Déploiement avancé

Set up and administration

NetApp
January 09, 2023

Table des matières

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

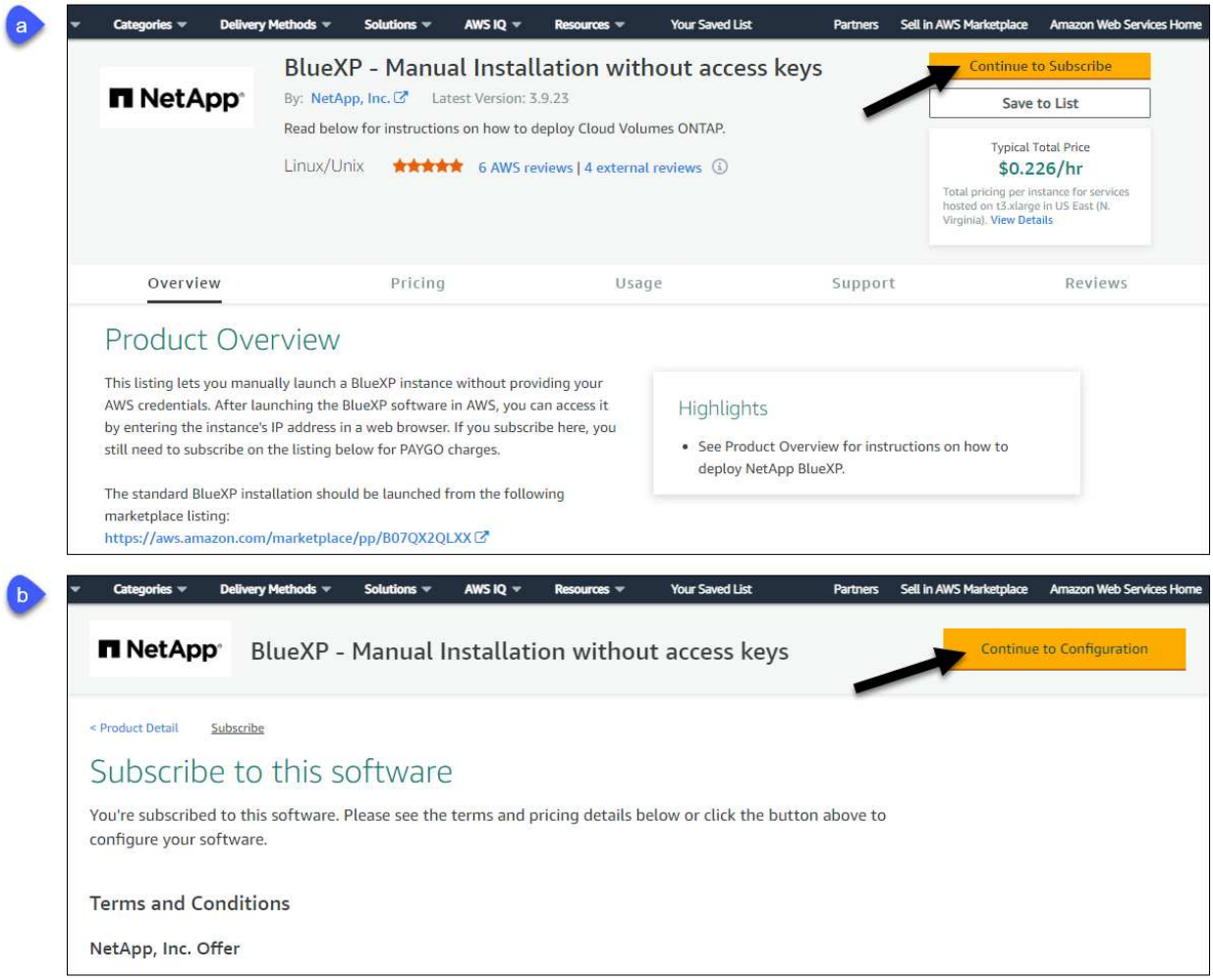
Vous pouvez lancer l'instance Connector dans une région commerciale d'AWS directement à partir de l'offre AWS Marketplace pour BlueXP.

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

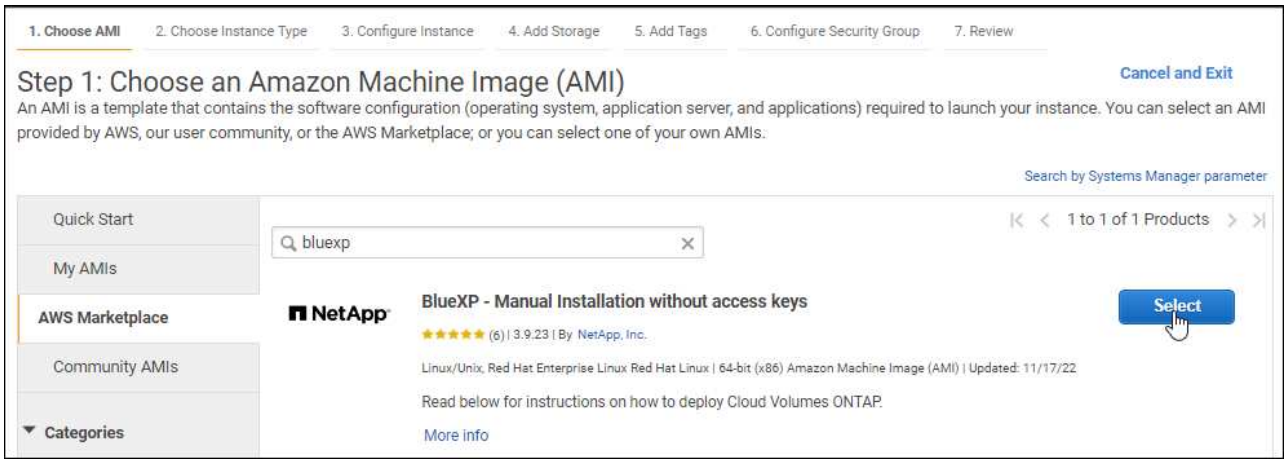
Pour déployer le connecteur dans une région AWS Government, vous devez accéder au service EC2 et sélectionner l'offre BlueXP depuis AWS Marketplace.

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.



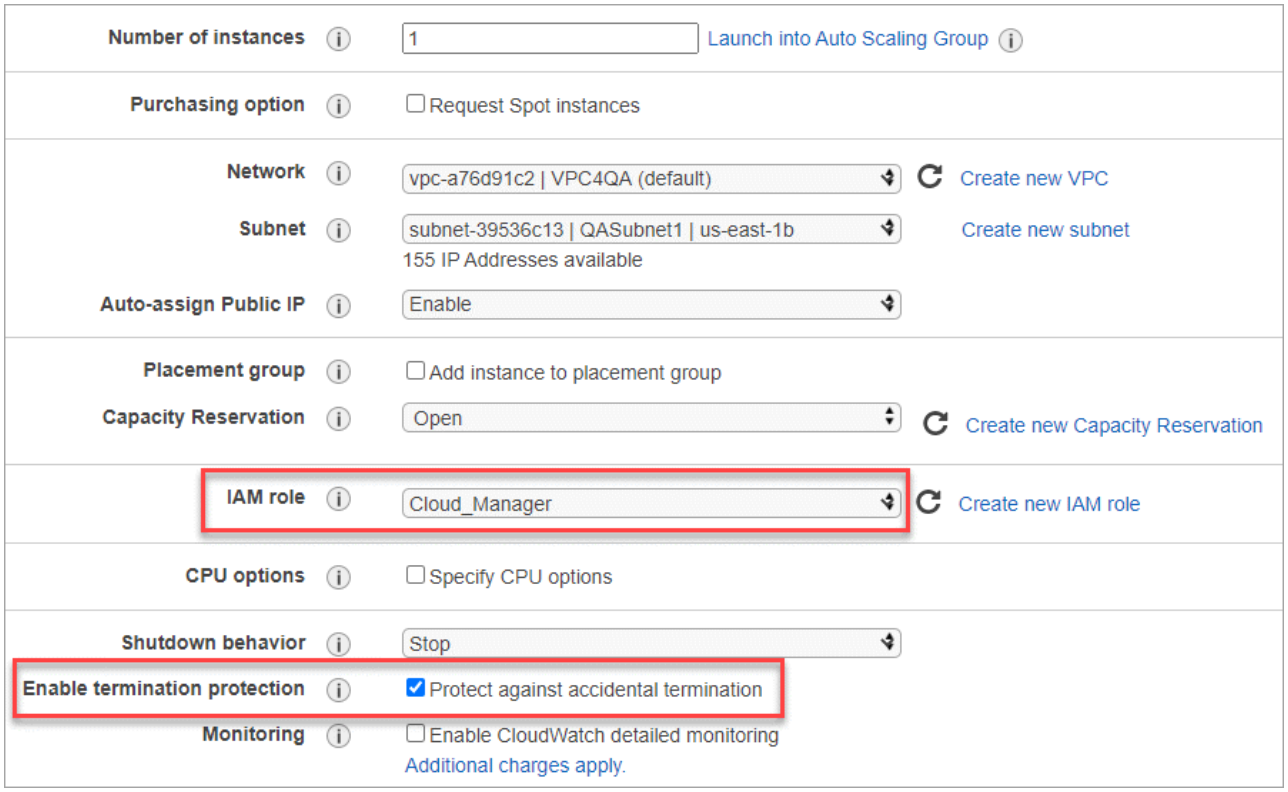
d. Cliquez sur **Continuer**.

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.



   - **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.

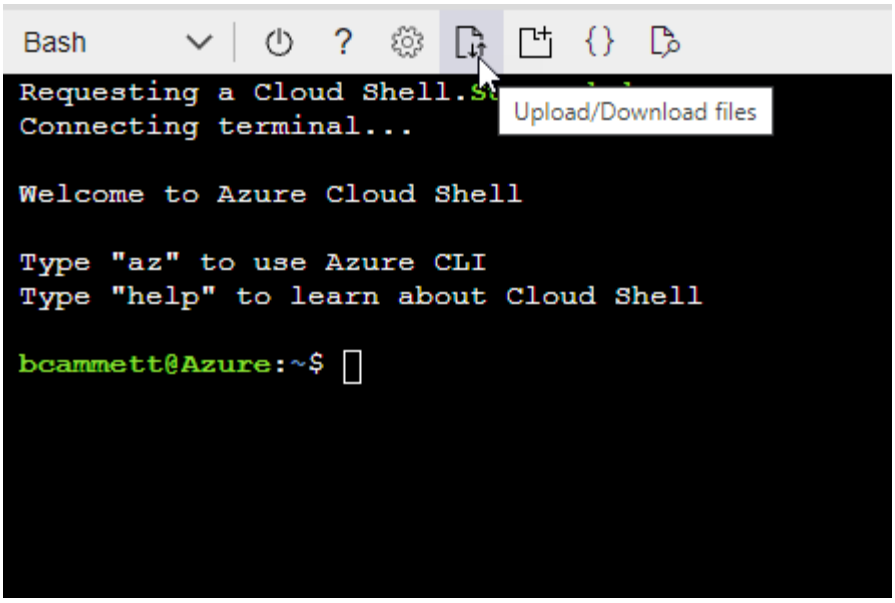
      Exemple

      ```
      "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.



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

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

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

2. Attribuez 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 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 Linuxhttps://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

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

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 Linuxhttps://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
```

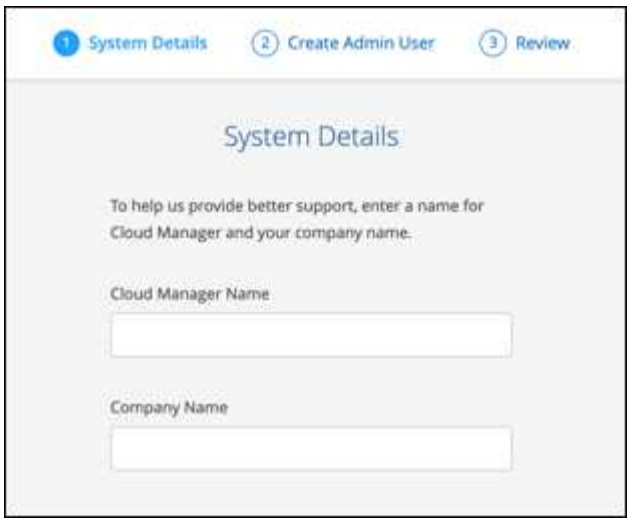
5. Exécutez le script d'installation :

```
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".