'informations d'identification lorsque vous déployez votre application dans un conteneur Docker : les informations d'identification de déploiement et les informations d'identification d'instance.

Les informations d'identification de déploiement sont utilisées par Publier un conteneur dansAWSassistant de création de l'environnement dans Amazon ECS. Elles incluent des éléments tels que des tâches, des services, des rôles IAM, un référentiel de conteneur Docker et, éventuellement, un équilibreur de charge.

Les informations d'identification d'instance sont utilisées par l'instance (y compris votre application) pour accéder à différents services AWS. Par exemple, si votre application ASP.NET Core 2.0 lit et écrit dans des objets Amazon S3, vous aurez besoin des autorisations appropriées. Vous pouvez fournir diverses informations d'identification en utilisant des méthodes différentes selon l'environnement. Par exemple, votre application ASP.NET Core 2 peut cibler des environnements de Développement et de Production. Vous pouvez utiliser une instance Docker locale et des informations d'identification pour le développement, ainsi qu'un rôle défini en production.

Spécification des informations d'identification de déploiement

LeAWSCompte que vous spécifiez dans lePublier un conteneur dansAWSl'assistant est l'assistantAWSCompte que l'assistant utilisera pour le déploiement sur Amazon ECS. Le profil de compte doit disposer des autorisations sur Amazon Elastic Compute Cloud, Amazon Elastic Container Service etAWS Identity and Access Management.

Si vous remarquez que des options manquent dans des listes déroulantes, cela peut être dû au fait que vous ne disposez pas des autorisations adéquates. Par exemple, si vous avez créé un cluster pour votre application, mais que vous ne le voyez pas sur laPublier un conteneur dansAWSpage Cluster de l'assistant. Si cela se produit, ajoutez les autorisations manquantes et relancez l'assistant.

Spécification des informations d'identification d'instance de développement

Pour les environnements autres que de production, vous pouvez configurer vos informations d'identification dans le fichier appsettings.<environment>.json. Par exemple, pour configurer vos informations d'identification dans le fichier appsettings.Development.json dans Visual Studio 2017 :

1. Ajoutez les packages AWSSDK.Extensions.NETCore.Setup NuGet à votre projet.
2. AdditionAWSparamètres de appsettings.Development.json. La configuration ci-dessous définit `Profile` et `Region`.

```
{
    "AWS": {
        "Profile": "local-test-profile",
        "Region": "us-west-2"
    }
}
```

Spécification des informations d'identification d'instance de production

Pour les instances de production, nous vous recommandons d'utiliser un rôle IAM pour contrôler les éléments accessibles par votre application (et le service). Par exemple, pour configurer un rôle IAM avec Amazon ECS en tant que mandataire principal doté d'autorisations sur Amazon Simple Storage Service et Amazon DynamoDB à partir de laAWS Management Console :

1. Connectez-vous à la AWS Management Console et ouvrez la console IAM à l'adresse https://console.aws.amazon.com/iam/.

2. Dans le panneau de navigation de la console IAM, sélectionnez Roles (Rôles), puis Create role (Créer un rôle).
3. Cliquez sur l'ongletAWSServiceType de rôle, puis choisissezEC2 Container Service.
4. Choisissez le cas d'utilisation EC2 Container Service Task (Tâche EC2 Container Service). Les cas d'utilisation sont définis par le service pour inclure la politique d'approbation nécessaire au service. Ensuite, sélectionnez Next (Suivant). Permissions (Autorisations).
5. Choisissez les stratégies d'autorisations AmazonS3FullAccess et AmazonDynamoDBFullAccess. Cochez la case en regard de chaque stratégie, puis choisissezSuivant: Vérification,
6. Pour Nom de rôle, tapez un nom de rôle ou le suffixe d'un nom de rôle vous permettant d'identifier l'objectif du rôle. Les noms de rôle de votre compte AWS doivent être uniques. Ils ne sont pas sensibles à la casse. Par exemple, vous ne pouvez pas créer deux rôles nommés `PRODROLE` et `prodrole`. Différentes entités peuvent référencer le rôle et il n'est donc pas possible de modifier son nom après sa création.
7. (Facultatif) Dans le champ Description du rôle, saisissez la description du nouveau rôle.
8. Passez en revue les informations du rôle, puis choisissez Créer un rôle.

Vous pouvez utiliser ce rôle en tant queRôle de tâchesur leDéfinition de tâche ECSPage de laPublier un conteneur dansAWSsorcier.

Pour en savoir plus, consultez Utilisation des rôles liés à un service.

Déploiement d'une application ASP.NET Core 2.0 sur Amazon ECS (Fargate) (ancienne version)

> **Important**
>
> Cette documentation fait référence aux services et fonctionnalités existants. Pour obtenir des guides et du contenu mis à jour, consultez le guide de l'outil de déploiementAWS .NET et la mise à jour de la table des matières du Déploiement vers laAWS table des matières.

Cette section explique comment utiliser l'AWSassistant Publish Container to, fourni dans le cadre de la Toolkit for Visual Studio, pour déployer une application ASP.NET Core 2.0 conteneurisée ciblant Linux via Amazon ECS à l'aide du type de lancement Fargate. Dans la mesure où une application web est destinée à s'exécuter en continu, elle sera déployée sous la forme d'un service.

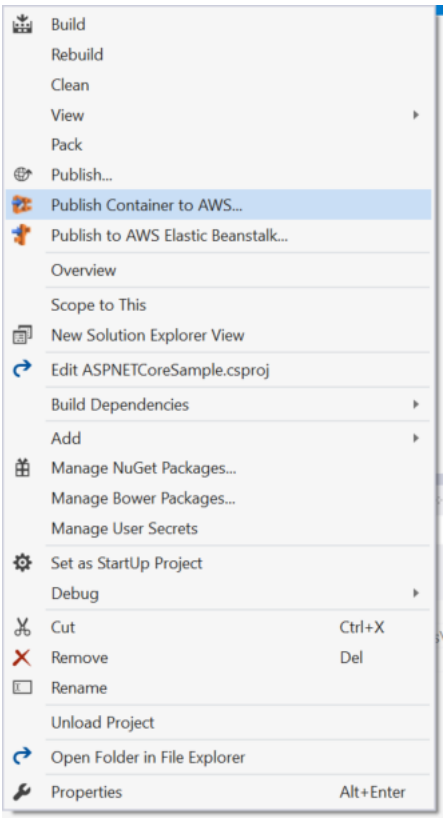
Avant de publier votre conteneur

Avant d'utiliser l'AWSassistant Publish Container to pour déployer votre application ASP.NET Core 2.0 :

- Spécifiez vosAWS informations d'identification et configurez-vous avec Amazon ECS.
- Installez Docker. Vous disposez de plusieurs options d'installation différentes, notamment Docker pour Windows.
- Dans Visual Studio, créez (ou ouvrez) un projet pour une application conteneurisée ASP.NET Core 2.0 ciblant Linux.

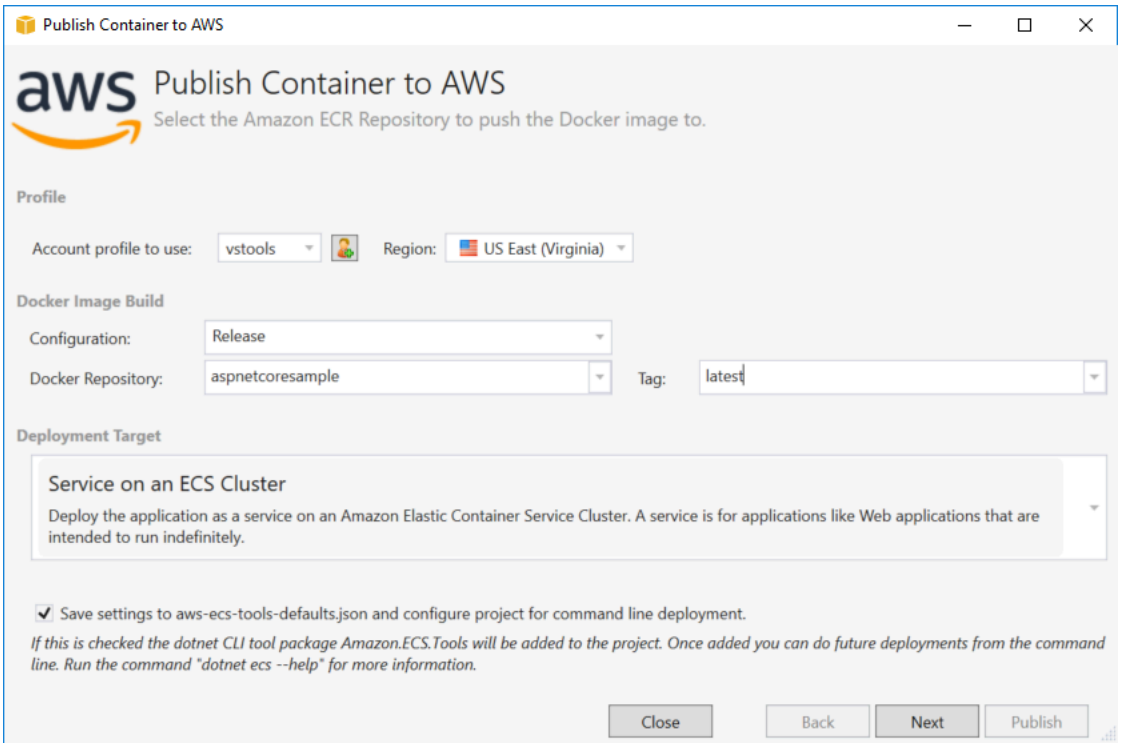
Accès à l'AWSassistant Publish Container to

Pour déployer une application conteneurisée ASP.NET Core 2.0 ciblant Linux, cliquez avec le bouton droit sur le projet dans l'Explorateur de solutions et sélectionnez Publier le conteneur surAWS.



Vous pouvez également sélectionner Publier le conteneur dansAWS le menu Visual Studio Build.

Publier le conteneur surAWS Wizard



Account profile to use (Profil de compte à utiliser) - Sélectionnez un profil de compte à utiliser.

Région - Choisissez la région du déploiement. Le profil et la région sont utilisés pour configurer les ressources de votre environnement de déploiement et pour sélectionner le registre Docker par défaut.

Configuration - Sélectionnez la configuration de génération de l'image Docker.

Docker Repository (Référentiel Docker) - Choisissez un référentiel Docker existant ou saisissez le nom d'un nouveau référentiel pour le créer. Il s'agit du référentiel auquel le conteneur de génération est envoyé.

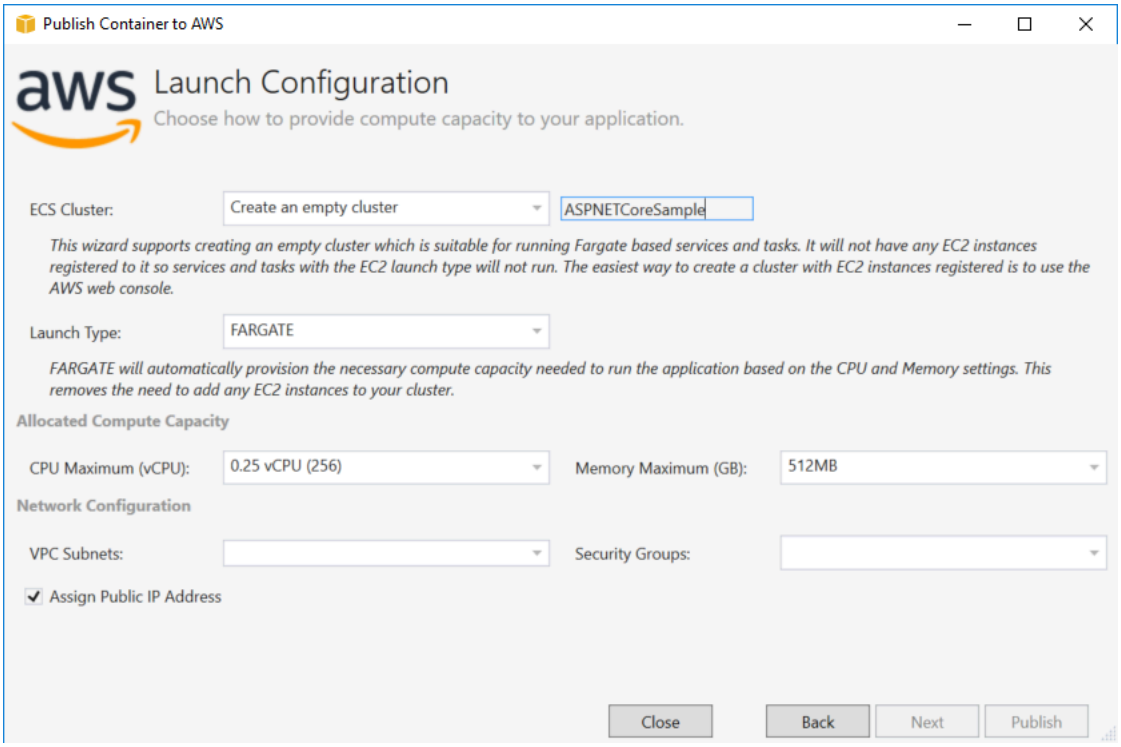
Balise - Sélectionnez une balise existante ou saisissez le nom d'une nouvelle balise. Les balises peuvent suivre des détails importants, tels que la version, les options ou d'autres éléments de configuration uniques du conteneur Docker.

Cible du déploiement - Sélectionnez Service on an ECS Cluster (Service sur un cluster ECS). Utilisez cette option de déploiement lorsque votre application est destinée à être de longue durée (comme une application web ASP.NET).

Enregistrer les paramètres dans **`aws-docker-tools-defaults.json`** et configurer le projet pour un déploiement de ligne de commande) - Cochez cette option si vous voulez profiter de la flexibilité

du déploiement à partir de la ligne de commande. Utilisez `dotnet ecs deploy` dans le répertoire de votre projet pour déployer et publier le conteneur via `dotnet ecs publish`.

Page Configuration de lancement



ECS Cluster (Cluster ECS) - Sélectionnez le cluster qui exécutera votre image Docker. Si vous choisissez de créer un cluster vide, indiquez un nom pour votre nouveau cluster.

Type de lancement - Choisissez FARGATE.

CPU Maximum (vCPU) (UC maximum (processeur virtuel)) - Choisissez la capacité de calcul maximale nécessaire à votre application. Pour voir les plages autorisées pour les valeurs d'UC et de mémoire, consultez taille de tâche.

Memory Maximum (GB) (Mémoire maximale (Go)) - Sélectionnez la taille maximale de mémoire disponible pour votre application.

VPC Subnets (Sous-réseaux VPC) - Choisissez un ou plusieurs sous-réseaux sous un seul VPC. Si vous choisissez plusieurs sous-réseaux, vos tâches seront réparties entre eux. Cela peut améliorer la disponibilité. Pour en savoir plus, consultez VPC par défaut et sous-réseaux par défaut.

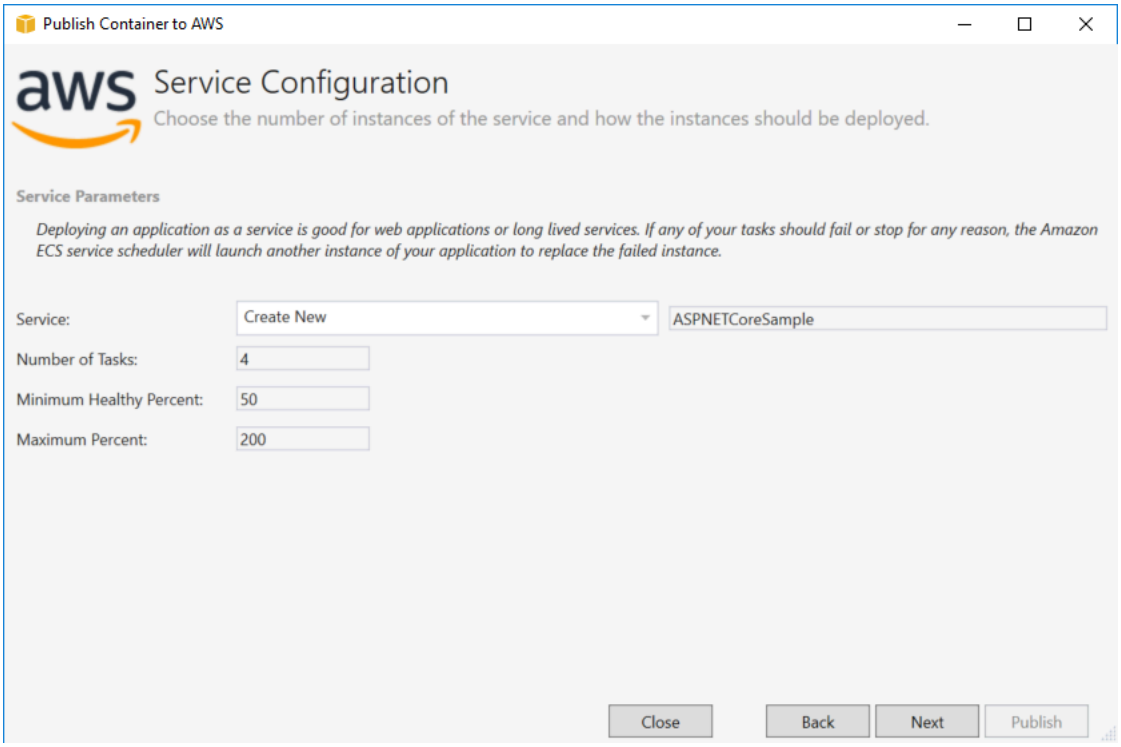
Groupes de sécurité - Choisissez un groupe de sécurité.

Un groupe de sécurité fait office de pare-feu pour les instances Amazon EC2 associées, en contrôlant le trafic entrant et le trafic sortant au niveau de l'instance.

Les groupes de sécurité par défaut sont configurés pour autoriser le trafic entrant en provenance d'instances attribuées au même groupe de sécurité et l'ensemble du trafic IPv4 sortant. Le trafic sortant doit être autorisé pour que le service puisse atteindre le référentiel de conteneur.

Assign Public IP Address (Attribuer une adresse IP publique) - Cochez cette case pour que votre tâche soit accessible depuis Internet.

Page Configuration de service



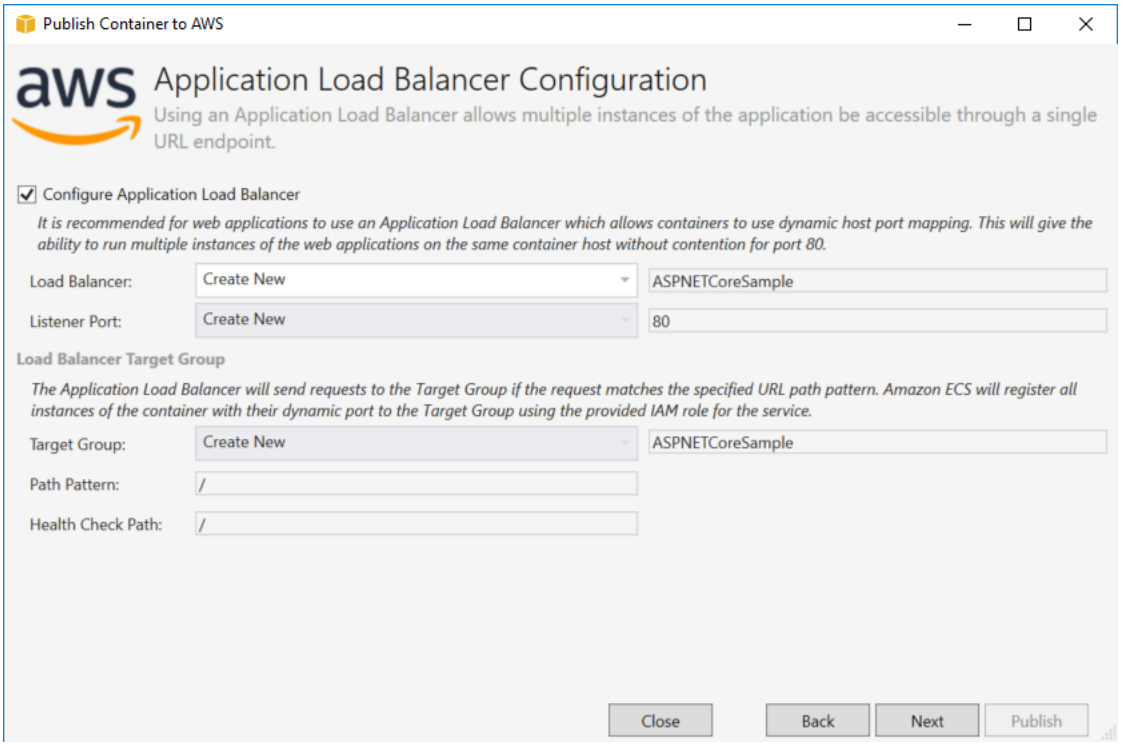
Service - Sélectionnez l'un des services dans le menu déroulant pour déployer votre conteneur dans un service existant. Vous pouvez également choisir Créer pour créer un nouveau service. Les noms de service doivent être uniques au sein d'un cluster, mais des services peuvent porter des noms similaires dans des clusters différents d'une même région ou de plusieurs régions.

Number of Tasks (Nombre de tâches) - Nombre de tâches à déployer et qui doivent continuer à s'exécuter sur votre cluster. Chaque tâche est une instance de votre conteneur.

Minimum Healthy Percent (Pourcentage minimum d'instances saines) - Pourcentage de tâches qui doivent rester à l'état `RUNNING` lors d'un déploiement, arrondi à la hausse à l'entier le plus proche.

Maximum Percent (Pourcentage maximum) - Pourcentage de tâches autorisées à l'état `RUNNING` ou `PENDING` lors d'un déploiement, arrondi à la baisse à l'entier le plus proche.

Page Équilibreur de charge d'application



Configure Application Load Balancer (Configurer un équilibreur de charge d'application) - Cochez cette case pour configurer un équilibreur de charge d'application.

Équilibreur de charge - Sélectionnez un équilibreur de charge existant ou choisissez Créer et saisissez le nom du nouvel équilibreur de charge.

Port d'écoute - Sélectionnez un port d'écoute existant ou choisissez Créer et saisissez un numéro de port. Le port par défaut, `80`, est approprié pour la plupart des applications web.

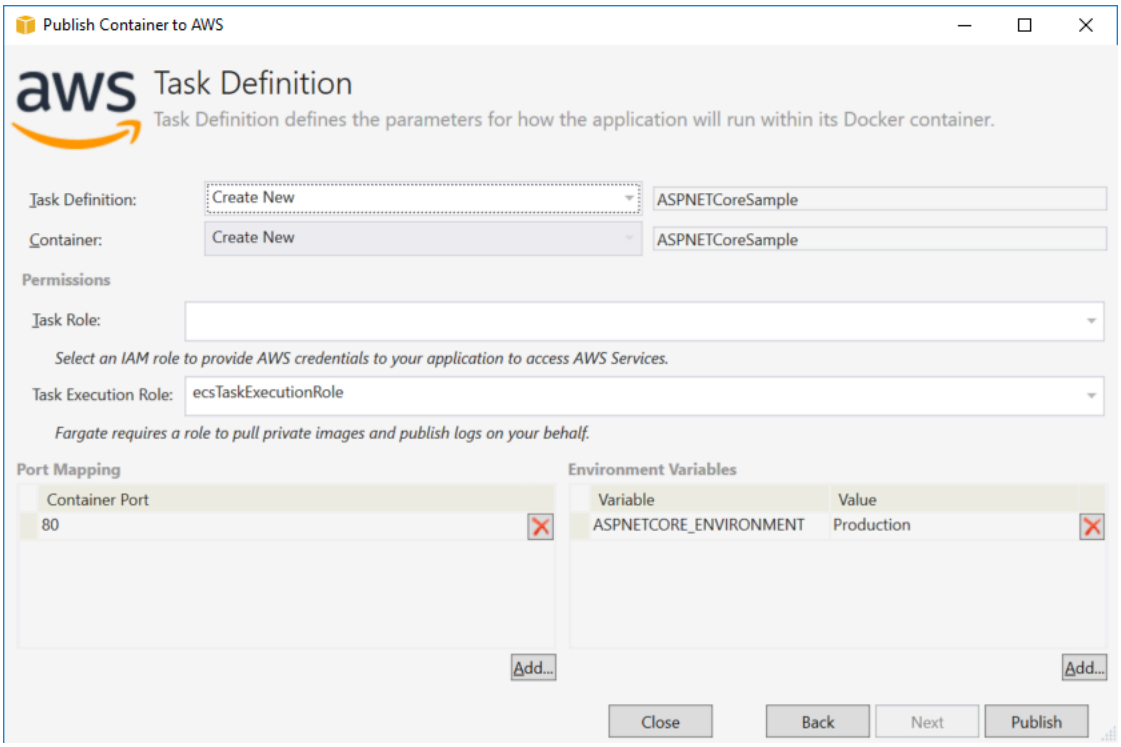
Groupe cible : sélectionnez le groupe cible auprès duquel Amazon ECS enregistrera les tâches auprès du service.

Modèle de chemin - L'équilibreur de charge utilisera le routage basé sur le chemin d'accès. Acceptez la barre oblique `/` par défaut ou indiquez un autre modèle. Le modèle de chemin est sensible à la casse, peut comporter jusqu'à 128 caractères et contient un jeu de caractères sélectionné.

Chemin de vérification de l'état - Chemin de ping, c'est-à-dire destination des vérifications de l'état sur les cibles. Par défaut, il s'agit de `/`. Entrez un chemin différent si nécessaire. Si le chemin que vous saisissez n'est pas valide, la vérification de l'état échoue et il est considéré comme non sain.

Si vous déployez plusieurs services et que chacun d'eux est déployé dans un chemin ou un emplacement différent, vous avez besoin de chemins de vérification personnalisés.

Page Définition de tâche



Définition de tâche - Sélectionnez une définition de tâche existante ou choisissez Créer et saisissez le nom de la nouvelle définition de tâche.

Conteneur - Sélectionnez un conteneur existant ou choisissez Créer et saisissez le nom du nouveau conteneur.

Rôle de tâche : sélectionnez un rôle IAM doté des informations d'identification dont votre application a besoin pour accéder auxAWS services. Il s'agit de la manière dont les informations d'identification sont transmises à votre application. Découvrez comment spécifier les informations d'identificationAWS de sécurité pour votre application.

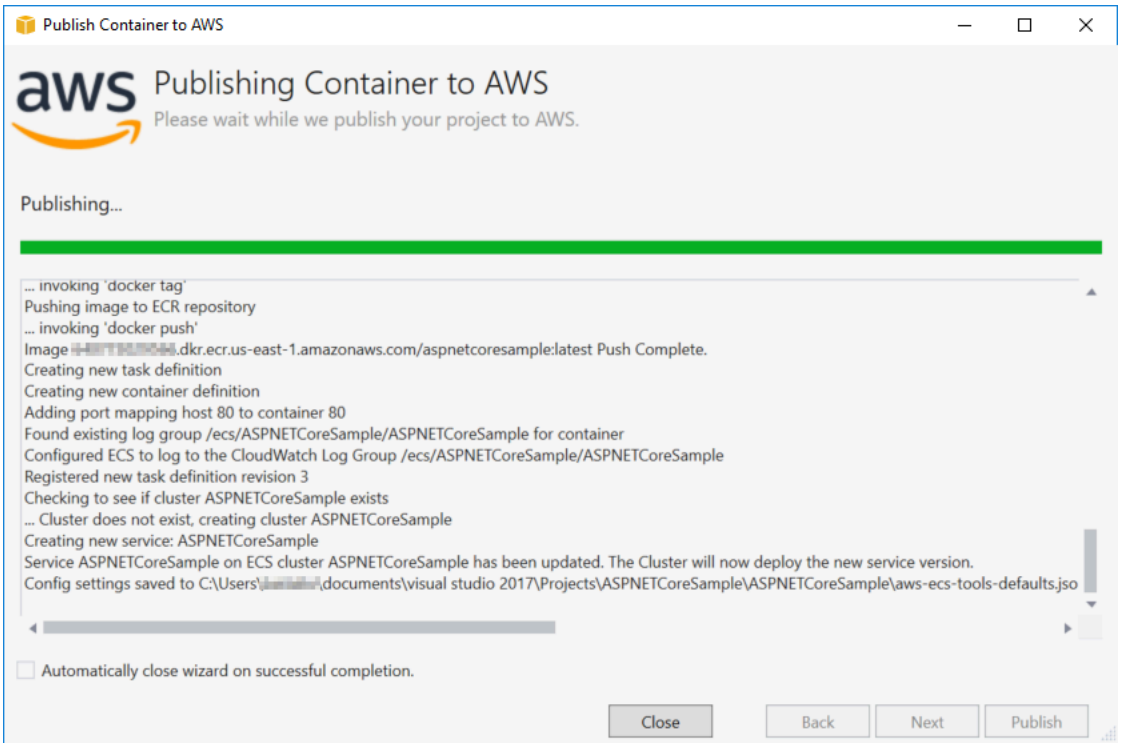
Rôle d'exécution des tâches : sélectionnez un rôle autorisé à extraire des images privées et à publier des journaux. AWS Fargate l'utilisera en votre nom.

Port Mapping (Mappage de port) - Choisissez le numéro de port sur le conteneur qui est lié au port hôte affecté automatiquement.

Variables d'environnement - Ajoutez, modifiez ou supprimez des variables d'environnement pour le conteneur. Vous pouvez les modifier en fonction de votre déploiement.

Lorsque la configuration vous satisfait, cliquez sur Publier pour commencer le processus de déploiement.

Publier un conteneur versAWS



Des événements sont affichés pendant le déploiement. L'assistant se ferme automatiquement une fois l'opération terminée avec succès. Pour modifier cela, décochez la case située en bas de la page.

Vous trouverez l'URL de vos nouvelles instances dans l'AWSExplorateur. Développez Amazon ECS and Clusters, puis cliquez sur votre cluster.

Déploiement d'une application ASP.NET Core 2.0 sur Amazon ECS (EC2)

Cette section décrit comment utiliser lePublier un conteneur dansAWSAssistant, fourni dans le cadre de Toolkit for Visual Studio, pour déployer une application de conteneur ASP.NET Core 2.0 ciblant Linux via Amazon ECS en utilisant le type de lancement EC2. Dans la mesure où une application web est destinée à s'exécuter en continu, elle sera déployée sous la forme d'un service.

Avant de publier votre conteneur

Avant d'utiliser lePublier un conteneur dansAWSPour déployer votre application ASP.NET Core 2.0 :

- Spécifiez votreAWSinformations d'identificationetConfiguration avec Amazon ECS.

- Installez Docker. Vous disposez de plusieurs options d'installation différentes, notamment Docker pour Windows.
- Créez un cluster Amazon ECS en fonction des besoins de votre application web. Il suffit de quelques étapes pour effectuer cette opération.
- Dans Visual Studio, créez (ou ouvrez) un projet pour une application conteneurisée ASP.NET Core 2.0 ciblant Linux.

Accès à l'assistant Publish Container toAWSsorcier

Pour déployer une application de conteneur ASP.NET Core 2.0 ciblant Linux, cliquez avec le bouton droit sur le projet dans l'Explorateur de solutions et sélectionnezPublier un conteneur dansAWS.

Vous pouvez également sélectionnerPublier un conteneur dansAWSdans le menu Génération de Visual Studio.

Publier un conteneur dansAWSAssistant

Account profile to use (Profil de compte à utiliser) - Sélectionnez un profil de compte à utiliser.

Région - Choisissez une région de déploiement. Le profil et la région sont utilisés pour configurer les ressources de votre environnement de déploiement et pour sélectionner le registre Docker par défaut.

Configuration - Sélectionnez la configuration de génération de l'image Docker.

Docker Repository (Référentiel Docker) - Choisissez un référentiel Docker existant ou saisissez le nom d'un nouveau référentiel pour le créer. Il s'agit du référentiel auquel l'image du conteneur de génération est envoyée.

Balise - Sélectionnez une balise existante ou saisissez le nom d'une nouvelle balise. Les balises peuvent suivre des détails importants, tels que la version, les options ou d'autres éléments de configuration uniques du conteneur Docker.

Déploiement - Sélectionnez Service on an ECS Cluster (Service sur un cluster ECS). Utilisez cette option de déploiement lorsque votre application est destinée à être de longue durée (comme une application web ASP.NET Core 2.0).

Enregistrer les paramètres dans **`aws-docker-tools-defaults.json`** et configurer le projet pour un déploiement de ligne de commande) - Cochez cette option si vous voulez profiter de la flexibilité du déploiement à partir de la ligne de commande. Utilisez `dotnet ecs deploy` dans le répertoire de votre projet pour déployer et publier le conteneur via `dotnet ecs publish`.

Page Configuration de lancement

ECS Cluster (Cluster ECS) - Sélectionnez le cluster qui exécutera votre image Docker. Vous pouvezCréation d'un cluster ECSUtilisation deAWSManagement Console.

Type de lancement - Choisissez EC2. Pour utiliser le type de lancement Fargate, consultez Déploiement d'une application ASP.NET Core 2.0 sur Amazon ECS (Fargate).

Page Configuration de service

Service - Sélectionnez l'un des services dans le menu déroulant pour déployer votre conteneur dans un service existant. Vous pouvez également choisir Créer pour créer un nouveau service. Les noms de service doivent être uniques au sein d'un cluster, mais des services peuvent porter des noms similaires dans des clusters différents d'une même région ou de plusieurs régions.

Number of Tasks (Nombre de tâches) - Nombre de tâches à déployer et qui doivent continuer à s'exécuter sur votre cluster. Chaque tâche est une instance de votre conteneur.

Minimum Healthy Percent (Pourcentage minimum d'instances saines) - Pourcentage de tâches qui doivent rester à l'état `RUNNING` lors d'un déploiement, arrondi à la hausse à l'entier le plus proche.

Maximum Percent (Pourcentage maximum) - Pourcentage de tâches autorisées à l'état `RUNNING` ou `PENDING` lors d'un déploiement, arrondi à la baisse à l'entier le plus proche.

Placement Templates (Modèles de placement) - Sélectionnez un modèle de placement de tâche.

Lorsque vous lancez une tâche dans un cluster, Amazon ECS doit déterminer où la placer en fonction des exigences spécifiées dans la définition de tâche, par exemple l'UC et la mémoire. De la même manière, lorsque vous réduisez le nombre de tâches, Amazon ECS doit déterminer quelles tâches doivent être résiliées.

Le modèle de placement contrôle la manière dont les tâches sont lancées dans un cluster :

- AZ Balanced Spread (Répartition équilibrée par AZ) – Permet de répartir les tâches entre les zones de disponibilité et les instances de conteneur dans la zone de disponibilité.
- AZ Balanced BinPack (BinPack équilibré par AZ) – Permet de répartir les tâches entre les zones de disponibilité et les instances de conteneur avec la quantité de mémoire disponible la moins élevée.
- BinPack – Permet de répartir les tâches en fonction de la quantité disponible la moins élevée d'UC ou de mémoire.

- One Task Per Host (Une tâche par hôte) – Permet de placer au maximum une tâche du service sur chaque instance de conteneur.

Pour en savoir plus, consultez Placement des tâches Amazon ECS.

Page Équilibreur de charge d'application

Configure Application Load Balancer (Configurer un équilibreur de charge d'application) - Cochez cette case pour configurer un équilibreur de charge d'application.

Select IAM role for service (Sélectionner un rôle IAM pour le service) - Sélectionnez un rôle existant ou choisissez Créer pour créer un nouveau rôle.

Équilibreur de charge - Sélectionnez un équilibreur de charge existant ou choisissez Créer et saisissez le nom du nouvel équilibreur de charge.

Port d'écoute - Sélectionnez un port d'écoute existant ou choisissez Créer et saisissez un numéro de port. Le port par défaut, `80`, est approprié pour la plupart des applications web.

Groupe cible - Par défaut, l'équilibreur de charge envoie des demandes à des cibles enregistrées à l'aide du port et du protocole que vous avez spécifiés pour le groupe cible. Vous pouvez remplacer ce port lorsque vous enregistrez chaque cible auprès du groupe cible.

Modèle de chemin - L'équilibreur de charge utilisera le routage basé sur le chemin d'accès. Acceptez la barre oblique `/` par défaut ou indiquez un autre modèle. Le modèle de chemin est sensible à la casse, peut comporter jusqu'à 128 caractères et contient un jeu de caractères sélectionné.

Chemin de vérification de l'état - Chemin de ping, c'est-à-dire destination des vérifications de l'état sur les cibles. Par défaut, il s'agit de `/`, qui est approprié pour les applications web. Entrez un chemin différent si nécessaire. Si le chemin que vous saisissez n'est pas valide, la vérification de l'état échoue et il est considéré comme non sain.

Si vous déployez plusieurs services et que chacun d'eux est déployé dans un chemin ou un emplacement différent, vous aurez peut-être besoin de chemins de vérification personnalisés.

Page Définition de tâche ECS

Définition de tâche - Sélectionnez une définition de tâche existante ou choisissez Créer et saisissez le nom de la nouvelle définition de tâche.

Conteneur - Sélectionnez un conteneur existant ou choisissez Créer et saisissez le nom du nouveau conteneur.

Mémoire (Mio) - Fournissez des valeurs pour Limite flexible et/ou Limite stricte.

La limite flexible (en MiB) de mémoire à réserver pour le conteneur. Docker tente de conserver la mémoire du conteneur sous la limite flexible. Le conteneur peut consommer davantage de mémoire, jusqu'à la limite stricte spécifiée avec le paramètre de mémoire (le cas échéant), ou la totalité de la mémoire disponible sur l'instance de conteneur, le premier des deux prévalant.

La limite stricte (en Mio) de la mémoire à présenter le conteneur. Si votre conteneur tente de dépasser la mémoire spécifiée ici, il sera désactivé.

Rôle de tâche- Sélectionnez un rôle de tâche pour un rôle IAM qui autorise le conteneur à appeler leAWSLes API spécifiées dans ses stratégies associées en votre nom. Il s'agit de la manière dont les informations d'identification sont transmises à votre application. VoirComment spécifierAWSInformations d'identification de sécurité de votre application.

Port Mapping (Mappage de port) - Ajoutez, modifiez ou supprimez des mappages de port pour le conteneur. Si un équilibreur de charge est activé, le port hôte est 0 par défaut et l'affectation de port est dynamique.

Variables d'environnement - Ajoutez, modifiez ou supprimez des variables d'environnement pour le conteneur.

Lorsque la configuration vous satisfait, cliquez sur Publier pour commencer le processus de déploiement.

Publier un conteneur dansAWS

Des événements sont affichés pendant le déploiement. L'assistant se ferme automatiquement une fois l'opération terminée avec succès. Pour modifier cela, décochez la case située en bas de la page.

Vous trouverez l'URL de vos nouvelles instances dans leAWSExplorer. Développez Amazon ECS and Clusters, puis cliquez sur votre cluster.

Résolution des problèmes AWS Toolkit for Visual Studio

Les sections suivantes contiennent des informations générales de résolution des problèmes concernant AWS Toolkit for Visual Studio les AWS services du kit d'outils et son utilisation.

> **Note**
>
> Les informations d'installation et de set-up-specific dépannage sont disponibles dans la rubrique Résolution des problèmes d'installation, située dans ce guide de l'utilisateur.

Rubriques

Bonnes pratiques de résolution des problèmes

Les meilleures pratiques recommandées pour résoudre les AWS Toolkit for Visual Studio problèmes sont les suivantes.

- Essayez de recréer votre problème ou votre erreur avant d'envoyer un rapport.
- Prenez des notes détaillées sur chaque étape, chaque réglage et chaque message d'erreur pendant le processus de recréation.
- Collectez les journaux du AWS kit d'outils Pour une description détaillée de la localisation des journaux de votre AWS boîte à outils, consultez la procédure Comment localiser vos AWS journaux, qui se trouve dans cette rubrique du guide.
- Vérifiez les demandes ouvertes, les solutions connues ou signalez votre problème non résolu dans la section AWS Toolkit for Visual Studio Problèmes du AWS Toolkit for Visual Studio GitHub référentiel.

Comment localiser les journaux de votre AWS boîte à outils

1. Dans le menu principal de Visual Studio, développez Extensions.
2. Choisissez le AWS kit d'outils pour développer le menu du AWS kit d'outils, puis choisissez Afficher les journaux du kit d'outils.

3. Lorsque le dossier des journaux du AWS Toolkit s'ouvre dans votre système d'exploitation, triez les fichiers par date et recherchez tout fichier journal contenant des informations relatives à votre problème actuel.

Amazon CodeWhisperer Sign In et Sign Out sont désactivés

Si vous rencontrez un problème avec le CodeWhisperer service lorsque les éléments de menu de connexion et de déconnexion sont désactivés, résolvez le problème en effectuant les étapes suivantes.

1. Dans l'explorateur de fichiers Windows, accédez au dossier de cache du AWS Toolkit situé à l'adresse :`%LOCALAPPDATA%/aws/toolkits/language-servers/CodeWhisperer`.
2. Effacez le contenu du dossier de cache.
3. Fermez puis rouvrez la solution actuelle.

Sécurité pour AWS Toolkit for Visual Studio

Chez Amazon Web Services (AWS), la sécurité dans le cloud est la priorité principale. En tant que client AWS , vous bénéficiez d'un centre de données et d'une architecture réseau conçus pour répondre aux exigences des organisations les plus pointilleuses sur la sécurité. La sécurité est une responsabilité partagée entre vous AWS et vous. Le modèle de responsabilité partagée décrit cela comme la sécurité du cloud et la sécurité dans le cloud.

Sécurité du cloud : AWS est chargée de protéger l'infrastructure qui exécute tous les services proposés dans le AWS cloud et de vous fournir des services que vous pouvez utiliser en toute sécurité. Notre responsabilité en matière de sécurité est notre priorité absolue AWS, et l'efficacité de notre sécurité est régulièrement testée et vérifiée par des auditeurs tiers dans le cadre des programmes de AWS conformité.

Sécurité dans le cloud — Votre responsabilité est déterminée par le AWS service que vous utilisez et par d'autres facteurs, notamment la sensibilité de vos données, les exigences de votre organisation et les lois et réglementations applicables.

Ce AWS produit ou service suit le modèle de responsabilité partagée par le biais des services Amazon Web Services (AWS) spécifiques qu'il prend en charge. Pour obtenir des informations sur la sécurité des AWS services, consultez la AWS page de documentation sur la sécuritéAWS des services et les services concernés par les efforts de AWS conformité par programme de conformité.

Rubriques

- Protection des données dans AWS Toolkit for Visual Studio
- Gestion de l’identité et des accès
- Validation de conformité pour ce AWS produit ou service
- Résilience pour ce AWS produit ou service
- Sécurité de l'infrastructure pour ce AWS produit ou service
- Analyse de configuration et de vulnérabilité dans AWS Toolkit for Visual Studio

Protection des données dans AWS Toolkit for Visual Studio

Le modèle de responsabilité AWS partagée s'applique à la protection des données dans AWS Toolkit for Visual Studio. Comme décrit dans ce modèle, AWS est chargé de protéger l'infrastructure mondiale qui gère tous les AWS Cloud. La gestion du contrôle de votre contenu hébergé sur

cette infrastructure relève de votre responsabilité. Vous êtes également responsable des tâches de configuration et de gestion de la sécurité des Services AWS que vous utilisez. Pour plus d'informations sur la confidentialité des données, consultez Questions fréquentes (FAQ) sur la confidentialité des données. Pour en savoir plus sur la protection des données en Europe, consultez le billet de blog Modèle de responsabilité partagée AWS et RGPD (Règlement général sur la protection des données) sur le Blog de sécuritéAWS .

À des fins de protection des données, nous vous recommandons de protéger les Compte AWS informations d'identification et de configurer les utilisateurs individuels avec AWS IAM Identity Center ou AWS Identity and Access Management (IAM). Ainsi, chaque utilisateur se voit attribuer uniquement les autorisations nécessaires pour exécuter ses tâches. Nous vous recommandons également de sécuriser vos données comme indiqué ci-dessous :

- Utilisez l'authentification multifactorielle (MFA) avec chaque compte.
- Utilisez le protocole SSL/TLS pour communiquer avec les ressources. AWS Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Configurez l'API et la journalisation de l'activité des utilisateurs avec AWS CloudTrail.
- Utilisez des solutions de AWS chiffrement, ainsi que tous les contrôles de sécurité par défaut qu'ils contiennent Services AWS.
- Utilisez des services de sécurité gérés avancés tels qu'Amazon Macie, qui contribuent à la découverte et à la sécurisation des données sensibles stockées dans Amazon S3.
- Si vous avez besoin de modules cryptographiques validés par la norme FIPS 140-2 pour accéder AWS via une interface de ligne de commande ou une API, utilisez un point de terminaison FIPS. Pour plus d'informations sur les points de terminaison FIPS (Federal Information Processing Standard) disponibles, consultez Federal Information Processing Standard (FIPS) 140-2 (Normes de traitement de l'information fédérale).

Nous vous recommandons fortement de ne jamais placer d'informations confidentielles ou sensibles, telles que les adresses e-mail de vos clients, dans des balises ou des champs de texte libre tels que le champ Name (Nom). Cela inclut lorsque vous travaillez avec Toolkit for Visual Studio ou un autre outil Services AWS à l'aide de la console, de l'API ou AWS des SDK. AWS CLI Toutes les données que vous entrez dans des balises ou des champs de texte de forme libre utilisés pour les noms peuvent être utilisées à des fins de facturation ou dans les journaux de diagnostic. Si vous fournissez une adresse URL à un serveur externe, nous vous recommandons fortement de ne pas inclure d'informations d'identification dans l'adresse URL permettant de valider votre demande adressée à ce serveur.

Gestion de l’identité et des accès

AWS Identity and Access Management (IAM) est un outil Service AWS qui permet à un administrateur de contrôler en toute sécurité l'accès aux AWS ressources. Les administrateurs IAM contrôlent qui peut être authentifié (connecté) et autorisé (autorisé) à utiliser AWS les ressources. IAM est un Service AWS outil que vous pouvez utiliser sans frais supplémentaires.

Rubriques

Public ciblé

La façon dont vous utilisez AWS Identity and Access Management (IAM) varie en fonction du travail que vous effectuez. AWS

Utilisateur du service : si vous avez l' Services AWS habitude de faire votre travail, votre administrateur vous fournit les informations d'identification et les autorisations dont vous avez besoin. Au fur et à mesure que vous utilisez de nouvelles AWS fonctionnalités pour effectuer votre travail, vous aurez peut-être besoin d'autorisations supplémentaires. En comprenant bien la gestion des accès, vous saurez demander les autorisations appropriées à votre administrateur. Si vous ne pouvez pas accéder à une fonctionnalité dans AWS, consultez Résolution des problèmes AWS d'identité et d'accès le guide de l'utilisateur du Service AWS que vous utilisez.

Administrateur du service — Si vous êtes responsable des AWS ressources de votre entreprise, vous avez probablement un accès complet à AWS. C'est à vous de déterminer les AWS fonctionnalités et les ressources auxquelles les utilisateurs de votre service doivent accéder. Vous devez ensuite soumettre les demandes à votre administrateur IAM pour modifier les autorisations des utilisateurs de votre service. Consultez les informations sur cette page pour comprendre les concepts de base d’IAM. Pour en savoir plus sur la façon dont votre entreprise peut utiliser IAM avec AWS, consultez le guide de l'utilisateur Service AWS que vous utilisez.

Administrateur IAM – Si vous êtes un administrateur IAM, vous souhaiterez peut-être en savoir plus sur la façon d’écrire des politiques pour gérer l’accès à AWS. Pour consulter des exemples

de politiques AWS basées sur l'identité que vous pouvez utiliser dans IAM, consultez le guide de l'utilisateur Service AWS que vous utilisez.

Authentification par des identités

L'authentification est la façon dont vous vous connectez à AWS l'aide de vos informations d'identification. Vous devez être authentifié (connecté à AWS) en tant qu'utilisateur IAM ou en assumant un rôle IAM. Utilisateur racine d'un compte AWS

Vous pouvez vous connecter en AWS tant qu'identité fédérée en utilisant les informations d'identification fournies par le biais d'une source d'identité. AWS IAM Identity Center Les utilisateurs (IAM Identity Center), l'authentification unique de votre entreprise et vos informations d'identification Google ou Facebook sont des exemples d'identités fédérées. Lorsque vous vous connectez avec une identité fédérée, votre administrateur aura précédemment configuré une fédération d'identités avec des rôles IAM. Lorsque vous accédez à AWS l'aide de la fédération, vous assumez indirectement un rôle.

Selon le type d'utilisateur que vous êtes, vous pouvez vous connecter au portail AWS Management Console ou au portail AWS d'accès. Pour plus d'informations sur la connexion à AWS, consultez la section Comment vous connecter à votre compte Compte AWS dans le guide de Connexion à AWS l'utilisateur.

Si vous y accédez AWS par programmation, AWS fournit un kit de développement logiciel (SDK) et une interface de ligne de commande (CLI) pour signer cryptographiquement vos demandes à l'aide de vos informations d'identification. Si vous n'utilisez pas d' AWS outils, vous devez signer vous-même les demandes. Pour plus d'informations sur l'utilisation de la méthode recommandée pour signer vous-même les demandes, consultez la section Signature des demandes AWS d'API dans le guide de l'utilisateur IAM.

Quelle que soit la méthode d'authentification que vous utilisez, vous devrez peut-être fournir des informations de sécurité supplémentaires. Par exemple, il vous AWS recommande d'utiliser l'authentification multifactorielle (MFA) pour renforcer la sécurité de votre compte. Pour en savoir plus, consultez Authentification multifactorielle dans le Guide de l'utilisateur AWS IAM Identity Center et Utilisation de l'authentification multifactorielle (MFA) dans l'interface AWS dans le Guide de l'utilisateur IAM.

Compte AWS utilisateur root

Lorsque vous créez un Compte AWS, vous commencez par une identité de connexion unique qui donne un accès complet à toutes Services AWS les ressources du compte. Cette identité est

appelée utilisateur Compte AWS root et est accessible en vous connectant avec l'adresse e-mail et le mot de passe que vous avez utilisés pour créer le compte. Il est vivement recommandé de ne pas utiliser l'utilisateur racine pour vos tâches quotidiennes. Protégez vos informations d'identification d'utilisateur racine et utilisez-les pour effectuer les tâches que seul l'utilisateur racine peut effectuer. Pour obtenir la liste complète des tâches qui vous imposent de vous connecter en tant qu'utilisateur root, consultez Tâches nécessitant des informations d'identification d'utilisateur root dans le Guide de l'utilisateur IAM.

Identité fédérée

La meilleure pratique consiste à obliger les utilisateurs humains, y compris ceux qui ont besoin d'un accès administrateur, à utiliser la fédération avec un fournisseur d'identité pour accéder à l'aide Services AWS d'informations d'identification temporaires.

Une identité fédérée est un utilisateur de l'annuaire des utilisateurs de votre entreprise, d'un fournisseur d'identité Web AWS Directory Service, du répertoire Identity Center ou de tout utilisateur qui y accède à l'aide des informations d'identification fournies Services AWS par le biais d'une source d'identité. Lorsque des identités fédérées y accèdent Comptes AWS, elles assument des rôles, qui fournissent des informations d'identification temporaires.

Pour une gestion des accès centralisée, nous vous recommandons d'utiliser AWS IAM Identity Center. Vous pouvez créer des utilisateurs et des groupes dans IAM Identity Center, ou vous pouvez vous connecter et synchroniser avec un ensemble d'utilisateurs et de groupes dans votre propre source d'identité afin de les utiliser dans toutes vos applications Comptes AWS et applications. Pour obtenir des informations sur IAM Identity Center, consultez Qu'est-ce que IAM Identity Center ? dans le Guide de l'utilisateur AWS IAM Identity Center .

Utilisateurs et groupes IAM

Un utilisateur IAM est une identité au sein de vous Compte AWS qui possède des autorisations spécifiques pour une seule personne ou une seule application. Dans la mesure du possible, nous vous recommandons de vous appuyer sur des informations d'identification temporaires plutôt que de créer des utilisateurs IAM ayant des informations d'identification à long terme tels que les clés d'accès. Toutefois, si certains cas d'utilisation spécifiques nécessitent des informations d'identification à long terme avec les utilisateurs IAM, nous vous recommandons de faire pivoter les clés d'accès. Pour plus d'informations, consultez Rotation régulière des clés d'accès pour les cas d'utilisation nécessitant des informations d'identification dans le Guide de l'utilisateur IAM.

Un groupe IAM est une identité qui concerne un ensemble d'utilisateurs IAM. Vous ne pouvez pas vous connecter en tant que groupe. Vous pouvez utiliser les groupes pour spécifier des autorisations pour plusieurs utilisateurs à la fois. Les groupes permettent de gérer plus facilement les autorisations pour de grands ensembles d'utilisateurs. Par exemple, vous pouvez avoir un groupe nommé IAMAdmins et accorder à ce groupe les autorisations d'administrer des ressources IAM.

Les utilisateurs sont différents des rôles. Un utilisateur est associé de manière unique à une personne ou une application, alors qu'un rôle est conçu pour être endossé par tout utilisateur qui en a besoin. Les utilisateurs disposent d'informations d'identification permanentes, mais les rôles fournissent des informations d'identification temporaires. Pour en savoir plus, consultez Quand créer un utilisateur IAM (au lieu d'un rôle) dans le Guide de l'utilisateur IAM.

Rôles IAM

Un rôle IAM est une identité au sein de vous Compte AWS dotée d'autorisations spécifiques. Le concept ressemble à celui d'utilisateur IAM, mais le rôle IAM n'est pas associé à une personne en particulier. Vous pouvez assumer temporairement un rôle IAM dans le en AWS Management Console changeant de rôle. Vous pouvez assumer un rôle en appelant une opération d' AWS API AWS CLI ou en utilisant une URL personnalisée. Pour plus d'informations sur les méthodes d'utilisation des rôles, consultez Utilisation de rôles IAM dans le Guide de l'utilisateur IAM.

Les rôles IAM avec des informations d'identification temporaires sont utiles dans les cas suivants :

- Accès utilisateur fédéré – Pour attribuer des autorisations à une identité fédérée, vous créez un rôle et définissez des autorisations pour le rôle. Quand une identité externe s'authentifie, l'identité est associée au rôle et reçoit les autorisations qui sont définies par celui-ci. Pour obtenir des informations sur les rôles pour la fédération, consultez Création d'un rôle pour un fournisseur d'identité tiers (fédération) dans le Guide de l'utilisateur IAM. Si vous utilisez IAM Identity Center, vous configurez un jeu d'autorisations. IAM Identity Center met en corrélation le jeu d'autorisations avec un rôle dans IAM afin de contrôler à quoi vos identités peuvent accéder après leur authentification. Pour plus d'informations sur les jeux d'autorisations, consultez la rubrique Jeux d'autorisations dans le Guide de l'utilisateur AWS IAM Identity Center .
- Autorisations d'utilisateur IAM temporaires : un rôle ou un utilisateur IAM peut endosser un rôle IAM pour profiter temporairement d'autorisations différentes pour une tâche spécifique.
- Accès intercompte : vous pouvez utiliser un rôle IAM pour permettre à un utilisateur (principal de confiance) d'un compte différent d'accéder aux ressources de votre compte. Les rôles constituent le principal moyen d'accorder l'accès intercompte. Toutefois, dans certains Services AWS cas, vous pouvez associer une politique directement à une ressource (au lieu d'utiliser un rôle comme

proxy). Pour en savoir plus sur la différence entre les rôles et les politiques basées sur les ressources pour l'accès intercompte, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

- Accès multiservices — Certains Services AWS utilisent des fonctionnalités dans d'autres Services AWS. Par exemple, lorsque vous effectuez un appel dans un service, il est courant que ce service exécute des applications dans Amazon EC2 ou stocke des objets dans Amazon S3. Un service peut le faire en utilisant les autorisations d'appel du principal, un rôle de service ou un rôle lié au service.
  - Sessions d'accès direct (FAS) : lorsque vous utilisez un utilisateur ou un rôle IAM pour effectuer des actions AWS, vous êtes considéré comme un mandant. Lorsque vous utilisez certains services, vous pouvez effectuer une action qui initie une autre action dans un autre service. FAS utilise les autorisations du principal appelant et Service AWS, associées Service AWS à la demande, pour adresser des demandes aux services en aval. Les demandes FAS ne sont effectuées que lorsqu'un service reçoit une demande qui nécessite des interactions avec d'autres personnes Services AWS ou des ressources pour être traitée. Dans ce cas, vous devez disposer d'autorisations nécessaires pour effectuer les deux actions. Pour plus de détails sur la politique relative à la transmission de demandes FAS, consultez Sessions de transmission d'accès.
  - Rôle de service : il s'agit d'un rôle IAM attribué à un service afin de réaliser des actions en votre nom. Un administrateur IAM peut créer, modifier et supprimer une fonction du service à partir d'IAM. Pour plus d'informations, consultez Création d'un rôle pour la délégation d'autorisations à un Service AWS dans le Guide de l'utilisateur IAM.
  - Rôle lié à un service — Un rôle lié à un service est un type de rôle de service lié à un. Service AWS Le service peut endosser le rôle afin d'effectuer une action en votre nom. Les rôles liés à un service apparaissent dans votre Compte AWS répertoire et appartiennent au service. Un administrateur IAM peut consulter, mais ne peut pas modifier, les autorisations concernant les rôles liés à un service.
- Applications exécutées sur Amazon EC2 : vous pouvez utiliser un rôle IAM pour gérer les informations d'identification temporaires pour les applications qui s'exécutent sur une instance EC2 et qui envoient des demandes d'API. AWS CLI AWS Cette solution est préférable au stockage des clés d'accès au sein de l'instance EC2. Pour attribuer un AWS rôle à une instance EC2 et le mettre à la disposition de toutes ses applications, vous devez créer un profil d'instance attaché à l'instance. Un profil d'instance contient le rôle et permet aux programmes qui s'exécutent sur l'instance EC2 d'obtenir des informations d'identification temporaires. Pour plus d'informations, consultez Utilisation d'un rôle IAM pour accorder des autorisations à des applications s'exécutant sur des instances Amazon EC2 dans le Guide de l'utilisateur IAM.

Pour savoir dans quel cas utiliser des rôles ou des utilisateurs IAM, consultez Quand créer un rôle IAM (au lieu d'un utilisateur) dans le Guide de l'utilisateur IAM.

Gestion des accès à l'aide de politiques

Vous contrôlez l'accès en AWS créant des politiques et en les associant à AWS des identités ou à des ressources. Une politique est un objet AWS qui, lorsqu'il est associé à une identité ou à une ressource, définit leurs autorisations. AWS évalue ces politiques lorsqu'un principal (utilisateur, utilisateur root ou session de rôle) fait une demande. Les autorisations dans les politiques déterminent si la demande est autorisée ou refusée. La plupart des politiques sont stockées AWS sous forme de documents JSON. Pour plus d'informations sur la structure et le contenu des documents de politique JSON, consultez Vue d'ensemble des politiques JSON dans le Guide de l'utilisateur IAM.

Les administrateurs peuvent utiliser les politiques AWS JSON pour spécifier qui a accès à quoi. C'est-à-dire, quel principal peut effectuer des actions sur quelles ressources et dans quelles conditions.

Par défaut, les utilisateurs et les rôles ne disposent d'aucune autorisation. Pour octroyer aux utilisateurs des autorisations d'effectuer des actions sur les ressources dont ils ont besoin, un administrateur IAM peut créer des politiques IAM. L'administrateur peut ensuite ajouter les politiques IAM aux rôles et les utilisateurs peuvent assumer les rôles.

Les politiques IAM définissent les autorisations d'une action, quelle que soit la méthode que vous utilisez pour exécuter l'opération. Par exemple, supposons que vous disposiez d'une politique qui autorise l'action `iam:GetRole`. Un utilisateur appliquant cette politique peut obtenir des informations sur le rôle à partir de AWS Management Console AWS CLI, de ou de l' AWS API.

Politiques basées sur l'identité

Les politiques basées sur l'identité sont des documents de politique d'autorisations JSON que vous pouvez attacher à une identité telle qu'un utilisateur, un groupe d'utilisateurs ou un rôle IAM. Ces politiques contrôlent quel type d'actions des utilisateurs et des rôles peuvent exécuter, sur quelles ressources et dans quelles conditions. Pour découvrir comment créer une politique basée sur l'identité, consultez Création de politiques IAM dans le Guide de l'utilisateur IAM.

Les politiques basées sur l'identité peuvent être classées comme des politiques en ligne ou des politiques gérées. Les politiques en ligne sont intégrées directement à un utilisateur, groupe ou rôle. Les politiques gérées sont des politiques autonomes que vous pouvez associer à plusieurs utilisateurs, groupes et rôles au sein de votre Compte AWS. Les politiques gérées incluent les

politiques AWS gérées et les politiques gérées par le client. Pour découvrir comment choisir entre une politique gérée et une politique en ligne, consultez Choix entre les politiques gérées et les politiques en ligne dans le Guide de l'utilisateur IAM.

politiques basées sur les ressources

Les politiques basées sur les ressources sont des documents de politique JSON que vous attachez à une ressource. Des politiques basées sur les ressources sont, par exemple, les politiques de confiance de rôle IAM et des politiques de compartiment. Dans les services qui sont compatibles avec les politiques basées sur les ressources, les administrateurs de service peuvent les utiliser pour contrôler l'accès à une ressource spécifique. Pour la ressource dans laquelle se trouve la politique, cette dernière définit quel type d'actions un principal spécifié peut effectuer sur cette ressource et dans quelles conditions. Vous devez spécifier un principal dans une politique basée sur les ressources. Les principaux peuvent inclure des comptes, des utilisateurs, des rôles, des utilisateurs fédérés ou. Services AWS

Les politiques basées sur les ressources sont des politiques en ligne situées dans ce service. Vous ne pouvez pas utiliser les politiques AWS gérées par IAM dans une stratégie basée sur les ressources.

Listes de contrôle d'accès (ACL)

Les listes de contrôle d'accès (ACL) vérifie quels principals (membres de compte, utilisateurs ou rôles) ont l'autorisation d'accéder à une ressource. Les listes de contrôle d'accès sont similaires aux politiques basées sur les ressources, bien qu'elles n'utilisent pas le format de document de politique JSON.

Amazon S3 et Amazon VPC sont des exemples de services qui prennent en charge les ACL. AWS WAF Pour en savoir plus sur les listes de contrôle d'accès, consultez Vue d'ensemble des listes de contrôle d'accès (ACL) dans le Guide du développeur Amazon Simple Storage Service.

Autres types de politique

AWS prend en charge d'autres types de politiques moins courants. Ces types de politiques peuvent définir le nombre maximum d'autorisations qui vous sont accordées par des types de politiques plus courants.

- Limite d'autorisations : une limite d'autorisations est une fonctionnalité avancée dans laquelle vous définissez le nombre maximal d'autorisations qu'une politique basée sur l'identité peut accorder à une entité IAM (utilisateur ou rôle IAM). Vous pouvez définir une limite d'autorisations pour

une entité. Les autorisations en résultant représentent la combinaison des politiques basées sur l'identité d'une entité et de ses limites d'autorisation. Les politiques basées sur les ressources qui spécifient l'utilisateur ou le rôle dans le champ `Principal` ne sont pas limitées par les limites d'autorisations. Un refus explicite dans l'une de ces politiques remplace l'autorisation. Pour plus d'informations sur les limites d'autorisations, consultez Limites d'autorisations pour des entités IAM dans le Guide de l'utilisateur IAM.

- Politiques de contrôle des services (SCP) — Les SCP sont des politiques JSON qui spécifient les autorisations maximales pour une organisation ou une unité organisationnelle (UO) dans. AWS Organizations AWS Organizations est un service permettant de regrouper et de gérer de manière centralisée Comptes AWS les multiples propriétés de votre entreprise. Si vous activez toutes les fonctionnalités d'une organisation, vous pouvez appliquer les politiques de contrôle des services (SCP) à l'un ou à l'ensemble de vos comptes. Le SCP limite les autorisations pour les entités figurant dans les comptes des membres, y compris chacune Utilisateur racine d'un compte AWS d'entre elles. Pour plus d'informations sur les organisations et les SCP, consultez Fonctionnement des SCP dans le Guide de l'utilisateur AWS Organizations .
- Politiques de séance : les politiques de séance sont des politiques avancées que vous utilisez en tant que paramètre lorsque vous créez par programmation une séance temporaire pour un rôle ou un utilisateur fédéré. Les autorisations de séance en résultant sont une combinaison des politiques basées sur l'identité de l'utilisateur ou du rôle et des politiques de séance. Les autorisations peuvent également provenir d'une politique basée sur les ressources. Un refus explicite dans l'une de ces politiques annule l'autorisation. Pour plus d'informations, consultez politiques de séance dans le Guide de l'utilisateur IAM.

Plusieurs types de politique

Lorsque plusieurs types de politiques s'appliquent à la requête, les autorisations en résultant sont plus compliquées à comprendre. Pour savoir comment AWS déterminer s'il faut autoriser une demande lorsque plusieurs types de politiques sont impliqués, consultez la section Logique d'évaluation des politiques dans le guide de l'utilisateur IAM.

Comment Services AWS travailler avec IAM

Pour obtenir une vue d'ensemble du Services AWS fonctionnement de la plupart des fonctionnalités IAM, consultez les AWS services compatibles avec IAM dans le guide de l'utilisateur IAM.

Pour savoir comment utiliser un service spécifique Service AWS avec IAM, consultez la section sécurité du guide de l'utilisateur du service concerné.

Résolution des problèmes AWS d'identité et d'accès

Utilisez les informations suivantes pour vous aider à diagnostiquer et à résoudre les problèmes courants que vous pouvez rencontrer lorsque vous travaillez avec AWS IAM.

Rubriques

Je ne suis pas autorisé à effectuer une action dans AWS

Si vous recevez une erreur qui indique que vous n'êtes pas autorisé à effectuer une action, vos politiques doivent être mises à jour afin de vous permettre d'effectuer l'action.

L'exemple d'erreur suivant se produit quand l'utilisateur IAM `mateojackson` tente d'utiliser la console pour afficher des informations détaillées sur une ressource *`my-example-widget`* fictive, mais ne dispose pas des autorisations `awes:`*`GetWidget`* fictives.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 awes:GetWidget on resource: my-example-widget
```

Dans ce cas, la politique qui s'applique à l'utilisateur `mateojackson` doit être mise à jour pour autoriser l'accès à la ressource *`my-example-widget`* à l'aide de l'action `awes:`*`GetWidget`*.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je ne suis pas autorisé à effectuer iam : PassRole

Si vous recevez une erreur selon laquelle vous n'êtes pas autorisé à exécuter `iam:PassRole` l'action, vos stratégies doivent être mises à jour afin de vous permettre de transmettre un rôle à AWS.

Certains vous Services AWS permettent de transmettre un rôle existant à ce service au lieu de créer un nouveau rôle de service ou un rôle lié à un service. Pour ce faire, un utilisateur doit disposer des autorisations nécessaires pour transmettre le rôle au service.

L'exemple d'erreur suivant se produit lorsqu'un utilisateur IAM nommé `marymajor` essaie d'utiliser la console pour exécuter une action dans AWS. Toutefois, l'action nécessite que le service ait des autorisations accordées par une fonction de service. Mary ne dispose pas des autorisations nécessaires pour transférer le rôle au service.

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

Dans ce cas, les politiques de Mary doivent être mises à jour pour lui permettre d'exécuter l'action `iam:PassRole`.

Si vous avez besoin d'aide, contactez votre AWS administrateur. Votre administrateur vous a fourni vos informations d'identification de connexion.

Je souhaite permettre à des personnes extérieures Compte AWS à moi d'accéder à mes AWS ressources

Vous pouvez créer un rôle que les utilisateurs provenant d'autres comptes ou les personnes extérieures à votre organisation pourront utiliser pour accéder à vos ressources. Vous pouvez spécifier qui est autorisé à assumer le rôle. Pour les services qui prennent en charge les politiques basées sur les ressources ou les listes de contrôle d'accès (ACL), vous pouvez utiliser ces politiques pour donner l'accès à vos ressources.

Pour en savoir plus, consultez les éléments suivants :

- Pour savoir si ces fonctionnalités sont prises AWS en charge, consultezComment Services AWS travailler avec IAM.
- Pour savoir comment fournir l'accès à vos ressources sur celles Comptes AWS que vous possédez, consultez la section Fournir l'accès à un utilisateur IAM dans un autre utilisateur Compte AWS que vous possédez dans le Guide de l'utilisateur IAM.
- Pour savoir comment fournir l'accès à vos ressources à des tiers Comptes AWS, consultez la section Fournir un accès à des ressources Comptes AWS détenues par des tiers dans le guide de l'utilisateur IAM.
- Pour savoir comment fournir un accès par le biais de la fédération d'identité, consultez Fournir un accès à des utilisateurs authentifiés en externe (fédération d'identité) dans le Guide de l'utilisateur IAM.

- Pour découvrir quelle est la différence entre l'utilisation des rôles et l'utilisation des politiques basées sur les ressources pour l'accès entre comptes, consultez Différence entre les rôles IAM et les politiques basées sur les ressources dans le Guide de l'utilisateur IAM.

Validation de conformité pour ce AWS produit ou service

Pour savoir si un programme Services AWS de conformité Service AWS s'inscrit dans le champ d'application de programmes de conformité spécifiques, consultez Services AWS la section de conformité et sélectionnez le programme de conformité qui vous intéresse. Pour des informations générales, voir Programmes de AWS conformité Programmes AWS de .

Vous pouvez télécharger des rapports d'audit tiers à l'aide de AWS Artifact. Pour plus d'informations, voir Téléchargement de rapports dans AWS Artifact .

Votre responsabilité en matière de conformité lors de l'utilisation Services AWS est déterminée par la sensibilité de vos données, les objectifs de conformité de votre entreprise et les lois et réglementations applicables. AWS fournit les ressources suivantes pour faciliter la mise en conformité :

- Guides de démarrage rapide sur la sécurité et la conformité : ces guides de déploiement abordent les considérations architecturales et indiquent les étapes à suivre pour déployer des environnements de base axés sur AWS la sécurité et la conformité.
- Architecture axée sur la sécurité et la conformité HIPAA sur Amazon Web Services : ce livre blanc décrit comment les entreprises peuvent créer des applications AWS conformes à la loi HIPAA.

> **Note**
>
> Tous ne Services AWS sont pas éligibles à la loi HIPAA. Pour plus d'informations, consultez le HIPAA Eligible Services Reference.

- AWS Ressources de https://aws.amazon.com/compliance/resources/ de conformité — Cette collection de classeurs et de guides peut s'appliquer à votre secteur d'activité et à votre région.
- AWS Guides de conformité destinés aux clients — Comprenez le modèle de responsabilité partagée sous l'angle de la conformité. Les guides résument les meilleures pratiques en matière de sécurisation Services AWS et décrivent les directives relatives aux contrôles de sécurité dans de nombreux cadres (notamment le National Institute of Standards and Technology (NIST),

le Payment Card Industry Security Standards Council (PCI) et l'Organisation internationale de normalisation (ISO)).

- Évaluation des ressources à l'aide des règles du guide du AWS Config développeur : le AWS Config service évalue dans quelle mesure les configurations de vos ressources sont conformes aux pratiques internes, aux directives du secteur et aux réglementations.
- AWS Security Hub— Cela Service AWS fournit une vue complète de votre état de sécurité interne AWS. Security Hub utilise des contrôles de sécurité pour évaluer vos ressources AWS et vérifier votre conformité par rapport aux normes et aux bonnes pratiques du secteur de la sécurité. Pour obtenir la liste des services et des contrôles pris en charge, consultez Référence des contrôles Security Hub.
- Amazon GuardDuty — Cela Service AWS détecte les menaces potentielles qui pèsent sur vos charges de travail Comptes AWS, vos conteneurs et vos données en surveillant votre environnement pour détecter toute activité suspecte et malveillante. GuardDuty peut vous aider à répondre à diverses exigences de conformité, telles que la norme PCI DSS, en répondant aux exigences de détection des intrusions imposées par certains cadres de conformité.
- AWS Audit Manager— Cela vous Service AWS permet d'auditer en permanence votre AWS utilisation afin de simplifier la gestion des risques et la conformité aux réglementations et aux normes du secteur.

Ce AWS produit ou service suit le modèle de responsabilité partagée par le biais des services Amazon Web Services (AWS) spécifiques qu'il prend en charge. Pour obtenir des informations sur la sécurité des AWS services, consultez la AWS page de documentation sur la sécuritéAWS des services et les services concernés par les efforts de AWS conformité par programme de conformité.

Résilience pour ce AWS produit ou service

L'infrastructure AWS mondiale est construite autour Régions AWS de zones de disponibilité.

Régions AWS fournissent plusieurs zones de disponibilité physiquement séparées et isolées, connectées par un réseau à faible latence, à haut débit et hautement redondant.

Avec les zones de disponibilité, vous pouvez concevoir et exploiter des applications et des bases de données qui basculent automatiquement d’une zone à l’autre sans interruption. Les zones de disponibilité sont davantage disponibles, tolérantes aux pannes et ont une plus grande capacité de mise à l’échelle que les infrastructures traditionnelles à un ou plusieurs centres de données.

Pour plus d'informations sur AWS les régions et les zones de disponibilité, consultez la section Infrastructure AWS mondiale.

Ce AWS produit ou service suit le modèle de responsabilité partagée par le biais des services Amazon Web Services (AWS) spécifiques qu'il prend en charge. Pour obtenir des informations sur la sécurité des AWS services, consultez la AWS page de documentation sur la sécuritéAWS des services et les services concernés par les efforts de AWS conformité par programme de conformité.

Sécurité de l'infrastructure pour ce AWS produit ou service

Ce AWS produit ou service utilise des services gérés et est donc protégé par la sécurité du réseau AWS mondial. Pour plus d'informations sur les services AWS de sécurité et sur la manière dont AWS l'infrastructure est protégée, consultez la section Sécurité du AWS cloud. Pour concevoir votre AWS environnement en utilisant les meilleures pratiques en matière de sécurité de l'infrastructure, consultez la section Protection de l'infrastructure dans le cadre AWS bien architecturé du pilier de sécurité.

Vous utilisez des appels d'API AWS publiés pour accéder à ce AWS produit ou service via le réseau. Les clients doivent prendre en charge les éléments suivants :

- Protocole TLS (Transport Layer Security). Nous exigeons TLS 1.2 et recommandons TLS 1.3.
- Ses suites de chiffrement PFS (Perfect Forward Secrecy) comme DHE (Ephemeral Diffie-Hellman) ou ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La plupart des systèmes modernes tels que Java 7 et les versions ultérieures prennent en charge ces modes.

En outre, les demandes doivent être signées à l'aide d'un ID de clé d'accès et d'une clé d'accès secrète associée à un principal IAM. Vous pouvez également utiliser AWS Security Token Service (AWS STS) pour générer des informations d'identification de sécurité temporaires et signer les demandes.

Ce AWS produit ou service suit le modèle de responsabilité partagée par le biais des services Amazon Web Services (AWS) spécifiques qu'il prend en charge. Pour obtenir des informations sur la sécurité des AWS services, consultez la AWS page de documentation sur la sécuritéAWS des services et les services concernés par les efforts de AWS conformité par programme de conformité.

Analyse de configuration et de vulnérabilité dans AWS Toolkit for Visual Studio

Le Toolkit for Visual Studio est publié sur Visual Studio Marketplace au fur et à mesure que de nouvelles fonctionnalités ou correctifs sont développés. Ces mises à jour incluent parfois des mises à jour de sécurité. Il est donc important de maintenir Toolkit for Visual Studio à jour.

Pour vérifier que les mises à jour automatiques des extensions sont activées

1. Ouvrez le gestionnaire d'extensions en choisissant Outils, extensions et mises à jour (Visual Studio 2017) ou Extensions, Gérer les extensions (Visual Studio 2019).
2. Choisissez Modifier les paramètres des extensions et des mises à jour (Visual Studio 2017) ou Modifier les paramètres des extensions (Visual Studio 2019).
3. Réglez les paramètres de votre environnement.

Si vous choisissez de désactiver les mises à jour automatiques pour les extensions, assurez-vous de vérifier les mises à jour de Toolkit for Visual Studio à des intervalles adaptés à votre environnement.

Historique du document du guide de AWS Toolkit for Visual Studio l'utilisateur

Dernière mise à jour de la documentation : 21 avril 2021

Historique de la documentation

Le tableau suivant décrit les modifications récentes importantes apportées au guide de l' AWS Toolkit for Visual Studio utilisateur. Pour recevoir les notifications concernant les mises à jour de cette documentation, abonnez-vous à un flux RSS.

Modification	Description	Date
Mises à jour et maintenance du contenu	Mise à jour du contenu pour tenir compte des modifications apportées à l'interface utilisateur et aux directives de AWS style.	6 mars 2024
Mises à jour et maintenance du contenu	Mise à jour du contenu pour tenir compte des modifications apportées à l'interface utilisateur et aux directives de AWS style.	6 mars 2024
Mises à jour et maintenance du contenu	Mise à jour du contenu pour tenir compte des modifications apportées à l'interface utilisateur et aux directives de AWS style.	6 mars 2024
Mises à jour et maintenance du contenu	Mise à jour du contenu pour tenir compte des modifications apportées à l'interface utilisateur et aux directives de AWS style.	6 mars 2024

Mises à jour et maintenance du contenu	Mise à jour du contenu pour tenir compte des modifications apportées à l'interface utilisateur et aux directives de AWS style.	6 mars 2024
Mises à jour relatives à la configuration et à l'authentification	Les rubriques relatives à la configuration et à l'authentification ont été mises à jour afin d'améliorer la sécurité et l'expérience d'intégration de la boîte à outils. Consultez les tables des matières relatives à la mise en route et à l'authentification et à l'accès pour consulter les modifications.	22 juin 2023
Authentification et accès	Fournir des AWS informations d'identification s'appelle désormais Authentification et accès. Refactorisation de la table des matières et des sous-rubriques pour répondre aux exigences de style et de sécurité AWS .	4 mai 2023
Nouvelle rubrique générale sur le dépannage	La rubrique Dépannage contient des informations générales sur le dépannage des services AWS Toolkit for Visual Studio et des services associés.	30 avril 2023

Mises à jour des sections et rubriques relatives à la configuration	Les AWS Toolkit for Visual Studio sections et rubriques de ce guide de l'utilisateur relatives à la configuration ont été mises à jour afin d'amélior er l'expérience d'intégration du AWS Toolkit for Visual Studio.	30 janvier 2023
Mises à jour des sections et rubriques relatives à la configuration	Les AWS Toolkit for Visual Studio sections et rubriques de ce guide de l'utilisateur relatives à la configuration ont été mises à jour afin d'amélior er l'expérience d'intégration du AWS Toolkit for Visual Studio.	30 janvier 2023
AWS Toolkit for Visual Studio Informations ajoutées en 2022	Support pour Visual Studio 2022 a été ajouté au AWS Toolkit for Visual Studio.	20 décembre 2022
Mises à jour du AWS guide Publish to	Mises à jour de la documenta tion pour refléter les modificat ions apportées au service pour le lancement de GA.	6 juillet 2022
Mises à jour des titres et relocalisation	Des modifications mineures ont été apportées au titre afin de mieux refléter le contenu. Le guide se trouve désormais dans le AWS guide Publishing to.	6 juillet 2022

Déploiement vers AWS : mises à jour du titre et du contenu	La section du guide, officiellement intitulée : Déploiement à l'aide du AWS kit d'outils, contient une table des matières (TOC) mise à jour et s'intitule désormais : Déploiement vers AWS. Les guides suivants sont devenus obsolètes et ne sont plus accessibles : Deploying to Elastic Beanstalk (Legacy) et Deploying to (Legacy). AWS CloudFormation Le contenu mis à jour concernant le déploiement sur Elastic Beanstalk et Cloudformation est disponible dans la table des matières mise à jour de ce guide.	6 juillet 2022
Le déploiement d'une application ASP.NET Core 2.0 (Fargate) est désormais un ancien guide	Cette documentation fait référence aux services et fonctionnalités existants. Pour obtenir des guides et du contenu mis à jour, consultez le guide de l'outil de déploiement AWS .NET et la AWS table des matières mise à jour du Déploiement vers.	6 juillet 2022

Déployer une application ASP.NET est désormais un ancien guide	Cette documentation fait référence aux services et fonctionnalités existants. Pour obtenir des guides et du contenu mis à jour, consultez le guide de l'outil de déploiement AWS .NET et la AWS table des matières mise à jour de Deploying to.	6 juillet 2022
Déployer une application ASP.NET est désormais un ancien guide	Cette documentation fait référence aux services et fonctionnalités existants. Pour obtenir des guides et du contenu mis à jour, consultez le guide de l'outil de déploiement AWS .NET et la AWS table des matières mise à jour de Deploying to.	6 juillet 2022
Nouveau sujet du guide : Utilisation des CloudWatch journaux dans Visual Studio	Création d'une nouvelle rubrique de présentation pour le guide d'intégration d'Amazon CloudWatch Logs dans Visual Studio.	29 juin 2022
Nouveau sujet du guide : Configuration de l'intégration CloudWatch des journaux pour Visual Studio	Création d'une nouvelle section de configuration pour le guide d'intégration d'Amazon CloudWatch Logs dans Visual Studio.	29 juin 2022

CloudWatch Intégration des journaux pour Visual Studio	Création d'un nouveau guide pour l'intégration d'Amazon CloudWatch Logs dans Visual Studio, y compris les rubriques suivantes : Configuration CloudWatch des journaux pour Visual Studio et utilisation des CloudWatch journaux dans Visual Studio.	29 juin 2022
Publier sur AWS	Publier sur n' AWS est plus disponible en version prélimina ire. Mises à jour pour refléter les modifications apportées à l'interface utilisateur et les améliorations apportées aux suggestions de publication.	1 juin 2022
La nouvelle publication sera AWS disponible en avant-pre mière	Expérience de déploieme nt améliorée qui fournit des conseils sur le AWS service le mieux adapté à votre applicati on.	21 octobre 2021
Support SSO et MFA pour les informations d'identification AWS	Mise à jour pour documente r la nouvelle prise en charge de l'authentification AWS unique (IAM Identity Center) et de l'authentification multifact orielle dans les informations d'identification. AWS	21 avril 2021
AWS Lambda Projet de base : création d'une image Docker	Ajout de la prise en charge pour les images de conteneur Lambda.	1er décembre 2020
Contenu relatif à la sécurité	Ajout du contenu de sécurité.	6 février 2020

Fournir des AWS informations d'identification	Mise à jour avec des informations sur la création de profils d'identification dans le fichier AWS d'informations d'identification partagé.	20 juin 2019
Utilisation du projet AWS Lambda dans le AWS Toolkit for Visual Studio	Support pour Visual Studio 2019 a été ajouté au AWS Toolkit for Visual Studio.	28 mars 2019
Tutoriel : Création d'une application Amazon Rekognition Lambda	Support pour Visual Studio 2019 a été ajouté au AWS Toolkit for Visual Studio.	28 mars 2019
Tutoriel : Création et test d'une application sans serveur avec Lambda AWS	Support pour Visual Studio 2019 a été ajouté au AWS Toolkit for Visual Studio.	28 mars 2019
Configuration du AWS Toolkit for Visual Studio	Support pour Visual Studio 2019 a été ajouté au AWS Toolkit for Visual Studio.	28 mars 2019
Déploiement d'une application ASP.NET Core 2.0 (Fargate)	Support pour Visual Studio 2019 a été ajouté au AWS Toolkit for Visual Studio.	28 mars 2019
Déploiement d'une application ASP.NET Core 2.0 (EC2)	Support pour Visual Studio 2019 a été ajouté au AWS Toolkit for Visual Studio.	28 mars 2019
Création d'un AWS CloudFormation modèle de projet dans Visual Studio	Support pour Visual Studio 2019 a été ajouté au AWS Toolkit for Visual Studio.	28 mars 2019

Vues détaillées du service de conteneurs	Ajout d'informations sur les vues détaillées des clusters et référentiels de conteneurs Amazon Elastic Container Service fournies par AWS Explorer.	16 février 2018
Déploiement sur Amazon EC2 Container Service	Ajout d'informations sur le déploiement vers Amazon EC2 Container Service.	16 février 2018
Déploiement de Container Service à l'aide de Fargate	Ajout d'informations sur le déploiement d'une application ASP.NET Core 2.0 conteneurisée ciblant Linux via Amazon ECS à l'aide du type de lancement Fargate.	16 février 2018
Déploiement du service de conteneur à l'aide d'EC2	Ajout d'informations sur le déploiement d'une application ASP.NET Core 2.0 conteneurisée ciblant Linux via Amazon ECS en utilisant le type de lancement EC2.	16 février 2018
Informations d'identification pour le déploiement sur Amazon EC2 Container Service	Ajout d'informations sur la façon de spécifier des informations d'identification lors du déploiement vers Amazon EC2 Container Service.	16 février 2018

Les traductions sont fournies par des outils de traduction automatique. En cas de conflit entre le contenu d'une traduction et celui de la version originale en anglais, la version anglaise prévaudra.