



# **Configuration et administration de BlueXP**

## **Set up and administration**

NetApp

December 01, 2022

# Table des matières

Configuration et administration de BlueXP	1
Notes de mise à jour	2
Quoi de neuf	2
Limites connues	12
Commencez	15
En savoir plus sur BlueXP	15
Checklist de mise en route	16
Connectez-vous à BlueXP	20
Configurez un compte NetApp	22
Configurer un connecteur	31
Par où aller plus loin	71
Administration de BlueXP	72
Comptes NetApp	72
Connecteurs	87
Gérer les abonnements et les contrats PAYGO	119
Stockage cloud découvert	120
Identifiants AWS	125
Identifiants Azure	134
Identifiants Google Cloud	146
Ajoutez et gérez des comptes du site de support NetApp dans BlueXP	154
Mes opportunités	161
Référence	162
Autorisations	162
Ports	214
Connaissances et support	219
S'inscrire pour obtenir de l'aide	219
Obtenez de l'aide	223
Mentions légales	227
Droits d'auteur	227
Marques déposées	227
Brevets	227
Politique de confidentialité	227
Source ouverte	227

# Configuration et administration de BlueXP

# Notes de mise à jour

## Quoi de neuf

Découvrez les nouveautés de BlueXP (anciennement Cloud Manager), qui inclut notamment les comptes NetApp, les connecteurs, les identifiants des fournisseurs cloud.

### 6 novembre 2022

#### Connecteur 3.9.23

- Vos abonnements PAYGO et vos contrats annuels pour BlueXP sont désormais disponibles pour la consultation et la gestion à partir du portefeuille numérique.

["Découvrez comment gérer vos abonnements"](#)

- Cette version du connecteur inclut également des améliorations Cloud Volumes ONTAP.

["Découvrez les améliorations apportées à Cloud Volumes ONTAP"](#)

### 1er novembre 2022

Cloud Manager vous invite à mettre à jour les identifiants associés à vos comptes sur le site de support NetApp lorsque le jeton de mise à jour associé à votre compte expire au bout de 3 mois. ["Découvrez comment gérer des comptes NSS"](#)

### 18 septembre 2022

#### Connecteur 3.9.22

- Nous avons amélioré l'assistant de déploiement de connecteur en ajoutant un *Guide produit* qui fournit des étapes permettant de répondre aux exigences minimales pour l'installation de connecteurs : autorisations, authentification et mise en réseau.
- Vous pouvez désormais créer un dossier de demande de support NetApp directement depuis Cloud Manager dans **support Dashboard**.

["Découvrez comment créer un dossier"](#).

- Cette version du connecteur inclut également des améliorations Cloud Volumes ONTAP.

["Découvrez les améliorations apportées à Cloud Volumes ONTAP"](#)

### 31 juillet 2022

#### Connecteur 3.9.21

- Nous avons introduit une nouvelle façon de découvrir les ressources clouds que vous n'êtes pas encore géré dans Cloud Manager.

Sur la toile, l'onglet **Mes opportunités** fournit un emplacement centralisé pour découvrir les ressources

existantes que vous pouvez ajouter à Cloud Manager afin d'assurer la cohérence des services de données et des opérations dans l'ensemble de votre environnement multicloud hybride.

Dans cette version initiale, My Opportunities vous permet de découvrir les systèmes de fichiers FSX pour ONTAP existants dans votre compte AWS.

["Découvrez comment découvrir FSX pour ONTAP à l'aide de Mes opportunités"](#)

- Cette version du connecteur inclut également des améliorations Cloud Volumes ONTAP.

["Découvrez les améliorations apportées à Cloud Volumes ONTAP"](#)

## 15 juillet 2022

### Changements de règles

Nous avons mis à jour la documentation en ajoutant des règles Cloud Manager directement dans les documents. Cela signifie que vous pouvez désormais afficher les autorisations requises pour le connecteur et le Cloud Volumes ONTAP en même temps que les étapes qui décrivent la configuration de ces connecteurs. Ces règles étaient auparavant accessibles à partir d'une page du site de support NetApp.

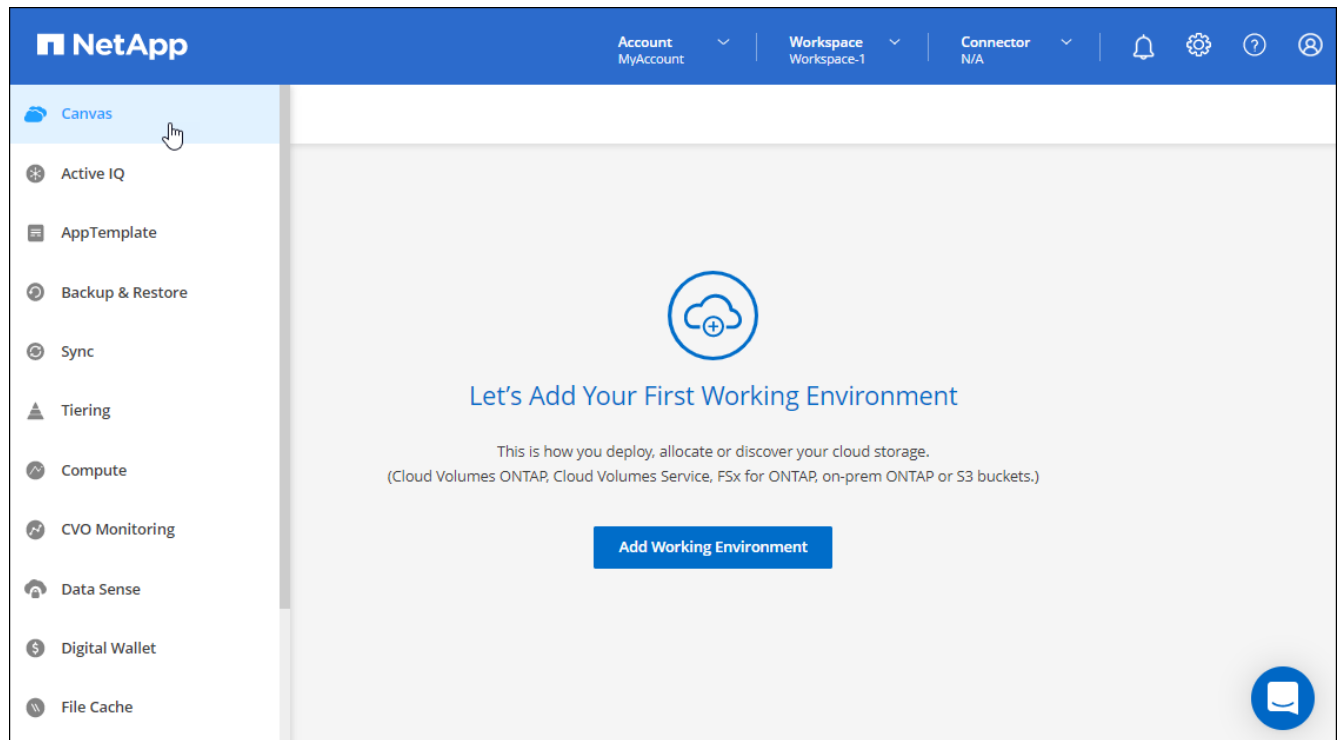
["Voici un exemple illustrant les autorisations de rôle IAM AWS utilisées pour créer un connecteur"](#).

Nous avons également créé une page qui contient des liens vers chacune des politiques. ["Consultez le récapitulatif des autorisations pour Cloud Manager"](#).

## 3 juillet 2022

### Connecteur 3.9.20

- Nous avons introduit une nouvelle façon de naviguer vers la liste croissante de fonctionnalités de l'interface Cloud Manager. Vous pouvez facilement accéder à toutes les fonctionnalités de Cloud Manager en passant le curseur de la souris sur le panneau de gauche.



- Vous pouvez désormais configurer Cloud Manager pour envoyer des notifications par e-mail, afin que vous soyez informé de l'activité importante du système, même lorsque vous n'êtes pas connecté au système.

["Pour en savoir plus sur la surveillance des opérations, consultez votre compte".](#)

- Cloud Manager prend désormais en charge le stockage Azure Blob et Google Cloud Storage en tant qu'environnements de travail, similaires à la prise en charge d'Amazon S3.

Une fois que vous avez installé un connecteur dans Azure ou Google Cloud, Cloud Manager détecte automatiquement des informations sur le stockage Azure Blob dans votre abonnement Azure ou sur Google Cloud Storage dans le projet sur lequel le connecteur est installé. Cloud Manager affiche le stockage objet sous forme d'environnement de travail que vous pouvez ouvrir pour afficher des informations plus détaillées.

Voici un exemple d'environnement de travail Azure Blob :

Azure blob

Overview

637

Total Storage Accounts

1.5

TiB

Total Capacity

16

Total Locations

637

Storage Accounts

Storage Account Name	Subscription	Location	Creation Date	Resource Group	Blob Capacity
ovu8llxvqdfypxn	OCCM QA1	West US	June 24, 2021	AdmAzureHa-rg	170 B
rootsa9ktpjzcm	OCCM QA1	West US	June 24, 2021	AdmAzureHa-rg	950.22 GiB
scvdwjcwehswli	OCCM QA1	West US	June 24, 2021	AdmAzureHa-rg	22.12 MiB
65qtx0smegmq2vt	OCCM QA1	West US	June 24, 2021	AdmAzureVsa-rg	170 B
bu9klxthymr1be	OCCM QA1	West US	June 24, 2021	AdmAzureVsa-rg	1.01 MiB
8jzsvybvjiweww8	OCCM QA1	Canada Central	December 12, 2019	aff1-rg	170 B

- Nous avons repensé la page des ressources d'un environnement de travail Amazon S3 en fournissant des informations plus détaillées sur les compartiments S3, comme la capacité, le chiffrement et plus encore.
- Le connecteur est désormais pris en charge dans les régions Google Cloud suivantes :
  - Madrid (europe-Sud-Ouest 1)
  - Paris (europe-Ouest 9)
  - Varsovie (europe centrale 2)
- Le connecteur est désormais pris en charge dans la région Azure West US 3.

["Afficher la liste complète des régions prises en charge"](#)

- Cette version du connecteur inclut également des améliorations Cloud Volumes ONTAP.

["Découvrez les améliorations apportées à Cloud Volumes ONTAP"](#)

## 28 juin 2022

### Connectez-vous avec les identifiants NetApp

Lorsque les nouveaux utilisateurs s'ouvrent sur Cloud Central, ils peuvent sélectionner l'option **se connecter avec NetApp** pour se connecter avec leurs identifiants du site de support NetApp. Il s'agit d'une alternative à la saisie d'une adresse e-mail et d'un mot de passe.



Les identifiants de connexion existants qui utilisent une adresse e-mail et un mot de passe doivent continuer à utiliser cette méthode de connexion. L'option connexion avec NetApp est disponible pour les nouveaux utilisateurs qui s'abonnent.

## 7 juin 2022

### Connecteur 3.9.19

- Le connecteur est maintenant pris en charge dans la région AWS Jakarta (ap-sud-est-3).

- Le connecteur est maintenant pris en charge dans la région du Sud-est d’Azure Brésil.

["Afficher la liste complète des régions prises en charge"](#)

- Cette version de Connector inclut également des améliorations apportées à Cloud Volumes ONTAP et des clusters ONTAP sur site.
  - ["Découvrez les améliorations apportées à Cloud Volumes ONTAP"](#)
  - ["Découvrez les améliorations apportées aux clusters sur site de ONTAP"](#)

## 12 mai 2022

### Connecteur 3.9.18 patch

Nous avons mis à jour le connecteur pour introduire des correctifs. La correction la plus notable est l'un des problèmes qui affecte le déploiement Cloud Volumes ONTAP dans Google Cloud lorsque le connecteur se trouve dans un VPC partagé.

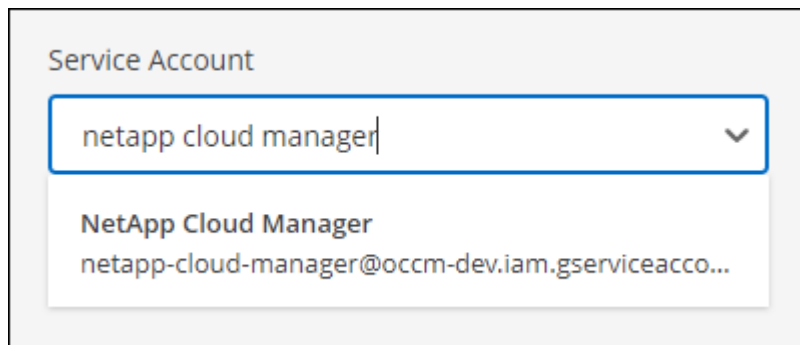
## 2 mai 2022

### Connecteur 3.9.18

- Le connecteur est désormais pris en charge dans les régions Google Cloud suivantes :
  - Delhi (asie-Sud 2)
  - Melbourne (australie-southeast2)
  - Milan (europe-Ouest 8)
  - Santiago (sud-ouest 1)

["Afficher la liste complète des régions prises en charge"](#)

- Lorsque vous sélectionnez le compte de service Google Cloud à utiliser avec le connecteur, Cloud Manager affiche désormais l'adresse e-mail associée à chaque compte de service. L'affichage de l'adresse e-mail peut faciliter la distinction entre les comptes de service partageant le même nom.



- Nous avons certifié le connecteur dans Google Cloud sur une instance de machine virtuelle avec un système d'exploitation pris en charge ["Fonctionnalités MV blindées"](#)
- Cette version du connecteur inclut également des améliorations Cloud Volumes ONTAP. ["Découvrez ces améliorations"](#)
- De nouvelles autorisations AWS sont requises pour que Connector puisse déployer Cloud Volumes ONTAP.



Les autorisations suivantes sont désormais nécessaires pour créer un groupe de placement AWS SprÃ ad se trouvant dans une même zone de disponibilité lors du déploiement d'une paire haute disponibilité :

```
"ec2:DescribePlacementGroups",  
"iam:GetRolePolicy"
```

Ces autorisations sont désormais nécessaires pour optimiser la façon dont Cloud Manager crée le groupe de placement.

Veillez à fournir ces autorisations à chaque ensemble d'identifiants AWS que vous avez ajoutés à Cloud Manager. ["Afficher la dernière règle IAM pour le connecteur"](#).

## 3 avril 2022

### Connecteur 3.9.17

- Vous pouvez maintenant créer un connecteur en laissant Cloud Manager assumer un rôle IAM que vous configurez dans votre environnement. Cette méthode d'authentification est plus sécurisée que le partage d'une clé d'accès AWS et d'une clé secrète.

["Apprendre à créer un connecteur à l'aide d'un rôle IAM"](#).

- Cette version du connecteur inclut également des améliorations Cloud Volumes ONTAP. ["Découvrez ces améliorations"](#)

## 27 février 2022

### Connecteur 3.9.16

- Lorsque vous créez un nouveau connecteur dans Google Cloud, Cloud Manager affichera désormais toutes vos politiques de pare-feu existantes. Auparavant, Cloud Manager n'affichera aucune règle ne disposant pas d'étiquette cible.
- Cette version du connecteur inclut également des améliorations Cloud Volumes ONTAP. ["Découvrez ces améliorations"](#)

## 30 janvier 2022

### Connecteur 3.9.15

Cette version du connecteur inclut des améliorations Cloud Volumes ONTAP. ["Découvrez ces améliorations"](#)

## 2 janvier 2022

### Réduction des points d'extrémité pour le connecteur

Nous avons réduit le nombre de terminaux qu'un connecteur doit contacter pour gérer les ressources et les processus au sein de votre environnement de cloud public.

["Afficher la liste des terminaux requis"](#)

## Chiffrement de disque EBS pour le connecteur

Lorsque vous déployez un nouveau connecteur dans AWS depuis Cloud Manager, vous pouvez désormais chiffrer les disques EBS du connecteur à l'aide de la clé principale par défaut ou d'une clé gérée.

The screenshot shows the 'Details' page in the AWS Cloud Manager console. At the top, there is a progress bar with six steps: 'Get Ready' (checked), 'AWS Credentials' (checked), 'Details' (active), 'Network' (4), 'Security Group' (5), and 'Review' (6). The main heading is 'Details'. Below this, there are two columns of configuration options. The left column includes 'Connector Instance Name' with a text input field containing 'Connector1', and a link '+ Add Tags to Connector Instance'. The right column includes 'Connector Role' with radio buttons for 'Create Role' (selected) and 'Select an existing Role', and 'Role Name' with a text input field containing 'Cloud-Manager-Operator-9yils3K'. At the bottom right, there is a toggle switch for 'AWS Managed Encryption' which is turned on (blue). A black arrow points to this toggle switch. Below the toggle, it says 'Master Key: aws/ebs (default)' and a 'Change Key' link.

## Adresse e-mail des comptes NSS

Cloud Manager peut désormais afficher l'adresse e-mail associée à un compte sur le site de support NetApp.



**28 novembre 2021**

### **Vous devez mettre à jour vos comptes sur le site de support NetApp**

Depuis décembre 2021, NetApp utilise désormais Microsoft Azure Active Directory comme fournisseur d'identités pour les services d'authentification spécifiques au support et aux licences. Suite à cette mise à jour, Cloud Manager vous demandera de mettre à jour les identifiants des comptes existants du site de support NetApp que vous avez ajoutés.

Si vous n'avez pas encore migré votre compte NSS vers IDaaS, vous devez d'abord migrer le compte, puis mettre à jour vos identifiants dans Cloud Manager.

- ["Découvrez comment mettre à jour un compte NSS avec la nouvelle méthode d'authentification"](#).
- ["En savoir plus sur l'utilisation par NetApp de Microsoft Azure AD pour la gestion des identités"](#)

### **Modifiez les comptes NSS pour Cloud Volumes ONTAP**

Si votre entreprise compte plusieurs comptes sur le site de support NetApp, vous pouvez désormais modifier le compte associé à un système Cloud Volumes ONTAP.

["Découvrez comment associer un environnement de travail à un autre compte NSS"](#).

## 4 novembre 2021

### Certification SOC 2 Type 2

Nous avons étudié Cloud Manager, Cloud Sync, Cloud Tiering, Cloud Data Sense et Cloud Backup (plateforme Cloud Manager), et confirmé que notre cabinet d'experts indépendants a réussi à produire des rapports SOC 2 Type 2 d'après les critères des services de confiance applicables.

["Consultez les rapports SOC 2 de NetApp"](#).

### Le connecteur n'est plus pris en charge en tant que proxy

Vous ne pouvez plus utiliser Cloud Manager Connector comme serveur proxy pour envoyer des messages AutoSupport depuis Cloud Volumes ONTAP. Cette fonctionnalité a été supprimée et n'est plus prise en charge. Vous devrez fournir une connectivité AutoSupport via une instance NAT ou les services proxy de votre environnement.

["En savoir plus sur la vérification de AutoSupport avec Cloud Volumes ONTAP"](#)

## 31 octobre 2021

### Authentification avec entité de service

Lorsque vous créez un nouveau connecteur dans Microsoft Azure, vous pouvez maintenant vous authentifier auprès d'un principal de service Azure, plutôt qu'avec les identifiants de compte Azure.

["Découvrez comment vous authentifier auprès d'un service principal Azure"](#).

### Amélioration des informations d'identification

Nous avons repensé la page d'informations d'identification pour être facile à utiliser et adapter à l'apparence actuelle de l'interface Cloud Manager.

## 2 septembre 2021

### Un nouveau service de notification a été ajouté

Le service de notification a été introduit afin de consulter l'état des opérations Cloud Manager que vous avez lancées pendant votre session de connexion en cours. Vous pouvez vérifier si l'opération a réussi ou si elle a échoué. ["Découvrez comment surveiller les opérations de votre compte"](#).

## 1er août 2021

### Prise en charge de RHEL 7.9 avec le connecteur

Le connecteur est désormais pris en charge sur un hôte exécutant Red Hat Enterprise Linux 7.9.

["Afficher la configuration système requise pour le connecteur"](#).

## 7 juillet 2021

## Améliorations apportées à l'assistant Ajout de connecteur

Nous avons repensé l'assistant **Add Connector** pour ajouter de nouvelles options et le rendre plus facile à utiliser. Vous pouvez à présent ajouter des balises, spécifier un rôle (pour AWS ou Azure), charger un certificat racine pour un serveur proxy, afficher du code pour l'automatisation Terraform, afficher des détails de progression, etc.

- ["Créez un connecteur dans AWS"](#)
- ["Créer un connecteur dans Azure"](#)
- ["Créer un connecteur dans GCP"](#)

## Gestion de comptes NSS depuis le tableau de bord du support

Les comptes du site de support NetApp sont désormais gérés depuis le tableau de bord du support plutôt que depuis le menu Paramètres. Grâce à ce changement, vous trouverez et gèrerez plus facilement toutes les informations relatives au support à partir d'un emplacement unique.

["Découvrez comment gérer des comptes NSS"](#).

NSS User Name	NSS User ID	Attached Working Environments
testcloud2	61e6b48b-371e-4681-a...	—

## 5 mai 2021

### Comptes dans le scénario

La chronologie dans Cloud Manager affiche désormais les actions et les événements liés à la gestion de compte. Ces actions incluent notamment l'association d'utilisateurs, la création d'espaces de travail et la création de connecteurs. La vérification de la chronologie peut être utile si vous devez identifier qui a effectué une action spécifique ou si vous devez identifier le statut d'une action.

["Découvrez comment filtrer la chronologie vers le service Tenancy"](#).

## 11 avril 2021

### Appels d'API directement vers Cloud Manager

Si vous avez configuré un serveur proxy, vous pouvez désormais activer une option pour envoyer des appels API directement à Cloud Manager sans passer par le proxy. Cette option est prise en charge avec les connecteurs qui s'exécutent dans AWS ou dans Google Cloud.

["En savoir plus sur ce paramètre"](#).

## Utilisateurs de compte de service

Vous pouvez désormais créer un utilisateur de compte de service.

Un compte de service fonctionne comme un « utilisateur » qui peut passer des appels d'API autorisés à Cloud Manager à des fins d'automatisation. Il est ainsi plus facile de gérer l'automatisation, car il n'est pas nécessaire de créer des scripts d'automatisation basés sur le compte d'utilisateur réel d'une personne qui quitte l'entreprise à tout moment. Et si vous utilisez la fédération, vous pouvez créer un jeton sans générer de jeton d'actualisation à partir du cloud.

["En savoir plus sur l'utilisation des comptes de service"](#).

## Aperçus privés

Vous pouvez désormais autoriser des aperçus privés de votre compte à accéder aux nouveaux services clouds NetApp lorsqu'ils sont disponibles dans Cloud Manager.

["En savoir plus sur cette option"](#).

## Services tiers

Vous pouvez également autoriser les services tiers de votre compte à accéder à des services tiers disponibles dans Cloud Manager.

["En savoir plus sur cette option"](#).

## 9 février 2021

### Améliorations du tableau de bord du support

Nous avons mis à jour le tableau de bord du support en vous permettant d'ajouter vos identifiants du site de support NetApp, qui vous permettent d'obtenir de l'aide. Vous pouvez également initier un dossier de demande de support NetApp directement à partir du tableau de bord. Cliquez simplement sur l'icône aide, puis sur **support**.

## Limites connues

Les limitations connues identifient les plateformes, les périphériques ou les fonctions qui ne sont pas pris en charge par cette version du produit, ou qui ne fonctionnent pas correctement avec elle. Examinez attentivement ces limites.

Ces limitations sont spécifiques à la configuration et à l'administration de BlueXP : le connecteur, la plateforme SaaS, et plus encore.

### Limitations du connecteur

#### Conflit possible avec les adresses IP dans la plage 172

BlueXP déploie le connecteur avec deux interfaces qui ont des adresses IP dans les plages 172.17.0.0/16 et 172.18.0.0/16.

Si votre réseau dispose d'un sous-réseau configuré avec l'une ou l'autre de ces plages, il se peut que vous ayez des défaillances de connectivité de BlueXP. Par exemple, la découverte de clusters ONTAP sur site dans

BlueXP peut échouer.

Consultez l'article de la base de connaissances ["Conflit IP connecteur BlueXP avec le réseau existant"](#) Pour obtenir des instructions sur la modification de l'adresse IP des interfaces du connecteur.

### **Seul un serveur proxy HTTP est pris en charge**

Si vos stratégies d'entreprise nécessitent l'utilisation d'un serveur proxy pour toutes les communications HTTP vers Internet, vous devez configurer vos connecteurs pour utiliser ce serveur proxy HTTP. Le serveur proxy peut se trouver dans le cloud ou dans votre réseau.

BlueXP ne prend pas en charge l'utilisation d'un proxy HTTPS avec le connecteur.

### **Le décryptage SSL n'est pas pris en charge**

BlueXP ne prend pas en charge les configurations de pare-feu pour lesquelles le décryptage SSL est activé. Si le décryptage SSL est activé, des messages d'erreur apparaissent dans BlueXP et l'instance de connecteur s'affiche comme inactive.

Pour une sécurité améliorée, vous avez la possibilité de ["Installation d'un certificat HTTPS signé par une autorité de certification \(CA\)"](#).

### **Page blanche lors du chargement de l'interface utilisateur locale**

Si vous chargez l'interface utilisateur locale pour un connecteur, il est possible que l'interface utilisateur ne s'affiche pas parfois, et il vous suffit d'obtenir une page vide.

Ce problème est lié à un problème de mise en cache. La solution consiste à utiliser une session de navigateur Web privée ou incognito.

### **Les hôtes Linux partagés ne sont pas pris en charge**

Le connecteur n'est pas pris en charge sur une machine virtuelle partagée avec d'autres applications. La machine virtuelle doit être dédiée au logiciel de connecteur.

### **agents et extensions tiers**

Les agents tiers ou les extensions VM ne sont pas pris en charge sur la VM Connector.

## **Limites de SaaS**

### **La plateforme SaaS est désactivée pour les régions du secteur public**

Si vous déployez un connecteur dans une région AWS GovCloud, une région Azure Government ou une région Azure DoD, l'accès à BlueXP est disponible uniquement via l'adresse IP hôte d'un connecteur. L'accès à la plateforme SaaS est désactivé pour l'ensemble du compte.

Cela signifie que seuls les utilisateurs privilégiés qui peuvent accéder au VPC/vNet interne de l'utilisateur final peuvent utiliser l'interface utilisateur ou l'API de BlueXP.

Il est à noter que les seuls services pris en charge dans ces régions sont Cloud Volumes ONTAP, Cloud Backup, Cloud Data Sense et la réplication. Aucun autre service NetApp n'est pris en charge dans les régions du secteur public.

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

## Restrictions du marché

### **Le paiement à l'utilisation n'est pas disponible pour les partenaires Azure et Google Cloud**

Si vous êtes un partenaire de fournisseur de solutions cloud Microsoft ou un partenaire Google Cloud, les abonnements avec paiement basé sur l'utilisation de NetApp ne sont pas disponibles. Vous devez acheter une licence et déployer des solutions clouds NetApp avec une licence BYOL.

Les abonnements avec le paiement à l'utilisation ne sont pas disponibles pour les services cloud NetApp suivants :

- Cloud Volumes ONTAP
- Tiering dans le cloud
- La sauvegarde dans le cloud
- Sens des données cloud



# Commencez

## En savoir plus sur BlueXP

BlueXP (anciennement Cloud Manager) permet aux experts IT et aux architectes cloud de gérer de manière centralisée leur infrastructure multicloud hybride à l'aide des solutions cloud NetApp.

### Caractéristiques

BlueXP est une plateforme de gestion SaaS professionnelle qui vous permet de garder le contrôle de vos données, où qu'elles se trouvent.

- Configuration et utilisation ["Cloud Volumes ONTAP"](#) pour une gestion efficace des données multiprotocole sur l'ensemble des clouds.
- Configuration et utilisation des services de stockage de fichiers :
  - ["Azure NetApp Files"](#)
  - ["Amazon FSX pour ONTAP"](#)
  - ["Cloud Volumes Service pour AWS"](#)
  - ["Cloud Volumes Service pour Google Cloud"](#)
- Découvrez et gérez les clusters ONTAP sur site en créant des volumes, en sauvegardant dans le cloud, en répliquant les données dans l'ensemble de votre cloud hybride et en effectuant le Tiering des données inactives dans le cloud.
- Profiter de services clouds intégrés, tels que :
  - ["Sens des données cloud"](#)
  - ["Cloud Insights"](#)
  - ["La sauvegarde dans le cloud"](#)

["En savoir plus sur BlueXP"](#).

### Fournisseurs de stockage objet pris en charge

BlueXP vous permet de gérer le stockage cloud et d'utiliser les services cloud dans Amazon Web Services, Microsoft Azure et Google Cloud.

### Le coût

BlueXP logiciel est gratuit auprès de NetApp.

Pour la plupart des tâches, BlueXP vous invite à déployer un connecteur dans votre réseau cloud, ce qui entraîne des frais pour l'instance de calcul et le stockage associé de votre fournisseur cloud. Vous avez la possibilité d'exécuter le logiciel de connecteur sur votre site.

["En savoir plus sur la configuration par défaut du connecteur"](#).

## Fonctionnement de BlueXP

BlueXP comprend une interface SaaS intégrée au site Web BlueXP et des connecteurs qui gèrent Cloud Volumes ONTAP et d'autres services Cloud.

### Services à la demande

BlueXP est accessible via un ["Interface utilisateur SaaS"](#) Et les API. Cette expérience SaaS vous permet d'accéder automatiquement aux toutes dernières fonctionnalités dès leur sortie et de basculer facilement d'un compte à l'autre de vos connecteurs et de vos comptes NetApp.



Si vous travaillez dans un environnement où l'accès Internet sortant n'est pas disponible, vous pouvez installer le logiciel Connector dans cet environnement et accéder à l'interface utilisateur locale disponible sur le connecteur. ["En savoir plus sur les connecteurs"](#).

### Site Web BlueXP

["Le site Web BlueXP"](#) cette solution est centralisée pour l'accès et la gestion ["Services clouds NetApp"](#). Avec l'authentification utilisateur centralisée, vous pouvez utiliser le même ensemble d'informations d'identification pour accéder à BlueXP et à d'autres services cloud comme Cloud Insights.

### Compte NetApp

Lorsque vous vous connectez à BlueXP pour la première fois, vous êtes invité à créer un *compte NetApp*. Ce compte fournit la colocation et vous permet d'organiser les utilisateurs et les ressources dans des *espaces de travail* isolés.

### Connecteurs

Dans la plupart des cas, un administrateur de compte BlueXP devra déployer un *Connector* dans votre réseau cloud ou sur site. BlueXP peut ainsi gérer les ressources et les processus au sein de votre environnement de cloud public.

["En savoir plus sur le moment où les connecteurs sont nécessaires et leur fonctionnement"](#).

## Certification SOC 2 Type 2

Nous avons étudié BlueXP, Cloud Sync, Cloud Tiering, Cloud Data Sense et Cloud Backup (plateforme BlueXP), et confirmé que leur cabinet d'experts-comptables indépendant a réussi à générer des rapports SOC 2 de type 2 d'après les critères des services de confiance applicables.

["Consultez les rapports SOC 2 de NetApp"](#)

## Checklist de mise en route

Utilisez cette liste de contrôle pour comprendre ce dont vous avez besoin pour être opérationnel avec BlueXP dans un déploiement typique où le connecteur dispose d'un accès Internet sortant.

### Un login

Pour vous connecter à BlueXP, vous pouvez utiliser vos identifiants du site de support NetApp ou vous inscrire à une connexion au cloud NetApp à l'aide de votre e-mail et de votre mot de passe. ["En savoir plus"](#)

sur la connexion".

## Accès au réseau à partir d'un navigateur Web vers plusieurs noeuds finaux

L'interface utilisateur BlueXP est accessible à partir d'un navigateur Web. Lorsque vous utilisez l'interface utilisateur BlueXP, il contacte plusieurs points de terminaison pour effectuer les tâches de gestion des données. La machine exécutant le navigateur Web doit disposer de connexions aux points finaux suivants.

Terminaux	Objectif
http://cloudmanager.netapp.com	Votre navigateur Web contacte cette URL lors de l'utilisation de l'interface utilisateur SaaS.
Services AWS (amazonaws.com): <ul style="list-style-type: none"><li>• CloudFormation</li><li>• Cogito</li><li>• Cloud de calcul élastique (EC2)</li><li>• Service de gestion des clés (KMS)</li><li>• Service de jetons de sécurité (STS)</li><li>• Service de stockage simple (S3)</li></ul>	Nécessaire pour déployer un connecteur depuis BlueXP dans AWS. Le point final exact dépend de la région dans laquelle vous déployez le connecteur. <a href="#">"Reportez-vous à la documentation AWS pour plus de détails."</a>
https://management.azure.com https://login.microsoftonline.com	Nécessaire au déploiement d'un connecteur depuis BlueXP dans la plupart des régions Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Nécessaire au déploiement d'un connecteur depuis BlueXP dans les régions d'Azure Allemagne.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Nécessaire au déploiement d'un connecteur de BlueXP dans les régions Azure Government.
https://www.googleapis.com	Nécessaire pour déployer un connecteur depuis BlueXP dans Google Cloud.
https://signin.b2c.netapp.com	Requis pour mettre à jour les identifiants du site de support NetApp (NSS) ou pour ajouter de nouvelles informations d'identification NSS à BlueXP.
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	Votre navigateur Web se connecte à ces points de terminaison pour une authentification utilisateur centralisée via BlueXP.
https://widget.intercom.io	Vous bénéficiez d'un chat en ligne pour discuter avec des experts du cloud NetApp.

Terminaux	Objectif
Adresse IP du connecteur	<p>Dans la plupart des cas, vous devez travailler avec BlueXP à partir de l'interface utilisateur SaaS, mais <a href="#">"Si vous utilisez l'interface utilisateur locale"</a>, Vous devez ensuite saisir l'adresse IP de l'hôte à partir d'un navigateur Web.</p> <p>Selon la connectivité à votre fournisseur de cloud, utilisez l'IP privée ou une adresse IP publique attribuée à l'hôte :</p> <ul style="list-style-type: none"> <li>• Une adresse IP privée fonctionne si vous disposez d'un VPN et d'un accès direct à votre réseau virtuel</li> <li>• Un IP public fonctionne dans tous les scénarios de mise en réseau</li> </ul> <p>Dans les deux cas, sécurisez l'accès au réseau en veillant à ce que les règles de groupe de sécurité autorisent l'accès à partir des adresses IP ou des sous-réseaux autorisés uniquement.</p>

### Mise en réseau sortante pour un connecteur

Une fois connecté à BlueXP, un administrateur de compte BlueXP devra déployer un *Connector* dans un fournisseur cloud ou dans votre réseau local. BlueXP peut ainsi gérer les ressources et les processus au sein de votre environnement de cloud public. Notez qu'un connecteur est nécessaire pour la plupart, mais pas pour tous les services et fonctionnalités de BlueXP. ["En savoir plus sur les connecteurs et leur fonctionnement"](#).

- L'emplacement réseau où vous déployez le connecteur doit disposer d'une connexion Internet sortante.

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

Terminaux	Objectif
<a href="https://support.netapp.com">https://support.netapp.com</a>	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
<a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a> <a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	Pour fournir des fonctions et des services SaaS dans BlueXP.
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a> <a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a>	Pour mettre à niveau le connecteur et ses composants Docker.

- Si vous choisissez d'installer manuellement le connecteur sur votre propre hôte Linux (et non directement à partir de l'interface BlueXP), le programme d'installation du connecteur nécessite l'accès aux points de terminaison suivants pendant le processus d'installation :
  - <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>
  - [https://\\*.blob.core.windows.net](https://*.blob.core.windows.net) ou <https://hub.docker.com>

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.

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

HTTP (80) et HTTPS (443) permettent d'accéder à 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 autorisations du fournisseur cloud

Vous devez disposer d'un compte disposant des autorisations pour déployer le connecteur dans votre fournisseur de cloud directement à partir de BlueXP.



Il existe d'autres façons de créer un connecteur : vous pouvez créer un connecteur à partir du ["AWS Marketplace"](#), le ["Azure Marketplace"](#), ou vous pouvez ["installer manuellement le logiciel"](#).

Emplacement	Étapes générales	Étapes détaillées
AWS	<ol style="list-style-type: none"><li>1. Utilisez un fichier JSON qui inclut les autorisations requises pour créer une règle IAM dans AWS.</li><li>2. Associez la règle à un rôle IAM ou à un utilisateur IAM.</li><li>3. Lorsque vous créez le connecteur, fournissez BlueXP avec l'ARN du rôle IAM ou la clé d'accès AWS et la clé secrète pour l'utilisateur IAM.</li></ol>	<a href="#">"Cliquez ici pour afficher les étapes détaillées"</a> .
Azure	<ol style="list-style-type: none"><li>1. Utilisez un fichier JSON qui inclut les autorisations requises pour créer un rôle personnalisé dans Azure.</li><li>2. Attribuez le rôle à l'utilisateur qui créera le connecteur à partir de BlueXP.</li><li>3. Lorsque vous créez le connecteur, connectez-vous avec le compte Microsoft qui dispose des autorisations requises (l'invite de connexion qui est détenue et hébergée par Microsoft).</li></ol>	<a href="#">"Cliquez ici pour afficher les étapes détaillées"</a> .

Emplacement	Étapes générales	Étapes détaillées
Google Cloud	<ol style="list-style-type: none"> <li>1. Utilisez un fichier YAML qui inclut les autorisations requises pour créer un rôle personnalisé dans Google Cloud.</li> <li>2. Reliez ce rôle à l'utilisateur qui créera le connecteur à partir de BlueXP.</li> <li>3. Si vous envisagez d'utiliser Cloud Volumes ONTAP, configurez un compte de service disposant des autorisations requises.</li> <li>4. Activez les API Google Cloud.</li> <li>5. Lorsque vous créez le connecteur, connectez-vous avec le compte Google qui dispose des autorisations requises (l'invite de connexion est détenue et hébergée par Google).</li> </ol>	<a href="#">"Cliquez ici pour afficher les étapes détaillées".</a>

### Mise en réseau pour des services individuels

Maintenant que votre configuration est terminée, vous êtes prêt à utiliser les services disponibles depuis BlueXP. Notez que chaque service présente ses propres exigences réseau. Pour plus de détails, reportez-vous aux pages suivantes.

- ["Cloud Volumes ONTAP pour AWS"](#)
- ["Cloud Volumes ONTAP pour Azure"](#)
- ["Cloud Volumes ONTAP pour GCP"](#)
- ["Réplication des données entre les systèmes ONTAP"](#)
- ["Déployer des solutions Cloud Data est logique"](#)
- ["Clusters ONTAP sur site"](#)
- ["Tiering dans le cloud"](#)
- ["La sauvegarde dans le cloud"](#)

## Connectez-vous à BlueXP

BlueXP est accessible depuis votre navigateur Web via une interface utilisateur SaaS.

Si vous accédez à BlueXP à partir d'une région gouvernementale ou d'un site qui n'a pas d'accès Internet sortant, vous devez vous connecter à l'interface utilisateur BlueXP qui fonctionne localement sur le connecteur. ["Découvrez comment accéder à l'interface utilisateur locale sur le connecteur".](#)

Vous pouvez vous connecter à BlueXP à l'aide de l'une des options suivantes :

- Vos identifiants existants du site de support NetApp (NSS)

Lorsque vous utilisez cette option, vos identifiants du site du support NetApp ne sont pas ajoutés à BlueXP dans le tableau de bord du support. Vous devez ajouter vos identifiants NSS à BlueXP pour activer les flux de travail clés pour Cloud Volumes ONTAP. ["Découvrez comment ajouter vos identifiants NSS à BlueXP".](#)

- Un identifiant NetApp Cloud avec votre adresse e-mail et un mot de passe

Cette option prend en charge les connexions fédérées. Vous pouvez utiliser l'authentification unique pour vous connecter à l'aide des informations d'identification de votre annuaire d'entreprise (identité fédérée). Pour en savoir plus, consultez le "[Centre d'aide BlueXP](#)" puis cliquez sur **options de connexion**.

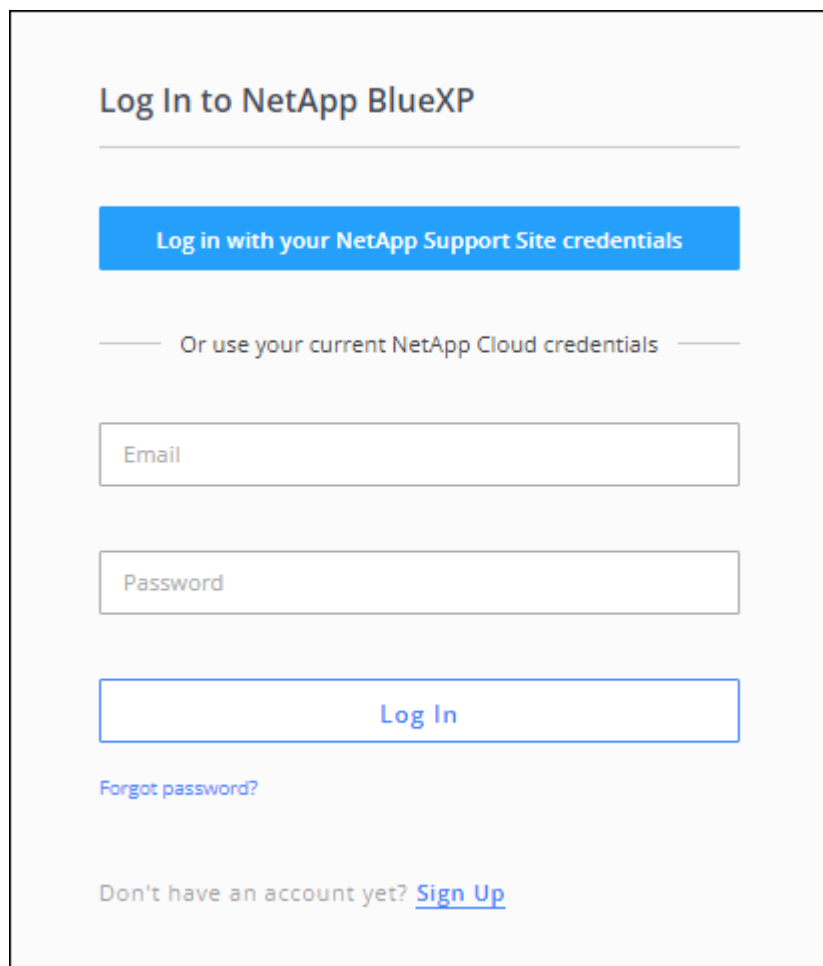
Chaque fois que vous vous connectez, vous devez utiliser la même option que celle que vous avez choisie lors de votre première connexion.

- Si vous vous êtes inscrit en vous connectant à l'aide de vos identifiants du site de support NetApp, vous devez utiliser cette option de connexion à chaque fois.
- Si vous vous êtes inscrit en saisissant votre e-mail et votre mot de passe, vous devez entrer ces informations d'identification chaque fois que vous vous connectez.

## Étapes

1. Ouvrez un navigateur Web et accédez au "[Console BlueXP](#)"

La page de connexion NetApp BlueXP s'affiche.



2. Choisissez l'une des options de connexion :

- Si vous avez déjà créé les identifiants cloud NetApp, connectez-vous à l'aide de votre e-mail et de votre mot de passe.
- Si vous ne possédez pas de identifiants cloud, mais que vous disposez déjà d'un compte sur le site de support NetApp (NSS), sélectionnez **Connectez-vous à l'aide de vos identifiants du site de support NetApp**.

- Si vous ne possédez pas de compte NSS et que vous n'avez pas créé les identifiants cloud NetApp, cliquez sur **Sign Up** pour créer un identifiant cloud NetApp.

Notez que seuls les caractères anglais sont autorisés dans le formulaire d'inscription.

Vous recevrez ensuite un e-mail de NetApp. Cliquez sur le lien dans l'e-mail pour vérifier votre adresse e-mail, puis connectez-vous.

Vous êtes maintenant connecté et pouvez commencer à utiliser BlueXP pour gérer votre infrastructure multicloud hybride.

## Configurez un compte NetApp

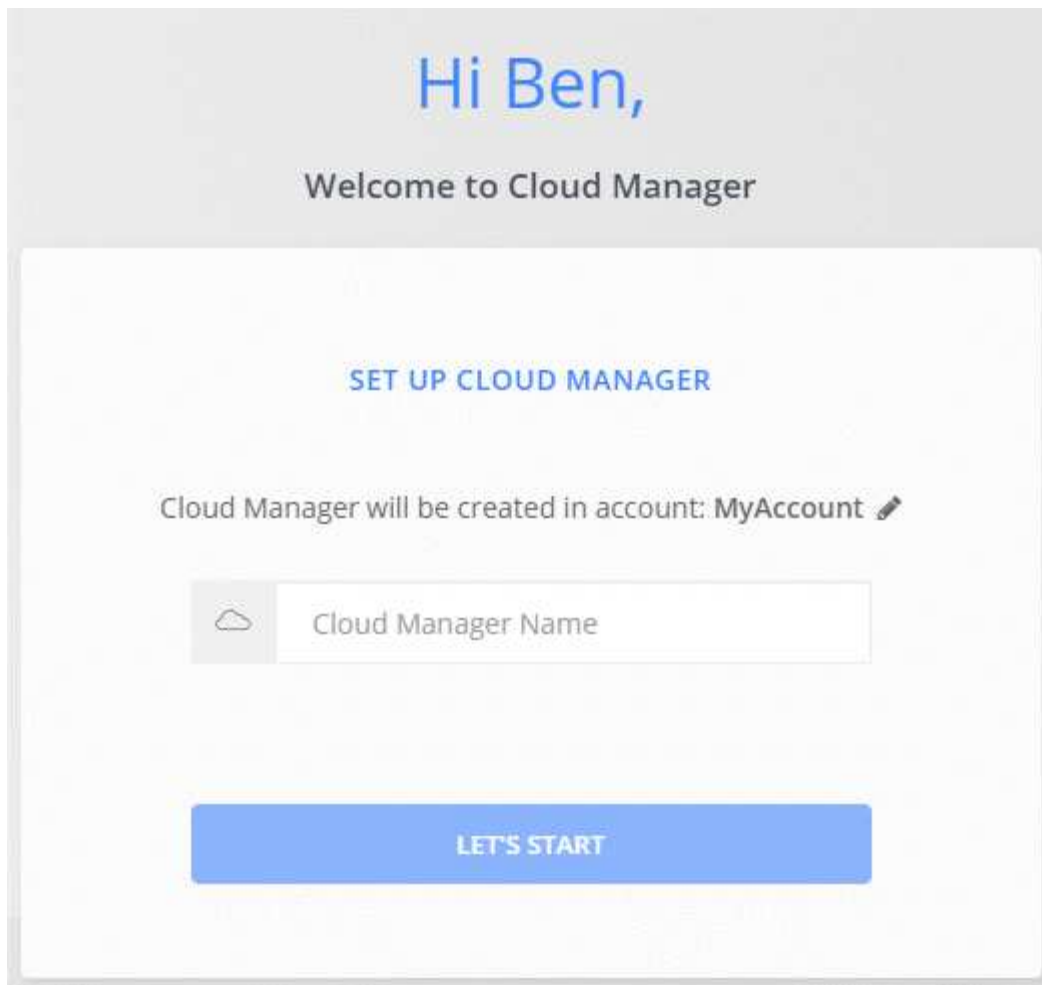
### En savoir plus sur les comptes NetApp

Un *compte NetApp* propose la colocation et vous permet d'organiser les utilisateurs et les ressources dans des espaces de travail isolés à partir de BlueXP.

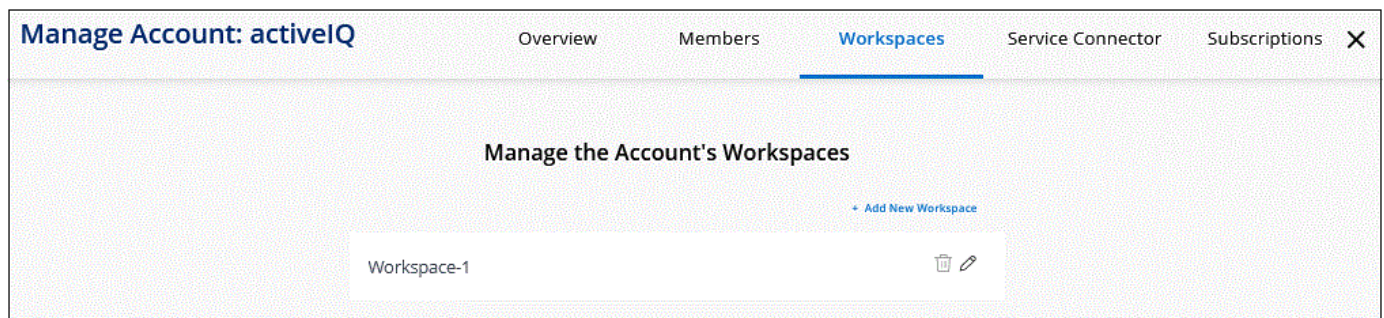
Par exemple, plusieurs utilisateurs peuvent déployer et gérer des systèmes Cloud Volumes ONTAP dans des environnements isolés appelés *espaces de travail*. Ces espaces de travail sont invisibles pour les autres utilisateurs, à moins qu'ils ne soient partagés.

Lorsque vous accédez pour la première fois à BlueXP, vous êtes invité à sélectionner ou à créer un compte NetApp :





Les administrateurs de compte BlueXP peuvent ensuite modifier les paramètres de ce compte en gérant les utilisateurs (membres), les espaces de travail, les connecteurs et les abonnements :



Pour obtenir des instructions détaillées, reportez-vous à la section "[Configuration du compte NetApp](#)".

### Paramètres du compte

Le widget gérer des comptes de BlueXP permet aux administrateurs de comptes de gérer un compte NetApp. Si vous venez de créer votre compte, vous commencerez de zéro. Mais si vous avez déjà configuré un compte, vous verrez *All* les utilisateurs, les espaces de travail, les connecteurs et les abonnements associés au compte.

## Présentation

La page vue d'ensemble affiche le nom du compte et l'ID du compte. Vous devrez peut-être fournir votre identifiant de compte lors de l'enregistrement de certains services. Cette page inclut également quelques options de configuration BlueXP.

## Membres

Les membres sont des utilisateurs BlueXP que vous associez à votre compte NetApp. L'association d'un utilisateur à un compte et d'un ou plusieurs espaces de travail dans ce compte permet à ces utilisateurs de créer et de gérer des environnements de travail dans BlueXP.

Lorsque vous associez un utilisateur, vous lui attribuez un rôle :

- *Account Admin*: Peut effectuer n'importe quelle action dans BlueXP.
- *Workspace Admin* : permet de créer et de gérer des ressources dans l'espace de travail affecté.
- *Compliance Viewer*: Peut uniquement afficher les informations de conformité Cloud Data Sense et générer des rapports pour les systèmes auxquels ils sont autorisés à accéder.
- *Admin SnapCenter*: Peut utiliser le service SnapCenter pour créer des sauvegardes cohérentes avec les applications et restaurer les données à l'aide de ces sauvegardes. *Ce service est actuellement en version bêta.*

["En savoir plus sur ces rôles"](#).

## Espaces de travail

Dans BlueXP, un espace de travail isole tout nombre d'environnements *fonctionnant* d'autres environnements de travail. Les administrateurs de l'espace de travail ne peuvent pas accéder aux environnements de travail dans un espace de travail à moins que l'administrateur du compte n'associe l'administrateur à cet espace de travail.

Un environnement de travail représente un système de stockage :

- Un système Cloud Volumes ONTAP à un seul nœud ou une paire HA
- Un cluster ONTAP sur site dans votre réseau
- Un cluster ONTAP dans une configuration de stockage privé NetApp

["Découvrez comment ajouter un espace de travail"](#).

## Connecteurs

Un connecteur permet à BlueXP de gérer les ressources et les processus au sein de votre environnement de cloud public. Il s'exécute sur une instance de machine virtuelle que vous déployez dans votre fournisseur cloud ou sur un hôte sur site que vous avez configuré.

Vous pouvez utiliser un connecteur avec plusieurs services de données cloud NetApp. Par exemple, si vous disposez déjà d'un connecteur pour BlueXP, vous pouvez le sélectionner lors de la configuration du service Cloud Tiering.

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

## Abonnements

Il s'agit des abonnements NetApp associés au compte sélectionné.

Lorsque vous vous abonnez à BlueXP depuis le marché d'un fournisseur de services Cloud, vous êtes redirigé vers le site Web BlueXP où vous devez enregistrer votre abonnement et l'associer à des comptes spécifiques.

Une fois que vous vous êtes abonné, chaque abonnement est disponible dans le widget gérer le compte. Vous ne verrez que les abonnements associés au compte que vous consultez actuellement.

Vous avez la possibilité de renommer un abonnement et de dissocier l'abonnement d'un ou plusieurs comptes.

Par exemple, disons que vous avez deux comptes et que chacun est facturé par le biais d'abonnements distincts. Vous pouvez dissocier un abonnement de l'un des comptes afin que les utilisateurs de ce compte ne choisissent pas accidentellement l'abonnement incorrect lors de la création d'un environnement de travail Cloud Volume ONTAP.

["Découvrez comment gérer vos abonnements".](#)

## Exemples

Les exemples suivants décrivent comment configurer vos comptes.

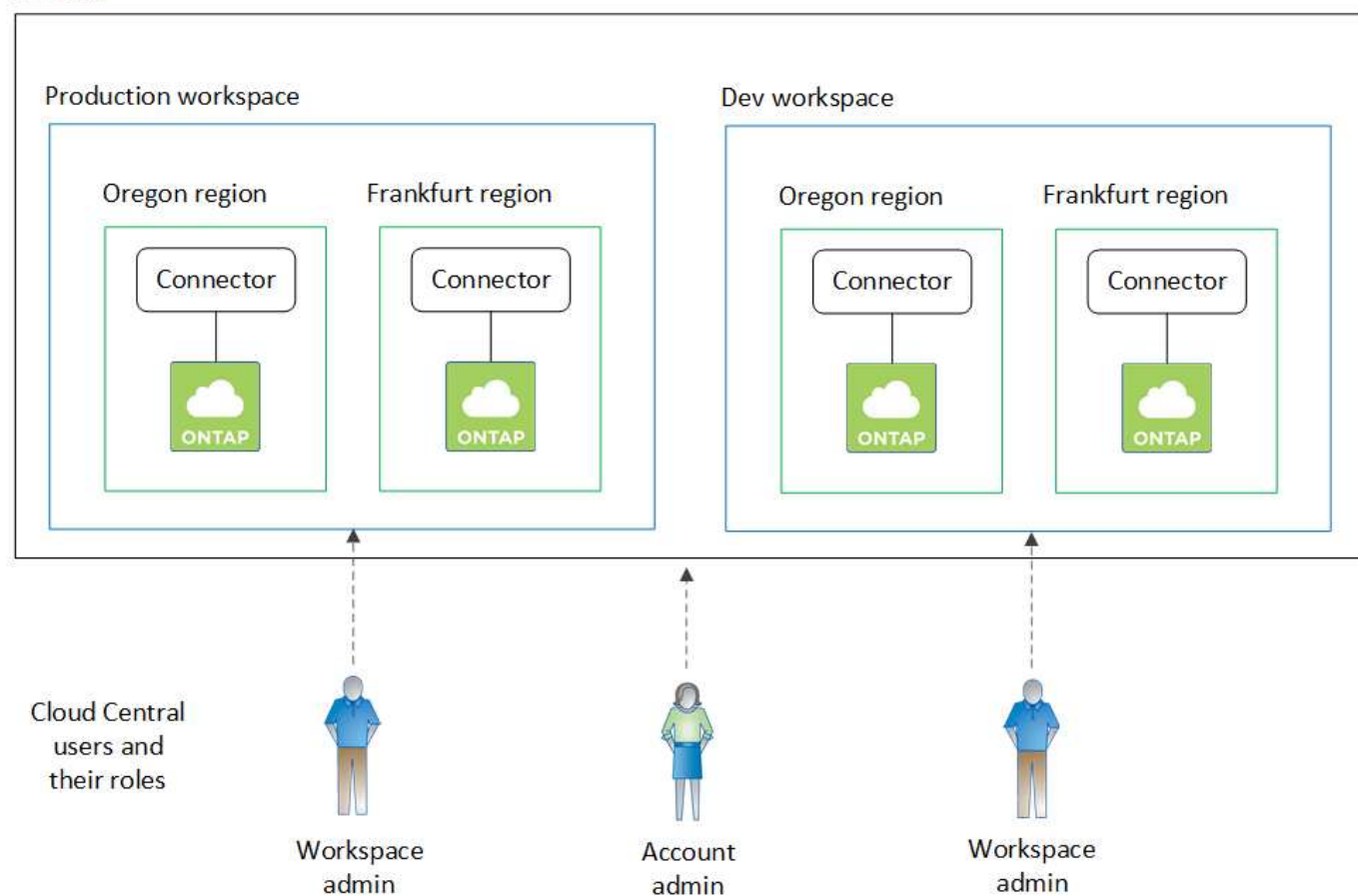


Dans les deux exemples d'images suivantes, le connecteur et les systèmes Cloud Volumes ONTAP ne résident pas *dans* le compte NetApp --ils s'exécutent dans un fournisseur cloud. Il s'agit d'une représentation conceptuelle de la relation entre chaque composant.

### Exemple 1

L'exemple suivant montre un compte qui utilise deux espaces de travail pour créer des environnements isolés. Le premier espace de travail est pour un environnement de production et le second pour un environnement de développement.

## Account



### Exemple 2

Voici un autre exemple illustrant le niveau de colocation le plus élevé en utilisant deux comptes NetApp distincts. Par exemple, un fournisseur de services peut utiliser BlueXP pour fournir des services à ses clients, tout en utilisant un autre compte pour fournir une reprise après incident pour l'une de ses unités commerciales.

Notez que le compte 2 comprend deux connecteurs distincts. Cela peut arriver si vous disposez de systèmes dans des régions distinctes ou dans des fournisseurs cloud distincts.



## Configurez des espaces de travail et des utilisateurs sur votre compte NetApp

Lorsque vous vous connectez à BlueXP pour la première fois, vous êtes invité à créer un *compte NetApp*. Ce compte fournit la colocation et vous permet d'organiser les utilisateurs et les ressources dans des *espaces de travail* isolés.

["Découvrez comment fonctionnent les comptes NetApp".](#)

Configurez votre compte NetApp afin que les utilisateurs puissent accéder à BlueXP et accéder aux environnements de travail dans un espace de travail. Il vous suffit d'ajouter un seul utilisateur ou plusieurs utilisateurs et espaces de travail.

### Ajouter des espaces de travail

Dans BlueXP, les espaces de travail vous permettent d'isoler un ensemble d'environnements de travail d'autres environnements de travail et d'autres utilisateurs. Par exemple, vous pouvez créer deux espaces de travail et associer des utilisateurs distincts à chaque espace de travail.

### Étapes

1. En haut de "BlueXP", Cliquez sur le menu déroulant **compte**.



2. Cliquez sur **gérer le compte** en regard du compte actuellement sélectionné.



3. Cliquez sur **espaces de travail**.
4. Cliquez sur **Ajouter un nouvel espace de travail**.
5. Entrez un nom pour l'espace de travail et cliquez sur **Ajouter**.

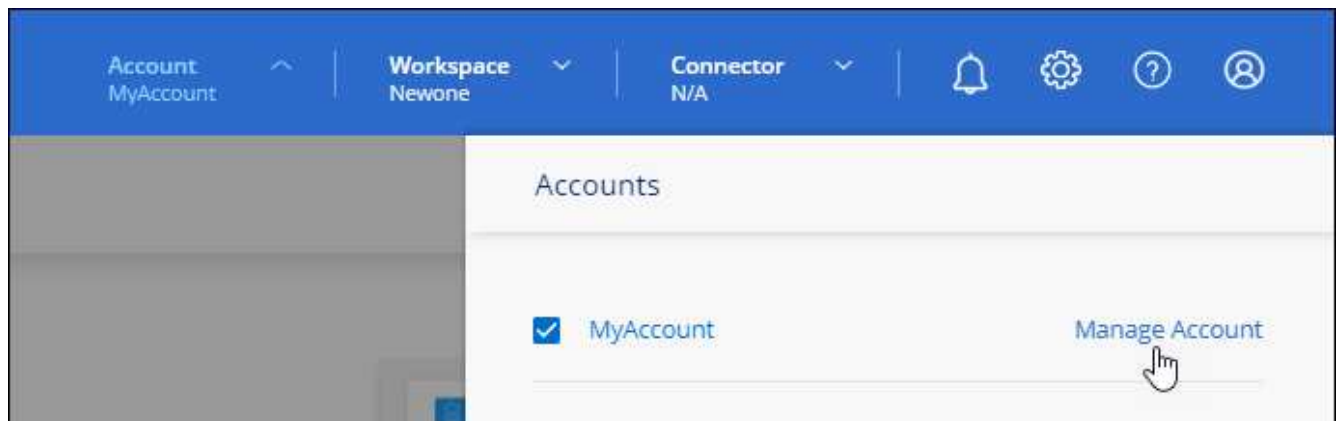
Si un administrateur d'espace de travail doit accéder à cet espace de travail, vous devez associer l'utilisateur. Vous devez également associer des connecteurs à l'espace de travail pour que les administrateurs de l'espace de travail puissent utiliser ces connecteurs.

### Ajouter des utilisateurs

Associez les utilisateurs à votre compte NetApp pour qu'ils puissent créer et gérer des environnements de travail dans BlueXP.

#### Étapes

1. Si l'utilisateur ne l'a pas déjà fait, demandez-lui d'aller à "[Site Web NetApp BlueXP](#)" et s'inscrire.
2. En haut de "[BlueXP](#)", Cliquez sur le menu déroulant **compte** et cliquez sur **gérer compte**.



3. Dans l'onglet membres, cliquez sur **associer utilisateur**.
4. Entrez l'adresse e-mail de l'utilisateur et sélectionnez un rôle pour l'utilisateur :
  - **Administrateur de compte**: Peut effectuer n'importe quelle action dans BlueXP.
  - **Workspace Admin** : permet de créer et de gérer des ressources dans des espaces de travail attribués.
  - **Compliance Viewer** : peut uniquement afficher les informations de gouvernance et de conformité de Cloud Data Sense et générer des rapports pour les espaces de travail auxquels ils sont autorisés à accéder.

- **Admin SnapCenter** : peut utiliser le service SnapCenter pour créer des sauvegardes cohérentes avec les applications et restaurer les données à l'aide de ces sauvegardes. Ce service est actuellement en version bêta.
5. Si vous avez sélectionné un compte autre que Account Admin, sélectionnez un ou plusieurs espaces de travail à associer à cet utilisateur.

**Associate User**

To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central.

User's Email

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1 x

Cancel Associate User

6. Cliquez sur **associé**.

L'utilisateur doit recevoir un e-mail de la part du site Web NetApp BlueXP intitulé « Account Association ». L'e-mail inclut les informations nécessaires pour accéder à BlueXP.

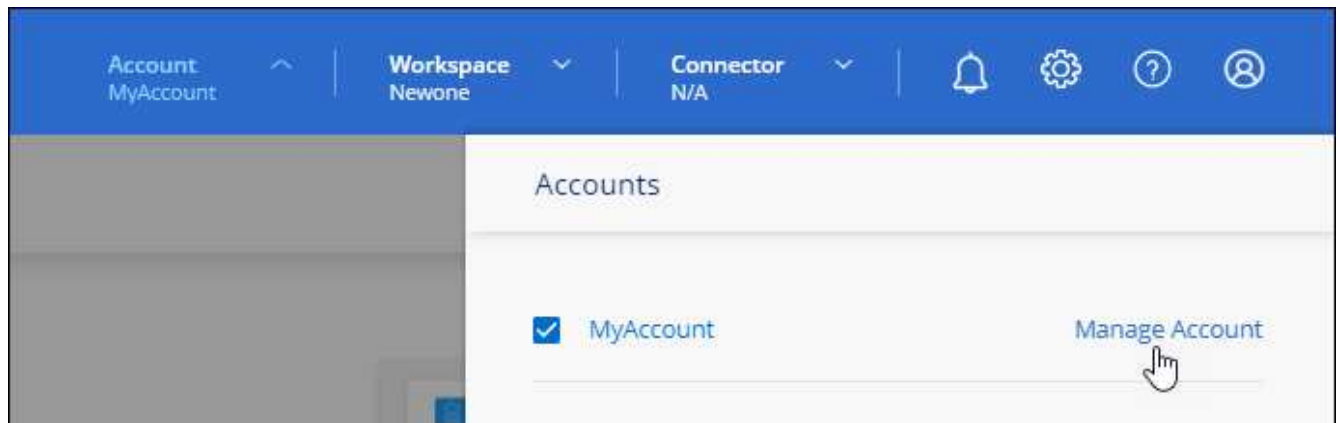
### Associer les administrateurs d'espace de travail aux espaces de travail

Vous pouvez associer des administrateurs d'espace de travail à des espaces de travail supplémentaires à tout moment. L'association de l'utilisateur lui permet de créer et d'afficher les environnements de travail dans cet espace de travail.

#### Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.





2. Dans l'onglet membres, cliquez sur le menu d'action de la ligne correspondant à l'utilisateur.



3. Cliquez sur **gérer les espaces de travail**.
4. Sélectionnez un ou plusieurs espaces de travail et cliquez sur **appliquer**.

L'utilisateur peut désormais accéder à ces espaces de travail depuis BlueXP, tant que le connecteur était également associé aux espaces de travail.

### Associer des connecteurs aux espaces de travail

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 sur les utilisateurs, les espaces de travail et les connecteurs"](#).

### Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.





2. Cliquez sur **connecteur**.
3. Cliquez sur **gérer les espaces de travail** pour le connecteur que vous souhaitez associer.
4. Sélectionnez un ou plusieurs espaces de travail et cliquez sur **appliquer**.

Les administrateurs d'espace de travail peuvent désormais utiliser ces connecteurs pour créer des systèmes Cloud Volumes ONTAP.

### Et la suite ?

Maintenant que vous avez configuré votre compte, vous pouvez le gérer à tout moment en supprimant des utilisateurs, en gérant des espaces de travail, des connecteurs et des abonnements. "[Découvrez comment gérer votre compte](#)".

## 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 multicloud (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. ["Apprenez quand un connecteur est nécessaire"](#).

Cette page explique comment créer un connecteur dans AWS 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.

## Démarrage rapide

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

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.

an IAM policy, Afficher le rôle IAM ou up AWS authentication, suivez les instructions étape par étape.

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.

up networking, Afficher les besoins en matière de mise en réseau.

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

a Connector, 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**.

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.

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.

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://*.cloudmanager.cloud.netapp.com</code> <code>https://cloudmanager.cloud.netapp.com</code>	Pour fournir des fonctions et des services SaaS dans BlueXP.
<code>https://cloudmanagerinfraproduct.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

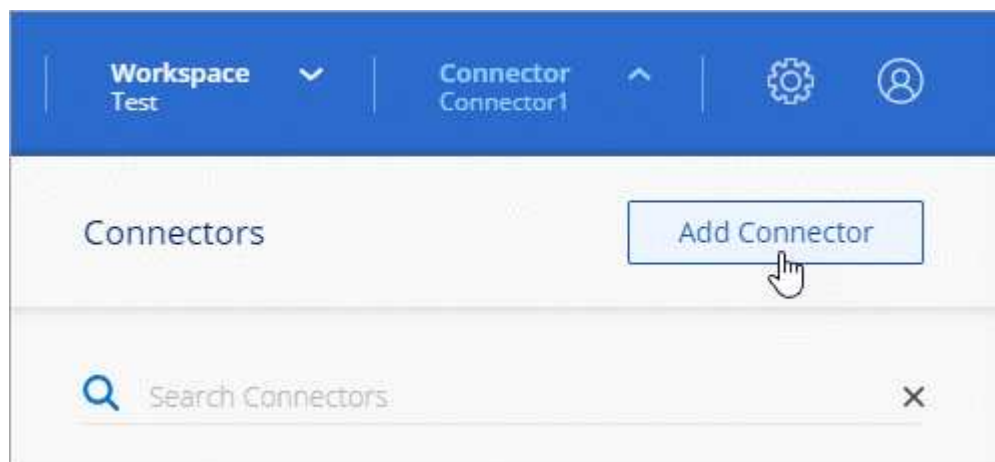
Il existe un conflit possible avec des adresses IP dans la plage 172. "[En savoir plus sur cette limitation](#)".

### 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 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 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.

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 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.

### 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. ["Apprenez quand un connecteur est nécessaire"](#).

Cette page explique comment créer un connecteur dans Azure 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.

## 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.

a Connector using your Azure account, 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.

a Connector using a service principal, 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.
https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com	Pour fournir des fonctions et des services SaaS dans BlueXP.
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

```

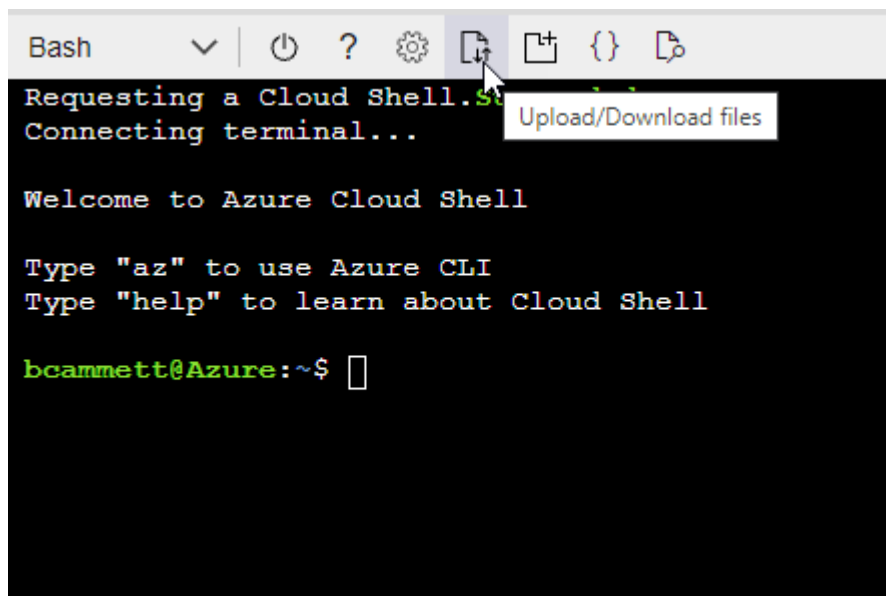
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],

```

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**.

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.

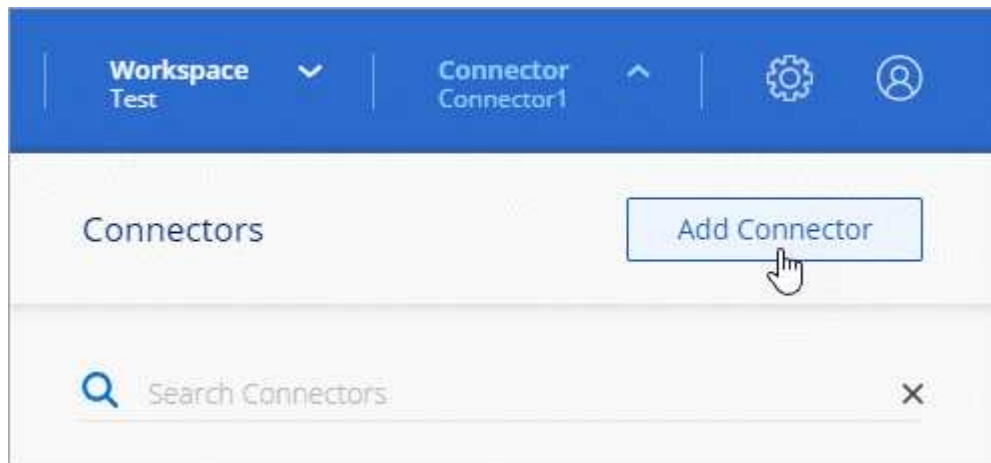
### Ce dont vous avez besoin, 8217;II

- 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.

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. an Azure Active Directory application.
2. the application to a role.
3. Windows Azure Service Management API permissions.
4. the application ID and directory ID.
5. a client secret.

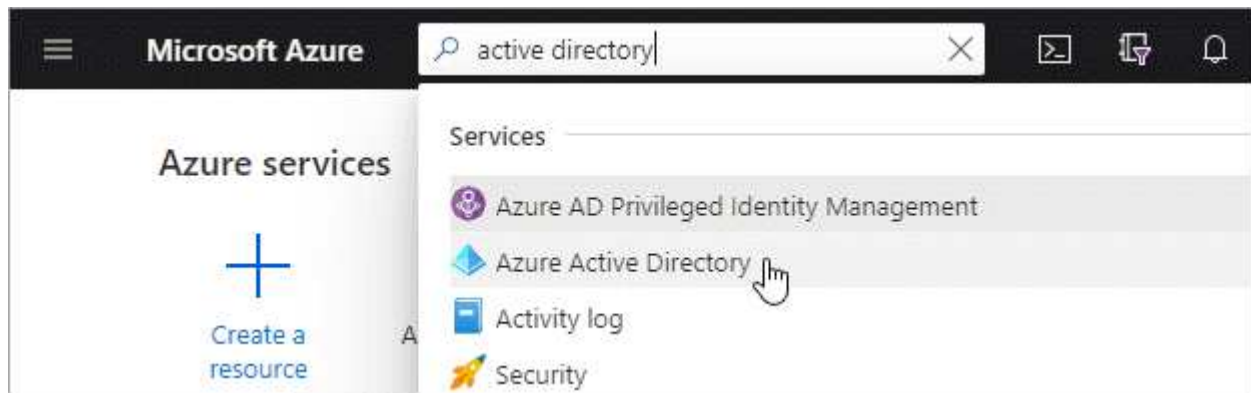
## Créez une application Azure Active Directory

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

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**.

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](#)

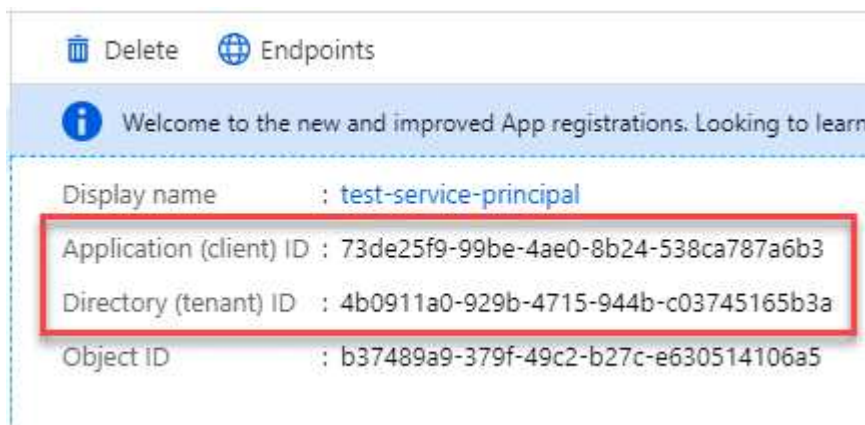
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> <b>user_impersonation</b> Access Azure Service Management as organization users (preview) ⓘ	-

## 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.

<a href="#">+ New client secret</a>		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA

Copy to clipboard

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, 8217;II

- 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 the application ID and directory ID.
    - ID de répertoire (locataire) : voir the application ID and directory ID.
    - Secret client : voir a client secret.
  - 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.

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'un administrateur 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 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.

## 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.

&lt;span class=« image »&gt;&lt;img src=«<a href=«https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-1.png""" class="bare">https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-1.png"</a> alt=« one »&gt;&lt;/span&gt; définissez les autorisations

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

```
up permissions to deploy the Connector.
```

- 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.


```
up a service account for the Connector.
```

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

```
up shared VPC permissions.
```

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.

```
up networking, Afficher les besoins en matière de mise en réseau.
```

 <https://raw.githubusercontent.com/NetAppDocs/common/main/media/number-3.png> alt="trois" data-bbox="75 491 491 522"/> Activer 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

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

```
a Connector, 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.

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".

- 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.

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"> <li>"<a href="#">Les autorisations trouvées dans cette section ci-dessus</a>"</li> </ul>	<ul style="list-style-type: none"> <li>compute.networkUser</li> </ul>	Déploiement du connecteur dans le projet de service
Connecteur de compte de service	Personnalisées	Projet de service	<ul style="list-style-type: none"> <li>"<a href="#">Les autorisations trouvées dans cette section ci-dessus</a>"</li> </ul>	<ul style="list-style-type: none"> <li>compute.networkUser</li> <li>deploymentmanager.editor</li> </ul>	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"> <li>storage.admin</li> <li>Membre: Compte de service BlueXP à partir de serviceAccount.user</li> </ul>	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"> <li>Editeur (par défaut)</li> </ul>	<ul style="list-style-type: none"> <li>compute.networkUser</li> </ul>	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	<ul style="list-style-type: none"> <li>Editeur (par défaut)</li> </ul>	<ul style="list-style-type: none"> <li>compute.networkUser</li> </ul>	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
<code>https://support.netapp.com</code>	Pour obtenir des informations sur les licences et envoyer des messages AutoSupport au support NetApp.
<code>https://*.cloudmanager.cloud.netapp.com</code> <code>https://cloudmanager.cloud.netapp.com</code>	Pour fournir des fonctions et des services SaaS dans BlueXP.
<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"](#).

## Activez les API Google Cloud

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

### Étape

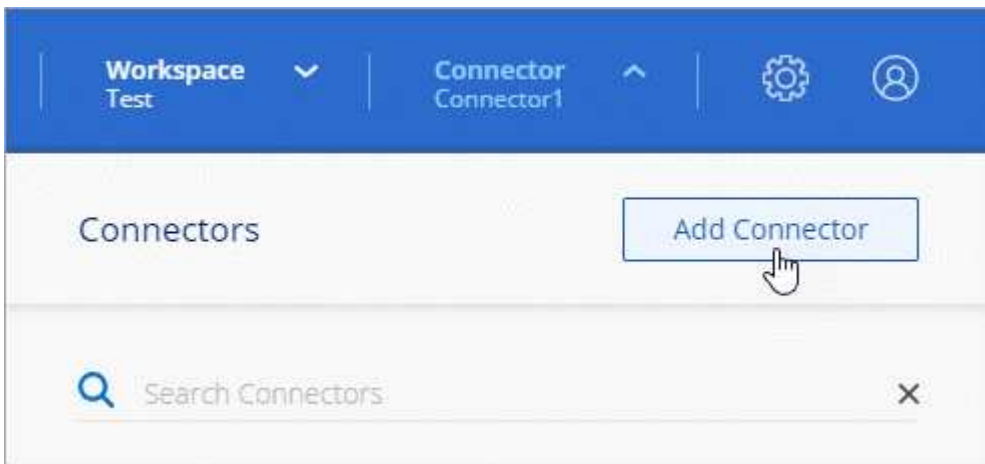
1. ["Activez les API Google Cloud suivantes dans votre projet"](#).
  - API Cloud Deployment Manager V2
  - API de journalisation cloud
  - API Cloud Resource Manager
  - API du moteur de calcul
  - API de gestion des identités et des accès

## 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.

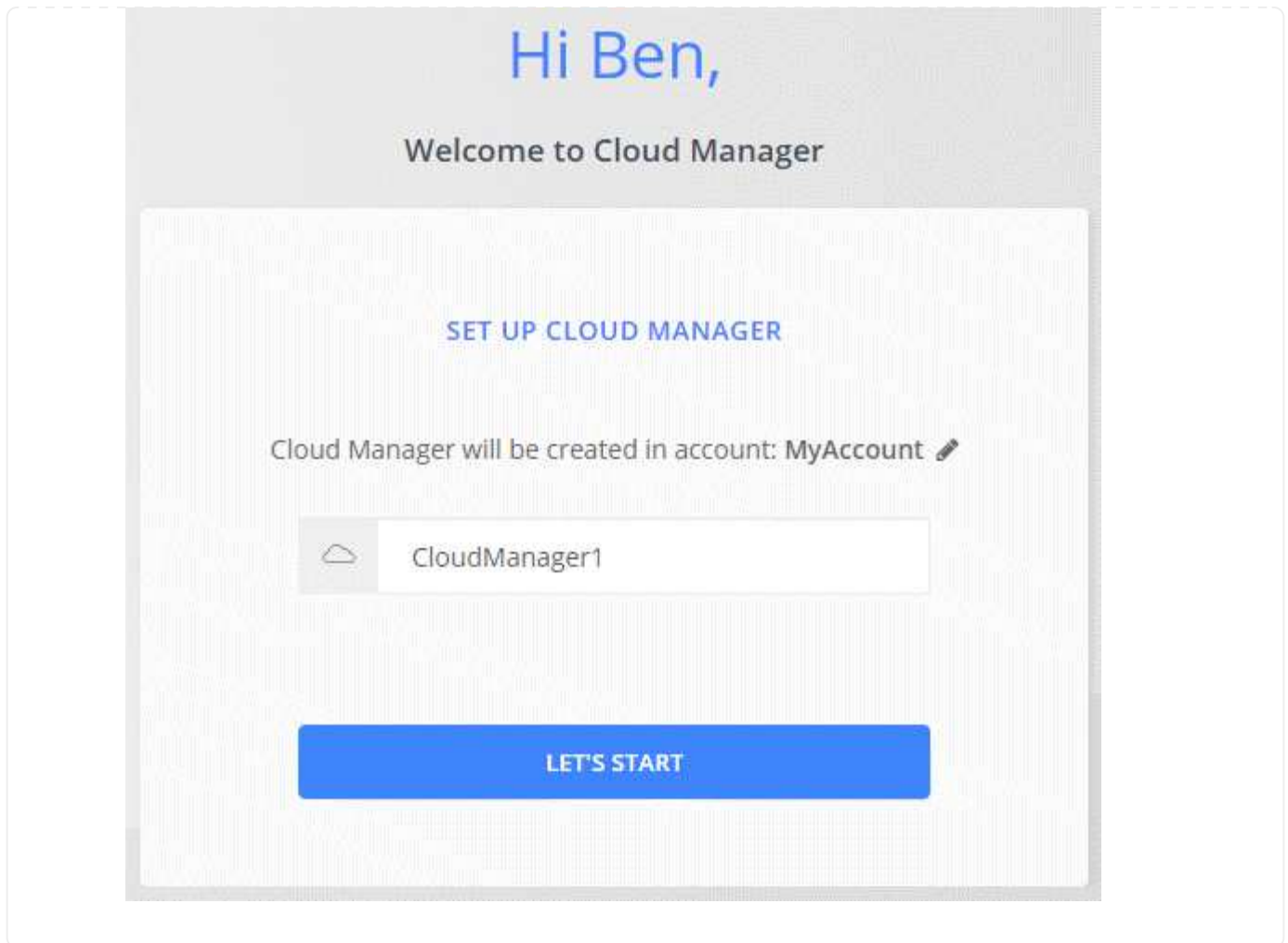
1. Ouvrez un navigateur Web à partir d'un hôte connecté à l'instance Connector et saisissez l'URL suivante :

`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.



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\[\]](https://ipaddress[])

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

## Par où aller plus loin

Maintenant que vous vous êtes connecté et que vous avez configuré BlueXP, les utilisateurs peuvent commencer à créer et découvrir des environnements de travail.

- ["Commencez avec Cloud Volumes ONTAP pour AWS"](#)
- ["Commencez avec Cloud Volumes ONTAP pour Azure"](#)
- ["Lancez-vous avec Cloud Volumes ONTAP pour Google Cloud"](#)
- ["Configurer Azure NetApp Files"](#)
- ["Configurer Amazon FSX pour ONTAP"](#)
- ["Configuration d'Cloud Volumes Service pour AWS"](#)
- ["Découvrez un cluster ONTAP sur site"](#)
- ["Découvrez vos compartiments Amazon S3"](#)

# Administration de BlueXP

## Comptes NetApp

### Gestion de votre compte NetApp

"Après avoir effectué la configuration initiale", Vous pouvez gérer les paramètres de votre compte ultérieurement en gérant les utilisateurs, les comptes de service, les espaces de travail, les connecteurs et les abonnements.

"Découvrez comment fonctionnent les comptes NetApp".

### Gestion de votre compte à l'aide de l'API de location

Si vous souhaitez gérer les paramètres de votre compte en envoyant des demandes API, vous devez utiliser l'API *Tenancy*. Cette API est différente de l'API BlueXP, que vous utilisez pour créer et gérer des environnements de travail Cloud Volumes ONTAP.

"Affichez les terminaux de l'API de colocation"

### Création et gestion des utilisateurs

L'utilisateur de votre compte peut accéder aux ressources de gestion des espaces de travail de votre compte.

#### Ajout d'utilisateurs

Associez les utilisateurs à votre compte NetApp pour qu'ils puissent créer et gérer des environnements de travail dans BlueXP.

#### Étapes

1. Si l'utilisateur ne l'a pas déjà fait, demandez-lui d'aller à "[Site Web NetApp BlueXP](#)" et s'inscrire.
2. En haut de BlueXP, cliquez sur la liste déroulante **Account**.



3. Cliquez sur **gérer le compte** en regard du compte actuellement sélectionné.



4. Dans l'onglet membres, cliquez sur **associer utilisateur**.
5. Entrez l'adresse e-mail de l'utilisateur et sélectionnez un rôle pour l'utilisateur :
  - **Administrateur de compte**: Peut effectuer n'importe quelle action dans BlueXP.
  - **Workspace Admin** : permet de créer et de gérer des ressources dans des espaces de travail attribués.
  - **Compliance Viewer** : peut uniquement afficher les informations de conformité de Cloud Data Sense et générer des rapports pour les espaces de travail auxquels ils sont autorisés à accéder.
  - **Admin SnapCenter** : peut utiliser le service SnapCenter pour créer des sauvegardes cohérentes avec les applications et restaurer les données à l'aide de ces sauvegardes. *Ce service est actuellement en version bêta.*
6. Si vous avez sélectionné Workspace Admin ou Compliance Viewer, sélectionnez un ou plusieurs espaces de travail à associer à cet utilisateur.



The image shows a dialog box titled "Associate User" with a user icon at the top. Below the title is a light blue banner with instructions: "To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central." The form contains three fields: "User's Email" with the text "test@netapp.com", "Role" with a dropdown menu showing "Workspace Admin", and "Associate User to Workspaces" with a dropdown menu showing "Workspace-1" and a close icon. At the bottom are two buttons: "Cancel" and "Associate User".



### Associate User

To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central.

User's Email

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1

Cancel Associate User

7. Cliquez sur **associé**.

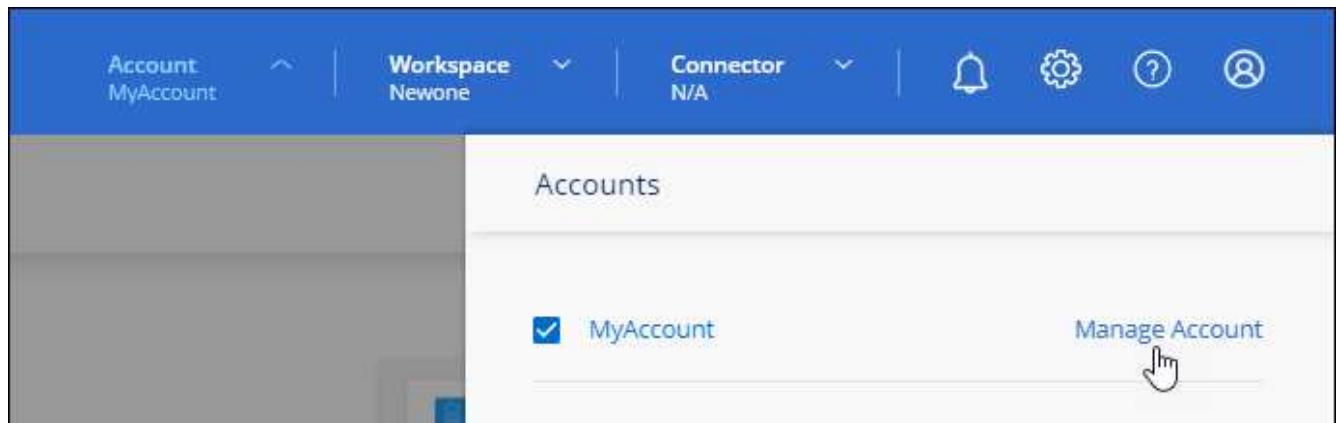
L'utilisateur doit recevoir un e-mail de NetApp BlueXP intitulé « Account Association ». L'e-mail inclut les informations nécessaires pour accéder à BlueXP.

#### Suppression d'utilisateurs

En effet, la dissociation permet d'interdire l'accès aux ressources d'un compte NetApp.

#### Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.



2. Dans l'onglet membres, cliquez sur le menu d'action de la ligne correspondant à l'utilisateur.



3. Cliquez sur **Disassocier utilisateur** et cliquez sur **Disassocier** pour confirmer.

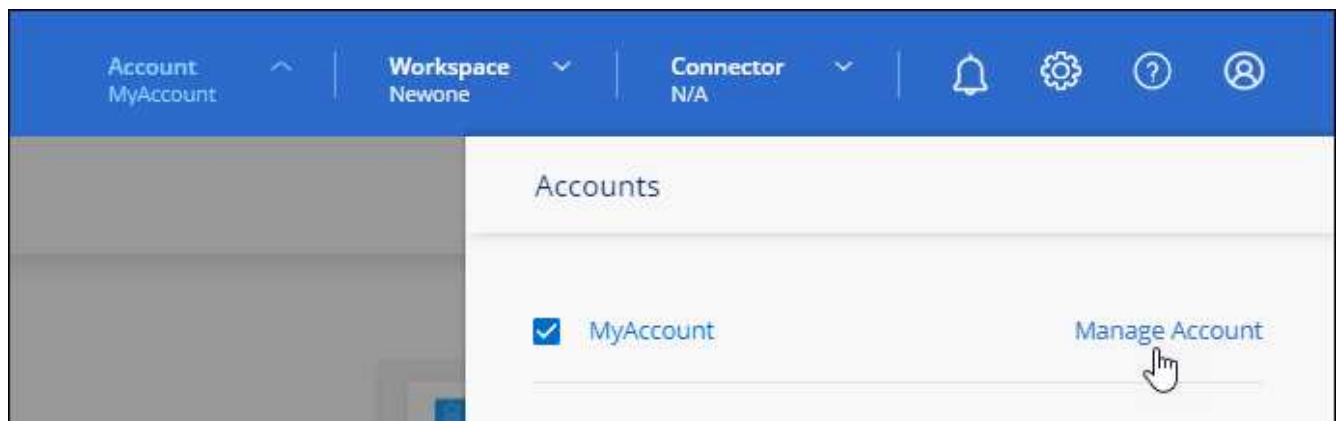
L'utilisateur ne peut plus accéder aux ressources de ce compte NetApp.

### Gestion des espaces de travail d'un Workspace Admin

Vous pouvez associer et dissocier les administrateurs d'espace de travail avec des espaces de travail à tout moment. L'association de l'utilisateur lui permet de créer et d'afficher les environnements de travail dans cet espace de travail.

### Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.



2. Dans l'onglet membres, cliquez sur le menu d'action de la ligne correspondant à l'utilisateur.

5 Members						
Type	Name	Email	Role	Workspace		
	Ben		☆ Account Admin	All Workspaces	...	
	Tom		☆ Account Admin	All Workspaces	...	
	Ben		Workspace Admin	Newone		

3. Cliquez sur **gérer les espaces de travail**.

4. Sélectionnez les espaces de travail à associer à l'utilisateur et cliquez sur **appliquer**.

L'utilisateur peut désormais accéder à ces espaces de travail depuis BlueXP, tant que le connecteur était également associé aux espaces de travail.

## Création et gestion des comptes de service

Un compte de service agit comme un « utilisateur » qui peut effectuer des appels API autorisés vers BlueXP à des fins d'automatisation. Il est ainsi plus facile de gérer l'automatisation, car il n'est pas nécessaire de créer des scripts d'automatisation basés sur le compte d'utilisateur réel d'une personne qui quitte l'entreprise à tout moment. Et si vous utilisez la fédération, vous pouvez créer un jeton sans générer de jeton d'actualisation à partir du cloud.

Vous donnez des autorisations à un compte de service en lui attribuant un rôle, tout comme n'importe quel autre utilisateur BlueXP. Vous pouvez également associer le compte de service à des espaces de travail spécifiques afin de contrôler les environnements de travail (ressources) auxquels le service peut accéder.

Lorsque vous créez le compte de service, BlueXP vous permet de copier ou de télécharger un ID client et un secret client pour le compte de service. Cette paire de clés est utilisée pour l'authentification avec BlueXP.

### Création d'un compte de service

Créez autant de comptes de services que nécessaire pour gérer les ressources de vos environnements de travail.

### Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account**.



2. Cliquez sur **gérer le compte** en regard du compte actuellement sélectionné.



3. Dans l'onglet membres, cliquez sur **Créer un compte de service**.
4. Entrez un nom et sélectionnez un rôle. Si vous avez choisi un rôle autre que Administrateur de compte, choisissez l'espace de travail à associer à ce compte de service.
5. Cliquez sur **Créer**.
6. Copiez ou téléchargez l'ID client et le secret client.

Le secret client n'est visible qu'une seule fois et n'est pas stocké n'importe où par BlueXP. Copiez ou téléchargez le secret et rangez-le en toute sécurité.

7. Cliquez sur **Fermer**.

#### Obtention d'un jeton de porteur pour un compte de service

Pour passer des appels API à "[API de location](#)", vous devrez obtenir un jeton de porteur pour un compte de service.

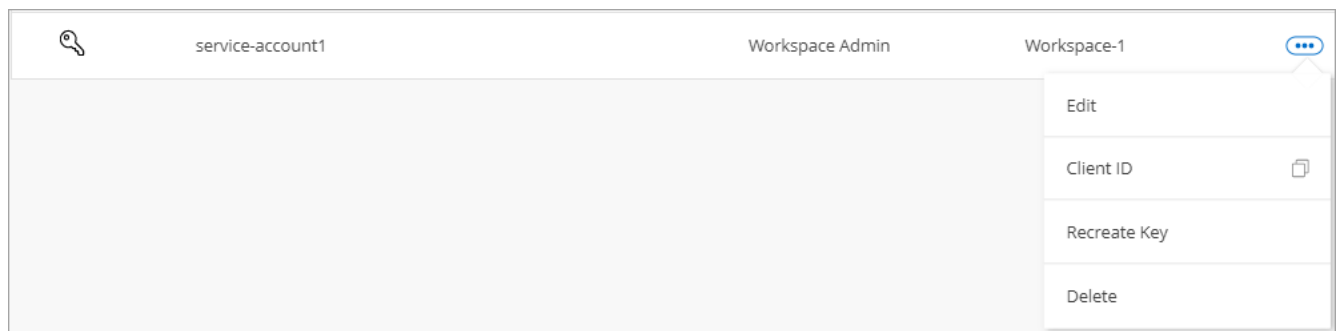
["Découvrez comment créer un jeton de compte de service"](#)

#### Copie de l'ID client

Vous pouvez copier l'ID client d'un compte de service à tout moment.

#### Étapes

1. Dans l'onglet membres, cliquez sur le menu d'action de la ligne correspondant au compte de service.



2. Cliquez sur **ID client**.
3. L'ID est copié dans le presse-papiers.

## Recréation des clés

La recréation de la clé supprimera la clé existante pour ce compte de service, puis créera une nouvelle clé. Vous ne pourrez pas utiliser la touche précédente.

### Étapes

1. Dans l'onglet membres, cliquez sur le menu d'action de la ligne correspondant au compte de service.



2. Cliquez sur **recréer la clé**.
3. Cliquez sur **recréer** pour confirmer.
4. Copiez ou téléchargez l'ID client et le secret client.

Le secret client n'est visible qu'une seule fois et n'est pas stocké n'importe où par BlueXP. Copiez ou téléchargez le secret et rangez-le en toute sécurité.

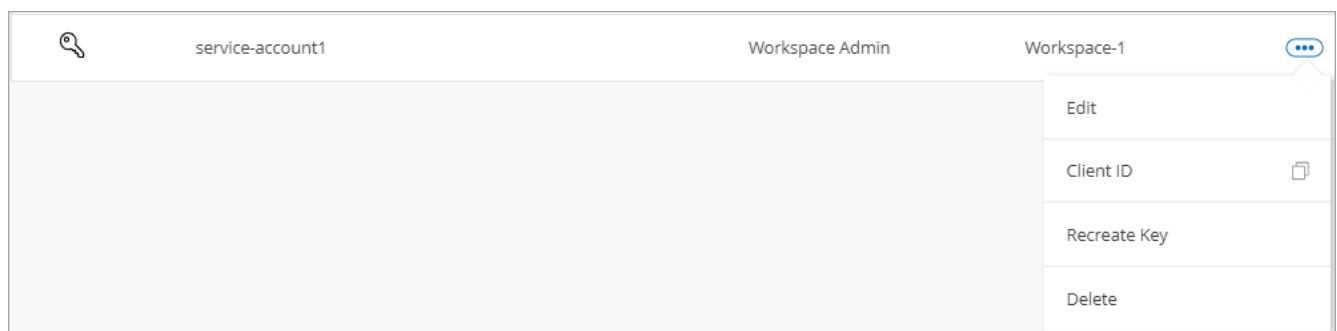
5. Cliquez sur **Fermer**.

## Suppression d'un compte de service

Supprimez un compte de service si vous n'avez plus besoin de l'utiliser.

### Étapes

1. Dans l'onglet membres, cliquez sur le menu d'action de la ligne correspondant au compte de service.



2. Cliquez sur **Supprimer**.
3. Cliquez à nouveau sur **Supprimer** pour confirmer.

## Gestion des espaces de travail

Gérez vos espaces de travail en les créant, en les renommant et en les supprimant. Notez que vous ne pouvez pas supprimer un espace de travail s'il contient des ressources. Elle doit être vide.



## Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.
2. Cliquez sur **espaces de travail**.
3. Choisissez l'une des options suivantes :
  - Cliquez sur **Ajouter un nouvel espace de travail** pour créer un nouvel espace de travail.
  - Cliquez sur **Renommer** pour renommer l'espace de travail.
  - Cliquez sur **Supprimer** pour supprimer l'espace de travail.

## Gestion des espaces de travail d'un connecteur

Vous devez associer le connecteur aux espaces de travail pour que les administrateurs d'espace de travail puissent accéder à ces espaces de travail depuis BlueXP.

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 sur les utilisateurs, les espaces de travail et les connecteurs"](#).

## Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.
2. Cliquez sur **connecteur**.
3. Cliquez sur **gérer les espaces de travail** pour le connecteur que vous souhaitez associer.
4. Sélectionnez les espaces de travail à associer au connecteur et cliquez sur **appliquer**.

## Gestion des abonnements

Après vous être abonné au Marketplace d'un fournisseur cloud, chaque abonnement est disponible dans le widget Account Settings. Vous avez la possibilité de renommer un abonnement et de dissocier l'abonnement d'un ou plusieurs comptes.

Par exemple, disons que vous avez deux comptes et que chacun est facturé par le biais d'abonnements distincts. Vous pouvez dissocier un abonnement de l'un des comptes afin que les utilisateurs de ce compte ne choisissent pas accidentellement l'abonnement incorrect lors de la création d'un environnement de travail Cloud Volume ONTAP.

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

## Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.
2. Cliquez sur **abonnements**.

Vous ne verrez que les abonnements associés au compte que vous consultez actuellement.

3. Cliquez sur le menu d'action de la ligne correspondant à l'abonnement que vous souhaitez gérer.

2 Subscriptions

Name	Service	Cloud Provider	Status
QA Subscription	test-service	aws	Unsubscribed
metering service subscription QA !!!!	cloud-volumes-ontap	aws	Subscribed

Rename Subscription  
Manage Accounts

4. Choisissez de renommer l'abonnement ou de gérer les comptes associés à l'abonnement.

### Modification du nom de votre compte

Changez le nom de votre compte à tout moment pour le changer en quelque chose de significatif pour vous.

#### Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.
2. Dans l'onglet **vue d'ensemble**, cliquez sur l'icône de modification en regard du nom du compte.
3. Saisissez un nouveau nom de compte et cliquez sur **Enregistrer**.

### Permettre des aperçus privés

Laissez des aperçus privés de votre compte accéder aux nouveaux services clouds NetApp disponibles dans BlueXP.

Les services d'aperçu privé ne sont pas garantis de se comporter comme prévu et peuvent supporter des interruptions et être des fonctionnalités manquantes.

#### Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.
2. Dans l'onglet **Présentation**, activez le paramètre **Autoriser aperçu privé**.

### Permettre des services tiers

Autoriser les services tiers de votre compte à accéder à des services tiers disponibles dans BlueXP. Les services clouds tiers sont similaires aux services proposés par NetApp, mais ils sont gérés et pris en charge par des sociétés tierces.

#### Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.
2. Dans l'onglet **Présentation**, activez le paramètre **Autoriser les services tiers**.

### Désactivation de la plateforme SaaS

Nous ne recommandons pas de désactiver la plate-forme SaaS sauf si vous devez vous conformer aux politiques de sécurité de votre entreprise. En désactivant la plateforme SaaS, vous vous limitez votre capacité à utiliser les services cloud intégrés de NetApp.

Les services suivants ne sont pas disponibles auprès de BlueXP si vous désactivez la plate-forme SaaS :

- Sens des données cloud
- Kubernetes
- Tiering dans le cloud
- Cache global de fichiers

Si vous désactivez la plateforme SaaS, vous devrez effectuer toutes les tâches à partir de ["Interface utilisateur locale disponible sur un connecteur"](#).



Il s'agit d'une action irréversible qui vous empêchera d'utiliser la plate-forme BlueXP SaaS. Vous devrez effectuer des actions à partir du connecteur local. Vous ne pourrez pas utiliser de nombreux services cloud intégrés de NetApp et mettre à disposition de la plateforme SaaS aura besoin de l'aide de NetApp.

## Étapes

1. En haut de BlueXP, cliquez sur la liste déroulante **Account** et cliquez sur **Manage Account**.
2. Dans l'onglet vue d'ensemble, activez l'option pour désactiver l'utilisation de la plateforme SaaS.

## Surveillance des opérations dans votre compte

Vous pouvez surveiller l'état des opérations que BlueXP effectue pour voir si des problèmes doivent être résolus. Vous pouvez afficher l'état dans le centre de notification, dans le calendrier ou envoyer des notifications à votre courrier électronique.

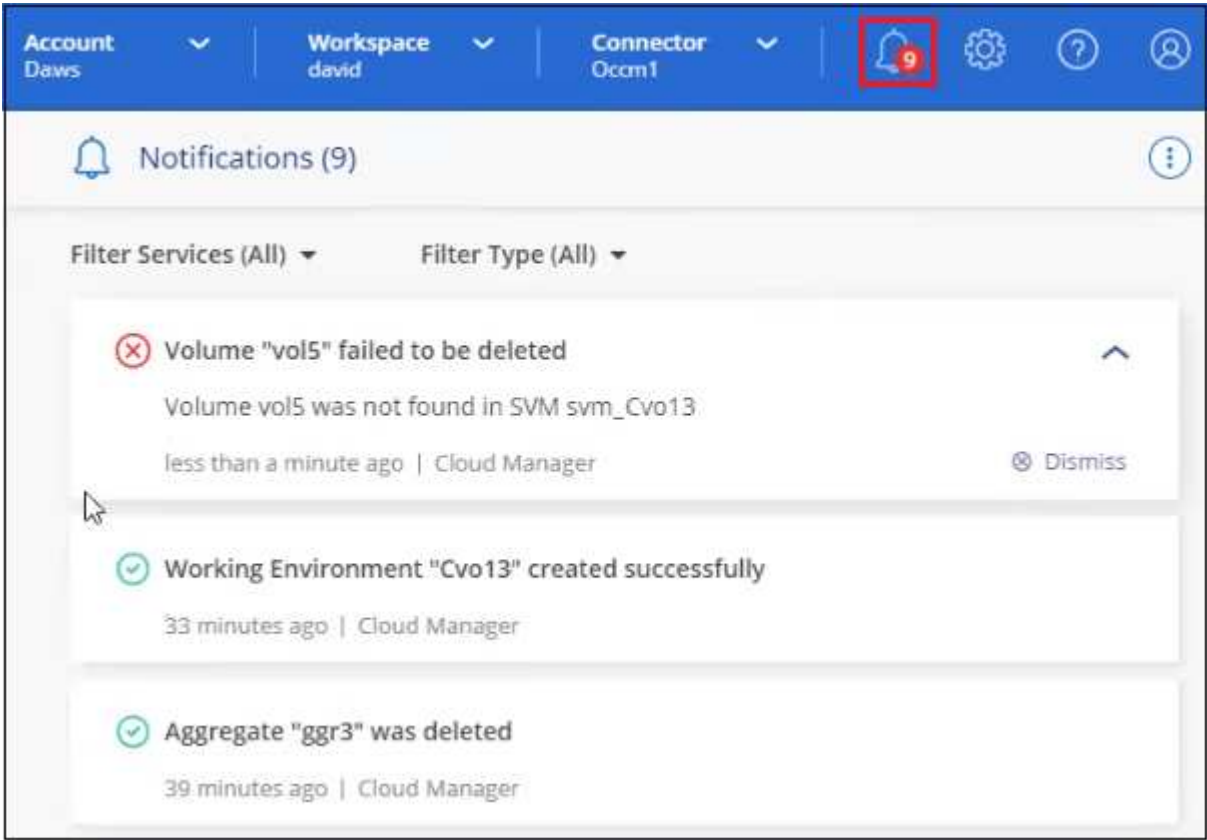
Ce tableau fournit une comparaison du centre de notification et du calendrier pour vous permettre de comprendre ce que chacun a à offrir.

Centre de notification	De la chronologie
Affiche l'état général des événements et des actions	Fournit des détails sur chaque événement ou action pour une enquête plus approfondie
Affiche l'état de la session de connexion en cours - les informations n'apparaîtront pas dans le Centre de notification après la déconnexion	Conserve le statut pour le dernier mois
Affiche uniquement les actions initiées dans l'interface utilisateur	Affiche toutes les actions à partir de l'interface utilisateur ou des API
Affiche les actions lancées par l'utilisateur	Affiche toutes les actions, qu'elles soient lancées par l'utilisateur ou par le système
Filtrez les résultats en fonction de l'importance	Filtrez par service, action, utilisateur, état, etc
Permet d'envoyer des notifications par e-mail aux utilisateurs du compte et à d'autres utilisateurs	Aucune capacité de messagerie

## Surveillance des activités à l'aide du Centre de notification

Les notifications suivent la progression des opérations que vous avez lancées dans BlueXP pour vous permettre de vérifier si l'opération a réussi ou non. Elles vous permettent d'afficher l'état de nombreuses actions BlueXP que vous avez lancées pendant votre session de connexion actuelle. Tous les services ne rapportent pas d'informations au Centre de notification pour le moment.

Vous pouvez afficher les notifications en cliquant sur le signal sonore de notification (🔔) dans la barre de menus. La couleur de la petite bulle dans la cloche indique la notification de gravité de niveau le plus élevé qui est active. Si vous voyez une bulle rouge, cela signifie qu'il y a une notification importante que vous devriez regarder.



Vous pouvez également configurer BlueXP pour envoyer des notifications par e-mail afin de vous informer de l'activité système importante, même lorsque vous n'êtes pas connecté au système. Des e-mails sont envoyés à tous les utilisateurs qui font partie de votre compte cloud NetApp ou à tout autre destinataire ayant besoin de connaître certains types d'activité système. Voir email notification settings, Définition des paramètres de notification par e-mail ci-dessous.

**Types de notification**

Les notifications sont classées dans les catégories suivantes :

Type de notification	Description
Primordial	Un problème peut entraîner une interruption des services si des mesures correctives ne sont pas prises immédiatement.
Erreur	Une action ou un processus s'est terminé avec un échec ou pourrait entraîner un échec si aucune mesure corrective n'est prise.
Avertissement	Un problème que vous devez savoir pour vous assurer qu'il n'atteint pas la gravité critique. Les notifications de ce niveau de gravité n'entraînent pas d'interruption des services, mais une action corrective immédiate peut ne pas être nécessaire.

Type de notification	Description
Recommandation	Il est recommandé de prendre des mesures pour améliorer le système ou un service donné, par exemple : réduction des coûts, suggestion de nouveaux services, configuration de sécurité recommandée, etc
Informations	Message fournissant des informations supplémentaires sur une action ou un processus.
Réussite	Une action ou un processus s'est terminé avec succès.

### Filtrage des notifications

Par défaut, toutes les notifications s'affichent. Vous pouvez filtrer les notifications que vous voyez dans le Centre de notification pour n'afficher que les notifications importantes pour vous. Vous pouvez filtrer par BlueXP "Service" et par notification "Type".

Par exemple, si vous souhaitez afficher uniquement les notifications "erreur" et "Avertissement" pour les opérations BlueXP, sélectionnez ces entrées et vous ne verrez que ces types de notifications.

### Définition des paramètres de notification par e-mail

Vous pouvez envoyer par e-mail des types de notifications spécifiques afin de vous informer de l'activité système importante, même lorsque vous n'êtes pas connecté à BlueXP. Il est possible d'envoyer des e-mails aux utilisateurs qui font partie de votre compte NetApp ou à tout autre destinataire ayant besoin de connaître certains types d'activité système.



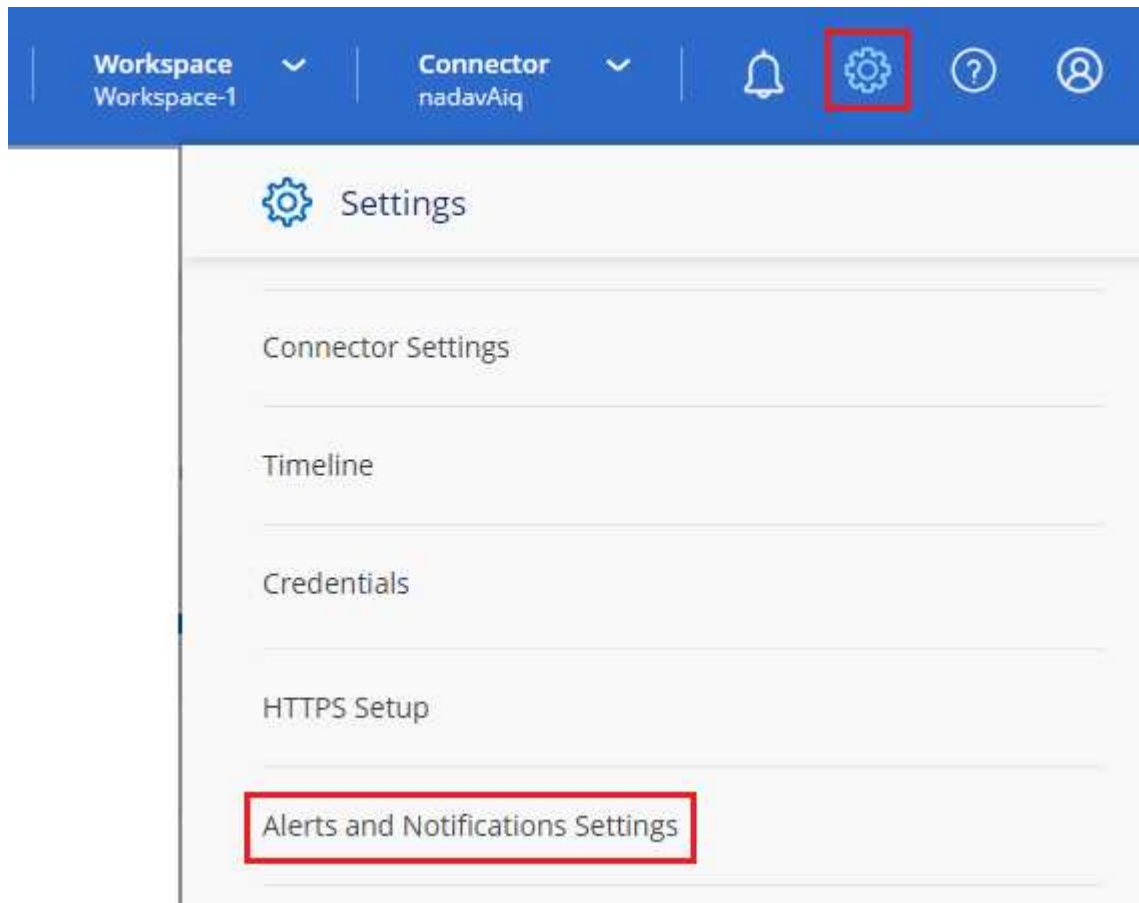
- À l'heure actuelle, seuls Cloud Sync et Cloud Backup envoient des notifications par e-mail. D'autres services seront ajoutés dans les prochaines versions.
- L'envoi de notifications par e-mail n'est pas pris en charge lorsque le connecteur est installé sur un site sans accès à Internet.

Par défaut, les administrateurs de compte BlueXP recevront des e-mails pour toutes les notifications « critiques » et « recommandations ». Par défaut, tous les autres utilisateurs et destinataires sont configurés pour ne pas recevoir d'e-mails de notification.

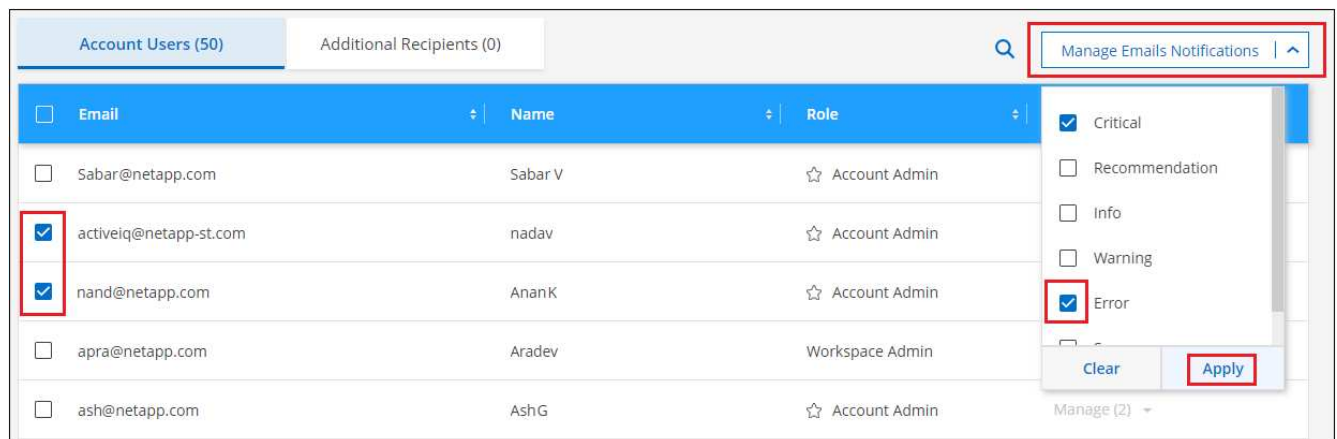
Pour personnaliser les paramètres de notifications, vous devez être administrateur de compte.

## Étapes

1. Dans la barre de menus BlueXP, cliquez sur **Paramètres > Paramètres d'alertes et de notifications**.



2. Sélectionnez un utilisateur ou plusieurs utilisateurs à partir de l'onglet *Account Users* ou de l'onglet *Additional Recipients*, puis choisissez le type de notifications à envoyer :
  - Pour apporter des modifications à un seul utilisateur, cliquez sur le menu dans la colonne Notifications de cet utilisateur, cochez les types de notifications à envoyer et cliquez sur **appliquer**.
  - Pour apporter des modifications à plusieurs utilisateurs, cochez la case de chaque utilisateur, cliquez sur **gérer les notifications par e-mail**, cochez les types de notifications à envoyer et cliquez sur **appliquer**.

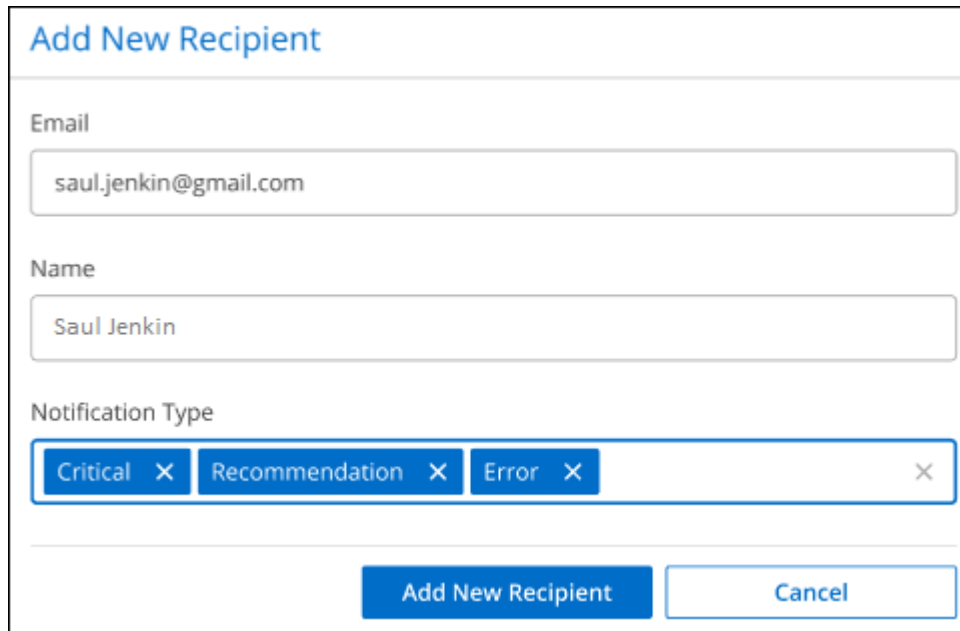


## Ajout de destinataires d'e-mail supplémentaires

Les utilisateurs qui s'affichent dans l'onglet *Account Users* sont automatiquement renseignés à partir du site NetApp Account (du "[Gérer le compte](#)"). Vous pouvez ajouter des adresses e-mail dans l'onglet *destinataires supplémentaires* pour d'autres personnes ou groupes qui n'ont pas accès à BlueXP, mais qui doivent être informés de certains types d'alertes et de notifications.

### Étapes

1. Dans la page Paramètres des alertes et notifications, cliquez sur **Ajouter de nouveaux destinataires**.



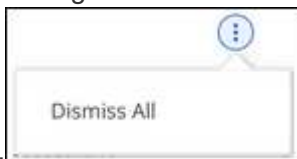
The screenshot shows a form titled "Add New Recipient". It has three input fields: "Email" with the value "saul.jenkin@gmail.com", "Name" with the value "Saul Jenkin", and "Notification Type" which is a multi-select dropdown containing "Critical", "Recommendation", and "Error". At the bottom, there are two buttons: "Add New Recipient" and "Cancel".

2. Entrez le nom, l'adresse e-mail et sélectionnez les types de notifications que le destinataire recevra, puis cliquez sur **Ajouter un nouveau destinataire**.

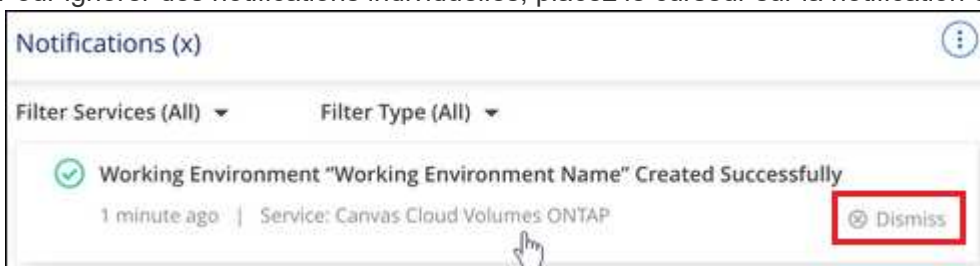
### Rejet des notifications

Vous pouvez supprimer des notifications de la page si vous n'avez plus besoin de les voir. Vous pouvez rejeter toutes les notifications en une seule fois ou rejeter les notifications individuelles.

Pour ignorer toutes les notifications, dans le Centre de notification, cliquez sur  Et sélectionnez **rejeter tout**



Pour ignorer des notifications individuelles, placez le curseur sur la notification et cliquez sur **rejeter**



## Audit de l'activité de l'utilisateur dans votre compte

Le Timeline de BlueXP affiche les actions que les utilisateurs ont effectuées pour gérer votre compte. Cela inclut des actions de gestion telles que l'association d'utilisateurs, la création d'espaces de travail, la création de connecteurs, etc.

La vérification de la chronologie peut être utile si vous devez identifier qui a effectué une action spécifique ou si vous devez identifier le statut d'une action.

### Étapes

1. Dans la barre de menus BlueXP, cliquez sur **Paramètres > Chronologie**.
2. Sous filtres, cliquez sur **Service**, activez **Tenancy** et cliquez sur **appliquer**.

La chronologie est mise à jour pour vous montrer les actions de gestion de compte.

### Rôles

Les rôles Administrateur de compte, Administrateur d'espace de travail, Visionneuse de conformité et Administrateur SnapCenter fournissent des autorisations spécifiques aux utilisateurs.

Le rôle Compliance Viewer permet l'accès en lecture seule à Cloud Data SENSE.

Tâche	Administrateur du compte	Administrateur de l'espace de travail	Visionneuse de conformité	Admin SnapCenter
Gérer les environnements de travail	Oui.	Oui.	Non	Non
Activer les services dans les environnements de travail	Oui.	Oui.	Non	Non
Afficher l'état de la réplication des données	Oui.	Oui.	Non	Non
Afficher la chronologie	Oui.	Oui.	Non	Non
Basculer entre les espaces de travail	Oui.	Oui.	Oui.	Non
Afficher les résultats de l'acquisition de détection de données	Oui.	Oui.	Oui.	Non
Supprimer les environnements de travail	Oui.	Non	Non	Non
Connectez les clusters Kubernetes aux environnements de travail	Oui.	Non	Non	Non



Tâche	Administrateur du compte	Administrateur de l'espace de travail	Visionneuse de conformité	Admin SnapCenter
Recevoir le rapport Cloud Volumes ONTAP	Oui.	Non	Non	Non
Créer des connecteurs	Oui.	Non	Non	Non
Gestion des comptes NetApp	Oui.	Non	Non	Non
Gérer les identifiants	Oui.	Non	Non	Non
Modifiez les paramètres BlueXP	Oui.	Non	Non	Non
Afficher et gérer le tableau de bord du support	Oui.	Non	Non	Non
Supprimez les environnements de travail de BlueXP	Oui.	Non	Non	Non
Installez un certificat HTTPS	Oui.	Non	Non	Non
Utiliser le service SnapCenter	Oui.	Oui.	Non	Oui.

#### Liens connexes

- ["Configuration d'espaces de travail et d'utilisateurs sur le compte NetApp"](#)
- ["Gestion des espaces de travail et des utilisateurs sur le compte NetApp"](#)

## Connecteurs

### Déploiement avancé

#### Créez un connecteur à partir d'AWS Marketplace

Dans le cas d'une région commerciale AWS, il est préférable de créer un connecteur directement depuis BlueXP, mais vous pouvez aussi lancer un connecteur depuis AWS Marketplace, si vous préférez. Pour les régions gouvernementales d'AWS, vous ne pouvez pas déployer le connecteur dans une région gouvernementale à partir du site Web BlueXP SaaS. La meilleure option consiste donc à le faire à partir d'AWS Marketplace.



Vous pouvez également télécharger et installer le logiciel Connector sur un hôte Linux existant de votre réseau ou dans le cloud. ["Découvrez comment installer le connecteur sur un hôte Linux existant"](#).

## Créez le connecteur dans une région commerciale d’AWS

Vous pouvez lancer l’instance Connector dans une région commerciale d’AWS directement à partir de l’offre AWS Marketplace pour BlueXP.

L’utilisateur IAM qui crée le connecteur doit disposer d’autorisations AWS Marketplace pour s’abonner et se désabonner.

### Étapes

1. Configurez les autorisations dans AWS :
  - a. À partir de la console IAM, créez les politiques requises en copiant et en collant le contenu de "[Les règles IAM pour le connecteur](#)".
  - b. Créez un rôle IAM avec le type de rôle Amazon EC2 et associez les règles créées à l’étape précédente au rôle.
2. Accédez au "[BlueXP, page sur AWS Marketplace](#)" Pour déployer le connecteur à partir d’une ami :
3. Sur la page Marketplace, cliquez sur **Continuer pour s’abonner**, puis cliquez sur **Continuer la configuration**.

**a**

Delivery Methods Solutions Migration Mapping Assistant Your Saved List **2** Partners Sell in AWS Marketplace Amazon Web Services Home

## Cloud Manager - Manual Installation without access keys

By: [NetApp, Inc.](#) Latest Version: 3.8.4

Read below for instructions on how to deploy Cloud Volumes ONTAP.

Linux/Unix ★★★★★ 6 AWS reviews

[Continue to Subscribe](#)

[Save to List](#)

Typical Total Price  
**\$0.226/hr**  
Total pricing per instance for services hosted on t3.xlarge in US East (N. Virginia). [View Details](#)

Overview Pricing Usage Support Reviews

### Product Overview

Do NOT subscribe on this page unless instructed by NetApp or redirected here from the NetApp website.

This listing lets you manually launch a Cloud Manager instance without providing your AWS credentials. After launching the Cloud Manager software in AWS, you can access it by entering the instance's IP address in a web browser. If you subscribe here, you still need to subscribe on the listing below for PAYGO charges.

### Highlights

- See Product Overview for instructions on how to deploy NetApp Cloud Manager.

**b**

Delivery Methods Solutions Migration Mapping Assistant Your Saved List **2** Partners Sell in AWS Marketplace Amazon Web Services Home

## Cloud Manager - Manual Installation without access keys

[Continue to Configuration](#)

[< Product Detail](#) [Subscribe](#)

### Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

### Terms and Conditions

#### NetApp, Inc. Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). Your use of AWS services remains subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services.

- Modifiez l'une des options par défaut et cliquez sur **Continuer pour lancer**.
- Sous **choisir action**, sélectionnez **lancer via EC2**, puis cliquez sur **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**.

- 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** : selon la disponibilité de la région, choisissez l'un des types d'instance pris en

charge (t3.XLarge est recommandé).

["Vérifiez les conditions requises pour l'instance"](#).

- **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.
- **Configurer le stockage** : conservez les options de stockage par défaut.
- **Détails avancés** : sous **profil d'instance IAM**, choisissez le rôle IAM que vous avez créé à l'étape 1.
- **Résumé** : consultez le résumé et cliquez sur **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.

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

`https://ipaddress[]`

8. 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.



9. Ouvrez un navigateur Web et accédez à <https://cloudmanager.netapp.com> Pour commencer à utiliser le connecteur avec BlueXP.

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 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](#)".

#### **Créez le connecteur dans une région du gouvernement AWS**

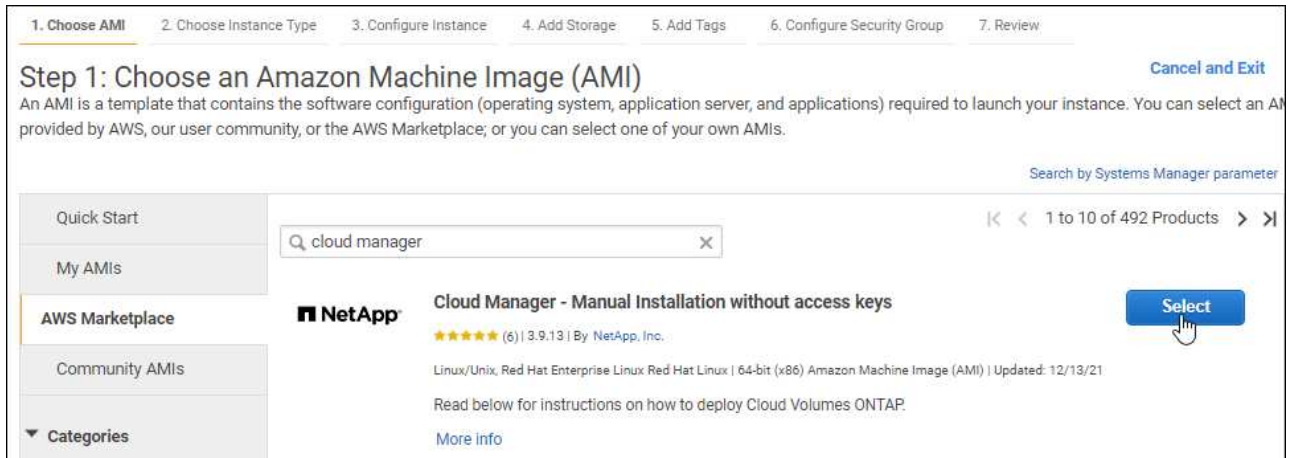
Pour déployer le connecteur dans une région AWS Government, vous devez accéder au service EC2 et sélectionner l'offre BlueXP depuis AWS Marketplace.

#### **Étapes**

1. Configurez les autorisations dans AWS :
  - a. À partir de la console IAM, créez votre propre politique en copiant et en collant le contenu de "[Politique IAM pour le connecteur](#)".
  - b. Créez un rôle IAM avec le type de rôle Amazon EC2 et associez la stratégie que vous avez créée à l'étape précédente au rôle.
2. Accédez à l'offre BlueXP sur AWS Marketplace.

L'utilisateur IAM doit disposer d'autorisations AWS Marketplace pour vous abonner et se désabonner.

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



- d. Cliquez sur **Continuer**.

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

- **Choisissez un type d'instance** : selon la disponibilité de la région, choisissez un des types d'instance pris en charge (t3.XLarge est recommandé).

"Vérifiez les conditions requises pour l'instance".

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

Number of instances	1	<a href="#">Launch into Auto Scaling Group</a>
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-a76d91c2   VPC4QA (default)	<a href="#">Create new VPC</a>
Subnet	subnet-39536c13   QASubnet1   us-east-1b 155 IP Addresses available	<a href="#">Create new subnet</a>
Auto-assign Public IP	Enable	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	<a href="#">Create new Capacity Reservation</a>
IAM role	Cloud_Manager	<a href="#">Create new IAM role</a>
CPU options	<input type="checkbox"/> Specify CPU options	
Shutdown behavior	Stop	
Enable termination protection	<input checked="" type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring <a href="#">Additional charges apply.</a>	

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

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

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

`https://ipaddress[]`

- Une fois connecté, configurez le connecteur :
  - Spécifiez le compte NetApp à associer au connecteur.

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

- Entrez un nom pour le système.



Le connecteur est désormais installé et configuré avec votre compte NetApp.

A chaque fois que vous souhaitez utiliser BlueXP, ouvrez votre navigateur Web et connectez-vous à l'adresse IP de l'instance de connecteur : `https://ipaddress[]`

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

#### **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.

#### **Créez un connecteur à partir d'Azure Marketplace**

Pour une région commerciale d'Azure, il est préférable de créer un connecteur



directement depuis BlueXP, mais vous pouvez lancer un connecteur depuis Azure Marketplace, si vous préférez. Pour les régions gouvernementales d’Azure, vous ne pouvez pas déployer le connecteur dans une région gouvernementale à partir du site Web BlueXP SaaS. La meilleure option consiste donc à le faire à partir d’Azure Marketplace.



Vous pouvez également télécharger et installer le logiciel Connector sur un hôte Linux existant de votre réseau ou dans le cloud. ["Découvrez comment installer le connecteur sur un hôte Linux existant"](#).

### Création d’un connecteur dans Azure

Déployez le connecteur dans Azure à l’aide de l’image contenue dans Azure Marketplace, puis connectez-vous au connecteur pour spécifier votre compte NetApp.

### Étapes

1. Rendez-vous sur la page NetApp Connector VM du Marketplace Azure.
  - ["Page Azure Marketplace pour les régions commerciales"](#)
  - ["Page Azure Marketplace pour les régions Azure Government"](#)
2. Cliquez sur **l’obtenir maintenant**, puis sur **Continuer**.
3. Sur le portail Azure, cliquez sur **Créer** et suivez les étapes de configuration de la machine virtuelle.

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

- Le connecteur offre des performances optimales avec des disques durs ou SSD.
- Choisissez une taille de machine virtuelle qui répond aux exigences en matière de CPU et de RAM. Nous recommandons DS3 v2.

["Vérifier les exigences relatives aux machines virtuelles"](#).

- Pour le groupe de sécurité réseau, le connecteur nécessite des connexions entrantes via SSH, HTTP et HTTPS.

["En savoir plus sur les règles de groupe de sécurité pour le connecteur"](#).

- Sous **Management**, activez **l’identité gérée attribuée par le système** pour le connecteur en sélectionnant **On**.

Ce paramètre est important car une identité gérée permet à la machine virtuelle Connector de s’identifier à Azure Active Directory sans fournir d’informations d’identification. ["En savoir plus sur les identités gérées pour les ressources Azure"](#).

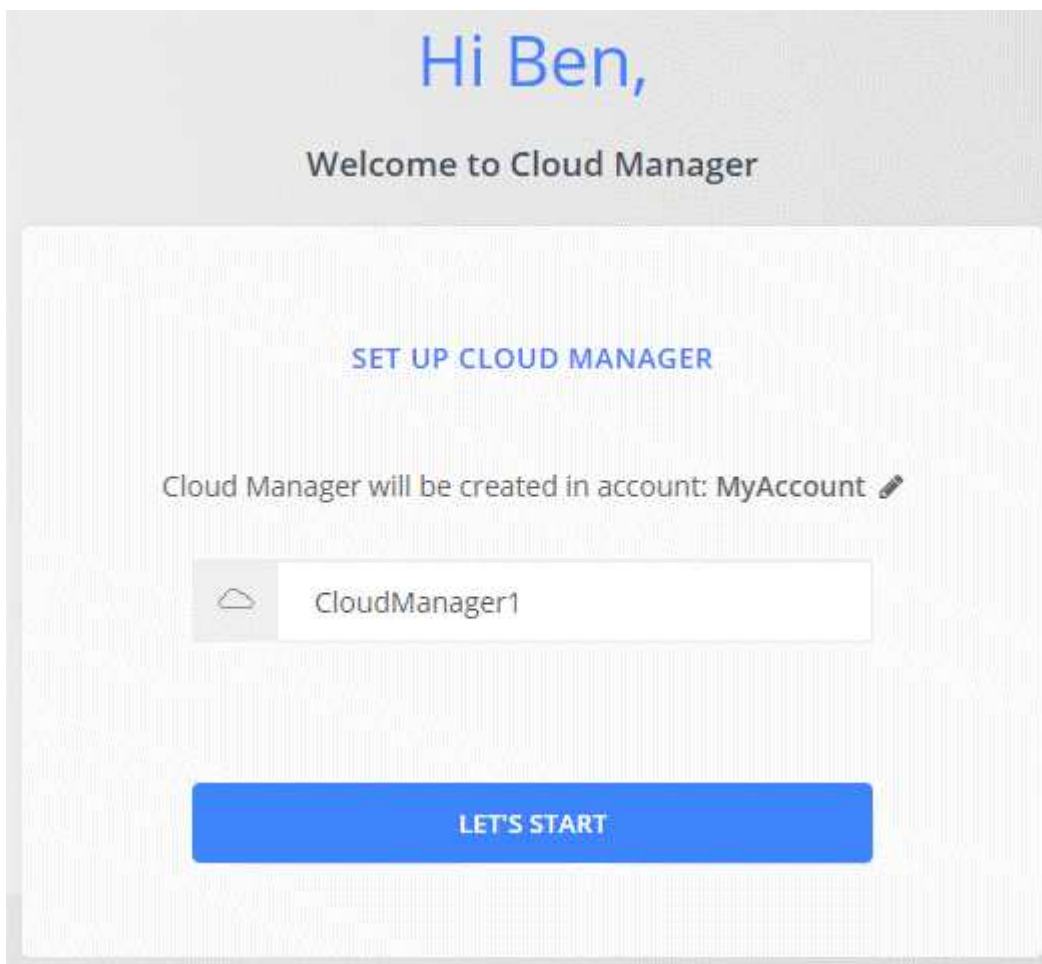
4. Dans la page **Revue + créer**, vérifiez vos sélections et cliquez sur **Créer** pour démarrer le déploiement.

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 NetApp à associer au connecteur.  
["En savoir plus sur les comptes NetApp"](#).
  - b. Entrez un nom pour le système.



Le connecteur est désormais installé et configuré avec votre compte NetApp.

Si le connecteur se trouve dans une région commerciale d'Azure, ouvrez un navigateur Web et rendez-vous sur <https://cloudmanager.netapp.com> Pour commencer à utiliser le connecteur avec BlueXP.

Si le connecteur se trouve dans une région d'administration Azure, vous pouvez utiliser BlueXP en ouvrant votre navigateur Web et en vous connectant à l'adresse IP de l'instance de connecteur : [https://ipaddress\[\]](https://ipaddress[])

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

#### Octroi d'autorisations Azure

Lorsque vous avez déployé le connecteur dans Azure, vous devez avoir activé un ["identité gérée attribuée par le système"](#). Vous devez maintenant accorder les autorisations Azure requises en créant un rôle personnalisé, puis en attribuant le rôle à la machine virtuelle Connector pour un ou plusieurs abonnements.

#### Étapes

## 1. Création d'un rôle personnalisé :

- Copier le contenu du "[Autorisations de rôle personnalisées pour le connecteur](#)" Et les enregistrer dans un fichier JSON.
- 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.

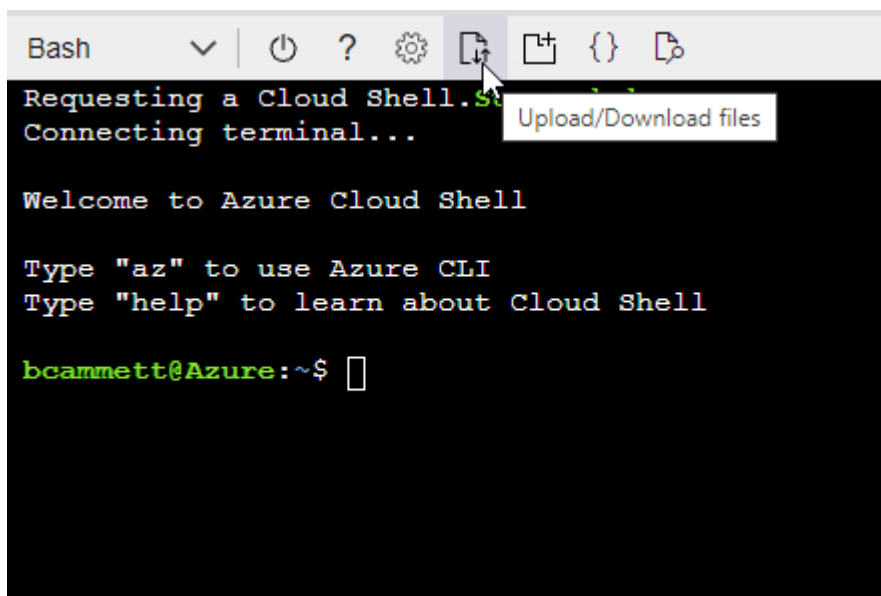
### Exemple

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

- 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.



- 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 opérateur BlueXP que vous pouvez affecter à la machine virtuelle connecteur.

2. Attribuez le rôle à la machine virtuelle Connector pour un ou plusieurs abonnements :

- a. Ouvrez le service **abonnements**, puis sélectionnez l'abonnement dans lequel vous souhaitez déployer des systèmes Cloud Volumes ONTAP.
- b. Cliquez sur **contrôle d'accès (IAM) > Ajouter > Ajouter affectation de rôle**.
- c. Dans l'onglet **role**, sélectionnez le rôle **BlueXP Operator** et cliquez sur **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.

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

- Attribuez l'accès à une identité **gérée**.
- Cliquez sur **Sélectionner les membres**, sélectionnez l'abonnement dans lequel la machine virtuelle de connecteur a été créée, choisissez **machine virtuelle**, puis sélectionnez la machine virtuelle de connecteur.
- Cliquez sur **Sélectionner**.
- Cliquez sur **Suivant**.

e. Cliquez sur **Revue + affecter**.

- f. Si vous souhaitez déployer Cloud Volumes ONTAP à partir d'abonnements supplémentaires, passez à cet abonnement, puis répétez ces étapes.

Le connecteur dispose désormais des autorisations nécessaires pour gérer les ressources et les processus au sein de votre environnement de cloud public. 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 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 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.

### Installez le connecteur sur un hôte Linux existant ayant accès à Internet

La manière la plus courante de créer un connecteur est directement depuis BlueXP ou depuis le marché d'un fournisseur cloud. Mais vous avez la possibilité de télécharger et d'installer le logiciel Connector sur un hôte Linux existant de votre réseau ou dans le cloud. Ces étapes sont spécifiques aux hôtes disposant d'un accès Internet.

["Découvrez d'autres méthodes de déploiement d'un connecteur".](#)



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.

#### **Vérifiez les besoins de 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.

#### **Un hôte dédié est requis**

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

#### **CPU**

4 cœurs ou 4 CPU virtuels

#### **RAM**

14 GO

#### **Type d'instance AWS EC2**

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

#### **Taille des machines virtuelles Azure**

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

#### **Type de machine GCP**

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"](#)

#### **Systèmes d'exploitation pris en charge**

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.6

Le système Red Hat Enterprise Linux doit être enregistré avec Red Hat Subscription Management. S'il n'est pas enregistré, le système ne peut pas accéder aux référentiels pour mettre à jour les logiciels

tiers requis pendant 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 CentOS ou Red Hat Enterprise Linux <https://access.redhat.com/certified-hypervisors>["Solution Red Hat : quels hyperviseurs sont certifiés pour l'exécution de Red Hat Enterprise Linux ?"^]

## 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 version 19 ou ultérieure est requis sur l'hôte avant d'installer le connecteur. "[Voir les instructions d'installation](#)"

## Accès Internet sortant

Le programme d'installation du connecteur doit accéder aux URL suivantes pendant le processus d'installation :

- <https://s3.amazonaws.com/aws-cli/awscli-bundle.zip>
- [https://\\*.blob.core.windows.net](https://*.blob.core.windows.net) ou <https://hub.docker.com>

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.

## Poser le connecteur

Après avoir vérifié que vous disposez d'un hôte Linux pris en charge, vous pouvez obtenir le logiciel Connector, puis l'installer.

Les privilèges root sont requis pour installer le connecteur.

## Description de la tâche

- L'installation installe les outils de ligne de commande AWS (awscli), afin d'activer les procédures de reprise à partir du support NetApp.

Si vous recevez un message indiquant que l'installation de awscli a échoué, vous pouvez ignorer le message en toute sécurité. Le connecteur peut fonctionner sans outils.

- 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. Téléchargez le logiciel du connecteur à partir du ["Site de support NetApp"](#), Puis copiez-le sur l'hôte Linux.

Pour obtenir de l'aide sur la connexion et la copie du fichier vers une instance EC2 dans AWS, reportez-vous à la section ["Documentation AWS : connexion à votre instance Linux à l'aide de SSH"](#).

3. Attribuez des autorisations pour exécuter le script.

```
chmod +x OnCommandCloudManager-V3.9.23.sh
```

4. Exécutez le script d'installation.

Si vous disposez d'un serveur proxy, vous devez entrer les paramètres de commande comme indiqué ci-dessous. Le programme d'installation ne vous invite pas à fournir des informations sur un proxy.

```
./OnCommandCloudManager-V3.9.23.sh --proxy  
http://occm:password@10.0.0.30:9090/ --cacert /root/rootca.pem
```

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.

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

[https://ipaddress\[\]](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.

6. S'inscrire ou se connecter.
7. Si vous avez installé le connecteur dans Google Cloud, configurez un compte de service disposant des autorisations nécessaires à BlueXP pour créer et gérer des systèmes Cloud Volumes ONTAP dans des projets.
  - a. ["Créer un rôle dans GCP"](#) qui inclut les autorisations définies dans le ["Règle de connecteur pour GCP"](#).
  - b. ["Créez un compte de service GCP et appliquez le rôle personnalisé que vous venez de créer"](#).
  - c. ["Associer ce compte de service à la VM Connector"](#).
  - d. 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.
8. Une fois connecté, configurez BlueXP :
  - a. Spécifiez le compte NetApp à associer au connecteur.  
["En savoir plus sur les comptes NetApp"](#).
  - b. Entrez un nom pour le système.



Le connecteur est désormais installé et configuré avec votre compte NetApp. BlueXP utilisera automatiquement ce connecteur lorsque vous créez de nouveaux environnements de travail.

Configurez des autorisations pour que BlueXP puisse gérer les ressources et les processus au sein de votre environnement de cloud public :

- AWS : ["Configurez un compte AWS, puis ajoutez-le à BlueXP"](#)
- Azure : ["Configurez un compte Azure, puis ajoutez-le à BlueXP"](#)
- Google Cloud : voir étape 7 ci-dessus

### Installez le connecteur sur site sans accès à Internet

Vous pouvez installer le connecteur sur un hôte Linux sur site qui n'a pas accès à Internet. Vous pouvez ensuite découvrir les clusters ONTAP sur site, répliquer les données entre eux, sauvegarder des volumes à l'aide de Cloud Backup et les analyser avec Cloud Data Sense.

Ces instructions d'installation s'affichent spécifiquement dans le cas d'utilisation décrit ci-dessus. ["Découvrez d'autres méthodes de déploiement d'un connecteur"](#).

### Vérifiez les besoins de 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.

### **Un hôte dédié est requis**

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

### **CPU**

4 cœurs ou 4 CPU virtuels

### **RAM**

14 GO

### **Systèmes d'exploitation pris en charge**

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.6

Le système Red Hat Enterprise Linux doit être enregistré avec Red Hat Subscription Management. S'il n'est pas enregistré, le système ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis pendant 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 CentOS ou Red Hat Enterprise Linux <https://access.redhat.com/certified-hypervisors>["Solution Red Hat : quels hyperviseurs sont certifiés pour l'exécution de Red Hat Enterprise Linux ?"]

### **Type de disque**

Un disque SSD est requis

### **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 version 19 ou ultérieure est requis sur l'hôte avant d'installer le connecteur. ["Voir les instructions d'installation"](#)

## Poser le connecteur

Après avoir vérifié que vous disposez d'un hôte Linux pris en charge, vous pouvez obtenir le logiciel Connector, puis l'installer.

Les privilèges root sont requis pour installer le connecteur.

### Étapes

1. Vérifiez que docker est activé et exécuté.

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

2. Téléchargez le logiciel du connecteur à partir du "[Site de support NetApp](#)"
3. Copiez le programme d'installation sur l'hôte Linux.
4. Attribuez des autorisations pour exécuter le script.

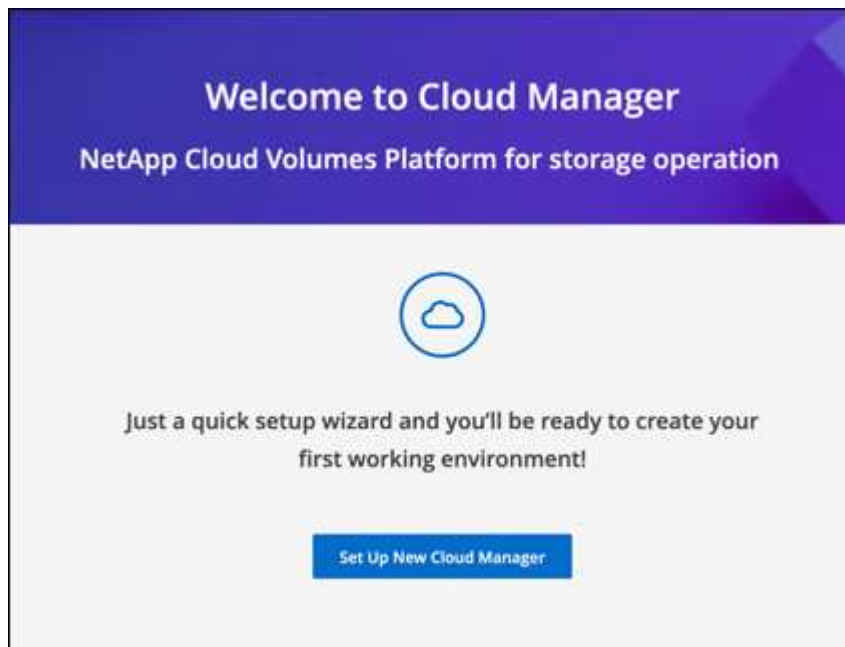
```
chmod +x /path/cloud-manager-connector-offline-v3.9.23
```

5. Exécutez le script d'installation :

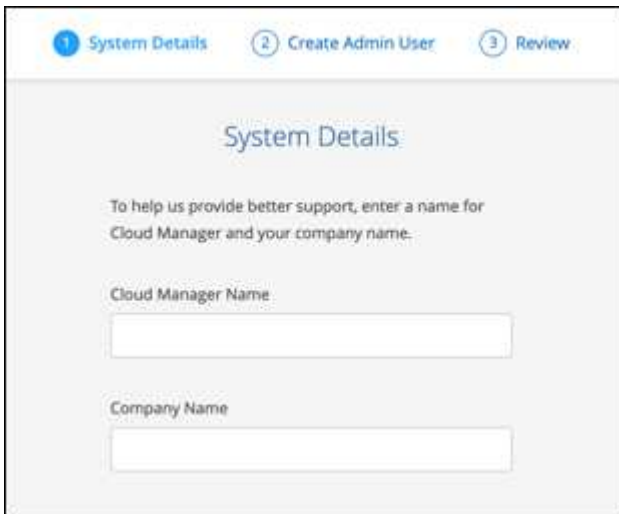
```
sudo /path/cloud-manager-connector-offline-v3.9.23
```

6. Ouvrez un navigateur Web et entrez `https://ipaddress[]` Où *ipaddress* est l'adresse IP de l'hôte Linux.

Vous devriez voir l'écran suivant.



7. Cliquez sur **configurer New BlueXP** et suivez les invites pour configurer le système.
  - **Détails du système** : saisissez un nom pour le connecteur et le nom de votre société.



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

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

- **Revue** : consultez les détails, acceptez le contrat de licence, puis cliquez sur **configurer**.

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

Le connecteur est maintenant installé et vous pouvez commencer à utiliser les fonctions BlueXP disponibles dans un déploiement de site sombre.

#### Que dois-je faire ?'s ensuite ?

- ["Découvrez les clusters ONTAP sur site"](#)
- ["Réplication des données entre les clusters ONTAP sur site"](#)
- ["Sauvegarde des données de volumes ONTAP sur site dans StorageGRID à l'aide de Cloud Backup"](#)
- ["Analysez les données de volume ONTAP sur site à l'aide de la solution Cloud Data Sense"](#)

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

## Recherche de l'ID système d'un connecteur

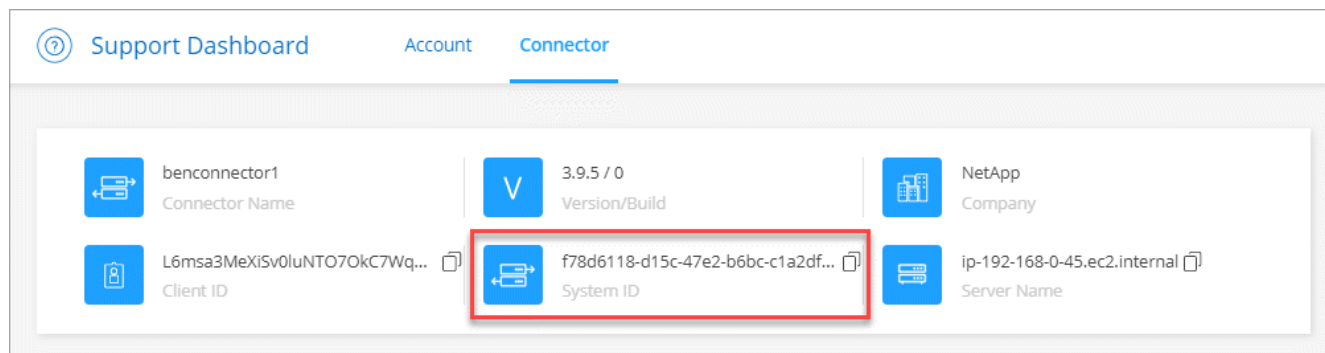
Pour vous aider à vous lancer, votre représentant NetApp peut vous demander l'ID système d'un connecteur. L'ID est généralement utilisé à des fins de licence et de dépannage.

### Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide.
2. Cliquez sur **support > connecteur**.

L'ID du système apparaît en haut.

### Exemple



## Gestion des connecteurs existants

Après avoir créé un ou plusieurs connecteurs, vous pouvez les gérer en passant d'un connecteur à l'autre, en vous connectant à l'interface utilisateur locale s'exécutant sur un connecteur, et plus encore.

### Basculer entre les connecteurs

Si vous avez plusieurs connecteurs, vous pouvez passer de l'un à l'autre pour voir les environnements de travail associés à un connecteur spécifique.

Imaginons par exemple que vous travaillez dans un environnement multicloud. Vous avez peut-être un connecteur dans AWS et un autre dans Google Cloud. Il faudrait basculer entre ces connecteurs pour gérer les systèmes Cloud Volumes ONTAP présents dans ces clouds.

### Étape

1. Cliquez sur la liste déroulante **Connector**, sélectionnez un autre connecteur, puis cliquez sur **Switch**.



BlueXP actualise et affiche les environnements de travail associés au connecteur sélectionné.

### Accédez à l'interface utilisateur locale

Bien que vous devriez effectuer presque toutes les tâches à partir de l'interface utilisateur SaaS, une interface utilisateur locale est toujours disponible sur le connecteur. Si vous accédez à BlueXP à partir d'une région du gouvernement ou d'un site qui ne dispose pas d'un accès Internet sortant, vous devez utiliser l'interface utilisateur locale s'exécutant sur le connecteur.

#### 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.

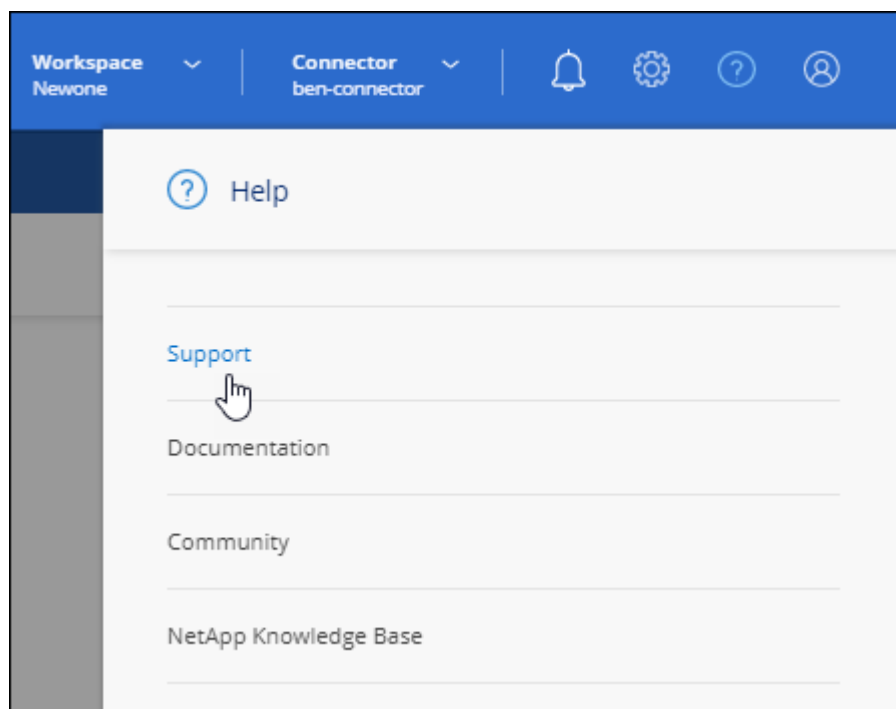
2. Entrez votre nom d'utilisateur et votre mot de passe pour vous connecter.

### Téléchargez ou envoyez un message AutoSupport

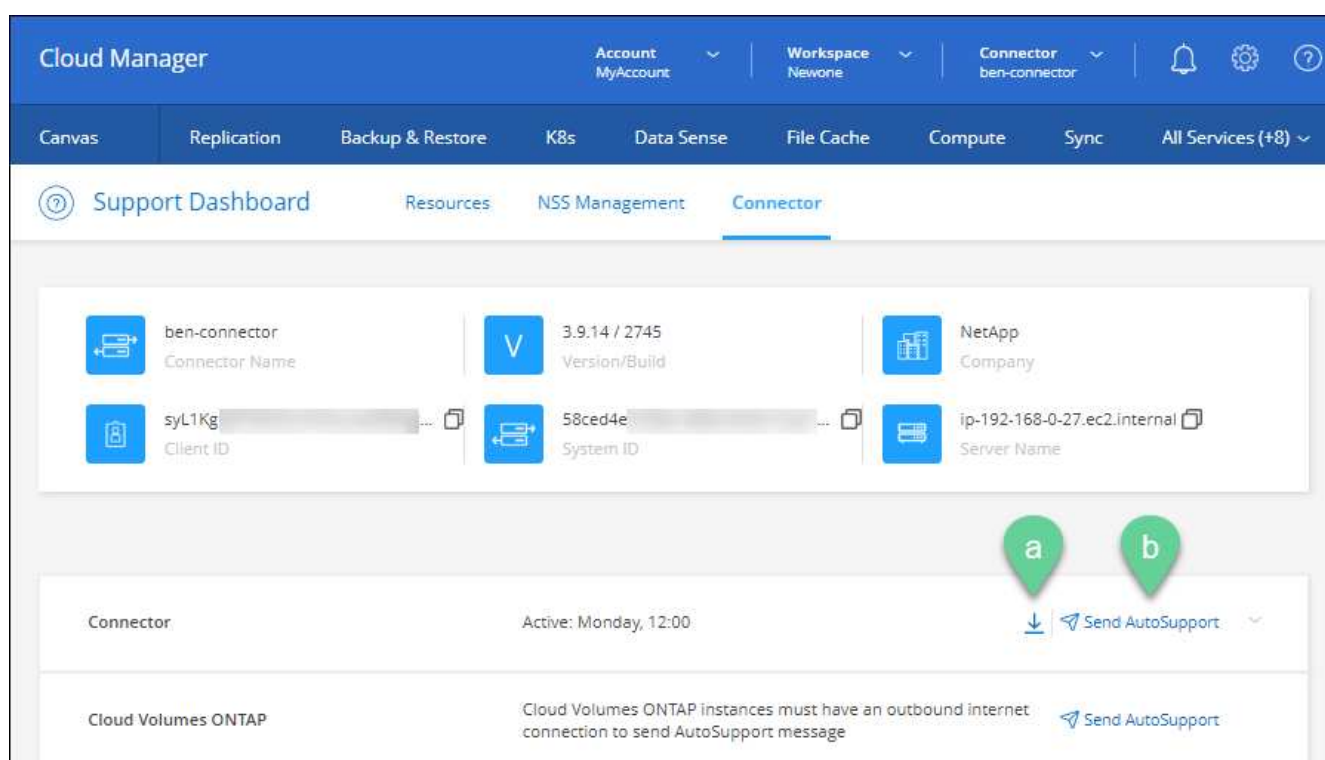
En cas de problème, les équipes NetApp peuvent vous demander d'envoyer un message AutoSupport au support NetApp à des fins de dépannage.

#### Étapes

1. Connectez-vous à l'interface utilisateur locale du connecteur, comme décrit dans la section ci-dessus.
2. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



3. Cliquez sur **connecteur**.
4. Selon le mode d'envoi des informations au support NetApp, choisissez l'une des options suivantes :
  - a. Sélectionnez l'option pour télécharger le message AutoSupport sur votre ordinateur local. Vous pouvez ensuite l'envoyer au support NetApp selon la méthode qui vous convient.
  - b. Cliquez sur **Envoyer AutoSupport** pour envoyer directement le message au support NetApp.



## Connectez-vous à la machine virtuelle Linux

Si vous devez vous connecter à la machine virtuelle Linux sur laquelle s'exécute le connecteur, vous pouvez utiliser les options de connectivité disponibles auprès de votre fournisseur de cloud.

### AWS

Lorsque vous avez créé l'instance Connector dans AWS, vous avez fourni une clé d'accès AWS et une clé secrète. Vous pouvez utiliser cette paire de clés vers SSH à l'instance.

["AWS Docs : connectez-vous à votre instance Linux"](#)

### Azure

Lorsque vous avez créé la machine virtuelle Connector dans Azure, vous avez choisi de vous authentifier avec un mot de passe ou une clé publique SSH. Utilisez la méthode d'authentification que vous avez choisie pour vous connecter à la machine virtuelle.

["Azure Docs : connexion SSH à votre machine virtuelle"](#)

### Google Cloud

Vous ne pouvez pas spécifier de méthode d'authentification lorsque vous créez un connecteur dans Google Cloud. Vous pouvez toutefois vous connecter à l'instance de machine virtuelle Linux à l'aide de Google Cloud Console ou de Google Cloud CLI (gCloud).

["Google Cloud Docs : connectez-vous aux machines virtuelles Linux"](#)

## Appliquer les mises à jour de sécurité

Mettez à jour le système d'exploitation sur le connecteur pour vous assurer qu'il a été corrigé avec les dernières mises à jour de sécurité.

### Étapes

1. Accéder au shell CLI sur l'hôte du connecteur.
2. Exécutez les commandes suivantes avec des privilèges élevés :

```
sudo -s
service netapp-service-manager stop
yum -y update --security
service netapp-service-manager start
```

## Modifiez l'adresse IP d'un connecteur

Si votre entreprise l'exige, vous pouvez modifier l'adresse IP interne et l'adresse IP publique de l'instance de connecteur qui est automatiquement attribuée par votre fournisseur de cloud.

### Étapes

1. Suivez les instructions de votre fournisseur de cloud pour modifier l'adresse IP locale ou l'adresse IP publique (ou les deux) de l'instance de connecteur.
2. Si vous avez modifié l'adresse IP publique et que vous devez vous connecter à l'interface utilisateur locale

s'exécutant sur le connecteur, redémarrez l'instance de connecteur pour enregistrer la nouvelle adresse IP avec BlueXP.

3. Si vous avez modifié l'adresse IP privée, mettez à jour l'emplacement de sauvegarde des fichiers de configuration Cloud Volumes ONTAP de manière à ce que les sauvegardes soient envoyées à la nouvelle adresse IP privée sur le connecteur.
  - a. Exécutez la commande suivante depuis l'interface de ligne de commande de Cloud Volumes ONTAP pour supprimer la cible de sauvegarde actuelle :

```
system configuration backup settings modify -destination ""
```

- b. Allez à BlueXP et ouvrez l'environnement de travail.
- c. Cliquez sur le menu et sélectionnez **Avancé > sauvegarde de la configuration**.
- d. Cliquez sur **définir la cible de sauvegarde**.

### Modifier les URI d'un connecteur

Ajouter et supprimer les URI d'un connecteur.

#### Étapes

1. Cliquez sur la liste déroulante **Connector** dans l'en-tête BlueXP.
2. Cliquez sur **gérer les connecteurs**.
3. Cliquez sur le menu d'action d'un connecteur et cliquez sur **Modifier URI**.
4. Ajoutez et supprimez des URI, puis cliquez sur **appliquer**.

### Corrigez les échecs de téléchargement lors de l'utilisation d'une passerelle Google Cloud NAT

Le connecteur télécharge automatiquement les mises à jour logicielles pour Cloud Volumes ONTAP. Le téléchargement peut échouer si votre configuration utilise une passerelle NAT Google Cloud. Vous pouvez corriger ce problème en limitant le nombre de pièces dans lesquelles l'image logicielle est divisée. Cette étape doit être effectuée à l'aide de l'API BlueXP.

#### Étape

1. Soumettre une demande PUT à `/ocm/config` au format JSON suivant :

```
{
  "maxDownloadSessions": 32
}
```

La valeur de `maxDownloadSessions` peut être 1 ou n'importe quel entier supérieur à 1. Si la valeur est 1, l'image téléchargée ne sera pas divisée.

Notez que 32 est un exemple de valeur. La valeur que vous devez utiliser dépend de votre configuration NAT et du nombre de sessions que vous pouvez avoir simultanément.

["En savoir plus sur l'appel API /ocm/config"](#).



## Mettez à niveau le connecteur sur site sans accès à Internet

Si vous "[Installez le connecteur sur un hôte sur site qui ne dispose pas d'un accès Internet](#)", Vous pouvez mettre à niveau le connecteur lorsqu'une version plus récente est disponible sur le site de support NetApp.

Le connecteur doit redémarrer pendant le processus de mise à niveau pour que l'interface utilisateur ne soit pas disponible pendant la mise à niveau.

### Étapes

1. Téléchargez le logiciel du connecteur à partir du "[Site de support NetApp](#)".
2. Copiez le programme d'installation sur l'hôte Linux.
3. Attribuez des autorisations pour exécuter le script.

```
chmod +x /path/cloud-manager-connector-offline-v3.9.14
```

4. Exécutez le script d'installation :

```
sudo /path/cloud-manager-connector-offline-v3.9.14
```

5. Une fois la mise à niveau terminée, vous pouvez vérifier la version du connecteur en accédant à **aide > support > connecteur**.

## Qu'en est-il des mises à niveau logicielles sur les hôtes disposant d'un accès Internet ?

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.

## Retirer les connecteurs de BlueXP

Si un connecteur est inactif, vous pouvez le retirer de la liste des connecteurs dans BlueXP. Vous pouvez le faire si vous avez supprimé la machine virtuelle Connector ou si vous avez désinstallé le logiciel Connector.

Notez ce qui suit sur le retrait d'un connecteur :

- Cette action ne supprime pas la machine virtuelle.
- Cette action ne peut pas être rétablie — une fois que vous avez supprimé un connecteur de BlueXP, vous ne pouvez pas l'ajouter à nouveau

### Étapes

1. Cliquez sur la liste déroulante **Connector** dans l'en-tête BlueXP.
2. Cliquez sur **gérer les connecteurs**.
3. Cliquez sur le menu d'action d'un connecteur inactif et cliquez sur **Supprimer le connecteur**.



4. Entrez le nom du connecteur à confirmer, puis cliquez sur Supprimer.

BlueXP supprime le connecteur de ses enregistrements.

### Désinstallez le logiciel du connecteur

Désinstallez le logiciel du connecteur pour résoudre les problèmes ou pour supprimer définitivement le logiciel de l'hôte. Les étapes que vous devez utiliser dépendent de l'installation ou non du connecteur sur un hôte disposant d'un accès Internet ou sur un hôte d'un réseau restreint ne disposant pas d'un accès Internet.

#### Désinstallation à partir d'un hôte disposant d'un accès à Internet

Le connecteur en ligne inclut un script de désinstallation que vous pouvez utiliser pour désinstaller le logiciel.

##### Étape

1. À partir de l'hôte Linux, exécutez le script de désinstallation :

**`/opt/application/netapp/cloudmanager/bin/uninstall.sh [silencieux]`**

*silent* exécute le script sans vous demander de confirmer.

#### Désinstallation à partir d'un hôte sans accès à Internet

Utilisez ces commandes si vous avez téléchargé le logiciel Connector depuis le site de support NetApp et l'avez installé dans un réseau restreint qui ne dispose pas d'un accès Internet.

##### Étape

1. Depuis l'hôte Linux, exécutez les commandes suivantes :

```
docker-compose -f /opt/application/netapp/ds/docker-compose.yml down -v
rm -rf /opt/application/netapp/ds
```

## Gestion d'un certificat HTTPS pour l'accès sécurisé

Par défaut, BlueXP utilise un certificat auto-signé pour l'accès HTTPS à la console Web. Vous pouvez installer un certificat signé par une autorité de certification (CA), qui offre une meilleure protection de la sécurité qu'un certificat auto-signé.

### Avant de commencer

Vous devez créer un connecteur avant de pouvoir modifier les paramètres BlueXP. "[Découvrez comment](#)".

### Installation d'un certificat HTTPS

Installez un certificat signé par une autorité de certification pour un accès sécurisé.

#### Étapes

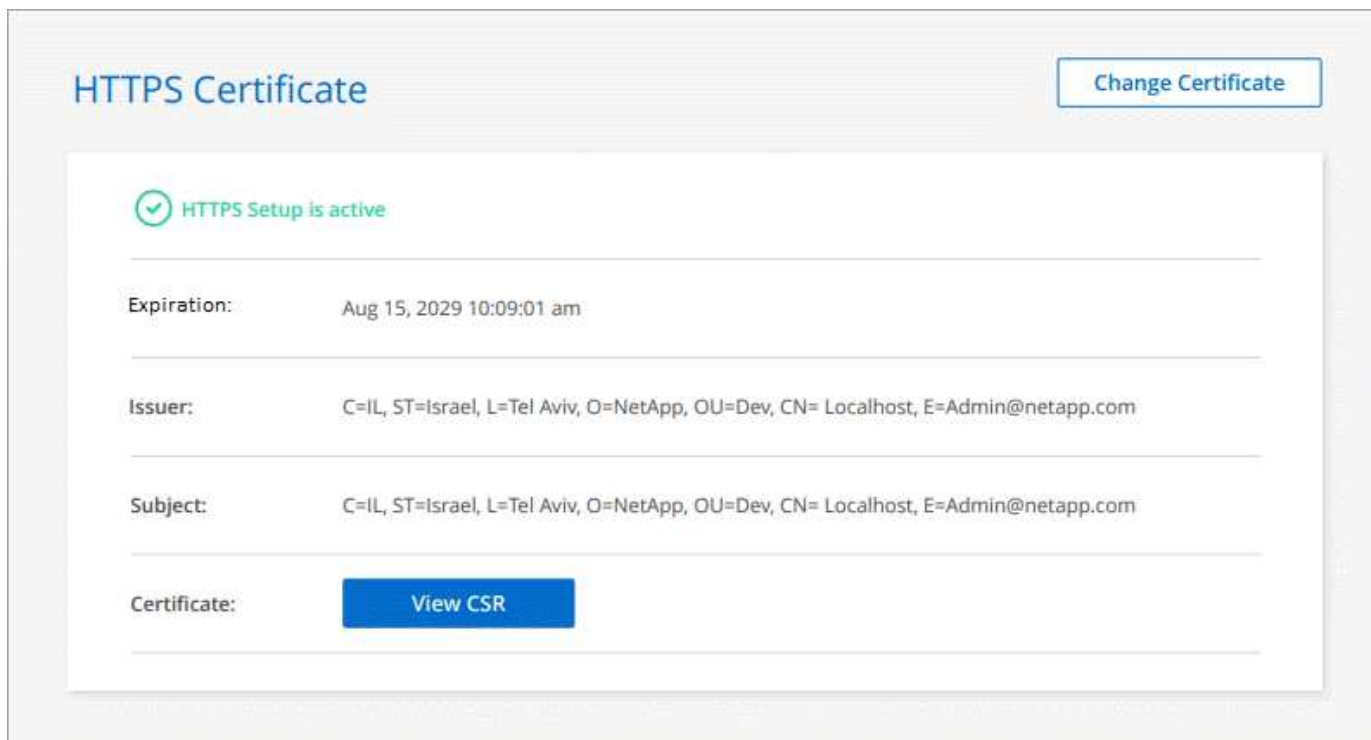
1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres et sélectionnez **HTTPS Setup**.



2. Dans la page Configuration HTTPS, installez un certificat en générant une requête de signature de certificat (CSR) ou en installant votre propre certificat signé par l'autorité de certification :

Option	Description
Générez une RSC	<ol style="list-style-type: none"><li>a. Entrez le nom d'hôte ou le DNS de l'hôte du connecteur (son nom commun), puis cliquez sur <b>generate CSR</b>.  BlueXP affiche une demande de signature de certificat.</li><li>b. Utilisez la RSC pour envoyer une demande de certificat SSL à une autorité de certification.  Le certificat doit utiliser le format X.509 encodé au format PEM (Privacy Enhanced Mail) Base-64.</li><li>c. Téléchargez le fichier de certificat, puis cliquez sur <b>installer</b>.</li></ol>
Installez votre propre certificat signé par l'autorité de certification	<ol style="list-style-type: none"><li>a. Sélectionnez <b>installer le certificat signé CA</b>.</li><li>b. Chargez le fichier de certificat et la clé privée, puis cliquez sur <b>installer</b>.  Le certificat doit utiliser le format X.509 encodé au format PEM (Privacy Enhanced Mail) Base-64.</li></ol>

BlueXP utilise désormais le certificat signé par l'autorité de certification pour fournir un accès HTTPS sécurisé. L'image suivante montre un compte BlueXP configuré pour un accès sécurisé :



## Renouvellement du certificat HTTPS BlueXP

Vous devez renouveler le certificat HTTPS BlueXP avant son expiration pour garantir un accès sécurisé à la console BlueXP. Si vous ne renouvelez pas le certificat avant son expiration, un avertissement s'affiche lorsque les utilisateurs accèdent à la console Web via HTTPS.

### Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres et sélectionnez **HTTPS Setup**.

Des détails sur le certificat BlueXP s'affichent, y compris la date d'expiration.

2. Cliquez sur **Modifier le certificat** et suivez les étapes pour générer une RSC ou installer votre propre certificat signé par une CA.

BlueXP utilise le nouveau certificat signé par une autorité de certification pour fournir un accès HTTPS sécurisé.

## Configuration d'un connecteur pour utiliser un serveur proxy HTTP

Si vos stratégies d'entreprise nécessitent l'utilisation d'un serveur proxy pour toutes les communications HTTP vers Internet, vous devez configurer vos connecteurs pour qu'ils utilisent un serveur proxy HTTP. Le serveur proxy peut se trouver dans le cloud ou dans votre réseau.



BlueXP ne prend pas en charge l'utilisation d'un proxy HTTPS avec le connecteur.

La configuration du connecteur pour utiliser un serveur proxy HTTP fournit un accès Internet sortant si une adresse IP publique ou une passerelle NAT n'est pas disponible. Ce serveur proxy fournit uniquement le connecteur avec une connexion sortante. Il n'offre aucune connectivité pour les systèmes Cloud Volumes

ONTAP.

Si les systèmes Cloud Volumes ONTAP ne disposent pas d'une connexion Internet sortante pour envoyer des messages AutoSupport, BlueXP configure automatiquement ces systèmes Cloud Volumes ONTAP pour utiliser 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 un proxy sur un connecteur

Lorsque vous configurez un connecteur pour utiliser un serveur proxy, ce connecteur et les systèmes Cloud Volumes ONTAP qu'il gère (y compris les médiateurs HA) utilisent tous le serveur proxy.

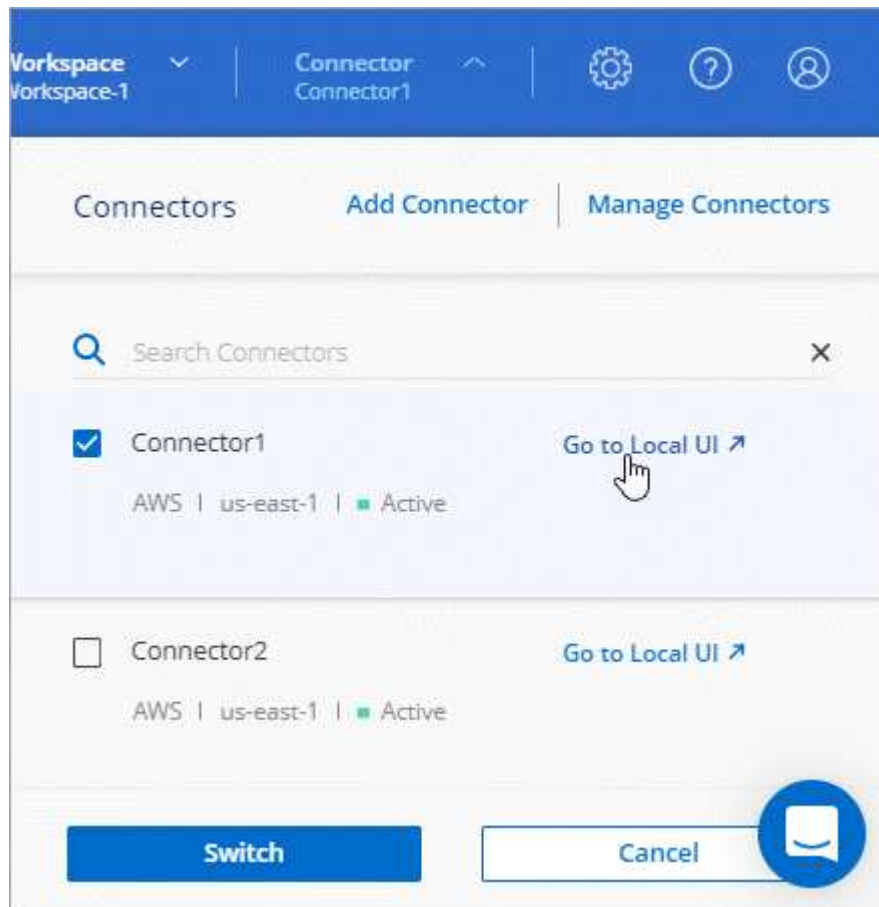
Notez que cette opération redémarre le connecteur. Assurez-vous que le connecteur n'effectue aucune opération avant de continuer.

### Étapes

1. "[Connectez-vous à l'interface BlueXP SaaS](#)" À partir d'une machine dotée d'une connexion réseau à l'instance de connecteur.

Si le connecteur n'est pas doté d'une adresse IP publique, vous aurez besoin d'une connexion VPN ou vous devrez vous connecter à partir d'un hôte de secours situé sur le même réseau que le connecteur.

2. Cliquez sur la liste déroulante **Connector**, puis cliquez sur **allez à l'interface utilisateur locale** pour un connecteur spécifique.



L'interface BlueXP exécutée sur le connecteur se charge dans un nouvel onglet de navigateur.

3. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres, puis sélectionnez **Paramètres du connecteur**.



4. Sous **général**, cliquez sur **Configuration du proxy HTTP**.
5. Configurez le proxy :
  - a. Cliquez sur **Activer proxy**.
  - b. Spécifiez le serveur à l'aide de la syntaxe `http://address:port[]`
  - c. Spécifiez un nom d'utilisateur et un mot de passe si une authentification de base est requise pour le serveur
  - d. Cliquez sur **Enregistrer**.



BlueXP ne prend pas en charge les mots de passe contenant le caractère @.

### Activation du trafic API direct

Si vous avez configuré un serveur proxy, vous pouvez envoyer des appels API directement à BlueXP sans passer par le proxy. Cette option est prise en charge avec des connecteurs s'exécutant dans AWS, dans Azure ou dans Google Cloud.

#### Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres, puis sélectionnez **Paramètres du connecteur**.



2. Sous **général**, cliquez sur **support Direct API Traffic**.
3. Cochez la case pour activer l'option, puis cliquez sur **Enregistrer**.

### Configuration par défaut du connecteur

Vous voudrez peut-être en savoir plus sur le connecteur avant de le déployer ou pour résoudre d'autres problèmes.

#### Configuration par défaut avec accès à Internet

Les informations de configuration suivantes s'appliquent si vous avez déployé le connecteur depuis BlueXP, depuis le Marketplace de votre fournisseur de services cloud ou si vous avez installé manuellement le connecteur sur un hôte Linux sur site disposant d'un accès Internet.

## Détails d’AWS

Si vous avez déployé le connecteur depuis BlueXP ou depuis le marché du fournisseur cloud, remarque :

- Le type d’instance EC2 est t3.XLarge.
- Le système d’exploitation de l’image est Red Hat Enterprise Linux 7.6 (HVM).

Le système d’exploitation n’inclut pas d’interface graphique. Vous devez utiliser un terminal pour accéder au système.

- Le nom d’utilisateur de l’instance Linux EC2 est utilisateur ec2.
- Le disque système par défaut est un disque gp2 de 100 Gio.

## Détails d’Azure

Si vous avez déployé le connecteur depuis BlueXP ou depuis le marché du fournisseur cloud, remarque :

- Le type de machine virtuelle est DS3 v2.
- Le système d’exploitation de l’image est CentOS 7.6.

Le système d’exploitation n’inclut pas d’interface graphique. Vous devez utiliser un terminal pour accéder au système.

- Le disque système par défaut est un disque SSD premium de 100 Gio.

## Détails sur Google Cloud

Si vous avez déployé le connecteur depuis BlueXP ou depuis le marché du fournisseur cloud, remarque :

- L’instance de machine virtuelle est n2-standard-4.
- Le système d’exploitation de l’image est Red Hat Enterprise Linux 8.6.

Le système d’exploitation n’inclut pas d’interface graphique. Vous devez utiliser un terminal pour accéder au système.

- Le disque système par défaut est un disque persistant SSD de 100 Gio.

## Dossier d’installation

Le dossier d’installation du connecteur se trouve à l’emplacement suivant :

/opt/application/netapp/cloudmanager

## Fichiers journaux

Les fichiers journaux sont contenus dans les dossiers suivants :

- /opt/application/netapp/cloudmanager/log

Les journaux de ce dossier fournissent des détails sur les images Connector et docker.

- /opt/application/netapp/cloudmanager/docker\_ocm/data/log

Les journaux de ce dossier fournissent des détails sur les services Cloud et le service BlueXP qui

s'exécute sur le connecteur.

### Service des connecteurs

- Le service BlueXP est nommé ocm.
- Le service occm dépend du service MySQL.

Si le service MySQL est en panne, le service occm est également en panne.

### Packs

BlueXP installe les modules suivants sur l'hôte Linux, s'ils ne sont pas déjà installés :

- 7Zip
- AWSCLI
- Java
- Kubectl
- MySQL
- Tridentctl
- Tirer
- Wget

### Ports

Le connecteur utilise les ports suivants sur l'hôte Linux :

- 80 pour l'accès HTTP
- 443 pour l'accès HTTPS
- 3306 pour la base de données BlueXP
- 8080 pour le proxy API BlueXP
- 8666 pour l'API du Gestionnaire de services
- 8777 pour l'API du service de conteneurs Health-Checker

### Configuration par défaut sans accès à Internet

La configuration suivante s'applique si vous avez installé manuellement le connecteur sur un hôte Linux sur site qui n'a pas accès à Internet. ["En savoir plus sur cette option d'installation"](#).

- Le dossier d'installation du connecteur se trouve à l'emplacement suivant :

`/opt/application/netapp/ds`

- Les fichiers journaux sont contenus dans les dossiers suivants :

`/var/lib/docker/volumes/ds_ocmdata/_data/log`

Les journaux de ce dossier fournissent des détails sur les images Connector et docker.



- Tous les services s'exécutent dans des conteneurs docker

Ces services dépendent du service d'exécution docker exécuté

- Le connecteur utilise les ports suivants sur l'hôte Linux :
  - 80 pour l'accès HTTP
  - 443 pour l'accès HTTPS

## Gérer les abonnements et les contrats PAYGO

Lorsque vous vous abonnez à BlueXP depuis le marché d'un fournisseur de services Cloud, vous êtes redirigé vers le site Web BlueXP où vous devez enregistrer votre abonnement et l'associer à des comptes spécifiques. Après votre inscription, vous pouvez gérer chaque abonnement à partir du porte-monnaie numérique.

### Afficher vos abonnements

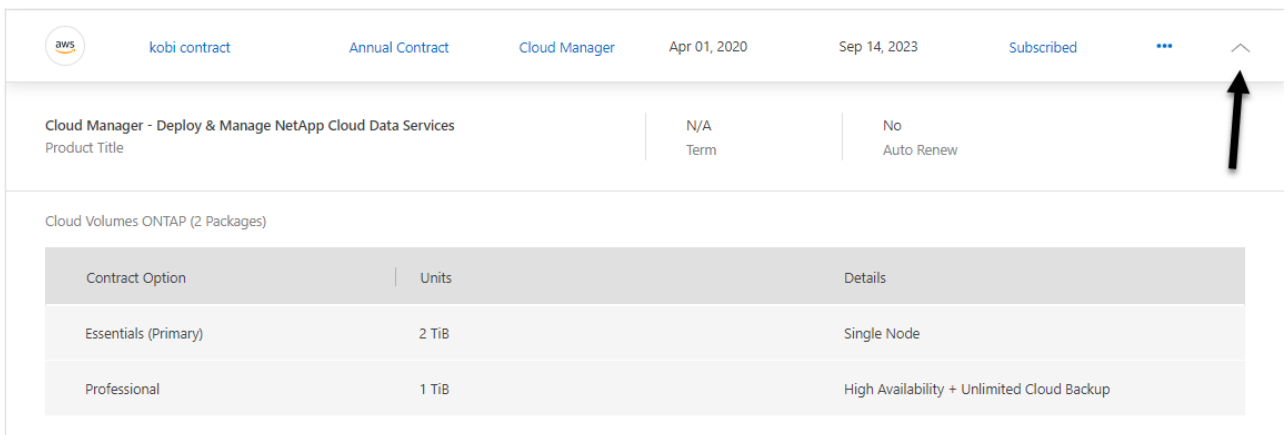
Le porte-monnaie numérique fournit des informations détaillées sur chaque abonnement PAYGO et contrat annuel associé à votre compte BlueXP et à Astra (Astra utilise le service de facturation de BlueXP).

#### Étapes

1. Dans le menu de navigation BlueXP, sélectionnez **gouvernance > porte-monnaie numérique**.
2. Sélectionnez **abonnements**.

Vous ne verrez que les abonnements associés au compte que vous consultez actuellement.

3. Lorsque vous affichez les informations relatives à vos abonnements, vous pouvez interagir avec les détails du tableau comme suit :
  - Développez une ligne pour afficher plus de détails.



aws	kobi contract	Annual Contract	Cloud Manager	Apr 01, 2020	Sep 14, 2023	Subscribed	...
Cloud Manager - Deploy & Manage NetApp Cloud Data Services	Product Title	N/A	Term	No	Auto Renew		
Cloud Volumes ONTAP (2 Packages)							
Contract Option	Units	Details					
Essentials (Primary)	2 TiB	Single Node					
Professional	1 TiB	High Availability + Unlimited Cloud Backup					

- Cliquez sur  pour choisir les colonnes qui s'affichent dans le tableau.

Notez que les colonnes Term et Auto Renew n'apparaissent pas par défaut. La colonne Renouvellement automatique affiche les informations de renouvellement des contrats Azure uniquement.

Notez ce qui suit à propos de ce que vous voyez dans le tableau :

## Date de début

La date de début est la date à laquelle vous avez correctement associé l'abonnement à votre compte et que la facturation a commencé.

## S/O

Si vous voyez N/A dans le tableau, les informations ne sont pas disponibles dans l'API du fournisseur de cloud pour le moment.

## Contrats

- Si vous développez les détails d'un contrat, le porte-monnaie numérique affiche les éléments disponibles pour votre plan actuel : les options et unités du contrat (capacité ou nombre de nœuds).
- Le porte-monnaie numérique identifie la date de fin et indique si le contrat sera bientôt renouvelé ou s'il a déjà pris fin.
- Si vous avez souscrit un contrat AWS et que vous avez modifié l'une des options du contrat après la date de début, veuillez à valider les options de contrat depuis AWS.

## Gérez vos abonnements

Vous pouvez gérer vos abonnements à partir du porte-monnaie numérique en renommant un abonnement et en choisissant les comptes associés à l'abonnement.

Par exemple, disons que vous avez deux comptes et que chacun est facturé par le biais d'abonnements distincts. Vous pouvez dissocier un abonnement de l'un des comptes afin que les utilisateurs de ce compte ne choisissent pas accidentellement l'abonnement incorrect lors de la création d'un environnement de travail Cloud Volume ONTAP.

### Étapes

1. Dans le menu de navigation BlueXP, sélectionnez **gouvernance > porte-monnaie numérique**.
2. Sélectionnez **abonnements**.
3. Cliquez sur le menu d'action de la ligne correspondant à l'abonnement que vous souhaitez gérer.

Provider	Name	Type	Service	Start Date	End Date	Status	
aws	aws-sub-a2	PAYGO	Cloud Manager	Apr 02, 2020	N/A	Subscribed	⋮
aws	Aleksey_aws_marketplace	Annual Contract	Astra	Oct 18, 2022	Oct 18, 2023		⋮
aws	By Capacity By Node 3	PAYGO	Cloud Manager	Mar 31, 2020	N/A	Subscribed	⋮

4. Vous pouvez renommer l'abonnement ou gérer les comptes NetApp associés à cet abonnement.

## Stockage cloud découvert

### Affichage des compartiments Amazon S3

Une fois que vous avez installé un connecteur dans AWS, BlueXP peut détecter automatiquement les informations relatives aux compartiments Amazon S3 qui résident

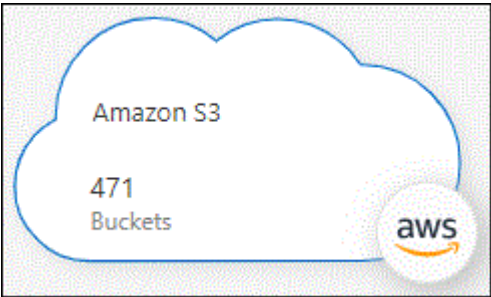
dans le compte AWS où le connecteur est installé. Un environnement de travail Amazon S3 est ajouté à Canvas pour que vous puissiez visualiser ces informations.

Vous pouvez afficher des informations détaillées sur vos compartiments S3, notamment la région, les règles d'accès, le compte, la capacité totale et utilisée. Ces compartiments peuvent être utilisés comme destinations pour les opérations Cloud Backup, Cloud Tiering ou Cloud Sync. Vous pouvez également utiliser Cloud Data Sense pour scanner ces compartiments.

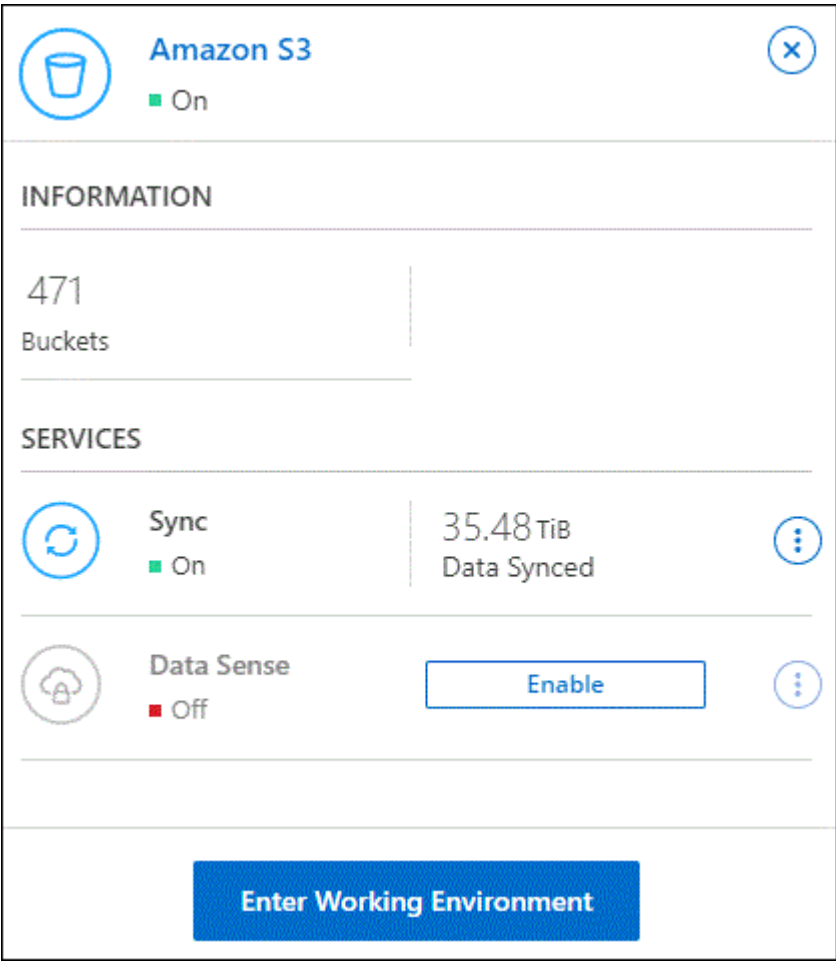
Étapes

- 1. "Installer un connecteur" Dans le compte AWS où vous souhaitez afficher vos compartiments Amazon S3.
- 2. Dans le menu de navigation, sélectionnez **stockage > Canvas**.

Vous devriez voir automatiquement un environnement de travail Amazon S3 peu après.



- 3. Cliquez sur l'environnement de travail et sélectionnez une action dans le volet droit.



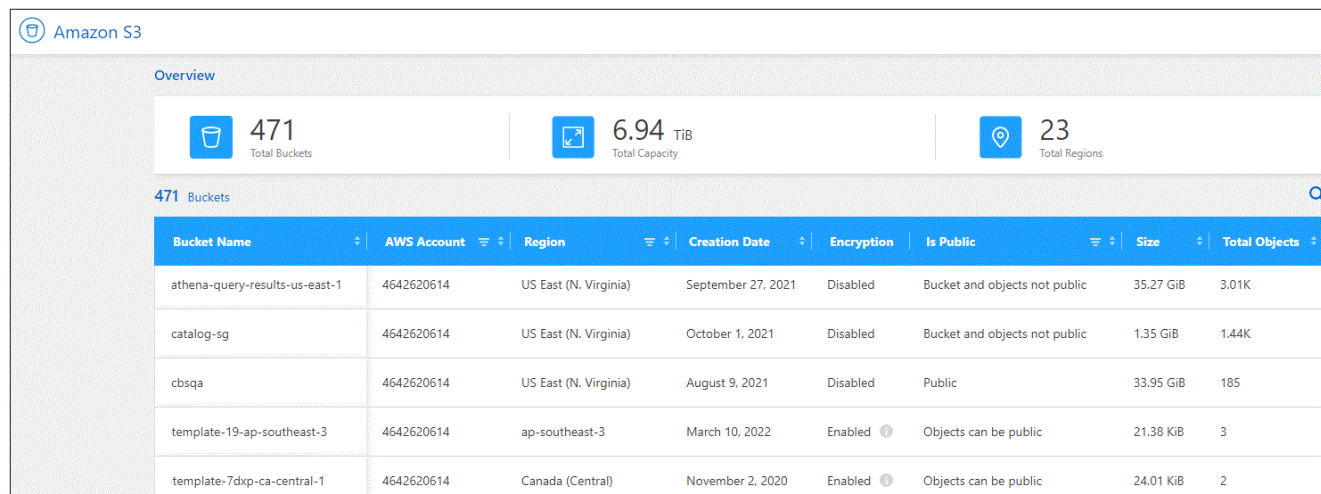
4. Cliquez sur **Synchroniser les données** pour synchroniser les données vers ou à partir de compartiments S3.

Pour plus de détails, voir ["La présentation du service Cloud Sync"](#).

5. Cliquez sur **Activer** si vous souhaitez que Cloud Data SENSE analyse les compartiments S3 pour les données personnelles et sensibles.

Pour plus de détails, voir ["Mise en route de Cloud Data Sense pour Amazon S3"](#).

6. Cliquez sur **entrer environnement de travail** pour afficher des détails sur les compartiments S3 de votre compte AWS.



Amazon S3 Overview

471 Total Buckets | 6.94 TiB Total Capacity | 23 Total Regions

471 Buckets

Bucket Name	AWS Account	Region	Creation Date	Encryption	Is Public	Size	Total Objects
athena-query-results-us-east-1	4642620614	US East (N. Virginia)	September 27, 2021	Disabled	Bucket and objects not public	35.27 GiB	3.01K
catalog-sg	4642620614	US East (N. Virginia)	October 1, 2021	Disabled	Bucket and objects not public	1.35 GiB	1.44K
cbsqa	4642620614	US East (N. Virginia)	August 9, 2021	Disabled	Public	33.95 GiB	185
template-19-ap-southeast-3	4642620614	ap-southeast-3	March 10, 2022	Enabled	Objects can be public	21.38 KiB	3
template-7dxc-ca-central-1	4642620614	Canada (Central)	November 2, 2020	Enabled	Objects can be public	24.01 KiB	2

## Affichage de vos comptes Azure Blob

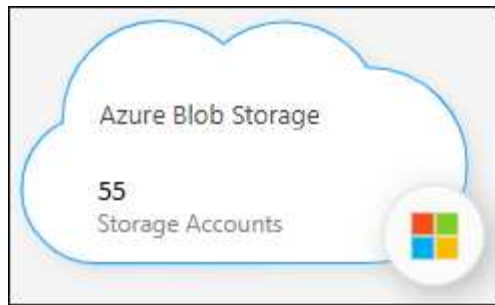
Une fois que vous avez installé un connecteur dans Azure, BlueXP peut détecter automatiquement des informations sur les comptes de stockage Azure qui résident dans les abonnements Azure où le connecteur est installé. Un environnement de travail Azure Blob est ajouté à Canvas pour vous permettre d'afficher ces informations.

Vous pouvez afficher des informations détaillées sur vos comptes de stockage Azure, notamment l'emplacement, le groupe de ressources, la capacité totale et utilisée, etc. Ces comptes peuvent être utilisés comme destinations pour les opérations Cloud Backup, Cloud Tiering ou Cloud Sync.

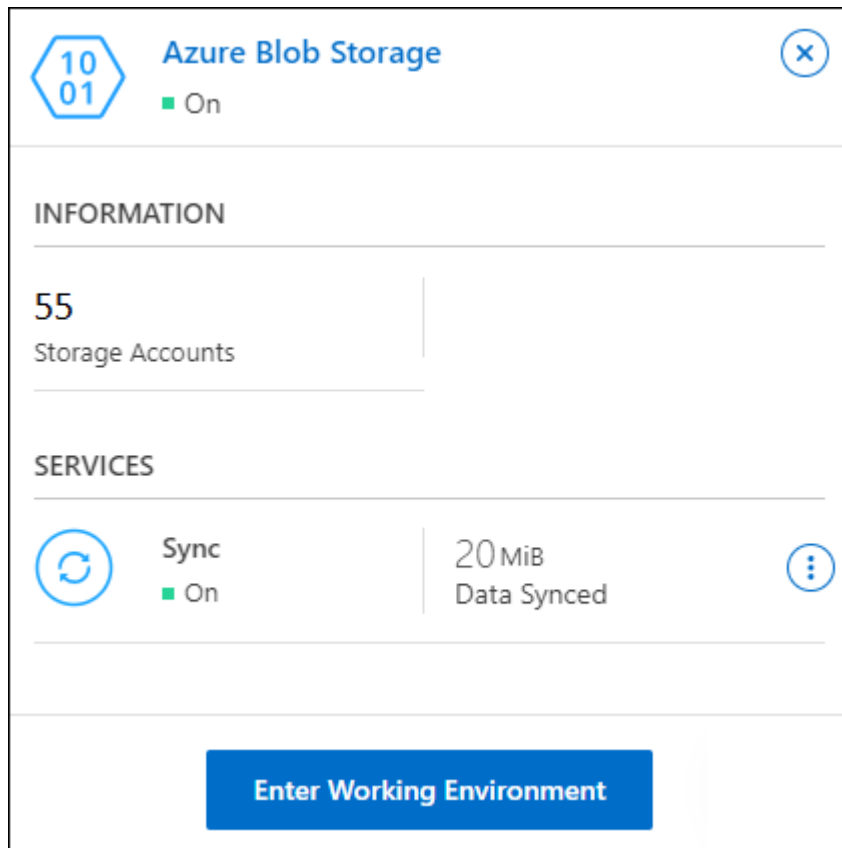
### Étapes

1. ["Installer un connecteur"](#) Dans le compte Azure où vous voulez afficher vos comptes de stockage Azure
2. Dans le menu de navigation, sélectionnez **stockage > Canvas**.

Vous devriez voir automatiquement un environnement de travail Azure Blob peu de temps après.



3. Cliquez sur l'environnement de travail et sélectionnez une action dans le volet droit.



4. Cliquez sur **Synchroniser les données** pour synchroniser les données vers ou depuis le stockage Azure Blob.

Pour plus de détails, voir "[La présentation du service Cloud Sync](#)".

5. Cliquez sur **entrer environnement de travail** pour afficher les détails sur les comptes de stockage Azure dans vos blobs Azure.

1001

Azure blob

Overview

1001

637

Total Storage Accounts

1.5 TiB

Total Capacity

16

Total Locations

637 Storage Accounts

Storage Account Name	Subscription	Location	Creation Date	Resource Group	Blob Capacity
ovu8llxvqdfypxn	OCCM QA1	West US	June 24, 2021	AdmAzureHa-rg	170 B
rootsa9ktpjzcm	OCCM QA1	West US	June 24, 2021	AdmAzureHa-rg	950.22 GiB
scvdwjcwehswli	OCCM QA1	West US	June 24, 2021	AdmAzureHa-rg	22.12 MiB
65qtx0smegmq2vt	OCCM QA1	West US	June 24, 2021	AdmAzureVsa-rg	170 B
bu9klxthymr1be	OCCM QA1	West US	June 24, 2021	AdmAzureVsa-rg	1.01 MiB
8jzsvybvjiwieww8	OCCM QA1	Canada Central	December 12, 2019	aff1-rg	170 B

## Afficher les compartiments de stockage Google Cloud

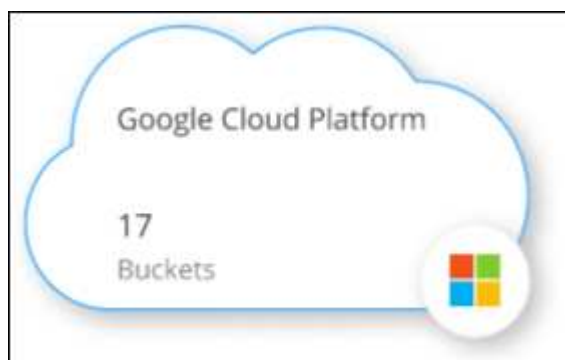
Après avoir installé un connecteur dans Google Cloud, BlueXP peut automatiquement découvrir des informations sur les compartiments Google Cloud Storage qui résident dans le compte Google où le connecteur est installé. Un environnement de travail Google Cloud Storage est ajouté à Canvas pour vous permettre de visualiser ces informations.

Vous trouverez des informations détaillées sur vos compartiments Google Cloud Storage : l'emplacement, l'état d'accès, la classe de stockage, la capacité totale et utilisée, entre autres. Ces compartiments peuvent être utilisés comme destinations pour les opérations Cloud Backup, Cloud Tiering ou Cloud Sync.

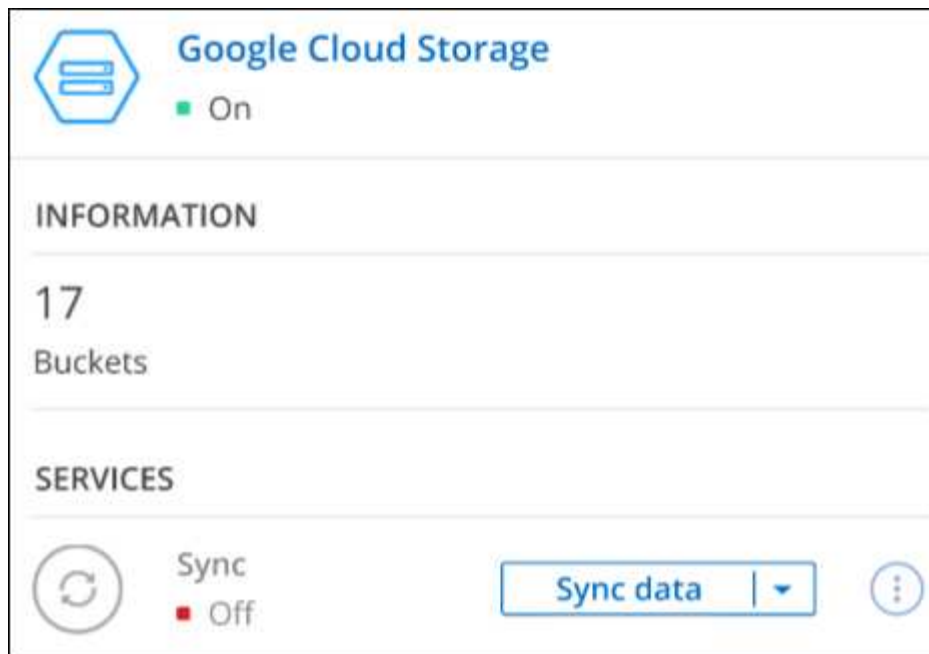
### Étapes

1. "Installer un connecteur" Dans le compte Google où vous souhaitez consulter vos compartiments Google Cloud Storage.
2. Dans le menu de navigation, sélectionnez **stockage > Canvas**.

Vous devriez voir automatiquement un environnement de travail Google Cloud Storage peu après.



3. Cliquez sur l'environnement de travail et sélectionnez une action dans le volet droit.



4. Cliquez sur **Synchroniser les données** pour synchroniser les données vers ou depuis des compartiments Google Cloud Storage.

Pour plus de détails, voir "[La présentation du service Cloud Sync](#)".

5. Cliquez sur **entrer environnement de travail** pour afficher les détails des rubriques de votre compte Google.

The screenshot shows the Google Cloud Storage Overview page. At the top, there's a header with the Google Cloud Storage logo. Below this is an 'Overview' section with three cards: '17 Total buckets', '1.76 TiB Total capacity | Calculating', and '6 Total locations'. Below the overview section is a table titled '17 Buckets'. The table has columns: Bucket Name, Location, Creation Date, Public Access, Default Storage Class, and Total Capacity. The table lists five buckets with their respective details.

Bucket Name	Location	Creation Date	Public Access	Default Storage Class	Total Capacity
BucketName 1	US East (N. Virginia)	May 04 2021	Yes	StorageClass 1	...
BucketName 2	US West (Oregon)	May 04 2021	Yes	StorageClass 2	...
BucketName 3	US East (N. Virginia)	May 04 2021	No	StorageClass 3	...
BucketName 4	US East (N. Virginia)	May 04 2021	No	StorageClass 4	...
BucketName 5	US East (N. Virginia)	May 04 2021	Yes	StorageClass 5	...

## Identifiants AWS

### Identifiants et autorisations AWS

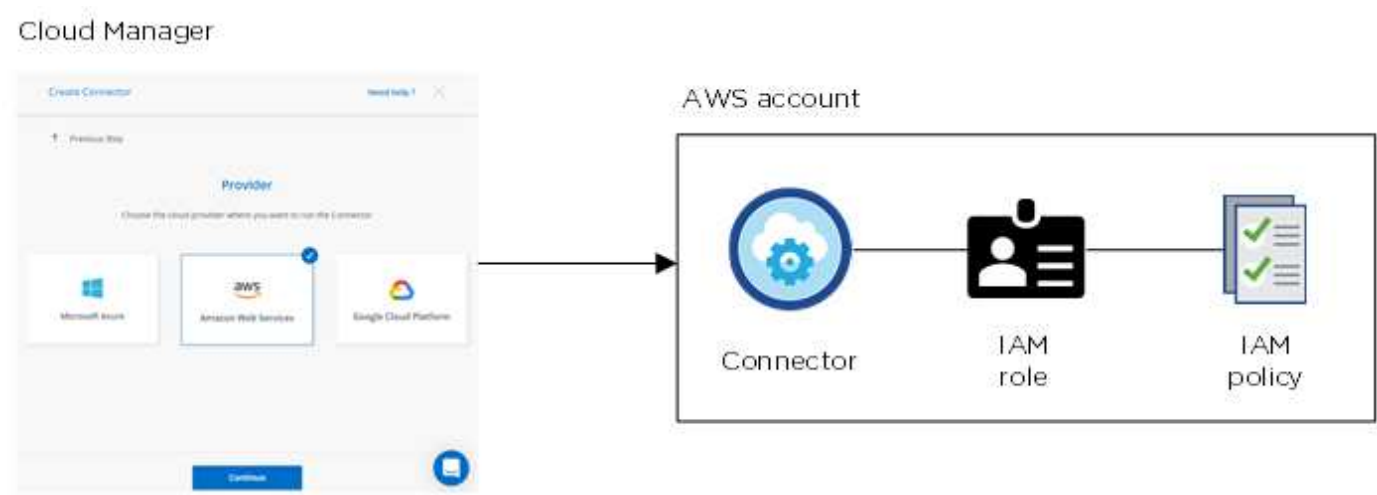
BlueXP vous permet de choisir les informations d'identification AWS à utiliser lors du déploiement de Cloud Volumes ONTAP. Vous pouvez déployer tous vos systèmes Cloud Volumes ONTAP à l'aide des identifiants AWS initiaux, ou ajouter des identifiants

supplémentaires.


Identifiants AWS initiaux

Lorsque vous déployez un connecteur depuis BlueXP, vous devez fournir l'ARN d'un rôle IAM ou de clés d'accès pour un utilisateur IAM. La méthode d'authentification que vous utilisez doit disposer des autorisations requises pour déployer l'instance de connecteur dans AWS. Les autorisations requises sont répertoriées dans le ["Règle de déploiement du connecteur pour AWS"](#).

Lorsque BlueXP lance l'instance Connector dans AWS, il crée un rôle IAM et un profil d'instance pour l'instance. Il attache également une règle qui fournit au connecteur les autorisations nécessaires pour gérer les ressources et les processus de ce compte AWS. ["Consultez la manière dont BlueXP utilise les autorisations"](#).



BlueXP sélectionne ces identifiants AWS par défaut lorsque vous créez un nouvel environnement de travail pour Cloud Volumes ONTAP :

Details & Credentials			
Instance Profile		QA Subscription	<a href="#">Edit Credentials</a>
Credentials	Account ID	Marketplace Subscription	

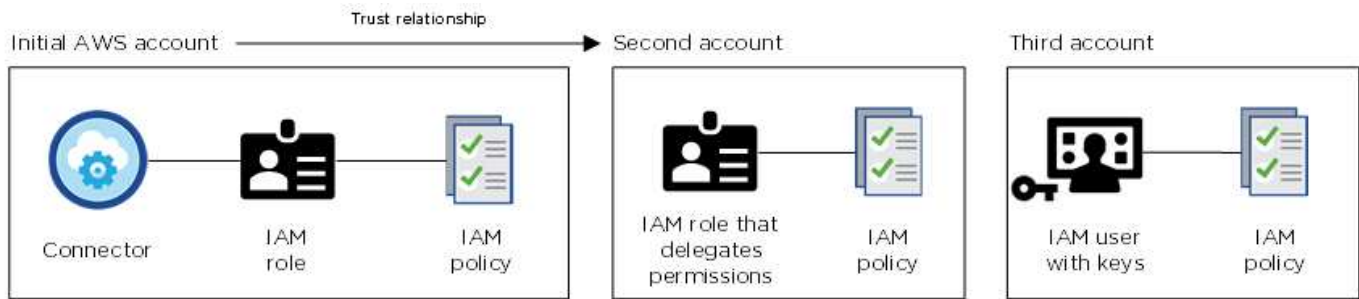
Autres identifiants AWS

Il existe deux façons d'ajouter des identifiants AWS supplémentaires.

Ajoutez des identifiants AWS à un connecteur existant

Si vous souhaitez lancer Cloud Volumes ONTAP sur différents comptes AWS, vous pouvez l'un ou l'autre ["Fournir des clés AWS pour un utilisateur IAM ou le numéro ARN d'un rôle dans un compte de confiance"](#). L'image suivante montre deux comptes supplémentaires, l'un avec des autorisations par le biais d'un rôle IAM dans un compte de confiance et l'autre avec les clés AWS d'un utilisateur IAM :





Vous le feriez alors "[Ajoutez les informations d'identification du compte à BlueXP](#)" En spécifiant le nom de ressource Amazon (ARN) du rôle IAM ou les clés AWS pour l'utilisateur IAM.

Après avoir ajouté un autre ensemble d'informations d'identification, vous pouvez les passer lors de la création d'un nouvel environnement de travail :

**Edit Credentials & Add Subscription**

Associate Subscription to Credentials ⓘ

Credentials

- keys | Account ID: [redacted]
- Instance Profile | Account ID: [redacted]
- casaba QA subscription

+ Add Subscription

Apply Cancel

#### Ajoutez des informations d'identification AWS directement à BlueXP

L'ajout de nouvelles informations d'identification AWS à BlueXP fournit les autorisations nécessaires pour créer et gérer un environnement de travail FSX pour ONTAP ou pour créer un connecteur.

#### Qu'en est-il des déploiements Marketplace et des déploiements sur site ?

Les sections ci-dessus décrivent la méthode de déploiement recommandée pour le connecteur, qui provient de BlueXP. Vous pouvez également déployer un connecteur dans AWS à partir du "[AWS Marketplace](#)" et vous le pouvez "[Installer le connecteur sur site](#)".

Si vous utilisez Marketplace, des autorisations sont fournies de la même manière. Il vous suffit de créer et de configurer manuellement le rôle IAM, puis de fournir des autorisations pour tous les comptes supplémentaires.

Pour les déploiements sur site, vous ne pouvez pas configurer de rôle IAM pour le système BlueXP, mais vous pouvez fournir des autorisations exactement comme pour d'autres comptes AWS.

## Comment faire tourner mes identifiants AWS en toute sécurité ?

Comme décrit ci-dessus, BlueXP vous permet de fournir des identifiants AWS de diverses manières : un rôle IAM associé à l'instance Connector, en assumant un rôle IAM dans un compte de confiance ou en fournissant des clés d'accès AWS.

Avec les deux premières options, BlueXP utilise AWS Security Token Service pour obtenir des informations d'identification temporaires qui tournent en permanence. Ce processus est la meilleure pratique—il est automatique et sécurisé.

Si vous fournissez des clés d'accès AWS BlueXP, vous devez les mettre à jour régulièrement dans BlueXP. Il s'agit d'un processus entièrement manuel.

## Gérez les informations d'identification et les abonnements AWS pour BlueXP

Ajoutez et gérez des identifiants AWS de sorte que BlueXP dispose des autorisations nécessaires pour déployer et gérer des ressources cloud dans vos comptes AWS. Si vous gérez plusieurs abonnements AWS, vous pouvez les attribuer à différentes informations d'identification AWS à partir de la page informations d'identification.

### Présentation

Vous pouvez ajouter des informations d'identification AWS à un connecteur existant ou directement à BlueXP :

- Ajoutez des identifiants AWS supplémentaires à un connecteur existant

L'ajout d'identifiants AWS à un connecteur existant offre les autorisations nécessaires pour gérer les ressources et les processus au sein de votre environnement de cloud public. [credentials to a Connector](#), Découvrez comment ajouter des identifiants AWS à un connecteur.

- Ajoutez des informations d'identification AWS à BlueXP pour créer un connecteur

L'ajout de nouvelles informations d'identification AWS à BlueXP offre à BlueXP les autorisations nécessaires pour créer un connecteur. [credentials to BlueXP for creating a Connector](#), Découvrez comment ajouter des identifiants AWS à BlueXP.

- Ajoutez des informations d'identification AWS à BlueXP pour FSX pour ONTAP

L'ajout de nouvelles informations d'identification AWS à BlueXP offre à BlueXP les autorisations nécessaires pour créer et gérer FSX pour ONTAP. ["Découvrez comment configurer des autorisations pour FSX pour ONTAP"](#)

## Comment faire pivoter les informations d'identification

BlueXP vous permet de fournir des identifiants AWS de diverses manières : un rôle IAM associé à l'instance Connector, en assumant un rôle IAM dans un compte de confiance ou en fournissant des clés d'accès AWS. ["En savoir plus sur les identifiants et les autorisations AWS"](#).

Avec les deux premières options, BlueXP utilise AWS Security Token Service pour obtenir des informations d'identification temporaires qui tournent en permanence. Ce processus est la meilleure pratique car il est automatique et sécurisé.

Si vous fournissez des clés d'accès AWS BlueXP, vous devez les mettre à jour régulièrement dans BlueXP. Il s'agit d'un processus entièrement manuel.

## Ajouter des informations d'identification à un connecteur

Ajoutez des identifiants AWS à un connecteur pour qu'il dispose des autorisations nécessaires pour gérer les ressources et les processus au sein de votre environnement de cloud public. Vous pouvez indiquer l'ARN d'un rôle IAM dans un autre compte ou fournir les clés d'accès AWS.

### Accorder des autorisations

Avant d'ajouter des identifiants AWS à un connecteur, vous devez fournir les autorisations requises. Les autorisations permettent à BlueXP de gérer les ressources et les processus au sein de ce compte AWS. La manière dont vous fournissez les autorisations dépend du fait que vous souhaitez fournir à BlueXP l'ARN d'un rôle dans un compte de confiance ou des clés AWS.



Si vous avez déployé un connecteur depuis BlueXP, BlueXP a automatiquement ajouté des informations d'identification AWS pour le compte dans lequel vous avez déployé le connecteur. Ce compte initial n'est pas ajouté si vous avez déployé le connecteur depuis AWS Marketplace ou si vous avez installé manuellement le logiciel Connector sur un système existant. ["En savoir plus sur les identifiants et les autorisations AWS"](#).

### Choix

- permissions by assuming an IAM role in another account
- permissions by providing AWS keys

### Accorder des autorisations en assumant un rôle IAM dans un autre compte

Vous pouvez définir une relation de confiance entre le compte AWS source dans lequel vous avez déployé l'instance Connector et d'autres comptes AWS en utilisant les rôles IAM. Vous fournissez ensuite à BlueXP les rôles ARN des IAM des comptes de confiance.

### Étapes

1. Accédez à la console IAM dans le compte cible dans lequel vous souhaitez fournir le connecteur avec les autorisations.
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 entrez l'ID du compte sur lequel réside l'instance de connecteur.
- Créez les politiques requises en copiant et en collant le contenu de ["Les règles IAM pour le connecteur"](#).

3. Copiez le rôle ARN du rôle IAM afin de pouvoir le coller ultérieurement dans BlueXP.

Le compte dispose désormais des autorisations requises. ,Vous pouvez désormais ajouter les informations d'identification à un connecteur.

### Accordez des autorisations en fournissant des clés AWS

Si vous voulez fournir des clés BlueXP avec AWS pour un utilisateur IAM, vous devez accorder les autorisations requises à cet utilisateur. La politique de BlueXP IAM définit les actions et les ressources AWS que BlueXP est autorisé à utiliser.

## Étapes

1. À partir de la console IAM, créez des politiques en copiant et en collant le contenu de "[Les règles IAM pour le connecteur](#)".

["Documentation AWS : création de règles IAM"](#)

2. Associez les règles à un rôle IAM ou à un utilisateur IAM.
  - ["Documentation AWS : création de rôles IAM"](#)
  - ["Documentation AWS : ajout et suppression de règles IAM"](#)

Le compte dispose désormais des autorisations requises. ,Vous pouvez désormais ajouter les informations d'identification à un connecteur.

### Ajoutez les informations d'identification

Une fois que vous avez passé un compte AWS avec les autorisations requises, vous pouvez ajouter les identifiants de ce compte à un connecteur existant. Cela vous permet de lancer des systèmes Cloud Volumes ONTAP dans ce compte à l'aide du même connecteur.

Si vous venez de créer ces identifiants dans votre fournisseur cloud, il vous faudra quelques minutes pour les utiliser. Attendez quelques minutes avant d'ajouter les informations d'identification à BlueXP.

## Étapes

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



3. Cliquez sur **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** : fournir l'ARN (Amazon Resource Name) d'un rôle IAM approuvé, ou entrer 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.

Pour payer Cloud Volumes ONTAP à l'heure (PAYGO) ou par un contrat annuel, vous devez associer des identifiants AWS à un abonnement à Cloud Volumes ONTAP depuis AWS Marketplace.

- d. **Review** : confirmez les détails des nouvelles informations d'identification et cliquez sur **Add**.

Vous pouvez maintenant passer à un autre ensemble d'informations d'identification à partir de la page Détails et informations d'identification lors de la création d'un nouvel environnement de travail :

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

- keys | Account ID: [redacted]
- Instance Profile | Account ID: [redacted]
- casaba QA subscription

+ Add Subscription

Apply Cancel

### Ajoutez des informations d'identification à BlueXP pour créer un connecteur

Ajoutez des informations d'identification AWS à BlueXP en fournissant l'ARN d'un rôle IAM qui donne à BlueXP les autorisations nécessaires pour créer un connecteur. Vous pouvez choisir ces informations d'identification lors de la création d'un nouveau connecteur.

#### Configurer le rôle IAM

Configurez un rôle IAM qui permet au service BlueXP SaaS de prendre en charge le rôle.

#### Étapes

1. Accédez à la console IAM 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 service BlueXP SaaS : 952013314444
- Créez une stratégie qui inclut les autorisations requises pour créer un connecteur.
  - ["Affichez les autorisations nécessaires pour FSX pour ONTAP"](#)
  - ["Afficher la règle de déploiement des connecteurs"](#)

3. Copiez le rôle ARN du rôle IAM afin de pouvoir le coller dans BlueXP à l'étape suivante.

Le rôle IAM dispose désormais des autorisations requises. ,Vous pouvez maintenant l'ajouter à BlueXP.

#### Ajoutez les informations d'identification

Une fois que vous avez autorisé le rôle IAM, ajoutez le rôle ARN à BlueXP.

Si vous venez de créer le rôle IAM, l'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, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.



2. Cliquez sur **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
  - a. **Informations d'identification Location** : sélectionnez **Amazon Web Services > BlueXP**.
  - b. **Définir les informations d'identification** : fournir l'ARN (Amazon Resource Name) du rôle IAM.
  - c. **Review** : confirmez les détails des nouvelles informations d'identification et cliquez sur **Add**.

Vous pouvez maintenant utiliser les informations d'identification lors de la création d'un nouveau connecteur.

### Associez un abonnement AWS

Après avoir ajouté vos identifiants AWS à BlueXP, vous pouvez associer un abonnement AWS Marketplace à ces identifiants. L'abonnement vous permet de payer le prix Cloud Volumes ONTAP à l'heure (PAYGO) ou de souscrire un contrat annuel et d'utiliser d'autres services cloud NetApp.

Deux scénarios peuvent vous être associés à un abonnement AWS Marketplace une fois que vous avez déjà ajouté les identifiants à BlueXP :

- Vous n'avez pas associé d'abonnement lorsque vous avez initialement ajouté les informations d'identification à BlueXP.
- Vous souhaitez remplacer un abonnement AWS Marketplace existant par un nouvel abonnement.

Vous devez créer un connecteur avant de pouvoir modifier les paramètres BlueXP. ["Apprenez à créer un connecteur"](#).

### Étapes

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



3. Sélectionnez un abonnement existant dans la liste déroulante ou cliquez sur **Ajouter un abonnement** et suivez les étapes pour créer un nouvel abonnement.

► [https://docs.netapp.com/fr-fr/cloud-manager-setup-admin//media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/fr-fr/cloud-manager-setup-admin//media/video_subscribing_aws.mp4) (video)

## Modifier les informations d'identification

Modifiez vos informations d'identification AWS dans BlueXP en modifiant le type de compte (clés AWS ou rôle supposons), en modifiant le nom ou en mettant à jour les informations d'identification elles-mêmes (clés ou rôle ARN).



Vous ne pouvez pas modifier les informations d'identification d'un profil d'instance associé à une instance de connecteur.

### Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.
2. Cliquez sur le menu d'action correspondant à un ensemble d'informations d'identification, puis sélectionnez **Modifier les informations d'identification**.
3. Apportez les modifications requises, puis cliquez sur **appliquer**.

## Suppression des informations d'identification

Si vous n'avez plus besoin d'un ensemble d'informations d'identification, vous pouvez les supprimer de BlueXP. Vous ne pouvez supprimer que les informations d'identification qui ne sont pas associées à un environnement de travail.



Vous ne pouvez pas supprimer les informations d'identification d'un profil d'instance associé à une instance de connecteur.

### Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.
2. Cliquez sur le menu d'action pour un ensemble d'informations d'identification, puis sélectionnez **Supprimer les informations d'identification**.
3. Cliquez sur **Supprimer** pour confirmer.



# Identifiants Azure

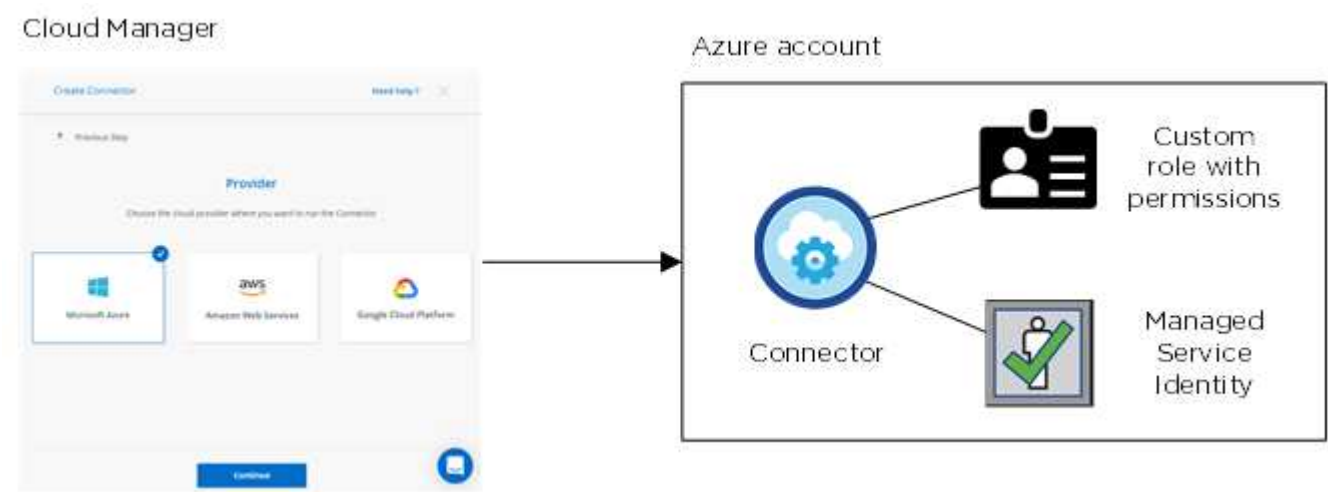
## Identifiants et autorisations Azure

BlueXP vous permet de choisir les informations d'identification Azure à utiliser lors du déploiement de Cloud Volumes ONTAP. Vous pouvez déployer tous vos systèmes Cloud Volumes ONTAP à l'aide des identifiants Azure initiaux, ou ajouter des identifiants supplémentaires.

### Les identifiants initiaux d'Azure

Lorsque vous déployez un connecteur depuis BlueXP, vous devez utiliser un compte ou un service principal Azure disposant des autorisations pour déployer la machine virtuelle Connector. Les autorisations requises sont répertoriées dans le ["Stratégie de déploiement de Connector pour Azure"](#).

Lorsque BlueXP déploie la machine virtuelle Connector dans Azure, il active un ["identité gérée attribuée par le système"](#) sur une machine virtuelle, crée un rôle personnalisé et le attribue à la machine virtuelle. Le rôle fournit à BlueXP les autorisations requises pour gérer les ressources et les processus au sein de cet abonnement Azure. ["Consultez la manière dont BlueXP utilise les autorisations"](#).



BlueXP sélectionne ces informations d'identification Azure par défaut lorsque vous créez un nouvel environnement de travail pour Cloud Volumes ONTAP :

Details & Credentials			
Managed Service Ide...	OCCM QA1	<span>ⓘ</span> No subscription is associated	<a href="#">Edit Credentials</a>
Credential Name	Azure Subscription	Marketplace Subscription	

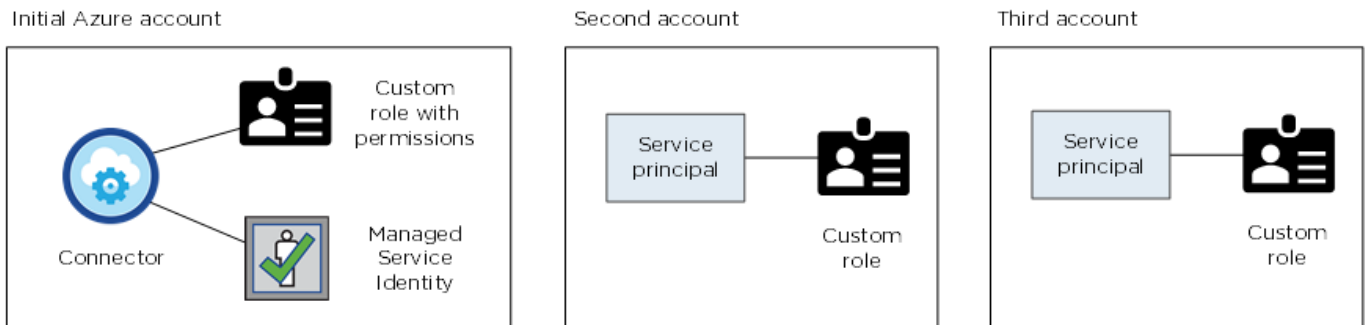
### Des abonnements Azure supplémentaires pour une identité gérée

L'identité gérée est associée à l'abonnement dans lequel vous avez lancé le connecteur. Si vous souhaitez sélectionner un autre abonnement Azure, vous devez le faire ["associez l'identité gérée à ces abonnements"](#).



## Autres identifiants Azure

Si vous souhaitez déployer Cloud Volumes ONTAP avec différents identifiants Azure, vous devez accorder les autorisations requises par "[Création et configuration d'une entité de service dans Azure Active Directory](#)" Pour chaque compte Azure. L'image suivante montre deux comptes supplémentaires, chacun étant doté d'un rôle principal de service et personnalisé qui fournit des autorisations :



Vous le feriez alors "[Ajoutez les informations d'identification du compte à BlueXP](#)" En fournissant des détails sur le principal du service AD.

Après avoir ajouté un autre ensemble d'informations d'identification, vous pouvez les passer lors de la création d'un nouvel environnement de travail :

The screenshot shows the **Edit Account & Add Subscription** dialog box. The **Credentials** section is active, displaying a text input field with a dropdown menu. The dropdown menu is open, showing the following options:

- cloud-manager-app | Application ID: 57c42424-88a0-480a.
- Managed Service Identity** (highlighted in blue)
- OCCM QA1 (Default)

## Qu'en est-il des déploiements Marketplace et des déploiements sur site ?

Les sections ci-dessus décrivent la méthode de déploiement recommandée pour le connecteur, qui provient de BlueXP. Vous pouvez également déployer un connecteur dans Azure à partir du "[Azure Marketplace](#)", et vous pouvez "[Installer le connecteur sur site](#)".

Si vous utilisez Marketplace, des autorisations sont fournies de la même manière. Il vous suffit de créer et de configurer manuellement l'identité gérée pour le connecteur, puis de fournir des autorisations pour tous les comptes supplémentaires.

Pour les déploiements sur site, vous ne pouvez pas configurer une identité gérée pour le connecteur, mais vous pouvez fournir des autorisations comme vous le feriez pour des comptes supplémentaires en utilisant une entité de service.

## Gestion des informations d'identification et des abonnements Azure pour BlueXP

Lorsque vous créez un système Cloud Volumes ONTAP, vous devez sélectionner les identifiants Azure à utiliser avec ce système. Vous devez également choisir un abonnement Marketplace, si vous utilisez une licence payante à l'utilisation. Suivez les étapes indiquées sur cette page si vous devez utiliser plusieurs identifiants Azure ou plusieurs abonnements Azure Marketplace pour Cloud Volumes ONTAP.

Il existe deux façons d'ajouter des abonnements et des informations d'identification Azure supplémentaires dans BlueXP.

1. Associez des abonnements Azure supplémentaires à l'identité gérée Azure.
2. Si vous souhaitez déployer Cloud Volumes ONTAP à l'aide de différentes informations d'identification Azure, accordez des autorisations Azure à l'aide d'un service principal et ajoutez ses informations d'identification à BlueXP.

### Association d'abonnements Azure supplémentaires à une identité gérée

BlueXP vous permet de choisir les identifiants Azure et l'abonnement Azure dans lesquels vous souhaitez déployer Cloud Volumes ONTAP. Vous ne pouvez pas sélectionner un autre abonnement Azure pour le profil d'identité gérée à moins d'associer le "[identité gérée](#)" avec ces abonnements.

Une identité gérée est "[Compte Azure initial](#)". Lorsque vous déployez un connecteur depuis BlueXP. Lorsque vous avez déployé le connecteur, BlueXP a créé le rôle opérateur BlueXP et l'a affecté à la machine virtuelle Connector.

### Étapes

1. Connectez-vous au portail Azure.
2. Ouvrez le service **abonnements**, puis sélectionnez l'abonnement dans lequel vous souhaitez déployer Cloud Volumes ONTAP.
3. Cliquez sur **contrôle d'accès (IAM)**.
  - a. Cliquez sur **Ajouter > Ajouter une affectation de rôle**, puis ajoutez les autorisations suivantes :
    - Sélectionnez le rôle **opérateur BlueXP**.



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

- Attribuez l'accès à une **machine virtuelle**.
- Sélectionnez l'abonnement dans lequel la machine virtuelle du connecteur a été créée.
- Sélectionnez la machine virtuelle Connector.
- Cliquez sur **Enregistrer**.

4. Répétez ces étapes pour les abonnements supplémentaires.

Lorsque vous créez un nouvel environnement de travail, vous devriez désormais pouvoir sélectionner plusieurs abonnements Azure pour le profil d'identité géré.

Edit Account & Add Subscription

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev

OCCM QA1 (Default)

No subscription is associated with this account

### Ajout d'informations d'identification Azure supplémentaires à BlueXP

Lorsque vous déployez un connecteur depuis BlueXP, BlueXP active une identité gérée attribuée par le système sur la machine virtuelle qui dispose des autorisations requises. BlueXP sélectionne ces informations d'identification Azure par défaut lorsque vous créez un nouvel environnement de travail pour Cloud Volumes ONTAP.



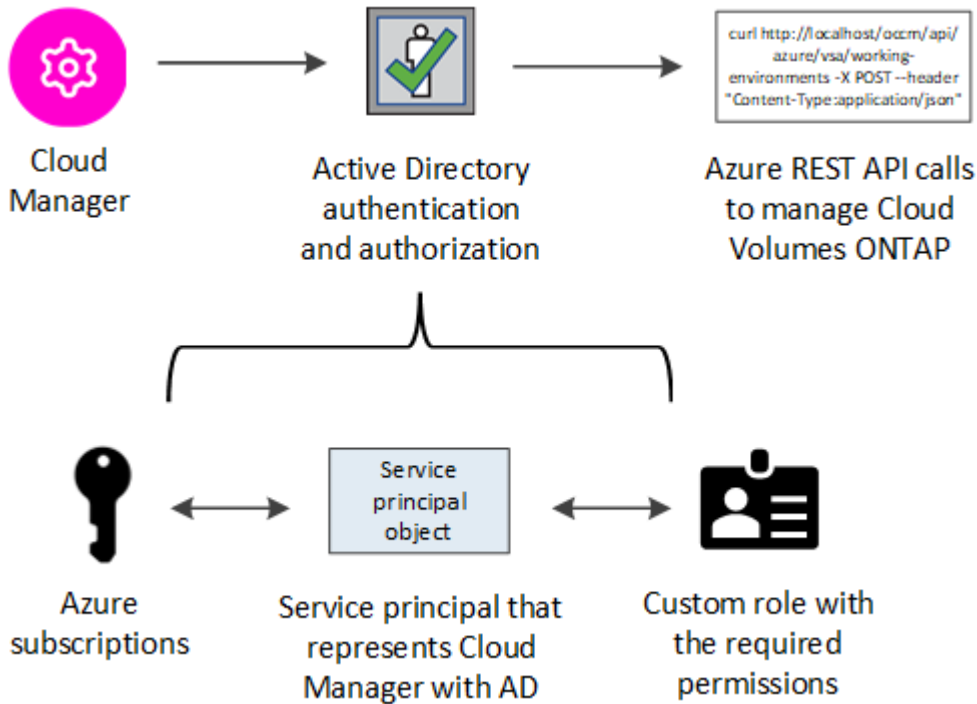
Un jeu initial d'informations d'identification n'est pas ajouté si vous avez installé manuellement le logiciel du connecteur sur un système existant. ["En savoir plus sur les identifiants et les autorisations Azure"](#).

Si vous souhaitez déployer Cloud Volumes ONTAP à l'aide de *diffus* Azure, vous devez accorder les autorisations requises en créant et en configurant un principal de service dans Azure Active Directory pour chaque compte Azure. Vous pouvez ensuite ajouter les nouvelles informations d'identification à BlueXP.

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

BlueXP a besoin d'autorisations pour effectuer des actions dans Azure. Vous pouvez accorder les autorisations requises à un compte Azure en créant et en configurant un service principal dans Azure Active Directory et en obtenant les informations d'identification Azure requises par BlueXP.

L'image suivante décrit comment BlueXP obtient les autorisations pour effectuer des opérations dans Azure. Un objet principal de service, lié à un ou plusieurs abonnements Azure, représente BlueXP dans Azure Active Directory et est affecté à un rôle personnalisé qui autorise les autorisations requises.



### Étapes

1. an Azure Active Directory application, Créez une application Azure Active Directory.
2. the application to a role, Attribuez l'application à un rôle.
3. Windows Azure Service Management API permissions, Ajoutez des autorisations d'API de gestion de service Windows Azure.
4. the application ID and directory ID, Obtenir l'ID de l'application et l'ID du répertoire.
5. a client secret, Créez un secret client.

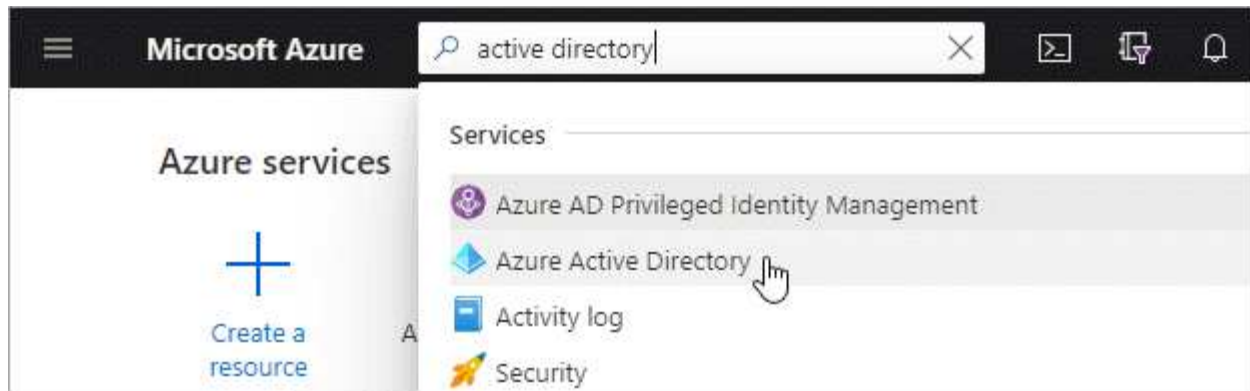
### Création d'une application Azure Active Directory

Créez une application et une entité de service Azure Active Directory (AD) que BlueXP peut utiliser pour le contrôle d'accès basé sur des rôles.

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**.

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

### Affectation de l'application à un rôle

Vous devez lier l'entité de service à un ou plusieurs abonnements Azure et lui attribuer le rôle "opérateur BlueXP" personnalisé afin que BlueXP dispose d'autorisations dans Azure.

### Étapes

1. Création d'un rôle personnalisé :
  - 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

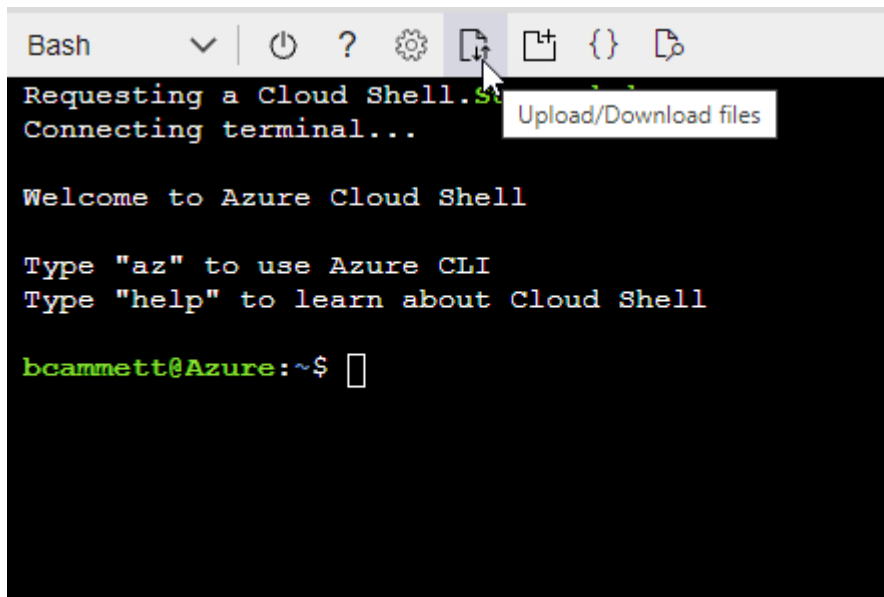
```
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

- 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.



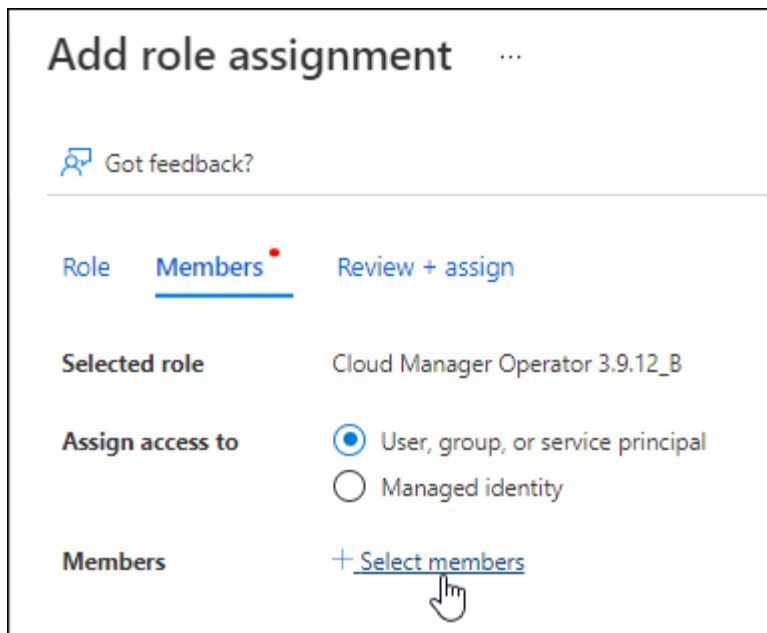
- Entrez la commande Azure CLI suivante :

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

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

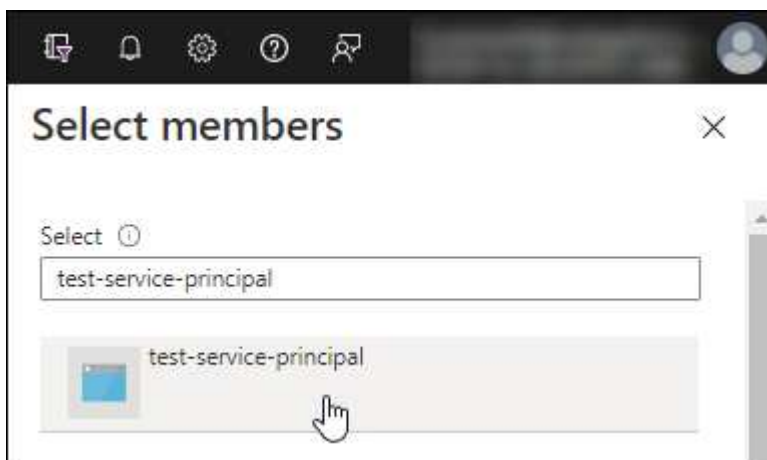
## 2. Attribuez l'application au rôle :

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



- Recherchez le nom de l'application.

Voici un exemple :



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

## Ajout d'autorisations d'API de gestion des services 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.

 <p><b>Azure Batch</b> Schedule large-scale parallel and HPC applications in the cloud</p>	 <p><b>Azure Data Catalog</b> Programmatic access to Data Catalog resources to register, annotate and search data assets</p>	 <p><b>Azure Data Explorer</b> Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions</p>
 <p><b>Azure Data Lake</b> Access to storage and compute for big data analytic scenarios</p>	 <p><b>Azure DevOps</b> Integrate with Azure DevOps and Azure DevOps server</p>	 <p><b>Azure Import/Export</b> Programmatic control of import/export jobs</p>
 <p><b>Azure Key Vault</b> Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults</p>	 <p><b>Azure Rights Management Services</b> Allow validated users to read and write protected content</p>	 <p><b>Azure Service Management</b> Programmatic access to much of the functionality available through the Azure portal</p>
 <p><b>Azure Storage</b> Secure, massively scalable object and data lake storage for unstructured and semi-structured data</p>	 <p><b>Customer Insights</b> Create profile and interaction models for your products</p>	 <p><b>Data Export Service for Microsoft Dynamics 365</b> Export data from Microsoft Dynamics CRM organization to an external destination</p>

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](#)

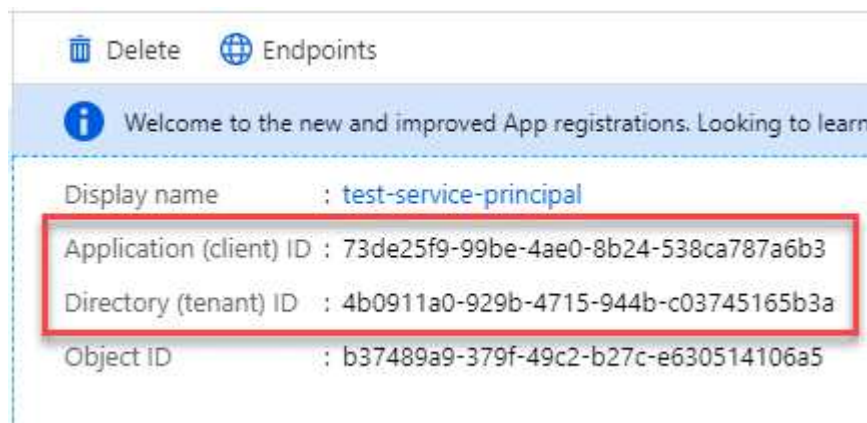
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> <b>user_impersonation</b> Access Azure Service Management as organization users (preview) ⓘ	-

## Obtention de l'ID d'application et de l'ID de répertoire

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.

### 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)**.



## Création d'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	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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.

#### Ajout des informations d'identification à BlueXP

Une fois que vous avez mis à disposition un compte Azure avec les autorisations requises, vous pouvez ajouter les informations d'identification pour ce compte à BlueXP. Cette étape vous permet de lancer Cloud Volumes ONTAP à l'aide de différents identifiants Azure.

Si vous venez de créer ces identifiants dans votre fournisseur cloud, il vous faudra quelques minutes pour les utiliser. Attendez quelques minutes avant d'ajouter les informations d'identification à BlueXP.

Vous devez créer un connecteur avant de pouvoir modifier les paramètres BlueXP. ["Découvrez comment"](#).

#### Étapes

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

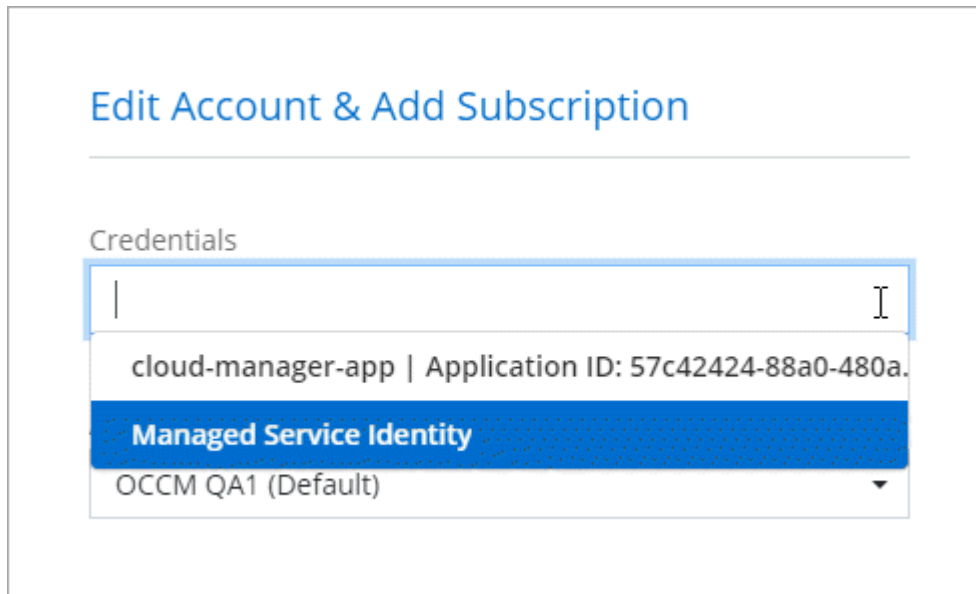


2. Cliquez sur **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
  - a. **Emplacement des informations d'identification** : sélectionnez **Microsoft Azure > connecteur**.
  - b. **Définir les informations d'identification** : saisissez des informations sur l'entité principale du service Azure Active Directory qui accorde les autorisations requises :
    - ID de l'application (client) : voir the application ID and directory ID.
    - ID de répertoire (locataire) : voir the application ID and directory ID.
    - Secret client : voir a client secret.
  - c. **Abonnement Marketplace** : associez un abonnement Marketplace à ces identifiants en vous abonnant maintenant ou en sélectionnant un abonnement existant.

Pour payer Cloud Volumes ONTAP à l'heure (PAYGO), ces identifiants Azure doivent être associés à un abonnement depuis Azure Marketplace.

d. **Review** : confirmez les détails des nouvelles informations d'identification et cliquez sur **Add**.

Vous pouvez maintenant passer à différents ensembles d'informations d'identification à partir de la page Détails et informations d'identification "[lors de la création d'un nouvel environnement de travail](#)"



### Gérer les identifiants existants

Gérez les informations d'identification Azure que vous avez déjà ajoutées à BlueXP en associant un abonnement Marketplace, en modifiant des informations d'identification et en les supprimant.

#### Association d'un abonnement à Azure Marketplace aux identifiants

Après avoir ajouté vos informations d'identification Azure à BlueXP, vous pouvez associer un abonnement Azure Marketplace à ces informations d'identification. Cet abonnement vous permet de créer un système Cloud Volumes ONTAP basé sur l'utilisation et d'utiliser d'autres services cloud NetApp.

Deux scénarios peuvent vous être associés à un abonnement Azure Marketplace une fois que vous avez déjà ajouté les informations d'identification à BlueXP :

- Vous n'avez pas associé d'abonnement lorsque vous avez initialement ajouté les informations d'identification à BlueXP.
- Vous souhaitez remplacer un abonnement Azure Marketplace existant par un nouvel abonnement.

Vous devez créer un connecteur avant de pouvoir modifier les paramètres BlueXP. "[Découvrez comment](#)".

### Étapes

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



3. Sélectionnez un abonnement dans la liste déroulante ou cliquez sur **Ajouter un abonnement** et suivez les étapes pour créer un nouvel abonnement.

La vidéo suivante démarre à partir du contexte de l'assistant de l'environnement de travail, mais vous montre le même flux de travail après avoir cliqué sur **Ajouter un abonnement** :

► [https://docs.netapp.com/fr-fr/cloud-manager-setup-admin//media/video\\_subscribing\\_azure.mp4](https://docs.netapp.com/fr-fr/cloud-manager-setup-admin//media/video_subscribing_azure.mp4) (video)

### Modification des informations d'identification

Modifiez vos informations d'identification Azure dans BlueXP en modifiant les informations d'identification de votre service Azure. Par exemple, vous devrez peut-être mettre à jour le secret client si un nouveau secret a été créé pour l'application principale du service.

#### Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.
2. Cliquez sur le menu d'action correspondant à un ensemble d'informations d'identification, puis sélectionnez **Modifier les informations d'identification**.
3. Apportez les modifications requises, puis cliquez sur **appliquer**.

### Suppression des informations d'identification

Si vous n'avez plus besoin d'un ensemble d'informations d'identification, vous pouvez les supprimer de BlueXP. Vous ne pouvez supprimer que les informations d'identification qui ne sont pas associées à un environnement de travail.

#### Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.
2. Cliquez sur le menu d'action pour un ensemble d'informations d'identification, puis sélectionnez **Supprimer les informations d'identification**.
3. Cliquez sur **Supprimer** pour confirmer.

## Identifiants Google Cloud

### Projets, autorisations et comptes Google Cloud

Un compte de service fournit à BlueXP des autorisations de déploiement et de gestion de

systèmes Cloud Volumes ONTAP dans le même projet que le connecteur, ou dans des projets différents.

### Projet et autorisations pour BlueXP

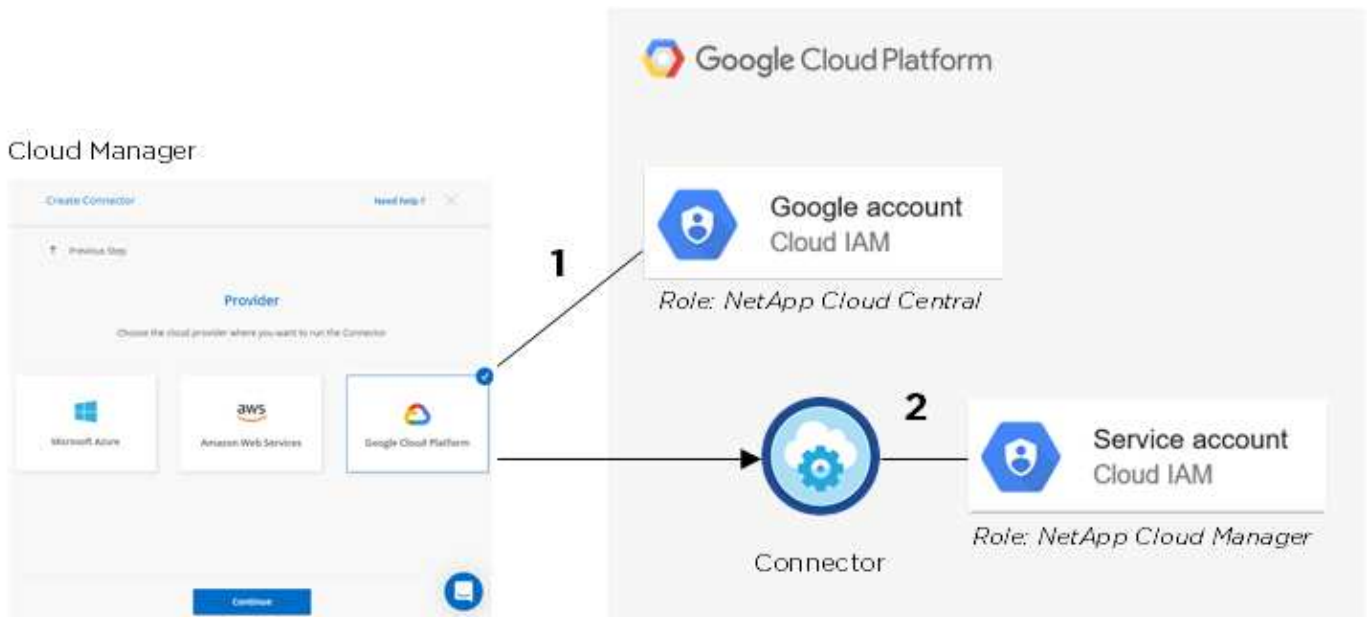
Avant de déployer Cloud Volumes ONTAP dans Google Cloud, vous devez d'abord déployer un connecteur dans un projet Google Cloud. Il ne peut pas s'exécuter sur site ou dans un autre fournisseur cloud.

Deux ensembles d'autorisations doivent être en place avant de déployer un connecteur directement depuis BlueXP :

1. Vous devez déployer un connecteur à l'aide d'un compte Google disposant des autorisations nécessaires pour lancer l'instance VM Connector à partir de BlueXP.
2. Lorsque vous déployez le connecteur, vous êtes invité à sélectionner un ["compte de service"](#) Pour l'instance de VM. BlueXP obtient les autorisations du compte de service pour créer et gérer des systèmes Cloud Volumes ONTAP en votre nom. Les autorisations sont fournies en ajoutant un rôle personnalisé au compte de service.

Nous avons configuré deux fichiers YAML qui incluent les autorisations requises pour l'utilisateur et le compte de service. ["Découvrez comment utiliser les fichiers YAML pour configurer les autorisations"](#).

L'image suivante décrit les conditions d'autorisation décrites aux numéros 1 et 2 ci-dessus :



### Projet pour Cloud Volumes ONTAP

Cloud Volumes ONTAP peut résider dans le même projet que le connecteur ou dans un autre projet. Pour déployer Cloud Volumes ONTAP dans un autre projet, vous devez d'abord ajouter le compte de service Connector et le rôle à ce projet.

- ["Découvrez comment configurer un compte de service"](#)
- ["Découvrez comment déployer Cloud Volumes ONTAP dans GCP et sélectionner un projet"](#)

## Gestion des informations d'identification et des abonnements Google Cloud pour BlueXP

Vous pouvez gérer les informations d'identification associées à l'instance de VM Connector.

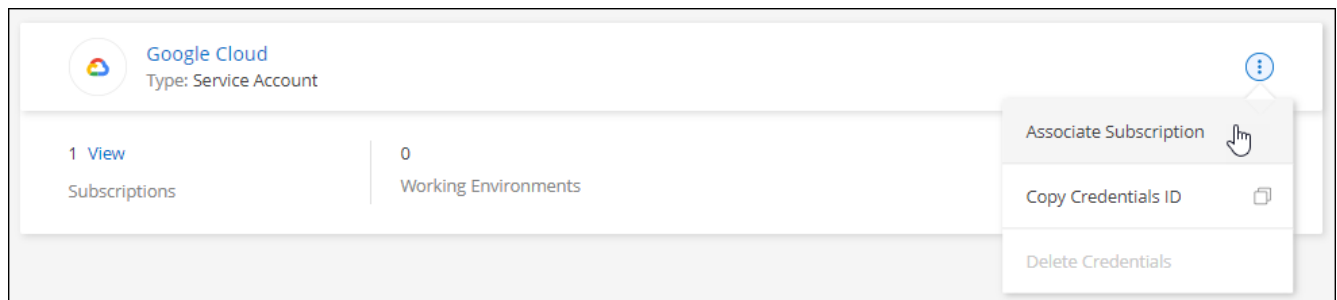
### Association d'un abonnement Marketplace aux informations d'identification GCP

Lorsque vous déployez un connecteur dans GCP, BlueXP crée un ensemble d'informations d'identification par défaut qui sont associées à l'instance de VM connecteur. Il s'agit des informations d'identification utilisées par BlueXP pour déployer Cloud Volumes ONTAP.

Vous pouvez à tout moment modifier l'abonnement Marketplace associé à ces informations d'identification. Cet abonnement vous permet de créer un système Cloud Volumes ONTAP basé sur l'utilisation et d'utiliser d'autres services cloud NetApp.

#### Étapes

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



3. Sélectionnez un projet et un abonnement Google Cloud dans la liste déroulante.

A screenshot of a form for selecting a Google Cloud Project and Subscription. The 'Google Cloud Project' dropdown menu is set to 'OCCM-Dev'. The 'Subscription' dropdown menu is set to 'GCP subscription for staging'. At the bottom, there is a blue button with a plus sign and the text 'Add Subscription'.

4. Cliquez sur **associé**.
5. Si vous n'avez pas encore d'abonnement, cliquez sur **Ajouter un abonnement** et suivez les étapes ci-

dessous pour créer un nouvel abonnement.




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

6. Redécouvrez les étapes de l'abonnement et cliquez sur **Continuer**.

### Add Subscription


Subscription Steps:


- 1 Cloud Manager**  
Clicking **Continue** to create your subscription from the Google Cloud Marketplace.
- 2 Google Cloud Marketplace**  
Subscribe and then then click **Register With NetApp** to configure your account from Cloud Central.
- 3 Cloud Central**  
Save your subscription.
- 4 Cloud Manager**  
Associate the Marketplace subscription with your Google Cloud project.

 View video instructions

ContinueCancel

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


Google Cloud Platform
My First Project



## Cloud Manager for Cloud Volumes ONTAP

NetApp, Inc.

Enterprise-grade data management and protection

**SUBSCRIBE**

OVERVIEW
PRICING
SUPPORT

### Overview

Cloud Volumes ONTAP is a data-management layer that runs natively on Google Cloud infrastructure enabling enhanced control, data protection, mobility and agility for business application data. Get consistent enterprise-grade storage across your hybrid cloud platforms with built-in disaster recovery, backup and ransomware protection. Seamlessly migrate enterprise applications without reengineering. Create company-wide file shares with simultaneous NFS and CIFS/SMB access and iSCSI block storage for GCE instances with scalability up to 368TB. Automate persistent storage provisioning for your Kubernetes clusters. Accelerate CI/CD cycles with instant, zero-capacity data replication. Reduce storage costs by 70% with advanced storage efficiencies. Cloud Manager is the console used to deploy, manage and automate Cloud Volumes ONTAP instances across the hybrid multi-cloud.

[Learn more](#)

### Additional details

Type: [APIs & services](#)

Last updated: 3/26/21

Category: [Storage](#)

Runs on: NetApp, Inc. Cloud Servers

8. Cliquez sur **Subscribe**.

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



## 2. Purchase details

Select a billing account \*  
Secondary\_Billing\_Account

## 3. Terms

### Cancellation and change policy

- Usage fee is billed every month.
- You can cancel the service at any time and it will take effect immediately. You will be billed by the amount you used for that month.

### Additional terms

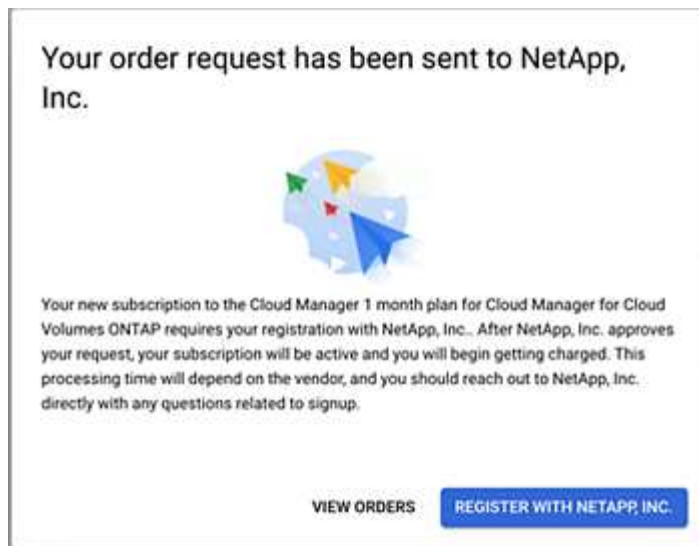
- ☒ I understand this subscription will be automatically renewed at the end of the current term.
- ☒ I authorize Google LLC and its affiliates ("Google") to share my purchase, usage, operational (e.g., project lifecycle events), support ticket, and account information with NetApp, Inc., its affiliates and subcontractors, for the purposes of providing the service, sales attribution, and technical support. I represent that I have the authority to bind my company.
- ☒ By deploying the software or accessing the service you are agreeing to comply with the [End User License Agreement](#), [GCP Marketplace Terms of Service](#), and the terms of applicable open source software licenses bundled with the software or service. Please review these terms and licenses carefully for details about any obligations you may have related to the software or service. To the limited extent an open source software license related to the software or service expressly supersedes the GCP Marketplace Terms of Service, that open source software license governs your use of that software or service.
- By using this product, you understand that certain account and usage information may be shared with NetApp, Inc. for the purposes of financial accounting, sales attribution, performance analysis, and support. ⓘ
- Google is providing this software or service "as-is" and any support for this software or service will be provided by NetApp, Inc. under their terms of service.

SUBSCRIBE

10. Cliquez sur **Subscribe**.

Cette étape envoie votre demande de transfert à NetApp.

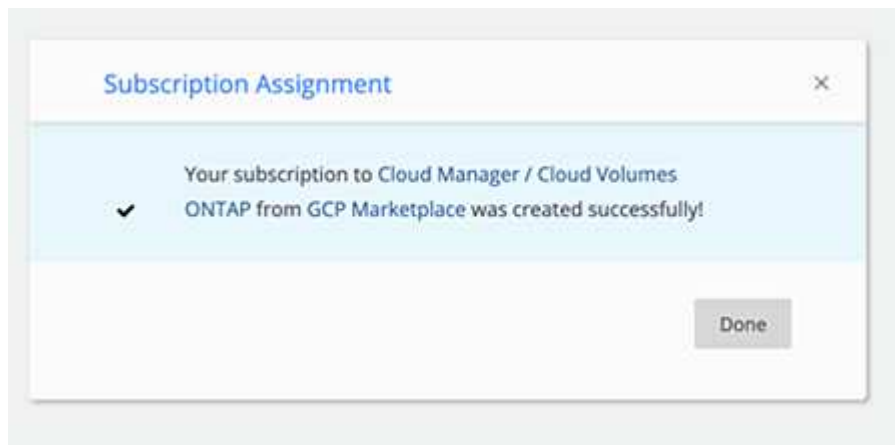
11. Dans la boîte de dialogue contextuelle, cliquez sur **s'inscrire auprès de NetApp, Inc.** pour être redirigé vers le site Web NetApp BlueXP.



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

12. Après avoir été redirigé vers BlueXP, connectez-vous ou inscrivez-vous, puis cliquez sur **Done** pour continuer.

L'abonnement GCP sera lié à tous les comptes NetApp auxquels vous êtes associé.



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

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

Google Cloud Project

OCCM-Dev
▼

Subscription

● GCP subscription for staging
▼

+ Add Subscription

## Dépannage du processus d'abonnement Marketplace

Parfois, l'abonnement à Cloud Volumes ONTAP via Google Cloud Marketplace peut devenir fragmenté en raison d'autorisations incorrectes ou accidentellement ne suivant pas la redirection vers le site Web BlueXP. Dans ce cas, procédez comme suit pour terminer le processus d'abonnement.

### Étapes

1. Accédez au ["Page NetApp BlueXP sur Google Cloud Marketplace"](#) pour vérifier l'état de la commande. Si la page indique **Manage on Provider**, faites défiler la page vers le bas et cliquez sur **Manage Orders**.

Pricing

✓ The product was purchased on 12/9/20.

MANAGE ORDERS

- a. Si la commande affiche une coche verte et que cela est inattendu, il est possible que quelqu'un d'autre de l'entreprise utilisant le même compte de facturation soit déjà abonné. Si cela est inattendu ou si vous avez besoin des détails de cet abonnement, contactez votre équipe commerciale NetApp.

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
✓	2eebbc...	Cloud Manager	-	10/21/21	1 month	-	Postpay	N/A	N/A	⋮

- b. Si la commande affiche une horloge et l'état **en attente**, revenez à la page Marketplace et choisissez **gérer sur fournisseur** pour terminer le processus comme indiqué ci-dessus.

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
🕒	d56c66...	Cloud Manager	-	Pending	1 month	Pending	Postpay	N/A	N/A	⋮

# Ajoutez et gérez des comptes du site de support NetApp dans BlueXP

Fournissez les identifiants de vos comptes sur le site du support NetApp (NSS) pour vous inscrire au support, activer des workflows clés pour Cloud Volumes ONTAP et bien plus encore.

## Présentation

Vous devez ajouter votre compte sur le site de support NetApp à BlueXP pour activer les tâches suivantes :

- Pour obtenir de l'aide
- Pour déployer Cloud Volumes ONTAP lorsque vous utilisez votre propre licence (BYOL)

Il est nécessaire de fournir votre compte NSS afin que BlueXP puisse télécharger votre clé de licence et activer l'abonnement pour la durée que vous avez achetée. Cela inclut des mises à jour automatiques pour les renouvellements de contrats.

- Pour enregistrer des systèmes Cloud Volumes ONTAP avec paiement à l'utilisation

Vous devez fournir votre compte NSS afin d'activer le support pour votre système et d'accéder aux ressources du support technique NetApp.

- Pour mettre à niveau le logiciel Cloud Volumes ONTAP vers la dernière version

Vous devrez également saisir vos informations d'identification NSS pour utiliser Digital Advisor (anciennement Active IQ) dans BlueXP. Ces informations d'identification sont directement associées à votre compte utilisateur et ne peuvent être utilisées qu'avec Digital Advisor. Vous trouverez plus de détails dans la section qui suit.

## Gérer un compte NSS associé à Digital Advisor

Lorsque vous accédez à Digital Advisor dans BlueXP, vous êtes invité à vous connecter à Digital Advisor en saisissant vos informations d'identification NSS. Une fois vos identifiants NSS saisi, ce compte NSS s'affiche en haut de la page gestion NSS. Vous pouvez alors gérer ces informations d'identification selon vos besoins.

Remarque :

- Le compte est géré au niveau de l'utilisateur, ce qui signifie qu'il n'est pas visible par les autres utilisateurs qui se connectent.
- Le compte ne peut pas être utilisé avec d'autres fonctionnalités BlueXP : pas avec la création, la licence ou le support Cloud Volumes ONTAP.
- Il ne peut y avoir qu'un seul compte NSS associé à Digital Advisor, par utilisateur.

## Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



2. Cliquez sur **NSS Management**.
3. Sous **vos informations d'identification NSS**, cliquez sur **action** et choisissez l'une des options suivantes :
  - **Utilisateur associé NSS** : ajoutez des identifiants pour un compte sur le site de support NetApp afin que vous puissiez accéder à Digital Advisor dans BlueXP.
  - **Mettre à jour vos identifiants existants** : mettez à jour les identifiants pour votre compte sur le site de support NetApp.
  - **Supprimer** : supprimez le compte associé à Digital Advisor.

BlueXP met à jour le compte NSS associé à Digital Advisor.

## Ajouter un compte NSS

Le tableau de bord du support vous permet d'ajouter et de gérer vos comptes sur le site de support NetApp pour les utiliser avec BlueXP au niveau de votre compte NetApp.

- Si vous avez un compte au niveau du client, vous pouvez ajouter un ou plusieurs comptes NSS.
- Si vous avez un compte partenaire ou revendeur, vous pouvez ajouter un ou plusieurs comptes NSS, mais ils ne peuvent pas être ajoutés en même temps que les comptes au niveau du client.

### Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



2. Cliquez sur **NSS Management > Ajouter un compte NSS**.
3. Lorsque vous y êtes invité, cliquez sur **Continuer** pour être redirigé vers une page de connexion Microsoft.

NetApp utilise Microsoft Azure Active Directory comme fournisseur d'identités pour les services d'authentification spécifiques au support et aux licences.

4. Sur la page de connexion, indiquez l'adresse e-mail et le mot de passe que vous avez enregistrés sur le site de support NetApp pour réaliser le processus d'authentification.

Ces actions permettent à BlueXP d'utiliser votre compte NSS pour des opérations telles que le téléchargement de licences, la vérification de la mise à niveau logicielle et les inscriptions de support futures.

Notez ce qui suit :

- Le compte doit être un compte de niveau client (et non un compte invité ou temporaire).
- Une fois la connexion établie, NetApp stockera le nom d'utilisateur NSS. Il s'agit d'un ID généré par le système qui correspond à votre courrier électronique. Sur la page **NSS Management**, vous pouvez afficher votre courriel à partir du **...** menu.
- Si vous avez besoin d'actualiser vos jetons d'identification de connexion, il existe également une option **mettre à jour les informations d'identification** dans le **...** menu. Cette option vous invite à vous reconnecter.

Les utilisateurs peuvent désormais sélectionner le compte lors de la création de nouveaux systèmes Cloud Volumes ONTAP, lors de l'enregistrement des systèmes Cloud Volumes ONTAP existants et lors de l'inscription au support.

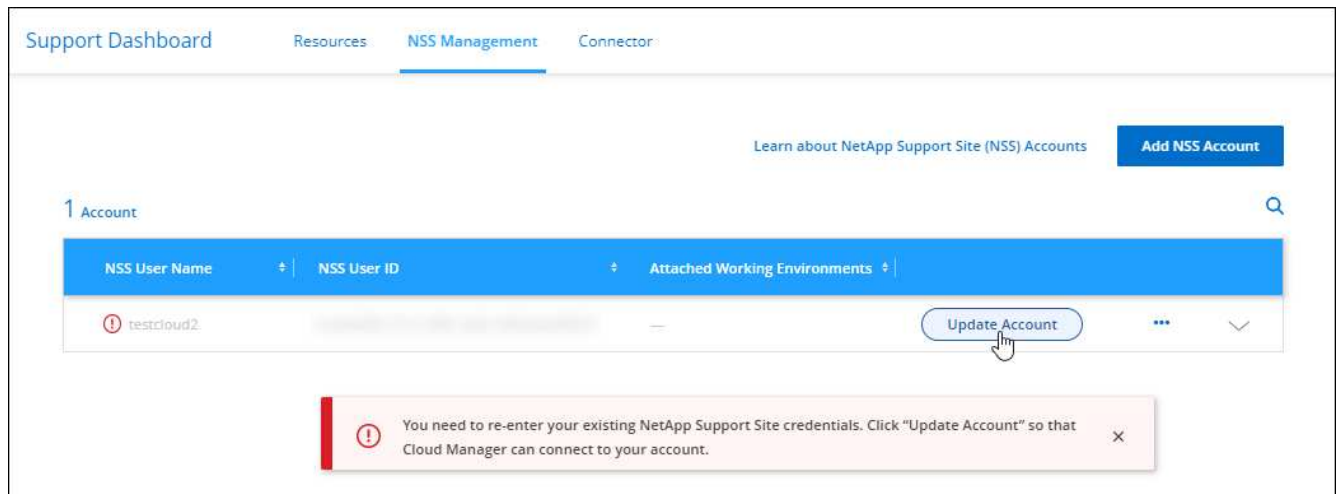
- ["Lancement d'Cloud Volumes ONTAP dans AWS"](#)
- ["Lancement d'Cloud Volumes ONTAP dans Azure"](#)
- ["Lancement d'Cloud Volumes ONTAP dans GCP"](#)
- ["Enregistrement des systèmes de paiement à l'utilisation"](#)

## Mettre à jour un compte NSS pour la nouvelle méthode d'authentification

Depuis novembre 2021, NetApp utilise désormais Microsoft Azure Active Directory comme fournisseur d'identités pour les services d'authentification spécifiques au support et aux licences. Suite à cette mise à jour, BlueXP vous invitera à mettre à jour les informations d'identification de tous les comptes existants que vous avez ajoutés précédemment.

### Étapes

1. Si ce n'est déjà fait, "[Créez un compte Microsoft Azure Active Directory B2C qui sera lié à votre compte NetApp actuel](#)".
2. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.
3. Cliquez sur **NSS Management**.
4. Pour le compte NSS à mettre à jour, cliquez sur **mettre à jour le compte**.



5. Lorsque vous y êtes invité, cliquez sur **Continuer** pour être redirigé vers une page de connexion Microsoft.

NetApp utilise Microsoft Azure Active Directory comme fournisseur d'identités pour les services d'authentification spécifiques au support et aux licences.

6. Sur la page de connexion, indiquez l'adresse e-mail et le mot de passe que vous avez enregistrés sur le site de support NetApp pour réaliser le processus d'authentification.

Une fois le processus terminé, le compte que vous avez mis à jour doit maintenant être répertorié comme un *nouveau* compte dans la table. La *vieille* version du compte est toujours répertoriée dans le tableau, ainsi que toutes les associations d'environnement de travail existantes.

7. Si des environnements de travail Cloud Volumes ONTAP existants sont associés à l'ancienne version du compte, suivez les étapes ci-dessous à a working environment to a different NSS account, Reliez ces environnements de travail à un autre compte NSS.
8. Accédez à l'ancienne version du compte NSS, cliquez sur **...** Puis sélectionnez **Supprimer**.

## Mettre à jour les identifiants NSS

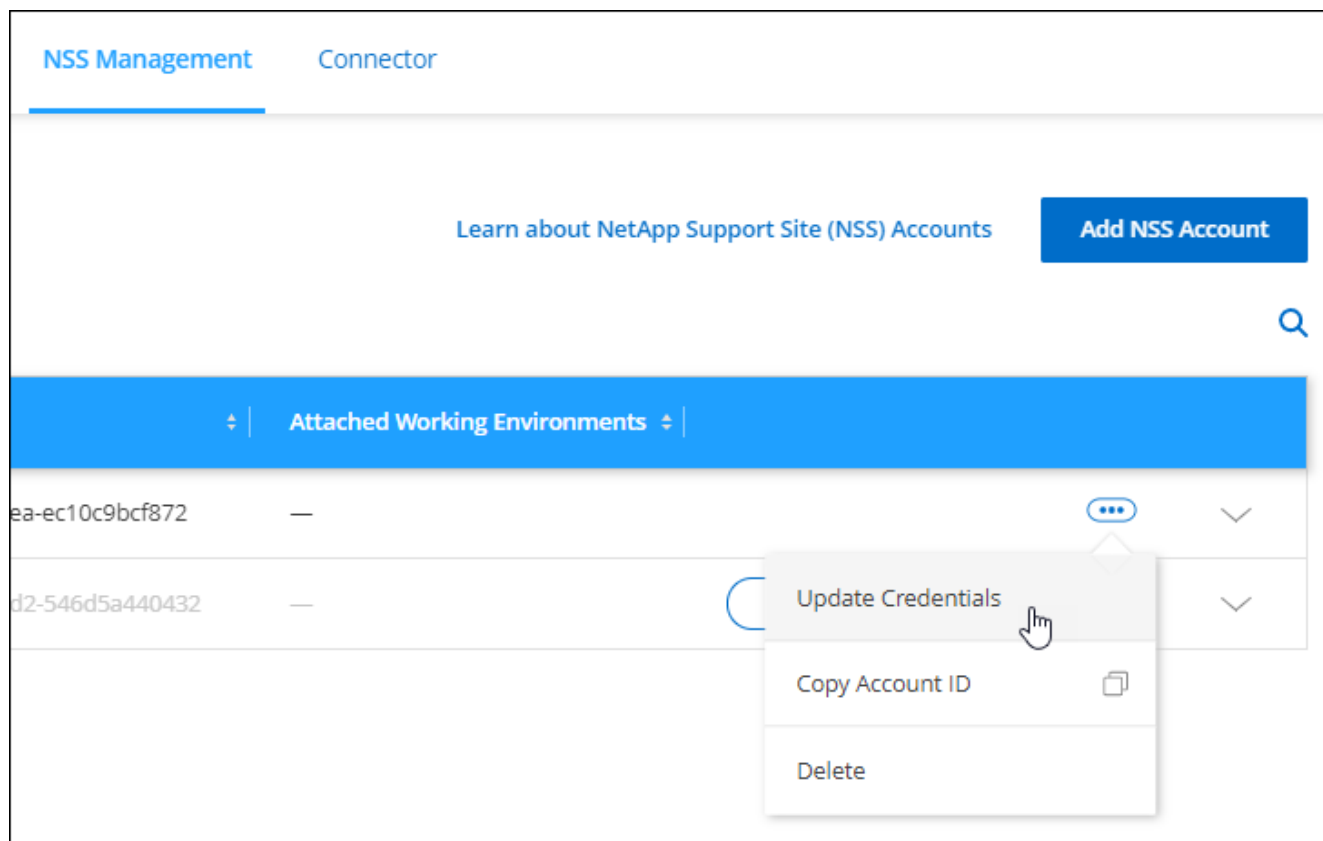
Vous devrez mettre à jour les informations d'identification de vos comptes NSS dans BlueXP lorsque l'un des cas suivants se produit :

- Vous modifiez les informations d'identification du compte

- Le jeton de renouvellement associé à votre compte expire au bout de 3 mois

## Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.
2. Cliquez sur **NSS Management**.
3. Pour le compte NSS que vous souhaitez mettre à jour, cliquez sur **...** Puis sélectionnez **mettre à jour les informations d'identification**.



4. Lorsque vous y êtes invité, cliquez sur **Continuer** pour être redirigé vers une page de connexion Microsoft.

NetApp utilise Microsoft Azure Active Directory comme fournisseur d'identités pour les services d'authentification spécifiques au support et aux licences.

5. Sur la page de connexion, indiquez l'adresse e-mail et le mot de passe que vous avez enregistrés sur le site de support NetApp pour réaliser le processus d'authentification.

## Associez un environnement de travail à un autre compte NSS

Si votre entreprise compte plusieurs comptes sur le site de support NetApp, vous pouvez modifier le compte associé à un système Cloud Volumes ONTAP.

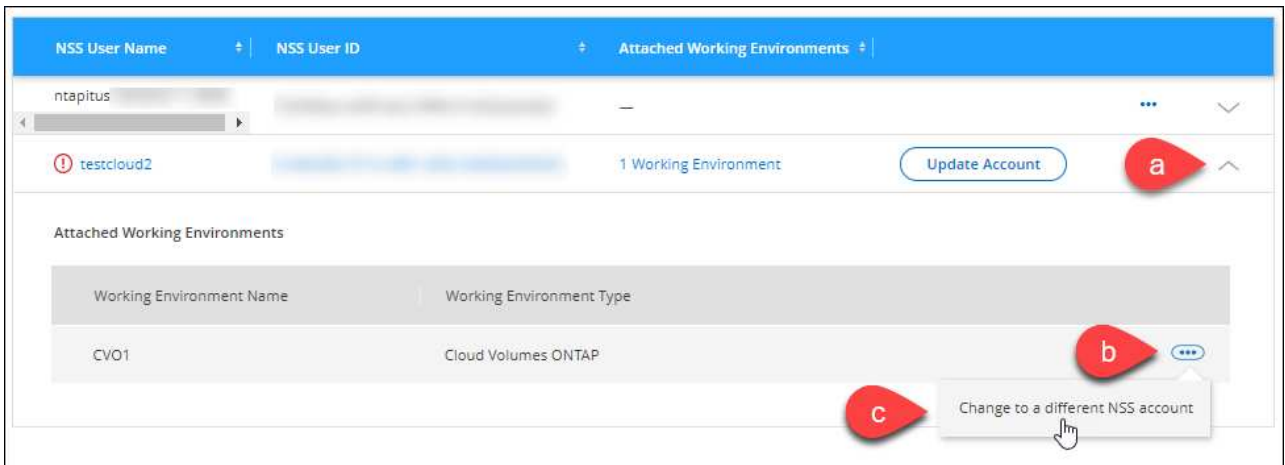
Cette fonctionnalité n'est prise en charge que avec les comptes NSS configurés pour utiliser Microsoft Azure AD adopté par NetApp pour la gestion des identités. Avant de pouvoir utiliser cette fonction, vous devez cliquer sur **Ajouter un compte NSS** ou **mettre à jour le compte**.

## Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



2. Cliquez sur **NSS Management**.
3. Pour modifier le compte NSS, procédez comme suit :
  - a. Développez la ligne du compte du site de support NetApp auquel l'environnement de travail est actuellement associé.
  - b. Pour l'environnement de travail pour lequel vous souhaitez modifier l'association, cliquez sur ...
  - c. Sélectionnez **changer pour un autre compte NSS**.



- d. Sélectionnez le compte, puis cliquez sur **Enregistrer**.

## Affichez l'adresse e-mail d'un compte NSS

Lorsque les comptes du site de support NetApp utilisent Microsoft Azure Active Directory pour les services d'authentification, le nom d'utilisateur NSS qui s'affiche dans BlueXP est généralement un identifiant généré par Azure AD. Par conséquent, il se peut que vous ne sachiez pas immédiatement l'adresse e-mail associée à ce compte. Mais BlueXP a une option pour vous montrer l'adresse e-mail associée.



Lorsque vous accédez à la page gestion NSS, BlueXP génère un jeton pour chaque compte de la table. Ce token inclut des informations sur l'adresse e-mail associée. Le jeton est alors supprimé lorsque vous quittez la page. Les informations ne sont jamais mises en cache, ce qui contribue à protéger votre vie privée.

### Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.
2. Cliquez sur **NSS Management**.
3. Pour le compte NSS que vous souhaitez mettre à jour, cliquez sur ... Puis sélectionnez **Afficher l'adresse électronique**.



BlueXP affiche le nom d'utilisateur du site de support NetApp ainsi que l'adresse e-mail associée. Vous pouvez utiliser le bouton Copier pour copier l'adresse e-mail.

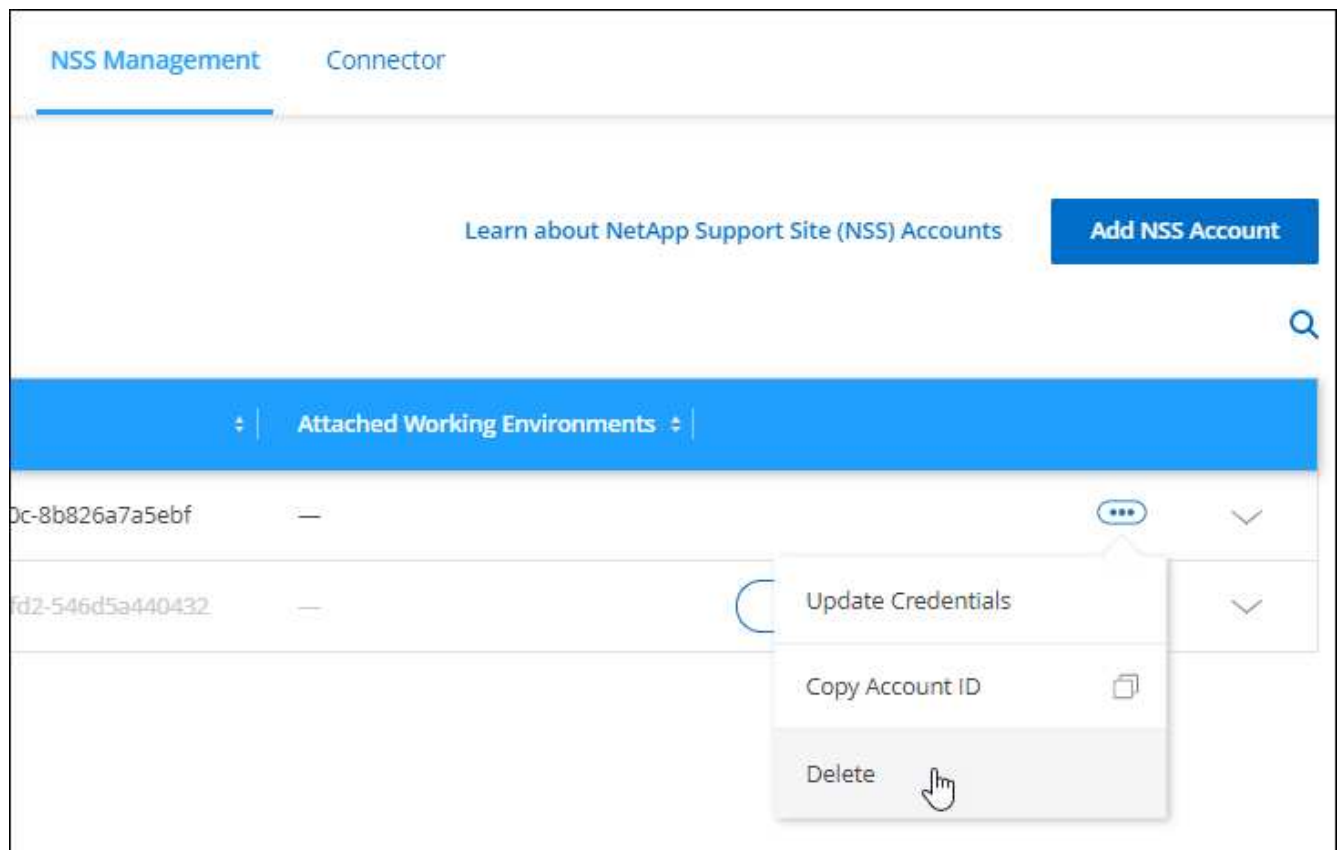
## Supprimer un compte NSS

Supprimez tous les comptes NSS que vous ne souhaitez plus utiliser avec BlueXP.

Notez que vous ne pouvez pas supprimer un compte actuellement associé à un environnement de travail Cloud Volumes ONTAP. Vous devez d'abord associer un environnement de travail à un autre compte NSS, Reliez ces environnements de travail à un autre compte NSS.

### Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.
2. Cliquez sur **NSS Management**.
3. Pour le compte NSS que vous souhaitez supprimer, cliquez sur **...** Puis sélectionnez **Supprimer**.



4. Cliquez sur **Supprimer** pour confirmer.

## Mes opportunités

Sur le Canvas, l'onglet **Mes opportunités** fournit un emplacement centralisé pour découvrir les ressources existantes que vous pouvez ajouter à BlueXP afin de garantir la cohérence des services de données et des opérations dans votre environnement multicloud hybride.

Actuellement, My Opportunities vous permet de découvrir les systèmes de fichiers FSX existants pour les systèmes de fichiers ONTAP dans votre compte AWS.

["Découvrez comment découvrir FSX pour ONTAP à l'aide de Mes opportunités"](#)

# Référence

## Autorisations

### Résumé des autorisations pour BlueXP

Pour utiliser les fonctionnalités et services de BlueXP, vous devez fournir des autorisations pour que BlueXP puisse effectuer des opérations dans votre environnement cloud. Utilisez les liens de cette page pour accéder rapidement aux autorisations dont vous avez besoin en fonction de votre objectif.

#### Autorisations AWS

Objectif	Description	Lien
Déploiement de connecteurs	L'utilisateur qui crée un connecteur depuis BlueXP a besoin d'autorisations spécifiques pour déployer l'instance dans AWS.	<a href="#">"Créez un connecteur dans AWS à partir de BlueXP"</a>
Fonctionnement du connecteur	Lorsque BlueXP lance le connecteur, il attache une stratégie à l'instance qui fournit les autorisations nécessaires pour gérer les ressources et les processus de votre compte AWS. Vous devez définir vous-même la stratégie si vous <a href="#">"Lancez un connecteur sur le Marketplace"</a> ou si vous <a href="#">"Ajoutez des identifiants AWS à un connecteur"</a> . Vous devez également vous assurer que la stratégie est à jour lorsque de nouvelles autorisations sont ajoutées dans les versions suivantes.	<a href="#">"Autorisations AWS pour le connecteur"</a>
Fonctionnement du Cloud Volumes ONTAP	Un rôle IAM doit être associé à chaque nœud Cloud Volumes ONTAP dans AWS. Il en va de même pour le médiateur HA. L'option par défaut est de permettre à BlueXP de créer les rôles IAM pour vous, mais vous pouvez utiliser votre propre.	<a href="#">"Découvrez comment configurer vous-même les rôles IAM"</a>

#### Autorisations Azure

Objectif	Description	Lien
Déploiement de connecteurs	Lorsque vous déployez un connecteur depuis BlueXP, vous devez utiliser un compte ou un service principal Azure disposant des autorisations pour déployer la machine virtuelle Connector dans Azure.	<a href="#">"Créez un connecteur dans Azure à partir de BlueXP"</a>

Objectif	Description	Lien
Fonctionnement du connecteur	<p>Lorsque BlueXP déploie la machine virtuelle Connector dans Azure, il crée un rôle personnalisé qui fournit les autorisations requises pour gérer les ressources et les processus au sein de cet abonnement Azure.</p> <p>Vous devez définir vous-même le rôle personnalisé si vous le souhaitez "<a href="#">Lancez un connecteur sur le Marketplace</a>" ou si vous "<a href="#">Ajoutez des identifiants Azure à un connecteur</a>".</p> <p>Vous devez également vous assurer que la stratégie est à jour lorsque de nouvelles autorisations sont ajoutées dans les versions suivantes.</p>	<a href="#">"Autorisations Azure pour le connecteur"</a>

## Autorisations Google Cloud

Objectif	Description	Lien
Déploiement de connecteurs	L'utilisateur Google Cloud qui déploie un connecteur depuis BlueXP a besoin d'autorisations spécifiques pour déployer le connecteur dans Google Cloud.	<a href="#">"Configurez les autorisations de déploiement du connecteur"</a>
Fonctionnement du connecteur	Le compte de service de l'instance de VM Connector doit disposer d'autorisations spécifiques pour les opérations quotidiennes. Vous devez associer le compte de service au connecteur lorsque vous le déployez depuis BlueXP. Vous devez également vous assurer que la stratégie est à jour lorsque de nouvelles autorisations sont ajoutées dans les versions suivantes.	<a href="#">"Configurez un compte de service pour le connecteur"</a>

## Autorisations AWS pour le connecteur

Lorsque BlueXP lance l'instance Connector dans AWS, il attache une règle à l'instance qui fournit au connecteur des autorisations pour gérer les ressources et les processus au sein de ce compte AWS. Le connecteur utilise les autorisations pour effectuer des appels d'API vers plusieurs services AWS, notamment EC2, S3, CloudFormation, IAM, Le service de gestion des clés (KMS), et plus encore.

### Règles IAM

Les règles IAM disponibles ci-dessous fournissent les autorisations nécessaires à un connecteur pour gérer les ressources et les processus au sein de votre environnement de cloud public, en fonction de votre région AWS.

Si vous créez un connecteur dans une région AWS standard directement depuis BlueXP, BlueXP applique automatiquement des stratégies au connecteur. Vous n'avez rien à faire dans ce cas.

Si vous déployez le connecteur depuis AWS Marketplace ou si vous installez manuellement le connecteur sur un hôte Linux, vous devrez définir vous-même les règles.

Vous devez également vous assurer que les règles sont à jour lorsque de nouvelles autorisations sont ajoutées dans les versions suivantes.

Sélectionnez votre région pour afficher les stratégies requises :

## Régions standard

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.

La première politique fournit des autorisations pour les services suivants :

- La sauvegarde dans le cloud
- Sens des données cloud
- Tiering dans le cloud
- Cloud Volumes ONTAP
- FSX pour ONTAP
- Découverte des compartiments S3

La deuxième politique fournit des autorisations pour les services suivants :

- Balisage AppTemplate
- Cache global de fichiers
- Kubernetes

## Politique no 1

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "cvoServicePolicy",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolumeAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:CreatePlacementGroup",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:AssignPrivateIpAddresses",
        "ec2:CreateRoute",
        "ec2:DescribeVpcs",
```



```
"ec2:ReplaceRoute",
"ec2:UnassignPrivateIpAddresses",
"ec2:DeleteSecurityGroup",
"ec2:DeleteNetworkInterface",
"ec2:DeleteSnapshot",
"ec2:DeleteTags",
"ec2:DeleteRoute",
"ec2:DeletePlacementGroup",
"ec2:DescribePlacementGroups",
"cloudformation:CreateStack",
"cloudformation:DescribeStacks",
"cloudformation:DescribeStackEvents",
"cloudformation:ValidateTemplate",
"cloudformation>DeleteStack",
"iam:PassRole",
"iam:CreateRole",
"iam:PutRolePolicy",
"iam:CreateInstanceProfile",
"iam:AddRoleToInstanceProfile",
"iam:RemoveRoleFromInstanceProfile",
"iam:ListInstanceProfiles",
"iam>DeleteRole",
"iam>DeleteRolePolicy",
"iam>DeleteInstanceProfile",
"iam:GetRolePolicy",
"iam:GetRole",
"sts:DecodeAuthorizationMessage",
"sts:AssumeRole",
"s3:GetBucketTagging",
"s3:GetBucketLocation",
"s3:ListBucket",
"s3>CreateBucket",
"s3:GetLifecycleConfiguration",
"s3:ListBucketVersions",
"s3:GetBucketPolicyStatus",
"s3:GetBucketPublicAccessBlock",
"s3:GetBucketPolicy",
"s3:GetBucketAcl",
"s3:PutObjectTagging",
"s3:GetObjectTagging",
"s3>DeleteObject",
"s3>DeleteObjectVersion",
"s3:PutObject",
"s3:ListAllMyBuckets",
"s3:GetObject",
"s3:GetEncryptionConfiguration",
```

```

        "kms:List*",
        "kms:ReEncrypt*",
        "kms:Describe*",
        "kms:CreateGrant",
        "ce:GetReservationUtilization",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsage",
        "ce:GetTags",
        "fsx:Describe*",
        "fsx:List*"
    ],
    "Resource": "*"
},
{
    "Sid": "backupPolicy",
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "kms:List*",
        "kms:Describe*",
        "ec2:describeVpcEndpoints",
        "kms:ListAliases",
        "athena:StartQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryExecution",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:CreateDatabase",
        "glue:GetPartitions",
    ]
}

```

```

        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition"
    ],
    "Resource": "*"
},
{
    "Sid": "backupS3Policy",
    "Effect": "Allow",
    "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketAcl",
        "s3:PutBucketPublicAccessBlock",
        "s3:GetObject",
        "s3:PutEncryptionConfiguration",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:DeleteBucket",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectRetention",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketVersioning",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketVersioning",
        "s3:BypassGovernanceRetention",
        "s3:PutBucketPolicy",
        "s3:PutBucketOwnershipControls"
    ],

```

```

        "Resource": [
            "arn:aws:s3:::netapp-backup-*"
        ]
    },
    {
        "Sid": "fabricPoolS3Policy",
        "Effect": "Allow",
        "Action": [
            "s3:CreateBucket",
            "s3:GetLifecycleConfiguration",
            "s3:PutLifecycleConfiguration",
            "s3:PutBucketTagging",
            "s3:ListBucketVersions",
            "s3:GetBucketPolicyStatus",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetBucketAcl",
            "s3:GetBucketPolicy",
            "s3:PutBucketPublicAccessBlock",
            "s3>DeleteBucket"
        ],
        "Resource": [
            "arn:aws:s3:::fabric-pool*"
        ]
    },
    {
        "Sid": "fabricPoolPolicy",
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeRegions"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec2:TerminateInstances"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/netapp-adc-manager": "*"
            }
        },
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ]
    }
}

```

```

    ],
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume",
        "ec2:StopInstances",
        "ec2>DeleteVolume"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/WorkingEnvironment": "*"
        }
      },
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": [
        "arn:aws:ec2:*:*:volume/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2>DeleteVolume"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/WorkingEnvironment": "*"
        }
      },
      "Resource": [
        "arn:aws:ec2:*:*:volume/*"
      ]
    }
  ]
}

```

```
}
```

## Politique no 2

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "K8sServicePolicy",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeRegions",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "iam:GetInstanceProfile"
      ],
      "Resource": "*"
    },
    {
      "Sid": "GFCservicePolicy",
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks",
        "cloudwatch:GetMetricStatistics",
        "cloudformation:ListStacks"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/GFCInstance": "*"
        }
      },
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ]
    },
    {
```

```
"Sid": "tagServicePolicy",
"Effect": "Allow",
"Action": [
    "ec2:CreateTags",
    "ec2>DeleteTags",
    "ec2:DescribeTags",
    "tag:getResources",
    "tag:getTagKeys",
    "tag:getTagValues",
    "tag:TagResources",
    "tag:UntagResources"
],
"Resource": "*"
}
]
```

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListInstanceProfiles",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "ec2:ModifyVolumeAttribute",
        "sts:DecodeAuthorizationMessage",
        "ec2:DescribeImages",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInstances",
        "iam:PassRole",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:DeleteVolume",
        "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:CreateSnapshot",
        "ec2:DeleteSnapshot",

```



```

        "ec2:DescribeSnapshots",
        "ec2:StopInstances",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2>DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:CreateBucket",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "kms:List*",
        "kms:ReEncrypt*",
        "kms:Describe*",
        "kms:CreateGrant",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ce:GetReservationUtilization",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsage",
        "ce:GetTags",
        "ec2:CreatePlacementGroup",
        "ec2>DeletePlacementGroup"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3>DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",

```

```

        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
    ],
    "Resource": [
        "arn:aws-us-gov:s3:::fabric-pool*"
    ]
},
{
    "Sid": "backupPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
    ],
    "Resource": [
        "arn:aws-us-gov:s3:::netapp-backup-*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Condition": {
        "StringLike": {

```

```

        "ec2:ResourceTag/WorkingEnvironment": "*"
    },
    "Resource": [
        "arn:aws-us-gov:ec2:*:*:instance/*"
    ],
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws-us-gov:ec2:*:*:volume/*"
        ]
    }
]
}

```

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceStatus",
      "ec2:RunInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:DescribeRouteTables",
      "ec2:DescribeImages",
      "ec2:CreateTags",
      "ec2:CreateVolume",
      "ec2:DescribeVolumes",
      "ec2:ModifyVolumeAttribute",
      "ec2>DeleteVolume",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteSecurityGroup",
      "ec2:DescribeSecurityGroups",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2>DeleteNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeDhcpOptions",
      "ec2:CreateSnapshot",
      "ec2>DeleteSnapshot",
      "ec2:DescribeSnapshots",
      "ec2:GetConsoleOutput",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeRegions",
      "ec2>DeleteTags",
      "ec2:DescribeTags",
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackEvents",
      "cloudformation:ValidateTemplate",
      "iam:PassRole",

```

```

        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "kms:List*",
        "kms:Describe*",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup",
        "iam:ListInstanceProfiles"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
    ],
    "Resource": [
        "arn:aws-iso:s3:::fabric-pool*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",

```

```

        "ec2:DetachVolume"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/WorkingEnvironment": "*"
        }
    },
    "Resource": [
        "arn:aws-iso:ec2:*:*:instance/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": [
        "arn:aws-iso:ec2:*:*:volume/*"
    ]
}
]
}

```

## Utilisation des autorisations AWS

Les sections suivantes décrivent la manière dont les autorisations sont utilisées pour chaque service cloud NetApp. Ces informations peuvent être utiles si vos stratégies d'entreprise exigent que les autorisations ne sont fournies que si nécessaire.

### Balises AppTemplate

Lorsque vous utilisez le service de balisage AppTemplate, le connecteur effectue les requêtes API suivantes pour gérer les balises sur les ressources AWS :

- ec2:CreateTags
- ec2>DeleteTags
- ec2:Etiquettes descriptives
- Tag:getResources
- Tag:getTagKeys
- Tag:getTagValues
- Tag:TagResources
- Tag:UntagResources

## La sauvegarde dans le cloud

Il crée les demandes d'API suivantes pour déployer l'instance de restauration pour Cloud Backup :

- ec2:déclarations de début
- ec2:StopInstances
- ec2:descriptifs
- ec2:DécritesInstanceStatus
- ec2:RunInstances
- ec2:désactivation des instructions
- ec2:DescribeInstanceAttribute
- ec2:descriptifs
- ec2:CreateTags
- ec2 : CreateVolume
- ec2:CreateSecurityGroup
- ec2:DescribeSubnets
- ec2 : descriptif
- ec2:régions descriptives
- Cloudformation:CreateStack
- Cloudformation>DeleteStack
- Cloudformation:DescribeStacks

Ce connecteur effectue les requêtes API suivantes pour gérer les sauvegardes dans Amazon S3 :

- s3:GetBucketLocation
- s3:ListAllMyBuckets
- s3:ListBucket
- s3:CreateBucket
- s3:GetLifecycleConfiguration
- s3:PutLifecycleConfiguration
- s3:PutBucketTagging
- s3:ListBucketVersions
- s3:GetBucketAcl
- s3:PutBucketPublicAccessBlock
- Km:liste\*
- Km:décrire\*
- s3:GetObject
- ec2:descriptionVpcEndpoints
- Kms:ListAliases
- s3:PutEncryptionConfiguration

Lorsque vous utilisez la méthode de recherche et de restauration pour restaurer des volumes et des fichiers, le connecteur effectue les demandes d'API suivantes :

- s3:CreateBucket
- s3:DeleteObject
- s3:DeleteObjectVersion
- s3:GetBucketAcl
- s3:ListBucket
- s3:ListBucketVersions
- s3:ListBucketMultipartUploads
- s3:PutObject
- s3:PutBucketAcl
- s3:PutLifecycleConfiguration
- s3:PutBucketPublicAccessBlock
- s3:AbortMultipartUpload
- s3:ListMultipartUploadParts
- athena:StartQueryExecution
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- Glue:CreateDatabase
- Glue:CreateTable
- Glue:BatchDeletePartition

Lorsque vous utilisez DataLock et protection contre les attaques par ransomware pour vos sauvegardes de volumes, le connecteur effectue les requêtes API suivantes :

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:DeleteObject
- s3:DeleteObjectTagging
- s3:GetObjectRetention
- s3:DeleteObjectVersionTagging
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:ListBucketByTags



- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBuckeVersions
- s3:ListBucket
- s3:PutBuckeTagging
- s3:GetObjectTagging
- s3:PutBuckeVersioning
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:BypassGovernanceRetention
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

Si vous utilisez un autre compte AWS pour vos sauvegardes Cloud Volumes ONTAP que ce que vous utilisez pour les volumes source, ce connecteur effectue les requêtes d'API suivantes :

- s3:PutBuckePolicy
- s3 : commandes PutBuckeOwnershipControls

#### **Sens des données cloud**

Il crée l'instance Cloud Data Sense suivante :

- ec2:descriptifs
- ec2:DécritesInstanceStatus
- ec2:RunInstances
- ec2:désactivation des instructions
- ec2:CreateTags
- ec2 : CreateVolume
- ec2 : AttachVolume
- ec2:CreateSecurityGroup
- ec2>DeleteSecurityGroup
- ec2:descriptifs des groupes de sécurité
- ec2:CreateNetworkinterface
- ec2:DescribeNetworkinterfaces
- ec2>DeleteNetworkinterface
- ec2:DescribeSubnets
- ec2 : descriptif
- ec2 : CreateSnapshot

- ec2:régions descriptives
- Cloudformation:CreateStack
- Cloudformation>DeleteStack
- Cloudformation:DescribeStacks
- Cloudformation:DescribeStackEvents
- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DetachIamInstanceProfileAssociations

Lors de l'utilisation de Cloud Data Sense, il effectue les demandes d'API suivantes pour analyser les compartiments S3 :

- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DetachIamInstanceProfileAssociations
- s3:GetBucketTagging
- s3:GetBucketLocation
- s3:ListAllMyBuckets
- s3:ListBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketPolicy
- s3:GetBucketAcl
- s3:GetObject
- iam:GetRole
- s3:DeleteObject
- s3:DeleteObjectVersion
- s3:PutObject
- sts : AssumeRole

### Tiering dans le cloud

Ce connecteur effectue les demandes d'API suivantes pour transférer les données vers Amazon S3 lorsque vous utilisez NetApp Cloud Tiering.

Action	Utilisé pour la configuration ?	Utilisé pour les opérations quotidiennes ?
s3:CreateBucket	Oui.	Non
s3:PutLifecycleConfiguration	Oui.	Non
s3:GetLifecycleConfiguration	Oui.	Oui.
ec2:régions descriptives	Oui.	Oui.

## Cloud Volumes ONTAP

Il effectue les requêtes d'API suivantes pour déployer et gérer Cloud Volumes ONTAP dans AWS.

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créer et gérer des rôles IAM et des profils d'instance pour les instances Cloud Volumes ONTAP	iam:ListenceProfiles	Oui.	Oui.	Non
	iam:CreateRole	Oui.	Non	Non
	iam>DeleteRole	Non	Oui.	Oui.
	iam:PutRolePolicy	Oui.	Non	Non
	iam:CreateInstanceProfile	Oui.	Non	Non
	iam>DeleteRolePolicy	Non	Oui.	Oui.
	iam:AddRoleToInstanceProfile	Oui.	Non	Non
	iam:RemoveRoleFromInstanceProfile	Non	Oui.	Oui.
	iam>DeleteInstanceProfile	Non	Oui.	Oui.
	iam:PassRole	Oui.	Non	Non
	ec2:AssociateIamInstanceProfile	Oui.	Oui.	Non
	ec2:DetachIamInstanceProfileAssociations	Oui.	Oui.	Non
	ec2:DisassociateIamInstanceProfile	Non	Oui.	Non
Décoder les messages d'état d'autorisation	sts:DecodeAuthorizationMessage	Oui.	Oui.	Non
Décrivez les images spécifiées (amis) disponibles pour le compte	ec2:describeImages	Oui.	Oui.	Non
Décrire les tableaux de routage d'un VPC (requis pour les paires haute disponibilité uniquement)	ec2:DescribeRouteTables	Oui.	Non	Non

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Arrêtez, démarrez et surveillez les instances	ec2:déclarations de début	Oui.	Oui.	Non
	ec2:StopInstances	Oui.	Oui.	Non
	ec2:descriptifs	Oui.	Oui.	Non
	ec2:DécritesInstance Status	Oui.	Oui.	Non
	ec2:RunInstances	Oui.	Non	Non
	ec2:désactivation des instructions	Non	Non	Oui.
	ec2:Modimodificace Attribute	Non	Oui.	Non
Vérifiez que la mise en réseau améliorée est activée pour les types d'instances pris en charge	ec2:DescribeInstanceAttribute	Non	Oui.	Non
Marquez les ressources avec les balises « WorkingEnvironment » et « WorkingEnvironment » qui sont utilisées pour la maintenance et l'allocation des coûts	ec2:CreateTags	Oui.	Oui.	Non
Gérez des volumes EBS que Cloud Volumes ONTAP utilise comme stockage interne	ec2 : CreateVolume	Oui.	Oui.	Non
	ec2:DescribeVolumes	Oui.	Oui.	Oui.
	ec2:ModifyVolumeAttribute	Non	Oui.	Oui.
	ec2 : AttachVolume	Oui.	Oui.	Non
	ec2:DeleteVolume	Non	Oui.	Oui.
	ec2 : DetachVolume	Non	Oui.	Oui.

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Création et gestion des groupes de sécurité pour Cloud Volumes ONTAP	ec2:CreateSecurityGroup	Oui.	Non	Non
	ec2:DeleteSecurityGroup	Non	Oui.	Oui.
	ec2:descriptifs des groupes de sécurité	Oui.	Oui.	Oui.
	ec2 : RevokeSecurityGroupEgress	Oui.	Non	Non
	ec2:AuthoreSecurityGroupEgress	Oui.	Non	Non
	ec2:AuthoreSecurityGroupIngress	Oui.	Non	Non
	ec2 : RevokeSecurityGroupIngress	Oui.	Oui.	Non
Créez et gérez des interfaces réseau pour Cloud Volumes ONTAP dans le sous-réseau cible	ec2:CreateNetworkInterface	Oui.	Non	Non
	ec2:DescribeNetworkInterfaces	Oui.	Oui.	Non
	ec2:DeleteNetworkInterface	Non	Oui.	Oui.
	ec2:ModilyNetworkInterfaceAttribute	Non	Oui.	Non
Obtenir la liste des sous-réseaux et groupes de sécurité de destination	ec2:DescribeSubnets	Oui.	Oui.	Non
	ec2 : descriptif	Oui.	Oui.	Non
Obtenir les serveurs DNS et le nom de domaine par défaut pour les instances Cloud Volumes ONTAP	ec2:DescribeDhcpOptions	Oui.	Non	Non
Prise de snapshots de volumes EBS pour Cloud Volumes ONTAP	ec2 : CreateSnapshot	Oui.	Oui.	Non
	ec2:DeleteSnapshot	Non	Oui.	Oui.
	ec2:snapshots descriptifs	Non	Oui.	Non

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Capturez la console Cloud Volumes ONTAP, qui est attachée aux messages AutoSupport	ec2:GetConsoleOutput	Oui.	Oui.	Non
Consultez la liste des paires de clés disponibles	ec2:Décrivez des Keypairs	Oui.	Non	Non
Consultez la liste des régions AWS disponibles	ec2:régions descriptives	Oui.	Oui.	Non
Gérez les balises des ressources associées aux instances Cloud Volumes ONTAP	ec2:DeleteTags	Non	Oui.	Oui.
	ec2:Etiquettes descriptives	Non	Oui.	Non
Créez et gérez des piles pour les modèles AWS CloudFormation	Cloudformation:CreateStack	Oui.	Non	Non
	Cloudformation>DeleteStack	Oui.	Non	Non
	Cloudformation:DescribeStacks	Oui.	Oui.	Non
	Cloudformation:DescribeStackEvents	Oui.	Non	Non
	Déformation:Validée Template	Oui.	Non	Non

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créez et gérez un compartiment S3 utilisé par un système Cloud Volumes ONTAP comme Tier de capacité pour le Tiering des données	s3:CreateBucket	Oui.	Oui.	Non
	s3>DeleteBucket	Non	Oui.	Oui.
	s3:GetLifecyclConfiguration	Non	Oui.	Non
	s3:PutLifecyclConfiguration	Non	Oui.	Non
	s3:PutBuckeTagging	Non	Oui.	Non
	s3:ListBuckeVersions	Non	Oui.	Non
	s3:GetBucketPolicyStatus	Non	Oui.	Non
	s3:GetBuckePublicAccessBlock	Non	Oui.	Non
	s3:GetBucketAcl	Non	Oui.	Non
	s3:GetBucketPolicy	Non	Oui.	Non
	s3:PutBuckePublicAccessBlock	Non	Oui.	Non
	s3:GetBucketTagging	Non	Oui.	Non
	s3:GetBucketLocation	Non	Oui.	Non
	s3:ListAllMyseaux	Non	Non	Non
	s3:ListBucket	Non	Oui.	Non
Chiffrement des données Cloud Volumes ONTAP possible à l'aide du service AWS Key Management Service (KMS)	Km:liste*	Oui.	Oui.	Non
	Kms:Recrypter*	Oui.	Non	Non
	Km:décrire*	Oui.	Oui.	Non
	Kms>CreateGrant	Oui.	Oui.	Non
Obtenez des données de coût AWS pour Cloud Volumes ONTAP	ce:GetReservationUtilization	Non	Oui.	Non
	ce:GetDimensionTMValues	Non	Oui.	Non
	ce : GetCostAndUtiusage	Non	Oui.	Non
	ce:GetTags	Non	Oui.	Non

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créez et gérez un groupe de placement AWS réparti sur deux nœuds HA et le médiateur dans une seule zone de disponibilité AWS	ec2:CreatePlacementGroup	Oui.	Non	Non
	ec2:DeletePlacementGroup	Non	Oui.	Oui.
Créer des rapports	fsx:describe*	Non	Oui.	Non
	fsx:list*	Non	Oui.	Non
Créez et gérez des agrégats prenant en charge la fonctionnalité Amazon EBS Elastic volumes	ec2:DescribeVolumesModifications	Non	Oui.	Non
	ec2:ModifyVolume	Non	Oui.	Non

### Cache global de fichiers

Le connecteur effectue les demandes d'API suivantes pour déployer des instances de cache de fichier global pendant le déploiement :

- Cloudformation:DescribeStacks
- cloudwatch:GetMetricStatistics
- Cloudformation:ListStacks

### FSX pour ONTAP

Le connecteur effectue les requêtes API suivantes pour gérer FSX pour ONTAP :

- ec2:describeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInstanceAttribute
- ec2:DescribeRouteTables
- ec2:describeSubnets
- ec2:CreateTags
- ec2:DescribeVolumes
- ec2:describeVolumes des groupes de sécurité
- ec2:DescribeNetworkInterfaces
- ec2:DescribeSubnets
- ec2 : describeVpc
- ec2:DescribeDhcpOptions



- ec2:snapshots descriptifs
- ec2:Décrivez des Keypairs
- ec2:régions descriptives
- ec2:Etiquettes descriptives
- ec2:DécriteslamInstanceProfileassociations
- ec2:DescribeReserveInstancesOfferings
- ec2:descriptionVpcEndpoints
- ec2 : descriptif
- ec2:DescribeVolumesModifications
- ec2:descriptifs des groupes
- Km:liste\*
- Km:décrire\*
- Kms>CreateGrant
- Kms:ListAliases
- fsx:décrire\*
- fsx:liste\*

### **Kubernetes**

Le connecteur effectue les requêtes API suivantes pour détecter et gérer les clusters Amazon EKS :

- ec2:régions descriptives
- eks:ListClusters
- eks:DescribeCluster
- iam:GetInstanceProfile

### **Découverte des compartiments S3**

Il effectue la demande d'API suivante pour détecter les compartiments Amazon S3 :

s3:GetEncryptionConfiguration

## **Autorisations Azure pour le connecteur**

Lorsque BlueXP lance la machine virtuelle Connector dans Azure, il attache un rôle personnalisé à la machine virtuelle qui fournit au connecteur les autorisations nécessaires pour gérer les ressources et les processus au sein de cet abonnement Azure. Le connecteur utilise les autorisations pour effectuer des appels API vers plusieurs services Azure.

### **Autorisations de rôles personnalisées**

Le rôle personnalisé illustré ci-dessous fournit les autorisations dont un connecteur a besoin pour gérer les ressources et les processus de votre réseau Azure.

Lorsque vous créez un connecteur directement à partir de BlueXP, BlueXP applique automatiquement ce rôle personnalisé au connecteur.

Si vous déployez le connecteur à partir d’Azure Marketplace ou si vous installez manuellement le connecteur sur un hôte Linux, vous devrez définir vous-même le rôle personnalisé.

Vous devez également vous assurer que le rôle est à jour lorsque de nouvelles autorisations sont ajoutées dans les versions suivantes.

```
{
  "Name": "BlueXP Operator",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/locations/vmSizes/read",
    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/powerOff/action",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Compute/virtualMachines/deallocate/action",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/vmSizes/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/images/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/virtualNetworks/read",

    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Network/virtualNetworks/subnets/write",

    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",

    "Microsoft.Network/virtualNetworks/virtualMachines/read",

    "Microsoft.Network/virtualNetworks/subnets/join/action",
```

```
"Microsoft.Resources/deployments/operations/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/write",
"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.Storage/checknameavailability/read",
    "Microsoft.Storage/operations/read",
    "Microsoft.Storage/storageAccounts/listkeys/action",
    "Microsoft.Storage/storageAccounts/read",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",

"Microsoft.Storage/storageAccounts/blobServices/containers/write",
    "Microsoft.Storage/usages/read",
    "Microsoft.Compute/snapshots/write",
    "Microsoft.Compute/snapshots/read",
    "Microsoft.Compute/availabilitySets/write",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Compute/disks/beginGetAccess/action",

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

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
    "Microsoft.Network/loadBalancers/read",
    "Microsoft.Network/loadBalancers/write",
    "Microsoft.Network/loadBalancers/delete",

"Microsoft.Network/loadBalancers/backendAddressPools/read",

"Microsoft.Network/loadBalancers/loadBalancingRules/read",
    "Microsoft.Network/loadBalancers/probes/read",
    "Microsoft.Network/loadBalancers/probes/join/action",
    "Microsoft.Authorization/locks/*",
```

```
"Microsoft.Network/routeTables/join/action",
"Microsoft.NetApp/netAppAccounts/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
"Microsoft.Network/privateEndpoints/write",

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action",

"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",

"Microsoft.Storage/storageAccounts/managementPolicies/read",

"Microsoft.Storage/storageAccounts/managementPolicies/write",
"Microsoft.Network/privateEndpoints/read",
"Microsoft.Network/privateDnsZones/write",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
"Microsoft.Network/virtualNetworks/join/action",
"Microsoft.Network/privateDnsZones/A/write",
"Microsoft.Network/privateDnsZones/read",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",

"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
"Microsoft.Compute/diskEncryptionSets/read",
"Microsoft.Compute/snapshots/delete",
"Microsoft.Network/privateEndpoints/delete",
"Microsoft.Compute/availabilitySets/delete",
"Microsoft.KeyVault/vaults/read",
"Microsoft.KeyVault/vaults/accessPolicies/write",
"Microsoft.Compute/diskEncryptionSets/write",
"Microsoft.KeyVault/vaults/deploy/action",
```

```

        "Microsoft.Compute/diskEncryptionSets/delete",
        "Microsoft.Resources/tags/read",
        "Microsoft.Resources/tags/write",
        "Microsoft.Resources/tags/delete",
        "Microsoft.Network/applicationSecurityGroups/write",
        "Microsoft.Network/applicationSecurityGroups/read",

        "Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",

        "Microsoft.Network/networkSecurityGroups/securityRules/write",
        "Microsoft.Network/applicationSecurityGroups/delete",

        "Microsoft.Network/networkSecurityGroups/securityRules/delete",

        "Microsoft.ContainerService/managedClusters/listClusterUserCredential/action",

        "Microsoft.ContainerService/managedClusters/read",
        "Microsoft.Synapse/workspaces/write",
        "Microsoft.Synapse/workspaces/read",
        "Microsoft.Synapse/workspaces/delete",
        "Microsoft.Synapse/register/action",
        "Microsoft.Synapse/checkNameAvailability/action",
        "Microsoft.Synapse/workspaces/operationStatuses/read",
        "Microsoft.Synapse/workspaces/firewallRules/read",

        "Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
        "Microsoft.Synapse/workspaces/operationResults/read",
        "Microsoft.Network/publicIPAddresses/delete",

        "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "BlueXP Permissions",
    "IsCustom": "true"
}

```

## Utilisation des autorisations Azure

Les sections suivantes décrivent la manière dont les autorisations sont utilisées pour chaque service cloud NetApp. Ces informations peuvent être utiles si vos stratégies d'entreprise exigent que les autorisations ne sont fournies que si nécessaire.

### Balises AppTemplate

Le connecteur effectue les requêtes API suivantes pour gérer les balises sur les ressources Azure lorsque vous utilisez le service de balisage AppTemplate :

- Microsoft.Ressources/ressources/lecture
- Microsoft.Ressources/abonnements/résultats d'opération/lecture
- Microsoft.Ressources/abonnements/resourceGroups/read
- Microsoft.Ressources/abonnements/groupes de ressources/ressources/lecture
- Microsoft.Ressources/balises/lecture
- Microsoft.Ressources/balises/écrire

### **Azure NetApp Files**

Il effectue les requêtes d'API suivantes pour gérer les environnements de travail Azure NetApp Files :

- Microsoft.NetApp/netAppAccounts/read
- Microsoft.NetApp/netAppAccounts/capacityPools/read
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete

### **La sauvegarde dans le cloud**

Il effectue les demandes d'API suivantes pour les opérations de sauvegarde et de restauration :

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.KeyVault/coffres-forts/lecture
- Microsoft.KeyVault/coffres-forts/Access Policies/write
- Microsoft.Network/networkInterfaces/read
- Microsoft.Ressources/abonnements/emplacements/lecture
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- Microsoft.Ressources/abonnements/resourceGroups/read
- Microsoft.Ressources/abonnements/groupes de ressources/ressources/lecture
- Microsoft.Ressources/abonnements/resourceGroups/write
- Microsoft.autorisation/verrous/\*
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/privateEndpoints/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/write

- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Network/privateDnsZones/A/write
- Microsoft.Network/privateDnsZones/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/read
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Ressources/déploiements/suppression
- Microsoft.Network/publicIPAddresses/delete
- Microsoft.Storage/storageAccounts/blobServices/containers/write
- Microsoft.ManagedIdentity/userAssignedIdentities/attributable/action

Le connecteur effectue les demandes d'API suivantes lorsque vous utilisez la fonction de recherche et de restauration :

- Microsoft.Synapse/espaces de travail/écriture
- Microsoft.Synapse/espaces de travail/lecture
- Microsoft.Synapse/espaces de travail/supprimer
- Microsoft.Synapse/registre/action
- Microsoft.Synapse/checkNameAvailability/action
- Microsoft.Synapse/espaces de travail/opérationnalStatenses/lecture
- Microsoft.Synapse/espaces de travail/firewallRules/read
- Microsoft.Synapse/espaces de travail/replace AllIpFirewallRules/action
- Microsoft.Synapse/espaces de travail/opérationnalizResults/read

#### Sens des données cloud

Lorsque vous utilisez Cloud Data Sense, il effectue les requêtes d'API suivantes.

Action	Utilisé pour la configuration ?	Utilisé pour les opérations quotidiennes ?
Microsoft.Compute/locations/operations/read	Oui.	Oui.
Microsoft.Compute/locations/vmSizes/read	Oui.	Oui.
Microsoft.Compute/operations/read	Oui.	Oui.
Microsoft.Compute/virtualMachines/instanceView/read	Oui.	Oui.
Microsoft.Compute/virtualMachines/powerOff/action	Oui.	Non

Action	Utilisé pour la configuration ?	Utilisé pour les opérations quotidiennes ?
Microsoft.Compute/virtualMachines/read	Oui.	Oui.
Microsoft.Compute/virtualMachines/restart/action	Oui.	Non
Microsoft.Compute/virtualMachines/start/action	Oui.	Non
Microsoft.Compute/virtualMachines/vmSizes/read	Non	Oui.
Microsoft.Compute/virtualMachines/write	Oui.	Non
Microsoft.Compute/images/read	Oui.	Oui.
Microsoft.Compute/disks/delete	Oui.	Non
Microsoft.Compute/disks/read	Oui.	Oui.
Microsoft.Compute/disks/write	Oui.	Non
Microsoft.Storage/checkkamedisponibilité/read	Oui.	Oui.
Microsoft.stockage/opérations/lecture	Oui.	Oui.
Microsoft.Storage/storageAccounts/listkeys/action	Oui.	Non
Microsoft.Storage/storageAccounts/read	Oui.	Oui.
Microsoft.Storage/storageAccounts/write	Oui.	Non
Microsoft.Storage/storageAccounts/delete	Non	Oui.
Microsoft.Storage/storageAccounts/blobServices/containers/read	Oui.	Oui.
Microsoft.Network/networkInterfaces/read	Oui.	Oui.
Microsoft.Network/networkInterfaces/write	Oui.	Non
Microsoft.Network/networkInterfaces/join/action	Oui.	Non
Microsoft.Network/networkSecurityGroups/read	Oui.	Oui.
Microsoft.Network/networkSecurityGroups/write	Oui.	Non



Action	Utilisé pour la configuration ?	Utilisé pour les opérations quotidiennes ?
Microsoft.Ressources/abonnements/emplacements/lecture	Oui.	Oui.
Microsoft.Network/locations/operationResults/read	Oui.	Oui.
Microsoft.Network/locations/operations/read	Oui.	Oui.
Microsoft.Network/virtualNetworks/read	Oui.	Oui.
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Oui.	Oui.
Microsoft.Network/virtualNetworks/subnets/read	Oui.	Oui.
Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Oui.	Oui.
Microsoft.Network/virtualNetworks/virtualMachines/read	Oui.	Oui.
Microsoft.Network/virtualNetworks/subnets/join/action	Oui.	Non
Microsoft.Network/virtualNetworks/subnets/write	Oui.	Non
Microsoft.Network/routeTables/join/action	Oui.	Non
Microsoft.Ressources/déploiements/opérations/lecture	Oui.	Oui.
Microsoft.Ressources/déploiements/lecture	Oui.	Oui.
Microsoft.Ressources/déploiements/écriture	Oui.	Non
Microsoft.Ressources/ressources/lecture	Oui.	Oui.
Microsoft.Ressources/abonnements/résultats d'opération/lecture	Oui.	Oui.
Microsoft.Ressources/abonnements/resourceGroups/delete	Oui.	Non
Microsoft.Ressources/abonnements/resourceGroups/read	Oui.	Oui.
Microsoft.Ressources/abonnements/groupe de ressources/ressources/lecture	Oui.	Oui.

Action	Utilisé pour la configuration ?	Utilisé pour les opérations quotidiennes ?
Microsoft.Ressources/abonnements/resourceGroups/write	Oui.	Non

#### Tiering dans le cloud

Lors de la configuration de Cloud Tiering, il effectue les requêtes d'API suivantes.

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Ressources/abonnements/resourceGroups/read
- Microsoft.Ressources/abonnements/emplacements/lecture

Le connecteur effectue les demandes d'API suivantes pour les opérations quotidiennes.

- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/blobServices/containers/write
- Microsoft.Storage/storageAccounts/managePolicies/read
- Microsoft.Storage/storageAccounts/managePolicies/write
- Microsoft.Storage/storageAccounts/read

#### Cloud Volumes ONTAP

Il effectue les requêtes d'API suivantes pour déployer et gérer Cloud Volumes ONTAP dans AWS.

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créer des VM, arrêter, démarrer, supprimer et obtenir l'état du système	Microsoft.Compute/locations/operations/read	Oui.	Oui.	Non
	Microsoft.Compute/locations/vmSizes/read	Oui.	Oui.	Non
	Microsoft.Ressources/abonnements/emplacements/lecture	Oui.	Non	Non
	Microsoft.Compute/operations/read	Oui.	Oui.	Non
	Microsoft.Compute/virtualMachines/instanceView/read	Oui.	Oui.	Non
	Microsoft.Compute/virtualMachines/powerOff/action	Oui.	Oui.	Non
	Microsoft.Compute/virtualMachines/read	Oui.	Oui.	Non
	Microsoft.Compute/virtualMachines/restart/action	Oui.	Oui.	Non
	Microsoft.Compute/virtualMachines/start/action	Oui.	Oui.	Non
	Microsoft.Compute/virtualMachines/deallocate/action	Non	Oui.	Oui.
	Microsoft.Compute/virtualMachines/vmSizes/read	Non	Oui.	Non
	Microsoft.Compute/virtualMachines/write	Oui.	Oui.	Non
Déployez à partir d'un VHD	Microsoft.Compute/images/read	Oui.	Non	Non

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créez et gérez des interfaces réseau dans le sous-réseau cible	Microsoft.Network/networkInterfaces/read	Oui.	Oui.	Non
	Microsoft.Network/networkInterfaces/write	Oui.	Oui.	Non
	Microsoft.Network/networkInterfaces/join/action	Oui.	Oui.	Non
Créez des groupes de sécurité réseau prédéfinis	Microsoft.Network/networkSecurityGroups/read	Oui.	Oui.	Non
	Microsoft.Network/networkSecurityGroups/write	Oui.	Oui.	Non
	Microsoft.Network/networkSecurityGroups/join/action	Oui.	Non	Non
Obtenez des informations réseau sur les régions, le vnet cible et le sous-réseau, et ajoutez les machines virtuelles à VNets	Microsoft.Network/locations/operationResults/read	Oui.	Oui.	Non
	Microsoft.Network/locations/operations/read	Oui.	Oui.	Non
	Microsoft.Network/virtualNetworks/read	Oui.	Non	Non
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Oui.	Non	Non
	Microsoft.Network/virtualNetworks/subnets/read	Oui.	Oui.	Non
	Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Oui.	Oui.	Non
	Microsoft.Network/virtualNetworks/virtualMachines/read	Oui.	Oui.	Non
	Microsoft.Network/virtualNetworks/subnets/join/action	Oui.	Oui.	Non

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créer et gérer des groupes de ressources	Microsoft.Ressources/déploiements/opérations/lecture	Oui.	Oui.	Non
	Microsoft.Ressources/déploiements/lecture	Oui.	Oui.	Non
	Microsoft.Ressources/déploiements/écriture	Oui.	Oui.	Non
	Microsoft.Ressources/ressources/lecture	Oui.	Oui.	Non
	Microsoft.Ressources/abonnements/résultats d'opération/lecture	Oui.	Oui.	Non
	Microsoft.Ressources/abonnements/resourceGroups/delete	Oui.	Oui.	Oui.
	Microsoft.Ressources/abonnements/resourceGroups/read	Non	Oui.	Non
	Microsoft.Ressources/abonnements/groupe de ressources/ressources/lecture	Oui.	Oui.	Non
	Microsoft.Ressources/abonnements/resourceGroups/write	Oui.	Oui.	Non

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Gérez les comptes et les disques de stockage Azure	Microsoft.Compute/disks/read	Oui.	Oui.	Oui.
	Microsoft.Compute/disks/write	Oui.	Oui.	Non
	Microsoft.Compute/disks/delete	Oui.	Oui.	Oui.
	Microsoft.Storage/checkkamedisponibilité/read	Oui.	Oui.	Non
	Microsoft.storage/opérations/lecture	Oui.	Oui.	Non
	Microsoft.Storage/storageAccounts/listkeys/action	Oui.	Oui.	Non
	Microsoft.Storage/storageAccounts/read	Oui.	Oui.	Non
	Microsoft.Storage/storageAccounts/delete	Non	Oui.	Oui.
	Microsoft.Storage/storageAccounts/write	Oui.	Oui.	Non
	Microsoft.Storage/usage/lecture	Non	Oui.	Non
Activez les sauvegardes sur le stockage Blob et le chiffrement des comptes de stockage	Microsoft.Storage/storageAccounts/blobServices/containers/read	Oui.	Oui.	Non
	Microsoft.KeyVault/certificates/lecture	Oui.	Oui.	Non
	Microsoft.KeyVault/certificates/Access Policies/write	Oui.	Oui.	Non
Activez les terminaux du service vnet pour le Tiering des données	Microsoft.Network/virtualNetworks/subnets/write	Oui.	Oui.	Non
	Microsoft.Network/routeTables/join/action	Oui.	Oui.	Non

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créez et gérez des snapshots gérés par Azure	Microsoft.Compute/snapshots/write	Oui.	Oui.	Non
	Microsoft.Compute/snapshots/read	Oui.	Oui.	Non
	Microsoft.Compute/snapshots/delete	Non	Oui.	Oui.
	Microsoft.Compute/disks/beginGetAccess/action	Non	Oui.	Non
Créer et gérer des ensembles de disponibilité	Microsoft.Compute/availabilitySets/write	Oui.	Non	Non
	Microsoft.Compute/availabilitySets/read	Oui.	Non	Non
Mettez en place des déploiements de programmation sur le marché	Microsoft.MarketplaceOrdering/Offres/éditeurs/offres/plans/accords/lecture	Oui.	Non	Non
	Microsoft.MarketplaceOrdering/Offres/éditeurs/offres/plans/accords/écrire	Oui.	Oui.	Non
Gérer un équilibreur de charge pour les paires HA	Microsoft.Network/loadBalancers/read	Oui.	Oui.	Non
	Microsoft.Network/loadBalancers/write	Oui.	Non	Non
	Microsoft.Network/loadBalancers/delete	Non	Oui.	Oui.
	Microsoft.Network/loadBalancers/backendAddressPools/read	Oui.	Oui.	Non
	Microsoft.Network/loadBalancers/loadBalancingRules/read	Oui.	Non	Non
	Microsoft.Network/loadBalancers/probes/read	Oui.	Non	Non
	Microsoft.Network/loadBalancers/probes/join/action	Oui.	Non	Non

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Activez la gestion des verrouillages sur les disques Azure	Microsoft.autorisatio n/verrous/*	Oui.	Oui.	Non
Activez des terminaux privés pour les paires haute disponibilité lorsque aucune connectivité ne se trouve en dehors du sous-réseau	Microsoft.Network/pr ivateEndpoints/write	Oui.	Oui.	Non
	Microsoft.Storage/st orageAccounts/Priva teEndpointConnectio nsApproval/action	Oui.	Non	Non
	Microsoft.Storage/st orageAccounts/priva teEndpointConnectio ns/read	Oui.	Oui.	Oui.
	Microsoft.Network/pr ivateEndpoints/read	Oui.	Oui.	Oui.
	Microsoft.Network/pr ivateDnsZones/write	Oui.	Oui.	Non
	Microsoft.Network/pr ivateDnsZones/virtu alNetworkLinks/write	Oui.	Oui.	Non
	Microsoft.Network/vir tualNetworks/join/act ion	Oui.	Oui.	Non
	Microsoft.Network/pr ivateDnsZones/A/wri te	Oui.	Oui.	Non
	Microsoft.Network/pr ivateDnsZones/read	Oui.	Oui.	Non
	Microsoft.Network/pr ivateDnsZones/virtu alNetworkLinks/read	Oui.	Oui.	Non
Requis par Azure pour certains déploiements de VM, en fonction du matériel physique sous-jacent	Microsoft.Ressource s/déploiements/opér ations Statelists/lecture	Oui.	Oui.	Non



Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Supprimer des ressources d'un groupe de ressources en cas d'échec ou de suppression du déploiement	Microsoft.Network/privateEndpoints/delete	Oui.	Oui.	Non
	Microsoft.Compute/availabilitySets/delete	Oui.	Oui.	Non
Activez l'utilisation de clés de chiffrement gérées par le client lors de l'utilisation de l'API	Microsoft.Compute/diskEncryptionSets/read	Oui.	Oui.	Oui.
	Microsoft.Compute/diskEncryptionSets/write	Oui.	Oui.	Non
	Microsoft.KeyVault/offres-forts/déploiement/action	Oui.	Non	Non
	Microsoft.Compute/diskEncryptionSets/delete	Oui.	Oui.	Oui.
Configurez un groupe de sécurité des applications pour une paire haute disponibilité afin d'isoler les cartes réseau d'interconnexion haute disponibilité et de cluster	Microsoft.Network/applicationSecurityGroups/write	Non	Oui.	Non
	Microsoft.Network/applicationSecurityGroups/read	Non	Oui.	Oui.
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	Non	Oui.	Non
	Microsoft.Network/networkSecurityGroups/securityRules/write	Oui.	Oui.	Non
	Microsoft.Network/applicationSecurityGroups/delete	Non	Oui.	Non
	Microsoft.Network/networkSecurityGroups/securityRules/delete	Non	Oui.	Oui.

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Balises de lecture, d'écriture et de suppression associées aux ressources Cloud Volumes ONTAP	Microsoft.Ressources/balises/lecture	Non	Oui.	Non
	Microsoft.Ressources/balises/écrire	Oui.	Oui.	Non
	Microsoft.Ressources/balises/Supprimer	Oui.	Non	Non
Crypter les comptes de stockage pendant leur création	Microsoft.ManagedIdentity/userAssignedIdentities/attributable/action	Oui.	Oui.	Non

### Cache global de fichiers

Lorsque vous utilisez Global File cache, le connecteur effectue les demandes d'API suivantes :

- Microsoft.Insights/Metrics/Read
- Microsoft.Compute/virtualMachines/extensions/write
- Microsoft.Compute/virtualMachines/extensions/read
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Ressources/déploiements/suppression

### Kubernetes

Ce connecteur effectue les requêtes d'API suivantes pour détecter et gérer les clusters exécutés dans Azure Kubernetes Service (AKS) :

- Microsoft.Compute/virtualMachines/read
- Microsoft.Ressources/abonnements/emplacements/lecture
- Microsoft.Ressources/abonnements/résultats d'opération/lecture
- Microsoft.Ressources/abonnements/resourceGroups/read
- Microsoft.Ressources/abonnements/groupes de ressources/ressources/lecture
- Microsoft.ContainerService/manageClusters/lecture
- Microsoft.ContainerService/manageClusters/listClusterUserCredential/action

### Journal des modifications

Lorsque des autorisations sont ajoutées et supprimées, nous les noterons dans les sections ci-dessous.

Les autorisations suivantes ont été ajoutées à la politique JSON :

- Microsoft.Storage/storageAccounts/blobServices/containers/write

Cette autorisation est requise pour Cloud Backup et Cloud Tiering.

- Microsoft.Network/publicIPAddresses/delete

Ces autorisations sont requises pour Cloud Backup.

Les autorisations suivantes ont été supprimées de la politique JSON car elles ne sont plus requises :

- Microsoft.Compute/images/write
- Microsoft.Network/loadBalancers/backendAddressPools/join/action
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read
- Microsoft.Storage/storageAccounts/regénérateur/action

## Autorisations Google Cloud pour le connecteur

BlueXP requiert des autorisations pour effectuer des actions dans Google Cloud. Ces autorisations sont incluses dans un rôle personnalisé fourni par NetApp. Vous voudrez peut-être comprendre ce que BlueXP fait avec ces autorisations.

### Autorisations de compte de service

Le rôle personnalisé illustré ci-dessous fournit les autorisations dont un connecteur a besoin pour gérer les ressources et les processus au sein de votre réseau Google Cloud.

Vous devez appliquer ce rôle personnalisé à un compte de service rattaché à la machine virtuelle Connector. ["Affichez les instructions détaillées"](#).

Vous devez également vous assurer que le rôle est à jour lorsque de nouvelles autorisations sont ajoutées dans les versions 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`

## Utilisation des autorisations Google Cloud

Actions	Objectif
- Compute.disks.create - Compute.disks.createSnapshot - compute.disks.delete - Compute.disks.get - Compute.disks.list - compute.disks.setLabels - compute.disks.use	Pour créer et gérer des disques pour Cloud Volumes ONTAP.
- compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list	Pour créer des règles de pare-feu pour Cloud Volumes ONTAP.
- Compute.globalOperations.get	Pour obtenir l'état des opérations.
- Compute.images.get - Compute.images.getFromFamily - Compute.images.list - compute.images.useReadOnly	Pour obtenir les images des instances de VM.
- compute.instances.attachDisk - compute.instances.detachDisk	Pour attacher et détacher les disques à Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Pour créer et supprimer des instances de VM Cloud Volumes ONTAP.
- compute.instances.get	Pour afficher la liste des instances de VM.
- compute.instances.getSerialPortOutput	Pour obtenir les journaux de la console.
- compute.instances.list	Pour récupérer la liste des instances dans une zone.
- compute.instances.setDeletionProtection	Pour définir la protection de suppression sur l'instance.
- compute.instances.setLabels	Pour ajouter des étiquettes.
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	Pour modifier le type de machine pour Cloud Volumes ONTAP.
- compute.instances.setMetadata	Pour ajouter des métadonnées.
- compute.instances.setTags	Pour ajouter des balises pour les règles de pare-feu.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Pour démarrer et arrêter Cloud Volumes ONTAP.
- Compute.machineTypes.get	Pour obtenir le nombre de cœurs à vérifier qoupas.
- compute.projects.get	Pour prendre en charge des projets multiples.
- Compute.snapshots.create - compute.snapshots.delete - Compute.snapshots.get - Compute.snapshots.list - compute.snapshots.setLabels	Pour créer et gérer des snapshots de disques persistants.
- compute.networks.get - compute.networks.list - Compute.rerégions.get - Compute.rerégions.list - Compute.subNetworks.get - Compute.subNetworks.list - Compute.zoneOperations.get - Compute.zones.get - Compute.zones.zones.list	Pour obtenir les informations de mise en réseau nécessaires à la création d'une nouvelle instance de machine virtuelle Cloud Volumes ONTAP.

Actions	Objectif
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifestes.get - deploymentmanager.manifestes.list - deploymentmanager.Operations.get - deploymentmanager.Operations.list - deploymentmanager.resources.get - deploymentmanager.resources.list - deploymentmanager.typeProviders.get.types.deploym entmanager.deploymentmanager.deploymentlist.types .deploymentmanager.deploymentlist.deploymentmana ger.deploymentmanager.Deploymenttypes.Deployeme ntManager.Deploymentlist.Deploymenttypes.Deploym entManager.Deployment	Pour déployer l'instance de machine virtuelle Cloud Volumes ONTAP à l'aide de Google Cloud Deployment Manager.
- Logging.logEntries.list - logging.privateLogEntries.list	Pour obtenir les disques de consignment des piles.
- resourcemanager.projects.get	Pour prendre en charge des projets multiples.
- storage.seaux.create - storage.buckets.delete - storage.seaux.get - storage.seaux.list - storage.seaux.update	Pour créer et gérer un compartiment Google Cloud Storage pour le Tiering des données.
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.get - cloudkms.crypKeys.list - cloudkms.keyrings.list	Pour utiliser des clés de chiffrement gérées par le client à partir du service Cloud Key Management avec Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - Storage.objects.get - Storage.objects.list	Pour définir un compte de service sur l'instance Cloud Volumes ONTAP. Ce compte de service fournit des autorisations de Tiering des données vers un compartiment Google Cloud Storage.
- compute.adresses.list	Pour récupérer les adresses d'une région lors du déploiement d'une paire haute disponibilité.
- Compute.backendServices.create - Compute.régionBackendServices.create - Compute.régionBackendServices.get - Compute.régionBackendServices.list	Pour configurer un service back-end pour la distribution du trafic dans une paire HA.
- compute.networks.updatePolicy	Pour appliquer des règles de pare-feu sur les VPC et les sous-réseaux d'une paire HA.
- compute.subnetworks.use - compute.subnetworks.useExternallp - compute.instances.addAccessConfig	Pour activer le sens des données du cloud.
- container.cluster.get - container.cluster.list	Pour détecter les clusters Kubernetes s'exécutant dans Google Kubernetes Engine.
- compute.instanceGroups.get - Compute.adresses.get	Pour créer et gérer des VM de stockage sur des paires haute disponibilité.

Actions	Objectif
- Monitoring.timeseries.list - Storage.seaux.getIamPolicy	Pour découvrir des compartiments Google Cloud Storage.

## Ports

### Règles de groupe de sécurité dans AWS

Le groupe de sécurité AWS du connecteur nécessite à la fois des règles entrantes et sortantes.

#### Règles entrantes

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale et des connexions à partir de l'instance Cloud Data Sense
TCP	3128	Permet à Cloud Volumes ONTAP d'accéder à Internet pour l'envoi des messages AutoSupport au support NetApp. Vous devez ouvrir ce port manuellement après le déploiement. server for AutoSupport messages, En savoir plus sur le serveur proxy du connecteur.
TCP	9060	Il est possible d'activer et d'utiliser Cloud Data Sense et Cloud Backup dans les déploiements dans le cloud pour les administrations publiques. Ce port est également requis pour Cloud Backup si vous désactivez l'interface SaaS dans votre compte BlueXP.

#### Règles de sortie

Le groupe de sécurité prédéfini pour le connecteur ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

#### Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour le connecteur inclut les règles de trafic sortant suivantes.

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles UDP	Tout	Tout le trafic sortant



## Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par le connecteur.



L'adresse IP source est l'hôte du connecteur.

Service	Protocole	Port	Destination	Objectif
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	Appels d'API vers AWS et ONTAP, vers le cloud Data Sense, vers le service ransomware et envoi de messages AutoSupport à NetApp
Appels API	TCP	3000	ONTAP HA médiateur	Communication avec le médiateur ONTAP HA
	TCP	8088	Sauvegarde vers S3	Appels d'API vers Backup vers S3
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par BlueXP

## Règles de groupe de sécurité dans Azure

Le groupe de sécurité Azure pour le connecteur nécessite à la fois des règles entrantes et sortantes.

### Règles entrantes

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale et des connexions à partir de l'instance Cloud Data Sense

Protocole	Port	Objectif
TCP	3128	Permet à Cloud Volumes ONTAP d'accéder à Internet pour l'envoi des messages AutoSupport au support NetApp. Vous devez ouvrir ce port manuellement après le déploiement. server for AutoSupport messages, En savoir plus sur le serveur proxy du connecteur.
TCP	9060	Il est possible d'activer et d'utiliser Cloud Data Sense et Cloud Backup dans les déploiements dans le cloud pour les administrations publiques. Ce port est également requis pour Cloud Backup si vous désactivez l'interface SaaS dans votre compte BlueXP.

## Règles de sortie

Le groupe de sécurité prédéfini pour le connecteur ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

### Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour le connecteur inclut les règles de trafic sortant suivantes.

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles UDP	Tout	Tout le trafic sortant

### Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par le connecteur.



L'adresse IP source est l'hôte du connecteur.

Service	Protocole	Port	Destination	Objectif
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	Appels d'API vers Azure et ONTAP, vers le cloud Data Sense, vers le service ransomware et envoi de messages AutoSupport à NetApp
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par BlueXP

## Règles de pare-feu dans Google Cloud

Les règles de pare-feu Google Cloud pour le connecteur exigent à la fois des règles entrantes et sortantes.

### Règles entrantes

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale
TCP	3128	Permet à Cloud Volumes ONTAP d'accéder à Internet pour l'envoi des messages AutoSupport au support NetApp. Vous devez ouvrir ce port manuellement après le déploiement. server for AutoSupport messages, En savoir plus sur le serveur proxy du connecteur.

### Règles de sortie

Les règles de pare-feu prédéfinies pour le connecteur ouvrent tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

### Règles de base pour les appels sortants

Les règles de pare-feu prédéfinies pour le connecteur comprennent les règles de trafic sortant suivantes.

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant

Protocole	Port	Objectif
Tous les protocoles UDP	Tout	Tout le trafic sortant

### Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par le connecteur.



L'adresse IP source est l'hôte du connecteur.

Service	Protocole	Port	Destination	Objectif
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	Appels d'API vers GCP et ONTAP, vers le cloud Data Sense, vers le service ransomware et envoi de messages AutoSupport à NetApp
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par BlueXP

### Ports pour le connecteur sur site

Le connecteur utilise les ports *Inbound* suivants lorsqu'il est installé manuellement sur un hôte Linux sur site.

Ces règles entrantes s'appliquent aux deux modèles de déploiement du connecteur sur site, installé avec accès à Internet ou sans accès à Internet.

Protocole	Port	Objectif
HTTP	80	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale

# Connaissances et support

## S'inscrire pour obtenir de l'aide

Avant d'ouvrir un dossier de demande de support auprès du support technique NetApp, vous devez ajouter un compte sur le site du support NetApp (NSS) à BlueXP, puis vous inscrire pour obtenir du support.

### Présentation de l'inscription au support

Il existe deux types d'inscription pour activer les droits d'assistance :

- Enregistrement de votre abonnement au support pour les identifiants de compte BlueXP (votre numéro de série à 20 chiffres 960xxxxxxx se trouve sur la page des ressources de support de BlueXP).

Il sert d'ID d'abonnement unique pour tous les services de BlueXP. Chaque abonnement au support BlueXP au niveau du compte doit être enregistré.

- Enregistrement des numéros de série Cloud Volumes ONTAP associés à un abonnement sur le marché de votre fournisseur cloud (numéros de série à 20 chiffres 909201xxxxxxx).

Ces numéros de série sont généralement appelés *PAYGO - numéros de série* et sont générés par BlueXP au moment du déploiement de Cloud Volumes ONTAP.

L'enregistrement des deux types de numéros de série offre des fonctionnalités telles que l'ouverture de tickets de support et la génération automatique de tickets.

La façon dont vous vous inscrivez dépend de votre présence ou de votre présence chez un client ou un partenaire nouveau ou existant.

- Client ou partenaire existant

En tant que client ou partenaire NetApp, vous pouvez utiliser votre compte SSO du site de support NetApp pour effectuer les enregistrements suivants. Dans le tableau de bord support, BlueXP fournit une page **NSS Management** où vous pouvez ajouter votre compte NSS. Une fois votre compte NSS ajouté, BlueXP enregistre automatiquement ces numéros de série pour vous.

an NSS account to BlueXP, Découvrez comment ajouter votre compte NSS.

- Nouveaux partenaires NetApp

Si vous êtes nouveau chez NetApp, vous devez enregistrer votre numéro de série BlueXP sur le site d'inscription du support NetApp. Une fois que vous avez terminé cette inscription et créé un nouveau compte NSS, vous pouvez utiliser ce compte dans BlueXP pour vous inscrire automatiquement à l'avenir.

with NetApp, Découvrez comment vous inscrire auprès de NetApp.

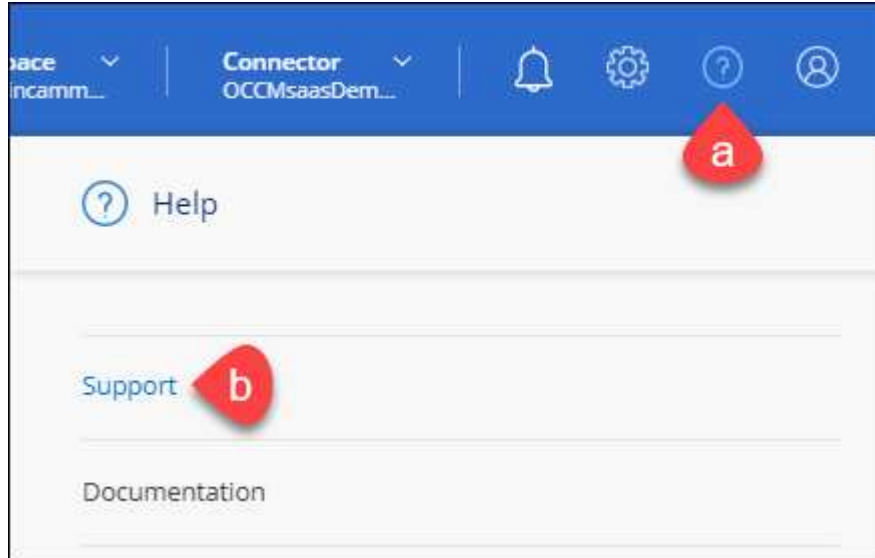
## Ajouter un compte NSS à BlueXP

Le tableau de bord du support vous permet d'ajouter et de gérer vos comptes du site de support NetApp pour BlueXP.

- Si vous avez un compte au niveau du client, vous pouvez ajouter un ou plusieurs comptes NSS.
- Si vous avez un compte partenaire ou revendeur, vous pouvez ajouter un ou plusieurs comptes NSS, mais ils ne peuvent pas être ajoutés en même temps que les comptes au niveau du client.

### Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



2. Cliquez sur **NSS Management > Ajouter un compte NSS**.
3. Lorsque vous y êtes invité, cliquez sur **Continuer** pour être redirigé vers une page de connexion Microsoft.

NetApp utilise Microsoft Azure Active Directory comme fournisseur d'identités pour les services d'authentification spécifiques au support et aux licences.

4. Sur la page de connexion, indiquez l'adresse e-mail et le mot de passe que vous avez enregistrés sur le site de support NetApp pour réaliser le processus d'authentification.

Ces actions permettent à BlueXP d'utiliser votre compte NSS pour des opérations telles que le téléchargement de licences, la vérification de la mise à niveau logicielle et les inscriptions de support futures.

Notez ce qui suit :

- Le compte doit être un compte de niveau client (et non un compte invité ou temporaire).
- Une fois la connexion établie, NetApp stockera le nom d'utilisateur NSS. Il s'agit d'un ID généré par le système qui correspond à votre courrier électronique. Sur la page **NSS Management**, vous pouvez afficher votre courriel à partir du **...** menu.
- Si vous avez besoin d'actualiser vos jetons d'identification de connexion, il existe également une option **mettre à jour les informations d'identification** dans le **...** menu. Cette option vous invite à vous reconnecter.

## Inscrivez-vous auprès de NetApp

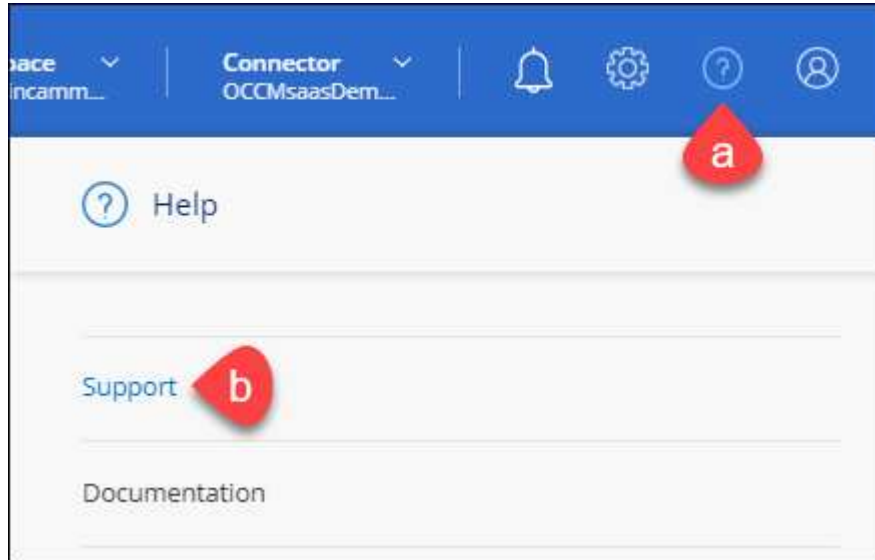
Le fait de vous inscrire au support NetApp dépend de la présence ou non d'un compte sur le site de support NetApp (NSS).

### Client existant avec un compte NSS

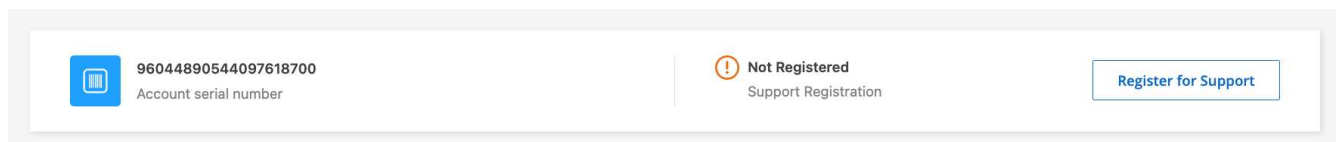
Si vous êtes client NetApp avec un compte NSS, il vous suffit de vous inscrire pour obtenir du support dans BlueXP.

#### Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



2. Si ce n'est déjà fait, ajoutez votre compte NSS à BlueXP.
3. Sur la page **Ressources**, cliquez sur **s'inscrire au support**.



### Client existant mais aucun compte NSS

Si vous êtes déjà client NetApp avec des licences et des numéros de série existants mais que *no* NSS, il vous suffit de créer un compte NSS.

#### Étapes

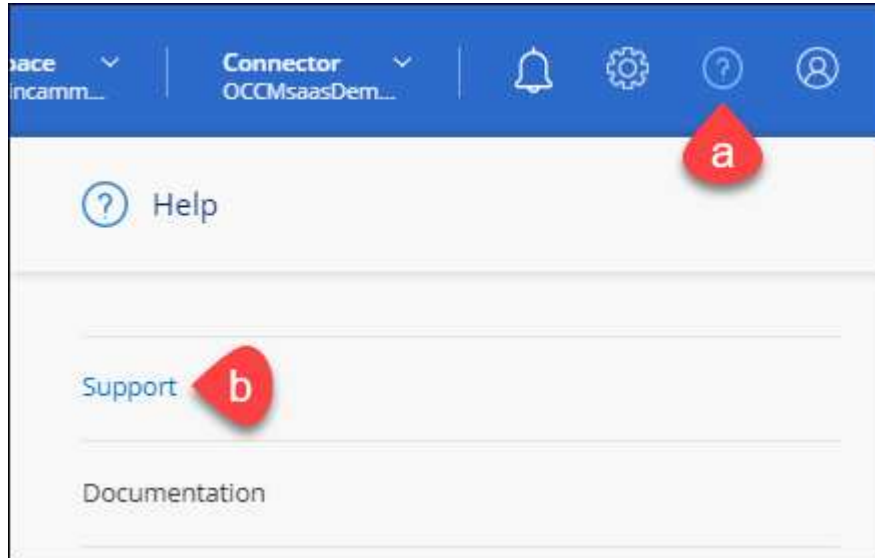
1. Créez un compte sur le site de support NetApp en complétant le "[Formulaire d'inscription de l'utilisateur du site de support NetApp](#)"
  - a. Veillez à sélectionner le niveau d'utilisateur approprié, qui est généralement **client/utilisateur final NetApp**.
  - b. Veillez à copier le numéro de série du compte BlueXP (960xxxx) utilisé ci-dessus pour le champ Numéro de série. Le traitement du compte sera ainsi accéléré.

## Découvrez la toute nouvelle gamme NetApp

Si vous êtes nouveau chez NetApp et que vous ne disposez pas d'un compte NSS, effectuez chacune des étapes ci-dessous.

### Étapes

1. Dans le coin supérieur droit de la console BlueXP, cliquez sur l'icône aide et sélectionnez **support**.



2. Recherchez le numéro de série de l'ID de compte sur la page d'inscription au support.



3. Accédez à "[Site d'inscription au support NetApp](#)" Et sélectionnez **je ne suis pas un client NetApp enregistré**.
4. Remplissez les champs obligatoires (ceux avec des astérisques rouges).
5. Dans le champ **Product Line**, sélectionnez **Cloud Manager**, puis votre fournisseur de facturation applicable.
6. Copiez le numéro de série de votre compte à l'étape 2 ci-dessus, vérifiez sa sécurité, puis lisez la Déclaration de confidentialité des données NetApp.

Un e-mail est immédiatement envoyé à la boîte aux lettres fournie pour finaliser cette transaction sécurisée. Assurez-vous de vérifier vos dossiers de courrier indésirable si l'e-mail de validation n'arrive pas dans quelques minutes.

7. Confirmez l'action à partir de l'e-mail.

La confirmation de la soumission de votre demande à NetApp et vous recommande de créer un compte sur le site de support NetApp.

8. Créez un compte sur le site de support NetApp en complétant le "[Formulaire d'inscription de l'utilisateur du site de support NetApp](#)"
  - a. Veillez à sélectionner le niveau d'utilisateur approprié, qui est généralement **client/utilisateur final NetApp**.



- b. Veillez à copier le numéro de série du compte (960xxxx) utilisé ci-dessus pour le champ Numéro de série. Le traitement du compte sera ainsi accéléré.

NetApp devrait vous contacter au cours de ce processus. Il s'agit d'un exercice d'intégration unique pour les nouveaux utilisateurs.

Une fois votre compte sur le site de support NetApp, vous pouvez accéder à BlueXP et ajouter ce compte NSS pour les inscriptions futures.

## Obtenez de l'aide

NetApp prend en charge BlueXP et ses services cloud de différentes manières. De nombreuses options d'auto-assistance gratuites sont disponibles 24 h/24 et 7 j/7, comme des articles de la base de connaissances (KB) et un forum communautaire. Votre inscription au support inclut un support technique à distance via la création de tickets en ligne.

### Auto-assistance

Ces options sont disponibles gratuitement, 24 heures sur 24, 7 jours sur 7 :

- ["Base de connaissances"](#)

Recherchez dans la base de connaissances BlueXP des articles utiles pour résoudre les problèmes.

- ["Communautés"](#)

Rejoignez la communauté BlueXP pour suivre des discussions en cours ou en créer de nouveaux.

- Documentation

La documentation BlueXP que vous consultez actuellement.

- Courrier électronique : [ng-cloudmanager-feedback@netapp.com](mailto:ng-cloudmanager-feedback@netapp.com)[E-mail de commentaires]

Nous accordons une grande importance à vos commentaires. Envoyez vos commentaires pour nous aider à améliorer BlueXP.

### Support NetApp

Outre les options d'auto-support mentionnées ci-dessus, vous pouvez travailler avec un spécialiste du support NetApp pour résoudre tous les problèmes après avoir activé le service de support.

Pour utiliser la fonction **Créer un cas**, vous devez d'abord effectuer un enregistrement unique de votre numéro de série d'ID de compte BlueXP (par exemple 960xxxx) avec NetApp. ["Découvrez comment vous inscrire à de l'aide"](#).

#### Étapes

1. Dans BlueXP, cliquez sur **aide > support**.
2. Choisissez l'une des options disponibles sous support technique :
  - a. Cliquez sur **appelez-nous** si vous souhaitez parler avec quelqu'un au téléphone. Vous serez dirigé vers une page [netapp.com](https://netapp.com) qui répertorie les numéros de téléphone que vous pouvez appeler.
  - b. Cliquez sur **Créer un dossier** pour ouvrir un dossier auprès des spécialistes du support NetApp :

- **Compte sur le site de support NetApp** : sélectionnez le compte NSS applicable associé à la personne qui ouvre le dossier de support. Cette personne sera le contact principal avec NetApp en plus de l'e-mail ci-dessous.

Si vous ne voyez pas votre compte NSS, vous pouvez accéder à l'onglet **NSS Management** de la section support de BlueXP pour l'ajouter.

- **Service** : sélectionnez le service auquel le problème est associé. Par exemple, BlueXP lorsqu'il est spécifique à un problème de support technique avec des flux de travail ou des fonctionnalités au sein du service.
- **Environnement de travail** : si applicable au stockage, sélectionnez **Cloud Volumes ONTAP** ou **sur site**, puis l'environnement de travail associé.


La liste des environnements de travail est comprise dans le cadre du compte, de l'espace de travail et du connecteur BlueXP que vous avez sélectionnés dans la bannière supérieure du service.

- **Priorité du cas** : choisissez la priorité du cas, qui peut être faible, Moyen, élevé ou critique.

Pour en savoir plus sur ces priorités, passez votre souris sur l'icône d'information située à côté du nom du champ.


- **Description du problème** : fournir une description détaillée de votre problème, y compris les messages d'erreur ou les étapes de dépannage applicables que vous avez effectués.
- **Adresses e-mail supplémentaires**: Entrez des adresses e-mail supplémentaires si vous souhaitez informer quelqu'un d'autre de ce problème.

Create a Case


TESTCLOUD2NTAP 


NetApp Support Site Account


Service

Cloud Manager 

Working Environment


Select... 

Case Priority 


Low- General Guidance 

Issue Description

Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.

Additional Email Addresses (Optional) 

Attachment (Optional) Coming Soon

No files selected 

Une fenêtre contextuelle contenant votre numéro de dossier de support s’affiche. Un spécialiste du support NetApp va étudier votre dossier et vous recontacterons très rapidement.

Pour consulter l’historique de vos dossiers d’assistance, vous pouvez cliquer sur **Paramètres > Chronologie** et rechercher les actions nommées "Créer un dossier de support". Un bouton à l’extrême droite vous permet de développer l’action pour voir les détails.

Il est possible que vous rencontriez le message d’erreur suivant lors de la création d’un dossier :

« Vous n’êtes pas autorisé à créer un dossier pour le service sélectionné »

Cette erreur peut signifier que le compte NSS et la société d’enregistrement auquel il est associé n’est pas la même société d’enregistrement pour le numéro de série du compte BlueXP (par exemple 960xxxx) ou le numéro de série de l’environnement de travail. Vous pouvez consulter votre liste de comptes NSS en haut du

formulaire **Créer un dossier** pour trouver la correspondance appropriée, ou vous pouvez demander de l'aide en utilisant l'une des options suivantes :

- Utilisez le chat du produit
- Soumettre un dossier non technique à <https://mysupport.netapp.com/site/help>

# Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

## Droits d'auteur

<http://www.netapp.com/us/legal/copyright.aspx>

## Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l'adresse suivante :

<https://www.netapp.com/us/media/patents-page.pdf>

## Politique de confidentialité

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

## Source ouverte

Les fichiers de notification fournissent des informations sur les droits d'auteur et les licences de tiers utilisés dans le logiciel NetApp.

- ["Note pour BlueXP"](#)

## 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.