



## **Connecteurs**

### **Set up and administration**

NetApp  
December 15, 2022

# Table des matières

- Connecteurs ..... 1
  - Déploiement avancé ..... 1
  - Recherche de l'ID système d'un connecteur ..... 16
  - Gestion des connecteurs existants ..... 17
  - Gestion d'un certificat HTTPS pour l'accès sécurisé ..... 24
  - Configuration d'un connecteur pour utiliser un serveur proxy HTTP ..... 25
  - Configuration par défaut du connecteur ..... 28

# 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.

#### Avant de commencer

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**.



4. Modifiez l'une des options par défaut et cliquez sur **Continuer pour lancer**.
5. 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**.

6. 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://console.bluexp.netapp.com> Pour commencer à utiliser le connecteur avec BlueXP.

## Résultat

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

Si vous disposez de compartiments 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

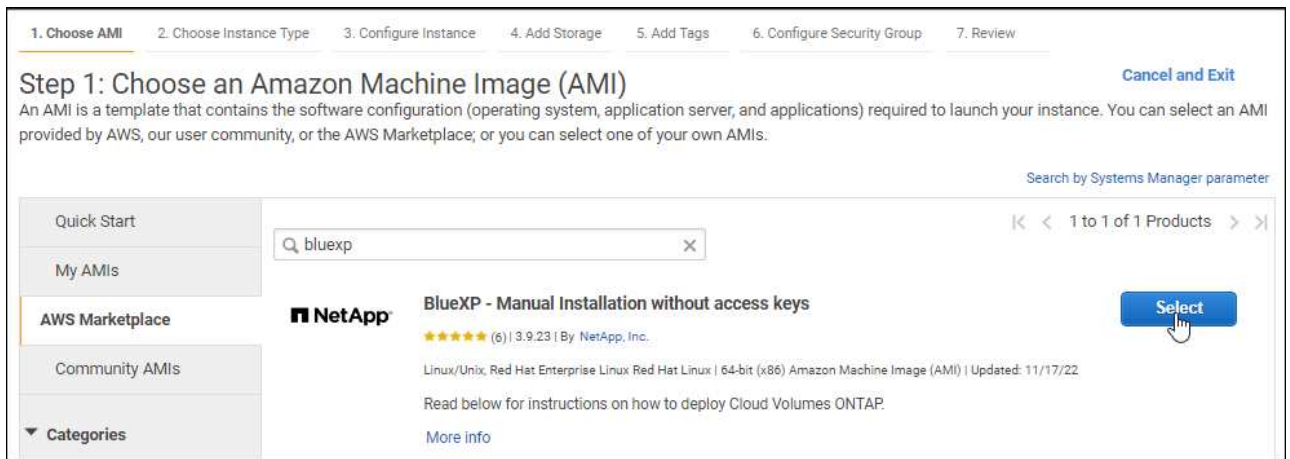
Pour déployer le connecteur dans une région AWS Government, vous devez accéder au service EC2 et sélectionner l'offre BlueXP depuis AWS Marketplace.

## 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.

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

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

`https://ipaddress[]`

5. Une fois connecté, configurez le connecteur :

- a. Spécifiez le compte NetApp à associer au connecteur.

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

- b. Entrez un nom pour le système.

## Résultat

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

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://console.bluexp.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.

### Résultat

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://console.bluexp.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[]`

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

## Résultat

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 sortantes strictes pour Cloud Volumes ONTAP, vous devrez également vous assurer que le groupe de sécurité Cloud Volumes ONTAP autorise les connexions *sortantes* sur le port 3128.

### 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 19.3.1 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://support.netapp.com>
- <https://mysupport.netapp.com>
- <https://cloudmanager.cloud.netapp.com/tenancy>
- <https://stream.cloudmanager.cloud.netapp.com>
- <https://cloudmanagerinfraprod.azurecr.io>
- <https://production-artifacts.cloudmanager.cloud.netapp.com>
- [https://\\*.blob.core.windows.net](https://*.blob.core.windows.net)

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.

### Ce dont vous avez besoin

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

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

- Certificat signé par une autorité de certification, si le serveur proxy utilise HTTPS.

### 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.

Vous devez télécharger le programme d'installation du connecteur destiné à être utilisé sur votre réseau ou dans le cloud.

### 3. Attribuez des autorisations pour exécuter le script.

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

### 4. Exécutez le script d'installation.

```
./OnCommandCloudManager-V3.9.23 --proxy <HTTP or HTTPS proxy server>  
--cacert <path and file name of a CA-signed certificate>
```

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

Voici un exemple de commande utilisant les deux paramètres facultatifs :

```
./OnCommandCloudManager-V3.9.23 --proxy  
https://user:password@10.0.0.30:8080/ --cacert  
/tmp/cacert/certificate.cer
```

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

- `http://address:port`
- `http://username:password@address:port`
- `https://address:port`
- `https://username:password@address:port`

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

## Résultat

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

## Configurer le connecteur

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

### Étapes

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

`https://ipaddress[]`

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

2. S'inscrire ou se connecter.
3. 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.
4. 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.

## Résultat

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

## Une fois que vous avez terminé

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 3 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

## Systemes 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.

## Privilèges requis

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.

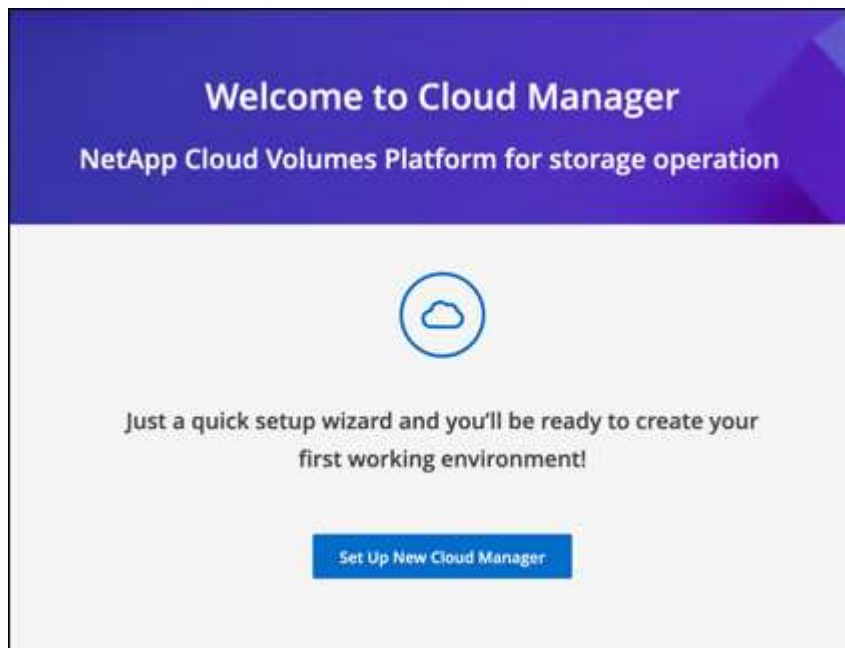
```
chmod +x /path/cloud-manager-connector-offline-v3.9.23
```

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.

### Résultat

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

### Et la suite ?

- ["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

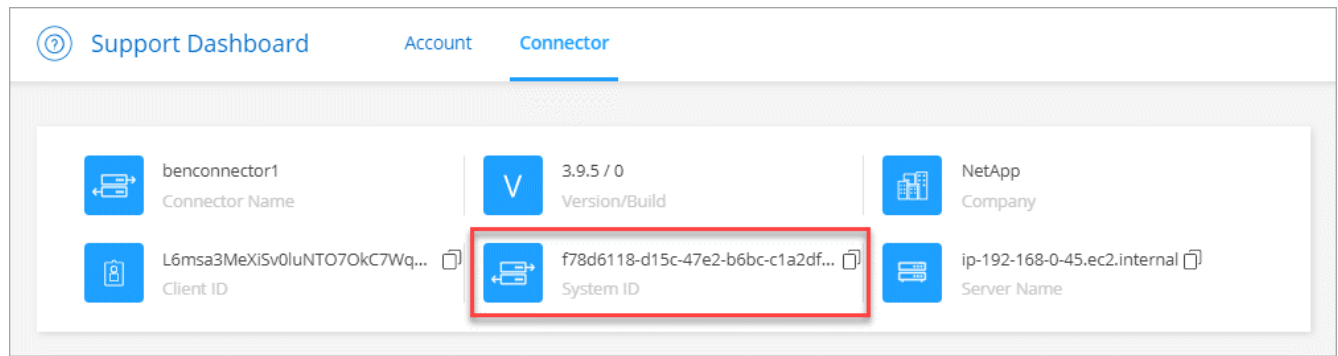
Pour vous aider à vous lancer, votre représentant NetApp peut vous demander l'ID système d'un connecteur. L'ID est généralement utilisé à des fins de licence et de dépannage.

### 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.

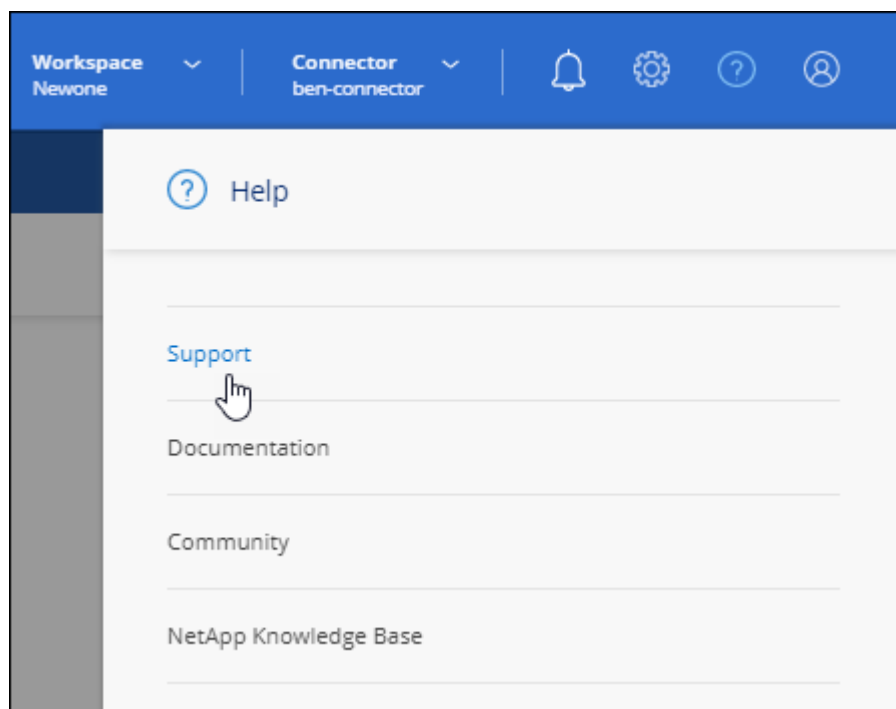
2. Entrez votre nom d'utilisateur et votre mot de passe pour vous connecter.

## Téléchargez ou envoyez un message AutoSupport

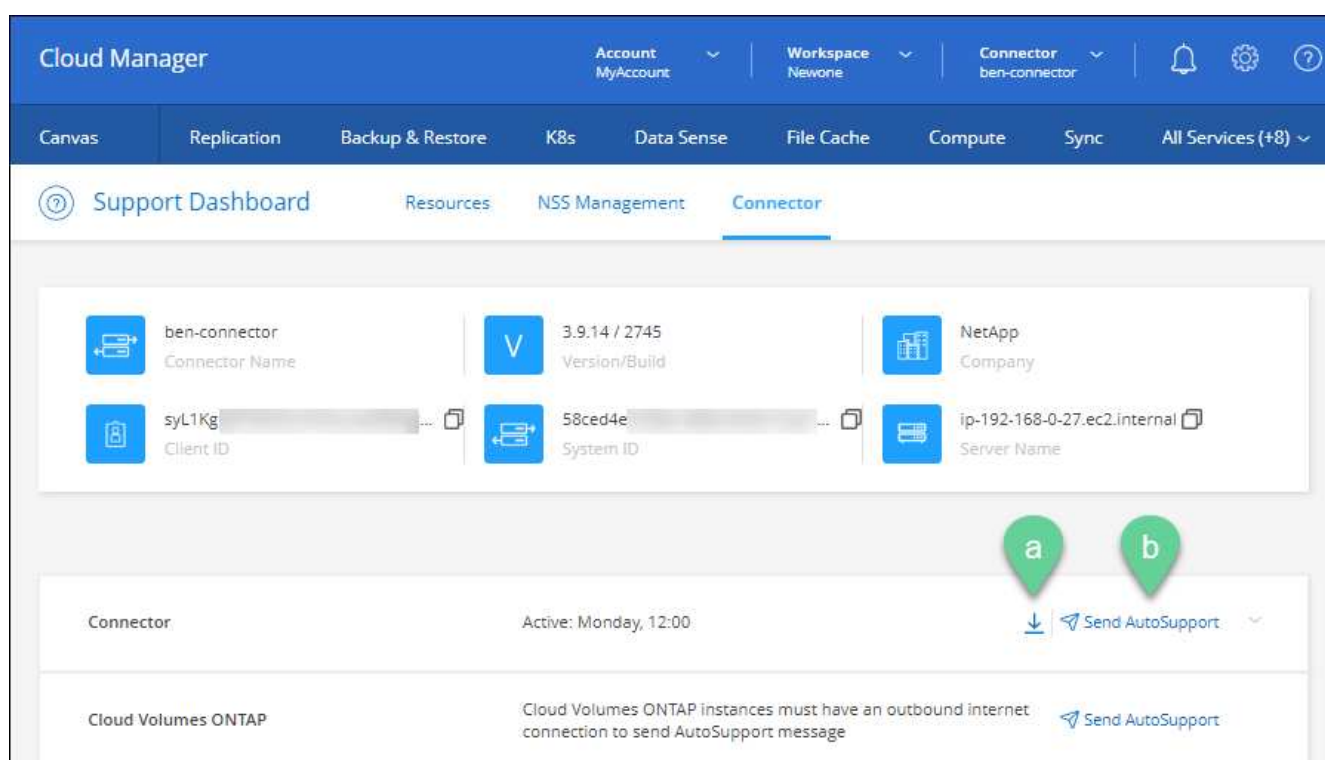
En cas de problème, les équipes NetApp peuvent vous demander d'envoyer un message AutoSupport au support NetApp à des fins de dépannage.

### 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.

### Résultat

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**.

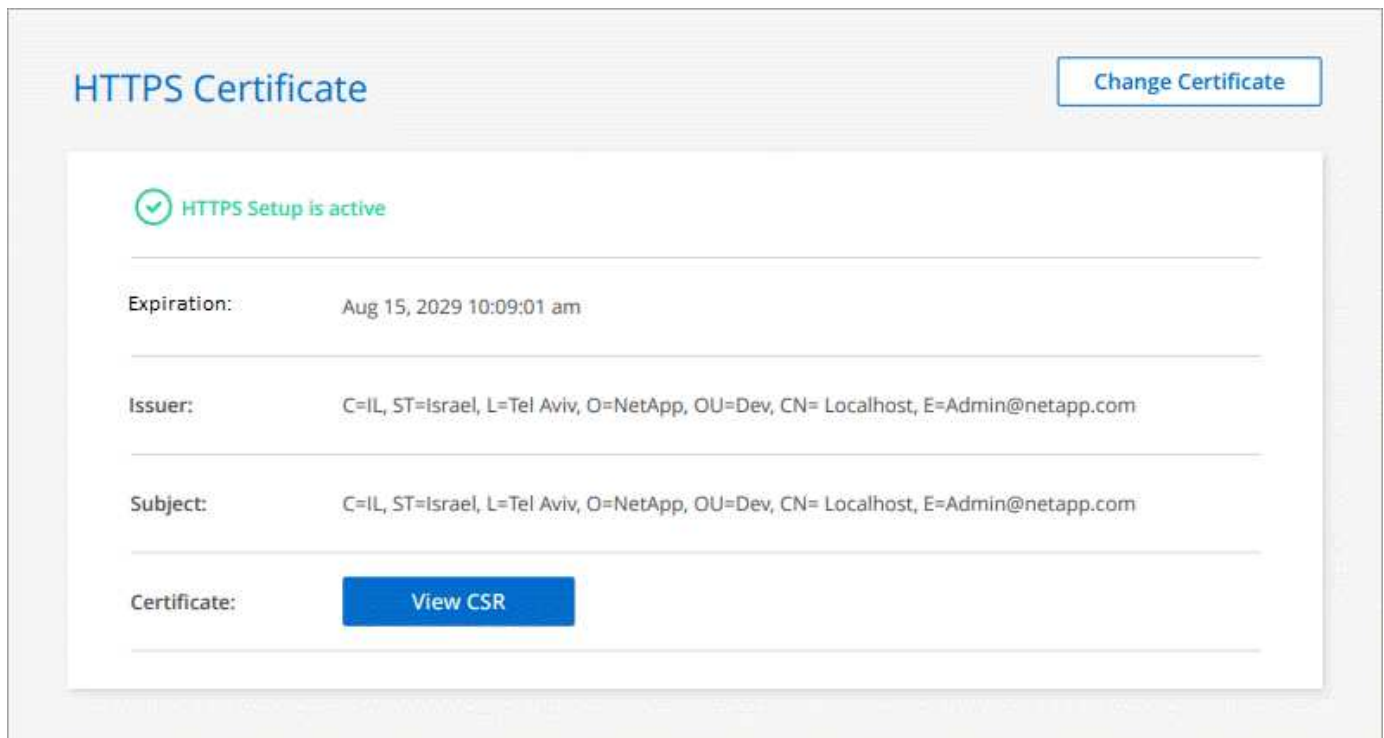


2. Dans la page Configuration HTTPS, installez un certificat en générant une requête de signature de certificat (CSR) ou en installant votre propre certificat signé par l'autorité de certification :

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>

### Résultat

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.

### Résultat

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` ou
- `/opt/application/netapp/service-manager-2/logs` (à partir de 3.9.23 nouvelles installations)

Les journaux de ces dossiers fournissent des détails sur le connecteur et les images de 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.

## Ports

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

- 80 pour l'accès HTTP
- 443 pour l'accès HTTPS

## 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



## 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.