Installer un agent sur site

NetApp Console setup and administration

NetApp
January 27, 2026

Sommaire

Installer un agent sur site

Installer manuellement un agent de console sur site

Installez un agent de console sur site, puis connectez-vous et configurez-le pour qu'il fonctionne avec votre organisation de console.

Si vous êtes un utilisateur VMWare, vous pouvez utiliser un OVA pour installer un agent de console dans votre VCenter."En savoir plus sur l'installation d'un agent dans un VCenter."

Avant l'installation, vous devez vous assurer que votre hôte (VM ou hôte Linux) répond aux exigences et que l'agent de la console disposera d'un accès sortant à Internet ainsi qu'aux réseaux ciblés. Si vous envisagez d'utiliser des services de données NetApp ou des options de stockage cloud telles que Cloud Volumes ONTAP, vous devrez créer des informations d'identification auprès de votre fournisseur de cloud à ajouter à la console afin que l'agent de la console puisse effectuer des actions dans le cloud en votre nom.

Préparez-vous à installer l'agent de la console

Avant d'installer un agent de console, vous devez vous assurer que vous disposez d'une machine hôte qui répond aux exigences d'installation. Vous devrez également travailler avec votre administrateur réseau pour vous assurer que l'agent de la console dispose d'un accès sortant aux points de terminaison requis et aux connexions aux réseaux ciblés.

Examen des exigences de l'hôte de l'agent de console

Exécutez l'agent de console sur un hôte x86 qui répond aux exigences du système d'exploitation, de la RAM et du port. Assurez-vous que votre hôte répond à ces exigences avant d'installer l'agent de console.

L'agent de console réserve la plage UID et GID de 19 000 à 19 200. Cette plage est fixe et ne peut pas être modifiée. Si un logiciel tiers sur votre hôte utilise des UID ou des GID dans cette plage, l'installation de l'agent échouera. NetApp recommande d'utiliser un hôte exempt de logiciels tiers pour éviter les conflits.

Hôte dédié

L'agent Console nécessite un hôte dédié. Toute architecture est prise en charge si elle répond aux exigences de taille suivantes :

- CPU : 8 cœurs ou 8 vCPU
- RAM : 32 Go
- Espace disque : 165 Go sont recommandés pour l'hôte, avec les exigences de partition suivantes :
  - `/opt`: 120 Go d'espace doivent être disponibles

    L'agent utilise `/opt` pour installer le `/opt/application/netapp` répertoire et son contenu.

  - `/var`: 40 Go d'espace doivent être disponibles

    L'agent Console a besoin de cet espace dans `/var` car Podman ou Docker sont conçus pour créer les conteneurs dans ce répertoire. Plus précisément, ils créeront des conteneurs dans le `/var/lib/containers/storage` répertoire et `/var/lib/docker` pour Docker. Les montages

externes ou les liens symboliques ne fonctionnent pas pour cet espace.

Hyperviseur

Un hyperviseur bare metal ou hébergé certifié pour exécuter un système d'exploitation pris en charge est requis.

Exigences relatives au système d'exploitation et aux conteneurs

L'agent de console est pris en charge avec les systèmes d'exploitation suivants lors de l'utilisation de la console en mode standard ou en mode restreint. Un outil d'orchestration de conteneurs est requis avant d'installer l'agent.

Système opérateur	Versions de systèmes d'exploitation prises en charge	Versions d'agent prises en charge	Outil de conteneur requis	SELinux
Red Hat Enterprise Linux		9,6 • Versions en langue anglaise uniquement. • L'hôte doit être enregistré auprès de Red Hat Subscription Management. S'il n'est pas enregistré, l'hôte ne peut pas accéder aux référentiels pour mettre à jour le logiciel tiers requis lors de l'installation de l'agent.	4.0.0 ou version ultérieure avec la console en mode standard ou en mode restreint	Podman version 5.4.0 avec podman-compose 1.5.0. Afficher les exigences de configuration de Podman .

Système opérateur	Versions de systèmes d'exploitation prises en charge	Versions d'agent prises en charge	Outil de conteneur requis	SELinux
Pris en charge en mode d'application ou en mode permissif		9,1 à 9,4 • Versions en langue anglaise uniquement. • L'hôte doit être enregistré auprès de Red Hat Subscription Management. S'il n'est pas enregistré, l'hôte ne peut pas accéder aux référentiels pour mettre à jour le logiciel tiers requis lors de l'installation de l'agent.	3.9.50 ou version ultérieure avec la console en mode standard ou en mode restreint	Podman version 4.9.4 avec podman-compose 1.5.0. Afficher les exigences de configuration de Podman .
Pris en charge en mode d'application ou en mode permissif		8,6 à 8,10 • Versions en langue anglaise uniquement. • L'hôte doit être enregistré auprès de Red Hat Subscription Management. S'il n'est pas enregistré, l'hôte ne peut pas accéder aux référentiels pour mettre à jour le logiciel tiers requis lors de l'installation de l'agent.	3.9.50 ou version ultérieure avec la console en mode standard ou en mode restreint	Podman version 4.6.1 ou 4.9.4 avec podman-compose 1.0.6. Afficher les exigences de configuration de Podman .
Pris en charge en mode d'application ou en mode permissif	Ubuntu		24,04 LTS	3.9.45 ou version ultérieure avec la NetApp Console en mode standard ou en mode restreint

Système opérateur	Versions de systèmes d'exploitation prises en charge	Versions d'agent prises en charge	Outil de conteneur requis	SELinux
Docker Engine 23.06 à 28.0.0.	Non pris en charge		22,04 LTS	3.9.50 ou version ultérieure

Configurer l'accès réseau pour l'agent de la console

Configurez l'accès au réseau pour garantir que l'agent de la console peut gérer les ressources. Il a besoin de connexions aux réseaux cibles et d'un accès Internet sortant vers des points de terminaison spécifiques.

Connexions aux réseaux cibles

L'agent de console nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des systèmes. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement local.

Accès Internet sortant

L'emplacement réseau où vous déployez l'agent de console doit disposer d'une connexion Internet sortante pour contacter des points de terminaison spécifiques.

Points de terminaison contactés à partir d'ordinateurs lors de l'utilisation de la NetApp Console

Les ordinateurs qui accèdent à la console à partir d'un navigateur Web doivent avoir la possibilité de contacter plusieurs points de terminaison. Vous devrez utiliser la console pour configurer l'agent de la console et pour l'utilisation quotidienne de la console.

"Préparer la mise en réseau pour la console NetApp" .

Points de terminaison contactés depuis l'agent de la console

L'agent de console nécessite un accès Internet sortant pour contacter les points de terminaison suivants afin de gérer les ressources et les processus au sein de votre environnement de cloud public pour les opérations quotidiennes.

Les points de terminaison répertoriés ci-dessous sont tous des entrées CNAME.

Un agent de console installé sur vos locaux ne peut pas gérer les ressources dans Google Cloud. Si vous souhaitez gérer les ressources Google Cloud, vous devez installer un agent dans Google Cloud.

AWS

Lorsque l'agent de console est installé sur site, il a besoin d'un accès réseau aux points de terminaison AWS suivants afin de gérer les systèmes NetApp (tels que Cloud Volumes ONTAP) déployés dans AWS.

Points de terminaison contactés depuis l'agent de la console

L'agent de console nécessite un accès Internet sortant pour contacter les points de terminaison suivants afin de gérer les ressources et les processus au sein de votre environnement de cloud public pour les opérations quotidiennes.

Les points de terminaison répertoriés ci-dessous sont tous des entrées CNAME.

Points de terminaison	But
Services AWS (amazonaws.com) : • CloudFormation • Cloud de calcul élastique (EC2) • Gestion des identités et des accès (IAM) • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Service de stockage simple (S3)	Pour gérer les ressources AWS. Le point de terminaison dépend de votre région AWS. "Consultez la documentation AWS pour plus de détails"
Amazon FSX pour NetApp ONTAP: • api.workloads.netapp.com	La console Web contacte ce point de terminaison pour interagir avec les API Workload Factory afin de gérer et d'exploiter les charges de travail basées sur FSx pour ONTAP .
\ https://mysupport.netapp.com	Pour obtenir des informations de licence et envoyer des messages AutoSupport au support NetApp .
\ https://signin.b2c.netapp.com	Pour mettre à jour les informations d'identification du site de support NetApp (NSS) ou pour ajouter de nouvelles informations d'identification NSS à la NetApp Console.
\ https://support.netapp.com	Pour obtenir des informations de licence et envoyer des messages AutoSupport au support NetApp ainsi que pour recevoir des mises à jour logicielles pour Cloud Volumes ONTAP.

Points de terminaison	But
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Pour fournir des fonctionnalités et des services au sein de la NetApp Console.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Pour obtenir des images pour les mises à niveau de l'agent de console. • Lorsque vous déployez un nouvel agent, le contrôle de validation teste la connectivité aux points de terminaison actuels. Si vous utilisez"points finaux précédents" , le contrôle de validation échoue. Pour éviter cet échec, ignorez la vérification de validation. Bien que les points de terminaison précédents soient toujours pris en charge, NetApp recommande de mettre à jour vos règles de pare-feu vers les points de terminaison actuels dès que possible. "Apprenez à mettre à jour votre liste de points de terminaison" . • Lorsque vous effectuez une mise à jour vers les points de terminaison actuels de votre pare-feu, vos agents existants continueront de fonctionner.

Azuré

Lorsque l'agent de console est installé sur site, il a besoin d'un accès réseau aux points de terminaison Azure suivants afin de gérer les systèmes NetApp (tels que Cloud Volumes ONTAP) déployés dans Azure.

Points de terminaison	But
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Pour gérer les ressources dans les régions publiques Azure.

Points de terminaison	But
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Pour gérer les ressources dans les régions Azure Chine.
\ https://mysupport.netapp.com	Pour obtenir des informations de licence et envoyer des messages AutoSupport au support NetApp .
\ https://signin.b2c.netapp.com	Pour mettre à jour les informations d'identification du site de support NetApp (NSS) ou pour ajouter de nouvelles informations d'identification NSS à la NetApp Console.
\ https://support.netapp.com	Pour obtenir des informations de licence et envoyer des messages AutoSupport au support NetApp ainsi que pour recevoir des mises à jour logicielles pour Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Pour fournir des fonctionnalités et des services au sein de la NetApp Console.

Points de terminaison	But
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Pour obtenir des images pour les mises à niveau de l'agent de console. • Lorsque vous déployez un nouvel agent, le contrôle de validation teste la connectivité aux points de terminaison actuels. Si vous utilisez"points finaux précédents" , le contrôle de validation échoue. Pour éviter cet échec, ignorez la vérification de validation. Bien que les points de terminaison précédents soient toujours pris en charge, NetApp recommande de mettre à jour vos règles de pare-feu vers les points de terminaison actuels dès que possible. "Apprenez à mettre à jour votre liste de points de terminaison" . • Lorsque vous effectuez une mise à jour vers les points de terminaison actuels de votre pare-feu, vos agents existants continueront de fonctionner.

Serveur proxy

NetApp prend en charge les configurations de proxy explicites et transparentes. Si vous utilisez un proxy transparent, vous devez uniquement fournir le certificat du serveur proxy. Si vous utilisez un proxy explicite, vous aurez également besoin de l'adresse IP et des informations d'identification.

- adresse IP
- Informations d'identification
- Certificat HTTPS

Ports

Il n'y a aucun trafic entrant vers l'agent de console, sauf si vous l'initiez ou s'il est utilisé comme proxy pour envoyer des messages AutoSupport de Cloud Volumes ONTAP au support NetApp .

- HTTP (80) et HTTPS (443) donnent accès à l'interface utilisateur locale, que vous utiliserez dans de rares circonstances.
- SSH (22) n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

- Les connexions entrantes via le port 3128 sont requises si vous déployez des systèmes Cloud Volumes ONTAP dans un sous-réseau où une connexion Internet sortante n'est pas disponible.

  Si les systèmes Cloud Volumes ONTAP ne disposent pas d'une connexion Internet sortante pour envoyer des messages AutoSupport , la console configure automatiquement ces systèmes pour utiliser un serveur proxy inclus avec l'agent de la console. La seule exigence est de s'assurer que le groupe de sécurité de l'agent de console autorise les connexions entrantes sur le port 3128. Vous devrez ouvrir ce port après avoir déployé l'agent de console.

Activer NTP

Si vous prévoyez d'utiliser NetApp Data Classification pour analyser vos sources de données d'entreprise, vous devez activer un service NTP (Network Time Protocol) sur l'agent de console et sur le système NetApp Data Classification afin que l'heure soit synchronisée entre les systèmes. "En savoir plus sur la classification des données NetApp"

Créer des autorisations cloud pour l'agent de console pour AWS ou Azure

Si vous souhaitez utiliser les services de données NetApp dans AWS ou Azure avec un agent de console sur site, vous devez configurer les autorisations dans votre fournisseur de cloud, puis ajouter les informations d'identification à l'agent de console après l'avoir installé.

Vous devez installer l'agent de console dans Google Cloud pour gérer toutes les ressources qui y résident.

AWS

Lorsque l'agent de console est installé sur site, vous devez fournir à la console des autorisations AWS en ajoutant des clés d'accès pour un utilisateur IAM disposant des autorisations requises.

Vous devez utiliser cette méthode d'authentification si l'agent de console est installé sur site. Vous ne pouvez pas utiliser un rôle IAM.

Étapes

1. Connectez-vous à la console AWS et accédez au service IAM.
2. Créer une politique:

   a. Sélectionnez **Politiques > Créer une politique**.

   b. Sélectionnez **JSON** et copiez et collez le contenu du"Politique IAM pour l'agent de console" .

   c. Terminez les étapes restantes pour créer la politique.

      Selon les services de données NetApp que vous prévoyez d'utiliser, vous devrez peut-être créer une deuxième stratégie.

   Pour les régions standard, les autorisations sont réparties sur deux politiques. Deux politiques sont requises en raison d'une limite de taille maximale de caractères pour les politiques gérées dans AWS. "En savoir plus sur les stratégies IAM pour l'agent de console" .

3. Attachez les politiques à un utilisateur IAM.
   - "Documentation AWS : Création de rôles IAM"
   - "Documentation AWS : Ajout et suppression de stratégies IAM"
4. Assurez-vous que l'utilisateur dispose d'une clé d'accès que vous pouvez ajouter à la NetApp Console après avoir installé l'agent de console.

Résultat

Vous devriez maintenant disposer des clés d'accès pour un utilisateur IAM disposant des autorisations requises. Après avoir installé l'agent de console, associez ces informations d'identification à l'agent de console à partir de la console.

Azuré

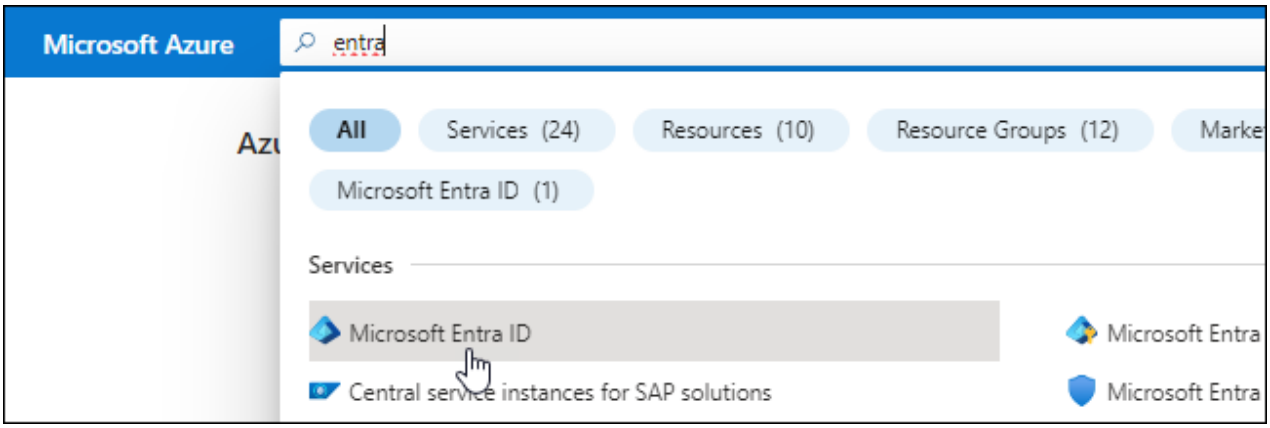
Lorsque l'agent de console est installé sur site, vous devez fournir à l'agent de console des autorisations Azure en configurant un principal de service dans Microsoft Entra ID et en obtenant les informations d'identification Azure dont l'agent de console a besoin.

Créer une application Microsoft Entra pour le contrôle d'accès basé sur les rôles

1. Assurez-vous que vous disposez des autorisations dans Azure pour créer une application Active Directory et attribuer l'application à un rôle.

   Pour plus de détails, reportez-vous à "Documentation Microsoft Azure : autorisations requises"

2. Depuis le portail Azure, ouvrez le service **Microsoft Entra ID**.



3. Dans le menu, sélectionnez **Inscriptions d'applications**.
4. Sélectionnez **Nouvelle inscription**.
5. Précisez les détails de l'application :
   - **Nom**: Saisissez un nom pour l'application.
   - **Type de compte** : sélectionnez un type de compte (n'importe lequel fonctionnera avec la NetApp Console).
   - **URI de redirection**: Vous pouvez laisser ce champ vide.
6. Sélectionnez **S'inscrire**.

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

Affecter l'application à un rôle

1. Créer un rôle personnalisé :

   Notez que vous pouvez créer un rôle personnalisé Azure à l'aide du portail Azure, d'Azure PowerShell, d'Azure CLI ou de l'API REST. Les étapes suivantes montrent comment créer le rôle à l'aide de l'interface de ligne de commande Azure. Si vous préférez utiliser une méthode différente, reportez-vous à "Documentation Azure"

   a. Copiez le contenu du"autorisations de rôle personnalisées pour l'agent de la console" et les enregistrer dans un fichier JSON.

   b. Modifiez le fichier JSON en ajoutant des ID d'abonnement Azure à l'étendue attribuable.

      Vous devez ajouter l'ID de chaque abonnement Azure à partir duquel les utilisateurs créeront des systèmes Cloud Volumes ONTAP .

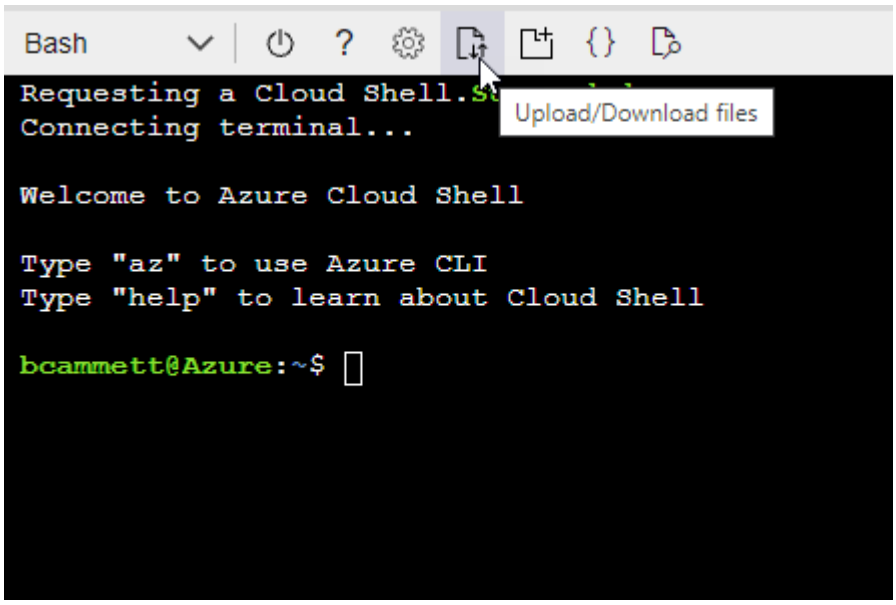
      Exemple

      ```
      "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 décrivent comment créer le rôle à l'aide de Bash dans Azure Cloud Shell.

- Commencer "Azure Cloud Shell" et choisissez l'environnement Bash.
- Téléchargez le fichier JSON.



- Utilisez l'interface de ligne de commande Azure pour créer le rôle personnalisé :

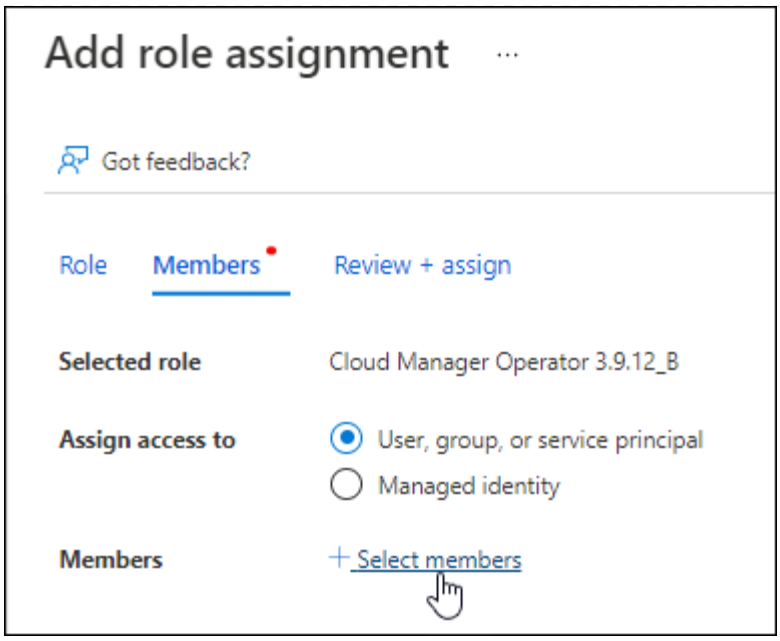
```
az role definition create --role-definition agent_Policy.json
```

Vous devriez maintenant avoir un rôle personnalisé appelé Opérateur de console que vous pouvez attribuer à la machine virtuelle de l'agent de console.

2. Affecter l'application au rôle :

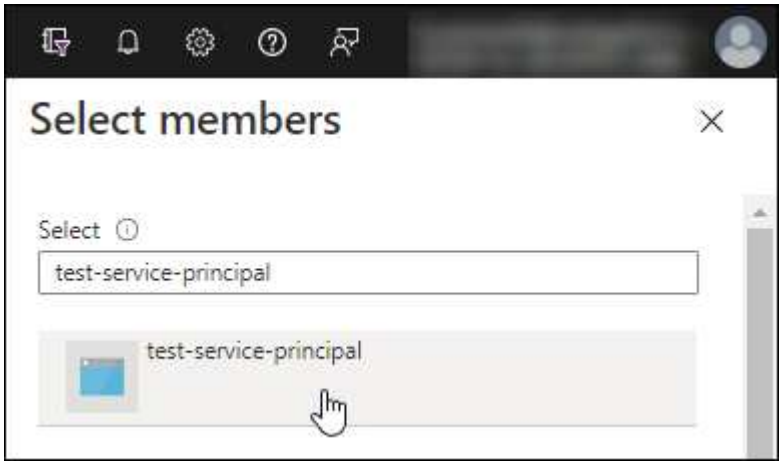
a. Depuis le portail Azure, ouvrez le service **Abonnements**.
b. Sélectionnez l'abonnement.
c. Sélectionnez **Contrôle d'accès (IAM) > Ajouter > Ajouter une attribution de rôle**.
d. Dans l'onglet **Rôle**, sélectionnez le rôle **Opérateur de console** et sélectionnez **Suivant**.
e. Dans l'onglet **Membres**, procédez comme suit :

- Gardez **Utilisateur, groupe ou principal du service** sélectionné.
- Sélectionnez **Sélectionner les membres**.



- Recherchez le nom de l'application.

  Voici un exemple :



- Sélectionnez l'application et sélectionnez **Sélectionner**.
- Sélectionnez **Suivant**.

f. Sélectionnez **Réviser + attribuer**.

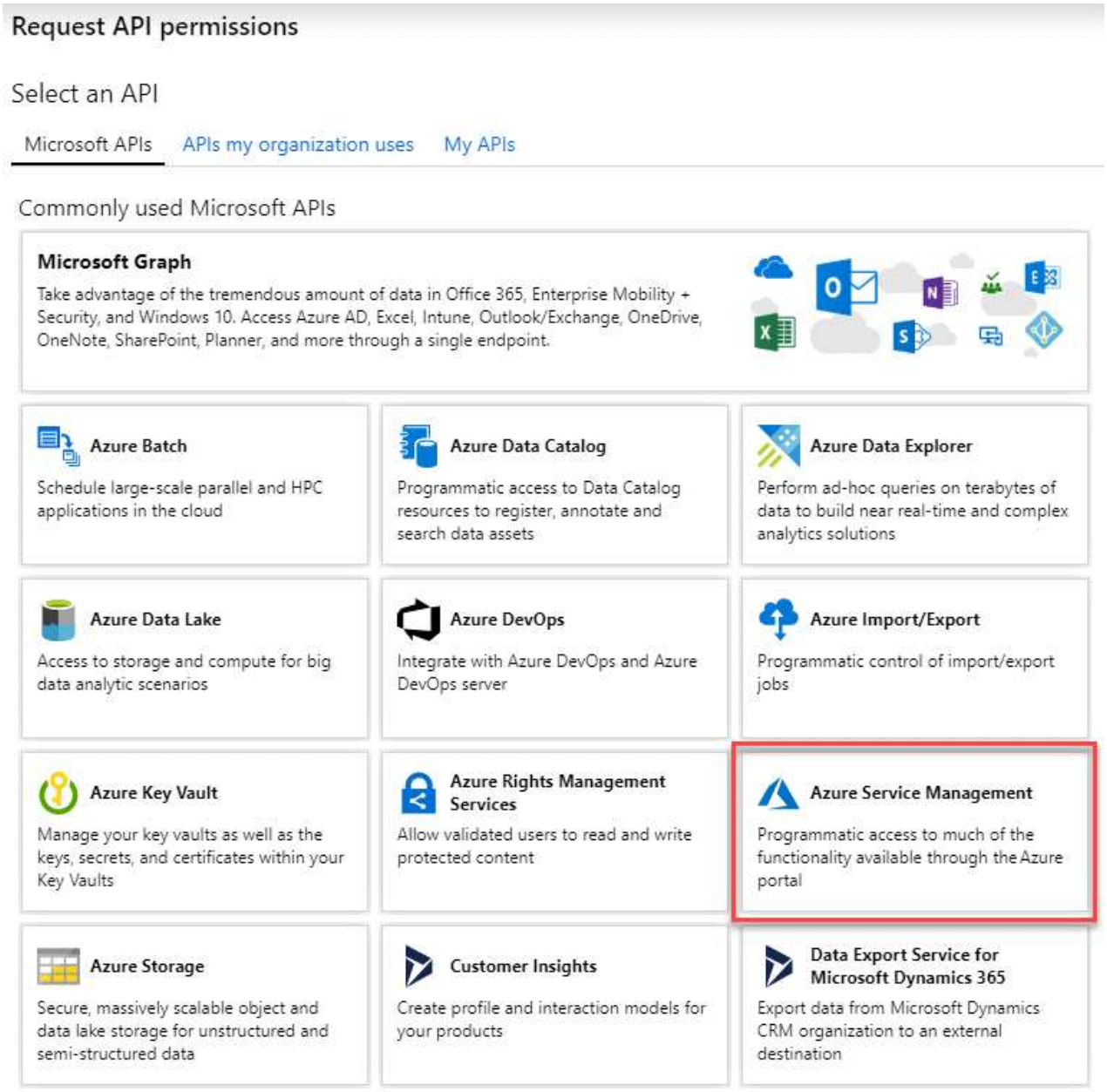
Le principal du service dispose désormais des autorisations Azure requises pour déployer l'agent de la console.

Si vous souhaitez déployer Cloud Volumes ONTAP à partir de plusieurs abonnements Azure, vous devez lier le principal de service à chacun de ces abonnements. Dans la NetApp Console, vous pouvez sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

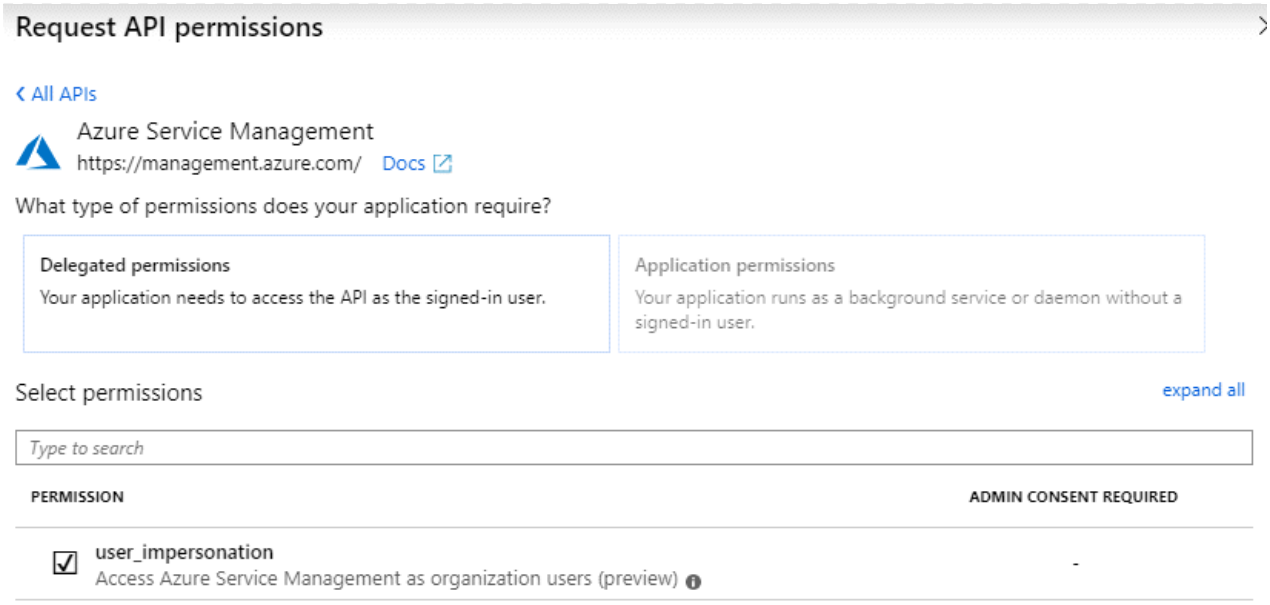
Ajouter des autorisations à l'API Windows Azure Service Management

1. Dans le service **Microsoft Entra ID**, sélectionnez **Inscriptions d'applications** et sélectionnez l'application.

2. Sélectionnez **Autorisations API > Ajouter une autorisation**.
3. Sous **API Microsoft**, sélectionnez **Azure Service Management**.

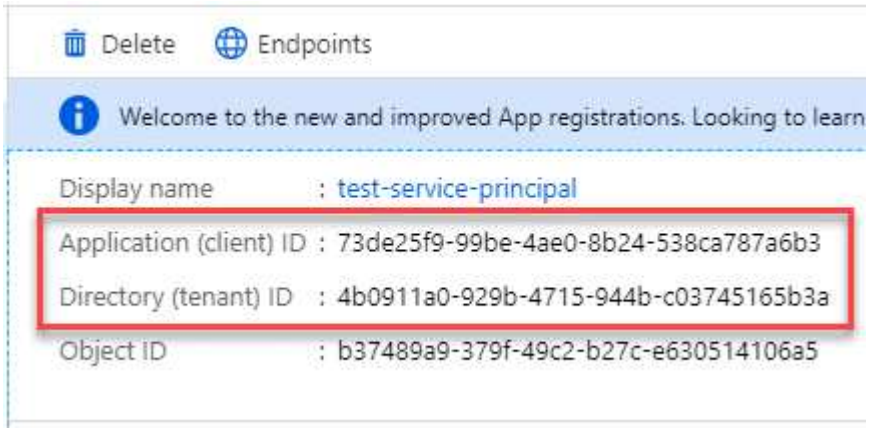


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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

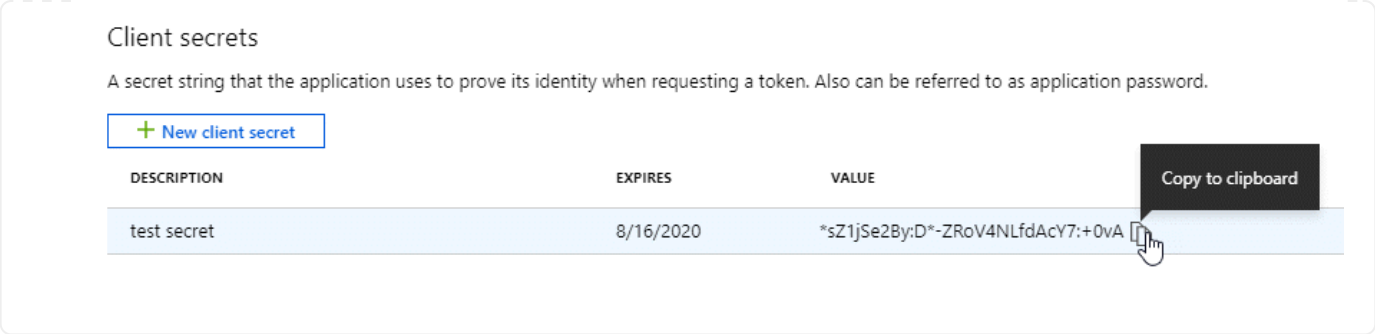
1. Dans le service **Microsoft Entra ID**, sélectionnez **Inscriptions d'applications** et sélectionnez l'application.
2. Copiez l'**ID d'application (client)** et l'**ID de répertoire (locataire)**.



Lorsque vous ajoutez le compte Azure à la console, vous devez fournir l'ID d'application (client) et l'ID de répertoire (locataire) de l'application. La console utilise les identifiants pour se connecter par programmation.

Créer un secret client

1. Ouvrez le service **Microsoft Entra ID**.
2. Sélectionnez **Inscriptions d'applications** et sélectionnez votre application.
3. Sélectionnez **Certificats et secrets > Nouveau secret client**.
4. Fournissez une description du secret et une durée.
5. Sélectionnez **Ajouter**.
6. Copiez la valeur du secret client.



Installer manuellement un agent de console

Lorsque vous installez manuellement un agent de console, vous devez préparer l'environnement de votre machine afin qu'il réponde aux exigences. Vous aurez besoin d'une machine Linux et vous devrez installer Podman ou Docker, selon votre système d'exploitation Linux.

Installer Podman ou Docker Engine

Selon votre système d'exploitation, Podman ou Docker Engine est requis avant l'installation de l'agent.

- Podman est requis pour Red Hat Enterprise Linux 8 et 9.

  Afficher les versions de Podman prises en charge .

- Docker Engine est requis pour Ubuntu.

  Afficher les versions de Docker Engine prises en charge .

Exemple 1. Étapes

Podman

Suivez ces étapes pour installer et configurer Podman :

- Activer et démarrer le service podman.socket
- Installer Python 3
- Installer le package podman-compose version 1.0.6
- Ajoutez podman-compose à la variable d'environnement PATH
- Si vous utilisez Red Hat Enterprise Linux, vérifiez que votre version Podman utilise Netavark Aardvark DNS au lieu de CNI

Ajustez le port aardvark-dns (par défaut : 53) après l'installation de l'agent pour éviter les conflits de port DNS. Suivez les instructions pour configurer le port.

Étapes

1. Supprimez le package podman-docker s'il est installé sur l'hôte.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Installez Podman.

   Vous pouvez obtenir Podman à partir des référentiels officiels de Red Hat Enterprise Linux.

   a. Pour Red Hat Enterprise Linux 9,6 :

   ```
   sudo dnf install podman-5:<version>
   ```

   Où <version> est la version prise en charge de Podman que vous installez. Afficher les versions de Podman prises en charge .

   b. Pour Red Hat Enterprise Linux 9.1 à 9.4 :

   ```
   sudo dnf install podman-4:<version>
   ```

   Où <version> est la version prise en charge de Podman que vous installez. Afficher les versions de Podman prises en charge .

   c. Pour Red Hat Enterprise Linux 8 :

   ```
   sudo dnf install podman-4:<version>
   ```

   Où <version> est la version prise en charge de Podman que vous installez. Afficher les versions de Podman prises en charge .

3. Activez et démarrez le service podman.socket.

```
sudo systemctl enable --now podman.socket
```

4. Installez python3.

```
sudo dnf install python3
```

5. Installez le package de référentiel EPEL s'il n'est pas déjà disponible sur votre système.

   Cette étape est nécessaire car podman-compose est disponible dans le référentiel Extra Packages for Enterprise Linux (EPEL).

6. Si vous utilisez Red Hat Enterprise 9 :

   a. Installez le paquetage du dépôt EPEL.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

   +

   a. Installez le package podman-compose 1.5.0.

```
sudo dnf install podman-compose-1.5.0
```

7. Si vous utilisez Red Hat Enterprise Linux 8 :

   a. Installez le paquetage du dépôt EPEL.

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

   b. Installez le package podman-compose 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```

   En utilisant le `dnf install` la commande répond à l'exigence d'ajout de podman-compose à la variable d'environnement PATH. La commande d'installation ajoute podman-compose à /usr/bin, qui est déjà inclus dans le `secure_path` option sur l'hôte.

   c. Si vous utilisez Red Hat Enterprise Linux 8, vérifiez que votre version Podman utilise NetAvark avec Aardvark DNS au lieu de CNI.

i. Vérifiez si votre networkBackend est défini sur CNI en exécutant la commande suivante :

```
podman info | grep networkBackend
```

ii. Si le networkBackend est défini sur `CNI` , vous devrez le changer en `netavark` .

iii. Installer `netavark` et `aardvark-dns` en utilisant la commande suivante :

```
dnf install aardvark-dns netavark
```

iv. Ouvrez le `/etc/containers/containers.conf` fichier et modifiez l'option network_backend pour utiliser « netavark » au lieu de « cni ».

Si `/etc/containers/containers.conf` n'existe pas, effectuez les modifications de configuration pour `/usr/share/containers/containers.conf` .

v. Redémarrez podman.

```
systemctl restart podman
```

vi. Confirmez que networkBackend est désormais modifié en « netavark » à l'aide de la commande suivante :

```
podman info | grep networkBackend
```

Moteur Docker

Suivez la documentation de Docker pour installer Docker Engine.

Étapes

1. "Afficher les instructions d'installation depuis Docker"

   Suivez les étapes pour installer une version de Docker Engine prise en charge. N'installez pas la dernière version, car elle n'est pas prise en charge par la console.

2. Vérifiez que Docker est activé et en cours d'exécution.

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

Installer l'agent de console manuellement

Téléchargez et installez le logiciel de l'agent de console sur un hôte Linux existant sur site.

Avant de commencer

Vous devriez avoir les éléments suivants :

- Privilèges root pour installer l'agent de la console.
- Détails sur un serveur proxy, si un proxy est requis pour l'accès Internet à partir de l'agent de la console.

  Vous avez la possibilité de configurer un serveur proxy après l'installation, mais cela nécessite le redémarrage de l'agent de la console.

- Un certificat signé par une autorité de certification, si le serveur proxy utilise HTTPS ou si le proxy est un proxy d'interception.

> Vous ne pouvez pas définir de certificat pour un serveur proxy transparent lors de l'installation manuelle de l'agent de console. Si vous devez définir un certificat pour un serveur proxy transparent, vous devez utiliser la console de maintenance après l'installation. En savoir plus sur le"Console de maintenance des agents" .

À propos de cette tâche

Après l'installation, l'agent de la console se met automatiquement à jour si une nouvelle version est disponible.

Étapes

1. Si les variables système *http_proxy* ou *https_proxy* sont définies sur l'hôte, supprimez-les :

   ```
   unset http_proxy
   unset https_proxy
   ```

   Si vous ne supprimez pas ces variables système, l'installation échoue.

2. Téléchargez le logiciel agent Console puis copiez-le sur l'hôte Linux. Vous pouvez le télécharger soit depuis la NetApp Console , soit depuis le site d'assistance NetApp .
   - NetApp Console: Accédez à **Agents > Gestion > Déployer l'agent > Sur site > Installation manuelle**.

     Choisissez de télécharger les fichiers d'installation de l'agent ou une URL vers ces fichiers.

   - Site d'assistance NetApp (nécessaire si vous n'avez pas déjà accès à la console) "Site de support NetApp" ,
3. Attribuer des autorisations pour exécuter le script.

   ```
   chmod +x NetApp_Console_Agent_Cloud_<version>
   ```

   Où <version> est la version de l'agent de console que vous avez téléchargé.

4. Si vous effectuez l'installation dans un environnement Government Cloud, désactivez les vérifications de configuration."Découvrez comment désactiver les vérifications de configuration pour les installations manuelles."
5. Exécutez le script d'installation.

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

Vous devrez ajouter les informations de proxy si votre réseau nécessite un proxy pour accéder à Internet. Vous pouvez ajouter un proxy explicite lors de l'installation. Les `--proxy` et `--cacert` paramètres sont facultatifs et il ne vous sera pas demandé de les ajouter. Si vous avez un serveur proxy explicite, vous devrez saisir les paramètres comme indiqué.

Si vous souhaitez configurer un proxy transparent, vous pouvez le faire après l'installation. "Découvrez la console de maintenance des agents"

+

Voici un exemple de configuration d'un serveur proxy explicite avec un certificat signé par une autorité de certification :

+

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert /tmp/cacert/certificate.cer
```

+
`--proxy` configure l'agent de la Console pour utiliser un serveur proxy HTTP ou HTTPS en utilisant l'un des formats suivants :

+ * http://adresse:port * http://nom-utilisateur:mot-de-passe@adresse:port * http://nom-de-domaine%92nom-utilisateur:mot-de-passe@adresse:port * https://adresse:port * https://nom-utilisateur:mot-de-passe@adresse:port * https://nom-de-domaine%92nom-utilisateur:mot-de-passe@adresse:port

+ Notez ce qui suit :

+ **L'utilisateur peut être un utilisateur local ou un utilisateur de domaine.** Pour un utilisateur de domaine, vous devez utiliser le code ASCII pour une \ comme indiqué ci-dessus. **L'agent Console ne prend pas en charge les noms d'utilisateur ni les mots de passe qui incluent le caractère @.** Si le mot de passe inclut l'un des caractères spéciaux suivants, vous devez échapper ce caractère spécial en le faisant précéder d'une barre oblique inverse : & ou !

+ Par exemple :

+ http://bxpproxyuser:netapp1\!@address:3128

1. Si vous avez utilisé Podman, vous devrez ajuster le port aardvark-dns.

   a. Connectez-vous en SSH à la machine virtuelle de l'agent de console.

   b. Ouvrez le fichier podman */usr/share/containers/containers.conf* et modifiez le port choisi pour le service DNS Aardvark. Par exemple, changez-le en 54.

      ```
      vi /usr/share/containers/containers.conf
      ```

Par exemple:

```
# Port to use for dns forwarding daemon with netavark in rootful bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services should
# run on the machine.
#
dns_bind_port = 54
```

a. Redémarrez la machine virtuelle de l'agent de console.

Quelle est la prochaine étape ?

Vous devrez enregistrer l'agent de console dans la NetApp Console.

Enregistrer l'agent de console auprès de la NetApp Console

Connectez-vous à la console et associez l'agent de la console à votre organisation. La manière dont vous vous connectez dépend du mode dans lequel vous utilisez la console. Si vous utilisez la console en mode standard, vous vous connectez via le site Web SaaS. Si vous utilisez la console en mode restreint, vous vous connectez localement à partir de l'hôte de l'agent de la console.

Étapes

1. Ouvrez un navigateur Web et entrez l'URL de l'hôte de l'agent de la console :

   L'URL de l'hôte de la console peut être un hôte local, une adresse IP privée ou une adresse IP publique, selon la configuration de l'hôte. Par exemple, si l'agent de console se trouve dans le cloud public sans adresse IP publique, vous devez saisir une adresse IP privée provenant d'un hôte disposant d'une connexion à l'hôte de l'agent de console.

2. Inscrivez-vous ou connectez-vous.
3. Après vous être connecté, configurez la console :
   a. Spécifiez l'organisation de la console à associer à l'agent de la console.
   b. Entrez un nom pour le système.
   c. Sous **Exécutez-vous dans un environnement sécurisé ?**, gardez le mode restreint désactivé.

      Le mode restreint n'est pas pris en charge lorsque l'agent de console est installé sur site.

   d. Sélectionnez **Commençons**.

Fournir les informations d'identification du fournisseur de cloud à la NetApp Console

Après avoir installé et configuré l'agent de console, ajoutez vos informations d'identification cloud afin que l'agent de console dispose des autorisations requises pour effectuer des actions dans AWS ou Azure.

AWS

Avant de commencer

Si vous venez de créer ces informations d'identification AWS, leur disponibilité peut prendre quelques minutes. Attendez quelques minutes avant d'ajouter les informations d'identification à la console.

Étapes

1. Sélectionnez **Administration > Informations d'identification**.
2. Sélectionnez **Informations d'identification de l'organisation**.
3. Sélectionnez **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
   a. **Emplacement des informations d'identification** : sélectionnez *Amazon Web Services > Agent.
   b. **Définir les informations d'identification** : saisissez une clé d'accès AWS et une clé secrète.
   c. **Abonnement Marketplace** : Associez un abonnement Marketplace à ces informations d'identification en vous abonnant maintenant ou en sélectionnant un abonnement existant.
   d. **Révision** : Confirmez les détails des nouvelles informations d'identification et sélectionnez **Ajouter**.

Vous pouvez désormais accéder à la "NetApp Console" pour commencer à utiliser l'agent de console.

Azuré

Avant de commencer

Si vous venez de créer ces informations d'identification Azure, leur disponibilité peut prendre quelques minutes. Attendez quelques minutes avant d'ajouter les informations d'identification de l'agent de la console.

Étapes

1. Sélectionnez **Administration > Informations d'identification**.
2. Sélectionnez **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
   a. **Emplacement des informations d'identification** : sélectionnez **Microsoft Azure > Agent**.
   b. **Définir les informations d'identification** : saisissez les informations sur le principal du service Microsoft Entra qui accorde les autorisations requises :
      - ID de l'application (client)
      - ID du répertoire (locataire)
      - Secret client
   c. **Abonnement Marketplace** : Associez un abonnement Marketplace à ces informations d'identification en vous abonnant maintenant ou en sélectionnant un abonnement existant.
   d. **Révision** : Confirmez les détails des nouvelles informations d'identification et sélectionnez **Ajouter**.

Résultat

L'agent de la console dispose désormais des autorisations nécessaires pour effectuer des actions dans Azure en votre nom. Vous pouvez désormais accéder à la "NetApp Console" pour commencer à utiliser l'agent de console.

Installer un agent de console sur site à l'aide de VCenter

Si vous êtes un utilisateur VMWare, vous pouvez utiliser un OVA pour installer un agent de console dans votre VCenter. Le téléchargement ou l'URL OVA est disponible via la NetApp Console.

Lorsque vous installez un agent de console avec vos outils VCenter, vous pouvez utiliser la console Web de la machine virtuelle pour effectuer des tâches de maintenance."En savoir plus sur la console VM pour l'agent."

Préparez-vous à installer l'agent de la console

Avant l'installation, assurez-vous que votre hôte de machine virtuelle répond aux exigences et que l'agent de console peut accéder à Internet et aux réseaux ciblés. Pour utiliser les services de données NetApp ou Cloud Volumes ONTAP, créez des informations d'identification de fournisseur de cloud pour que l'agent de la console effectue des actions en votre nom.

Examen des exigences de l'hôte de l'agent de console

Assurez-vous que votre machine hôte répond aux exigences d'installation avant d'installer l'agent de console.

- CPU : 8 cœurs ou 8 vCPU
- RAM : 32 Go
- Espace disque : 165 Go (provisionnement épais)
- vSphere 7.0 ou supérieur
- Hôte ESXi 7.03 ou supérieur

Installez l'agent dans un environnement vCenter plutôt que directement sur un hôte ESXi.

Configurer l'accès réseau pour l'agent de la console

Travaillez avec votre administrateur réseau pour vous assurer que l'agent de la console dispose d'un accès sortant aux points de terminaison requis et aux connexions aux réseaux ciblés.

Connexions aux réseaux cibles

L'agent de console nécessite une connexion réseau à l'emplacement où vous prévoyez de créer et de gérer des systèmes. Par exemple, le réseau sur lequel vous prévoyez de créer des systèmes Cloud Volumes ONTAP ou un système de stockage dans votre environnement local.

Accès Internet sortant

L'emplacement réseau où vous déployez l'agent de console doit disposer d'une connexion Internet sortante pour contacter des points de terminaison spécifiques.

Points de terminaison contactés à partir d'ordinateurs lors de l'utilisation de la NetApp Console

Les ordinateurs qui accèdent à la console à partir d'un navigateur Web doivent avoir la possibilité de contacter plusieurs points de terminaison. Vous devrez utiliser la console pour configurer l'agent de la console et pour l'utilisation quotidienne de la console.

"Préparer la mise en réseau pour la console NetApp" .

Points de terminaison contactés depuis l'agent de la console

L'agent de console nécessite un accès Internet sortant pour contacter les points de terminaison suivants afin de gérer les ressources et les processus au sein de votre environnement de cloud public pour les opérations quotidiennes.

Les points de terminaison répertoriés ci-dessous sont tous des entrées CNAME.

> Vous ne pouvez pas gérer les ressources dans Google Cloud avec un agent de console installé sur vos locaux. Pour gérer les ressources Google Cloud, installez un agent dans Google Cloud.

AWS

Lorsque l'agent de console est installé sur site, il a besoin d'un accès réseau aux points de terminaison AWS suivants afin de gérer les systèmes NetApp (tels que Cloud Volumes ONTAP) déployés dans AWS.

Points de terminaison contactés depuis l'agent de la console

L'agent de console nécessite un accès Internet sortant pour contacter les points de terminaison suivants afin de gérer les ressources et les processus au sein de votre environnement de cloud public pour les opérations quotidiennes.

Les points de terminaison répertoriés ci-dessous sont tous des entrées CNAME.

Points de terminaison	But
Services AWS (amazonaws.com) : • CloudFormation • Cloud de calcul élastique (EC2) • Gestion des identités et des accès (IAM) • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Service de stockage simple (S3)	Pour gérer les ressources AWS. Le point de terminaison dépend de votre région AWS. "Consultez la documentation AWS pour plus de détails"
Amazon FSX pour NetApp ONTAP: • api.workloads.netapp.com	La console Web contacte ce point de terminaison pour interagir avec les API Workload Factory afin de gérer et d'exploiter les charges de travail basées sur FSx pour ONTAP .
\ https://mysupport.netapp.com	Pour obtenir des informations de licence et envoyer des messages AutoSupport au support NetApp .
\ https://signin.b2c.netapp.com	Pour mettre à jour les informations d'identification du site de support NetApp (NSS) ou pour ajouter de nouvelles informations d'identification NSS à la NetApp Console.
\ https://support.netapp.com	Pour obtenir des informations de licence et envoyer des messages AutoSupport au support NetApp ainsi que pour recevoir des mises à jour logicielles pour Cloud Volumes ONTAP.

Points de terminaison	But
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Pour fournir des fonctionnalités et des services au sein de la NetApp Console.
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Pour obtenir des images pour les mises à niveau de l'agent de console. • Lorsque vous déployez un nouvel agent, le contrôle de validation teste la connectivité aux points de terminaison actuels. Si vous utilisez"points finaux précédents" , le contrôle de validation échoue. Pour éviter cet échec, ignorez la vérification de validation. Bien que les points de terminaison précédents soient toujours pris en charge, NetApp recommande de mettre à jour vos règles de pare-feu vers les points de terminaison actuels dès que possible. "Apprenez à mettre à jour votre liste de points de terminaison" . • Lorsque vous effectuez une mise à jour vers les points de terminaison actuels de votre pare-feu, vos agents existants continueront de fonctionner.

Azuré

Lorsque l'agent de console est installé sur site, il a besoin d'un accès réseau aux points de terminaison Azure suivants afin de gérer les systèmes NetApp (tels que Cloud Volumes ONTAP) déployés dans Azure.

Points de terminaison	But
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Pour gérer les ressources dans les régions publiques Azure.

Points de terminaison	But
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Pour gérer les ressources dans les régions Azure Chine.
\ https://mysupport.netapp.com	Pour obtenir des informations de licence et envoyer des messages AutoSupport au support NetApp .
\ https://signin.b2c.netapp.com	Pour mettre à jour les informations d'identification du site de support NetApp (NSS) ou pour ajouter de nouvelles informations d'identification NSS à la NetApp Console.
\ https://support.netapp.com	Pour obtenir des informations de licence et envoyer des messages AutoSupport au support NetApp ainsi que pour recevoir des mises à jour logicielles pour Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Pour fournir des fonctionnalités et des services au sein de la NetApp Console.

Points de terminaison	But
\ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io	Pour obtenir des images pour les mises à niveau de l'agent de console. • Lorsque vous déployez un nouvel agent, le contrôle de validation teste la connectivité aux points de terminaison actuels. Si vous utilisez"points finaux précédents" , le contrôle de validation échoue. Pour éviter cet échec, ignorez la vérification de validation. Bien que les points de terminaison précédents soient toujours pris en charge, NetApp recommande de mettre à jour vos règles de pare-feu vers les points de terminaison actuels dès que possible. "Apprenez à mettre à jour votre liste de points de terminaison" . • Lorsque vous effectuez une mise à jour vers les points de terminaison actuels de votre pare-feu, vos agents existants continueront de fonctionner.

Serveur proxy

NetApp prend en charge les configurations de proxy explicites et transparentes. Si vous utilisez un proxy transparent, vous devez uniquement fournir le certificat du serveur proxy. Si vous utilisez un proxy explicite, vous aurez également besoin de l'adresse IP et des informations d'identification.

- adresse IP
- Informations d'identification
- Certificat HTTPS

Ports

Il n'y a aucun trafic entrant vers l'agent de console, sauf si vous l'initiez ou s'il est utilisé comme proxy pour envoyer des messages AutoSupport de Cloud Volumes ONTAP au support NetApp .

- HTTP (80) et HTTPS (443) donnent accès à l'interface utilisateur locale, que vous utiliserez dans de rares circonstances.
- SSH (22) n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

- Les connexions entrantes via le port 3128 sont requises si vous déployez des systèmes Cloud Volumes ONTAP dans un sous-réseau où une connexion Internet sortante n'est pas disponible.

  Si les systèmes Cloud Volumes ONTAP ne disposent pas d'une connexion Internet sortante pour envoyer des messages AutoSupport , la console configure automatiquement ces systèmes pour utiliser un serveur proxy inclus avec l'agent de la console. La seule exigence est de s'assurer que le groupe de sécurité de l'agent de console autorise les connexions entrantes sur le port 3128. Vous devrez ouvrir ce port après avoir déployé l'agent de console.

Activer NTP

Si vous prévoyez d'utiliser NetApp Data Classification pour analyser vos sources de données d'entreprise, vous devez activer un service NTP (Network Time Protocol) sur l'agent de console et sur le système NetApp Data Classification afin que l'heure soit synchronisée entre les systèmes. "En savoir plus sur la classification des données NetApp"

Créer des autorisations cloud pour l'agent de console pour AWS ou Azure

Si vous souhaitez utiliser les services de données NetApp dans AWS ou Azure avec un agent de console sur site, vous devez configurer des autorisations dans votre fournisseur de cloud afin de pouvoir ajouter les informations d'identification à l'agent de console après son installation.

Vous ne pouvez pas gérer les ressources dans Google Cloud avec un agent de console installé sur vos locaux. Si vous souhaitez gérer les ressources Google Cloud, vous devez installer un agent dans Google Cloud.

AWS

Pour les agents de console sur site, fournissez des autorisations AWS en ajoutant des clés d'accès utilisateur IAM.

Utilisez les clés d'accès utilisateur IAM pour les agents de console sur site ; les rôles IAM ne sont pas pris en charge pour les agents de console sur site.

Étapes

1. Connectez-vous à la console AWS et accédez au service IAM.
2. Créer une politique:

   a. Sélectionnez **Politiques > Créer une politique**.

   b. Sélectionnez **JSON** et copiez et collez le contenu du"Politique IAM pour l'agent de console" .

   c. Terminez les étapes restantes pour créer la politique.

      Selon les services de données NetApp que vous prévoyez d'utiliser, vous devrez peut-être créer une deuxième stratégie.

   Pour les régions standard, les autorisations sont réparties sur deux politiques. Deux politiques sont requises en raison d'une limite de taille maximale de caractères pour les politiques gérées dans AWS. "En savoir plus sur les stratégies IAM pour l'agent de console" .

3. Attachez les politiques à un utilisateur IAM.
   - "Documentation AWS : Création de rôles IAM"
   - "Documentation AWS : Ajout et suppression de stratégies IAM"
4. Assurez-vous que l'utilisateur dispose d'une clé d'accès que vous pouvez ajouter à la NetApp Console après avoir installé l'agent de console.

Résultat

Vous devez maintenant disposer des clés d'accès utilisateur IAM avec les autorisations requises. Après avoir installé l'agent de console, associez ces informations d'identification à l'agent de console à partir de la console.

Azuré

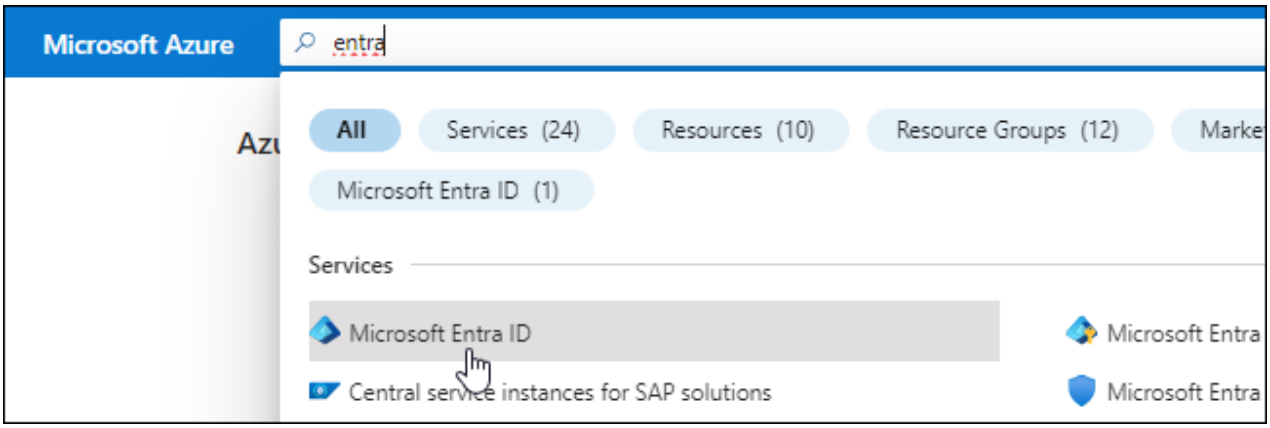
Lorsque l'agent de console est installé sur site, vous devez lui accorder des autorisations Azure en configurant un principal de service dans Microsoft Entra ID et en obtenant les informations d'identification Azure dont l'agent de console a besoin.

Créer une application Microsoft Entra pour le contrôle d'accès basé sur les rôles

1. Assurez-vous que vous disposez des autorisations dans Azure pour créer une application Active Directory et attribuer l'application à un rôle.

   Pour plus de détails, reportez-vous à "Documentation Microsoft Azure : autorisations requises"

2. Depuis le portail Azure, ouvrez le service **Microsoft Entra ID**.



3. Dans le menu, sélectionnez **Inscriptions d'applications**.
4. Sélectionnez **Nouvelle inscription**.
5. Précisez les détails de l'application :
   - **Nom**: Saisissez un nom pour l'application.
   - **Type de compte** : sélectionnez un type de compte (n'importe lequel fonctionnera avec la NetApp Console).
   - **URI de redirection**: Vous pouvez laisser ce champ vide.
6. Sélectionnez **S'inscrire**.

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

Affecter l'application à un rôle

1. Créer un rôle personnalisé :

   Notez que vous pouvez créer un rôle personnalisé Azure à l'aide du portail Azure, d'Azure PowerShell, d'Azure CLI ou de l'API REST. Les étapes suivantes montrent comment créer le rôle à l'aide de l'interface de ligne de commande Azure. Si vous préférez utiliser une méthode différente, reportez-vous à "Documentation Azure"

   a. Copiez le contenu du"autorisations de rôle personnalisées pour l'agent de la console" et les enregistrer dans un fichier JSON.

   b. Modifiez le fichier JSON en ajoutant des ID d'abonnement Azure à l'étendue attribuable.

      Vous devez ajouter l'ID de chaque abonnement Azure à partir duquel les utilisateurs créeront des systèmes Cloud Volumes ONTAP .

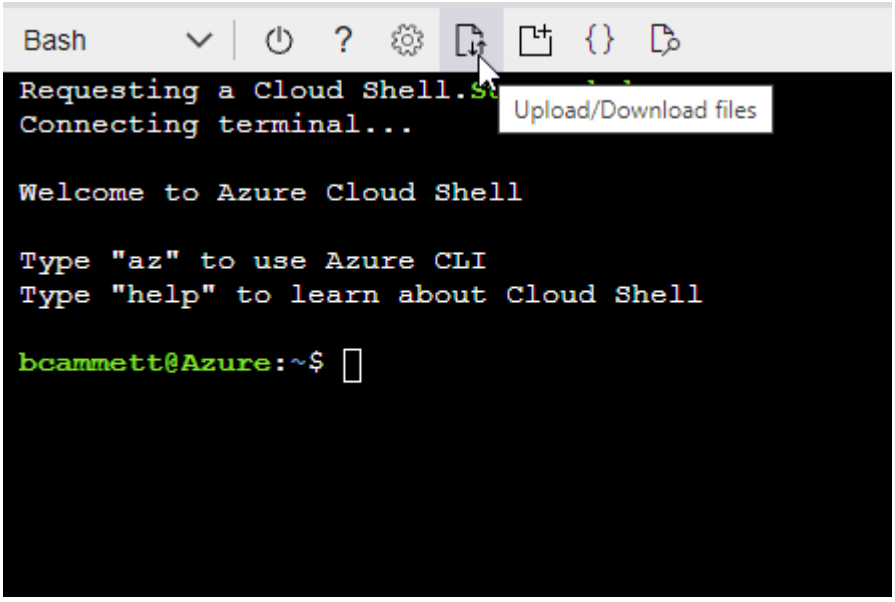
      Exemple

      ```
      "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 décrivent comment créer le rôle à l'aide de Bash dans Azure Cloud Shell.

- Commencer "Azure Cloud Shell" et choisissez l'environnement Bash.
- Téléchargez le fichier JSON.



- Utilisez l'interface de ligne de commande Azure pour créer le rôle personnalisé :

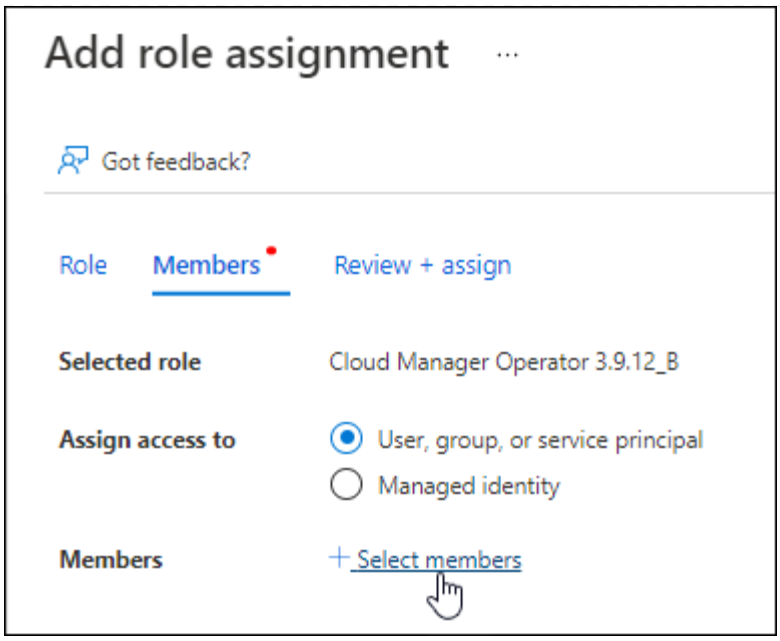
```
az role definition create --role-definition agent_Policy.json
```

Vous devriez maintenant avoir un rôle personnalisé appelé Opérateur de console que vous pouvez attribuer à la machine virtuelle de l'agent de console.

2. Affecter l'application au rôle :

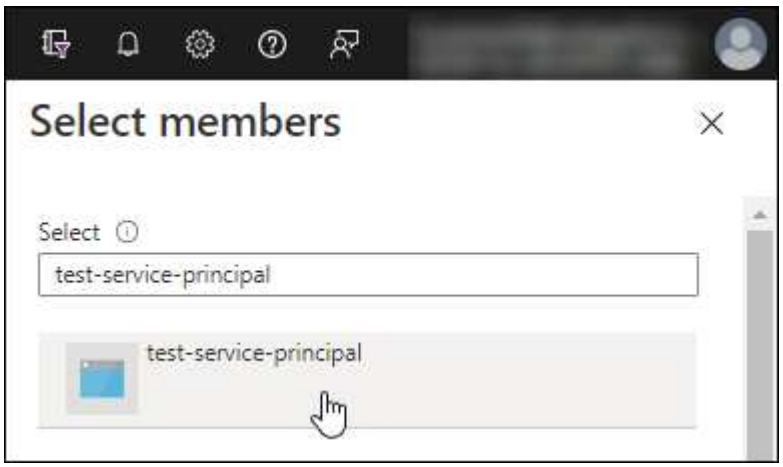
a. Depuis le portail Azure, ouvrez le service **Abonnements**.
b. Sélectionnez l'abonnement.
c. Sélectionnez **Contrôle d'accès (IAM) > Ajouter > Ajouter une attribution de rôle**.
d. Dans l'onglet **Rôle**, sélectionnez le rôle **Opérateur de console** et sélectionnez **Suivant**.
e. Dans l'onglet **Membres**, procédez comme suit :

- Gardez **Utilisateur, groupe ou principal du service** sélectionné.
- Sélectionnez **Sélectionner les membres**.



- Recherchez le nom de l'application.

  Voici un exemple :



- Sélectionnez l'application et sélectionnez **Sélectionner**.
- Sélectionnez **Suivant**.

f. Sélectionnez **Réviser + attribuer**.

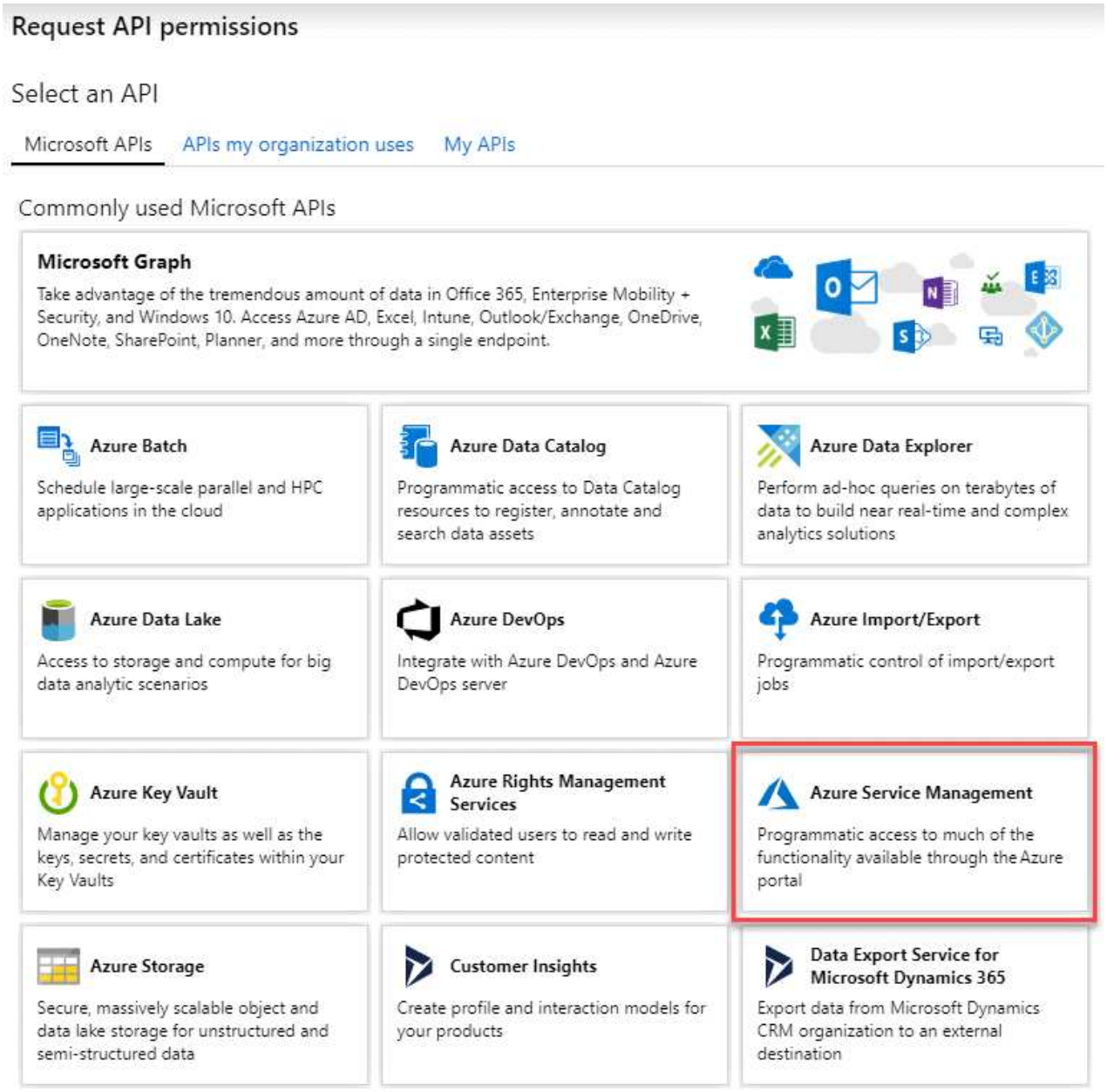
Le principal du service dispose désormais des autorisations Azure requises pour déployer l'agent de la console.

Si vous souhaitez déployer Cloud Volumes ONTAP à partir de plusieurs abonnements Azure, vous devez lier le principal de service à chacun de ces abonnements. Dans la NetApp Console, vous pouvez sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

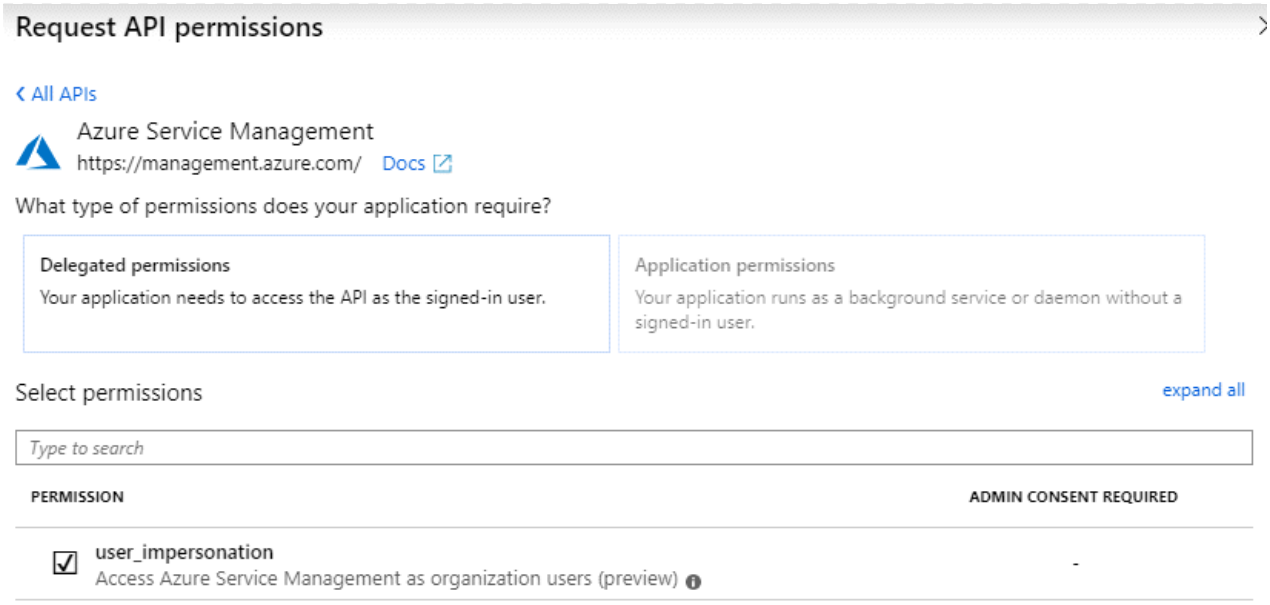
Ajouter des autorisations à l'API Windows Azure Service Management

1. Dans le service **Microsoft Entra ID**, sélectionnez **Inscriptions d'applications** et sélectionnez l'application.

2. Sélectionnez **Autorisations API > Ajouter une autorisation**.
3. Sous **API Microsoft**, sélectionnez **Azure Service Management**.

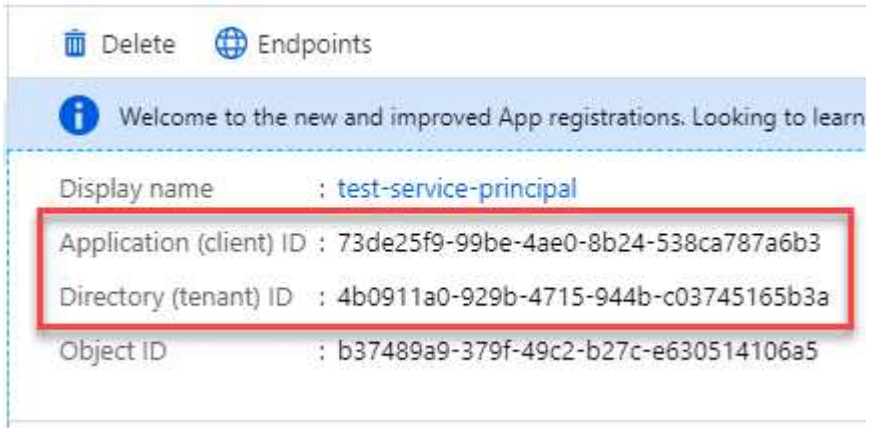


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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

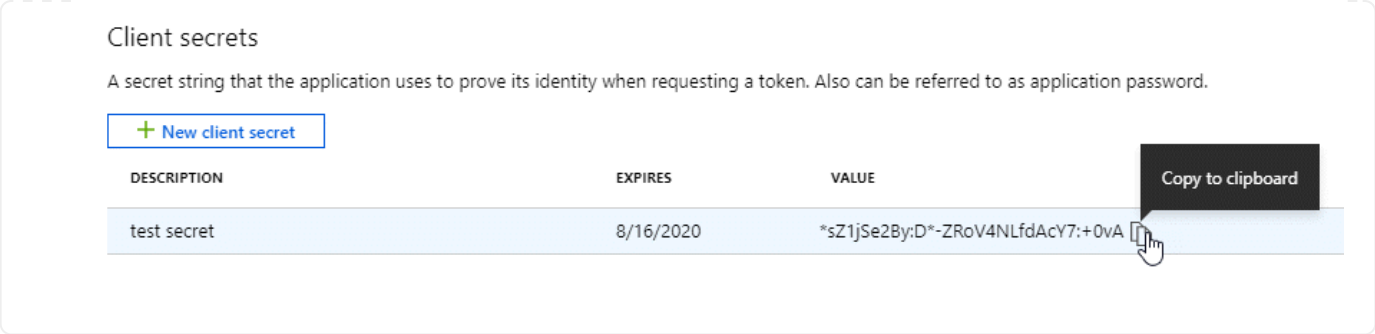
1. Dans le service **Microsoft Entra ID**, sélectionnez **Inscriptions d'applications** et sélectionnez l'application.
2. Copiez l'**ID d'application (client)** et l'**ID de répertoire (locataire)**.



Lorsque vous ajoutez le compte Azure à la console, vous devez fournir l'ID d'application (client) et l'ID de répertoire (locataire) de l'application. La console utilise les identifiants pour se connecter par programmation.

Créer un secret client

1. Ouvrez le service **Microsoft Entra ID**.
2. Sélectionnez **Inscriptions d'applications** et sélectionnez votre application.
3. Sélectionnez **Certificats et secrets > Nouveau secret client**.
4. Fournissez une description du secret et une durée.
5. Sélectionnez **Ajouter**.
6. Copiez la valeur du secret client.



Installer un agent de console dans votre environnement VCenter

NetApp prend en charge l'installation de l'agent de console dans votre environnement VCenter. Le fichier OVA inclut une image VM préconfigurée que vous pouvez déployer dans votre environnement VMware. Un téléchargement de fichier ou un déploiement d'URL est disponible directement depuis la NetApp Console. Il comprend le logiciel agent de console et un certificat auto-signé.

Téléchargez l'OVA ou copiez l'URL

Téléchargez l'OVA ou copiez l'URL de l'OVA directement depuis la NetApp Console.

1. Sélectionnez **Administration > Agents**.
2. Sur la page **Aperçu**, sélectionnez **Déployer l'agent > Sur site**.
3. Sélectionnez **Avec OVA**.
4. Choisissez de télécharger l'OVA ou de copier l'URL à utiliser dans VCenter.

Déployez l'agent dans votre VCenter

Connectez-vous à votre environnement VCenter pour déployer l'agent.

Étapes

1. Téléchargez le certificat auto-signé sur vos certificats de confiance si votre environnement l'exige. Vous remplacez ce certificat après l'installation."Découvrez comment remplacer le certificat auto-signé."
2. Déployez l'OVA à partir de la bibliothèque de contenu ou du système local.

Du système local	De la bibliothèque de contenu
a. Cliquez avec le bouton droit de la souris et sélectionnez **Déployer le modèle OVF…**. b. Choisissez le fichier OVA à partir de l'URL ou accédez à son emplacement, puis sélectionnez **Suivant**.	a. Accédez à votre bibliothèque de contenu et sélectionnez l'agent de console OVA. b. Sélectionnez **Actions** > **Nouvelle machine virtuelle à partir de ce modèle**.

3. Terminez l'assistant de déploiement de modèle OVF pour déployer l'agent de console.
4. Sélectionnez un nom et un dossier pour la machine virtuelle, puis sélectionnez **Suivant**.
5. Sélectionnez une ressource de calcul, puis sélectionnez **Suivant**.
6. Vérifiez les détails du modèle, puis sélectionnez **Suivant**.
7. Acceptez le contrat de licence, puis sélectionnez **Suivant**.
8. Choisissez le type de configuration proxy que vous souhaitez utiliser : proxy explicite, proxy transparent ou

aucun proxy.

9. Sélectionnez le magasin de données dans lequel vous souhaitez déployer la machine virtuelle, puis sélectionnez **Suivant**. Assurez-vous qu'il répond aux exigences de l'hôte.
10. Sélectionnez le réseau auquel vous souhaitez connecter la VM, puis sélectionnez **Suivant**. Assurez-vous que le réseau est IPv4 et dispose d'un accès Internet sortant vers les points de terminaison requis.
11. dans la fenêtre **Personnaliser le modèle**, remplissez les champs suivants :
    - **Informations proxy**
      - Si vous avez sélectionné un proxy explicite, entrez le nom d'hôte ou l'adresse IP et le numéro de port du serveur proxy, ainsi que le nom d'utilisateur et le mot de passe.
      - Si vous avez sélectionné un proxy transparent, téléchargez le certificat correspondant.
    - **Configuration de la machine virtuelle**
      - **Ignorer la vérification de configuration** : cette case à cocher est décochée par défaut, ce qui signifie que l'agent exécute une vérification de configuration pour valider l'accès au réseau.
        - NetApp recommande de laisser cette case décochée afin que l'installation inclue une vérification de la configuration de l'agent. La vérification de configuration valide que l'agent dispose d'un accès réseau aux points de terminaison requis. Si le déploiement échoue en raison de problèmes de connectivité, vous pouvez accéder au rapport de validation et aux journaux à partir de l'hôte de l'agent. Dans certains cas, si vous êtes sûr que l'agent dispose d'un accès au réseau, vous pouvez choisir d'ignorer la vérification. Par exemple, si vous utilisez toujours le"points finaux précédents" utilisé pour les mises à niveau de l'agent, la validation échoue avec une erreur. Pour éviter cela, cochez la case pour installer sans vérification de validation. "Apprenez à mettre à jour votre liste de points de terminaison" .
      - **Mot de passe de maintenance** : Définissez le mot de passe pour le `maint` utilisateur qui permet l'accès à la console de maintenance de l'agent.
      - **Serveurs NTP** : spécifiez un ou plusieurs serveurs NTP pour la synchronisation horaire.
      - **Nom d'hôte** : définissez le nom d'hôte pour cette machine virtuelle. Il ne doit pas inclure le domaine de recherche. Par exemple, un FQDN de console10.searchdomain.company.com doit être saisi comme console10.
      - **DNS principal** : spécifiez le serveur DNS principal à utiliser pour la résolution de noms.
      - **DNS secondaire** : spécifiez le serveur DNS secondaire à utiliser pour la résolution de noms.
      - Domaines de recherche : spécifiez le nom de domaine de recherche à utiliser lors de la résolution du nom d'hôte. Par exemple, si le nom de domaine complet est console10.searchdomain.company.com, saisissez searchdomain.company.com.
      - **Adresse IPv4** : l'adresse IP qui est mappée au nom d'hôte.
      - **Masque de sous-réseau IPv4** : Le masque de sous-réseau pour l'adresse IPv4.
      - **Adresse de passerelle IPv4** : l'adresse de passerelle pour l'adresse IPv4.
12. Sélectionnez **Suivant**.
13. Vérifiez les détails dans la fenêtre **Prêt à terminer**, sélectionnez **Terminer**.

    La barre des tâches vSphere affiche la progression du déploiement de l'agent de console.

14. Allumez la VM.

Si le déploiement échoue, vous pouvez accéder au rapport de validation et aux journaux à partir de l'hôte de l'agent."Découvrez comment résoudre les problèmes d'installation."

Enregistrer l’agent de console auprès de la NetApp Console

Connectez-vous à la console et associez l’agent de la console à votre organisation. La manière dont vous vous connectez dépend du mode dans lequel vous utilisez la console. Si vous utilisez la console en mode standard, vous vous connectez via le site Web SaaS. Si vous utilisez la console en mode restreint ou privé, vous vous connectez localement à partir de l’hôte de l’agent de la console.

Étapes

1. Ouvrez un navigateur Web et entrez l’URL de l’hôte de l’agent de la console :

   L’URL de l’hôte de la console peut être un hôte local, une adresse IP privée ou une adresse IP publique, selon la configuration de l’hôte. Par exemple, si l’agent de console se trouve dans le cloud public sans adresse IP publique, vous devez saisir une adresse IP privée provenant d’un hôte disposant d’une connexion à l’hôte de l’agent de console.

2. Inscrivez-vous ou connectez-vous.
3. Après vous être connecté, configurez la console :
   a. Spécifiez l’organisation de la console à associer à l’agent de la console.
   b. Entrez un nom pour le système.
   c. Sous **Exécutez-vous dans un environnement sécurisé ?**, gardez le mode restreint désactivé.

      Le mode restreint n’est pas pris en charge lorsque l’agent de console est installé sur site.

   d. Sélectionnez **Commençons**.

Ajouter les informations d’identification du fournisseur de cloud à la console

Après avoir installé et configuré l’agent de console, ajoutez vos informations d’identification cloud afin que l’agent de console dispose des autorisations requises pour effectuer des actions dans AWS ou Azure.

AWS

Avant de commencer

Si vous venez de créer ces informations d'identification AWS, leur disponibilité peut prendre quelques minutes. Attendez quelques minutes avant d'ajouter les informations d'identification à la console.

Étapes

1. Sélectionnez **Administration > Informations d'identification**.
2. Sélectionnez **Informations d'identification de l'organisation**.
3. Sélectionnez **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
   a. **Emplacement des informations d'identification** : sélectionnez *Amazon Web Services > Agent.
   b. **Définir les informations d'identification** : saisissez une clé d'accès AWS et une clé secrète.
   c. **Abonnement Marketplace** : Associez un abonnement Marketplace à ces informations d'identification en vous abonnant maintenant ou en sélectionnant un abonnement existant.
   d. **Révision** : Confirmez les détails des nouvelles informations d'identification et sélectionnez **Ajouter**.

Vous pouvez désormais accéder à la "NetApp Console" pour commencer à utiliser l'agent de console.

Azuré

Avant de commencer

Si vous venez de créer ces informations d'identification Azure, leur disponibilité peut prendre quelques minutes. Attendez quelques minutes avant d'ajouter les informations d'identification de l'agent de la console.

Étapes

1. Sélectionnez **Administration > Informations d'identification**.
2. Sélectionnez **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
   a. **Emplacement des informations d'identification** : sélectionnez **Microsoft Azure > Agent**.
   b. **Définir les informations d'identification** : saisissez les informations sur le principal du service Microsoft Entra qui accorde les autorisations requises :
      - ID de l'application (client)
      - ID du répertoire (locataire)
      - Secret client
   c. **Abonnement Marketplace** : Associez un abonnement Marketplace à ces informations d'identification en vous abonnant maintenant ou en sélectionnant un abonnement existant.
   d. **Révision** : Confirmez les détails des nouvelles informations d'identification et sélectionnez **Ajouter**.

Résultat

L'agent de console dispose désormais des autorisations nécessaires pour effectuer des actions dans Azure en votre nom. Vous pouvez désormais accéder à la "NetApp Console" pour commencer à utiliser l'agent de console.

Ports pour l’agent de console sur site

L’agent de console utilise les ports *inbound* lorsqu’il est installé manuellement sur un hôte Linux local. Consultez ces ports à des fins de planification.

Ces règles entrantes s’appliquent à tous les modes de déploiement de la NetApp Console .

Protocole	Port	But
HTTP	80	• Fournit un accès HTTP depuis les navigateurs Web clients vers l’interface utilisateur locale • Utilisé pendant le processus de mise à niveau de Cloud Volumes ONTAP
HTTPS	443	Fournit un accès HTTPS depuis les navigateurs Web clients vers l’interface utilisateur locale

Informations sur le copyright

Informations sur les marques commerciales