



# **Déploiement avancé**

## **Set up and administration**

NetApp

December 05, 2022

# Table des matières

- Déploiement avancé. . . . . 1
  - Créez un connecteur à partir d’AWS Marketplace . . . . . 1
  - Créez un connecteur à partir d’Azure Marketplace . . . . . 8
  - Installez le connecteur sur un hôte Linux existant ayant accès à Internet. . . . . 12
  - Installez le connecteur sur site sans accès à Internet . . . . . 15

# 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://console.bluexp.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://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 :

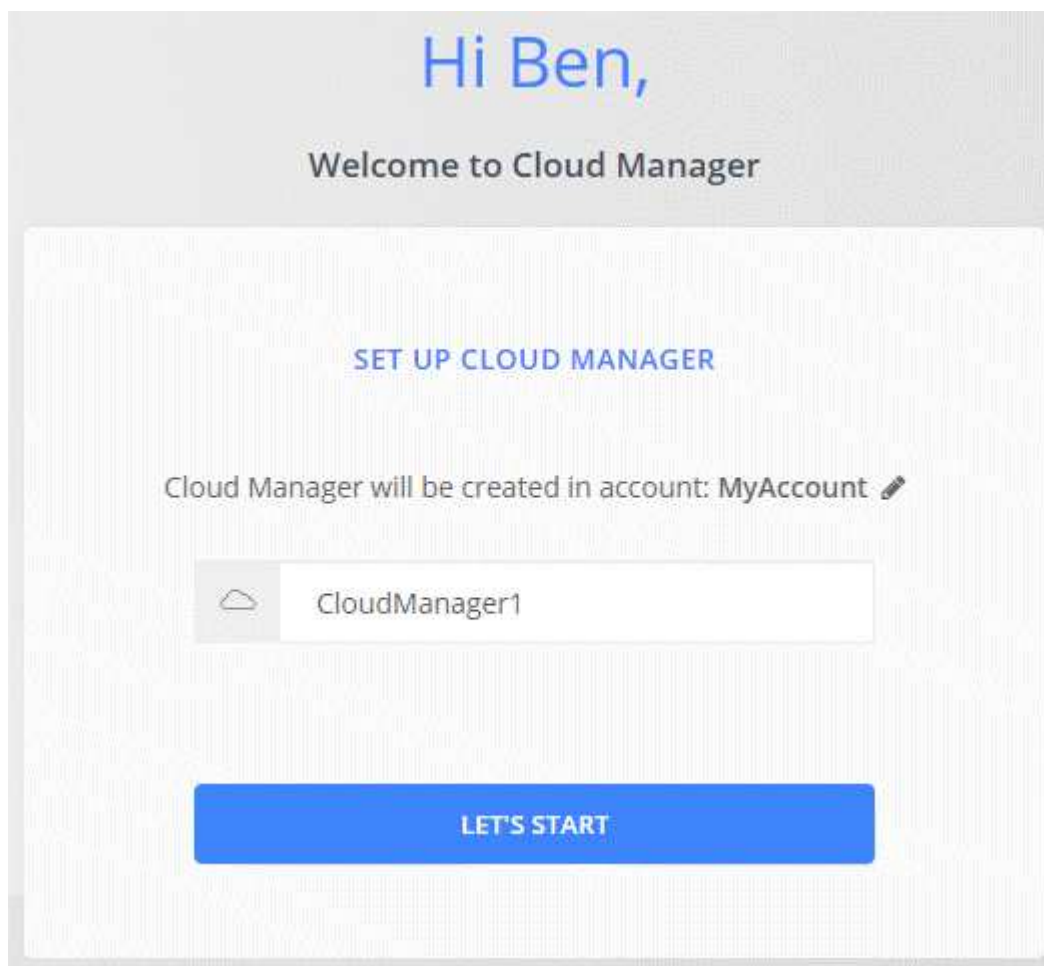
[https://ipaddress\[\]](https://ipaddress[])

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://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\[\]](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 :

- 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.

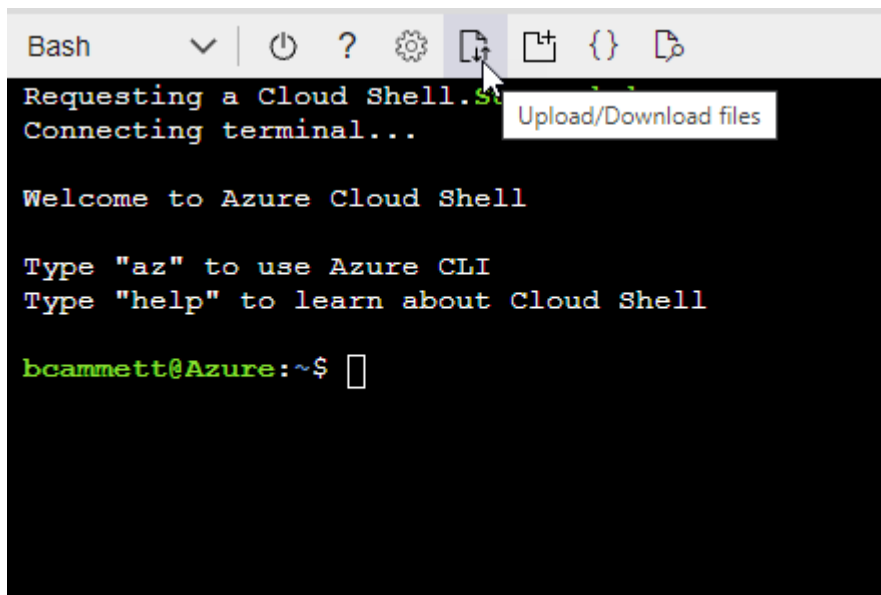
### Exemple

```
"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 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 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 :

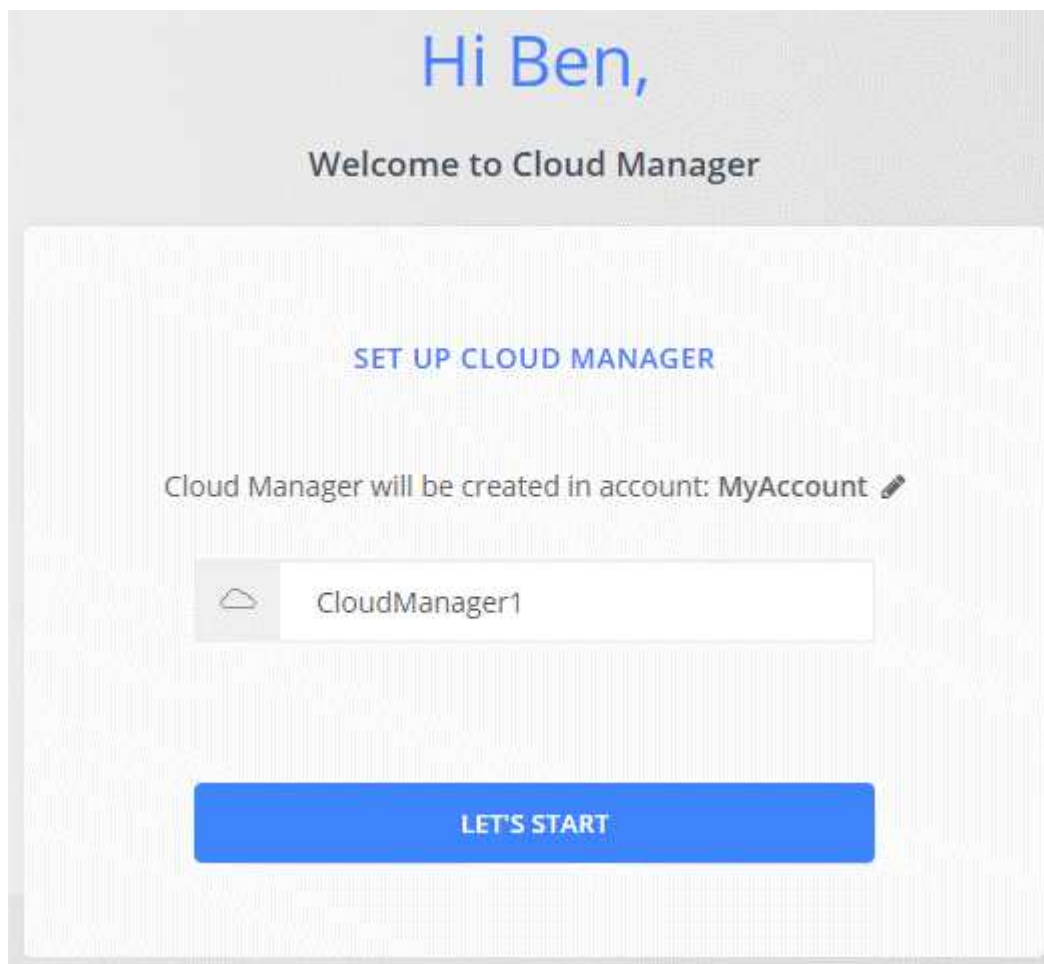
`https://ipaddress[]`

*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"](#).

## 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.