



Configurer un connecteur

Set up and administration

NetApp

December 15, 2022

Table des matières

- Configurer un connecteur 1
 - En savoir plus sur les connecteurs 1
 - Créez un connecteur dans AWS à partir de BlueXP 5
 - Créez un connecteur dans Azure à partir de BlueXP 11
 - Créez un connecteur dans Google Cloud à partir de BlueXP 28
 - Créer un connecteur dans une région gouvernementale 41

Configurer un connecteur

En savoir plus sur les connecteurs

Dans la plupart des cas, un administrateur de compte BlueXP devra déployer un *Connector* dans votre réseau cloud ou sur site. Le connecteur est un composant essentiel pour l'utilisation quotidienne de BlueXP. BlueXP peut ainsi gérer les ressources et les processus dans votre environnement de cloud public.

Lorsqu'un connecteur est nécessaire

Un connecteur est nécessaire pour utiliser de nombreuses fonctionnalités et services dans BlueXP.

Administratifs

- Fonctions de gestion d'Amazon FSX pour ONTAP
- Découverte Amazon S3
- Découverte d'Azure Blob
- La sauvegarde dans le cloud
- Sens des données cloud
- Tiering dans le cloud
- Cloud Volumes ONTAP
- Systèmes E-Series
- Cache global de fichiers
- Découverte de Google Cloud Storage
- Clusters Kubernetes
- Clusters ONTAP sur site
- StorageGRID

Un connecteur est requis **NOT** pour les services suivants :

- Conseiller digital
- La création d'un environnement de travail Amazon FSX pour ONTAP même si un connecteur n'est pas nécessaire pour créer un environnement de travail, il est nécessaire de créer et de gérer des volumes, de répliquer des données et d'intégrer FSX pour ONTAP avec les services cloud NetApp, tels que Data Sense et Cloud Sync.
- Azure NetApp Files

Même si un connecteur n'est pas nécessaire pour configurer et gérer Azure NetApp Files, il est nécessaire d'utiliser un connecteur si vous souhaitez analyser les données Azure NetApp Files avec Cloud Data SENSE.

- Cloud Volumes Service pour Google Cloud
- Cloud Sync

Portefeuille numérique

Dans presque tous les cas, vous pouvez ajouter une licence au porte-monnaie numérique sans connecteur.

La seule fois qu'un connecteur est nécessaire pour ajouter une licence au porte-monnaie numérique est pour les licences Cloud Volumes ONTAP *node-based*. Dans ce cas, un connecteur est requis car les données sont extraites des licences installées sur les systèmes Cloud Volumes ONTAP.

Emplacements pris en charge

Un connecteur est pris en charge aux emplacements suivants :

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- Sur site
- Sur place, sans accès à Internet

Remarque sur les déploiements Azure

Si vous déployez le connecteur dans Azure, il 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"](#).

Remarque sur les déploiements Google Cloud

Pour créer un système Cloud Volumes ONTAP dans Google Cloud, vous devez disposer d'un connecteur exécuté dans Google Cloud. Vous ne pouvez pas utiliser un connecteur exécuté sur AWS, Azure ou sur site.

Les connecteurs doivent rester en fonctionnement

Un connecteur doit rester en fonctionnement en permanence. Il est important pour la santé et le fonctionnement continus des services que vous proposez.

Par exemple, un connecteur est un composant clé de la santé et du fonctionnement de Cloud Volumes ONTAP. Si un connecteur est hors tension, les systèmes Cloud Volumes ONTAP PAYGO et les systèmes BYOL basés sur la capacité sont arrêtés après avoir perdu la communication avec un connecteur pendant plus de 14 jours. Cela se produit car le connecteur actualise les licences du système chaque jour.



Si votre système Cloud Volumes ONTAP dispose d'une licence BYOL basée sur des nœuds, le système reste opérationnel au bout de 14 jours, car la licence est installée sur le système Cloud Volumes ONTAP.

Comment créer un connecteur

Un administrateur de compte BlueXP peut créer un connecteur de différentes façons :

- Directement depuis BlueXP (recommandé)
 - ["Création dans AWS"](#)

- ["Création dans Azure"](#)
- ["Création dans GCP"](#)
- En installant manuellement le logiciel sur votre propre hôte Linux
 - ["Sur un hôte ayant accès à Internet"](#)
 - ["Sur un hôte sur site qui ne dispose pas d'un accès Internet"](#)
- Sur le marché de votre fournisseur cloud
 - ["AWS Marketplace"](#)
 - ["Azure Marketplace"](#)

Si vous travaillez dans une région gouvernementale, vous devez déployer un connecteur à partir du marché de votre fournisseur de cloud ou installer manuellement le logiciel Connector sur un hôte Linux existant. Vous ne pouvez pas déployer le connecteur dans une région gouvernementale à partir du site Web SaaS de BlueXP.

Autorisations

Des autorisations spécifiques sont nécessaires pour créer le connecteur et un autre ensemble d'autorisations est nécessaire pour l'instance de connecteur elle-même.

Autorisations pour créer un connecteur

L'utilisateur qui crée un connecteur depuis BlueXP a besoin d'autorisations spécifiques pour déployer l'instance dans le fournisseur de cloud de votre choix.

- ["Affichez les autorisations AWS requises"](#)
- ["Affichez les autorisations Azure requises"](#)
- ["Affichez les autorisations Google Cloud requises"](#)

Autorisations pour l'instance de connecteur

Le connecteur nécessite des autorisations spécifiques de fournisseurs cloud pour effectuer des opérations en votre nom. Par exemple, pour déployer et gérer Cloud Volumes ONTAP.

Lorsque vous créez un connecteur directement à partir de BlueXP, BlueXP crée le connecteur avec les autorisations dont il a besoin. Vous n'avez rien à faire.

Si vous créez vous-même le connecteur à partir d'AWS Marketplace, d'Azure Marketplace ou d'une installation manuelle du logiciel, vous devez vous assurer que les autorisations appropriées sont en place.

- ["Découvrez comment Connector utilise les autorisations AWS"](#)
- ["Découvrez comment le connecteur utilise les autorisations Azure"](#)
- ["Découvrez comment Connector utilise les autorisations Google Cloud"](#)

Mises à niveau des connecteurs

Nous mettons généralement à jour le logiciel de connecteur chaque mois pour introduire de nouvelles fonctions et améliorer la stabilité. Bien que la plupart des services et fonctionnalités de la plate-forme BlueXP soient proposés par le logiciel SaaS, quelques fonctionnalités dépendent de la version du connecteur. Qui inclut la gestion Cloud Volumes ONTAP, la gestion de clusters ONTAP sur site, la configuration et l'aide.

Le connecteur met automatiquement à jour son logiciel avec la dernière version, tant qu'il dispose d'un accès Internet sortant pour obtenir la mise à jour du logiciel.

Nombre d'environnements de travail par connecteur

Un connecteur peut gérer plusieurs environnements de travail dans BlueXP. Le nombre maximum d'environnements de travail qu'un seul connecteur doit gérer varie. Cela dépend du type d'environnements de travail, du nombre de volumes, de la capacité gérée et du nombre d'utilisateurs.

Si vous disposez d'un déploiement à grande échelle, contactez votre représentant NetApp pour dimensionner votre environnement. Si vous rencontrez des problèmes pendant le trajet, contactez-nous en utilisant le chat produit.

Quand utiliser plusieurs connecteurs

Dans certains cas, vous n'avez peut-être besoin que d'un seul connecteur, mais vous pourriez avoir besoin de deux connecteurs ou plus.

Voici quelques exemples :

- Vous utilisez un environnement multcloud (AWS et Azure), c'est pourquoi vous avez un connecteur dans AWS et un autre dans Azure. Chacun gère les systèmes Cloud Volumes ONTAP exécutés dans ces environnements.
- Un fournisseur de services peut utiliser un seul compte NetApp pour fournir des services à ses clients, tout en utilisant un autre compte pour assurer la reprise après incident de l'une de ses unités commerciales. Chaque compte aurait des connecteurs distincts.

Utilisation de plusieurs connecteurs avec le même environnement de travail

Vous pouvez gérer un environnement de travail à l'aide de plusieurs connecteurs en même temps pour la reprise après sinistre. Si un connecteur tombe en panne, vous pouvez passer à l'autre connecteur pour gérer immédiatement l'environnement de travail.

Pour configurer cette configuration :

1. ["Basculer vers un autre connecteur"](#)
2. Découvrir l'environnement de travail existant
 - ["Ajout de systèmes Cloud Volumes ONTAP existants à BlueXP"](#)
 - ["Découvrir les clusters ONTAP"](#)
3. Réglez le ["Mode de gestion de la capacité"](#)

Seul le connecteur principal doit être réglé sur **mode automatique**. Si vous basculez vers un autre connecteur pour la reprise après incident, vous pouvez modifier le mode de gestion de la capacité selon vos besoins.

Quand passer d'un connecteur à un autre

Lorsque vous créez votre premier connecteur, BlueXP utilise automatiquement ce connecteur pour chaque environnement de travail supplémentaire créé. Une fois que vous avez créé un connecteur supplémentaire, vous devrez passer de l'un à l'autre pour voir les environnements de travail spécifiques à chaque connecteur.

["Apprenez à passer d'un connecteur à un autre".](#)

Interface utilisateur locale

Pendant que vous devriez effectuer presque toutes les tâches à partir du ["Interface utilisateur SaaS"](#), Une interface utilisateur locale est toujours disponible sur le connecteur. Cette interface est nécessaire si vous installez le connecteur dans un environnement qui n'a pas accès à Internet (comme une région du gouvernement), et pour quelques tâches qui doivent être effectuées à partir du connecteur lui-même, au lieu de l'interface SaaS :

- ["Configuration d'un serveur proxy"](#)
- Installation d'un correctif (en général, vous travaillerez avec le personnel NetApp pour installer un correctif)
- Téléchargement de messages AutoSupport (généralement dirigés par le personnel NetApp en cas de problème)

["Découvrez comment accéder à l'interface utilisateur locale".](#)

Créez un connecteur dans AWS à partir de BlueXP

Un administrateur de compte BlueXP doit déployer un *Connector* avant de pouvoir utiliser la plupart des fonctions BlueXP. BlueXP peut ainsi gérer les ressources et les processus au sein de votre environnement de cloud public.

Ces étapes décrivent comment créer un connecteur dans une région commerciale d'AWS directement à partir du site Web BlueXP SaaS.

- ["Découvrez comment déployer un connecteur dans une région gouvernementale"](#)
- ["Découvrez d'autres méthodes de déploiement d'un connecteur"](#)

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

Configurez l'authentification

Pour lancer le connecteur dans AWS, BlueXP doit s'authentifier auprès d'AWS en assumant un rôle IAM ou en utilisant les clés d'accès AWS. Dans les deux cas, une règle IAM est requise.

[Afficher le rôle IAM](#) ou [suivez les instructions étape par étape.](#)

2

Configurer la mise en réseau

Vous avez besoin d'un VPC et d'un sous-réseau avec un accès Internet sortant à des terminaux spécifiques. Si un proxy HTTP est requis pour l'Internet sortant, vous aurez besoin de l'adresse IP, des identifiants et du certificat HTTPS.

[Afficher les besoins en matière de mise en réseau.](#)

Cliquez sur la liste déroulante connecteur, sélectionnez **Ajouter connecteur** et suivez les invites.

[Suivez les instructions étape par étape.](#)

Configuration de l'authentification 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

Dans les deux cas, vous devez d'abord commencer par créer une stratégie IAM qui inclut les autorisations requises.

Créer une règle IAM

Cette politique contient uniquement les autorisations nécessaires pour lancer l'instance Connector dans AWS 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 l'instance Connector qui permet au connecteur de gérer les ressources de votre environnement de cloud public.

Étapes

1. Accédez à la console IAM AWS.
2. Cliquez sur **stratégies > Créer une stratégie**.
3. Cliquez sur **JSON**.
4. Copiez et collez la stratégie suivante :

```
{
  "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",
      "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",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "iam:ListRoles",
        "kms:ListAliases"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:TerminateInstances"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/OCCMInstance": "*"
        }
    }
},
    "Resource": [

```

```
    "arn:aws:ec2:*:*:instance/*"
  ]
}
]
```

5. Cliquez sur **Suivant** et ajoutez des balises, si nécessaire.
6. Cliquez sur **Suivant** et entrez un nom et une description.
7. Cliquez sur **Créer une stratégie**.

Et la suite ?

Joignez la politique à un rôle IAM que BlueXP peut assumer ou à un utilisateur IAM.

Configurer un rôle IAM

Configurez un rôle IAM que BlueXP peut prendre en compte pour déployer le connecteur dans AWS.

Étapes

1. Accédez à la console IAM AWS dans le compte cible.
2. Sous gestion des accès, cliquez sur **rôles > Créer un rôle** et suivez les étapes pour créer le rôle.

Assurez-vous de faire ce qui suit :

- Sous **Type d'entité approuvée**, sélectionnez **compte AWS**.
 - Sélectionnez **un autre compte AWS** et saisissez l'ID du compte BlueXP SaaS : 952013314444
 - Sélectionnez la stratégie que vous avez créée dans la section précédente.
3. Après avoir créé le rôle, copiez le rôle ARN afin de pouvoir le coller dans BlueXP lorsque vous créez le connecteur.

Résultat

Le rôle IAM dispose désormais des autorisations requises.

Configurer les autorisations pour un utilisateur IAM

Lorsque vous créez un connecteur, vous pouvez fournir une clé d'accès AWS et une clé secrète pour un utilisateur IAM qui dispose des autorisations requises pour déployer l'instance de connecteur.

Étapes

1. Dans la console IAM AWS, cliquez sur **utilisateurs**, puis sélectionnez le nom d'utilisateur.
2. Cliquez sur **Ajouter des autorisations > attacher des stratégies existantes directement**.
3. Sélectionnez la stratégie que vous avez créée.
4. Cliquez sur **Suivant**, puis sur **Ajouter des autorisations**.
5. Assurez-vous d'avoir accès à une clé d'accès et à une clé secrète pour l'utilisateur IAM.

Résultat

L'utilisateur AWS dispose désormais des autorisations nécessaires pour créer le connecteur à partir de BlueXP. Vous devez spécifier les clés d'accès AWS pour cet utilisateur lorsque BlueXP vous le demande.

Configurer la mise en réseau

Configurez votre réseau de sorte que le connecteur puisse gérer les ressources et les processus au sein de votre environnement de cloud public. En dehors de la présence d'un VPC et d'un sous-réseau pour le connecteur, vous devez vous assurer que les exigences suivantes sont respectées.


Connexion aux réseaux cibles

Un connecteur nécessite une connexion réseau au type d'environnement de travail que vous créez et aux services que vous prévoyez d'activer.

Par exemple, si vous installez un connecteur sur le réseau de votre entreprise, vous devez configurer une connexion VPN sur le VPC dans lequel vous lancez Cloud Volumes ONTAP.

Accès Internet sortant

Le connecteur nécessite un accès Internet sortant pour gérer les ressources et les processus au sein de votre environnement de cloud public.

Terminaux	Objectif
<code>https://support.netapp.com</code>	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
<code>https://*.api.blueexp.netapp.com</code> <code>https://api.blueexp.netapp.com</code> <code>https://*.cloudmanager.cloud.netapp.com</code> <code>https://cloudmanager.cloud.netapp.com</code>	<div> Le connecteur est en train de contacter « cloudmanager.cloud.netapp.com », mais il commencera à contacter « api.blueexp.netapp.com » dans une prochaine version.</div>
<code>https://cloudmanagerinfraprod.azurecr.io</code> <code>https://*.blob.core.windows.net</code>	Pour mettre à niveau le connecteur et ses composants Docker.

Serveur proxy

Si votre organisation nécessite le déploiement d'un proxy HTTP pour tout le trafic Internet sortant, obtenez les informations suivantes concernant votre proxy HTTP :

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Groupe de sécurité

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous le lancez ou si le connecteur est utilisé comme proxy pour les messages AutoSupport. HTTP et HTTPS permettent l'accès au ["Interface utilisateur locale"](#), que vous utiliserez dans de rares circonstances. SSH n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

Limitation de l'adresse IP

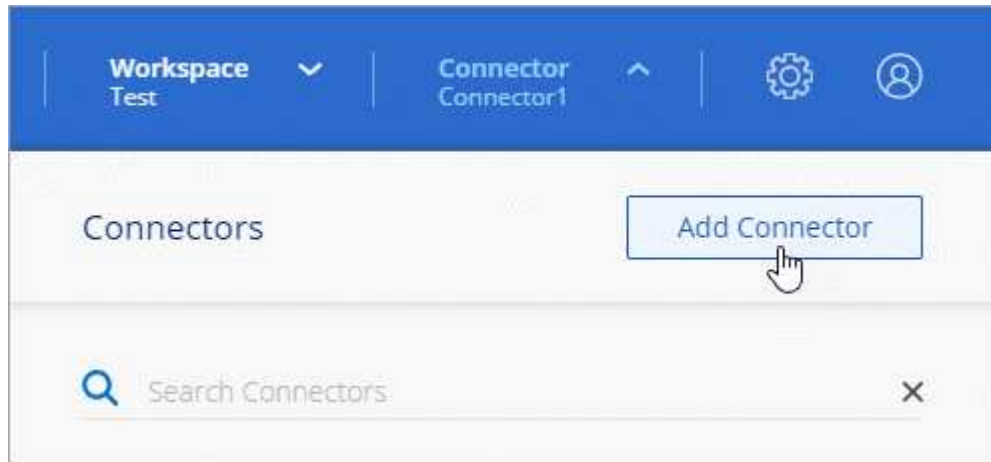
Il existe un conflit possible avec des adresses IP dans la plage 172. ["En savoir plus sur cette limitation"](#).

Créer un connecteur

BlueXP vous permet de créer un connecteur dans AWS directement à partir de son interface utilisateur.

Étapes

1. Si vous créez votre premier environnement de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites. Sinon, cliquez sur la liste déroulante **Connector** et sélectionnez **Add Connector**.



2. Choisissez **Amazon Web Services** comme fournisseur de cloud et cliquez sur **Continuer**.
3. Sur la page **déploiement d'un connecteur**, consultez les détails de ce dont vous aurez besoin. Vous avez deux options :
 - a. Cliquez sur **Continuer** pour préparer le déploiement à l'aide du guide d'utilisation du produit. Chaque étape du guide du produit inclut les informations contenues sur cette page de la documentation.
 - b. Cliquez sur **passer au déploiement** si vous avez 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"](#)

requis".

- 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 ou non un nouveau groupe de sécurité ou de sélectionner un groupe de sécurité existant qui autorise l'accès HTTP, HTTPS et SSH entrant.
- **Review** : consultez vos sélections pour vérifier que votre configuration est correcte.

5. Cliquez sur **Ajouter**.

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

Une fois que vous avez terminé

Si vous disposez de compartiments Amazon S3 sur le même compte AWS que celui sur lequel vous avez créé le connecteur, l'environnement de travail Amazon S3 s'affiche automatiquement sur la fenêtre Canvas.

["Découvrez ce que vous pouvez faire dans cet environnement de travail"](#).

Ouvrez le port 3128 pour les messages AutoSupport

Si vous prévoyez de déployer des systèmes Cloud Volumes ONTAP dans un sous-réseau où aucune connexion Internet sortante n'est disponible, BlueXP configure automatiquement Cloud Volumes ONTAP pour utiliser le connecteur comme serveur proxy.

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.

Si vous utilisez le groupe de sécurité par défaut pour Cloud Volumes ONTAP, aucune modification n'est nécessaire pour son groupe de sécurité. Mais si vous prévoyez de définir des règles de trafic sortantes strictes pour Cloud Volumes ONTAP, vous devrez également vous assurer que le groupe de sécurité Cloud Volumes ONTAP autorise les connexions *sortantes* sur le port 3128.

Créez un connecteur dans Azure à partir de BlueXP

Un administrateur de compte BlueXP doit déployer un *Connector* avant de pouvoir utiliser la plupart des fonctions BlueXP. BlueXP peut ainsi gérer les ressources et les processus au sein de votre environnement de cloud public.

Ces étapes décrivent comment créer un connecteur dans une région commerciale d'Azure directement à partir du site Web BlueXP SaaS.

- ["Découvrez comment déployer un connecteur dans une région gouvernementale"](#)
- ["Découvrez d'autres méthodes de déploiement d'un connecteur"](#)

Présentation

Pour déployer un connecteur, vous devez fournir à BlueXP un identifiant qui dispose des autorisations requises pour créer la machine virtuelle Connector dans Azure.

Vous avez deux options :

1. Connectez-vous avec votre compte Microsoft lorsque vous y êtes invité. Ce compte doit disposer d'autorisations Azure spécifiques. Il s'agit de l'option par défaut.

[Suivez les étapes ci-dessous pour commencer.](#)

2. Fournir des détails sur une entité principale de service Azure AD. Ce service principal nécessite également des autorisations spécifiques.

[Suivez les étapes ci-dessous pour commencer.](#)

Remarque sur les régions Azure

Le connecteur doit être déployé dans la même région Azure que les systèmes Cloud Volumes ONTAP qu'il gère ou dans "[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"](#)

Configurer la mise en réseau

Configurez votre réseau de sorte que le connecteur puisse gérer les ressources et les processus au sein de votre environnement de cloud public. En dehors de la présence d'un VNet et d'un sous-réseau pour le connecteur, vous devez vous assurer que les exigences suivantes sont respectées.

Connexion aux réseaux cibles

Un connecteur nécessite une connexion réseau au type d'environnement de travail que vous créez et aux services que vous prévoyez d'activer.

Par exemple, si vous installez un connecteur dans votre réseau d'entreprise, vous devez configurer une connexion VPN sur le vnet dans lequel vous lancez Cloud Volumes ONTAP.

Accès Internet sortant

Le connecteur nécessite un accès Internet sortant pour gérer les ressources et les processus au sein de votre environnement de cloud public.

Terminaux	Objectif
https://support.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.

Terminaux	Objectif
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com	Pour fournir des fonctions et des services SaaS dans BlueXP. <div>  Le connecteur est en train de contacter « cloudmanager.cloud.netapp.com », mais il commencera à contacter « api.bluexp.netapp.com » dans une prochaine version. </div>
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	Pour mettre à niveau le connecteur et ses composants Docker.

Serveur proxy

Si votre organisation nécessite le déploiement d'un proxy HTTP pour tout le trafic Internet sortant, obtenez les informations suivantes concernant votre proxy HTTP :

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Groupe de sécurité

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous le lancez ou si le connecteur est utilisé comme proxy pour les messages AutoSupport. HTTP et HTTPS permettent l'accès au ["Interface utilisateur locale"](#), que vous utiliserez dans de rares circonstances. SSH n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

Limitation de l'adresse IP

Il existe un conflit possible avec des adresses IP dans la plage 172. ["En savoir plus sur cette limitation"](#).

Créez un connecteur à l'aide de votre compte Azure

La méthode par défaut pour créer un connecteur dans Azure consiste à vous connecter avec votre compte Azure lorsque vous y êtes invité. Le formulaire de connexion est détenu et hébergé par Microsoft. Vos identifiants ne sont pas fournis à NetApp.

Configurez les autorisations pour votre compte Azure

Avant de pouvoir déployer un connecteur depuis BlueXP, vous devez vous assurer que votre compte Azure dispose des autorisations appropriées.

Étapes

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



Cette politique 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

```

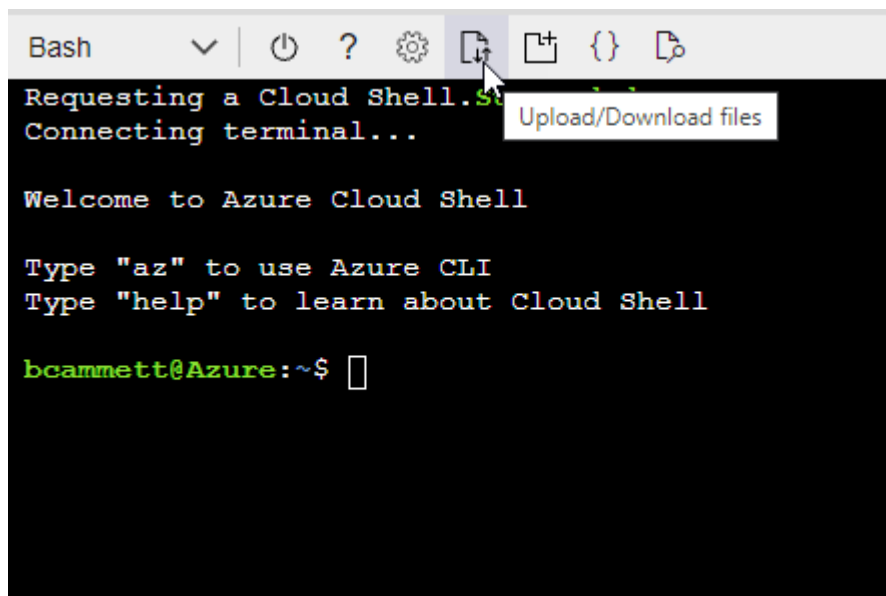
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],

```

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*.

4. Attribuez le rôle à l'utilisateur qui déploiera le connecteur depuis BlueXP :
 - a. Ouvrez le service **abonnements** et sélectionnez l'abonnement de l'utilisateur.
 - b. Cliquez sur **contrôle d'accès (IAM)**.
 - c. Cliquez sur **Ajouter > Ajouter une affectation de rôle**, puis ajoutez les autorisations suivantes :
 - 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.

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

Résultat

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

BlueXP.

Créez le connecteur en vous connectant avec votre compte Azure

BlueXP vous permet de créer un connecteur dans Azure directement à partir de son interface utilisateur.

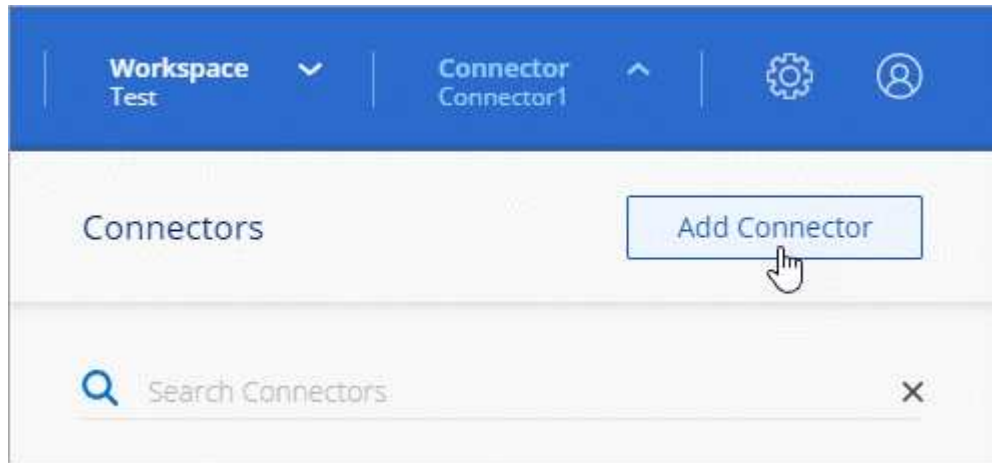
Ce dont vous avez besoin

- Un abonnement Azure.
- Un vnet et un sous-réseau dans votre région Azure de votre choix.
- 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 jeu d'autorisations différent de ce que vous avez configuré précédemment pour déployer simplement le connecteur.

Étapes

1. Si vous créez votre premier environnement de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites. Sinon, cliquez sur la liste déroulante **Connector** et sélectionnez **Add Connector**.



2. Choisissez **Microsoft Azure** comme fournisseur cloud.
3. Sur la page **déploiement d'un connecteur**, consultez les détails de ce dont vous aurez besoin. Vous avez deux options :
 - a. Cliquez sur **Continuer** pour préparer le déploiement à l'aide du guide d'utilisation du produit. Chaque étape comprend des informations contenues sur cette page de la documentation.
 - b. Cliquez sur **passer au déploiement** si vous avez 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 Microsoft, qui devrait disposer des autorisations requises pour créer la machine virtuelle.

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.

- **Authentification VM** : choisissez un abonnement Azure, un emplacement, un nouveau groupe de ressources ou un groupe de ressources existant, puis choisissez une méthode d'authentification.
- **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 associés à ce rôle. Chaque abonnement que vous choisissez fournit au connecteur les autorisations de déploiement de Cloud Volumes ONTAP dans ces abonnements.

- **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 ou non un nouveau groupe de sécurité ou de sélectionner un groupe de sécurité existant qui autorise l'accès HTTP, HTTPS et SSH entrant.
- **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.

Une fois que vous avez terminé

Vous devez associer un connecteur aux espaces de travail pour que les administrateurs d'espace de travail puissent utiliser ces connecteurs pour créer des systèmes Cloud Volumes ONTAP. Si vous ne disposez que d'administrateurs de compte, il n'est pas nécessaire d'associer le connecteur aux espaces de travail. Les administrateurs de comptes peuvent accéder à tous les espaces de travail dans BlueXP par défaut. "[En savoir plus >>](#)".

Si vous disposez d'un stockage Azure Blob dans le même compte Azure que celui sur lequel vous avez créé le connecteur, un environnement de travail Azure Blob s'affiche automatiquement sur la toile. "[Découvrez ce que vous pouvez faire dans cet environnement de travail](#)".

Créer un connecteur à l'aide d'un entité de service

Au lieu de vous connecter avec votre compte Azure, vous avez également la possibilité de fournir à BlueXP les informations d'identification pour un service principal Azure disposant des autorisations requises.

Octroi d'autorisations Azure à l'aide d'une entité de sécurité de service

Accordez les autorisations requises pour déployer un connecteur dans Azure en créant et en configurant un service principal dans Azure Active Directory et en obtenant les informations d'identification Azure requises par BlueXP.

Étapes

1. [Créez une application Azure Active Directory](#).
2. [https://docs.netapp.com/fr-fr/cloud-manager-setup-admin/Attribuez l&.html#8217;application à un rôle](https://docs.netapp.com/fr-fr/cloud-manager-setup-admin/Attribuez%20l%27application%20à%20un%20rôle.html#8217;application%20à%20un%20rôle)>[https://docs.netapp.com/fr-fr/cloud-manager-setup-admin/Attribuez l&.html#8217;application à un rôle](https://docs.netapp.com/fr-fr/cloud-manager-setup-admin/Attribuez l&.html#8217;application%20à%20un%20rôle).
3. [https://docs.netapp.com/fr-fr/cloud-manager-setup-admin/Ajoutez des autorisations d&.html#8217;API de gestion de service Windows Azure](https://docs.netapp.com/fr-fr/cloud-manager-setup-admin/Ajoutez%20des%20autorisations%20d%27API%20de%20gestion%20de%20service%20Windows%20Azure.html#8217;API%20de%20gestion%20de%20service%20Windows%20Azure)>[https://docs.netapp.com/fr-fr/cloud-manager-setup-admin/Ajoutez des autorisations d&.html#8217;API de gestion de service Windows Azure](https://docs.netapp.com/fr-fr/cloud-manager-setup-admin/Ajoutez%20des%20autorisations%20d%27API%20de%20gestion%20de%20service%20Windows%20Azure.html#8217;API%20de%20gestion%20de%20service%20Windows%20Azure).

4. [https://docs.netapp.com/fr-fr/cloud-manager-setup-admin/Obtenir l'ID de l'application et l'ID du répertoire](https://docs.netapp.com/fr-fr/cloud-manager-setup-admin/Obtenir%20ID%20de%20application%20et%20ID%20du%20répertoire)

5. Créez un secret client.

Créez une application Azure Active Directory

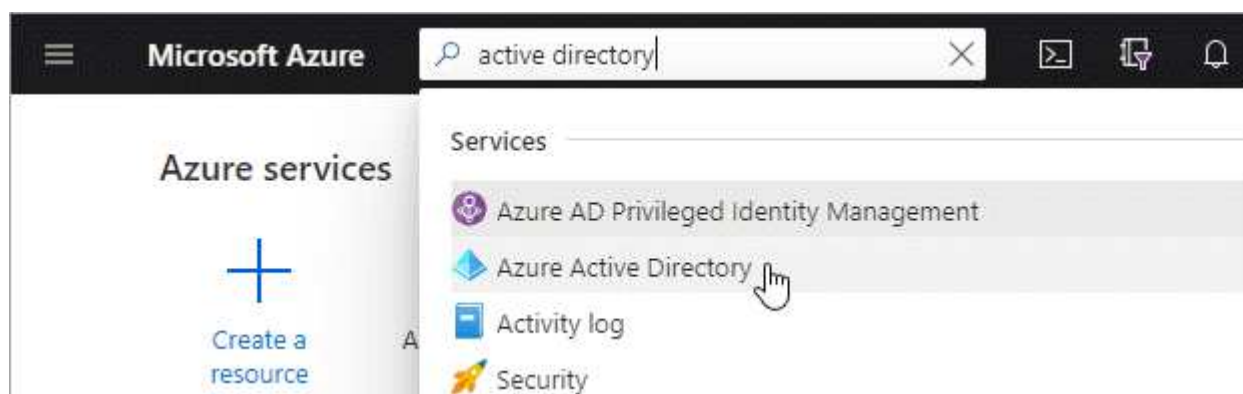
Créez une application et une entité de service Azure Active Directory (AD) que BlueXP peut utiliser pour déployer le connecteur.

Avant de commencer

Vous devez disposer des droits d'accès 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](#)".

Étapes

1. À partir du portail Azure, ouvrez le service **Azure Active Directory**.



2. Dans le menu, cliquez sur **enregistrements d'applications**.

3. Cliquez sur **Nouvelle inscription**.

4. 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.

5. Cliquez sur **Enregistrer**.

Résultat

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

Attribuez l'application à un rôle

Vous devez lier le principal de service à l'abonnement Azure dans lequel vous prévoyez de déployer le connecteur et lui affecter le rôle « Azure SetupAsService » personnalisé.

Étapes

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



Cette politique 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/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
]

```

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*.

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

Add role assignment ...

[Got feedback?](#)

[Role](#) **[Members](#)** [Review + assign](#)

Selected role Cloud Manager Operator 3.9.12_B

Assign access to ☒ User, group, or service principal
☐ Managed identity

Members [+ Select members](#)

- Recherchez le nom de l'application.

Voici un exemple :

Select members ✕

Select ⓘ

test-service-principal

test-service-principal

- Sélectionnez l'application et cliquez sur **Sélectionner**.
- Cliquez sur **Suivant**.
 - a. Cliquez sur **Revue + affecter**.

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

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

Le principal de service doit disposer d'autorisations « API de gestion des services Windows Azure ».

Étapes

1. Dans le service **Azure Active Directory**, cliquez sur **App inscriptions** et sélectionnez l'application.
2. Cliquez sur **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. Cliquez sur **Access Azure Service Management en tant qu'utilisateurs d'organisation**, puis sur **Add permissions**.

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
<input checked="" type="checkbox"/> user_impersonation Access Azure Service Management as organization users (preview) ⓘ	-

Obtenir l'ID de l'application et l'ID du répertoire

Lorsque vous créez le connecteur à partir de 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.

Étapes

1. Dans le service **Azure Active Directory**, cliquez sur **App inscriptions** et sélectionnez l'application.
2. Copiez l'ID **application (client)** et l'ID **Directory (tenant)**.



Créez un secret client

Vous devez créer un secret client, puis fournir à BlueXP la valeur du secret pour que BlueXP puisse l'utiliser pour s'authentifier avec Azure AD.

Étapes

1. Ouvrez le service **Azure Active Directory**.
2. Cliquez sur **App Inregistrations** et sélectionnez votre application.
3. Cliquez sur **certificats et secrets > Nouveau secret client**.

4. Fournissez une description du secret et une durée.
5. Cliquez sur **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
test secret	8/16/2020	*sZ1jSe2By:D*-ZR0V4NLfdAcY7:+0vA

Copy to clipboard

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.

Créez le connecteur en vous connectant avec le principal de service

BlueXP vous permet de créer un connecteur dans Azure directement à partir de son interface utilisateur.

Ce dont vous avez besoin

- Un abonnement Azure.
- Un vnet et un sous-réseau dans votre région Azure de votre choix.
- Détails sur un proxy HTTP, si votre organisation nécessite un proxy pour tout le trafic Internet sortant :
 - Adresse IP
 - Informations d'identification
 - Certificat HTTPS
- 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 jeu d'autorisations différent de ce que vous avez configuré précédemment pour déployer simplement le connecteur.

Étapes

1. Si vous créez votre premier environnement de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites. Sinon, cliquez sur la liste déroulante **Connector** et sélectionnez **Add Connector**.



2. Choisissez **Microsoft Azure** comme fournisseur cloud.
3. Sur la page **déploiement d'un connecteur** :
 - a. Sous **Authentication**, cliquez sur **Active Directory Service principal** et entrez des informations sur le principal du service Azure Active Directory qui accorde les autorisations requises :
 - ID de l'application (client) : voir [https://docs.netapp.com/fr-fr/cloud-manager-setup-admin/Obtenir l'ID de l'application et l'ID du répertoire](https://docs.netapp.com/fr-fr/cloud-manager-setup-admin/Obtenir%20ID%20de%20l'application%20et%20ID%20du%20répertoire)
 - ID de répertoire (locataire) : voir [https://docs.netapp.com/fr-fr/cloud-manager-setup-admin/Obtenir l'ID de l'application et l'ID du répertoire](https://docs.netapp.com/fr-fr/cloud-manager-setup-admin/Obtenir%20ID%20de%20l'application%20et%20ID%20du%20répertoire)
 - Secret client : voir [Créez un secret client](#).
 - b. Cliquez sur **connexion**.
 - c. Vous avez désormais deux options :
 - Cliquez sur **Continuer** pour préparer le déploiement à l'aide du guide d'utilisation du produit. Chaque étape du guide du produit inclut les informations contenues sur cette page de la documentation.
 - Cliquez sur **passer au déploiement** si vous avez déjà préparé en suivant les étapes de cette page.
4. Suivez les étapes de l'assistant pour créer le connecteur :
 - **Authentification VM** : choisissez un abonnement Azure, un emplacement, un nouveau groupe de ressources ou un groupe de ressources existant, puis choisissez une méthode d'authentification.
 - **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 associés à ce rôle. Chaque abonnement que vous choisissez fournit au connecteur les autorisations de déploiement de Cloud Volumes ONTAP dans ces abonnements.

- **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 ou non un nouveau groupe de sécurité ou de sélectionner

un groupe de sécurité existant qui autorise l'accès HTTP, HTTPS et SSH entrant.

- **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.

Une fois que vous avez terminé

Vous devez associer un connecteur aux espaces de travail pour que les administrateurs d'espace de travail puissent utiliser ces connecteurs pour créer des systèmes Cloud Volumes ONTAP. Si vous ne disposez que d'administrateurs de compte, il n'est pas nécessaire d'associer le connecteur aux espaces de travail. Les administrateurs de comptes peuvent accéder à tous les espaces de travail dans BlueXP par défaut. "[En savoir plus >>](#)".

Si vous disposez d'un stockage Azure Blob dans le même compte Azure que celui sur lequel vous avez créé le connecteur, un environnement de travail Azure Blob s'affiche automatiquement sur la toile. "[Découvrez ce que vous pouvez faire dans cet environnement de travail](#)".

Ouvrez le port 3128 pour les messages AutoSupport

Si vous prévoyez de déployer des systèmes Cloud Volumes ONTAP dans un sous-réseau où aucune connexion Internet sortante n'est disponible, BlueXP configure automatiquement Cloud Volumes ONTAP pour utiliser le connecteur comme serveur proxy.

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.

Si vous utilisez le groupe de sécurité par défaut pour Cloud Volumes ONTAP, aucune modification n'est nécessaire pour son groupe de sécurité. Mais si vous prévoyez de définir des règles de trafic sortantes strictes pour Cloud Volumes ONTAP, vous devrez également vous assurer que le groupe de sécurité Cloud Volumes ONTAP autorise les connexions *sortantes* sur le port 3128.

Créez un connecteur dans Google Cloud à partir de BlueXP

Un administrateur de compte BlueXP doit déployer un *Connector* avant de pouvoir utiliser la plupart des fonctions BlueXP. "[Apprenez quand un connecteur est nécessaire](#)". BlueXP peut ainsi gérer les ressources et les processus au sein de votre environnement de cloud public.

Cette page explique comment créer un connecteur dans Google Cloud directement à partir de BlueXP. "[Découvrez d'autres méthodes de déploiement d'un connecteur](#)".

Ces étapes doivent être réalisées par un utilisateur qui a le rôle d'administrateur de compte. Un administrateur d'espace de travail ne peut pas créer de connecteur.



Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, BlueXP vous invite à créer un connecteur si vous n'en avez pas encore.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1

Configurez les autorisations

- Assurez-vous que votre compte Google Cloud dispose des autorisations appropriées en créant et en attachant un rôle personnalisé.

[Configurez les autorisations de déploiement du connecteur.](#)

- Lorsque vous créez la machine virtuelle Connector, vous devez l'associer à un compte de service. Ce compte de service doit avoir un rôle personnalisé qui dispose d'autorisations pour gérer des ressources dans Google Cloud.

[Configurez un compte de service pour le connecteur.](#)

- Si vous utilisez un VPC partagé, configurez des autorisations dans le projet de service et le projet hôte.

[Configurez les autorisations VPC partagées.](#)

2

Configurer la mise en réseau

Vous avez besoin d'un VPC et d'un sous-réseau avec un accès Internet sortant à des terminaux spécifiques. Si un proxy HTTP est requis pour l'Internet sortant, vous aurez besoin de l'adresse IP, des identifiants et du certificat HTTPS.

[Afficher les besoins en matière de mise en réseau.](#)

3

Activez les API Google Cloud

- 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

4

Créer le connecteur

Cliquez sur la liste déroulante connecteur, sélectionnez **Ajouter connecteur** et suivez les invites.

[Suivez les instructions étape par étape.](#)

Configurez les autorisations

Des autorisations sont requises pour les éléments suivants :

- L'utilisateur qui va déployer la machine virtuelle de connecteur

- Un compte de service que vous devez connecter à la machine virtuelle Connector pendant le déploiement
- Des autorisations VPC partagées, si vous utilisez un VPC partagé pour déployer des ressources dans un projet de service

Configurez les autorisations de déploiement du connecteur

Avant de déployer un connecteur, vous devez vous assurer que votre compte Google Cloud dispose des autorisations appropriées.

Étapes

1. "Créer un rôle personnalisé" 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`

2. Reliez le rôle personnalisé à l'utilisateur qui déploiera le connecteur depuis BlueXP.

Résultat

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

Configurez un compte de service pour le connecteur

Un compte de service est requis pour fournir au connecteur l'autorisation requise pour gérer les ressources dans Google Cloud. Vous allez associer ce compte de service à la machine virtuelle Connector lors de sa création.

Les autorisations du compte de service sont différentes des autorisations que vous avez définies dans la section précédente.

Étapes

1. "Créer un rôle personnalisé" qui inclut les autorisations suivantes :

```
title: NetApp BlueXP
description: Permissions for the service account associated with the
Connector instance.
```

```
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- 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.addAccessConfig
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
```

- `compute.regions.list`
- `compute.snapshots.create`
- `compute.snapshots.delete`
- `compute.snapshots.get`
- `compute.snapshots.list`
- `compute.snapshots.setLabels`
- `compute.subnetworks.get`
- `compute.subnetworks.list`
- `compute.subnetworks.use`
- `compute.subnetworks.useExternalIp`
- `compute.zoneOperations.get`
- `compute.zones.get`
- `compute.zones.list`
- `compute.instances.setServiceAccount`
- `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`
- `logging.logEntries.list`
- `logging.privateLogEntries.list`
- `resourcemanager.projects.get`
- `storage.buckets.create`
- `storage.buckets.delete`
- `storage.buckets.get`
- `storage.buckets.list`
- `cloudkms.cryptoKeyVersions.useToEncrypt`
- `cloudkms.cryptoKeys.get`
- `cloudkms.cryptoKeys.list`
- `cloudkms.keyRings.list`
- `storage.buckets.update`
- `iam.serviceAccounts.getIamPolicy`
- `iam.serviceAccounts.list`
- `storage.objects.get`
- `storage.objects.list`

- `monitoring.timeSeries.list`
- `storage.buckets.getIamPolicy`

2. "Créez un compte de service Google Cloud et appliquez le rôle personnalisé que vous venez de créer".
3. Si vous souhaitez déployer Cloud Volumes ONTAP dans d'autres projets, "Accordez l'accès en ajoutant le compte de service avec le rôle BlueXP à ce projet". Vous devrez répéter cette étape pour chaque projet.

Résultat

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

Configurez les autorisations VPC partagées

Si vous utilisez un VPC partagé pour déployer des ressources dans un projet de service, vous devez disposer des autorisations suivantes. Ce tableau est fourni à titre de référence et votre environnement doit refléter la table des autorisations lorsque la configuration IAM est terminée.

Identité	Créateur	Hébergé dans	Autorisations de projet de service	Autorisations de projet hôte	Objectif
Compte Google utilisé pour déployer le connecteur	Personnalisées	Projet de service	<ul style="list-style-type: none"> "Les autorisations trouvées dans cette section ci-dessus" 	<ul style="list-style-type: none"> compute.networkUser 	Déploiement du connecteur dans le projet de service
Connecteur de compte de service	Personnalisées	Projet de service	<ul style="list-style-type: none"> "Les autorisations trouvées dans cette section ci-dessus" 	<ul style="list-style-type: none"> compute.networkUser 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	<ul style="list-style-type: none"> storage.admin Membre: Compte de service BlueXP à partir de serviceAccount.user 	S/O	(Facultatif) pour le Tiering des données et la sauvegarde dans le cloud
Agent de service Google API	Google Cloud	Projet de service	<ul style="list-style-type: none"> Editeur (par défaut) 	<ul style="list-style-type: none"> compute.networkUser 	Interagit avec les API Google Cloud pour le compte du déploiement. Permet à BlueXP d'utiliser le réseau partagé.

Identité	Créateur	Hébergé dans	Autorisations de projet de service	Autorisations de projet hôte	Objectif
Compte de service par défaut Google Compute Engine	Google Cloud	Projet de service	<ul style="list-style-type: none"> Editeur (par défaut) 	<ul style="list-style-type: none"> compute.networkUser 	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.

Configurer la mise en réseau

Configurez votre réseau de sorte que le connecteur puisse gérer les ressources et les processus au sein de votre environnement de cloud public. En dehors de la présence d'un VPC et d'un sous-réseau pour le connecteur, vous devez vous assurer que les exigences suivantes sont respectées.

Connexion aux réseaux cibles


Un connecteur nécessite une connexion réseau au type d'environnement de travail que vous créez et aux services que vous prévoyez d'activer.

Par exemple, si vous installez un connecteur sur le réseau de votre entreprise, vous devez configurer une connexion VPN sur le VPC dans lequel vous lancez Cloud Volumes ONTAP.

Accès Internet sortant

Le connecteur nécessite un accès Internet sortant pour gérer les ressources et les processus au sein de votre environnement de cloud public.

Terminaux	Objectif
https://support.netapp.com	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.

Terminaux	Objectif
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com	Pour fournir des fonctions et des services SaaS dans BlueXP. <div>  Le connecteur est en train de contacter « cloudmanager.cloud.netapp.com », mais il commencera à contacter « api.bluexp.netapp.com » dans une prochaine version. </div>
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	Pour mettre à niveau le connecteur et ses composants Docker.

Serveur proxy

Si votre organisation nécessite le déploiement d'un proxy HTTP pour tout le trafic Internet sortant, obtenez les informations suivantes concernant votre proxy HTTP :

- Adresse IP
- Informations d'identification
- Certificat HTTPS

Groupe de sécurité

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous le lancez ou si le connecteur est utilisé comme proxy pour les messages AutoSupport. HTTP et HTTPS permettent l'accès au ["Interface utilisateur locale"](#), que vous utiliserez dans de rares circonstances. SSH n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

Limitation de l'adresse IP

Il existe un conflit possible avec des adresses IP dans la plage 172. ["En savoir plus sur cette limitation"](#).

Activez les API Google Cloud

Plusieurs API sont nécessaires pour déployer le connecteur et Cloud Volumes ONTAP.

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

Créer un connecteur

Créez un connecteur dans Google Cloud directement à partir de l'interface utilisateur BlueXP ou en utilisant

gcloud.

BlueXP

1. Si vous créez votre premier environnement de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites. Sinon, cliquez sur la liste déroulante **Connector** et sélectionnez **Add Connector**.



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. Cliquez sur **Continuer** pour préparer le déploiement à l'aide du guide d'utilisation du produit. Chaque étape du guide du produit inclut les informations contenues sur cette page de la documentation.
 - b. Cliquez sur **passer au déploiement** si vous avez 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.
- **Politique de pare-feu** : Choisissez si vous souhaitez créer une nouvelle politique de pare-feu ou si vous souhaitez sélectionner une politique de pare-feu existante qui autorise l'accès HTTP, HTTPS et SSH entrant.
- **Review** : consultez vos sélections pour vérifier que votre configuration est correcte.

5. Cliquez sur **Ajouter**.

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

gcloud

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 NetApp à associer au connecteur.

["En savoir plus sur les comptes NetApp"](#).

- b. Entrez un nom pour le système.

Résultat

Le connecteur est désormais installé et configuré avec votre compte NetApp. BlueXP utilisera automatiquement ce connecteur lorsque vous créez de nouveaux environnements de travail. Mais si vous avez plus d'un connecteur, vous devrez le faire ["basculer entre eux"](#).

Si vous disposez de compartiments Google Cloud Storage dans le même compte Google Cloud sur lequel vous avez créé le connecteur, un environnement de travail Google Cloud Storage s'affiche automatiquement sur la toile. ["Découvrez ce que vous pouvez faire dans cet environnement de travail"](#).

Ouvrez le port 3128 pour les messages AutoSupport

Si vous prévoyez de déployer des systèmes Cloud Volumes ONTAP dans un sous-réseau où aucune connexion Internet sortante n'est disponible, BlueXP configure automatiquement Cloud Volumes ONTAP pour utiliser le connecteur comme serveur proxy.

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.

Si vous utilisez le groupe de sécurité par défaut pour Cloud Volumes ONTAP, aucune modification n'est nécessaire pour son groupe de sécurité. Mais si vous prévoyez de définir des règles de trafic sortant strictes pour Cloud Volumes ONTAP, vous devrez également vous assurer que le groupe de sécurité Cloud Volumes ONTAP autorise les connexions *sortantes* sur le port 3128.

Créer un connecteur dans une région gouvernementale

Si vous travaillez dans une région gouvernementale, vous devez déployer un connecteur à partir du marché de votre fournisseur de cloud ou installer manuellement le logiciel Connector sur un hôte Linux existant. Vous ne pouvez pas déployer le connecteur dans une région gouvernementale à partir du site Web SaaS de BlueXP.

Utilisez l'un des liens suivants pour afficher les instructions de création d'un connecteur :

- ["Créez un connecteur à partir d'AWS Marketplace"](#)
- ["Créer un connecteur et une Cloud Volumes ONTAP dans l'environnement C2S AWS"](#)
- ["Créez un connecteur à partir d'Azure Marketplace"](#)
- ["Installez un connecteur sur votre propre hôte Linux"](#)

Pour les installations manuelles sur votre propre hôte Linux, vous devez utiliser le programme d'installation en ligne pour installer le connecteur sur un hôte ayant accès à Internet. Un programme d'installation séparé « hors ligne » est disponible pour le connecteur, mais il est uniquement pris en charge sur les sites sur site qui ne disposent pas d'un accès Internet. Elle n'est pas soutenue par les régions gouvernementales.

Une fois le connecteur déployé, vous pouvez accéder à BlueXP en ouvrant votre navigateur Web et en vous connectant à l'adresse IP de l'instance Connector : `https://ipaddress[]`

Comme le connecteur a été déployé dans une région du gouvernement, il n'est pas accessible à partir de <https://console.bluexp.netapp.com>.

Informations sur le copyright

Copyright © 2022 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.