



Créer un connecteur

Setup and administration

NetApp
April 26, 2024

Sommaire

- Créer un connecteur 1
 - AWS 1
 - Azure 23
 - Google Cloud 66
- Installez et configurez un connecteur sur site 87

Créer un connecteur

AWS

Options d'installation des connecteurs dans AWS

Il existe plusieurs façons de créer un connecteur dans AWS. La méthode la plus courante est d'accéder directement à BlueXP.

Les options d'installation suivantes sont disponibles :

- ["Créez le connecteur directement à partir de BlueXP"](#) (il s'agit de l'option standard)

Cette action lance une instance EC2 exécutant Linux et le logiciel Connector dans un VPC de votre choix.

- ["Créez un connecteur à partir d'AWS Marketplace"](#)

Cette action lance également une instance EC2 exécutant Linux et le logiciel Connector, mais le déploiement est initié directement à partir d'AWS Marketplace plutôt que de BlueXP.

- ["Téléchargez et installez manuellement le logiciel sur votre propre hôte Linux"](#)

L'option d'installation que vous choisissez a une incidence sur la préparation de l'installation. Vous pouvez notamment fournir à BlueXP les autorisations requises pour authentifier et gérer les ressources dans AWS.

Créez un connecteur dans AWS à partir de BlueXP

Pour créer un connecteur dans AWS à partir de BlueXP, vous devez configurer votre réseau, préparer les autorisations AWS, puis créer le connecteur.

Avant de commencer

Vous devriez passer en revue ["Limitations du connecteur"](#).

Étape 1 : configuration du réseau

Assurez-vous que l'emplacement réseau où vous prévoyez d'installer le connecteur prend en charge les exigences suivantes. En répondant à ces exigences, il peut gérer les ressources et les processus dans votre environnement de cloud hybride.

VPC et sous-réseau

Lorsque vous créez le connecteur, vous devez spécifier le VPC et le sous-réseau sur lesquels le connecteur doit résider.

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des environnements de travail. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement sur site.

Accès Internet sortant

L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante pour contacter des points finaux spécifiques.

Points d'extrémité contactés depuis le connecteur

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 pour les opérations quotidiennes.

Notez que les points finaux répertoriés ci-dessous sont tous des entrées CNAME.

Terminaux	Objectif
Services AWS (amazonaws.com): <ul style="list-style-type: none">• 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"
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	Pour mettre à niveau le connecteur et ses composants Docker.

Terminaux contactés depuis la console BlueXP

Lorsque vous utilisez la console web BlueXP fournie via la couche SaaS, elle contacte plusieurs terminaux pour effectuer les tâches de gestion des données. Cela inclut les terminaux contactés pour déployer le connecteur à partir de la console BlueXP.

["Consultez la liste des terminaux contactés depuis la console BlueXP"](#).

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"](#)

Vous devrez implémenter cette exigence de mise en réseau après avoir créé le connecteur.

Étape 2 : configurez les autorisations AWS

BlueXP doit s'authentifier auprès d'AWS avant de pouvoir déployer l'instance de connecteur dans votre VPC. Vous pouvez choisir l'une des méthodes d'authentification suivantes :

- BlueXP assume un rôle IAM qui dispose des autorisations requises
- Fournissez une clé d'accès AWS et une clé secrète pour un utilisateur IAM qui dispose des autorisations nécessaires

Quelle que soit l'option choisie, la première étape consiste à créer une politique IAM. Cette politique contient uniquement les autorisations nécessaires pour lancer l'instance Connector dans AWS à partir de BlueXP.

Si nécessaire, vous pouvez restreindre la politique IAM à l'aide de l'IAM Condition élément. ["Documentation AWS : élément de condition"](#)



Lorsque BlueXP crée le connecteur, il applique un nouvel ensemble d'autorisations à l'instance Connector qui permet au connecteur de gérer les ressources AWS.

Étapes

1. Accédez à la console IAM AWS.

2. Sélectionnez **stratégies > Créer une stratégie**.
3. Sélectionnez **JSON**.
4. Copiez et collez la stratégie suivante :

Pour rappel, cette règle contient uniquement les autorisations nécessaires pour lancer l'instance Connector dans AWS à partir de BlueXP. ["Droits d'accès requis pour l'instance de connecteur elle-même"](#).

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam>DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2>DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2>DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
```

```

        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "kms:ListAliases",
        "cloudformation:ListStacks"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:TerminateInstances"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/OCCMInstance": "*"
        }
    },
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ]
}
]
}

```

5. Sélectionnez **Suivant** et ajoutez des balises, si nécessaire.
6. Sélectionnez **Suivant** et entrez un nom et une description.
7. Sélectionnez **Créer une stratégie**.
8. Reliez la règle à un rôle IAM que BlueXP peut assumer ou à un utilisateur IAM pour que vous puissiez fournir BlueXP avec des clés d'accès :
 - (Option 1) configurer un rôle IAM que BlueXP peut assumer :
 - i. Accédez à la console IAM AWS dans le compte cible.
 - ii. Sous gestion des accès, sélectionnez **rôles** > **Créer un rôle** et suivez les étapes pour créer le rôle.
 - iii. Sous **Type d'entité approuvée**, sélectionnez **compte AWS**.
 - iv. Sélectionnez **un autre compte AWS** et saisissez l'ID du compte BlueXP SaaS : 952013314444

- v. Sélectionnez la stratégie que vous avez créée dans la section précédente.
- vi. Après avoir créé le rôle, copiez le rôle ARN afin de pouvoir le coller dans BlueXP lorsque vous créez le connecteur.
- (Option 2) configurez les autorisations d'accès pour un utilisateur IAM afin que vous puissiez fournir BlueXP avec des clés d'accès :
 - i. Dans la console IAM AWS, sélectionnez **Users**, puis sélectionnez le nom d'utilisateur.
 - ii. Sélectionnez **Ajouter des autorisations > joindre des stratégies existantes directement**.
 - iii. Sélectionnez la stratégie que vous avez créée.
 - iv. Sélectionnez **Suivant**, puis **Ajouter des autorisations**.
 - v. Assurez-vous que vous disposez de la clé d'accès et de la clé secrète pour l'utilisateur IAM.

Résultat

Vous devez maintenant disposer d'un rôle IAM qui possède les autorisations requises ou d'un utilisateur IAM qui dispose des autorisations requises. Lorsque vous créez le connecteur à partir de BlueXP, vous pouvez fournir des informations sur le rôle ou les clés d'accès.

Étape 3 : créer le connecteur

Créez le connecteur directement à partir de la console web BlueXP.

Description de la tâche

La création du connecteur à partir de BlueXP déploie une instance EC2 dans AWS à l'aide d'une configuration par défaut. Après avoir créé le connecteur, vous ne devez pas passer à un type d'instance EC2 plus petit qui a moins de CPU ou de RAM. ["En savoir plus sur la configuration par défaut du connecteur"](#).

Avant de commencer

Vous devez disposer des éléments suivants :

- Méthode d'authentification AWS : rôle IAM ou clés d'accès pour un utilisateur IAM disposant des autorisations requises.
- VPC et sous-réseau qui répondent aux exigences réseau.
- Une paire de clés pour l'instance EC2.
- Détails sur un serveur proxy, si un proxy est requis pour accéder à Internet à partir du connecteur.

Étapes

1. Sélectionnez la liste déroulante **Connector** et sélectionnez **Ajouter un connecteur**.



2. Choisissez **Amazon Web Services** comme fournisseur de cloud et sélectionnez **Continuer**.
3. Sur la page **déploiement d'un connecteur**, consultez les détails de ce dont vous aurez besoin. Vous avez deux options :
 - a. Sélectionnez **Continuer** pour préparer le déploiement à l'aide du guide produit. Chaque étape du guide du produit inclut les informations contenues sur cette page de la documentation.
 - b. Sélectionnez **passer au déploiement** si vous êtes déjà préparé en suivant les étapes de cette page.
4. Suivez les étapes de l'assistant pour créer le connecteur :
 - **Soyez prêt**: Passez en revue ce dont vous aurez besoin.
 - **Informations d'identification AWS** : spécifiez votre région AWS puis choisissez une méthode d'authentification, qui est soit un rôle IAM que BlueXP peut assumer, soit une clé d'accès AWS et une clé secrète.



Si vous choisissez **supposons rôle**, vous pouvez créer le premier ensemble d'informations d'identification à partir de l'assistant de déploiement de connecteur. Tout ensemble supplémentaire d'informations d'identification doit être créé à partir de la page informations d'identification. Ils seront ensuite disponibles à partir de l'assistant dans une liste déroulante. "[Découvrez comment ajouter des identifiants supplémentaires](#)".

- **Détails** : fournir des détails sur le connecteur.
 - Entrez un nom pour l'instance.
 - Ajoutez des balises personnalisées (métadonnées) à l'instance.
 - Choisissez si vous souhaitez que BlueXP crée un nouveau rôle avec les autorisations requises, ou si vous souhaitez sélectionner un rôle existant que vous avez configuré avec "[les autorisations requises](#)".
 - Indiquez si vous souhaitez chiffrer les disques EBS du connecteur. Vous pouvez utiliser la clé de chiffrement par défaut ou utiliser une clé personnalisée.
- **Network** : spécifiez un VPC, un sous-réseau et une paire de clés pour l'instance, choisissez d'activer ou non une adresse IP publique et, éventuellement, spécifiez une configuration proxy.

Assurez-vous que vous disposez de la paire de clés appropriée à utiliser avec le connecteur. Sans paire de clés, vous ne pourrez pas accéder à la machine virtuelle Connector.

- **Groupe de sécurité** : choisissez de créer un nouveau groupe de sécurité ou de sélectionner un groupe de sécurité existant qui autorise les règles entrantes et sortantes requises.

["Afficher les règles des groupes de sécurité pour AWS"](#).

- **Review** : consultez vos sélections pour vérifier que votre configuration est correcte.

5. Sélectionnez **Ajouter**.

L'instance doit être prête dans environ 7 minutes. Vous devez rester sur la page jusqu'à ce que le processus soit terminé.

Résultat

Une fois le processus terminé, le connecteur est disponible pour être utilisé depuis BlueXP.

Si vous avez des compartiments Amazon S3 dans le même compte AWS que vous avez créé le connecteur, un environnement de travail Amazon S3 s'affiche automatiquement sur le canevas BlueXP. ["Découvrez comment gérer des compartiments S3 à partir de BlueXP"](#)

Créez un connecteur à partir d'AWS Marketplace

Pour créer un connecteur à partir d'AWS Marketplace, vous devez configurer votre réseau, préparer les autorisations AWS, examiner les exigences d'instance, puis créer le connecteur.

Avant de commencer

Vous devriez passer en revue ["Limitations du connecteur"](#).

Étape 1 : configuration du réseau

Assurez-vous que l'emplacement réseau où vous prévoyez d'installer le connecteur prend en charge les exigences suivantes. En répondant à ces exigences, il peut gérer les ressources et les processus dans votre environnement de cloud hybride.

VPC et sous-réseau

Lorsque vous créez le connecteur, vous devez spécifier le VPC et le sous-réseau sur lesquels le connecteur doit résider.

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des environnements de travail. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement sur site.

Accès Internet sortant

L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante pour contacter des points finaux spécifiques.

Points d'extrémité contactés depuis le connecteur

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 pour les opérations quotidiennes.

Notez que les points finaux répertoriés ci-dessous sont tous des entrées CNAME.

Terminaux	Objectif
Services AWS (amazonaws.com): <ul style="list-style-type: none"> • 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"
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	Pour mettre à niveau le connecteur et ses composants Docker.

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"](#)

Vous devrez implémenter cette exigence de mise en réseau après avoir créé le connecteur.

Étape 2 : configurez les autorisations AWS

Pour préparer un déploiement Marketplace, créez des politiques IAM dans AWS et associez-les à un rôle IAM. Lorsque vous créez le connecteur à partir d'AWS Marketplace, vous êtes invité à sélectionner ce rôle IAM.

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. 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 pouvez désormais associer un rôle IAM à l'instance EC2 lors du déploiement depuis AWS Marketplace.

Étape 3 : passez en revue les exigences relatives aux instances

Lorsque vous créez le connecteur, vous devez choisir un type d'instance EC2 qui répond aux exigences suivantes.

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.

Étape 4 : créer le connecteur

Créez le connecteur directement à partir d'AWS Marketplace.

Description de la tâche

La création du connecteur à partir d'AWS Marketplace déploie une instance EC2 dans AWS à l'aide d'une configuration par défaut. ["En savoir plus sur la configuration par défaut du connecteur"](#).

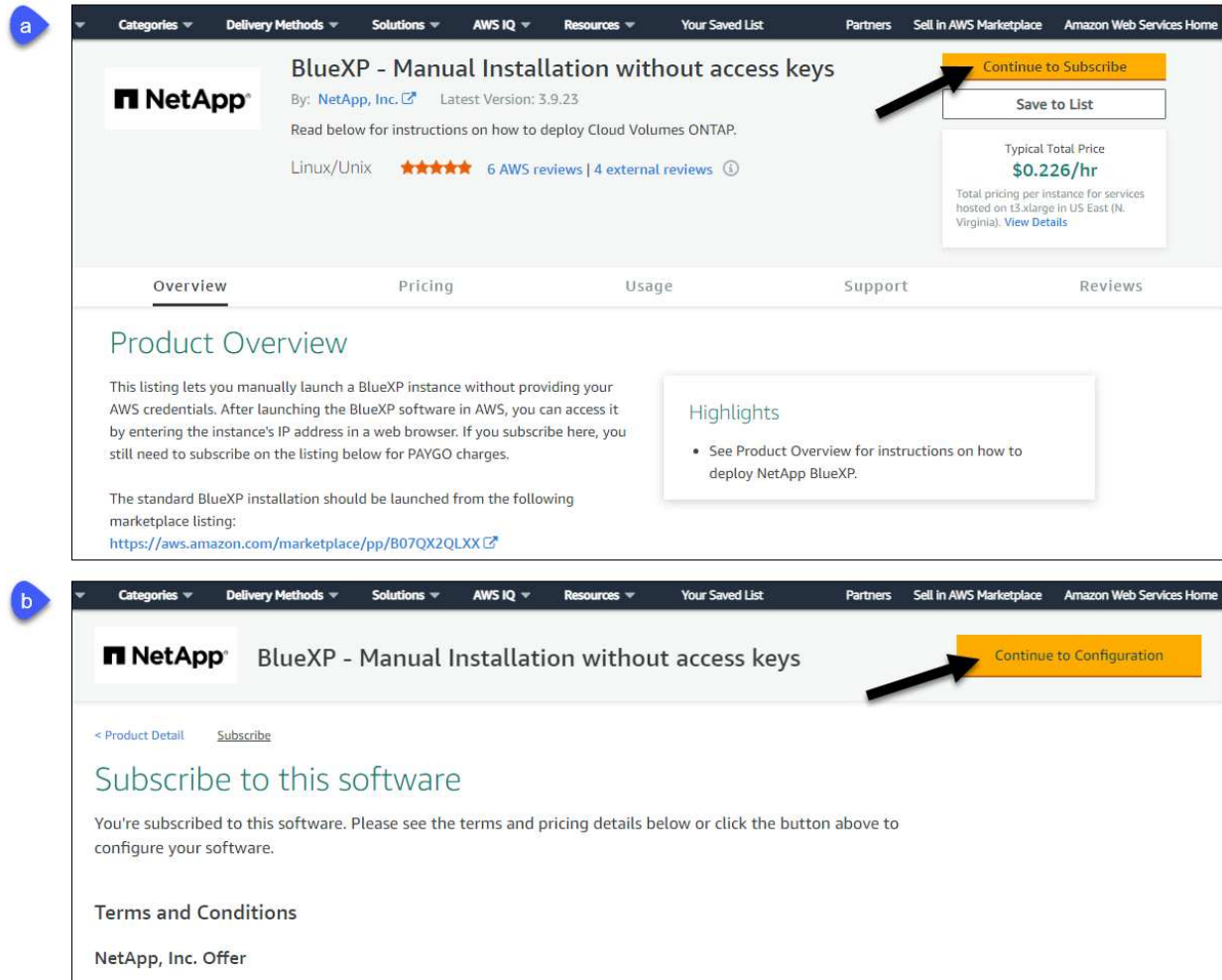
Avant de commencer

Vous devez disposer des éléments suivants :

- VPC et sous-réseau qui répondent aux exigences réseau.
- Un rôle IAM avec une stratégie jointe qui inclut les autorisations requises pour le connecteur.
- 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.
- 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**.

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

6. Ouvrez un navigateur Web à partir d'un hôte connecté à la machine virtuelle Connector et entrez l'URL suivante :

`https://ipaddress`

7. Une fois connecté, configurez le connecteur :

- a. Spécifiez le compte BlueXP à associer au connecteur.
- b. Entrez un nom pour le système.
- c. Sous **exécutez-vous dans un environnement sécurisé ?** maintenez le mode restreint désactivé.

Vous devez désactiver le mode restreint, car ces étapes décrivent l'utilisation de BlueXP en mode standard. Vous devez activer le mode restreint uniquement si vous disposez d'un environnement sécurisé et souhaitez déconnecter ce compte des services back-end BlueXP. Si c'est le cas, ["Suivez les étapes pour démarrer avec BlueXP en mode restreint"](#).

- d. Sélectionnez **commençons**.

Résultat

Le connecteur est maintenant installé et configuré avec votre compte BlueXP.

Ouvrez un navigateur Web et accédez au ["Console BlueXP"](#) Pour commencer à utiliser le connecteur avec BlueXP.

Si vous avez des compartiments Amazon S3 dans le même compte AWS que vous avez créé le connecteur, un environnement de travail Amazon S3 s'affiche automatiquement sur le canevas BlueXP. ["Découvrez comment gérer des compartiments S3 à partir de BlueXP"](#)

Installez manuellement le connecteur dans AWS

Pour installer manuellement le connecteur sur votre propre hôte Linux, vous devez vérifier la configuration requise pour l'hôte, configurer le réseau, préparer les autorisations AWS, installer le connecteur, puis fournir les autorisations que vous avez préparées.

Avant de commencer

Vous devriez passer en revue ["Limitations du connecteur"](#).

Étape 1 : 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.

Paire de clés

Lorsque vous créez le connecteur, vous devez sélectionner une paire de clés EC2 à utiliser avec l'instance.

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 2 : configuration du réseau

Assurez-vous que l'emplacement réseau où vous prévoyez d'installer le connecteur prend en charge les exigences suivantes. En répondant à ces exigences, il peut gérer les ressources et les processus dans votre environnement de cloud hybride.

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des environnements de travail. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement sur site.

Accès Internet sortant

L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante pour contacter des points finaux spécifiques.

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>

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.

Points d'extrémité contactés depuis le connecteur

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 pour les opérations quotidiennes.

Notez que les points finaux répertoriés ci-dessous sont tous des entrées CNAME.

Terminaux	Objectif
Services AWS (amazonaws.com): <ul style="list-style-type: none">• 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://support.netapp.com https://mysupport.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
https://*.api.blueexp.netapp.com https://api.blueexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	<p>Pour fournir des fonctions et des services SaaS dans BlueXP.</p> <p>Notez que le connecteur est actuellement en contact avec « cloudmanager.cloud.netapp.com », mais il commencera à contacter « api.blueexp.netapp.com » dans une prochaine version.</p>
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Pour mettre à niveau le connecteur et ses composants Docker.

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"](#)

Étape 3 : configurer les autorisations

Vous devez fournir des autorisations AWS à BlueXP via l'une des options suivantes :

- Option 1 : créez des règles IAM et associez-les à un rôle IAM que vous pouvez associer à l'instance EC2.
- Option 2 : fournissez à BlueXP la clé d'accès AWS pour un utilisateur IAM qui dispose des autorisations requises.

Suivez les étapes pour préparer les autorisations pour BlueXP.

Rôle IAM

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. 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 que vous pouvez associer à l'instance EC2 après avoir installé le connecteur.

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

Vous disposez désormais d'un utilisateur IAM qui dispose des autorisations requises et d'une clé d'accès que vous pouvez fournir à BlueXP.

Étape 4 : installez le connecteur

Une fois la configuration requise terminée, vous pouvez installer manuellement le logiciel sur votre propre hôte Linux.

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 contenant 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.

6. Attendez la fin de l'installation.

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

7. Ouvrez un navigateur Web à partir d'un hôte connecté à la machine virtuelle Connector et entrez l'URL suivante :

`https://ipaddress`

8. Une fois connecté, configurez le connecteur :

- a. Spécifiez le compte BlueXP à associer au connecteur.
- b. Entrez un nom pour le système.
- c. Sous **exécutez-vous dans un environnement sécurisé ?** maintenez le mode restreint désactivé.

Vous devez désactiver le mode restreint, car ces étapes décrivent l'utilisation de BlueXP en mode standard. Vous devez activer le mode restreint uniquement si vous disposez d'un environnement sécurisé et souhaitez déconnecter ce compte des services back-end BlueXP. Si c'est le cas, "[Suivez les étapes pour démarrer avec BlueXP en mode restreint](#)".

- d. Sélectionnez **commençons**.

Résultat

Le connecteur est maintenant installé et configuré avec votre compte BlueXP.

Si vous avez des compartiments Amazon S3 dans le même compte AWS que vous avez créé le connecteur, un environnement de travail Amazon S3 s'affiche automatiquement sur le canevas BlueXP. "[Découvrez comment gérer des compartiments S3 à partir de BlueXP](#)"

Étape 5 : fournissez des autorisations à BlueXP

Maintenant que vous avez installé le connecteur, vous devez fournir à BlueXP les autorisations AWS que vous avez précédemment configurées. Si vous disposez des autorisations requises, BlueXP peut gérer vos données et votre infrastructure de stockage dans AWS.

Rôle IAM

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.

Accédez au "[Console BlueXP](#)" Pour commencer à utiliser le connecteur avec BlueXP.

Clé d'accès AWS

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

Étapes

1. Assurez-vous que le bon connecteur est actuellement sélectionné dans BlueXP.
2. Dans le coin supérieur droit de la console BlueXP, sélectionnez l'icône Paramètres, puis sélectionnez **informations d'identification**.



3. 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.

Accédez au "[Console BlueXP](#)" Pour commencer à utiliser le connecteur avec BlueXP.

Azure

Options d'installation des connecteurs dans Azure

Il existe plusieurs façons de créer un connecteur dans Azure. La méthode la plus courante est d'accéder directement à BlueXP.

Les options d'installation suivantes sont disponibles :

- ["Créez un connecteur directement à partir de BlueXP"](#) (il s'agit de l'option standard)

Cette action lance une machine virtuelle exécutant Linux et le logiciel Connector dans un réseau virtuel de votre choix.

- ["Créez un connecteur à partir d'Azure Marketplace"](#)

Cette action lance également une machine virtuelle qui exécute Linux et le logiciel Connector. Le déploiement est initié directement depuis Azure Marketplace plutôt que depuis BlueXP.

- ["Téléchargez et installez manuellement le logiciel sur votre propre hôte Linux"](#)

L'option d'installation que vous choisissez a une incidence sur la préparation de l'installation. Vous pouvez notamment fournir à BlueXP les autorisations requises pour authentifier et gérer les ressources dans Azure.

Créez un connecteur dans Azure à partir de BlueXP

Pour créer un connecteur dans Azure à partir de BlueXP, vous devez configurer votre réseau, préparer les autorisations Azure, puis créer le connecteur.

Avant de commencer

Vous devriez passer en revue ["Limitations du connecteur"](#).

Étape 1 : configuration du réseau

Assurez-vous que l'emplacement réseau où vous prévoyez d'installer le connecteur prend en charge les exigences suivantes. En répondant à ces exigences, il peut gérer les ressources et les processus dans votre environnement de cloud hybride.

Région Azure

Si vous utilisez Cloud Volumes ONTAP, le connecteur doit être déployé dans la même région Azure que les systèmes Cloud Volumes ONTAP qu'il gère, ou dans le ["Paire de régions Azure"](#) Pour les systèmes Cloud Volumes ONTAP. Cette exigence garantit qu'une connexion Azure Private Link est utilisée entre Cloud Volumes ONTAP et les comptes de stockage associés.

["Découvrez comment Cloud Volumes ONTAP utilise une liaison privée Azure"](#)

Vnet et sous-réseau

Lorsque vous créez le connecteur, vous devez spécifier le réseau virtuel et le sous-réseau dans lesquels le connecteur doit résider.

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer

des environnements de travail. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement sur site.

Accès Internet sortant

L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante pour contacter des points finaux spécifiques.

Points d'extrémité contactés depuis le connecteur

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 pour les opérations quotidiennes.

Notez que les points finaux répertoriés ci-dessous sont tous des entrées CNAME.

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.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://support.netapp.com https://mysupport.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
https://*.api.blueexp.netapp.com https://api.blueexp.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.blueexp.netapp.com » dans une prochaine version.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Pour mettre à niveau le connecteur et ses composants Docker.

Terminaux contactés depuis la console BlueXP

Lorsque vous utilisez la console web BlueXP fournie via la couche SaaS, elle contacte plusieurs terminaux pour effectuer les tâches de gestion des données. Cela inclut les terminaux contactés pour déployer le connecteur à partir de la console BlueXP.

["Consultez la liste des terminaux contactés depuis la console BlueXP"](#).

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"](#)

Vous devrez implémenter cette exigence de mise en réseau après avoir créé le connecteur.

Étape 2 : créez un rôle personnalisé

Créez un rôle personnalisé Azure que vous pouvez attribuer à votre compte Azure ou à un principal de service Microsoft Entra. BlueXP s'authentifie auprès d'Azure et utilise ces autorisations pour créer l'instance de connecteur en votre nom.

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. Copiez les autorisations requises pour un nouveau rôle personnalisé dans Azure et enregistrez-les dans un fichier JSON.



Ce rôle personnalisé contient uniquement les autorisations nécessaires pour lancer la machine virtuelle Connector dans Azure à partir de BlueXP. N'utilisez pas cette politique dans d'autres situations. Lorsque BlueXP crée le connecteur, il applique un nouvel ensemble d'autorisations à la VM Connector qui permet au connecteur de gérer les ressources de votre environnement de cloud public.

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",

    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/read",

    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/read",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Network/publicIPAddresses/join/action",
```

```

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/read",
    "Microsoft.Network/networkInterfaces/ipConfigurations/read",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Resources/deployments/validate/action",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/operationresults/read",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Authorization/roleDefinitions/write",
    "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Authorization/roleAssignments/read"
],
"NotActions": [],
"AssignableScopes": [],
>Description": "Azure SetupAsService",
>IsCustom": "true"
}

```

2. Modifiez le fichier JSON en ajoutant votre ID d'abonnement Azure à la portée attribuable.

Exemple

```

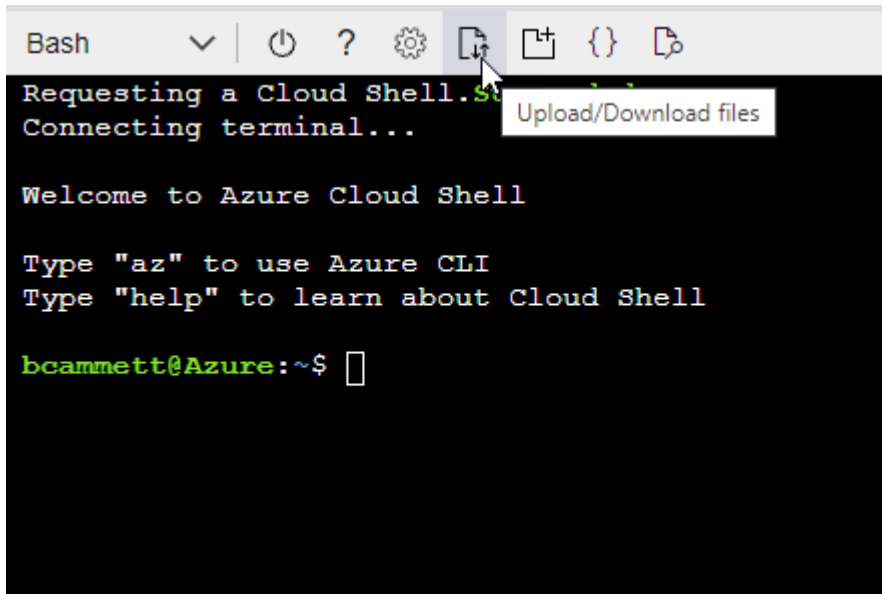
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],

```

3. 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. Entrez la commande Azure CLI suivante :

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

Vous devez maintenant avoir un rôle personnalisé appelé *Azure SetupAsService*. Vous pouvez maintenant appliquer ce rôle personnalisé à votre compte d'utilisateur ou à un principal de service.

Étape 3 : configuration de l'authentification

Lors de la création du connecteur à partir de BlueXP, vous devez fournir un identifiant qui permet à BlueXP de s'authentifier auprès d'Azure et de déployer la machine virtuelle. Vous avez deux options :

1. Connectez-vous à l'aide de votre compte Azure lorsque vous y êtes invité. Ce compte doit disposer d'autorisations Azure spécifiques. Il s'agit de l'option par défaut.
2. Fournir des détails sur une entité de service Microsoft Entra. Ce service principal nécessite également des autorisations spécifiques.

Suivez les étapes pour préparer l'une de ces méthodes d'authentification à utiliser avec BlueXP.

Compte Azure

Attribuez le rôle personnalisé à l'utilisateur qui va déployer le connecteur à partir de BlueXP.

Étapes

1. Dans le portail Azure, ouvrez le service **Subscriptions** et sélectionnez l'abonnement de l'utilisateur.
2. Cliquez sur **contrôle d'accès (IAM)**.
3. Cliquez sur **Ajouter > Ajouter une affectation de rôle**, puis ajoutez les autorisations suivantes :
 - a. Sélectionnez le rôle **Azure SetupAsService** et cliquez sur **Suivant**.



Azure SetupAsService est le nom par défaut fourni dans la stratégie de déploiement du connecteur pour Azure. Si vous avez choisi un autre nom pour le rôle, sélectionnez-le à la place.

- b. Conserver **utilisateur, groupe ou entité de service** sélectionnée.
- c. Cliquez sur **Sélectionner les membres**, choisissez votre compte utilisateur et cliquez sur **Sélectionner**.
- d. Cliquez sur **Suivant**.
- e. Cliquez sur **Revue + affecter**.

Résultat

L'utilisateur Azure dispose désormais des autorisations nécessaires pour déployer le connecteur depuis BlueXP.

Principal du service

Au lieu de vous connecter à votre compte Azure, vous pouvez fournir à BlueXP les identifiants d'un principal de service Azure qui dispose des autorisations requises.

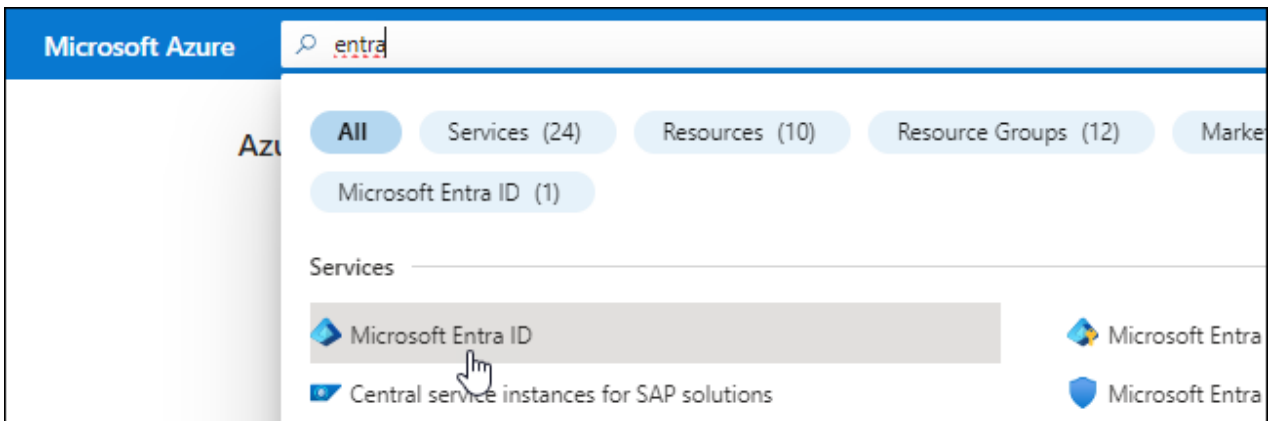
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont BlueXP a besoin.

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**.

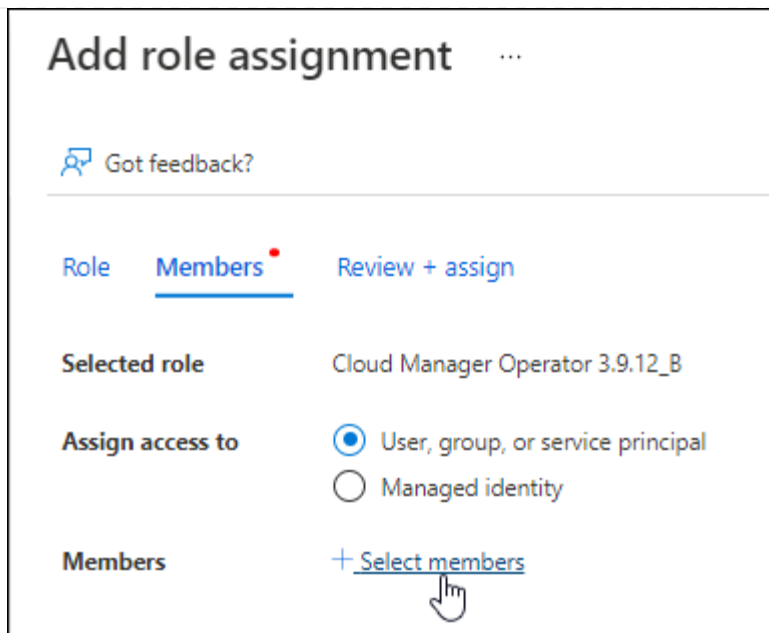


3. Dans le menu, sélectionnez **enregistrements d'applications**.
4. Sélectionnez **nouvel enregistrement**.
5. Spécifiez les détails de l'application :
 - **Nom** : saisissez un nom pour l'application.
 - **Type de compte** : sélectionnez un type de compte (tout fonctionne avec BlueXP).
 - **URI de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

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

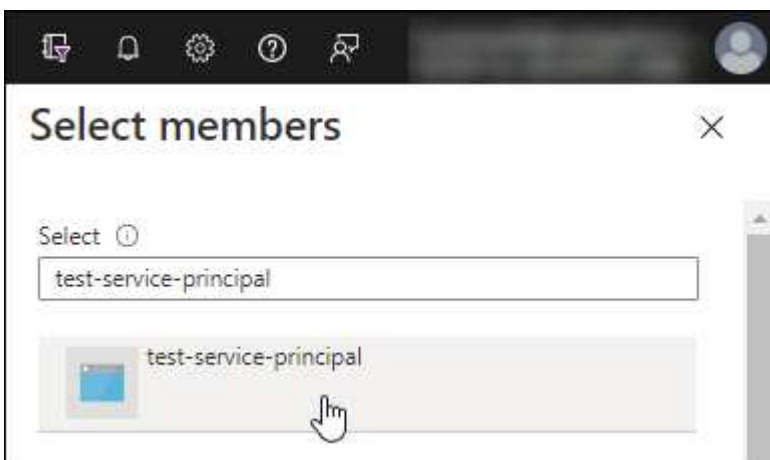
Attribuez le rôle personnalisé à l'application

1. À partir du portail Azure, ouvrez le service **abonnements**.
2. Sélectionnez l'abonnement.
3. Cliquez sur **contrôle d'accès (IAM) > Ajouter > Ajouter une affectation de rôle**.
4. Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et cliquez sur **Next**.
5. Dans l'onglet **membres**, procédez comme suit :
 - a. Conserver **utilisateur, groupe ou entité de service** sélectionnée.
 - b. Cliquez sur **Sélectionner les membres**.



c. Recherchez le nom de l'application.

Voici un exemple :



a. Sélectionnez l'application et cliquez sur **Sélectionner**.

b. Cliquez sur **Suivant**.

6. Cliquez sur **Revue + affecter**.

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

Si vous souhaitez gérer les ressources de plusieurs abonnements Azure, vous devez lier le principal de service à chacun de ces abonnements. Par exemple, 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**.

Request API permissions

Select an API

Microsoft APIs [APIs my organization uses](#) [My APIs](#)

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export

Programmatic control of import/export jobs

Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights

Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

[< All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

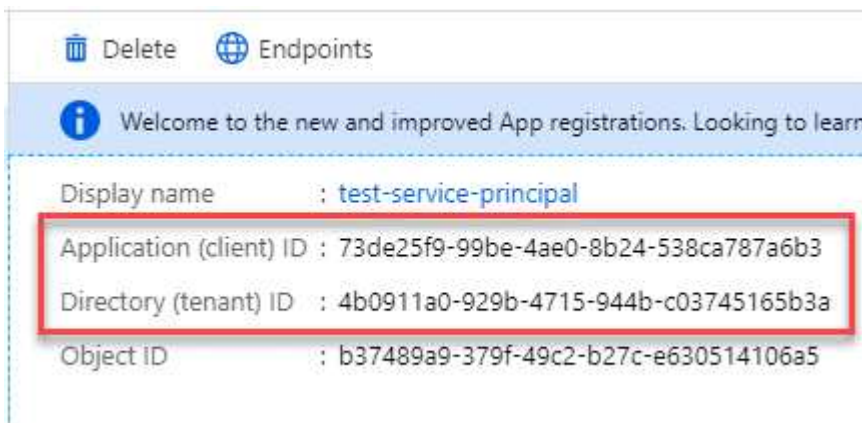


user_impersonation

Access Azure Service Management as organization users (preview)

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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 créez le connecteur.

Étape 4 : créer le connecteur

Créez le connecteur directement à partir de la console web BlueXP.

Description de la tâche

La création du connecteur à partir de BlueXP déploie une machine virtuelle dans Azure à l'aide d'une configuration par défaut. Après avoir créé le connecteur, vous ne devez pas passer à un type de machine virtuelle plus petit qui a moins de CPU ou de RAM. ["En savoir plus sur la configuration par défaut du connecteur"](#).

Avant de commencer

Vous devez disposer des éléments suivants :

- Un abonnement Azure.
- Un vnet et un sous-réseau dans votre région Azure de votre choix.
- Détails sur un serveur proxy, si votre organisation nécessite un proxy pour tout le trafic Internet sortant :
 - Adresse IP
 - Informations d'identification
 - Certificat HTTPS
- Une clé publique SSH, si vous souhaitez utiliser cette méthode d'authentification pour la machine virtuelle Connector. L'autre option de la méthode d'authentification est d'utiliser un mot de passe.

["Découvrez comment vous connecter à une VM Linux dans Azure"](#)

- Si vous ne souhaitez pas que BlueXP crée automatiquement un rôle Azure pour le connecteur, vous devrez créer votre propre rôle ["utilisation de la stratégie sur cette page"](#).

Ces autorisations sont pour l'instance de connecteur elle-même. Il s'agit d'un ensemble d'autorisations différent de ce que vous avez configuré précédemment pour déployer la machine virtuelle Connector.

Étapes

1. Sélectionnez la liste déroulante **Connector** et sélectionnez **Ajouter un connecteur**.



2. Choisissez **Microsoft Azure** comme fournisseur cloud.

3. Sur la page **déploiement d'un connecteur** :

a. Sous **Authentication**, sélectionnez l'option d'authentification qui correspond à la façon dont vous configurez les autorisations Azure :

- Sélectionnez **compte utilisateur Azure** pour vous connecter à votre compte Microsoft, qui doit disposer des autorisations requises.

Ce formulaire est détenu et hébergé par Microsoft. Vos identifiants ne sont pas fournis à NetApp.



Si vous êtes déjà connecté à un compte Azure, BlueXP utilisera automatiquement ce compte. Si vous avez plusieurs comptes, vous devrez peut-être vous déconnecter d'abord pour vous assurer que vous utilisez le bon compte.

- Sélectionnez **Active Directory service principal** pour saisir des informations sur le service principal Microsoft Entra qui accorde les autorisations requises :
 - ID de l'application (client)
 - ID du répertoire (locataire)
 - Secret client

[Apprenez à obtenir ces valeurs pour un principal de service.](#)

4. Suivez les étapes de l'assistant pour créer le connecteur :

- **VM Authentication** : choisissez un abonnement Azure, un emplacement, un nouveau groupe de ressources ou un groupe de ressources existant, puis choisissez une méthode d'authentification pour la machine virtuelle Connector que vous créez.

La méthode d'authentification de la machine virtuelle peut être un mot de passe ou une clé publique SSH.

["Découvrez comment vous connecter à une VM Linux dans Azure"](#)

- **Détails** : saisissez un nom pour l'instance, spécifiez les balises et choisissez si vous souhaitez que BlueXP crée un nouveau rôle avec les autorisations requises ou si vous souhaitez sélectionner un rôle existant avec lequel vous avez configuré ["les autorisations requises"](#).

Notez que vous pouvez choisir les abonnements Azure associés à ce rôle. Chaque abonnement que

vous choisissez fournit les autorisations de connecteur pour gérer les ressources de cet abonnement (par exemple, Cloud Volumes ONTAP).

- **Réseau** : choisissez un réseau VNet et un sous-réseau, si vous souhaitez activer une adresse IP publique, et spécifiez éventuellement une configuration proxy.
- **Groupe de sécurité** : choisissez de créer un nouveau groupe de sécurité ou de sélectionner un groupe de sécurité existant qui autorise les règles entrantes et sortantes requises.

["Afficher les règles des groupes de sécurité pour Azure"](#).

- **Review** : consultez vos sélections pour vérifier que votre configuration est correcte.

5. Cliquez sur **Ajouter**.

La machine virtuelle doit être prête en 7 minutes environ. Vous devez rester sur la page jusqu'à ce que le processus soit terminé.

Résultat

Une fois le processus terminé, le connecteur est disponible pour être utilisé depuis BlueXP.

Si vous disposez d'un stockage Azure Blob dans le même abonnement Azure que celui sur lequel vous avez créé le connecteur, un environnement de travail du stockage Azure Blob apparaît automatiquement sur le canevas BlueXP. ["Découvrez comment gérer le stockage Azure Blob à partir de BlueXP"](#)

Créez un connecteur à partir d'Azure Marketplace

Pour créer un connecteur à partir d'Azure Marketplace, vous devez configurer votre réseau, préparer les autorisations Azure, examiner les exigences d'instance, puis créer le connecteur.

Avant de commencer

Vous devriez passer en revue ["Limitations du connecteur"](#).

Étape 1 : configuration du réseau

Assurez-vous que l'emplacement réseau où vous prévoyez d'installer le connecteur prend en charge les exigences suivantes. En répondant à ces exigences, il peut gérer les ressources et les processus dans votre environnement de cloud hybride.

Région Azure

Si vous utilisez Cloud Volumes ONTAP, le connecteur doit être déployé dans la même région Azure que les systèmes Cloud Volumes ONTAP qu'il gère, ou dans le ["Paire de régions Azure"](#) Pour les systèmes Cloud Volumes ONTAP. Cette exigence garantit qu'une connexion Azure Private Link est utilisée entre Cloud Volumes ONTAP et les comptes de stockage associés.

["Découvrez comment Cloud Volumes ONTAP utilise une liaison privée Azure"](#)

Vnet et sous-réseau

Lorsque vous créez le connecteur, vous devez spécifier le réseau virtuel et le sous-réseau dans lesquels le connecteur doit résider.

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des environnements de travail. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement sur site.

Accès Internet sortant

L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante pour contacter des points finaux spécifiques.

Points d'extrémité contactés depuis le connecteur

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 pour les opérations quotidiennes.

Notez que les points finaux répertoriés ci-dessous sont tous des entrées CNAME.

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.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://support.netapp.com https://mysupport.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
https://*.api.blueexp.netapp.com https://api.blueexp.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.blueexp.netapp.com » dans une prochaine version.
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Pour mettre à niveau le connecteur et ses composants Docker.

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"](#)

Vous devrez implémenter cette exigence de mise en réseau après avoir créé le connecteur.

Étape 2 : passez en revue les exigences relatives aux ordinateurs virtuels

Lorsque vous créez le connecteur, vous devez choisir un type de machine virtuelle répondant aux exigences suivantes.

CPU

4 cœurs ou 4 CPU virtuels

RAM

14 GO

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.

Étape 3 : configurer les autorisations

Vous pouvez fournir des autorisations de l'une des manières suivantes :

- Option 1 : attribuez un rôle personnalisé à la machine virtuelle Azure en utilisant une identité gérée attribuée par le système.

- Option 2 : fournissez à BlueXP les identifiants d'un principal de service Azure qui possède les autorisations requises.

Procédez comme suit pour configurer des autorisations pour BlueXP.

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"](#)

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 du service

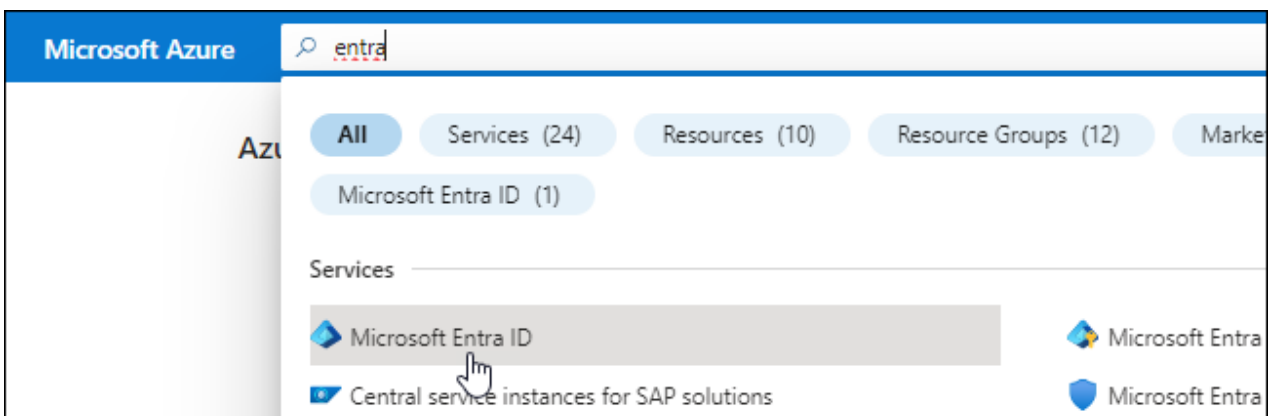
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont BlueXP a besoin.

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.



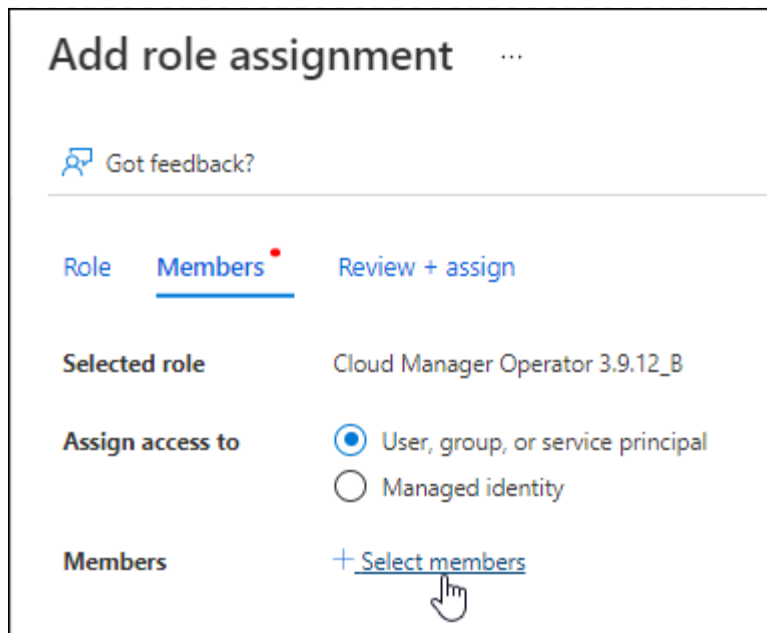
- Pour créer le rôle personnalisé, utilisez l'interface de ligne de commandes Azure :

```
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.

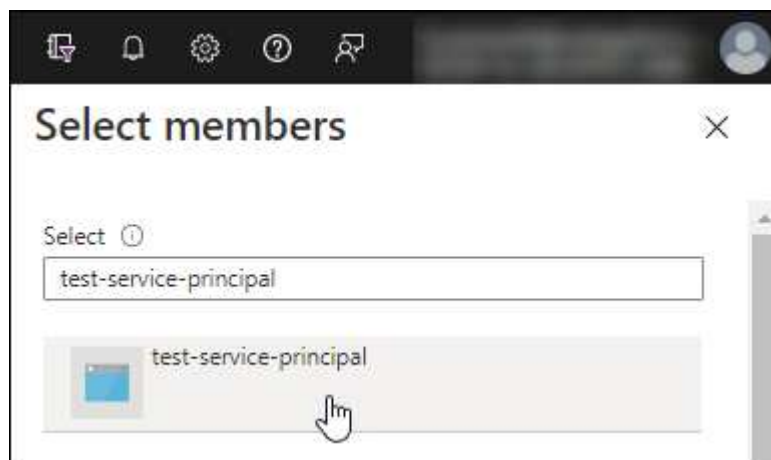
2. Attribuez l'application au rôle :

- À partir du portail Azure, ouvrez le service **abonnements**.
- Sélectionnez l'abonnement.
- Sélectionnez **contrôle d'accès (IAM) > Ajouter > Ajouter une affectation de rôle**.
- Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et sélectionnez **Next**.
- 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**.

Request API permissions

Select an API

Microsoft APIs [APIs my organization uses](#) [My APIs](#)

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export

Programmatic control of import/export jobs

Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights

Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

[< All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

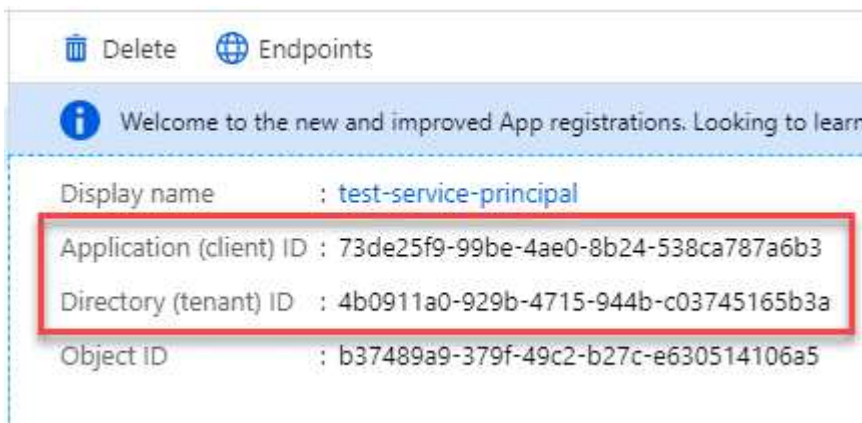


user_impersonation

Access Azure Service Management as organization users (preview)

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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.

Étape 4 : créer le connecteur

Lancez Connector directement à partir d'Azure Marketplace.

Description de la tâche

La création du connecteur à partir d'Azure Marketplace déploie une machine virtuelle dans Azure à l'aide d'une configuration par défaut. ["En savoir plus sur la configuration par défaut du connecteur"](#).

Avant de commencer

Vous devez disposer des éléments suivants :

- Un abonnement Azure.
- Un vnet et un sous-réseau dans votre région Azure de votre choix.
- Détails sur un serveur proxy, si votre organisation nécessite un proxy pour tout le trafic Internet sortant :
 - Adresse IP
 - Informations d'identification
 - Certificat HTTPS
- Une clé publique SSH, si vous souhaitez utiliser cette méthode d'authentification pour la machine virtuelle Connector. L'autre option de la méthode d'authentification est d'utiliser un mot de passe.

["Découvrez comment vous connecter à une VM Linux dans Azure"](#)

- Si vous ne souhaitez pas que BlueXP crée automatiquement un rôle Azure pour le connecteur, vous devrez créer votre propre rôle ["utilisation de la stratégie sur cette page"](#).

Ces autorisations sont pour l'instance de connecteur elle-même. Il s'agit d'un ensemble d'autorisations différent de ce que vous avez configuré précédemment pour déployer la machine virtuelle Connector.

Étapes

1. Rendez-vous sur la page NetApp Connector VM du Marketplace Azure.

["Page Azure Marketplace pour les régions commerciales"](#)

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.
- **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.

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.

5. Ouvrez un navigateur Web à partir d'un hôte connecté à la machine virtuelle Connector et entrez l'URL suivante :

`https://ipaddress`

6. Une fois connecté, configurez le connecteur :

- a. Spécifiez le compte BlueXP à associer au connecteur.
- b. Entrez un nom pour le système.
- c. Sous **exécutez-vous dans un environnement sécurisé ?** maintenez le mode restreint désactivé.

Vous devez désactiver le mode restreint, car ces étapes décrivent l'utilisation de BlueXP en mode standard. Vous devez activer le mode restreint uniquement si vous disposez d'un environnement sécurisé et souhaitez déconnecter ce compte des services back-end BlueXP. Si c'est le cas, ["Suivez les étapes pour démarrer avec BlueXP en mode restreint"](#).

- d. Sélectionnez **commençons**.

Résultat

Le connecteur est maintenant installé et configuré avec votre compte BlueXP.

Si vous disposez d'un stockage Azure Blob dans le même abonnement Azure que celui sur lequel vous avez créé le connecteur, un environnement de travail du stockage Azure Blob apparaît automatiquement sur le canevas BlueXP. ["Découvrez comment gérer le stockage Azure Blob à partir de BlueXP"](#)

Étape 5 : fournissez des autorisations à BlueXP

Maintenant que vous avez créé le connecteur, vous devez fournir à BlueXP les autorisations que vous avez précédemment configurées. Si vous disposez des autorisations requises, BlueXP peut gérer vos données et

votre infrastructure de stockage dans Azure.

Rôle personnalisé

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.

Et la suite ?

Accédez au ["Console BlueXP"](#) Pour commencer à utiliser le connecteur avec BlueXP.

Principal du service

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.

Installez manuellement le connecteur dans Azure

Pour installer manuellement le connecteur sur votre propre hôte Linux, vous devez vérifier la configuration requise pour l'hôte, configurer votre réseau, préparer les autorisations Azure, installer le connecteur, puis fournir les autorisations que vous avez préparées.

Avant de commencer

Vous devriez passer en revue "[Limitations du connecteur](#)".

Étape 1 : 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

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.

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 2 : configuration du réseau

Assurez-vous que l'emplacement réseau où vous prévoyez d'installer le connecteur prend en charge les exigences suivantes. En répondant à ces exigences, il peut gérer les ressources et les processus dans votre environnement de cloud hybride.

Région Azure

Si vous utilisez Cloud Volumes ONTAP, le connecteur doit être déployé dans la même région Azure que les systèmes Cloud Volumes ONTAP qu'il gère, ou dans le ["Paire de régions Azure"](#) Pour les systèmes Cloud Volumes ONTAP. Cette exigence garantit qu'une connexion Azure Private Link est utilisée entre Cloud Volumes ONTAP et les comptes de stockage associés.

["Découvrez comment Cloud Volumes ONTAP utilise une liaison privée Azure"](#)

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des environnements de travail. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement sur site.

Accès Internet sortant

L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante pour contacter des points finaux spécifiques.

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>

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.

Points d'extrémité contactés depuis le connecteur

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 pour les opérations quotidiennes.

Notez que les points finaux répertoriés ci-dessous sont tous des entrées CNAME.

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.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://support.netapp.com https://mysupport.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
https://*.api.blueexp.netapp.com https://api.blueexp.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.blueexp.netapp.com » dans une prochaine version.

Terminaux	Objectif
https://*.blob.core.windows.net	Pour mettre à niveau le connecteur et ses composants Docker.
https://cloudmanagerinfraprod.azurecr.io	

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"](#)

Étape 3 : configurer les autorisations

Vous devez fournir des autorisations Azure à BlueXP via l'une des options suivantes :

- Option 1 : attribuez un rôle personnalisé à la machine virtuelle Azure en utilisant une identité gérée attribuée par le système.
- Option 2 : fournissez à BlueXP les identifiants d'un principal de service Azure qui possède les autorisations requises.

Suivez les étapes pour préparer les autorisations pour BlueXP.

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"](#)

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.

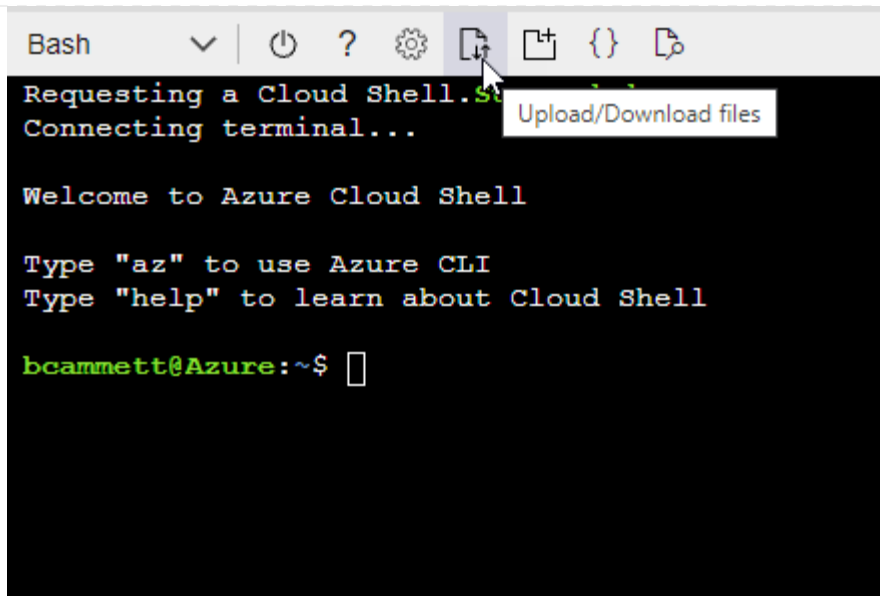
Exemple

```
"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 du service

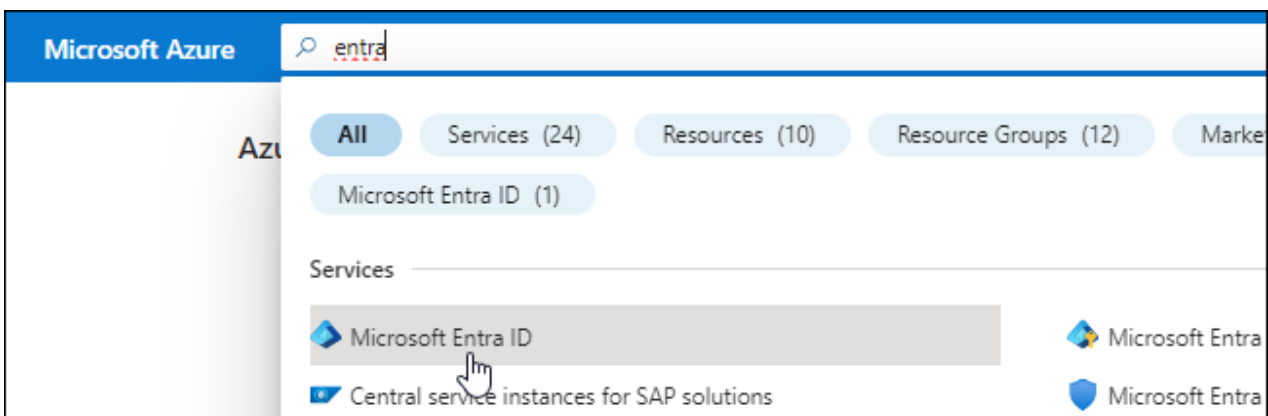
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont BlueXP a besoin.

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.

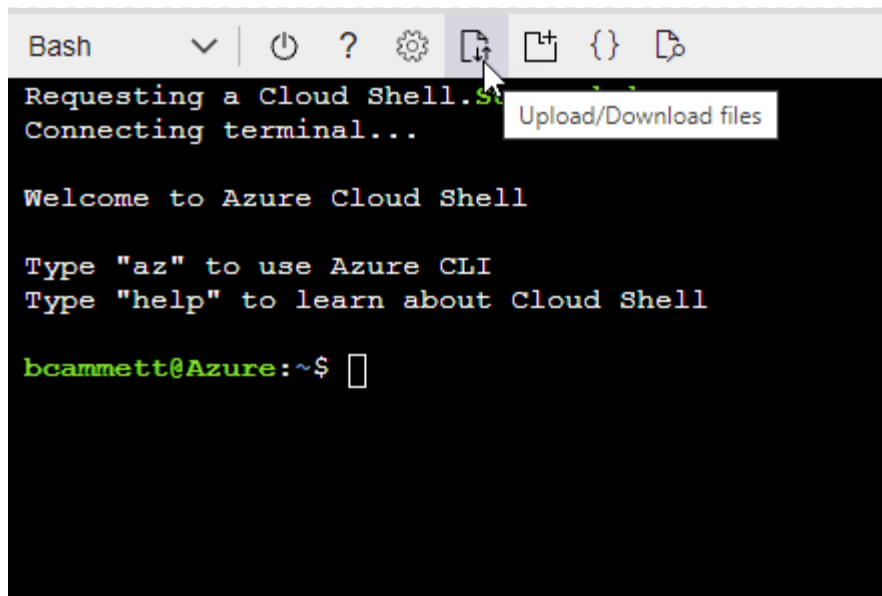
Exemple

```
"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.



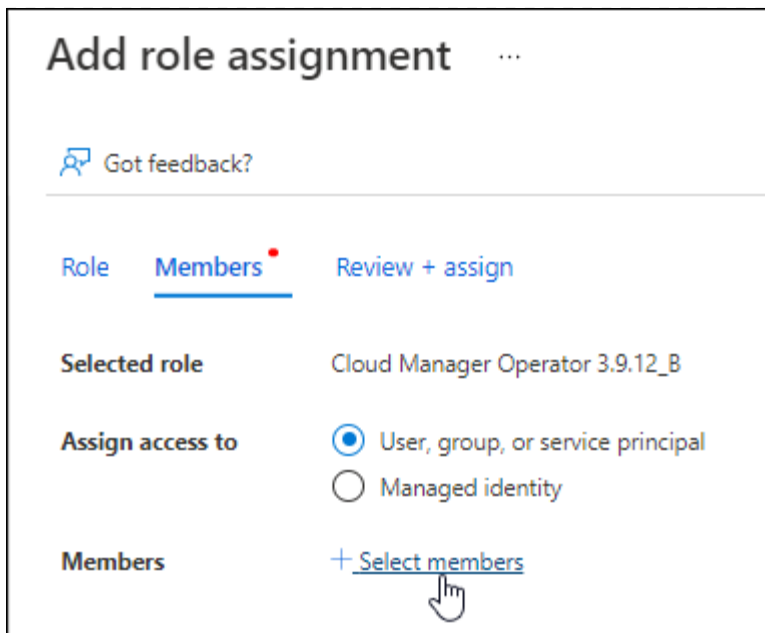
- Pour créer le rôle personnalisé, utilisez l'interface de ligne de commandes Azure :

```
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.

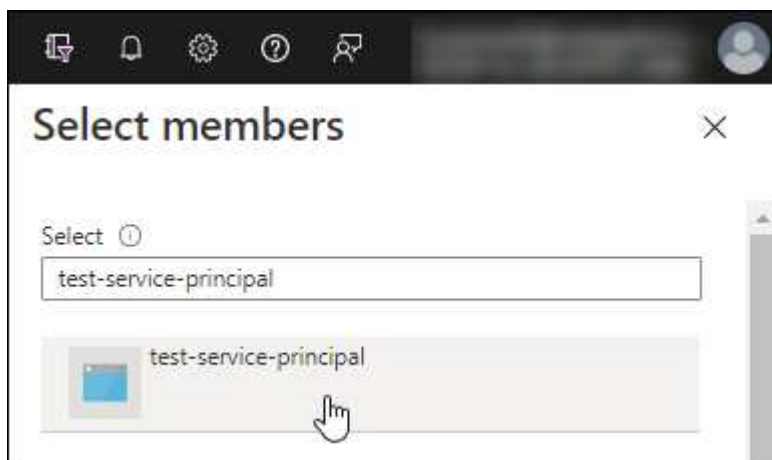
2. Attribuez l'application au rôle :

- À partir du portail Azure, ouvrez le service **abonnements**.
- Sélectionnez l'abonnement.
- Sélectionnez **contrôle d'accès (IAM) > Ajouter > Ajouter une affectation de rôle**.
- Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et sélectionnez **Next**.
- 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**.

Request API permissions

Select an API

Microsoft APIs [APIs my organization uses](#) [My APIs](#)

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export

Programmatic control of import/export jobs

Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights

Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

[← All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

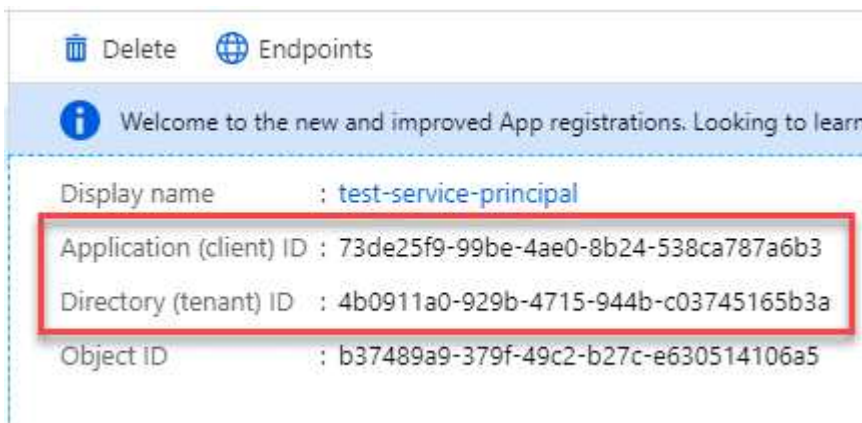


user_impersonation

Access Azure Service Management as organization users (preview)

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

+ New client secret

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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.

Étape 4 : installez le connecteur

Une fois la configuration requise terminée, vous pouvez installer manuellement le logiciel sur votre propre hôte Linux.

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.
- Identité gérée activée sur la machine virtuelle dans Azure, qui permet 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"](#)

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 contenant 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.

6. Attendez la fin de l'installation.

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

7. Ouvrez un navigateur Web à partir d'un hôte connecté à la machine virtuelle Connector et entrez l'URL suivante :

`https://ipaddress`

8. Une fois connecté, configurez le connecteur :

- Spécifiez le compte BlueXP à associer au connecteur.
- Entrez un nom pour le système.
- Sous **exécutez-vous dans un environnement sécurisé ?** maintenez le mode restreint désactivé.

Vous devez désactiver le mode restreint, car ces étapes décrivent l'utilisation de BlueXP en mode standard. Vous devez activer le mode restreint uniquement si vous disposez d'un environnement sécurisé et souhaitez déconnecter ce compte des services back-end BlueXP. Si c'est le cas, "[Suivez les étapes pour démarrer avec BlueXP en mode restreint](#)".

- Sélectionnez **commençons**.

Résultat

Le connecteur est maintenant installé et configuré avec votre compte BlueXP.

Si vous disposez d'un stockage Azure Blob dans le même abonnement Azure que celui sur lequel vous avez créé le connecteur, un environnement de travail du stockage Azure Blob apparaît automatiquement sur le canevas BlueXP. "[Découvrez comment gérer le stockage Azure Blob à partir de BlueXP](#)"

Étape 5 : fournissez des autorisations à BlueXP

Maintenant que vous avez installé le connecteur, vous devez fournir à BlueXP les autorisations Azure que vous avez précédemment configurées. Si vous disposez des autorisations requises, BlueXP peut gérer vos données et votre infrastructure de stockage dans Azure.

Rôle personnalisé

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.

Et la suite ?

Accédez au ["Console BlueXP"](#) Pour commencer à utiliser le connecteur avec BlueXP.

Principal du service

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.

Google Cloud

Options d'installation de Connector dans Google Cloud

Il existe plusieurs façons de créer un connecteur dans Google Cloud. La méthode la plus courante est d'accéder directement à BlueXP.

Les options d'installation suivantes sont disponibles :

- ["Créez le connecteur directement à partir de BlueXP"](#) (il s'agit de l'option standard)

Cette action lance une instance de serveur virtuel exécutant Linux et le logiciel Connector dans un VPC de votre choix.

- ["Créer le connecteur à l'aide de gcloud"](#)

Cette action lance également une instance de VM exécutant Linux et le logiciel Connector, mais le déploiement est initié directement depuis Google Cloud plutôt que depuis BlueXP.

- ["Téléchargez et installez manuellement le logiciel sur votre propre hôte Linux"](#)

L'option d'installation que vous choisissez a une incidence sur la préparation de l'installation. Vous pouvez notamment fournir à BlueXP les autorisations requises pour authentifier et gérer les ressources dans Google Cloud.

Créez un connecteur dans Google Cloud à partir de BlueXP ou gcloud

Pour créer un connecteur dans Google Cloud à partir de BlueXP ou à l'aide de gcloud, vous devez configurer votre réseau, préparer les autorisations Google Cloud, activer les API Google Cloud, puis créer le connecteur.

Avant de commencer

Vous devriez passer en revue ["Limitations du connecteur"](#).

Étape 1 : configuration du réseau

Configurez votre réseau de manière à ce que Connector puisse gérer les ressources et les processus dans votre environnement de cloud hybride. Par exemple, vous devez vous assurer que les connexions sont disponibles pour les réseaux cibles et que l'accès Internet sortant est disponible.

VPC et sous-réseau

Lorsque vous créez le connecteur, vous devez spécifier le VPC et le sous-réseau sur lesquels le connecteur doit résider.

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des environnements de travail. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement sur site.

Accès Internet sortant

L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante pour contacter des points finaux spécifiques.

Points d'extrémité contactés depuis le connecteur

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 pour les opérations quotidiennes.

Notez que les points finaux répertoriés ci-dessous sont tous des entrées CNAME.

Terminaux	Objectif
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.

Terminaux	Objectif
https://*.blob.core.windows.net	Pour mettre à niveau le connecteur et ses composants Docker.
https://cloudmanagerinfraprod.azurecr.io	

Terminaux contactés depuis la console BlueXP

Lorsque vous utilisez la console web BlueXP fournie via la couche SaaS, elle contacte plusieurs terminaux pour effectuer les tâches de gestion des données. Cela inclut les terminaux contactés pour déployer le connecteur à partir de la console BlueXP.

["Consultez la liste des terminaux contactés depuis la console BlueXP"](#).

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"](#)

Vous devrez implémenter cette exigence de mise en réseau après avoir créé le connecteur.

Étape 2 : définissez les autorisations nécessaires pour créer le connecteur

Avant de déployer un connecteur à partir de BlueXP ou à l'aide de gcloud, vous devez définir des autorisations pour l'utilisateur Google Cloud qui va déployer la VM Connector.

Étapes

1. Créez un rôle personnalisé dans Google Cloud :
 - a. Créez un fichier YAML qui inclut les autorisations suivantes :

```
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from
BlueXP
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
```

- `compute.subnetworks.get`
- `compute.subnetworks.list`
- `compute.zoneOperations.get`
- `compute.zones.get`
- `compute.zones.list`
- `deploymentmanager.compositeTypes.get`
- `deploymentmanager.compositeTypes.list`
- `deploymentmanager.deployments.create`
- `deploymentmanager.deployments.delete`
- `deploymentmanager.deployments.get`
- `deploymentmanager.deployments.list`
- `deploymentmanager.manifests.get`
- `deploymentmanager.manifests.list`
- `deploymentmanager.operations.get`
- `deploymentmanager.operations.list`
- `deploymentmanager.resources.get`
- `deploymentmanager.resources.list`
- `deploymentmanager.typeProviders.get`
- `deploymentmanager.typeProviders.list`
- `deploymentmanager.types.get`
- `deploymentmanager.types.list`
- `resourcemanager.projects.get`
- `compute.instances.setServiceAccount`
- `iam.serviceAccounts.list`

- b. Dans Google Cloud, activez le shell cloud.
- c. Téléchargez le fichier YAML qui inclut les autorisations requises.
- d. Créez un rôle personnalisé à l'aide de `gcloud iam roles create` commande.

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

Les rôles iam gcloud créent `connectDeployment --project=myproject --file=Connector-deployment.yaml`

["Documents Google Cloud : création et gestion de rôles personnalisés"](#)

2. Attribuez ce rôle personnalisé à l'utilisateur qui va déployer le connecteur à partir de BlueXP ou à l'aide de gcloud.

["Documents Google Cloud : attribuez un rôle unique"](#)

Résultat

L'utilisateur Google Cloud dispose désormais des autorisations nécessaires pour créer le connecteur.

Étape 3 : définissez les autorisations pour le connecteur

Un compte de service Google Cloud est requis pour fournir le connecteur avec les autorisations dont BlueXP a besoin pour gérer les ressources dans Google Cloud. Lorsque vous créez le connecteur, vous devez associer ce compte de service à la machine virtuelle Connector.

Étapes

1. Créez un rôle personnalisé dans Google Cloud :
 - a. Créez un fichier YAML qui inclut le contenu du ["Autorisations de compte de service pour le connecteur"](#).
 - b. Dans Google Cloud, activez le shell cloud.
 - c. Téléchargez le fichier YAML qui inclut les autorisations requises.
 - 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. Créer un compte de service dans Google Cloud et attribuer le rôle au compte de service :
 - 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"](#)

3. Si vous prévoyez de déployer des systèmes Cloud Volumes ONTAP dans différents projets que le projet sur lequel réside le connecteur, vous devrez fournir au compte de service du connecteur l'accès à ces projets.

Disons, par exemple, que le connecteur est dans le projet 1 et que vous voulez créer des systèmes Cloud Volumes ONTAP dans le projet 2. Vous devrez accorder l'accès au compte de service dans le projet 2.

- a. Dans le service IAM & Admin, sélectionnez le projet Google Cloud où vous souhaitez créer les systèmes Cloud Volumes ONTAP.
- b. Sur la page **IAM**, sélectionnez **accorder accès** et fournissez les détails nécessaires.
 - Saisissez l'e-mail du compte de service du connecteur.
 - Sélectionnez le rôle personnalisé du connecteur.
 - Sélectionnez **Enregistrer**.

Pour plus de détails, reportez-vous à ["Documentation Google Cloud"](#)

Résultat

Le compte de service de la machine virtuelle Connector est configuré.

Étape 4 : configuration des autorisations VPC partagées

Si vous utilisez un VPC partagé pour déployer des ressources dans un projet de service, vous devrez préparer vos autorisations.

Ce tableau est fourni à titre de référence et votre environnement doit refléter la table des autorisations lorsque la configuration IAM est terminée.

Afficher les autorisations VPC partagées

Identité	Créateur	Hébergé dans	Autorisations de projet de service	Autorisations de projet hôte	Objectif
Compte Google pour déployer le connecteur	Personnalisées	Projet de service	"Stratégie de déploiement de connecteur"	compute.network User	Déploiement du connecteur dans le projet de service
Connecteur de compte de service	Personnalisées	Projet de service	"Stratégie de compte de service de connecteur"	compute.network User deploymentmanager.editor	Déploiement et maintenance de Cloud Volumes ONTAP et des services dans le projet de service
Compte de service Cloud Volumes ONTAP	Personnalisées	Projet de service	storage.admin Membre: Compte de service BlueXP à partir de serviceAccount.user	S/O	(Facultatif) pour le Tiering des données et la sauvegarde et la restauration BlueXP
Agent de service Google API	Google Cloud	Projet de service	Editeur (par défaut)	compute.network User	Interagit avec les API Google Cloud pour le compte du déploiement. Permet à BlueXP d'utiliser le réseau partagé.
Compte de service par défaut Google Compute Engine	Google Cloud	Projet de service	Editeur (par défaut)	compute.network User	Déploie les instances Google Cloud et l'infrastructure de calcul pour le compte du déploiement. Permet à BlueXP d'utiliser le réseau partagé.

Remarques :

1. deploymentmanager.Editor est uniquement requis au niveau du projet hôte si vous ne passez pas de règles de pare-feu au déploiement et que vous choisissez de laisser BlueXP les créer pour vous. BlueXP créera un déploiement dans le projet hôte qui contient la règle de pare-feu VPC0 si aucune règle n'est spécifiée.
2. Firewall.create et firewall.delete ne sont nécessaires que si vous ne passez pas de règles de pare-feu au déploiement et que vous choisissez de laisser BlueXP les créer pour vous. Ces autorisations résident dans le fichier .yaml du compte BlueXP. Si vous déployez une paire HA à l'aide d'un VPC partagé, ces autorisations seront utilisées pour créer les règles de pare-feu pour VPC1, 2 et 3. Pour tous les autres déploiements, ces autorisations seront également utilisées pour créer des règles pour VPC0.

3. Pour le Tiering des données, le compte de service de Tiering doit avoir le rôle serviceAccount.user sur le compte de service, et pas seulement au niveau du projet. Actuellement, si vous attribuez serviceAccount.user au niveau du projet, les autorisations ne s'affichent pas lorsque vous interrogez le compte de service avec getIAMPolicy.

Étape 5 : activez les API Google Cloud

Vous devez activer plusieurs API Google Cloud avant de pouvoir déployer le connecteur et 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))

["Documentation Google Cloud : activation des API"](#)

Étape 6 : créer le connecteur

Créez un connecteur directement à partir de la console web BlueXP ou à l'aide de gcloud.

Description de la tâche

La création du connecteur déploie une instance de machine virtuelle dans Google Cloud à l'aide d'une configuration par défaut. Après avoir créé le connecteur, vous ne devez pas passer à une instance de machine virtuelle plus petite qui a moins de CPU ou de RAM. ["En savoir plus sur la configuration par défaut du connecteur"](#).

BlueXP

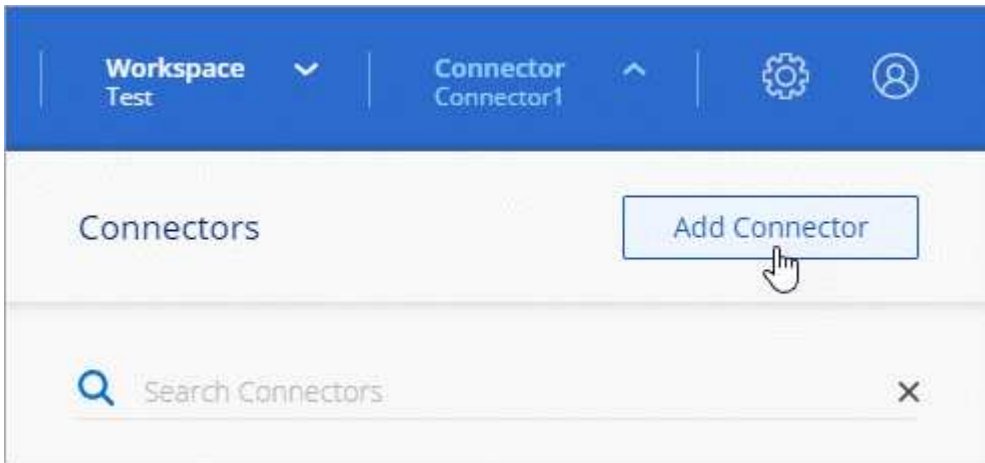
Avant de commencer

Vous devez disposer des éléments suivants :

- Les autorisations Google Cloud requises pour créer le connecteur et un compte de service pour la VM Connector.
- VPC et sous-réseau qui répondent aux exigences réseau.
- Détails sur un serveur proxy, si un proxy est requis pour accéder à Internet à partir du connecteur.

Étapes

1. Sélectionnez la liste déroulante **Connector** et sélectionnez **Ajouter un connecteur**.



2. Choisissez **Google Cloud Platform** comme fournisseur de cloud.
3. Sur la page **déploiement d'un connecteur**, consultez les détails de ce dont vous aurez besoin. Vous avez deux options :
 - a. Sélectionnez **Continuer** pour préparer le déploiement à l'aide du guide produit. Chaque étape du guide du produit inclut les informations contenues sur cette page de la documentation.
 - b. Sélectionnez **passer au déploiement** si vous êtes déjà préparé en suivant les étapes de cette page.
4. Suivez les étapes de l'assistant pour créer le connecteur :
 - Si vous y êtes invité, connectez-vous à votre compte Google, qui devrait disposer des autorisations requises pour créer l'instance de machine virtuelle.

Le formulaire est détenu et hébergé par Google. Vos identifiants ne sont pas fournis à NetApp.

- **Détails** : saisissez un nom pour l'instance de machine virtuelle, spécifiez des balises, sélectionnez un projet, puis sélectionnez le compte de service qui dispose des autorisations requises (reportez-vous à la section ci-dessus pour plus de détails).
- **Location** : spécifiez une région, une zone, un VPC et un sous-réseau pour l'instance.
- **Réseau** : permet d'activer ou non une adresse IP publique et de spécifier éventuellement une configuration proxy.
- **Stratégie de pare-feu** : choisissez de créer une nouvelle politique de pare-feu ou de sélectionner une politique de pare-feu existante qui autorise les règles entrantes et sortantes requises.

"Règles de pare-feu dans Google Cloud"

- **Review** : consultez vos sélections pour vérifier que votre configuration est correcte.

5. Sélectionnez **Ajouter**.

L'instance doit être prête dans environ 7 minutes. Vous devez rester sur la page jusqu'à ce que le processus soit terminé.

Résultat

Une fois le processus terminé, le connecteur est disponible pour être utilisé depuis BlueXP.

Si vous avez des compartiments Google Cloud Storage dans le même compte Google Cloud où vous avez créé le connecteur, un environnement de travail Google Cloud Storage s'affiche automatiquement sur le canevas BlueXP. ["Découvrez comment gérer le stockage Google Cloud à partir de BlueXP"](#)

gcloud

Avant de commencer

Vous devez disposer des éléments suivants :

- Les autorisations Google Cloud requises pour créer le connecteur et un compte de service pour la VM Connector.
- VPC et sous-réseau qui répondent aux exigences réseau.
- Compréhension des exigences des instances VM.
 - **CPU** : 4 cœurs ou 4 vCPU
 - **RAM**: 14 GO
 - **Type de machine**: Nous recommandons n2-standard-4.

Le connecteur est pris en charge dans Google Cloud sur une instance de machine virtuelle avec un système d'exploitation qui prend en charge les fonctionnalités de machine virtuelle blindée.

Étapes

1. Connectez-vous au SDK gcloud à l'aide de la méthodologie que vous préférez.

Dans nos exemples, nous allons utiliser un shell local avec le SDK gcloud installé, mais vous pouvez utiliser le Google Cloud Shell natif dans la console Google Cloud.

Pour plus d'informations sur le kit de développement logiciel Google Cloud, rendez-vous sur le ["Page de documentation du SDK Google Cloud"](#).

2. Vérifiez que vous êtes connecté en tant qu'utilisateur disposant des autorisations requises définies dans la section ci-dessus :

```
gcloud auth list
```

Le résultat doit indiquer les éléments suivants où le compte d'utilisateur * est le compte d'utilisateur souhaité pour être connecté en tant que :

Credentialed Accounts

ACTIVE ACCOUNT

some_user_account@domain.com

* desired_user_account@domain.com

To set the active account, run:

```
$ gcloud config set account `ACCOUNT`
```

Updates are available for some Cloud SDK components. To install them,

please run:

```
$ gcloud components update
```

3. Exécutez le `gcloud compute instances create` commande :

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-4
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

nom de l'instance

Nom d'instance souhaité pour l'instance de VM.

projet

(Facultatif) le projet où vous souhaitez déployer la machine virtuelle.

compte de service

Compte de service spécifié dans la sortie de l'étape 2.

zone

La zone où vous souhaitez déployer la machine virtuelle

pas d'adresse

(Facultatif) aucune adresse IP externe n'est utilisée (vous avez besoin d'un NAT ou d'un proxy cloud pour acheminer le trafic vers l'Internet public)

balise réseau

(Facultatif) Ajouter un marquage réseau pour lier une règle de pare-feu à l'aide de balises à l'instance de connecteur

chemin du réseau

(Facultatif) Ajoutez le nom du réseau dans lequel déployer le connecteur (pour un VPC partagé, vous avez besoin du chemin complet)

chemin-sous-réseau

(Facultatif) Ajouter le nom du sous-réseau dans lequel déployer le connecteur (pour un VPC partagé, vous devez disposer du chemin complet)

km-key-path

(Facultatif) Ajouter une clé KMS pour chiffrer les disques du connecteur (les autorisations IAM doivent également être appliquées)

Pour plus d'informations sur ces indicateurs, visitez le ["Documentation du kit de développement logiciel de calcul Google Cloud"](#).

+

L'exécution de la commande déploie le connecteur à l'aide de l'image de référence NetApp. L'instance de connecteur et le logiciel doivent s'exécuter dans environ cinq minutes.

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

`https://ipaddress`

2. Une fois connecté, configurez le connecteur :
 - a. Spécifiez le compte BlueXP à associer au connecteur.

["Découvrez les comptes BlueXP"](#).

- b. Entrez un nom pour le système.

Résultat

Le connecteur est maintenant installé et configuré avec votre compte BlueXP.

Ouvrez un navigateur Web et accédez au ["Console BlueXP"](#) Pour commencer à utiliser le connecteur avec BlueXP.

Installez manuellement le connecteur dans Google Cloud

Pour installer manuellement le connecteur sur votre propre hôte Linux, vous devez vérifier la configuration requise pour l'hôte, configurer votre réseau, préparer les autorisations Google Cloud, activer les API Google Cloud, installer le connecteur, puis fournir les autorisations que vous avez préparées.

Avant de commencer

Vous devriez passer en revue ["Limitations du connecteur"](#).

Étape 1 : 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 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 2 : configuration du réseau

Configurez votre réseau de manière à ce que Connector puisse gérer les ressources et les processus dans votre environnement de cloud hybride. Par exemple, vous devez vous assurer que les connexions sont disponibles pour les réseaux cibles et que l'accès Internet sortant est disponible.

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des environnements de travail. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement sur site.

Accès Internet sortant

L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante pour contacter des points finaux spécifiques.

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://cloudmanagerinfraproduct.azurecr.io>

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.

Points d'extrémité contactés depuis le connecteur

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 pour les opérations quotidiennes.

Notez que les points finaux répertoriés ci-dessous sont tous des entrées CNAME.

Terminaux	Objectif
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.

Terminaux	Objectif
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.blueexp.netapp.com https://api.blueexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	<p>Pour fournir des fonctions et des services SaaS dans BlueXP.</p> <p>Notez que le connecteur est actuellement en contact avec « cloudmanager.cloud.netapp.com », mais il commencera à contacter « api.blueexp.netapp.com » dans une prochaine version.</p>
https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	Pour mettre à niveau le connecteur et ses composants Docker.

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"](#)

Étape 3 : définissez les autorisations pour le connecteur

Un compte de service Google Cloud est requis pour fournir le connecteur avec les autorisations dont BlueXP a besoin pour gérer les ressources dans Google Cloud. Lorsque vous créez le connecteur, vous devez associer ce compte de service à la machine virtuelle Connector.

Étapes

1. Créez un rôle personnalisé dans Google Cloud :

- a. Créez un fichier YAML qui inclut le contenu du ["Autorisations de compte de service pour le connecteur"](#).
- b. Dans Google Cloud, activez le shell cloud.
- c. Téléchargez le fichier YAML qui inclut les autorisations requises.
- 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. Créer un compte de service dans Google Cloud et attribuer le rôle au compte de service :

- 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"](#)

3. Si vous prévoyez de déployer des systèmes Cloud Volumes ONTAP dans différents projets que le projet sur lequel réside le connecteur, vous devrez fournir au compte de service du connecteur l'accès à ces projets.

Disons, par exemple, que le connecteur est dans le projet 1 et que vous voulez créer des systèmes Cloud Volumes ONTAP dans le projet 2. Vous devrez accorder l'accès au compte de service dans le projet 2.

- a. Dans le service IAM & Admin, sélectionnez le projet Google Cloud où vous souhaitez créer les systèmes Cloud Volumes ONTAP.
- b. Sur la page **IAM**, sélectionnez **accorder accès** et fournissez les détails nécessaires.
 - Saisissez l'e-mail du compte de service du connecteur.
 - Sélectionnez le rôle personnalisé du connecteur.
 - Sélectionnez **Enregistrer**.

Pour plus de détails, reportez-vous à ["Documentation Google Cloud"](#)

Résultat

Le compte de service de la machine virtuelle Connector est configuré.

Étape 4 : configuration des autorisations VPC partagées

Si vous utilisez un VPC partagé pour déployer des ressources dans un projet de service, vous devrez préparer vos autorisations.

Ce tableau est fourni à titre de référence et votre environnement doit refléter la table des autorisations lorsque la configuration IAM est terminée.

Afficher les autorisations VPC partagées

Identité	Créateur	Hébergé dans	Autorisations de projet de service	Autorisations de projet hôte	Objectif
Compte Google pour déployer le connecteur	Personnalisées	Projet de service	"Stratégie de déploiement de connecteur"	compute.network User	Déploiement du connecteur dans le projet de service
Connecteur de compte de service	Personnalisées	Projet de service	"Stratégie de compte de service de connecteur"	compute.network User deploymentmanager.editor	Déploiement et maintenance de Cloud Volumes ONTAP et des services dans le projet de service
Compte de service Cloud Volumes ONTAP	Personnalisées	Projet de service	storage.admin Membre: Compte de service BlueXP à partir de serviceAccount.user	S/O	(Facultatif) pour le Tiering des données et la sauvegarde et la restauration BlueXP
Agent de service Google API	Google Cloud	Projet de service	Editeur (par défaut)	compute.network User	Interagit avec les API Google Cloud pour le compte du déploiement. Permet à BlueXP d'utiliser le réseau partagé.
Compte de service par défaut Google Compute Engine	Google Cloud	Projet de service	Editeur (par défaut)	compute.network User	Déploie les instances Google Cloud et l'infrastructure de calcul pour le compte du déploiement. Permet à BlueXP d'utiliser le réseau partagé.

Remarques :

1. deploymentmanager.Editor est uniquement requis au niveau du projet hôte si vous ne passez pas de règles de pare-feu au déploiement et que vous choisissez de laisser BlueXP les créer pour vous. BlueXP créera un déploiement dans le projet hôte qui contient la règle de pare-feu VPC0 si aucune règle n'est spécifiée.
2. Firewall.create et firewall.delete ne sont nécessaires que si vous ne passez pas de règles de pare-feu au déploiement et que vous choisissez de laisser BlueXP les créer pour vous. Ces autorisations résident dans le fichier .yaml du compte BlueXP. Si vous déployez une paire HA à l'aide d'un VPC partagé, ces autorisations seront utilisées pour créer les règles de pare-feu pour VPC1, 2 et 3. Pour tous les autres déploiements, ces autorisations seront également utilisées pour créer des règles pour VPC0.

3. Pour le Tiering des données, le compte de service de Tiering doit avoir le rôle `serviceAccount.user` sur le compte de service, et pas seulement au niveau du projet. Actuellement, si vous attribuez `serviceAccount.user` au niveau du projet, les autorisations ne s'affichent pas lorsque vous interrogez le compte de service avec `getIAMPolicy`.

Étape 5 : activez les API Google Cloud

Vous devez activer plusieurs API Google Cloud avant de pouvoir déployer les systèmes 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))

["Documentation Google Cloud : activation des API"](#)

Étape 6 : installez le connecteur

Une fois la configuration requise terminée, vous pouvez installer manuellement le logiciel sur votre propre hôte Linux.

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 contenant 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.

6. Attendez la fin de l'installation.

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

7. Ouvrez un navigateur Web à partir d'un hôte connecté à la machine virtuelle Connector et entrez l'URL suivante :

`https://ipaddress`

8. Une fois connecté, configurez le connecteur :

- Spécifiez le compte BlueXP à associer au connecteur.
- Entrez un nom pour le système.
- Sous **exécutez-vous dans un environnement sécurisé ?** maintenez le mode restreint désactivé.

Vous devez désactiver le mode restreint, car ces étapes décrivent l'utilisation de BlueXP en mode standard. Vous devez activer le mode restreint uniquement si vous disposez d'un environnement sécurisé et souhaitez déconnecter ce compte des services back-end BlueXP. Si c'est le cas, "[Suivez les étapes pour démarrer avec BlueXP en mode restreint](#)".

- Sélectionnez **commençons**.

Résultat

Le connecteur est maintenant installé et configuré avec votre compte BlueXP.

Si vous avez des compartiments Google Cloud Storage dans le même compte Google Cloud où vous avez créé le connecteur, un environnement de travail Google Cloud Storage s'affiche automatiquement sur le canevas BlueXP. "[Découvrez comment gérer le stockage Google Cloud à partir de BlueXP](#)"

Étape 7 : fournissez des autorisations à BlueXP

Vous devez fournir à BlueXP les autorisations Google Cloud que vous avez précédemment configurées. Si vous disposez des autorisations requises, BlueXP peut gérer vos données et votre infrastructure de stockage dans Google Cloud.

Étapes

- 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 Google Cloud, autorisez 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.

Installez et configurez un connecteur sur site

Installez un connecteur sur site, puis connectez-vous et configurez-le pour qu'il fonctionne avec votre compte BlueXP.

Avant de commencer

Vous devriez passer en revue "[Limitations du connecteur](#)".

Étape 1 : 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. Assurez-vous que votre hôte répond à ces exigences avant d'installer le connecteur.

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

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 2 : configuration du réseau

Configurez votre réseau de manière à ce que Connector puisse gérer les ressources et les processus dans votre environnement de cloud hybride. Par exemple, vous devez vous assurer que les connexions sont disponibles pour les réseaux cibles et que l'accès Internet sortant est disponible.

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des environnements de travail. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement sur site.

Accès Internet sortant

L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante pour contacter des points finaux spécifiques.

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>

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.

Points d'extrémité contactés depuis le connecteur

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 pour les opérations quotidiennes.

Notez que les points finaux répertoriés ci-dessous sont tous des entrées CNAME.

Terminaux	Objectif
Services AWS (amazonaws.com): <ul style="list-style-type: none"> • 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"
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.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.blueexp.netapp.com https://api.blueexp.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.blueexp.netapp.com » dans une prochaine version.

Terminaux	Objectif
https://*.blob.core.windows.net	Pour mettre à niveau le connecteur et ses composants Docker.
https://cloudmanagerinfraprod.azurecr.io	

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"](#)

Étape 3 : configurez les autorisations cloud

Si vous souhaitez utiliser les services BlueXP dans AWS ou Azure avec un connecteur sur site, vous devez configurer des autorisations dans votre fournisseur cloud afin de pouvoir ajouter les informations d'identification au connecteur une fois que vous l'avez installé.



Pourquoi ne pas Google Cloud ? Une fois le connecteur installé sur votre site, il ne peut pas gérer vos ressources dans Google Cloud. Le connecteur doit être installé dans Google Cloud pour gérer toutes les ressources qui y résident.

AWS

Lorsque le connecteur est installé sur site, vous devez fournir BlueXP avec des autorisations AWS en ajoutant des clés d'accès à un utilisateur IAM qui dispose des autorisations requises.

Vous devez utiliser cette méthode d'authentification si le connecteur est installé sur site. Vous ne pouvez pas utiliser de rôle IAM.

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

Vous devez maintenant disposer des clés d'accès pour un utilisateur IAM qui dispose des autorisations requises. Après avoir installé le connecteur, vous devez associer ces informations d'identification au connecteur de BlueXP.

Azure

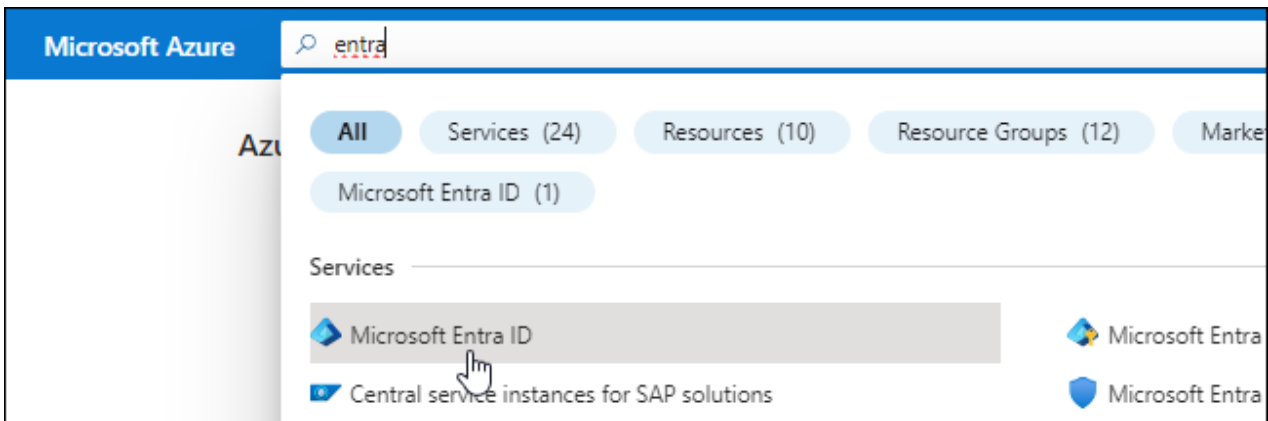
Lorsque le connecteur est installé sur site, vous devez fournir BlueXP avec des autorisations Azure en configurant une entité de service dans Microsoft Entra ID et en obtenant les identifiants Azure requis par BlueXP.

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.

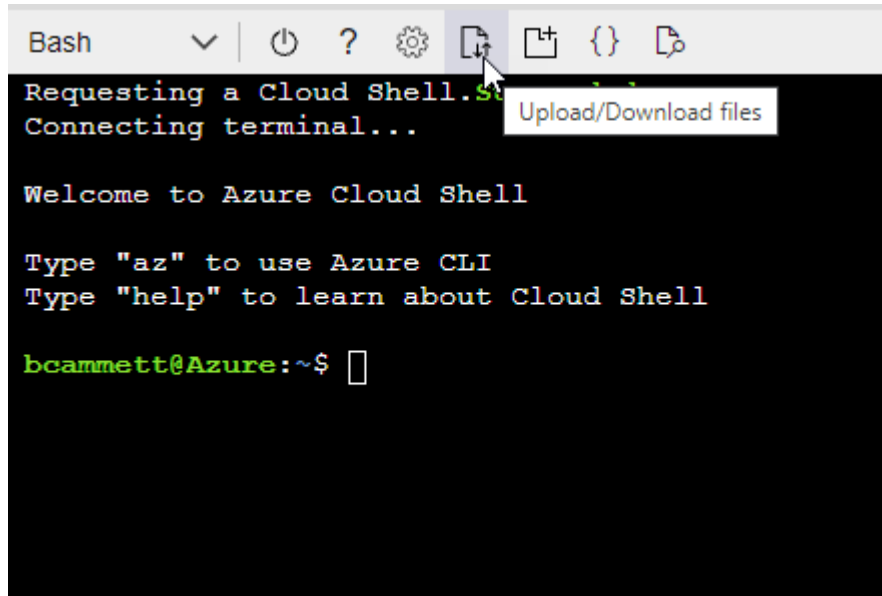
Exemple

```
"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.



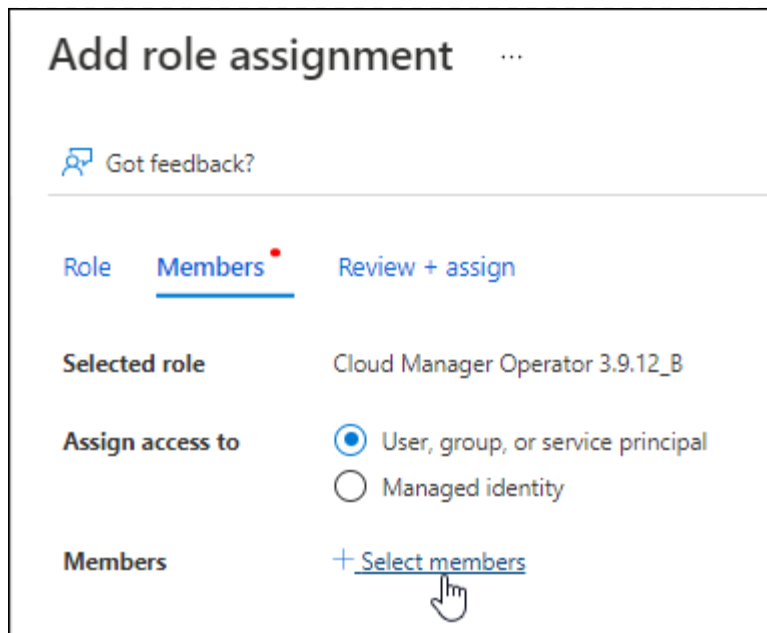
- Pour créer le rôle personnalisé, utilisez l'interface de ligne de commandes Azure :

```
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.

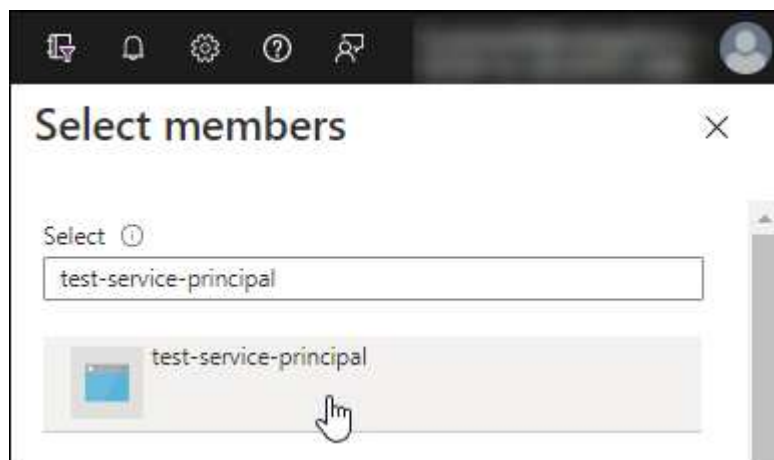
2. Attribuez l'application au rôle :

- À partir du portail Azure, ouvrez le service **abonnements**.
- Sélectionnez l'abonnement.
- Sélectionnez **contrôle d'accès (IAM) > Ajouter > Ajouter une affectation de rôle**.
- Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et sélectionnez **Next**.
- 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**.

Request API permissions

Select an API

Microsoft APIs [APIs my organization uses](#) [My APIs](#)

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export

Programmatic control of import/export jobs

Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

Customer Insights

Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

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

Request API permissions

[< All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

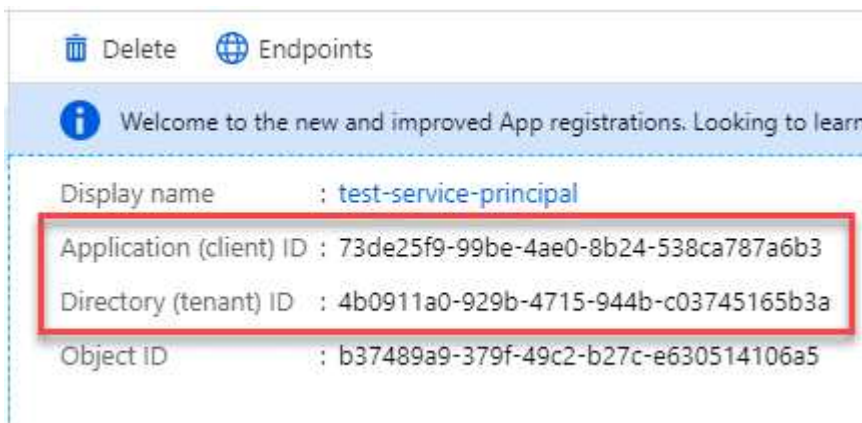


user_impersonation

Access Azure Service Management as organization users (preview)

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.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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. Après avoir installé le connecteur, vous devez associer ces informations d'identification au connecteur de BlueXP.

Étape 4 : installez le connecteur

Téléchargez et installez le logiciel Connector sur un hôte Linux existant sur site.

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 contenant 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.

Étape 5 : configurer le connecteur

Inscrivez-vous ou connectez-vous, puis configurez le connecteur pour qu'il fonctionne avec votre compte BlueXP.

Étapes

1. Ouvrez un navigateur Web et entrez l'URL suivante :

`https://ipaddress`

Ipaddress peut être localhost, une adresse IP privée ou une adresse IP publique, selon la configuration de l'hôte. Par exemple, si le connecteur est dans le Cloud public sans adresse IP publique, vous devez entrer une adresse IP privée à partir d'un hôte qui a une connexion à l'hôte du connecteur.

2. S'inscrire ou se connecter.
3. Une fois connecté, configurez BlueXP :
 - a. Spécifiez le compte BlueXP à associer au connecteur.
 - b. Entrez un nom pour le système.
 - c. Sous **exécutez-vous dans un environnement sécurisé ?** maintenez le mode restreint désactivé.

Vous devez désactiver le mode restreint, car ces étapes décrivent l'utilisation de BlueXP en mode standard. (En outre, le mode restreint n'est pas pris en charge lorsque le connecteur est installé sur site.)

- d. Sélectionnez **commençons**.

Résultat

BlueXP est maintenant configuré avec le connecteur que vous venez d'installer.

Étape 6 : fournissez des autorisations à BlueXP

Une fois que vous avez installé et configuré le connecteur, ajoutez vos identifiants cloud afin que BlueXP dispose des autorisations requises pour effectuer des actions dans AWS ou Azure.

AWS

Avant de commencer

Si vous venez de créer ces identifiants dans AWS, leur utilisation peut prendre quelques minutes. Attendez quelques minutes avant d'ajouter les informations d'identification à BlueXP.

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.

Vous pouvez maintenant accéder au "[Console BlueXP](#)" Pour commencer à utiliser le connecteur avec BlueXP.

Azure

Avant de commencer

Si vous venez de créer ces identifiants dans Azure, leur mise à disposition peut prendre quelques minutes. Attendez quelques minutes avant d'ajouter les informations d'identification à BlueXP.

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. Vous pouvez maintenant accéder au "[Console BlueXP](#)" Pour commencer à utiliser le connecteur avec BlueXP.

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.