Commencez avec le mode restreint

Setup and administration

NetApp
April 26, 2024

Sommaire

Commencez avec le mode restreint

Démarrage du flux de travail (mode restreint)

Commencez à utiliser BlueXP en mode restreint en préparant votre environnement, en déployant le connecteur et en vous abonnant à BlueXP.

Le mode restreint est généralement utilisé par les administrations publiques et locales, ainsi que par les entreprises réglementées, y compris les déploiements dans les régions AWS GovCloud et Azure Government. Avant de commencer, vous devez avoir une compréhension de "Comptes BlueXP", "Connecteurs", et "modes de déploiement".

1 **"Préparation du déploiement"**

1. Préparez un hôte Linux dédié qui répond aux exigences en matière de processeur, de RAM, d'espace disque, de moteur Docker et bien plus encore.
2. Configurez le réseau qui fournit un accès aux réseaux cibles, un accès Internet sortant pour les installations manuelles et un accès Internet sortant pour un accès quotidien.
3. Configurez des autorisations dans votre fournisseur de cloud afin que vous puissiez les associer à l'instance Connector après le déploiement.

2 **"Déployez le connecteur"**

1. Installez le connecteur à partir du Marketplace de votre fournisseur de cloud ou en installant manuellement le logiciel sur votre propre hôte Linux.
2. Configurez BlueXP en ouvrant un navigateur Web et en entrant l'adresse IP de l'hôte Linux.
3. Fournissez à BlueXP les autorisations que vous avez précédemment configurées.

3 **"Abonnez-vous à BlueXP"**

Abonnez-vous à BlueXP sur le marché de votre fournisseur cloud pour payer les services BlueXP à un taux horaire (PAYGO) ou un contrat annuel.

Préparez le déploiement en mode restreint

Préparez votre environnement avant de déployer BlueXP en mode restreint. Par exemple, vous devez examiner les exigences relatives aux hôtes, préparer la mise en réseau, configurer les autorisations, etc.

Étape 1 : comprendre le fonctionnement du mode restreint

Avant de commencer, vous devez connaître le fonctionnement de BlueXP en mode restreint.

Par exemple, vous devez comprendre que vous devez utiliser l'interface web disponible localement à partir du connecteur BlueXP que vous devez installer. BlueXP n'est pas accessible depuis la console web fournie via la couche SaaS.

En outre, les services BlueXP ne sont pas tous disponibles.

"Découvrez le fonctionnement du mode restreint".

Étape 2 : passez en revue les options d'installation

En mode restreint, vous pouvez uniquement installer le connecteur dans le nuage. Les options d'installation suivantes sont disponibles :

- Depuis AWS Marketplace
- À partir d'Azure Marketplace
- Installation manuelle du connecteur sur votre propre hôte Linux exécuté dans AWS, Azure ou Google Cloud

Étape 3 : vérifiez la configuration requise pour l'hôte

Le logiciel du connecteur doit être exécuté sur un hôte qui répond à des exigences spécifiques du système d'exploitation, de la RAM, des ports, etc.

Lorsque vous déployez le connecteur à partir d'AWS ou d'Azure Marketplace, l'image inclut le système d'exploitation et les composants logiciels requis. Il vous suffit de choisir un type d'instance qui répond aux exigences en termes de processeur et de RAM.

Hôte dédié

Le connecteur n'est pas pris en charge sur un hôte partagé avec d'autres applications. L'hôte doit être un hôte dédié.

Systèmes d'exploitation pris en charge

- Ubuntu 22.04 LTS
- CentOS 7.6, 7.7, 7.8 et 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8 et 7.9

  L'hôte doit être enregistré auprès de Red Hat Subscription Management. S'il n'est pas enregistré, l'hôte ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis lors de l'installation du connecteur.

  Le connecteur est pris en charge sur les versions en anglais de ces systèmes d'exploitation.

Hyperviseur

Un hyperviseur bare Metal ou hébergé certifié pour exécuter Ubuntu, CentOS ou Red Hat Enterprise Linux est requis.

"Solution Red Hat : quels hyperviseurs sont certifiés pour l'exécution de Red Hat Enterprise Linux ?"

CPU

4 cœurs ou 4 CPU virtuels

RAM

14 GO

Type d'instance AWS EC2

Type d'instance qui répond aux exigences relatives au CPU et à la RAM indiquées ci-dessus. Nous recommandons une instance t3.XLarge.

Taille des machines virtuelles Azure

Type d'instance qui répond aux exigences relatives au CPU et à la RAM indiquées ci-dessus. Nous recommandons DS3 v2.

Type de machine Google Cloud

Type d'instance qui répond aux exigences relatives au CPU et à la RAM indiquées ci-dessus. Nous recommandons n2-standard-4.

Ce connecteur est pris en charge dans Google Cloud sur une instance de machine virtuelle avec un système d'exploitation pris en charge "Fonctionnalités MV blindées"

Espace disque dans /opt

100 Gio d'espace doit être disponible

Espace disque dans /var

20 Gio d'espace doit être disponible

Moteur Docker

Docker Engine est requis sur l'hôte avant d'installer le connecteur.

- La version minimale prise en charge est 19.3.1.
- La version maximale prise en charge est 25.0.5.

"Voir les instructions d'installation"

Étape 4 : préparer le réseau

Configurez votre réseau de sorte que le connecteur puisse gérer les ressources et les processus au sein de votre environnement de cloud public. Outre le fait de disposer d'un réseau virtuel et d'un sous-réseau pour le connecteur, vous devez vous assurer que les exigences suivantes sont respectées.

Connexions aux réseaux cibles

Le connecteur doit disposer d'une connexion réseau à l'emplacement où vous prévoyez de gérer le stockage. Par exemple, le VPC ou le vnet sur lequel vous prévoyez de déployer Cloud Volumes ONTAP, ou le data Center dans lequel résident vos clusters ONTAP sur site.

Préparez la mise en réseau pour l'accès utilisateur à la console BlueXP

En mode restreint, l'interface utilisateur BlueXP est accessible depuis le connecteur. Lorsque vous utilisez l'interface utilisateur BlueXP, le service est en contact avec quelques terminaux pour effectuer les tâches de gestion des données. Ces terminaux sont contactés depuis l'ordinateur d'un utilisateur lorsqu'ils effectuent des actions spécifiques à partir de la console BlueXP.

Terminaux	Objectif
https://signin.b2c.netapp.com	Requis pour mettre à jour les identifiants du site de support NetApp (NSS) ou pour ajouter de nouvelles informations d'identification NSS à BlueXP.

Terminaux	Objectif
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	Votre navigateur Web se connecte à ces points de terminaison pour une authentification utilisateur centralisée via BlueXP.
https://widget.intercom.io	Vous bénéficiez d'un chat en ligne pour discuter avec des experts du cloud NetApp.

Points finaux contactés lors de l'installation manuelle

Lorsque vous installez manuellement le connecteur sur votre propre hôte Linux, le programme d'installation du connecteur nécessite l'accès aux URL suivantes pendant le processus d'installation :

- https://support.netapp.com
- https://mysupport.netapp.com
- https://cloudmanager.cloud.netapp.com/tenancy
- https://stream.cloudmanager.cloud.netapp.com
- https://production-artifacts.cloudmanager.cloud.netapp.com
- https://*.blob.core.windows.net
- https://cloudmanagerinfraprod.azurecr.io

  Ce terminal n'est pas requis dans les régions Azure Government.

- https://occmclientinfragov.azurecr.us

  Ce terminal n'est requis que dans les régions Azure Government.

L'hôte peut essayer de mettre à jour les packages du système d'exploitation lors de l'installation. L'hôte peut contacter différents sites de mise en miroir pour ces packages OS.

Accès Internet sortant pour les opérations quotidiennes

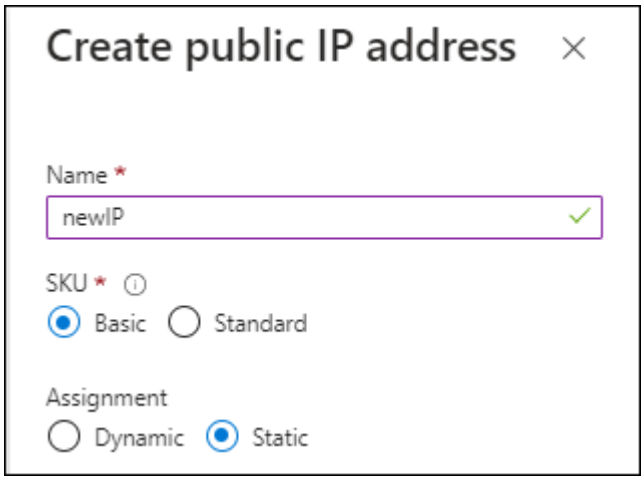
L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante. Le connecteur nécessite un accès Internet sortant pour contacter les terminaux suivants afin de gérer les ressources et les processus au sein de votre environnement de cloud public.

Terminaux	Objectif
Services AWS (amazonaws.com): • CloudFormation • Cloud de calcul élastique (EC2) • Gestion des identités et des accès • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Service de stockage simple (S3)	Pour gérer les ressources dans AWS. Le terminal exact dépend de la région AWS que vous utilisez. "Pour plus d'informations, consultez la documentation AWS"

Terminaux	Objectif
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	Afin de gérer les ressources dans les régions publiques d'Azure.
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	De gérer les ressources dans les régions Azure Government.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	De gérer les ressources dans les régions Azure China.
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	De gérer des ressources dans Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	Pour fournir des fonctions et des services SaaS dans BlueXP. Notez que le connecteur est actuellement en contact avec « cloudmanager.cloud.netapp.com", mais il commencera à contacter « api.bluexp.netapp.com" dans une prochaine version.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io Ce terminal n'est pas requis dans les régions Azure Government. https://occmclientinfragov.azurecr.us Ce terminal n'est requis que dans les régions Azure Government.	Pour mettre à niveau le connecteur et ses composants Docker.

Adresse IP publique dans Azure

Si vous souhaitez utiliser une adresse IP publique avec la machine virtuelle du connecteur dans Azure, l'adresse IP doit utiliser une référence de base pour garantir que BlueXP utilise cette adresse IP publique.



Si vous utilisez une adresse IP de référence standard, BlueXP utilise l'adresse IP *private* du connecteur, au lieu de l'adresse IP publique. Si la machine que vous utilisez pour accéder à la console BlueXP n'a pas accès à cette adresse IP privée, les actions de la console BlueXP échouent.

"Documentation Azure : référence IP publique"

Serveur proxy

Si votre organisation nécessite le déploiement d'un serveur proxy pour tout le trafic Internet sortant, procurez-vous les informations suivantes sur votre proxy HTTP ou HTTPS. Vous devrez fournir ces informations pendant l'installation.

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Notez que BlueXP ne prend pas en charge les serveurs proxy transparents.

Ports

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous l'initiez ou si le connecteur est utilisé comme proxy pour envoyer des messages AutoSupport de Cloud Volumes ONTAP au support NetApp.

- HTTP (80) et HTTPS (443) permettent d'accéder à l'interface utilisateur locale que vous utiliserez dans de rares circonstances.
- SSH (22) n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.
- Les connexions entrantes via le port 3128 sont requises si vous déployez des systèmes Cloud Volumes ONTAP dans un sous-réseau où aucune connexion Internet sortante n'est disponible.

  Si les systèmes Cloud Volumes ONTAP ne disposent pas d'une connexion Internet sortante pour envoyer des messages AutoSupport, BlueXP les configure automatiquement pour qu'ils utilisent un serveur proxy inclus avec le connecteur. La seule condition est de s'assurer que le groupe de sécurité du connecteur autorise les connexions entrantes sur le port 3128. Vous devrez ouvrir ce port après le déploiement du connecteur.

Activez le protocole NTP

Si vous prévoyez d'utiliser la classification BlueXP pour analyser vos sources de données d'entreprise, vous devez activer un service NTP (Network Time Protocol) sur le système de connecteur BlueXP et le système de classification BlueXP afin que l'heure soit synchronisée entre les systèmes. "En savoir plus sur la classification BlueXP"

Si vous prévoyez de créer le connecteur à partir du marché de votre fournisseur de cloud, vous devrez mettre en œuvre cette exigence de mise en réseau après avoir créé le connecteur.

Étape : 5 Préparez les autorisations cloud

BlueXP requiert l'autorisation de votre fournisseur cloud pour déployer Cloud Volumes ONTAP dans un réseau virtuel et utiliser les services de données BlueXP. Vous devez définir des autorisations dans votre fournisseur de cloud, puis les associer au connecteur.

Pour afficher les étapes requises, sélectionnez l'option d'authentification que vous souhaitez utiliser pour votre fournisseur de cloud.

Rôle IAM AWS

Utilisez un rôle IAM pour fournir au connecteur des autorisations.

Si vous créez le connecteur à partir d'AWS Marketplace, vous serez invité à sélectionner ce rôle IAM au lancement de l'instance EC2.

Si vous installez manuellement le connecteur sur votre propre hôte Linux, vous devrez associer le rôle à l'instance EC2.

Étapes

1. Connectez-vous à la console AWS et accédez au service IAM.
2. Création d'une règle :
   a. Sélectionnez **stratégies > Créer une stratégie**.
   b. Sélectionnez **JSON** et copiez et collez le contenu du "Politique IAM pour le connecteur".
   c. Terminez les étapes restantes pour créer la stratégie.
3. Créer un rôle IAM :
   a. Sélectionnez **rôles > Créer un rôle**.
   b. Sélectionnez **AWS service > EC2**.
   c. Ajoutez des autorisations en joignant la stratégie que vous venez de créer.
   d. Terminez les étapes restantes pour créer le rôle.

Résultat

Vous disposez désormais d'un rôle IAM pour l'instance de connecteur EC2.

Clé d'accès AWS

Configurer les autorisations et une clé d'accès pour un utilisateur IAM. Une fois le connecteur installé et configuré BlueXP, vous devez fournir BlueXP avec la clé d'accès AWS.

Étapes

1. Connectez-vous à la console AWS et accédez au service IAM.
2. Création d'une règle :

   a. Sélectionnez **stratégies > Créer une stratégie**.
   b. Sélectionnez **JSON** et copiez et collez le contenu du "Politique IAM pour le connecteur".
   c. Terminez les étapes restantes pour créer la stratégie.

      Selon les services BlueXP que vous prévoyez d'utiliser, il peut être nécessaire de créer une seconde règle.

   Pour les régions standard, les autorisations sont réparties entre deux règles. Deux règles sont requises en raison d'une taille maximale de caractères pour les stratégies gérées dans AWS. "En savoir plus sur les règles IAM pour le connecteur".

3. Associer les règles à un utilisateur IAM.
   - "Documentation AWS : création de rôles IAM"
   - "Documentation AWS : ajout et suppression de règles IAM"

4. Assurez-vous que l'utilisateur dispose d'une clé d'accès que vous pouvez ajouter à BlueXP après l'installation du connecteur.

Résultat

Le compte dispose désormais des autorisations requises.

Rôle d'Azure

Créez un rôle Azure personnalisé avec les autorisations requises. Vous allez attribuer ce rôle à la machine virtuelle Connector.

Notez que vous pouvez créer un rôle personnalisé Azure à l'aide du portail Azure, d'Azure PowerShell, de l'interface de ligne de commandes Azure ou de l'API REST. La procédure suivante explique comment créer le rôle à l'aide de l'interface de ligne de commandes Azure. Si vous préférez utiliser une autre méthode, reportez-vous à la section "Documentation Azure"

Étapes

1. Si vous prévoyez d'installer manuellement le logiciel sur votre propre hôte, activez une identité gérée attribuée par le système sur la machine virtuelle afin de fournir les autorisations Azure requises via un rôle personnalisé.

   "Documentation Microsoft Azure : configurez les identités gérées des ressources Azure sur une machine virtuelle à l'aide du portail Azure"

2. Copier le contenu du "Autorisations de rôle personnalisées pour le connecteur" Et les enregistrer dans un fichier JSON.
3. Modifiez le fichier JSON en ajoutant des identifiants d'abonnement Azure à l'étendue assignable.

   Vous devez ajouter l'identifiant de chaque abonnement Azure que vous souhaitez utiliser avec BlueXP.

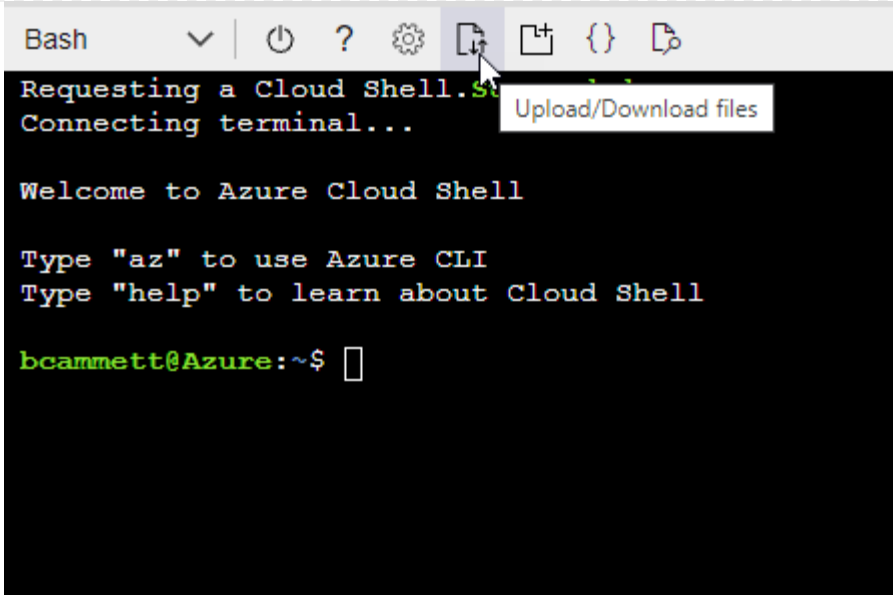
   Exemple

   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

4. Utilisez le fichier JSON pour créer un rôle personnalisé dans Azure.

   Les étapes suivantes expliquent comment créer le rôle à l'aide de Bash dans Azure Cloud Shell.

   a. Démarrer "Shell cloud Azure" Et choisissez l'environnement Bash.
   b. Téléchargez le fichier JSON.



c. Pour créer le rôle personnalisé, utilisez l'interface de ligne de commandes Azure :

```
az role definition create --role-definition Connector_Policy.json
```

Résultat

Vous devez maintenant avoir un rôle personnalisé appelé opérateur BlueXP que vous pouvez affecter à la machine virtuelle connecteur.

Principal de service Azure

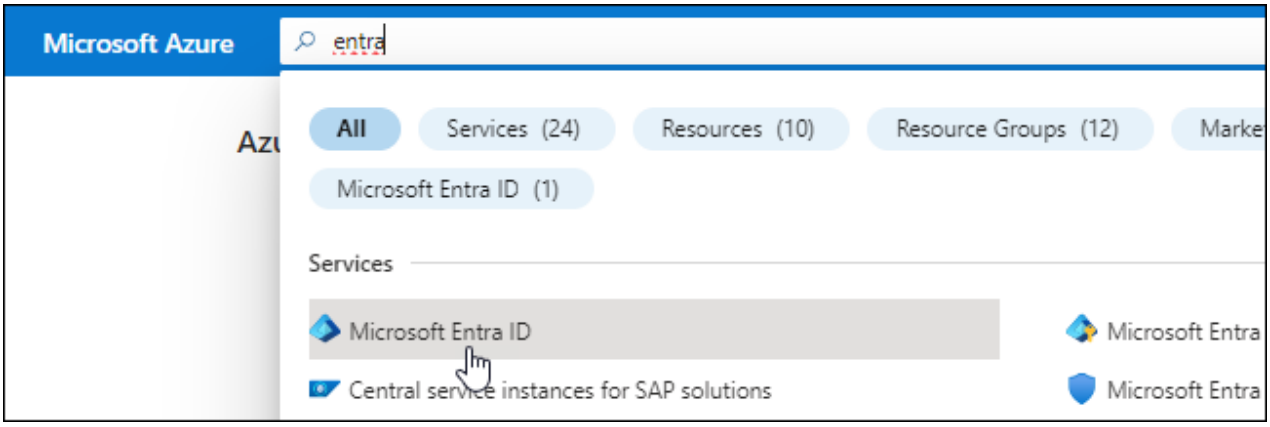
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont BlueXP a besoin. Après avoir installé le connecteur et configuré BlueXP, vous devez fournir ces informations d'identification à BlueXP.

Créez une application Microsoft Entra pour le contrôle d'accès basé sur les rôles

1. Assurez-vous que vous disposez des autorisations dans Azure pour créer une application Active Directory et attribuer l'application à un rôle.

   Pour plus de détails, reportez-vous à "Documentation Microsoft Azure : autorisations requises"

2. À partir du portail Azure, ouvrez le service **Microsoft Entra ID**.



3. Dans le menu, sélectionnez **enregistrements d'applications**.
4. Sélectionnez **nouvel enregistrement**.
5. Spécifiez les détails de l'application :
   - **Nom** : saisissez un nom pour l'application.
   - **Type de compte** : sélectionnez un type de compte (tout fonctionne avec BlueXP).
   - **URI de redirection**: Vous pouvez laisser ce champ vide.
6. Sélectionnez **Enregistrer**.

   Vous avez créé l'application AD et le principal de service.

Attribuez l'application à un rôle

1. Création d'un rôle personnalisé :

   Notez que vous pouvez créer un rôle personnalisé Azure à l'aide du portail Azure, d'Azure PowerShell, de l'interface de ligne de commandes Azure ou de l'API REST. La procédure suivante explique comment créer le rôle à l'aide de l'interface de ligne de commandes Azure. Si vous préférez utiliser une autre méthode, reportez-vous à la section "Documentation Azure"

   a. Copier le contenu du "Autorisations de rôle personnalisées pour le connecteur" Et les enregistrer dans un fichier JSON.
   b. Modifiez le fichier JSON en ajoutant des identifiants d'abonnement Azure à l'étendue assignable.

      Vous devez ajouter l'ID de chaque abonnement Azure à partir duquel les utilisateurs créeront des systèmes Cloud Volumes ONTAP.

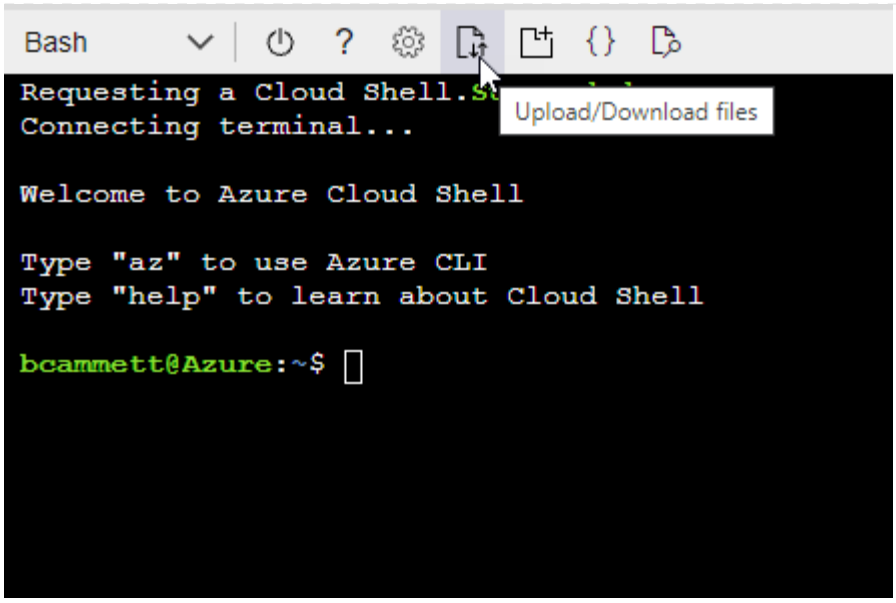
      Exemple

      ```
      "AssignableScopes": [
      "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
      "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
      "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
      ```

   c. Utilisez le fichier JSON pour créer un rôle personnalisé dans Azure.

      Les étapes suivantes expliquent comment créer le rôle à l'aide de Bash dans Azure Cloud Shell.

      - Démarrer "Shell cloud Azure" Et choisissez l'environnement Bash.
      - Téléchargez le fichier JSON.



- Pour créer le rôle personnalisé, utilisez l'interface de ligne de commandes Azure :

```
az role definition create --role-definition
Connector_Policy.json
```

Vous devez maintenant avoir un rôle personnalisé appelé opérateur BlueXP que vous pouvez affecter à la machine virtuelle connecteur.

2. Attribuez l'application au rôle :

   a. À partir du portail Azure, ouvrez le service **abonnements**.

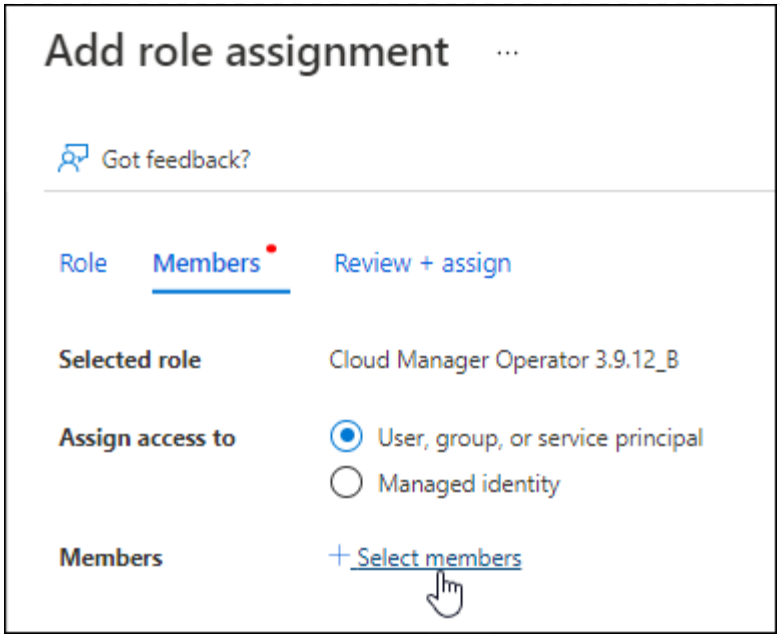
   b. Sélectionnez l'abonnement.

   c. Sélectionnez **contrôle d'accès (IAM) > Ajouter > Ajouter une affectation de rôle**.

   d. Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et sélectionnez **Next**.

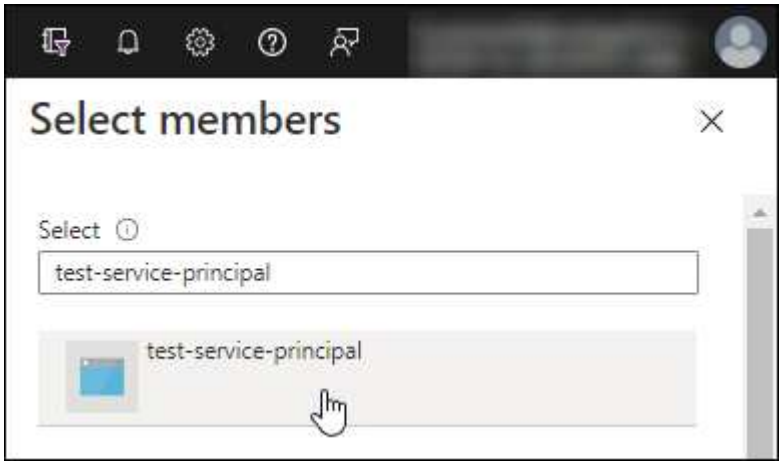
   e. Dans l'onglet **membres**, procédez comme suit :

      - Conserver **utilisateur, groupe ou entité de service** sélectionnée.
      - Sélectionnez **Sélectionner membres**.



- Recherchez le nom de l'application.

  Voici un exemple :



- Sélectionnez l'application et sélectionnez **Sélectionner**.
- Sélectionnez **Suivant**.

f. Sélectionnez **consulter + affecter**.

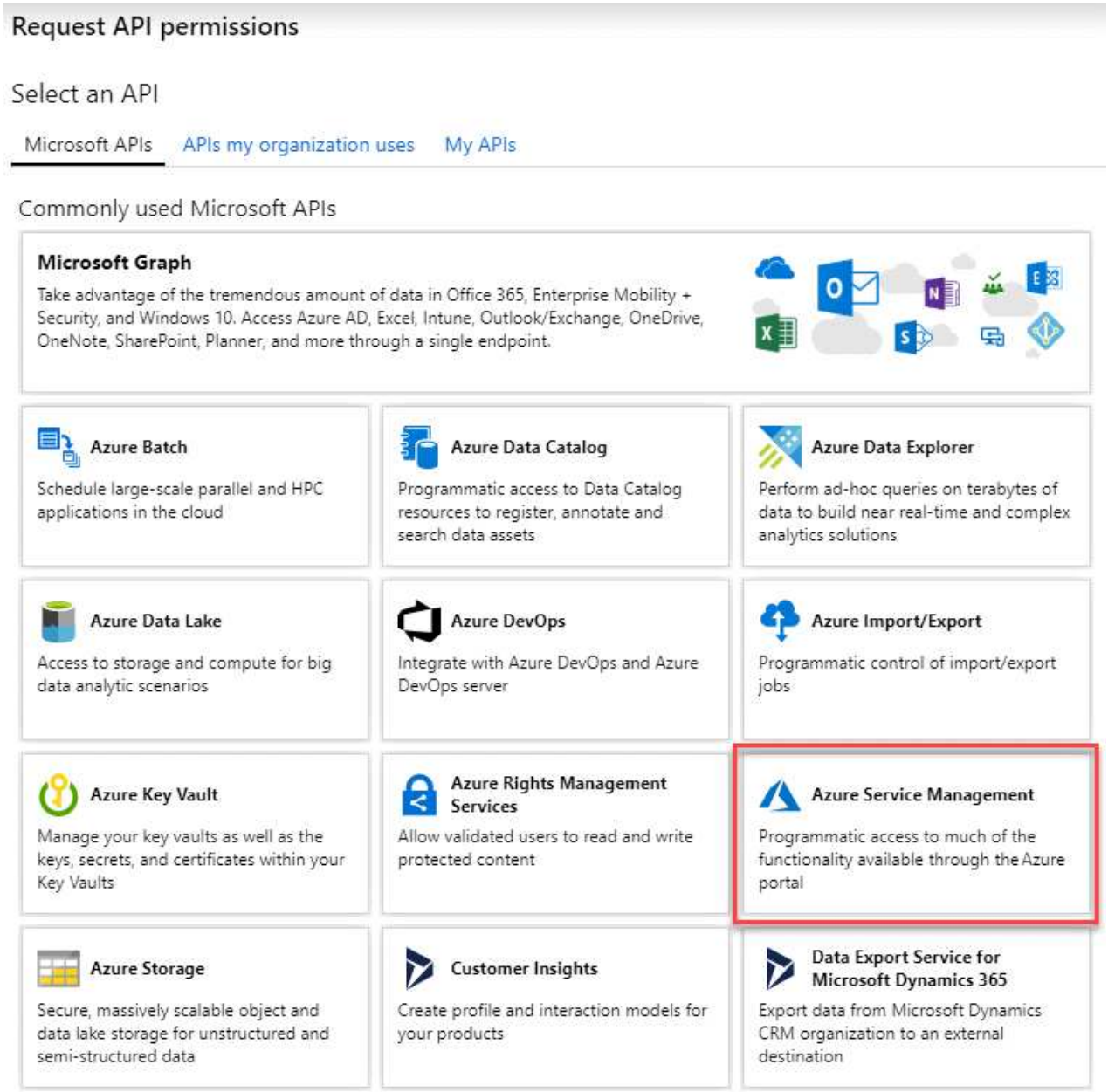
   Le principal de service dispose désormais des autorisations Azure nécessaires pour déployer le connecteur.

Si vous souhaitez déployer Cloud Volumes ONTAP à partir de plusieurs abonnements Azure, vous devez lier le principal de service à chacun de ces abonnements. BlueXP vous permet de sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

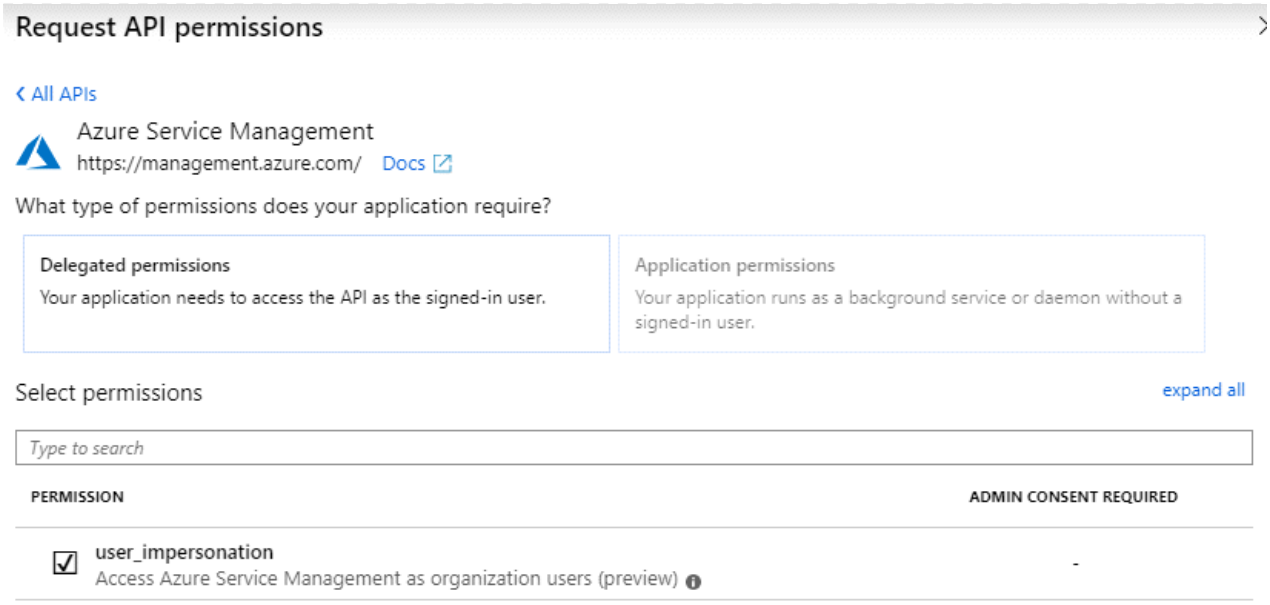
Ajoutez des autorisations d'API de gestion de service Windows Azure

1. Dans le service **Microsoft Entra ID**, sélectionnez **enregistrements d'applications** et sélectionnez l'application.
2. Sélectionnez **autorisations API > Ajouter une autorisation**.

3. Sous **Microsoft API**, sélectionnez **Azure Service Management**.

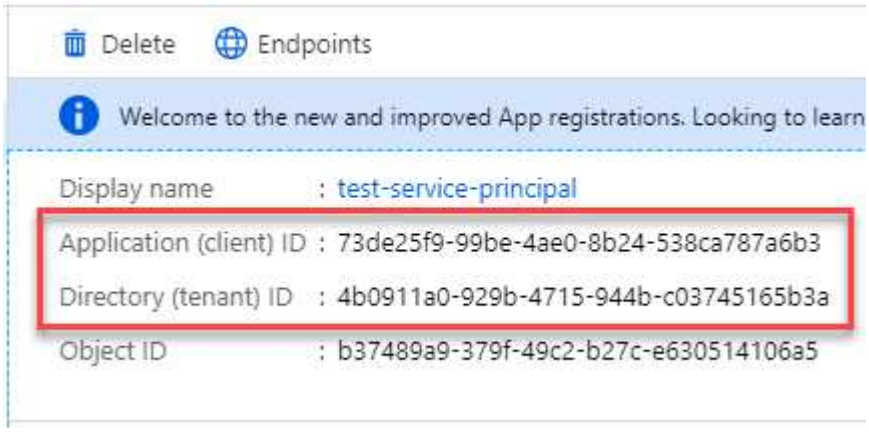


4. Sélectionnez **accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



Obtenez l'ID d'application et l'ID de répertoire de l'application

1. Dans le service **Microsoft Entra ID**, sélectionnez **enregistrements d'applications** et sélectionnez l'application.
2. Copiez l'ID **application (client)** et l'ID **Directory (tenant)**.



Lorsque vous ajoutez le compte Azure à BlueXP, vous devez fournir l'ID d'application (client) et l'ID de répertoire (tenant) de l'application. BlueXP utilise les ID pour se connecter par programmation.

Créez un secret client

1. Ouvrez le service **Microsoft Entra ID**.
2. Sélectionnez **enregistrements d'applications** et sélectionnez votre application.
3. Sélectionnez **certificats et secrets > Nouveau secret client**.
4. Fournissez une description du secret et une durée.
5. Sélectionnez **Ajouter**.
6. Copier la valeur du secret client.

BlueXP peut maintenant utiliser un code client pour s'authentifier auprès de Microsoft Entra ID.

Résultat

Votre principal de service est maintenant configuré et vous devez avoir copié l'ID de l'application (client), l'ID du répertoire (tenant) et la valeur du secret client. Vous devez saisir ces informations dans BlueXP lorsque vous ajoutez un compte Azure.

Compte de service Google Cloud

Créez un rôle et appliquez-le à un compte de service que vous utiliserez pour l'instance de la machine virtuelle Connector.

Étapes

1. Créez un rôle personnalisé dans Google Cloud :

   a. Créez un fichier YAML qui inclut les autorisations définies dans le "Règle de connecteur pour Google Cloud".

   b. Dans Google Cloud, activez le shell cloud.

   c. Téléchargez le fichier YAML qui inclut les autorisations requises pour le connecteur.

   d. Créez un rôle personnalisé à l'aide de `gcloud iam roles create` commande.

      L'exemple suivant crée un rôle nommé « connecteur » au niveau du projet :

```
gcloud iam roles create connector --project=myproject
--file=connector.yaml
```

   +
   "Documents Google Cloud : création et gestion de rôles personnalisés"

2. Créez un compte de service dans Google Cloud :

   a. Dans le service IAM & Admin, sélectionnez **comptes de service > Créer un compte de service**.

   b. Entrez les détails du compte de service et sélectionnez **Créer et continuer**.

   c. Sélectionnez le rôle que vous venez de créer.

   d. Terminez les étapes restantes pour créer le rôle.

      "Documents Google Cloud : création d'un compte de service"

Résultat

Vous disposez désormais d'un compte de service que vous pouvez attribuer à l'instance VM Connector.

Étape 6 : activez les API Google Cloud

Plusieurs API sont requises pour déployer Cloud Volumes ONTAP dans Google Cloud.

Étape

1. "Activez les API Google Cloud suivantes dans votre projet"
    - API Cloud Deployment Manager V2
    - API de journalisation cloud
    - API Cloud Resource Manager
    - API du moteur de calcul
    - API de gestion des identités et des accès
    - API KMS (Cloud Key Management Service

      (Requis uniquement si vous prévoyez d'utiliser la sauvegarde et la restauration BlueXP avec des clés de chiffrement gérées par le client (CMEK))

Déployez le connecteur en mode restreint

Déployez le connecteur en mode restreint pour utiliser BlueXP avec une connectivité sortante limitée vers la couche SaaS BlueXP. Pour commencer, installez le connecteur, configurez BlueXP en accédant à l'interface utilisateur exécutée sur le connecteur, puis fournissez les autorisations cloud que vous avez précédemment configurées.

Étape 1 : installez le connecteur

Installez le connecteur à partir du Marketplace de votre fournisseur de cloud ou en installant manuellement le logiciel sur votre propre hôte Linux.

AWS commercial Marketplace

Avant de commencer

Vous devez disposer des éléments suivants :

- VPC et sous-réseau qui répondent aux exigences réseau.

  "En savoir plus sur les exigences de mise en réseau"

- Un rôle IAM avec une stratégie jointe qui inclut les autorisations requises pour le connecteur.

  "Découvrez comment configurer des autorisations AWS"

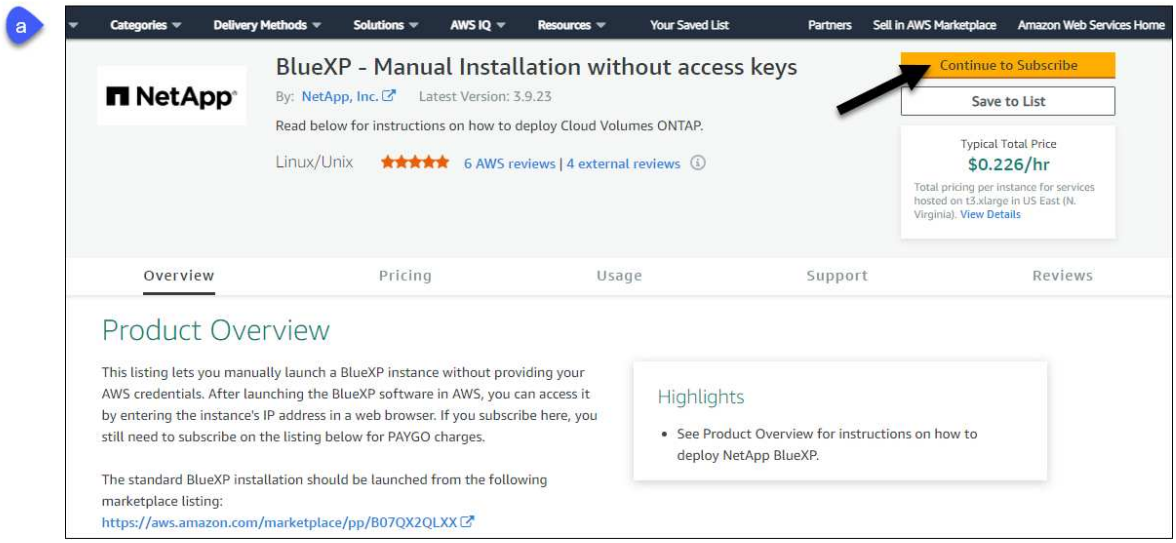
- Autorisations de vous abonner à AWS Marketplace et de vous désabonner pour votre utilisateur IAM.
- Compréhension des exigences en termes de CPU et de RAM pour l'instance.

  "Passez en revue les exigences relatives aux instances".

- Une paire de clés pour l'instance EC2.

Étapes

1. Accédez au "BlueXP, page sur AWS Marketplace"
2. Sur la page Marketplace, sélectionnez **Continuer pour s'abonner**, puis sélectionnez **Continuer à la configuration**.



3. Modifiez l'une des options par défaut et sélectionnez **Continuer pour lancer**.
4. Sous **Choisissez action**, sélectionnez **lancer via EC2**, puis **lancer**.

   Ces étapes décrivent comment lancer l'instance à partir de la console EC2, car la console vous permet d'associer un rôle IAM à l'instance de connecteur. Cela n'est pas possible en utilisant l'action **lancer à partir du site Web**.

5. Suivez les invites pour configurer et déployer l'instance :

   - **Nom et balises** : saisissez un nom et des balises pour l'instance.
   - **Image de l'application et de l'OS** : passez cette section. Le connecteur ami est déjà sélectionné.
   - **Type d'instance** : en fonction de la disponibilité de la région, choisissez un type d'instance qui répond aux exigences de RAM et de CPU (t3.xlarge est recommandé).
   - **Paire de clés (login)** : sélectionnez la paire de clés que vous souhaitez utiliser pour vous connecter en toute sécurité à l'instance.
   - **Paramètres réseau** : modifiez les paramètres réseau selon vos besoins :
     - Choisissez le VPC et le sous-réseau souhaités.
     - Spécifiez si l'instance doit avoir une adresse IP publique.
     - Spécifiez les paramètres de pare-feu qui activent les méthodes de connexion requises pour l'instance de connecteur : SSH, HTTP et HTTPS.

       Quelques règles supplémentaires sont requises pour des configurations spécifiques.

   "Afficher les règles des groupes de sécurité pour AWS".

   - **Configurer le stockage** : conservez la taille et le type de disque par défaut pour le volume racine.

     Si vous souhaitez activer le chiffrement Amazon EBS sur le volume racine, sélectionnez **Avancé**, développez **Volume 1**, sélectionnez **crypté**, puis choisissez une clé KMS.

   - **Détails avancés** : sous **profil d'instance IAM**, choisissez le rôle IAM qui inclut les autorisations requises pour le connecteur.
   - **Résumé** : passez en revue le résumé et sélectionnez **lancer l'instance**.

Résultat

AWS lance le logiciel avec les paramètres spécifiés. L'instance de connecteur et le logiciel doivent s'exécuter dans environ cinq minutes.

Et la suite ?

Configurez BlueXP.

AWS Gov Marketplace

Avant de commencer

Vous devez disposer des éléments suivants :

- VPC et sous-réseau qui répondent aux exigences réseau.

  "En savoir plus sur les exigences de mise en réseau"

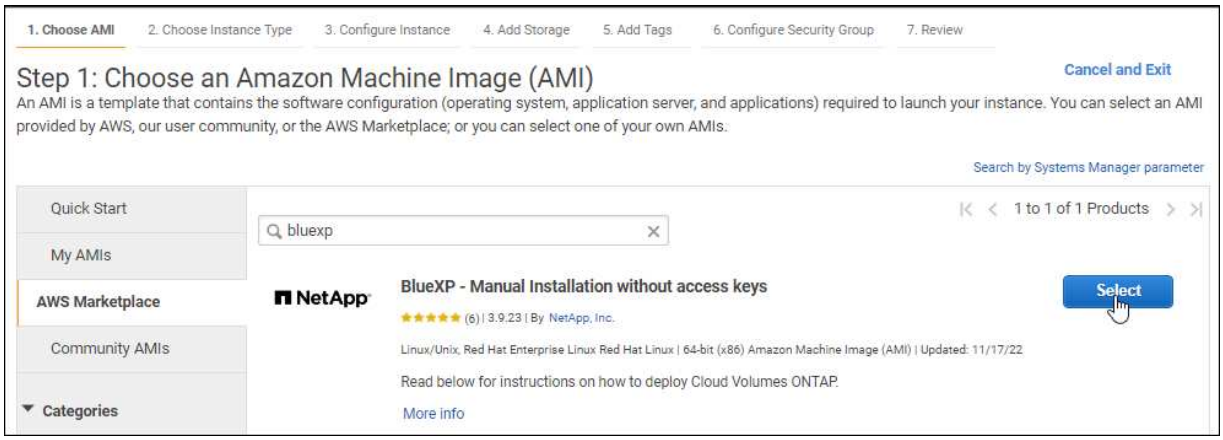
- Un rôle IAM avec une stratégie jointe qui inclut les autorisations requises pour le connecteur.

  "Découvrez comment configurer des autorisations AWS"

- Autorisations de vous abonner à AWS Marketplace et de vous désabonner pour votre utilisateur IAM.
- Une paire de clés pour l'instance EC2.

Étapes

1. Accédez à l'offre BlueXP sur AWS Marketplace.
   a. Ouvrez le service EC2 et sélectionnez **lancer l'instance**.
   b. Sélectionnez **AWS Marketplace**.
   c. Recherchez BlueXP et sélectionnez l'offre.

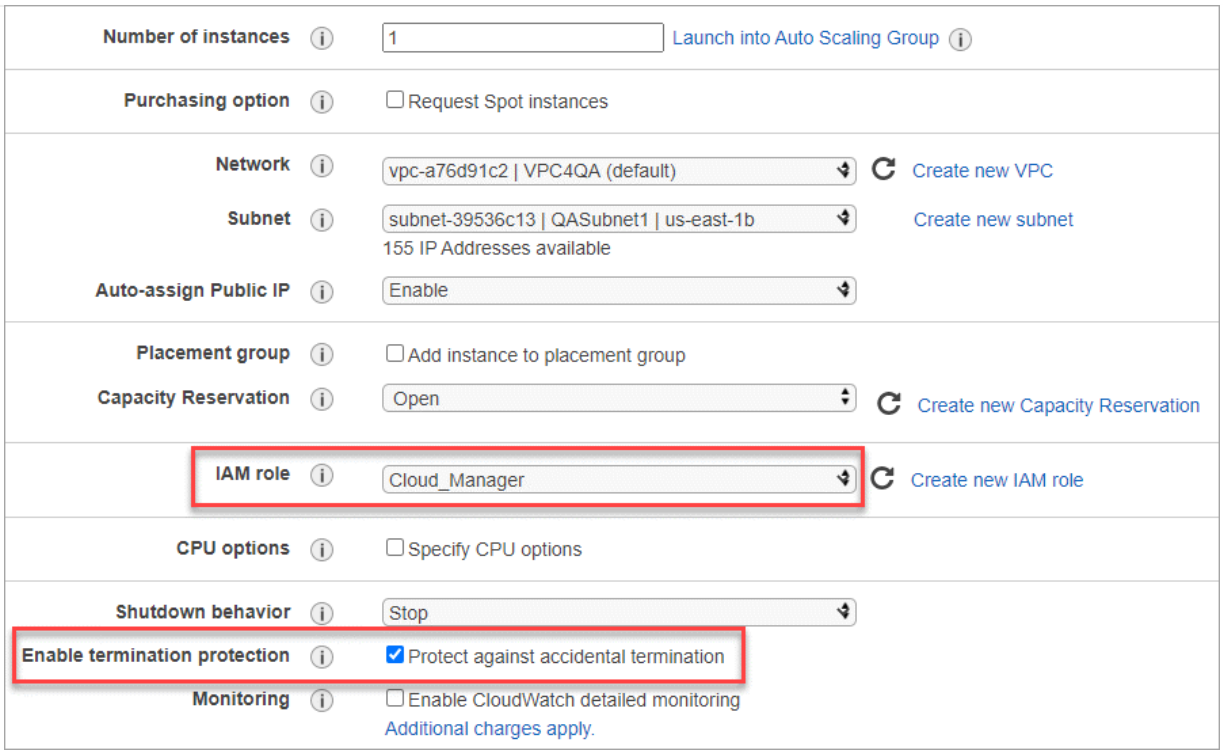


   d. Sélectionnez **Continuer**.

2. Suivez les invites pour configurer et déployer l'instance :
   - **Choisissez un type d'instance** : selon la disponibilité de la région, choisissez un des types d'instance pris en charge (t3.XLarge est recommandé).

     "Vérifiez les conditions requises pour l'instance".

   - **Configurer les détails de l'instance** : sélectionnez un VPC et un sous-réseau, choisissez le rôle IAM que vous avez créé à l'étape 1, activez la protection de terminaison (recommandée) et choisissez toutes les autres options de configuration qui répondent à vos exigences.



- **Ajouter stockage** : conservez les options de stockage par défaut.
- **Ajouter des balises** : saisissez des balises pour l'instance, si vous le souhaitez.
- **Configurer le groupe de sécurité** : spécifiez les méthodes de connexion requises pour l'instance de connecteur : SSH, HTTP et HTTPS.
- **Revoir** : passez en revue vos sélections et sélectionnez **lancer**.

Résultat

AWS lance le logiciel avec les paramètres spécifiés. L'instance de connecteur et le logiciel doivent s'exécuter dans environ cinq minutes.

Et la suite ?

Configurez BlueXP.

Azure Marketplace

Avant de commencer

Vous devez disposer des éléments suivants :

- Vnet et sous-réseau répondant aux exigences de mise en réseau.

  "En savoir plus sur les exigences de mise en réseau"

- Rôle personnalisé Azure qui inclut les autorisations requises pour le connecteur.

  "Découvrez comment configurer des autorisations Azure"

Étapes

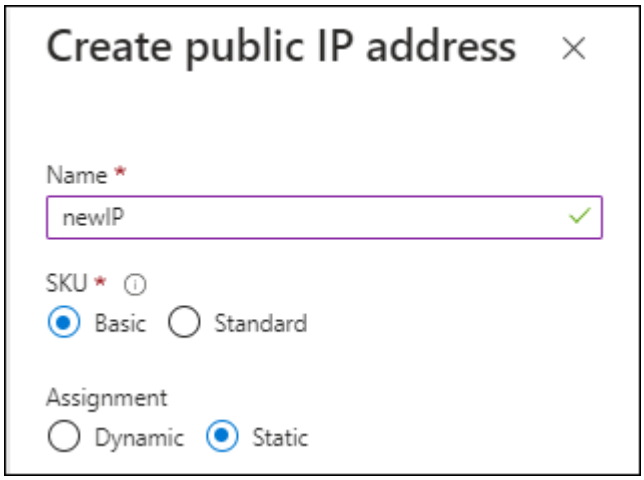
1. Rendez-vous sur la page NetApp Connector VM du Marketplace Azure.
   - "Page Azure Marketplace pour les régions commerciales"

- "Page Azure Marketplace pour les régions Azure Government"

2. Sélectionnez **obtenir maintenant**, puis **Continuer**.
3. Dans le portail Azure, sélectionnez **Create** et suivez les étapes pour configurer la machine virtuelle.

   Noter les éléments suivants lors de la configuration de la machine virtuelle :

   - **Taille de la VM** : choisissez une taille de VM qui répond aux exigences de CPU et de RAM. Nous recommandons DS3 v2.
   - **Disques** : le connecteur peut fonctionner de manière optimale avec des disques durs ou SSD.
   - **Public IP** : si vous souhaitez utiliser une adresse IP publique avec la machine virtuelle du connecteur, l'adresse IP doit utiliser une référence SKU de base pour garantir que BlueXP utilise cette adresse IP publique.



     Si vous utilisez une adresse IP de référence standard, BlueXP utilise l'adresse IP *private* du connecteur, au lieu de l'adresse IP publique. Si la machine que vous utilisez pour accéder à la console BlueXP n'a pas accès à cette adresse IP privée, les actions de la console BlueXP échouent.

   "Documentation Azure : référence IP publique"

   - **Groupe de sécurité réseau** : le connecteur nécessite des connexions entrantes utilisant SSH, HTTP et HTTPS.

     "Afficher les règles des groupes de sécurité pour Azure".

   - **Identité** : sous **gestion**, sélectionnez **Activer l'identité gérée attribuée par le système**.

     Ce paramètre est important car une identité gérée permet à la machine virtuelle Connector de s'identifier à Microsoft Entra ID sans fournir d'informations d'identification. "En savoir plus sur les identités gérées pour les ressources Azure".

4. Sur la page **consulter + créer**, vérifiez vos sélections et sélectionnez **Créer** pour démarrer le déploiement.

Résultat

Azure déploie la machine virtuelle avec les paramètres spécifiés. Le logiciel de la machine virtuelle et du connecteur doit s'exécuter en cinq minutes environ.

Et la suite ?

Configurez BlueXP.

Installation manuelle

Avant de commencer

Vous devez disposer des éléments suivants :

- Privilèges root pour installer le connecteur.
- Détails sur un serveur proxy, si un proxy est requis pour accéder à Internet à partir du connecteur.

  Vous avez la possibilité de configurer un serveur proxy après l'installation, mais cela nécessite de redémarrer le connecteur.

  Notez que BlueXP ne prend pas en charge les serveurs proxy transparents.

- Un certificat signé par une autorité de certification, si le serveur proxy utilise HTTPS ou si le proxy est un proxy interceptant.

Description de la tâche

Le programme d'installation disponible sur le site du support NetApp peut être une version antérieure. Après l'installation, le connecteur se met automatiquement à jour si une nouvelle version est disponible.

Étapes

1. Vérifiez que docker est activé et exécuté.

   ```
   sudo systemctl enable docker && sudo systemctl start docker
   ```

2. Si les variables système *http_proxy* ou *https_proxy* sont définies sur l'hôte, supprimez-les :

   ```
   unset http_proxy
   unset https_proxy
   ```

   Si vous ne supprimez pas ces variables système, l'installation échouera.

3. Téléchargez le logiciel du connecteur à partir du "Site de support NetApp", Puis copiez-le sur l'hôte Linux.

   Vous devez télécharger le programme d'installation du connecteur « en ligne » destiné à être utilisé sur votre réseau ou dans le cloud. Un programme d'installation séparé « hors ligne » est disponible pour le connecteur, mais il n'est pris en charge que pour les déploiements en mode privé.

4. Attribuez des autorisations pour exécuter le script.

   ```
   chmod +x BlueXP-Connector-Cloud-<version>
   ```

   Où <version> est la version du connecteur que vous avez téléchargé.

5. Exécutez le script d'installation.

```
./BlueXP-Connector-Cloud-<version> --proxy <HTTP or HTTPS proxy
server> --cacert <path and file name of a CA-signed certificate>
```

Les paramètres --proxy et --cacert sont facultatifs. Si vous disposez d'un serveur proxy, vous devez entrer les paramètres comme indiqué. Le programme d'installation ne vous invite pas à fournir des informations sur un proxy.

Voici un exemple de commande utilisant les deux paramètres facultatifs :

```
./BlueXP-Connector-Cloud-v3.9.38 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

--proxy configure le connecteur pour utiliser un serveur proxy HTTP ou HTTPS à l'aide de l'un des formats suivants :

- http://address:port
- http://user-name:password@address:port
- http://domain-name%92user-name:password@address:port
- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

  Notez ce qui suit :

  - L'utilisateur peut être un utilisateur local ou un utilisateur de domaine.
  - Pour un utilisateur de domaine, vous devez utiliser le code ASCII du \ comme indiqué ci-dessus.
  - BlueXP ne prend pas en charge les mots de passe comprenant le caractère @.

--cacert spécifie un certificat signé par une autorité de certification à utiliser pour l'accès HTTPS entre le connecteur et le serveur proxy. Ce paramètre est requis uniquement si vous spécifiez un serveur proxy HTTPS ou si le proxy est un proxy interceptant.

Résultat

Le connecteur est maintenant installé. À la fin de l'installation, le service connecteur (ocm) redémarre deux fois si vous avez spécifié un serveur proxy.

Et la suite ?

Configurez BlueXP.

Étape 2 : configuration de BlueXP

Lorsque vous accédez pour la première fois à la console BlueXP, vous êtes invité à choisir un compte auquel associer le connecteur et vous devez activer le mode restreint.

Si vous avez déjà un compte et que vous souhaitez en créer un autre, vous devez utiliser l'API de location. "Découvrez comment créer un compte BlueXP supplémentaire".

Étapes

1. Ouvrez un navigateur Web à partir d'un hôte connecté à l'instance Connector et saisissez l'URL suivante :

   https://ipaddress

2. Inscrivez-vous ou connectez-vous à BlueXP.
3. Une fois connecté, configurez BlueXP :

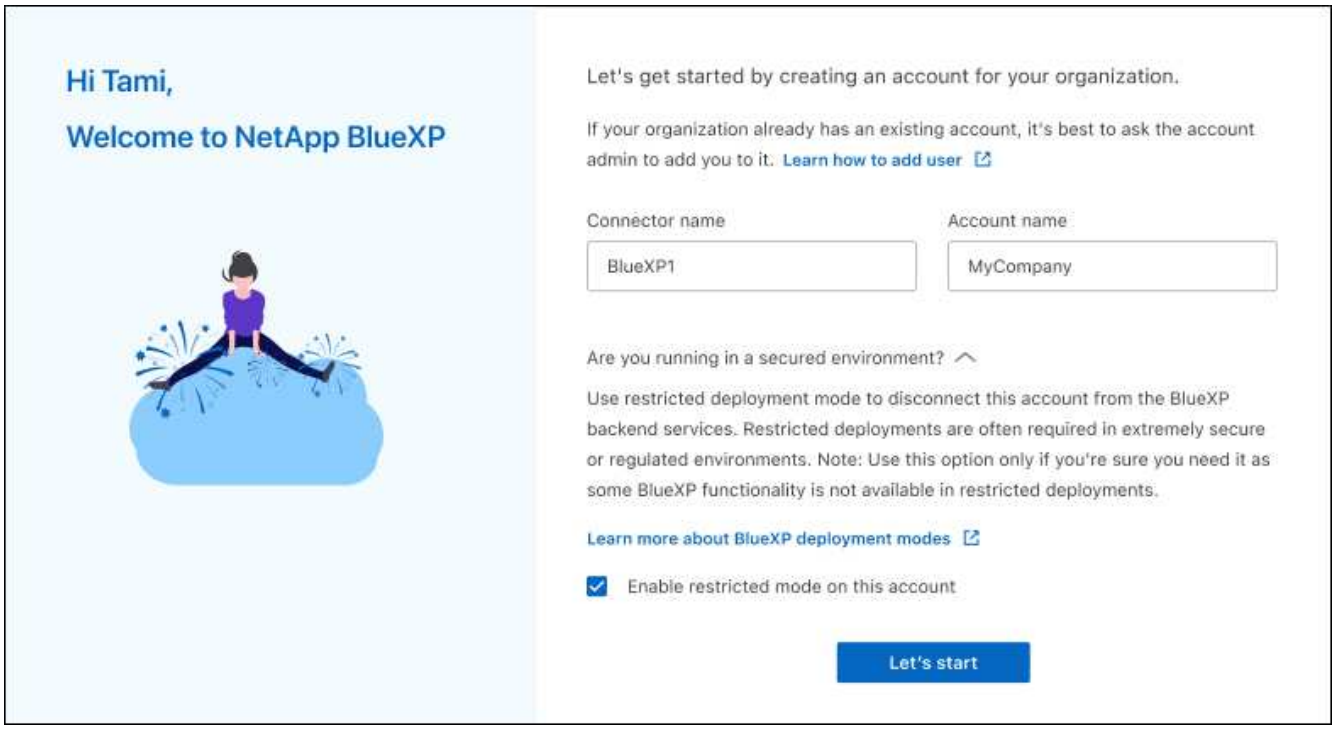
   a. Entrez un nom pour le connecteur.
   b. Entrez le nom d'un nouveau compte BlueXP ou sélectionnez un compte existant.

      Vous pouvez sélectionner un compte existant si votre connexion est déjà associée à un compte BlueXP.

   c. Sélectionnez **exécutez-vous dans un environnement sécurisé ?**
   d. Sélectionnez **Activer le mode restreint sur ce compte**.

      Notez que vous ne pouvez pas modifier ce paramètre après la création du compte par BlueXP. Vous ne pouvez pas activer le mode restreint ultérieurement et vous ne pouvez pas le désactiver ultérieurement.

      Si vous avez déployé le connecteur dans une région gouvernementale, la case à cocher est déjà activée et ne peut pas être modifiée. En effet, le mode restreint est le seul mode pris en charge dans les régions gouvernementales.



   a. Sélectionnez **commençons**.

Résultat

Le connecteur est maintenant installé et configuré avec votre compte BlueXP. Tous les utilisateurs doivent accéder à BlueXP via l'adresse IP de l'instance de connecteur.

Et la suite ?

Fournissez à BlueXP les autorisations que vous avez précédemment configurées.

Étape 3 : fournissez des autorisations à BlueXP

Si vous avez déployé le connecteur à partir d'Azure Marketplace ou si vous avez installé manuellement le logiciel Connector, vous devez fournir les autorisations que vous avez précédemment configurées pour vous permettre d'utiliser les services BlueXP.

Ces étapes ne s'appliquent pas si vous avez déployé Connector à partir d'AWS Marketplace, car vous avez choisi le rôle IAM requis pendant le déploiement.

"Découvrez comment préparer les autorisations cloud".

Rôle IAM AWS

Reliez le rôle IAM que vous avez créé précédemment à l'instance EC2 sur laquelle vous avez installé le connecteur.

Ces étapes s'appliquent uniquement si vous avez installé manuellement le connecteur dans AWS. Pour les déploiements AWS Marketplace, vous avez déjà associé l'instance Connector à un rôle IAM qui inclut les autorisations requises.

Étapes

1. Accédez à la console Amazon EC2.
2. Sélectionnez **instances**.
3. Sélectionnez l'instance de connecteur.
4. Sélectionnez **actions > sécurité > Modifier le rôle IAM**.
5. Sélectionnez le rôle IAM et sélectionnez **mettre à jour le rôle IAM**.

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans AWS en votre nom.

Clé d'accès AWS

Fournissez à BlueXP la clé d'accès AWS pour un utilisateur IAM qui dispose des autorisations requises.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône Paramètres, puis sélectionnez **informations d'identification**.

2. Sélectionnez **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
   a. **Emplacement des informations d'identification** : sélectionnez **Amazon Web Services > connecteur**.
   b. **Définir les informations d'identification** : saisissez une clé d'accès AWS et une clé secrète.
   c. **Abonnement Marketplace** : associez un abonnement Marketplace à ces identifiants en vous abonnant maintenant ou en sélectionnant un abonnement existant.
   d. **Révision** : confirmez les détails des nouvelles informations d'identification et sélectionnez **Ajouter**.

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans AWS en votre nom.

Rôle d'Azure

Accédez au portail Azure et attribuez le rôle personnalisé Azure à la machine virtuelle Connector pour un ou plusieurs abonnements.

Étapes

1. Sur le portail Azure, ouvrez le service **Subscriptions** et sélectionnez votre abonnement.

   Il est important d'attribuer le rôle à partir du service **Subscriptions** car cela spécifie la portée de l'affectation de rôle au niveau de l'abonnement. Le *scope* définit l'ensemble des ressources auxquelles l'accès s'applique. Si vous spécifiez une étendue à un niveau différent (par exemple, au niveau des machines virtuelles), votre capacité à effectuer des actions depuis BlueXP sera affectée.

   "Documentation Microsoft Azure : étendue du contrôle d'accès basé sur des rôles Azure"

2. Sélectionnez **contrôle d'accès (IAM)** > **Ajouter** > **Ajouter une affectation de rôle**.
3. Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et sélectionnez **Next**.

   BlueXP Operator est le nom par défaut fourni dans la stratégie BlueXP. Si vous avez choisi un autre nom pour le rôle, sélectionnez-le à la place.

4. Dans l'onglet **membres**, procédez comme suit :
   a. Attribuez l'accès à une identité **gérée**.
   b. Sélectionnez **Sélectionner les membres**, sélectionnez l'abonnement dans lequel la machine virtuelle du connecteur a été créée, sous **identité gérée**, choisissez **machine virtuelle**, puis sélectionnez la machine virtuelle du connecteur.
   c. Sélectionnez **Sélectionner**.
   d. Sélectionnez **Suivant**.
   e. Sélectionnez **consulter + affecter**.
   f. Si vous souhaitez gérer les ressources d'autres abonnements Azure, passez à cet abonnement, puis répétez ces étapes.

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans Azure en votre nom.

Principal de service Azure

Fournissez à BlueXP les informations d'identification du principal de service Azure que vous avez précédemment configuré.

Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône Paramètres, puis sélectionnez **informations d'identification**.

2. Sélectionnez **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
   a. **Emplacement des informations d'identification** : sélectionnez **Microsoft Azure > connecteur**.
   b. **Définir les informations d'identification** : saisissez les informations relatives à l'entité de service Microsoft Entra qui accorde les autorisations requises :
      - ID de l'application (client)

    - ID du répertoire (locataire)
    - Secret client

c. **Abonnement Marketplace** : associez un abonnement Marketplace à ces identifiants en vous abonnant maintenant ou en sélectionnant un abonnement existant.

d. **Révision** : confirmez les détails des nouvelles informations d'identification et sélectionnez **Ajouter**.

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions dans Azure en votre nom.

Compte de service Google Cloud

Associez le compte de service à la VM Connector.

Étapes

1. Accédez au portail Google Cloud et attribuez le compte de service à l'instance de la VM Connector.

   "Documentation Google Cloud : modification du compte de service et des étendues d'accès pour une instance"

2. Si vous souhaitez gérer des ressources dans d'autres projets, accordez l'accès en ajoutant le compte de service doté du rôle BlueXP à ce projet. Vous devrez répéter cette étape pour chaque projet.

Résultat

BlueXP dispose désormais des autorisations dont il a besoin pour effectuer des actions en votre nom dans Google Cloud.

Abonnement à BlueXP (mode restreint)

Abonnez-vous à BlueXP sur le marché de votre fournisseur cloud pour payer les services BlueXP à un taux horaire (PAYGO) ou un contrat annuel. Si vous avez acheté une licence NetApp (BYOL), vous devez également souscrire à l'offre Marketplace. Votre licence est toujours facturée en premier, mais vous serez facturé au taux horaire si vous dépassez votre capacité sous licence ou si la période de validité de la licence expire.

Un abonnement Marketplace permet de facturer les services BlueXP suivants en mode restreint :

- Sauvegarde et restauration
- Classement
- Cloud Volumes ONTAP

Avant de commencer

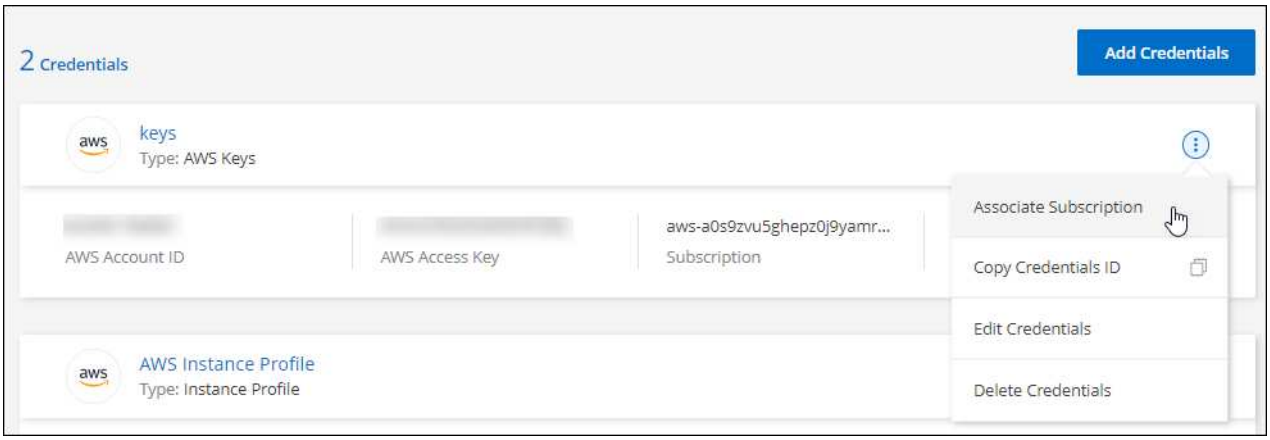
L'abonnement à BlueXP implique d'associer un abonnement Marketplace aux informations d'identification cloud associées à un connecteur. Si vous avez suivi le flux de travail « commencer avec le mode restreint », vous devriez déjà avoir un connecteur. Pour en savoir plus, consultez le "Démarrage rapide de BlueXP en mode restreint".

AWS

Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône Paramètres, puis sélectionnez **informations d'identification**.
2. Sélectionnez le menu d'action correspondant à un ensemble d'informations d'identification, puis sélectionnez **abonnement associé**.

   Vous devez sélectionner les informations d'identification associées à un connecteur. Vous ne pouvez pas associer un abonnement Marketplace aux informations d'identification associées à BlueXP.



3. Pour associer les informations d'identification à un abonnement existant, sélectionnez l'abonnement dans la liste déroulante et sélectionnez **associer**.
4. Pour associer les informations d'identification à un nouvel abonnement, sélectionnez **Ajouter un abonnement > Continuer** et suivez les étapes indiquées dans AWS Marketplace :

   a. Sélectionnez **Afficher les options d'achat**.

   b. Sélectionnez **s'abonner**.

   c. Sélectionnez **configurer votre compte**.

      Vous serez redirigé vers le site Web BlueXP.

   d. À partir de la page **attribution d'abonnement** :

      - Sélectionnez les comptes BlueXP avec lesquels vous souhaitez associer cet abonnement.
      - Dans le champ **remplacer l'abonnement existant**, choisissez si vous souhaitez remplacer automatiquement l'abonnement existant pour un compte par ce nouvel abonnement.

        BlueXP remplace l'abonnement existant pour toutes les informations d'identification du compte par ce nouvel abonnement. Si un ensemble d'informations d'identification n'a jamais été associé à un abonnement, ce nouvel abonnement ne sera pas associé à ces informations d'identification.

      Pour tous les autres comptes, vous devez associer manuellement l'abonnement en répétant ces étapes.

      - Sélectionnez **Enregistrer**.

        La vidéo suivante décrit la procédure de souscription à partir d'AWS Marketplace :

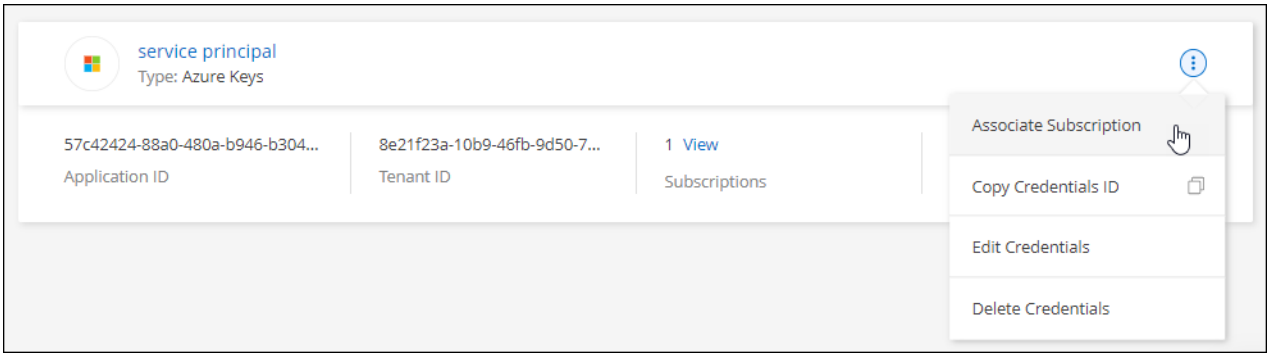
Abonnez-vous à BlueXP sur AWS Marketplace

Azure

Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône Paramètres, puis sélectionnez **informations d'identification**.
2. Sélectionnez le menu d'action correspondant à un ensemble d'informations d'identification, puis sélectionnez **abonnement associé**.

   Vous devez sélectionner les informations d'identification associées à un connecteur. Vous ne pouvez pas associer un abonnement Marketplace aux informations d'identification associées à BlueXP.



3. Pour associer les informations d'identification à un abonnement existant, sélectionnez l'abonnement dans la liste déroulante et sélectionnez **associer**.
4. Pour associer les informations d'identification à un nouvel abonnement, sélectionnez **Ajouter un abonnement > Continuer** et suivez les étapes dans Azure Marketplace :

   a. Si vous y êtes invité, connectez-vous à votre compte Azure.

   b. Sélectionnez **s'abonner**.

   c. Remplissez le formulaire et sélectionnez **s'abonner**.

   d. Une fois le processus d'abonnement terminé, sélectionnez **configurer le compte maintenant**.

      Vous serez redirigé vers le site Web BlueXP.

   e. À partir de la page **attribution d'abonnement** :

      - Sélectionnez les comptes BlueXP avec lesquels vous souhaitez associer cet abonnement.
      - Dans le champ **remplacer l'abonnement existant**, choisissez si vous souhaitez remplacer automatiquement l'abonnement existant pour un compte par ce nouvel abonnement.

        BlueXP remplace l'abonnement existant pour toutes les informations d'identification du compte par ce nouvel abonnement. Si un ensemble d'informations d'identification n'a jamais été associé à un abonnement, ce nouvel abonnement ne sera pas associé à ces informations d'identification.

      Pour tous les autres comptes, vous devez associer manuellement l'abonnement en répétant ces étapes.

      - Sélectionnez **Enregistrer**.

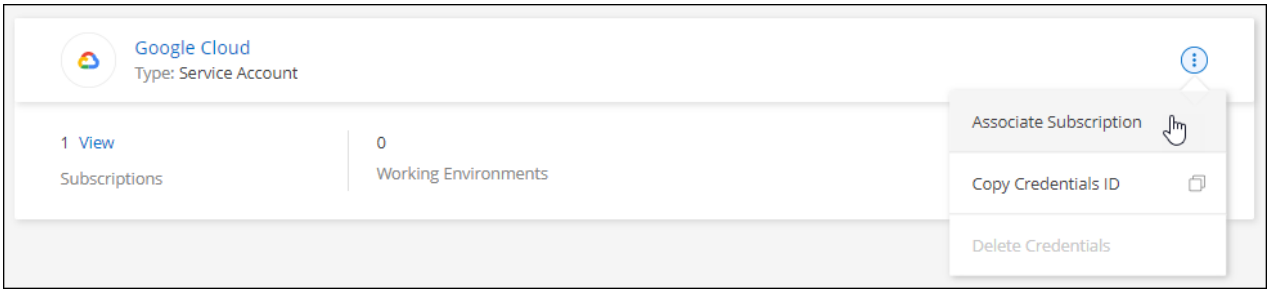
La vidéo suivante explique comment vous abonner à Azure Marketplace :

Abonnez-vous à BlueXP depuis Azure Marketplace

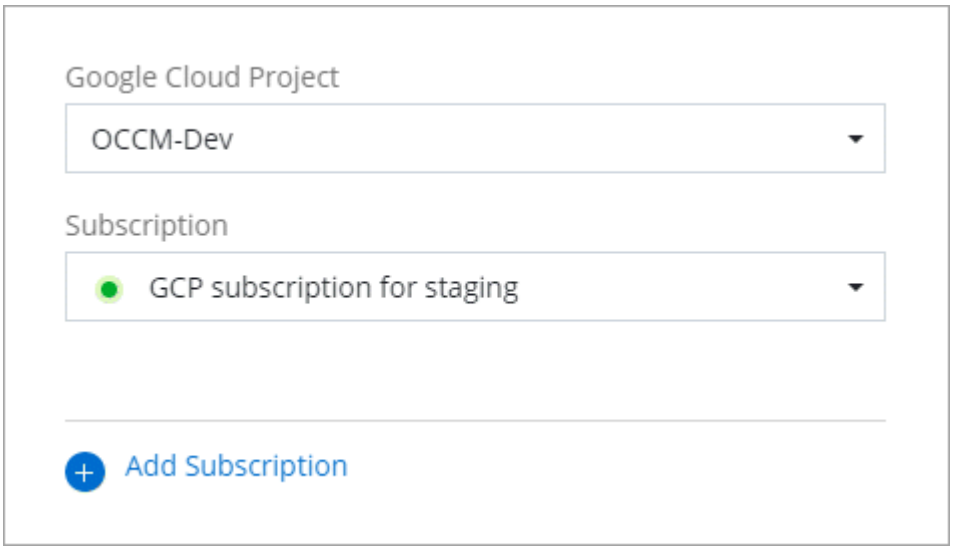
Google Cloud

Étapes

1. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône Paramètres, puis sélectionnez **informations d'identification**.
2. Sélectionnez le menu d'action correspondant à un ensemble d'informations d'identification, puis sélectionnez **abonnement associé**.



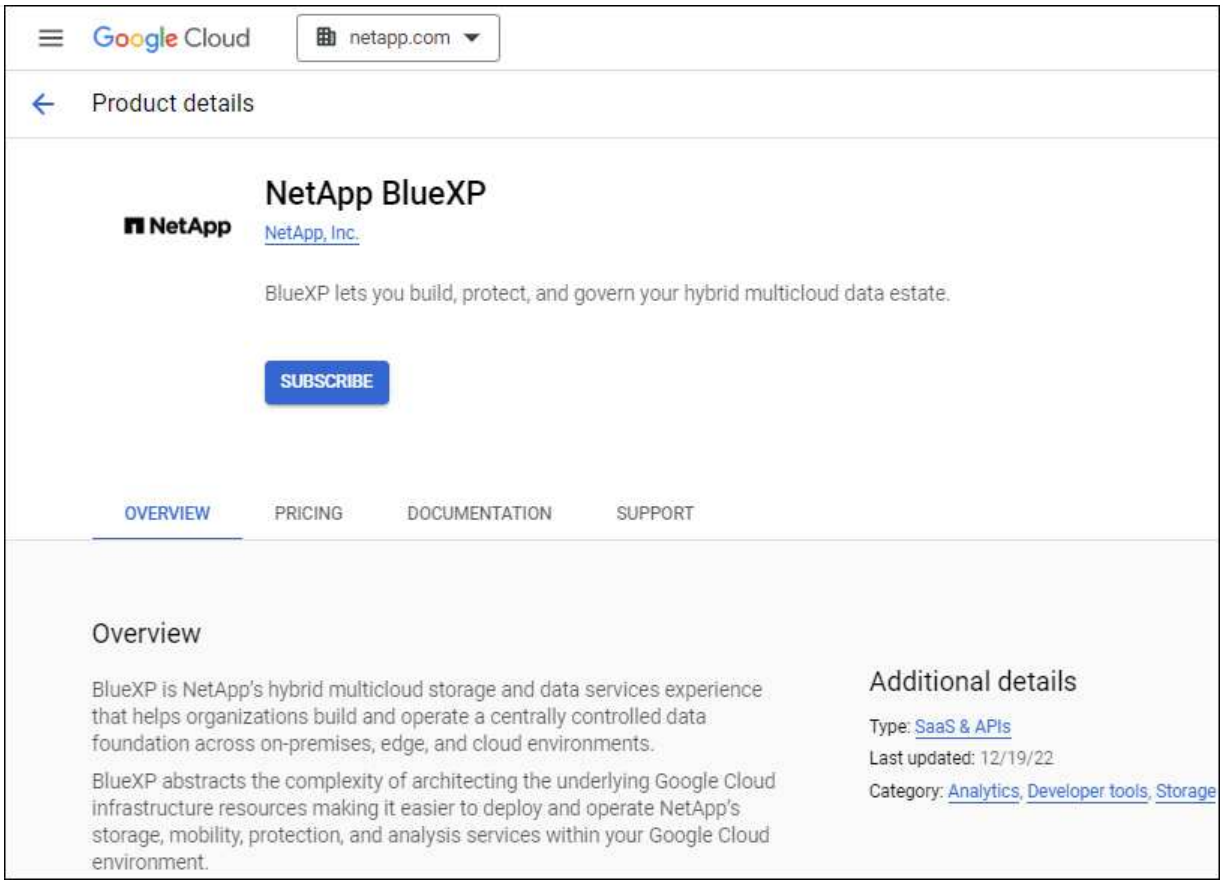
3. Pour associer les informations d'identification à un abonnement existant, sélectionnez un projet Google Cloud et un abonnement dans la liste déroulante, puis sélectionnez **associer**.



4. Si vous n'avez pas encore d'abonnement, sélectionnez **Ajouter un abonnement > Continuer** et suivez les étapes indiquées dans Google Cloud Marketplace.

> Avant de terminer les étapes suivantes, assurez-vous que vous disposez des deux privilèges d'administrateur de facturation dans votre compte Google Cloud ainsi que d'une connexion BlueXP.

   a. Après avoir été redirigé vers le "Page NetApp BlueXP sur Google Cloud Marketplace", assurez-vous que le projet correct est sélectionné dans le menu de navigation supérieur.



b. Sélectionnez **s'abonner**.

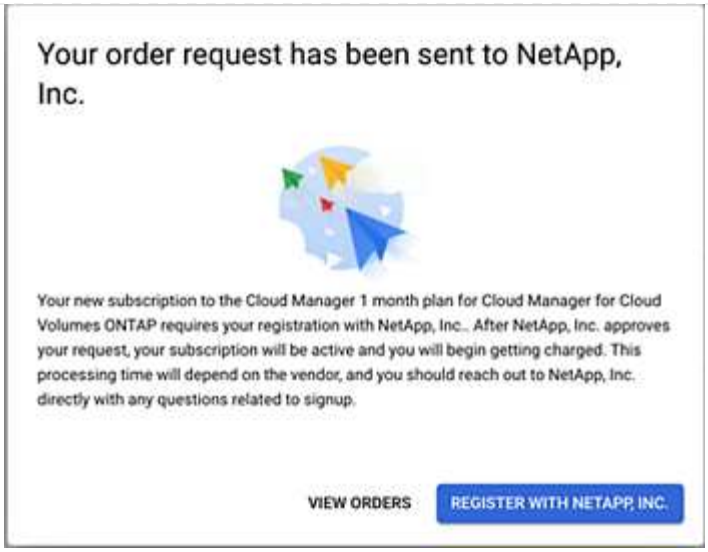
c. Sélectionnez le compte de facturation approprié et acceptez les conditions générales.

d. Sélectionnez **s'abonner**.

   Cette étape envoie votre demande de transfert à NetApp.

e. Dans la boîte de dialogue qui s'affiche, sélectionnez **s'inscrire auprès de NetApp, Inc.**

   Cette étape doit être effectuée pour lier l'abonnement Google Cloud à votre compte BlueXP. Le processus de liaison d'un abonnement n'est pas terminé tant que vous n'êtes pas redirigé à partir de cette page, puis vous connecter à BlueXP.



f. Suivez les étapes de la page **attribution d'abonnement** :

> Si un membre de votre entreprise a déjà souscrit à l'abonnement NetApp BlueXP à partir de votre compte de facturation, vous serez redirigé vers "La page Cloud Volumes ONTAP sur le site web de BlueXP" à la place. Si cela est inattendu, contactez votre équipe commerciale NetApp. Google n'autorise qu'un seul abonnement par compte de facturation Google.

- Sélectionnez les comptes BlueXP avec lesquels vous souhaitez associer cet abonnement.
- Dans le champ **remplacer l'abonnement existant**, choisissez si vous souhaitez remplacer automatiquement l'abonnement existant pour un compte par ce nouvel abonnement.

  BlueXP remplace l'abonnement existant pour toutes les informations d'identification du compte par ce nouvel abonnement. Si un ensemble d'informations d'identification n'a jamais été associé à un abonnement, ce nouvel abonnement ne sera pas associé à ces informations d'identification.

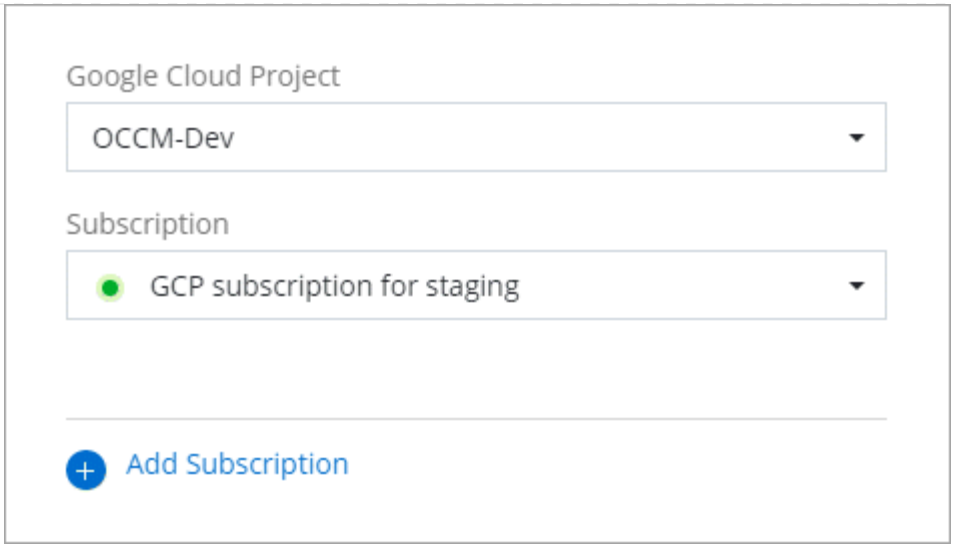
Pour tous les autres comptes, vous devez associer manuellement l'abonnement en répétant ces étapes.

- Sélectionnez **Enregistrer**.

  Dans cette vidéo, vous instructions pour vous abonner à Google Cloud Marketplace :

Abonnez-vous à BlueXP depuis Google Cloud Marketplace

a. Une fois ce processus terminé, revenez à la page d'informations d'identification dans BlueXP et sélectionnez ce nouvel abonnement.



Liens connexes

- "Gérez les licences BYOL basées sur la capacité pour Cloud Volumes ONTAP"
- "Gérez les licences BYOL pour les services de données BlueXP"
- "Gérez les informations d'identification et les abonnements AWS pour BlueXP"
- "Gérez les informations d'identification et les abonnements Azure pour BlueXP"
- "Gérez les identifiants Google Cloud et les abonnements pour BlueXP"

Ce que vous pouvez faire ensuite (mode restreint)

Une fois que vous êtes opérationnel avec BlueXP en mode restreint, vous pouvez commencer à utiliser les services BlueXP pris en charge avec le mode restreint.

Pour obtenir de l'aide, reportez-vous à la documentation de ces services :

- "Documents Amazon FSX pour ONTAP"
- "Documentation Azure NetApp Files"
- "Documents de sauvegarde et de restauration"
- "Documents de classification"
- "Documentation Cloud Volumes ONTAP"
- "Documentation sur le cluster ONTAP sur site"
- "Documents de réplication"

Lien associé

"Modes de déploiement BlueXP"