Commencez en mode privé

Setup and administration

NetApp
April 26, 2024

Sommaire

Commencez en mode privé

Mise en route du flux de travail (mode privé)

Commencez à utiliser BlueXP en mode privé en préparant votre environnement et en déployant Connector.

Le mode privé est généralement utilisé avec les environnements sur site qui ne disposent pas de connexion Internet et avec les régions cloud sécurisées, notamment "Cloud secret AWS", "Le cloud le plus secret d'AWS", et "Azure IL6"

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 permet d'accéder aux réseaux cibles.
3. Pour les déploiements cloud, configurez des autorisations dans votre fournisseur de cloud afin que vous puissiez les associer au connecteur après avoir installé le logiciel.

2 **"Déployez le connecteur"**

1. Installez le logiciel Connector sur votre propre hôte Linux.
2. Configurez BlueXP en ouvrant un navigateur Web et en entrant l'adresse IP de l'hôte Linux.
3. Pour les déploiements cloud, fournissez à BlueXP les autorisations que vous avez précédemment configurées.

Préparez le déploiement en mode privé

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

> Si vous souhaitez utiliser BlueXP dans le "Cloud secret AWS" ou le "Le cloud le plus secret d'AWS", vous devez alors suivre des instructions séparées pour démarrer dans ces environnements. "Découvrez comment vous lancer avec Cloud Volumes ONTAP dans le cloud secret AWS ou le cloud secret"

Étape 1 : comprendre le fonctionnement du mode privé

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

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.

"En savoir plus sur le fonctionnement du mode privé".

Étape 2 : passez en revue les options d'installation

En mode privé, vous pouvez installer le connecteur sur site ou dans le cloud en installant manuellement le connecteur sur votre propre hôte Linux.

L'emplacement d'installation du connecteur détermine les services et fonctionnalités BlueXP disponibles lorsque vous utilisez le mode privé. Par exemple, le connecteur doit être installé dans le cloud si vous souhaitez déployer et gérer Cloud Volumes ONTAP. "En savoir plus sur le mode privé".

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.

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 la mise en réseau pour le connecteur

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.

Terminaux des opérations quotidiennes

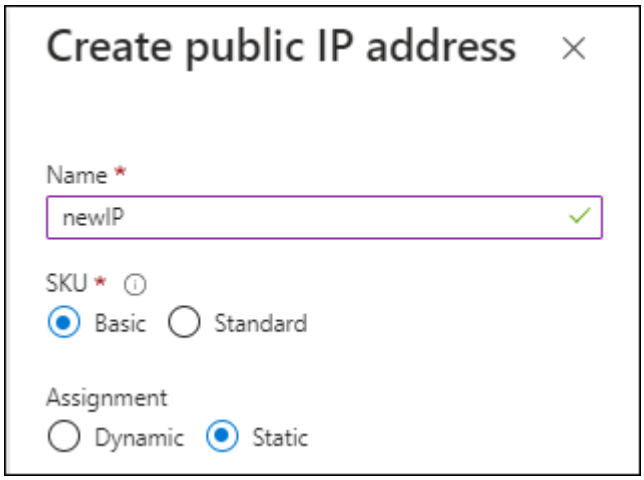
Le connecteur contacte les terminaux suivants pour gérer les ressources et les processus au sein de votre environnement de cloud public.

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.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	Pour gérer les ressources dans la région d'Azure IL6.
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.

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.

+
Avec le mode privé, la seule fois que BlueXP envoie le trafic sortant est à votre fournisseur cloud pour créer un système Cloud Volumes ONTAP.

Ports

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous le lancez.

HTTP (80) et HTTPS (443) permettent d'accéder à la console BlueXP. SSH (22) n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

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"

Étape 5 : préparez les autorisations cloud

Si le connecteur est installé dans le cloud et que vous prévoyez de créer des systèmes Cloud Volumes ONTAP, BlueXP requiert les autorisations de votre fournisseur cloud. Vous devez définir des autorisations dans votre fournisseur de cloud, puis les associer à l'instance Connector après l'avoir installée.

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. Vous devrez associer manuellement le rôle à l'instance EC2 du connecteur.

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. Activez une identité gérée attribuée par le système sur la machine virtuelle où vous prévoyez d'installer le connecteur 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.

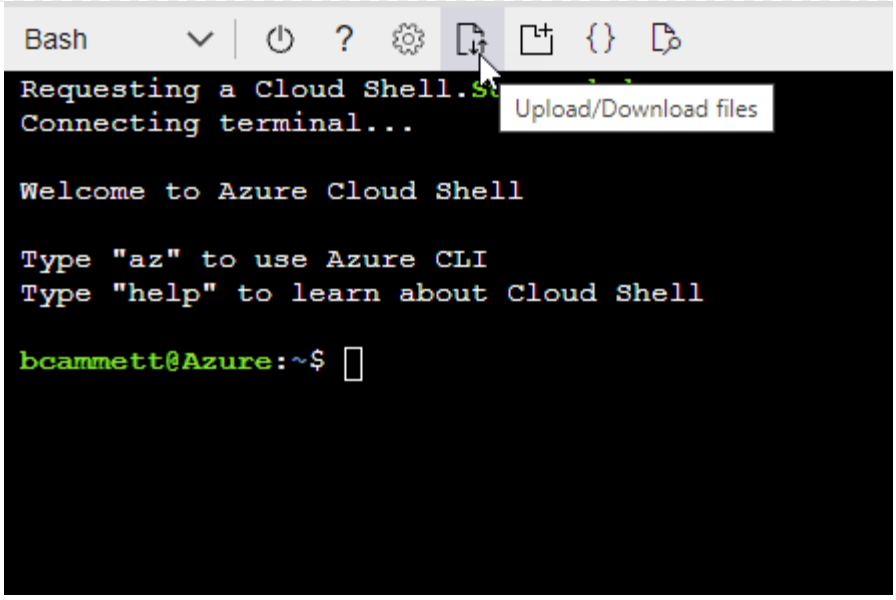
   Exemple

   ```
   "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

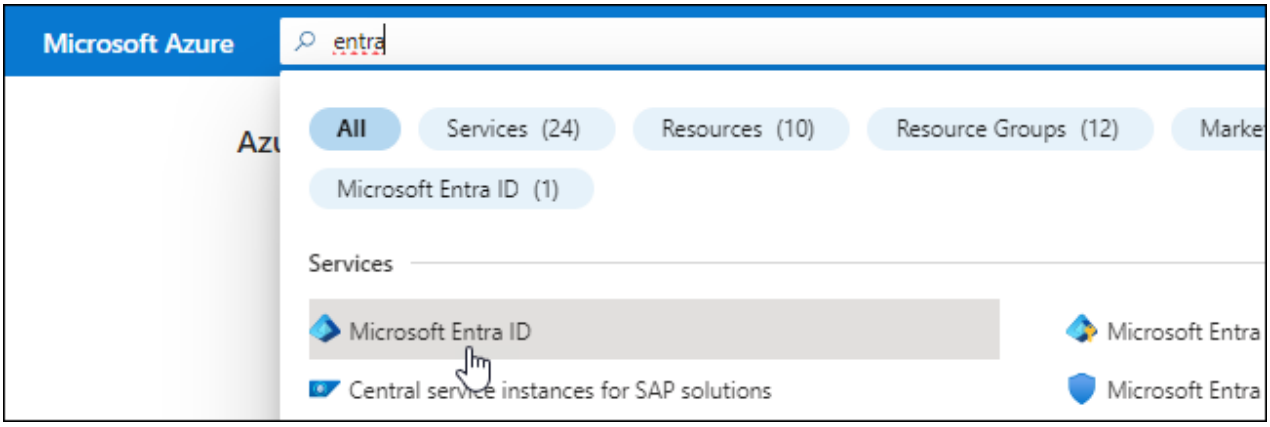
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont BlueXP a besoin. Après avoir installé le connecteur et configuré BlueXP, vous devez fournir ces informations d'identification à BlueXP.

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.

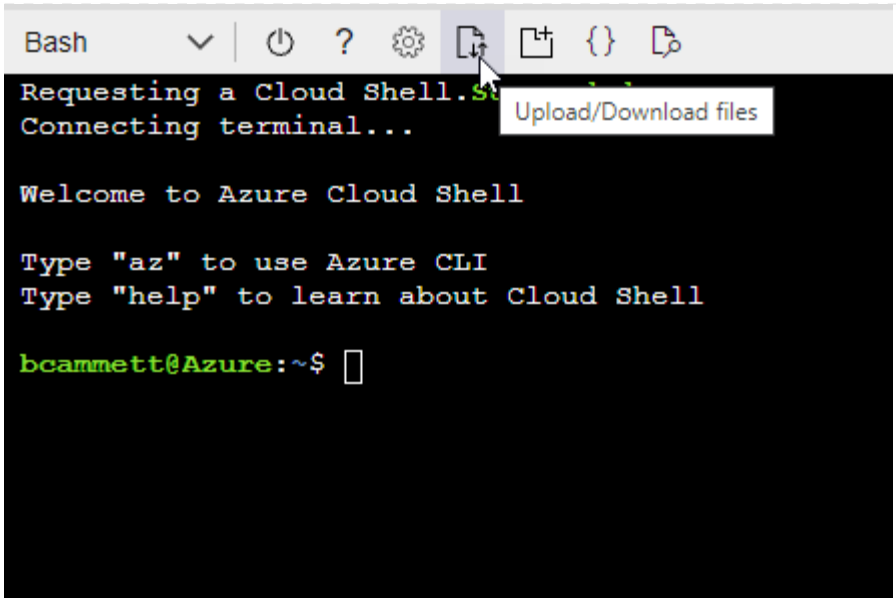
      Exemple

      ```
      "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**.

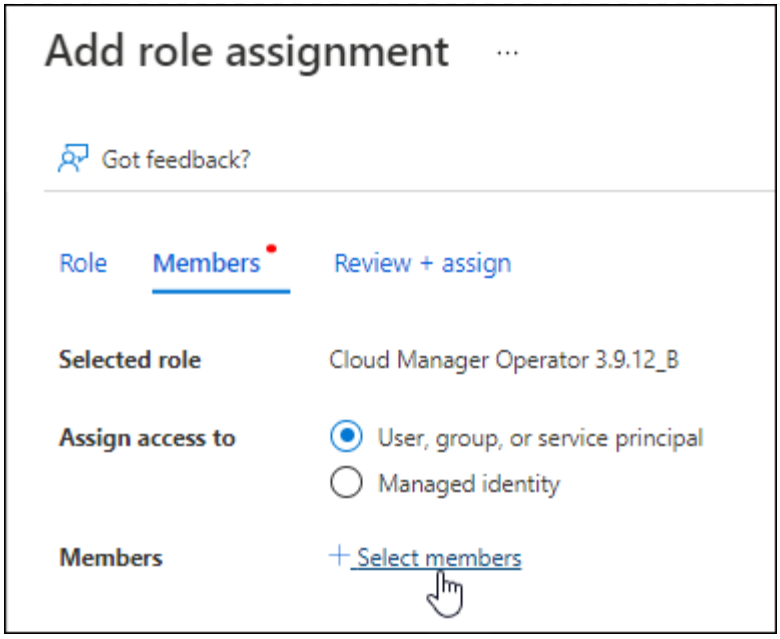
   b. Sélectionnez l'abonnement.

   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**.

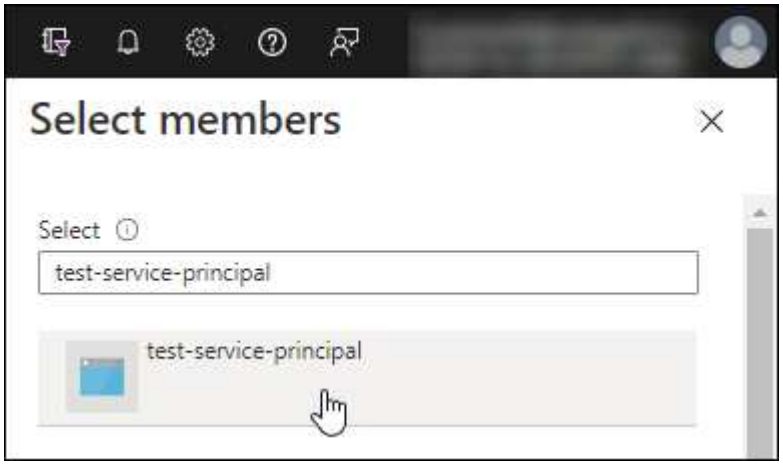
   e. Dans l'onglet **membres**, procédez comme suit :

      - 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**.

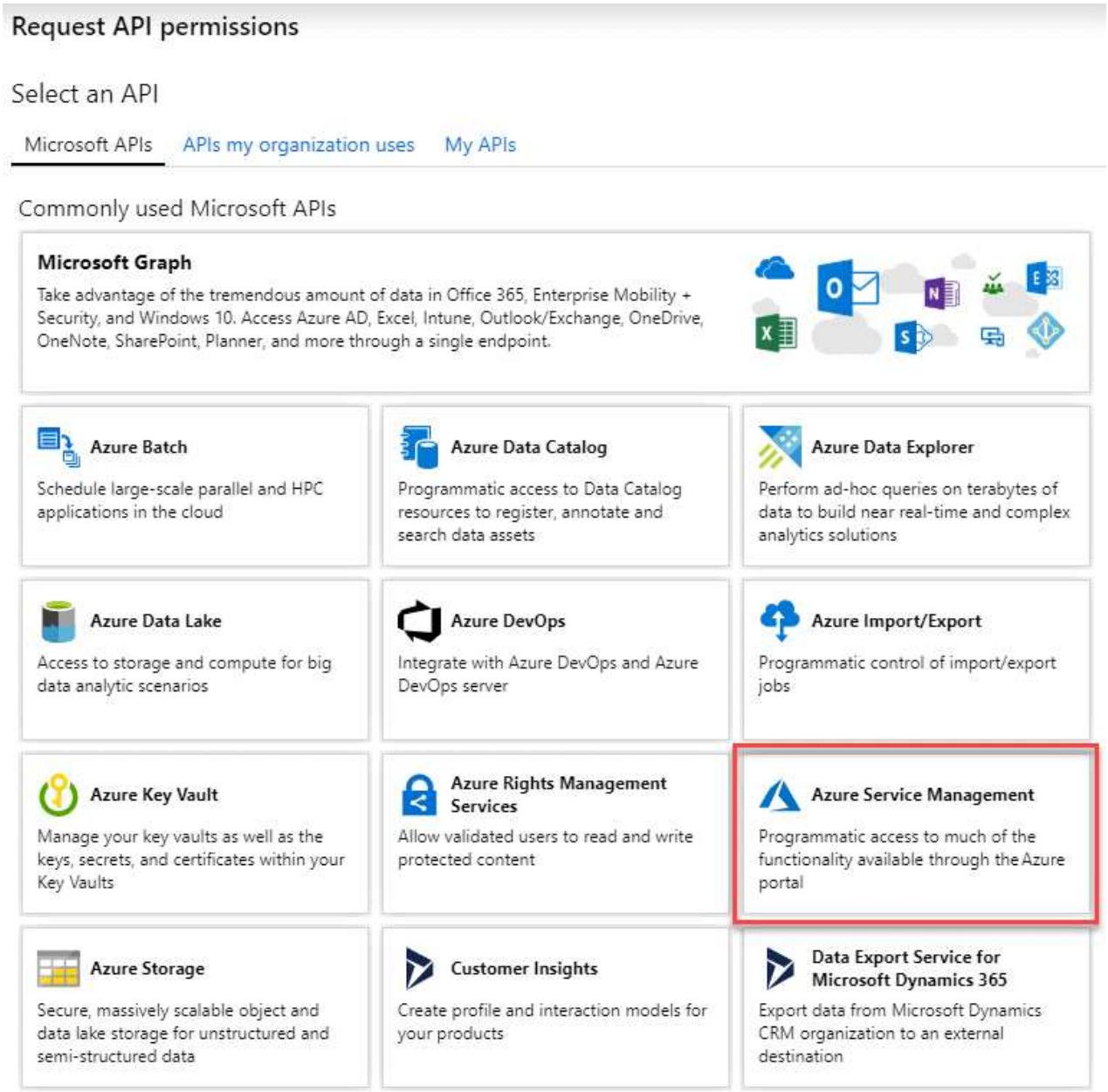
   Le principal de service dispose désormais des autorisations Azure nécessaires pour déployer le connecteur.

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.

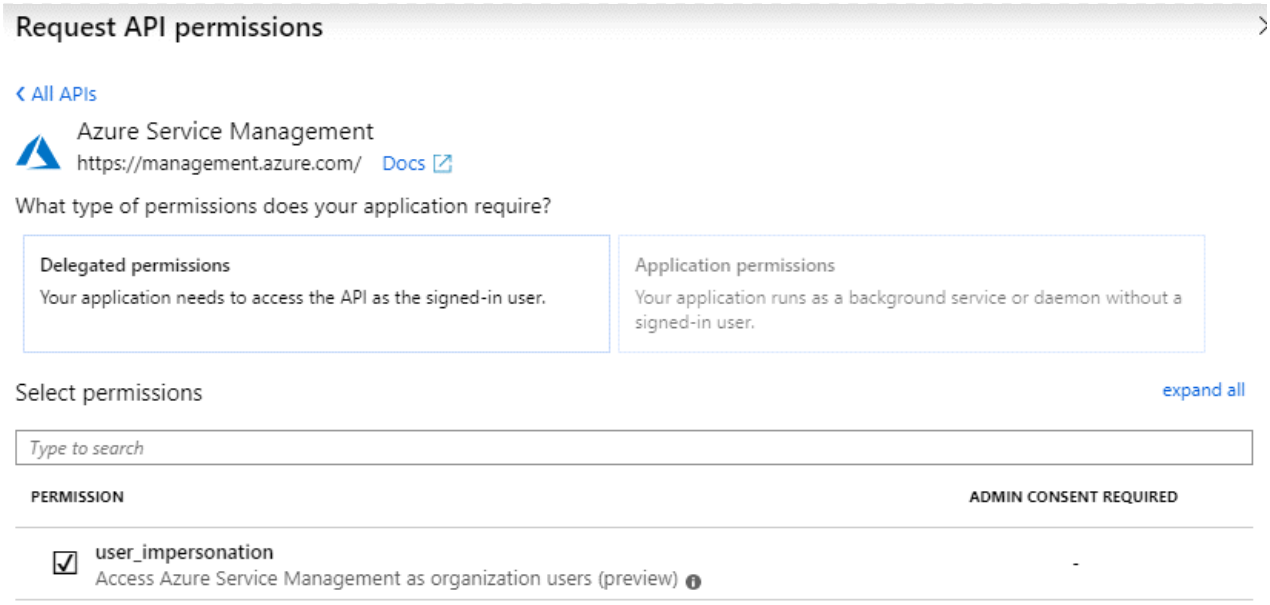
Ajoutez des autorisations d'API de gestion de service Windows Azure

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**.

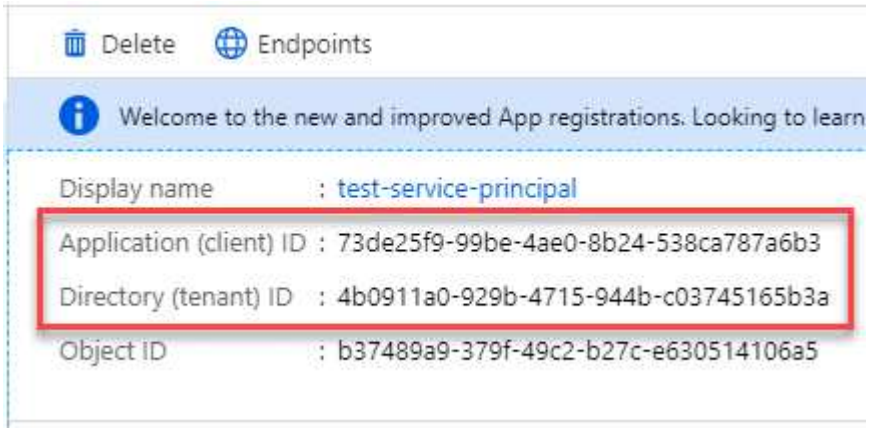


4. Sélectionnez **accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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 privé

Déployez le connecteur en mode privé pour utiliser BlueXP sans connectivité sortante à 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

Téléchargez le programme d'installation du produit sur le site de support NetApp, puis installez manuellement le connecteur sur votre propre hôte Linux.

Si vous souhaitez utiliser BlueXP dans le "Cloud secret AWS" ou le "Le cloud le plus secret d'AWS", vous devez alors suivre des instructions séparées pour démarrer dans ces environnements. "Découvrez comment vous lancer avec Cloud Volumes ONTAP dans le cloud secret AWS ou le cloud secret"

Avant de commencer

Les privilèges root sont requis pour installer le connecteur.

Étapes

1. Vérifiez que docker est activé et exécuté.

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

2. Téléchargez le logiciel du connecteur à partir du "Site de support NetApp"

   Assurez-vous de télécharger le programme d'installation hors ligne pour les réseaux privés sans accès à Internet.

3. Copiez le programme d'installation sur l'hôte Linux.
4. Attribuez des autorisations pour exécuter le script.

```
chmod +x /path/BlueXP-Connector-offline-<version>
```

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

5. Exécutez le script d'installation :

```
sudo /path/BlueXP-Connector-offline-<version>
```

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

Résultat

Le logiciel du connecteur est installé. Vous pouvez maintenant configurer BlueXP.

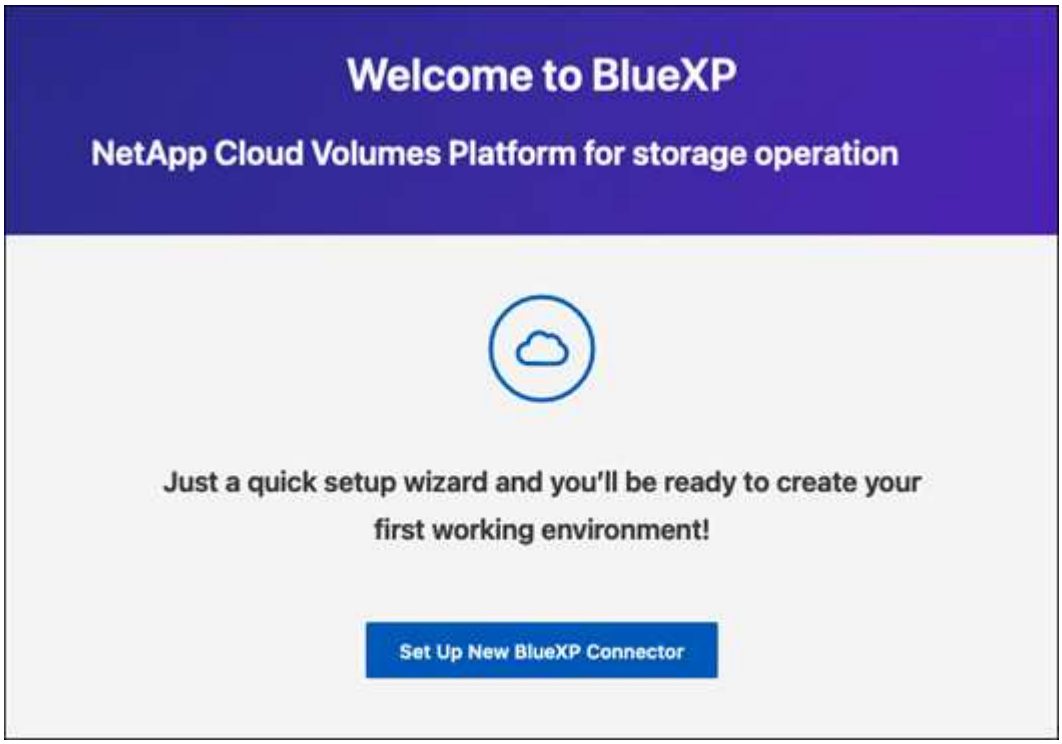
Étape 2 : configuration de BlueXP

Lorsque vous accédez pour la première fois à la console BlueXP, vous êtes invité à configurer BlueXP.

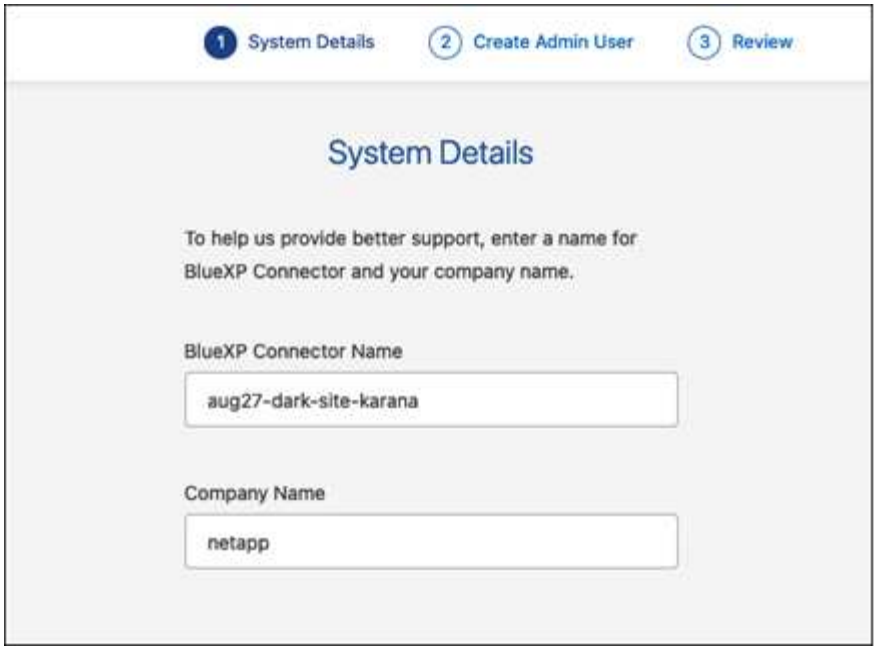
Étapes

1. Ouvrez un navigateur Web et entrez https://ipaddress Où ipaddress est l’adresse IP de l’hôte Linux où vous avez installé le connecteur.

   Vous devriez voir l'écran suivant.



2. Sélectionnez **configurer Nouveau connecteur BlueXP** et suivez les invites pour configurer le système.
   - **Détails du système** : saisissez un nom pour le connecteur et le nom de votre société.



- **Créer un utilisateur Admin** : créez l'utilisateur admin du système.

  Ce compte utilisateur s'exécute localement sur le système. Il n'y a pas de connexion au service auth0 disponible via BlueXP.

- **Révision** : consultez les détails, acceptez le contrat de licence, puis sélectionnez **configurer**.

3. Connectez-vous à BlueXP à l'aide de l'utilisateur admin que vous venez de créer.

Résultat

Le connecteur est maintenant installé et configuré.

Dès que de nouvelles versions du logiciel Connector sont disponibles, elles seront publiées sur le site de support NetApp. "Apprenez à mettre à niveau le connecteur".

Et la suite ?

Fournissez à BlueXP les autorisations que vous avez précédemment configurées.

Étape 3 : fournissez des autorisations à BlueXP

Si vous souhaitez créer des environnements de travail Cloud Volumes ONTAP, vous devez fournir à BlueXP les autorisations cloud que vous avez précédemment configurées.

"Découvrez comment préparer les autorisations cloud".

Rôle IAM AWS

Reliez le rôle IAM que vous avez créé précédemment à l'instance Connector EC2.

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.

Que faire ensuite (mode privé)

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

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

- "Création de systèmes Cloud Volumes ONTAP"
- "Découvrez les clusters ONTAP sur site"
- "Réplication des données"
- "Analysez les données de volumes ONTAP sur site à l'aide de la classification BlueXP"
- "Sauvegardez les données de volumes ONTAP sur site dans StorageGRID à l'aide de la sauvegarde et de la restauration BlueXP"

Lien associé

"Modes de déploiement BlueXP"