Premiers pas avec la NetApp Console (mode restreint)

NetApp Console setup and administration

NetApp
February 11, 2026

Sommaire

Premiers pas avec la NetApp Console (mode restreint)

Démarrage du flux de travail (mode restreint)

Commencez à utiliser la NetApp Console en mode restreint en préparant votre environnement et en déployant l'agent de la console.

Le mode restreint est généralement utilisé par les gouvernements étatiques et locaux et les entreprises réglementées, y compris les déploiements dans les régions AWS GovCloud et Azure Government. Avant de commencer, assurez-vous d'avoir une bonne compréhension de"Agents de console" et"modes de déploiement" .

1 "Préparez-vous au déploiement"

1. Préparez un hôte Linux dédié qui répond aux exigences en matière de CPU, de RAM, d'espace disque, d'outil d'orchestration de conteneurs, etc.
2. Configurez un réseau qui fournit un accès aux réseaux cibles, un accès Internet sortant pour les installations manuelles et un accès Internet sortant pour l'accès quotidien.
3. Configurez les autorisations dans votre fournisseur de cloud afin de pouvoir associer ces autorisations à l'instance de l'agent de console après son déploiement.

2 "Déployer l'agent de console"

1. Installez l'agent de console à partir de la place de marché de votre fournisseur de cloud ou en installant manuellement le logiciel sur votre propre hôte Linux.
2. Configurez la NetApp Console en ouvrant un navigateur Web et en saisissant l'adresse IP de l'hôte Linux.
3. Fournissez à l'agent de console les autorisations que vous avez précédemment configurées.

3 "Abonnez-vous aux NetApp Intelligent Services (facultatif)"

Facultatif : abonnez-vous à NetApp Intelligent Services depuis la place de marché de votre fournisseur de cloud pour payer les services de données à un tarif horaire (PAYGO) ou via un contrat annuel. Les NetApp Intelligent Services incluent NetApp Backup and Recovery, Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience et NetApp Disaster Recovery. La NetApp Data Classification est incluse dans votre abonnement sans frais supplémentaires.

Préparez-vous au déploiement en mode restreint

Préparez votre environnement avant de déployer la NetApp Console en mode restreint. Vous devez examiner les exigences de l'hôte, préparer la mise en réseau, configurer les autorisations, etc.

Étape 1 : Comprendre le fonctionnement du mode restreint

Comprendre le fonctionnement de la NetApp Console en mode restreint avant de commencer.

Utilisez l'interface basée sur un navigateur disponible localement à partir de l'agent NetApp Console installé. Vous ne pouvez pas accéder à la NetApp Console à partir de la console Web fournie via la couche SaaS.

De plus, toutes les fonctionnalités de la console et les services de données NetApp ne sont pas disponibles.

"Découvrez comment fonctionne le mode restreint" .

Étape 2 : Examiner les options d'installation

En mode restreint, vous ne pouvez installer l'agent de console que dans le cloud. Les options d'installation suivantes sont disponibles :

- Depuis la place de marché AWS
- Depuis la place de marché Azure
- Installation manuelle de l'agent de console sur votre propre hôte Linux exécuté dans AWS, Azure ou Google Cloud

Étape 3 : Examiner les exigences de l'hôte

Un hôte doit répondre à des exigences spécifiques en matière de système d'exploitation, de RAM et de port pour exécuter l'agent de console.

Lorsque vous déployez l'agent de console à partir d'AWS ou d'Azure Marketplace, l'image inclut les composants logiciels et de système d'exploitation requis. Il vous suffit de choisir un type d'instance qui répond aux exigences en matière de CPU et de RAM.

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.

Type d'instance AWS EC2

Un type d'instance qui répond aux exigences de CPU et de RAM. NetApp recommande t3.2xlarge.

Taille de la machine virtuelle Azure

Un type d'instance qui répond aux exigences de CPU et de RAM. NetApp recommande Standard_D8s_v3.

Type de machine Google Cloud

Un type d'instance qui répond aux exigences de CPU et de RAM. NetApp recommande n2-standard-8.

L'agent de console est pris en charge dans Google Cloud sur une instance de machine virtuelle avec un système d'exploitation prenant en charge "Fonctionnalités de la machine virtuelle blindée"

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

Étape 4 : installer Podman ou Docker Engine

Pour installer manuellement l'agent de console, préparez l'hôte en installant 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
```

Étape 5 : Préparer l'accès au réseau

Configurez l'accès au réseau afin que l'agent de la console puisse gérer les ressources de votre cloud public. En plus de disposer d'un réseau virtuel et d'un sous-réseau pour l'agent de console, vous devez vous assurer que les exigences suivantes sont respectées.

Connexions aux réseaux cibles

Assurez-vous que l'agent de console dispose d'une connexion réseau aux emplacements de stockage. Par exemple, le VPC ou le VNet sur lequel vous prévoyez de déployer Cloud Volumes ONTAP, ou le centre de données où résident vos clusters ONTAP sur site.

Préparer le réseau pour l'accès des utilisateurs à la NetApp Console

En mode restreint, les utilisateurs accèdent à la console à partir de la machine virtuelle de l'agent de console. L'agent de console contacte quelques points de terminaison pour effectuer des tâches de gestion des données. Ces points de terminaison sont contactés depuis l'ordinateur d'un utilisateur lors de l'exécution d'actions spécifiques à partir de la console.

Les agents de console antérieurs à la version 4.0.0 ont besoin de points de terminaison supplémentaires. Si vous avez effectué une mise à niveau vers la version 4.0.0 ou une version ultérieure, vous pouvez supprimer les anciens points de terminaison de votre liste d'autorisation."En savoir plus sur l'accès réseau requis pour les versions antérieures à 4.0.0."

+

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://cdn.auth0.com \ https://services.cloud.netapp.com	Votre navigateur Web se connecte à ces points de terminaison pour une authentification utilisateur centralisée via la NetApp Console.

Accès Internet sortant pour les opérations quotidiennes

L'emplacement réseau de l'agent de console doit disposer d'un accès Internet sortant. Il doit pouvoir accéder aux services SaaS de la NetApp Console ainsi qu'aux points de terminaison au sein de votre environnement de cloud public respectif.

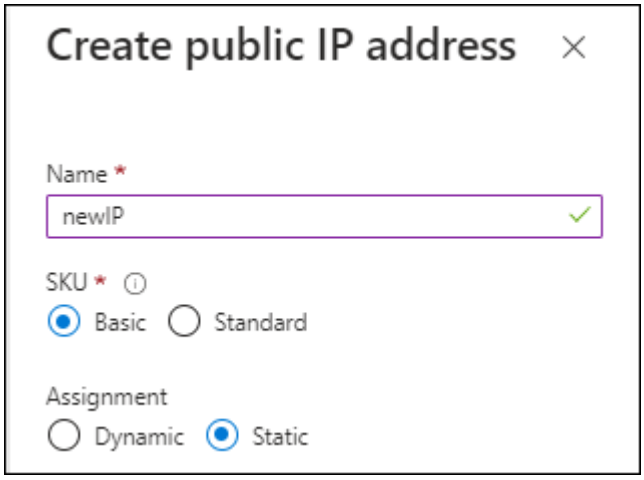
Points de terminaison	But
Environnements AWS	Services AWS (amazonaws.com) : • CloudFormation • Cloud de calcul élastique (EC2) • Gestion des identités et des accès (IAM) • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Service de stockage simple (S3)
Pour gérer les ressources 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 .	**Environnements Azure**
\ 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.
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	Pour gérer les ressources dans les régions Azure Government.
\ 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.

Points de terminaison	But
Environnements Google Cloud	\ https://www.googleapis.com/compute/v1/ \ https://compute.googleapis.com/compute/v1 \ https://cloudresourcemanager.googleapis.com/v1/projects \ https://www.googleapis.com/compute/beta \ https://storage.googleapis.com/storage/v1 \ https://www.googleapis.com/storage/v1 \ https://iam.googleapis.com/v1 \ https://cloudkms.googleapis.com/v1 \ https://config.googleapis.com/v1/projects
Pour gérer les ressources dans Google Cloud.	• Points de terminaison de la NetApp Console *
\ 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.

Adresse IP publique dans Azure

Si vous souhaitez utiliser une adresse IP publique avec la machine virtuelle de l'agent de console dans Azure, l'adresse IP doit utiliser une référence SKU de base pour garantir que la console utilise cette adresse IP publique.



Si vous utilisez plutôt une adresse IP SKU standard, la console utilise l'adresse IP *privée* de l'agent de la

console, au lieu de l'adresse IP publique. Si la machine que vous utilisez pour accéder à la console n'a pas accès à cette adresse IP privée, les actions de la console échoueront.

"Documentation Azure : Référence IP publique"

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"

Si vous envisagez de créer un agent de console à partir de la place de marché de votre fournisseur de cloud, implémentez cette exigence de mise en réseau après avoir créé l'agent de console.

Étape 6 : Préparer les autorisations cloud

L'agent de console nécessite des autorisations de votre fournisseur de cloud pour déployer Cloud Volumes ONTAP dans un réseau virtuel et pour utiliser les services de données NetApp . Vous devez configurer des autorisations auprès de votre fournisseur de cloud, puis associer ces autorisations à l'agent de la console.

Pour afficher les étapes requises, choisissez l'option d'authentification à utiliser pour votre fournisseur de cloud.

Rôle AWS IAM

Utilisez un rôle IAM pour fournir des autorisations à l'agent de la console.

Si vous créez l'agent de console à partir d'AWS Marketplace, vous êtes invité à sélectionner ce rôle IAM lorsque vous lancez l'instance EC2.

Si vous installez manuellement l'agent de console sur votre propre hôte Linux, attachez le rôle à l'instance EC2.

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.
3. Créer un rôle IAM :
   a. Sélectionnez **Rôles > Créer un rôle**.
   b. Sélectionnez **Service AWS > EC2**.
   c. Ajoutez des autorisations en joignant la politique que vous venez de créer.
   d. Terminez les étapes restantes pour créer le rôle.

Résultat

Vous disposez désormais d'un rôle IAM pour l'instance EC2 de l'agent de console.

Clé d'accès AWS

Configurez des autorisations et une clé d'accès pour un utilisateur IAM. Vous devrez fournir à la console la clé d'accès AWS après avoir installé l'agent de la console et configuré la console.

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.

Rôle Azure

Créez un rôle personnalisé Azure avec les autorisations requises. Vous attribuerez ce rôle à la machine virtuelle de l'agent de console.

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"

Étapes

1. Si vous prévoyez d'installer manuellement le logiciel sur votre propre hôte, activez une identité gérée attribuée par le système sur la machine virtuelle afin de pouvoir fournir les autorisations Azure requises via un rôle personnalisé.

   "Documentation Microsoft Azure : Configurer des identités gérées pour les ressources Azure sur une machine virtuelle à l'aide du portail Azure"

2. Copiez le contenu du"autorisations de rôle personnalisées pour le connecteur" et les enregistrer dans un fichier JSON.
3. Modifiez le fichier JSON en ajoutant des ID d'abonnement Azure à l'étendue attribuable.

   Vous devez ajouter l'ID de chaque abonnement Azure que vous souhaitez utiliser avec la NetApp Console.

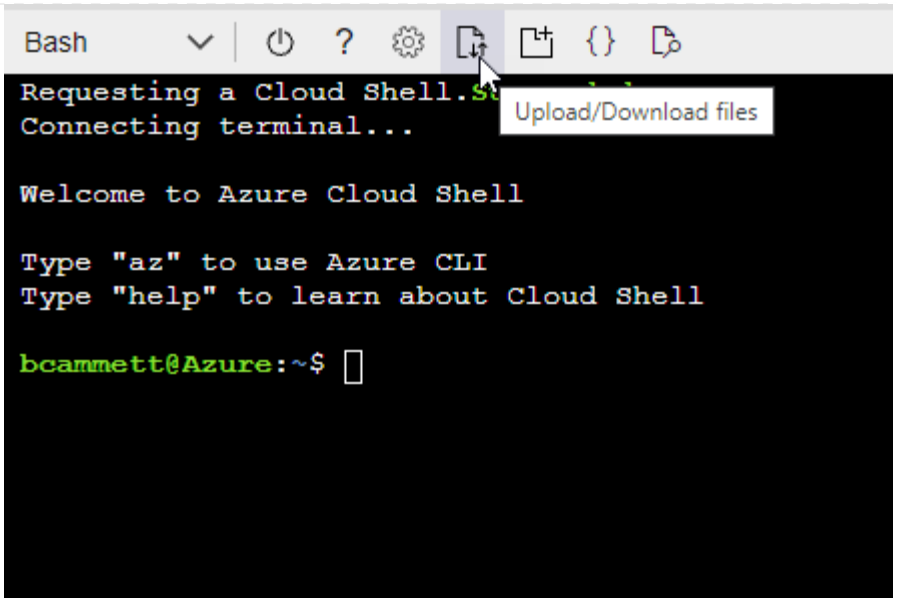
   Exemple

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

4. 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.

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



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

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

Principal de service Azure

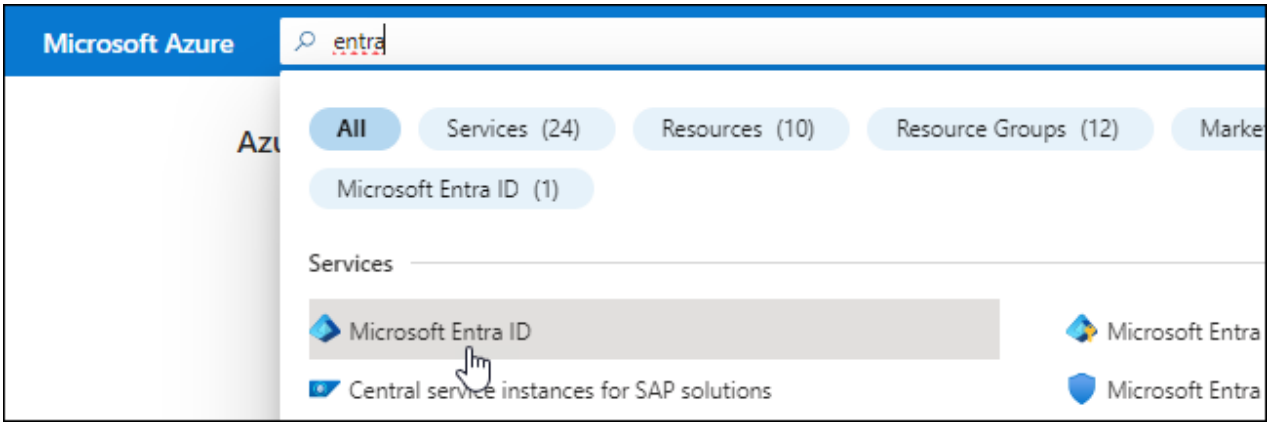
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont la console a besoin. Vous devez fournir ces informations d'identification à la console après avoir installé l'agent de la console.

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 .

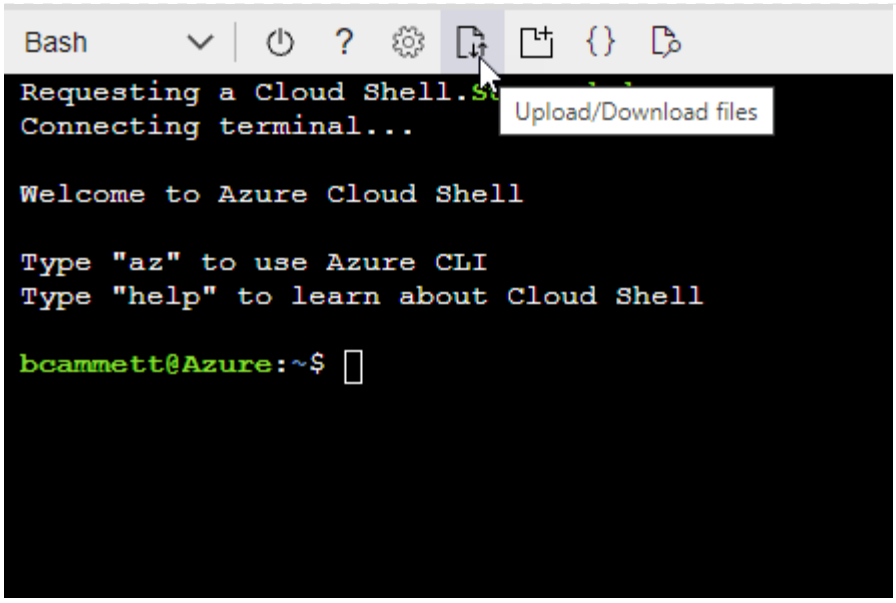
      Exemple

      ```
      "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**.

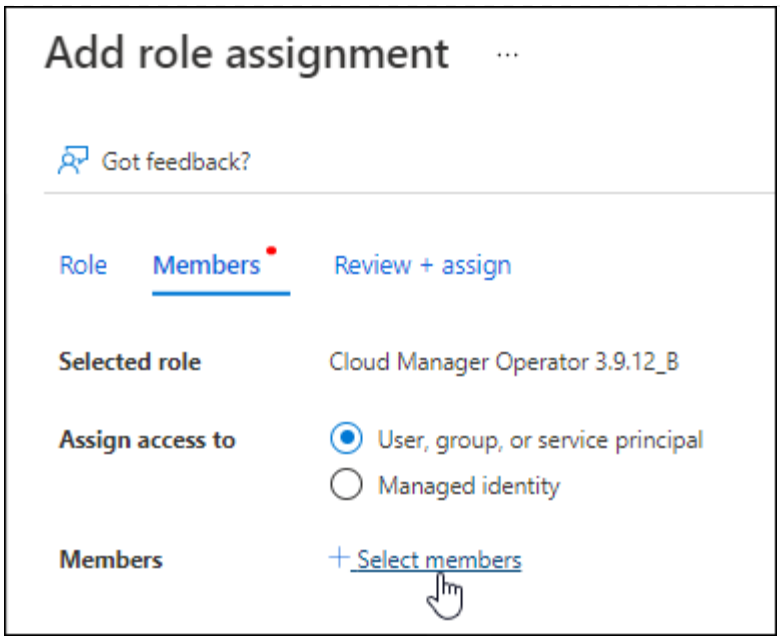
   b. Sélectionnez l'abonnement.

   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**.

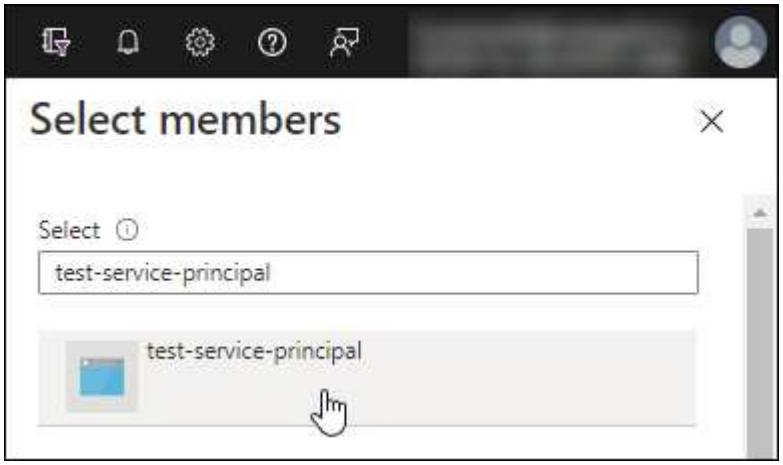
   e. Dans l'onglet **Membres**, procédez comme suit :

      - 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**.

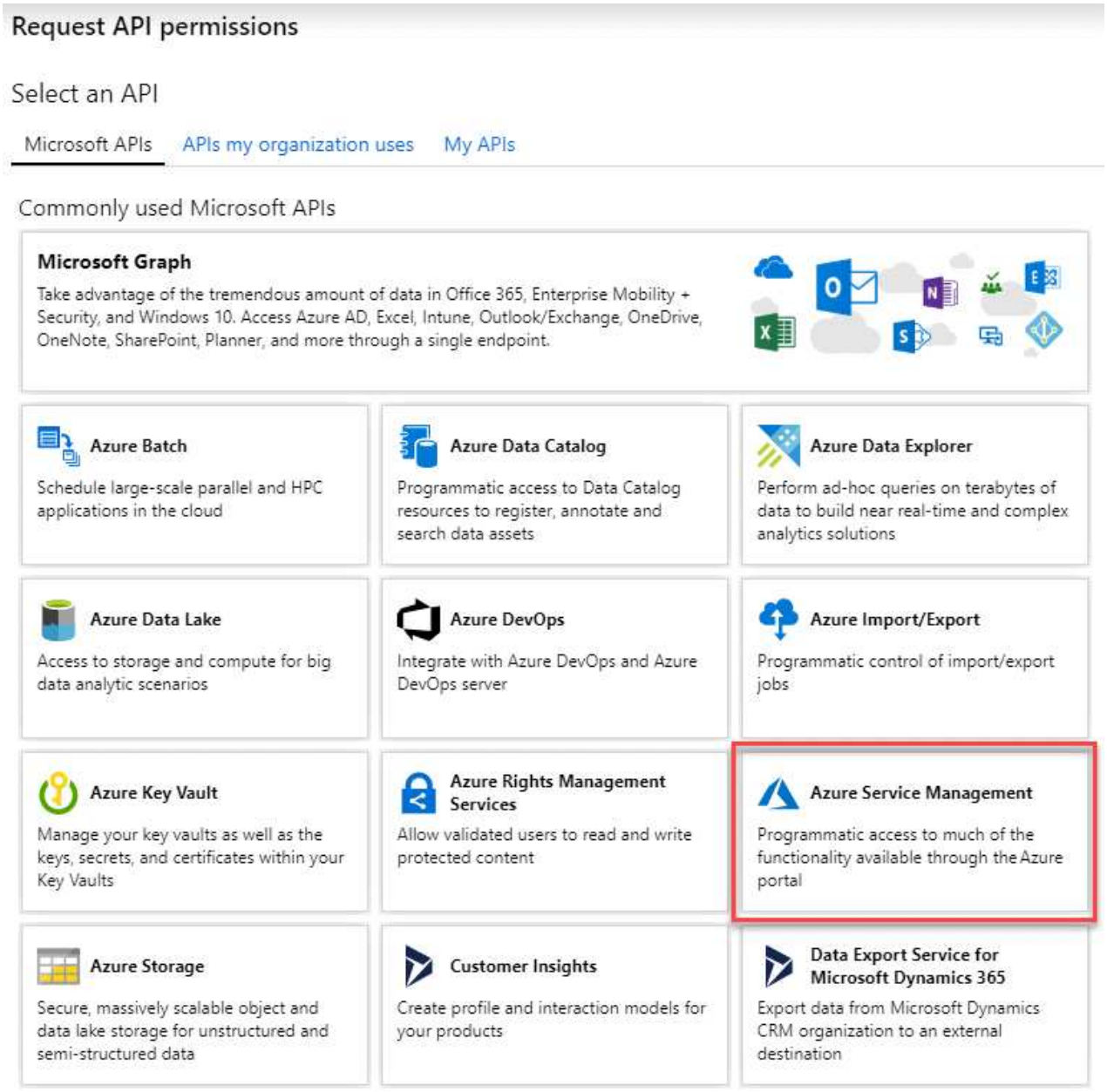
Le principal du service dispose désormais des autorisations Azure requises pour déployer l'agent de la console.

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.

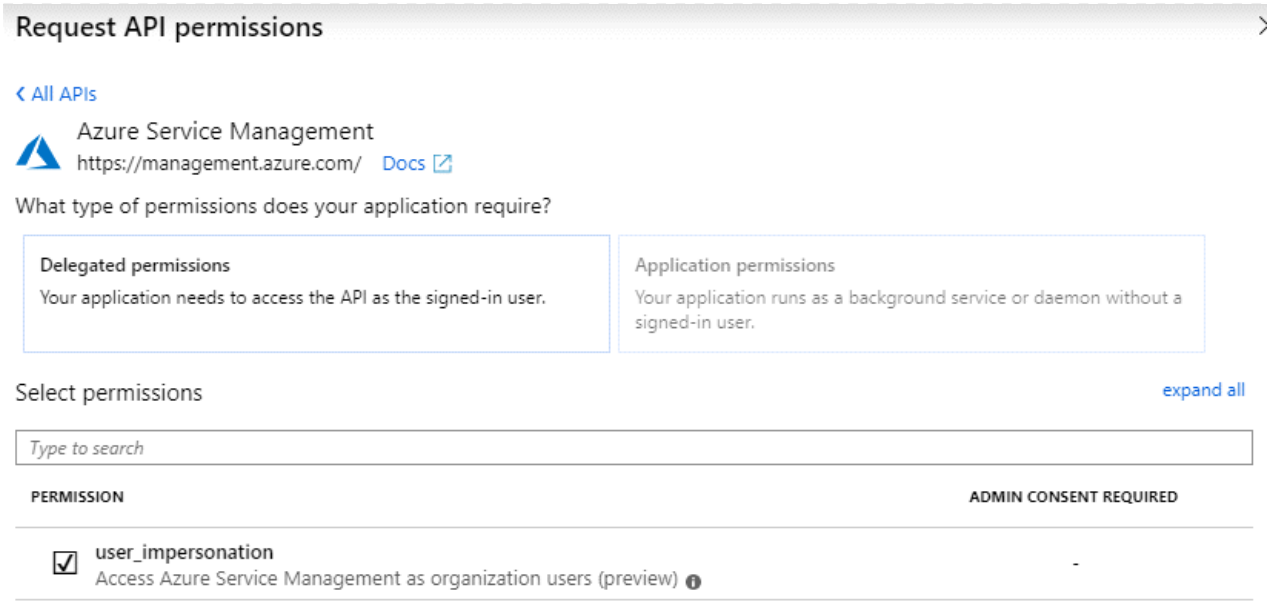
Ajouter des autorisations à l'API Windows Azure Service Management

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**.

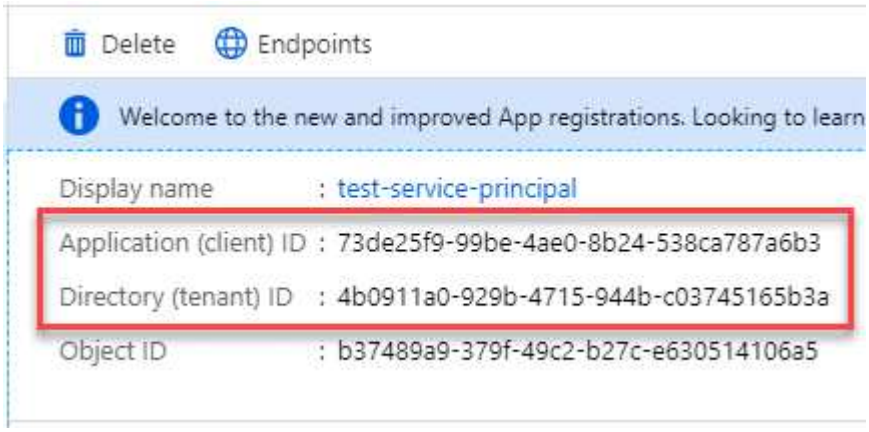


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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.

Résultat

Votre principal de service est maintenant configuré et vous devez avoir copié l'ID de l'application (client), l'ID du répertoire (locataire) et la valeur du secret client. Vous devez saisir ces informations dans la console lorsque vous ajoutez un compte Azure.

Compte de service Google Cloud

Créez un rôle et appliquez-le à un compte de service que vous utiliserez pour l'instance de machine virtuelle de l'agent de console.

Étapes

1. Créer un rôle personnalisé dans Google Cloud :

   a. Créez un fichier YAML qui inclut les autorisations définies dans le"Politique de l'agent de console pour Google Cloud" .

   b. Depuis Google Cloud, activez Cloud Shell.

   c. Téléchargez le fichier YAML qui inclut les autorisations requises pour l'agent de la console.

   d. Créez un rôle personnalisé en utilisant le `gcloud iam roles create` commande.

      L'exemple suivant crée un rôle nommé « agent » au niveau du projet :

```
gcloud iam roles create agent --project=myproject --file=agent.yaml
```

   +
   "Documentation Google Cloud : Création et gestion de rôles personnalisés"

2. Créer un compte de service dans Google Cloud :

   a. Depuis le service IAM & Admin, sélectionnez **Comptes de service > Créer un compte de service**.

   b. Saisissez les détails du compte de service et sélectionnez **Créer et continuer**.

   c. Sélectionnez le rôle que vous venez de créer.

   d. Terminez les étapes restantes pour créer le rôle.

      "Documentation Google Cloud : Création d'un compte de service"

Étape 7 : Activer les API Google Cloud

Plusieurs API sont nécessaires pour déployer Cloud Volumes ONTAP dans Google Cloud.

Étape

1. "Activez les API Google Cloud suivantes dans votre projet"
    - API du gestionnaire de déploiement cloud V2
    - API Cloud Infrastructure Manager
    - API de journalisation dans le cloud
    - API du gestionnaire de ressources cloud
    - API Compute Engine
    - API de gestion des identités et des accès (IAM)
    - API du service de gestion des clés cloud (KMS) (Requise uniquement si vous prévoyez d'utiliser NetApp Backup and Recovery avec des clés de chiffrement gérées par le client (CMEK))
    - API Cloud Quotas (requise pour les déploiements Cloud Volumes ONTAP utilisant Infrastructure Manager)

Déployer l'agent de console en mode restreint

Déployez l'agent de console en mode restreint afin de pouvoir utiliser la NetApp Console avec une connectivité sortante limitée. Pour commencer, installez l'agent de console, configurez la console en accédant à l'interface utilisateur qui s'exécute sur l'agent de console, puis fournissez les autorisations cloud que vous avez précédemment configurées.

Étape 1 : Installer l'agent de console

Installez l'agent de console à partir de la place de marché de votre fournisseur de cloud ou manuellement sur un hôte Linux.

Vous devez avoir préparé votre environnement avant d'installer l'agent Console. Vous pouvez l'installer depuis AWS Marketplace, depuis Azure Marketplace ou manuellement sur votre propre hôte Linux exécuté sur AWS, Azure ou Google Cloud.

Place de marché commerciale AWS

Avant de commencer

Veuillez vous munir des éléments suivants :

- Un VPC et un sous-réseau qui répondent aux exigences de mise en réseau.

  "En savoir plus sur les exigences de mise en réseau"

- Un rôle IAM avec une politique attachée qui inclut les autorisations requises pour l'agent de la console.

  "Découvrez comment configurer les autorisations AWS"

- Autorisations d'abonnement et de désabonnement de la place de marché AWS pour votre utilisateur IAM.
- Une compréhension des exigences en matière de CPU et de RAM pour l'agent.

  "Examen des exigences des agents".

- Une paire de clés pour l'instance EC2.

Étapes

1. Aller à la "Liste des agents de la NetApp Console sur AWS Marketplace"
2. Sur la page Marketplace, sélectionnez **Continuer pour s'abonner**.
3. Pour vous abonner au logiciel, sélectionnez **Accepter les conditions**.

   Le processus d'abonnement peut prendre quelques minutes.

4. Une fois le processus d'abonnement terminé, sélectionnez **Continuer vers la configuration**.
5. Sur la page **Configurer ce logiciel**, assurez-vous d'avoir sélectionné la bonne région, puis sélectionnez **Continuer pour lancer**.
6. Sur la page **Lancer ce logiciel**, sous **Choisir une action**, sélectionnez **Lancer via EC2**, puis sélectionnez **Lancer**.

   Utilisez la console EC2 pour lancer l'instance et attacher un rôle IAM. Cela n'est pas possible avec l'action **Lancer depuis le site Web**.

7. Suivez les instructions pour configurer et déployer l'instance :
   - **Nom et balises** : saisissez un nom et des balises pour l'instance.
   - **Images d'application et de système d'exploitation** : ignorez cette section. L'AMI de l'agent de console est déjà sélectionné.
   - **Type d'instance** : Selon la disponibilité de la région, choisissez un type d'instance qui répond aux exigences de RAM et de CPU (t3.2xlarge est présélectionné et recommandé).
   - **Paire de clés (connexion)** : 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 du groupe de sécurité qui activent les méthodes de connexion requises pour l'instance de l'agent de console : SSH, HTTP et HTTPS.

          "Afficher les règles du groupe de sécurité pour AWS" .

    - **Configurer le stockage** : Conservez la taille et le type de disque par défaut pour le volume racine.

      Si vous souhaitez activer le chiffrement Amazon EBS sur le volume racine, sélectionnez **Avancé**, développez **Volume 1**, sélectionnez **Chiffré**, puis choisissez une clé KMS.

    - **Détails avancés** : Sous **Profil d'instance IAM**, choisissez le rôle IAM qui inclut les autorisations requises pour l'agent de la console.
    - **Résumé** : Consultez le résumé et sélectionnez **Lancer l'instance**.

Résultat

AWS lance le logiciel avec les paramètres spécifiés. L'agent de console se déploie en environ cinq minutes.

Quelle est la prochaine étape ?

Configurer la NetApp Console.

AWS Gov Marketplace

Avant de commencer

Veuillez vous munir des éléments suivants :

- Un VPC et un sous-réseau qui répondent aux exigences de mise en réseau.

  "En savoir plus sur les exigences de mise en réseau"

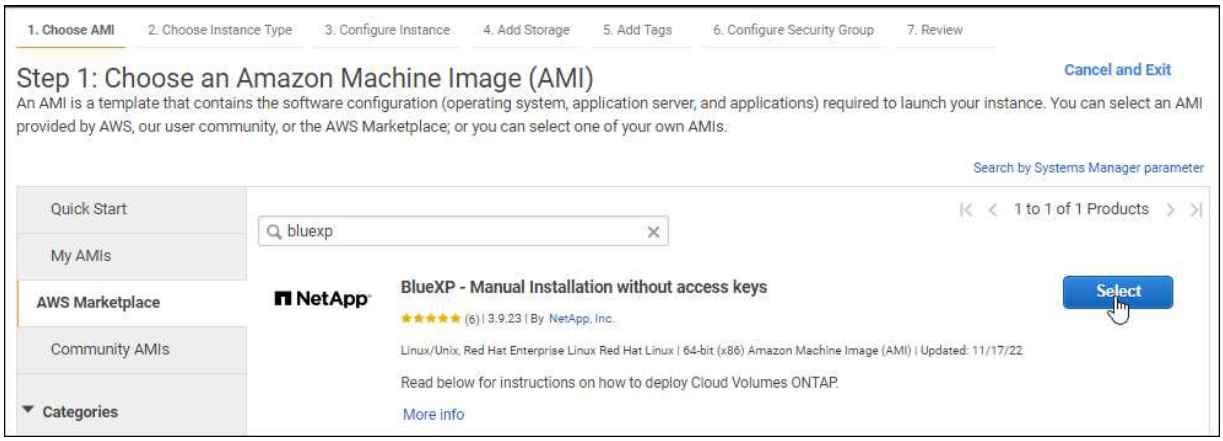
- Un rôle IAM avec une politique attachée qui inclut les autorisations requises pour l'agent de la console.

  "Découvrez comment configurer les autorisations AWS"

- Autorisations d'abonnement et de désabonnement de la place de marché AWS pour votre utilisateur IAM.
- Une paire de clés pour l'instance EC2.

Étapes

1. Accédez à l'offre d'agent NetApp Console sur AWS Marketplace.
    a. Ouvrez le service EC2 et sélectionnez **Lancer l'instance**.
    b. Sélectionnez **AWS Marketplace**.
    c. Recherchez la NetApp Console et sélectionnez l'offre.



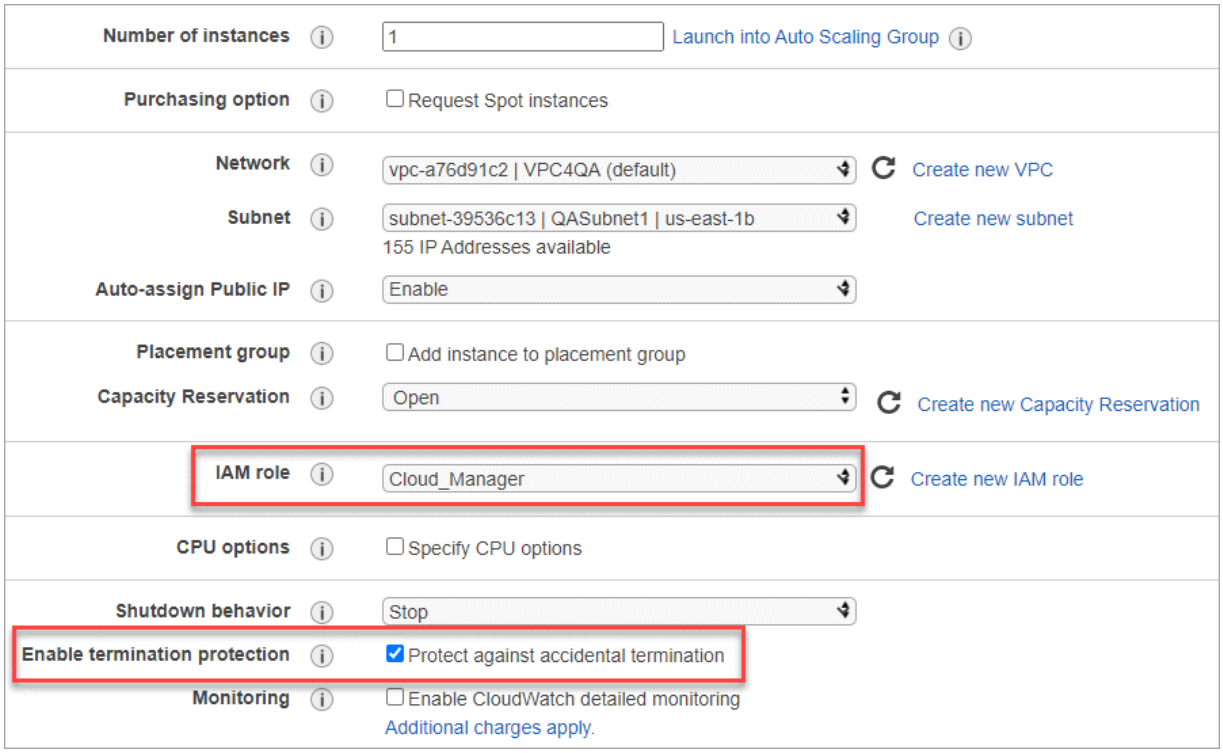
d. Sélectionnez **Continuer**.

2. Suivez les instructions pour configurer et démarrer l'instance :

- **Choisissez un type d'instance** : Selon la disponibilité de la région, choisissez l'un des types d'instance pris en charge (t3.2xlarge est recommandé).

  "Examiner les exigences de 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 (recommandé) et choisissez toute autre option de configuration qui répond à vos besoins.



- **Ajouter du 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 l'agent de console : SSH, HTTP et HTTPS.
- **Révision** : Vérifiez vos sélections et sélectionnez **Lancer**.

Résultat

AWS lance le logiciel avec les paramètres spécifiés. L'agent de console se déploie en environ cinq minutes.

Quelle est la prochaine étape ?

Configurer la console.

Place de marché Azure Gov

Avant de commencer

Vous devriez avoir les éléments suivants :

- Un réseau virtuel et un sous-réseau qui répondent aux exigences de mise en réseau.

  "En savoir plus sur les exigences de mise en réseau"

- Un rôle personnalisé Azure qui inclut les autorisations requises pour l'agent de la console.

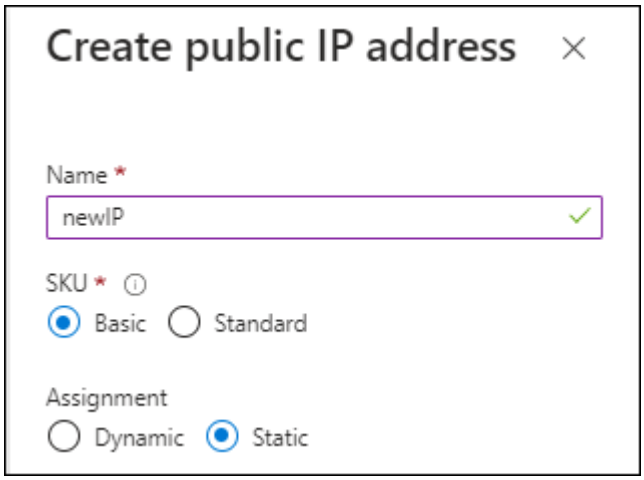
  "Découvrez comment configurer les autorisations Azure"

Étapes

1. Accédez à la page de la machine virtuelle de l'agent de la NetApp Console dans la Place de marché Azure.
   - "Page de la place de marché Azure pour les régions commerciales"
   - "Page de la place de marché Azure pour les régions Azure Government"
2. Sélectionnez **Obtenir maintenant** puis sélectionnez **Continuer**.
3. Depuis le portail Azure, sélectionnez **Créer** et suivez les étapes pour configurer la machine virtuelle.

   Notez les points suivants lorsque vous configurez la machine virtuelle :

   - **Taille de la VM** : Choisissez une taille de VM qui répond aux exigences de CPU et de RAM. Nous recommandons Standard_D8s_v3.
   - **Disques** : L'agent de console peut fonctionner de manière optimale avec des disques HDD ou SSD.
   - **Adresse IP publique** : Pour utiliser une adresse IP publique avec la machine virtuelle de l'agent Console, sélectionnez une référence SKU de base.



Si vous utilisez plutôt une adresse IP SKU standard, la console utilise l'adresse IP *privée* de l'agent de la console, au lieu de l'adresse IP publique. Si la machine que vous utilisez pour accéder à la console ne peut pas atteindre l'adresse IP privée, la console ne fonctionne pas.

"Documentation Azure : Référence IP publique"

- **Groupe de sécurité réseau** : l'agent de console nécessite des connexions entrantes utilisant SSH, HTTP et HTTPS.

  "Afficher les règles du groupe de sécurité pour Azure" .

- **Identité** : Sous **Gestion**, sélectionnez **Activer l'identité gérée attribuée par le système**.

  Une identité gérée permet à la machine virtuelle de l'agent Console de s'identifier auprès de Microsoft Entra ID sans avoir besoin d'informations d'identification. "En savoir plus sur les identités gérées pour les ressources Azure" .

4. Sur la page **Réviser + créer**, vérifiez vos sélections et sélectionnez **Créer** pour démarrer le déploiement.

Résultat

Azure déploie la machine virtuelle avec les paramètres spécifiés. La machine virtuelle et le logiciel de l'agent de console devraient être exécutés dans environ cinq minutes.

Quelle est la prochaine étape ?

Configurer la NetApp Console.

Installation manuelle (obligatoire pour Google Cloud)

Vous pouvez installer manuellement l'agent Console sur votre propre hôte Linux exécuté sur AWS, Azure ou Google Cloud.

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" .

- Vous devez désactiver la vérification de configuration qui vérifie la connectivité sortante lors de l'installation. L'installation manuelle échoue si cette vérification n'est pas désactivée."Découvrez comment désactiver les vérifications de configuration pour les installations manuelles."
- Selon votre système d'exploitation, Podman ou Docker Engine est requis avant d'installer l'agent de

console.

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.

Résultat

L'agent de console est maintenant installé. À la fin de l'installation, le service de l'agent de console (occm) redémarre deux fois si vous avez spécifié un serveur proxy.

Quelle est la prochaine étape ?

Configurer la NetApp Console.

Étape 2 : Configurer la NetApp Console

Lorsque vous accédez à la console pour la première fois, vous êtes invité à choisir une organisation pour l'agent de la console et devez activer le mode restreint.

Avant de commencer

La personne qui configure l'agent de la console doit se connecter à la console à l'aide d'un identifiant qui n'appartient pas déjà à une organisation de la console.

Si votre compte est associé à une autre organisation, vous devez créer un nouveau compte. Sinon, l'option permettant d'activer le mode restreint n'apparaît pas sur l'écran de configuration.

Étapes

1. Ouvrez un navigateur Web à partir d'un hôte disposant d'une connexion à l'instance de l'agent de console et entrez l'URL suivante de l'agent de console que vous avez installé.
2. Inscrivez-vous ou connectez-vous à la NetApp Console.
3. Une fois connecté, configurez la console :

   a. Entrez un nom pour l'agent de la console.

   b. Saisissez un nom pour une nouvelle organisation de console.

   c. Sélectionnez **Exécutez-vous dans un environnement sécurisé ?**

   d. Sélectionnez **Activer le mode restreint sur ce compte**.

      Notez que vous ne pouvez pas modifier ce paramètre une fois le compte créé. Vous ne pouvez pas activer le mode restreint ultérieurement et vous ne pouvez pas le désactiver ultérieurement.

   Si vous avez déployé l'agent de console dans une région gouvernementale, la case à cocher est déjà activée et ne peut pas être modifiée. Cela est dû au fait que le mode restreint est le seul mode pris en charge dans les régions gouvernementales.

a. Sélectionnez **Commençons**.

Résultat

L'agent de console est maintenant installé et configuré avec votre organisation de console. Tous les utilisateurs doivent accéder à la console à l'aide de l'adresse IP de l'instance de l'agent de la console.

Quelle est la prochaine étape ?

Fournissez à la console les autorisations que vous avez précédemment configurées.

Étape 3 : Accorder des autorisations à l'agent de la console

Si vous avez installé l'agent Console à partir d'Azure Marketplace ou manuellement, vous devez lui accorder les autorisations que vous avez configurées précédemment.

Ces étapes ne s'appliquent pas si vous avez déployé l'agent de console à partir d'AWS Marketplace, car vous avez choisi le rôle IAM requis lors du déploiement.

"Apprenez à préparer les autorisations cloud" .

Rôle AWS IAM

Attachez le rôle IAM que vous avez précédemment créé à l'instance EC2 sur laquelle vous avez installé l'agent de console.

Ces étapes s'appliquent uniquement si vous avez installé manuellement l'agent de console dans AWS. Pour les déploiements AWS Marketplace, vous avez déjà associé l'instance de l'agent de console à un rôle IAM qui inclut les autorisations requises.

Étapes

1. Accédez à la console Amazon EC2.
2. Sélectionnez **Instances**.
3. Sélectionnez l'instance de l'agent de console.
4. Sélectionnez **Actions > Sécurité > Modifier le rôle IAM**.
5. Sélectionnez le rôle IAM et sélectionnez **Mettre à jour le rôle IAM**.

Clé d'accès AWS

Fournissez à la NetApp Console la clé d'accès AWS pour un utilisateur IAM disposant des autorisations requises.

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**.

Rôle Azure

Accédez au portail Azure et attribuez le rôle personnalisé Azure à la machine virtuelle de l'agent de console pour un ou plusieurs abonnements.

Étapes

1. Depuis le portail Azure, ouvrez le service **Abonnements** et sélectionnez votre abonnement.

   Il est important d'attribuer le rôle à partir du service **Abonnements** car cela spécifie la portée de l'attribution du rôle au niveau de l'abonnement. La *scope* définit l'ensemble des ressources auxquelles l'accès s'applique. Si vous spécifiez une étendue à un niveau différent (par exemple, au niveau de la machine virtuelle), votre capacité à effectuer des actions à partir de la NetApp Console sera affectée.

   "Documentation Microsoft Azure : Comprendre la portée d'Azure RBAC"

2. Sélectionnez **Contrôle d'accès (IAM)** > **Ajouter** > **Ajouter une attribution de rôle**.
3. Dans l'onglet **Rôle**, sélectionnez le rôle **Opérateur de console** et sélectionnez **Suivant**.

L'opérateur de console est le nom par défaut fourni dans la politique. Si vous avez choisi un nom différent pour le rôle, sélectionnez plutôt ce nom.

4. Dans l'onglet **Membres**, procédez comme suit :
   a. Attribuer l'accès à une **identité gérée**.
   b. Sélectionnez **Sélectionner les membres**, sélectionnez l'abonnement dans lequel la machine virtuelle de l'agent de console a été créée, sous **Identité gérée**, choisissez **Machine virtuelle**, puis sélectionnez la machine virtuelle de l'agent de console.
   c. Sélectionnez **Sélectionner**.
   d. Sélectionnez **Suivant**.
   e. Sélectionnez **Réviser + attribuer**.
   f. Si vous souhaitez gérer des ressources dans des abonnements Azure supplémentaires, passez à cet abonnement, puis répétez ces étapes.

Principal de service Azure

Fournissez à la NetApp Console les informations d'identification du principal de service Azure que vous avez précédemment configuré.

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

la NetApp Console dispose désormais des autorisations nécessaires pour effectuer des actions dans Azure en votre nom.

Compte de service Google Cloud

Associez le compte de service à la machine virtuelle de l'agent de console.

Étapes

1. Accédez au portail Google Cloud et attribuez le compte de service à l'instance de machine virtuelle de l'agent de la console.

   "Documentation Google Cloud : Modification du compte de service et des étendues d'accès pour une instance"

2. Si vous souhaitez gérer les ressources d'autres projets, accordez l'accès en ajoutant le compte de service avec le rôle d'agent de console à ce projet. Vous devrez répéter cette étape pour chaque projet.

S'abonner aux NetApp Intelligent Services (mode restreint)

Abonnez-vous aux NetApp Intelligent Services depuis la place de marché de votre fournisseur de cloud pour payer les services de données à un tarif horaire (PAYGO) ou via un contrat annuel. Si vous avez acheté une licence auprès de NetApp (BYOL), vous devez également vous abonner à l'offre de la place de marché. Votre licence est toujours facturée en premier, mais vous serez facturé au tarif horaire si vous dépassez votre capacité autorisée ou si la durée de la licence expire.

Un abonnement marketplace permet de facturer les services de données suivants avec un mode restreint :

- NetApp Backup and Recovery
- Cloud Volumes ONTAP
- NetApp Cloud Tiering
- NetApp Ransomware Resilience
- NetApp Disaster Recovery

La NetApp Data Classification est activée via votre abonnement, mais l'utilisation de la classification est gratuite.

Avant de commencer

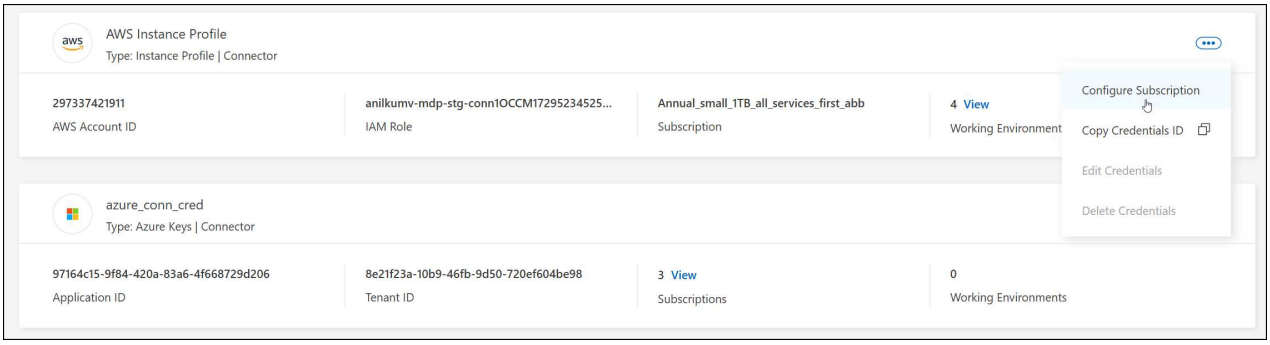
Vous devez déjà avoir déployé un agent de console pour vous abonner aux services de données. Vous devez associer un abonnement au marché aux informations d'identification cloud connectées à un agent de console.

AWS

Étapes

1. Sélectionnez **Administration > Informations d'identification**.
2. Sélectionnez **Informations d'identification de l'organisation**.
3. Sélectionnez le menu d'action pour un ensemble d'informations d'identification associées à un agent de console, puis sélectionnez **Configurer l'abonnement**.

   Vous devez sélectionner les informations d'identification associées à un agent de console. Vous ne pouvez pas associer un abonnement au marché aux informations d'identification associées à la NetApp Console.



4. Pour associer les informations d'identification à un abonnement existant, sélectionnez l'abonnement dans la liste déroulante et sélectionnez **Configurer**.
5. Pour associer les informations d'identification à un nouvel abonnement, sélectionnez **Ajouter un abonnement > Continuer** et suivez les étapes dans AWS Marketplace :

   a. Sélectionnez **Afficher les options d'achat**.

   b. Sélectionnez **S'abonner**.

   c. Sélectionnez **Configurer votre compte**.

      Vous serez redirigé vers la NetApp Console.

   d. À partir de la page **Affectation d'abonnement** :

      - Sélectionnez les organisations ou les comptes de la console auxquels vous souhaitez associer cet abonnement.
      - Dans le champ **Remplacer l'abonnement existant**, choisissez si vous souhaitez remplacer automatiquement l'abonnement existant pour une organisation ou un compte par ce nouvel abonnement.

        La console remplace l'abonnement existant pour toutes les informations d'identification de l'organisation ou du compte par ce nouvel abonnement. Si un ensemble d'informations d'identification n'a jamais été associé à un abonnement, ce nouvel abonnement ne sera pas associé à ces informations d'identification.

   Pour toutes les autres organisations ou comptes, vous devrez associer manuellement l'abonnement en répétant ces étapes.

   ◦ Sélectionnez **Enregistrer**.

Azuré

Étapes

1. Sélectionnez **Administration > Informations d'identification**.
2. Sélectionnez **Informations d'identification de l'organisation**.
3. Sélectionnez le menu d'action pour un ensemble d'informations d'identification associées à un agent de console, puis sélectionnez **Configurer l'abonnement**.

   Vous devez sélectionner les informations d'identification associées à un agent de console. Vous ne pouvez pas associer un abonnement au marché aux informations d'identification associées à la NetApp Console.

4. Pour associer les informations d'identification à un abonnement existant, sélectionnez l'abonnement dans la liste déroulante et sélectionnez **Configurer**.
5. Pour associer les informations d'identification à un nouvel abonnement, sélectionnez **Ajouter un abonnement > Continuer** et suivez les étapes dans la Place de marché Azure :

   a. Si vous y êtes invité, connectez-vous à votre compte Azure.

   b. Sélectionnez **S'abonner**.

   c. Remplissez le formulaire et sélectionnez **S'abonner**.

   d. Une fois le processus d'abonnement terminé, sélectionnez **Configurer le compte maintenant**.

      Vous serez redirigé vers la NetApp Console.

   e. À partir de la page **Affectation d'abonnement** :

      - Sélectionnez les organisations ou les comptes de la console auxquels vous souhaitez associer cet abonnement.
      - Dans le champ **Remplacer l'abonnement existant**, choisissez si vous souhaitez remplacer automatiquement l'abonnement existant pour une organisation ou un compte par ce nouvel abonnement.

        La console remplace l'abonnement existant pour toutes les informations d'identification de l'organisation ou du compte par ce nouvel abonnement. Si un ensemble d'informations d'identification n'a jamais été associé à un abonnement, ce nouvel abonnement ne sera pas associé à ces informations d'identification.

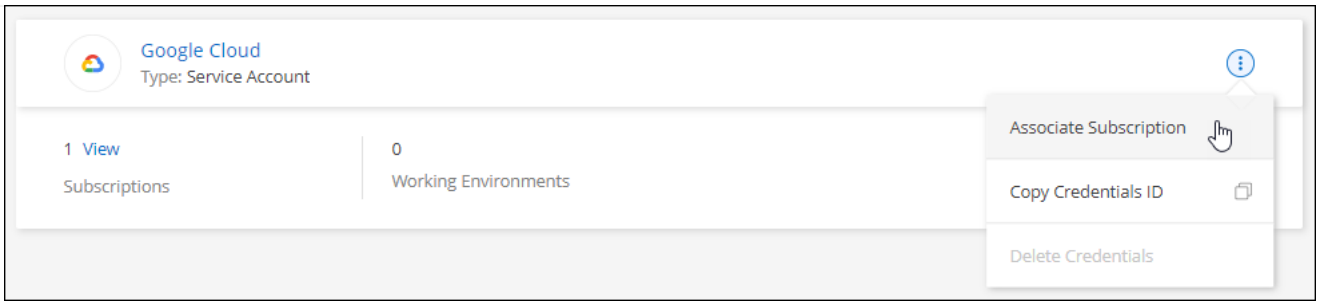
   Pour toutes les autres organisations ou comptes, vous devrez associer manuellement l'abonnement en répétant ces étapes.

   ◦ Sélectionnez **Enregistrer**.

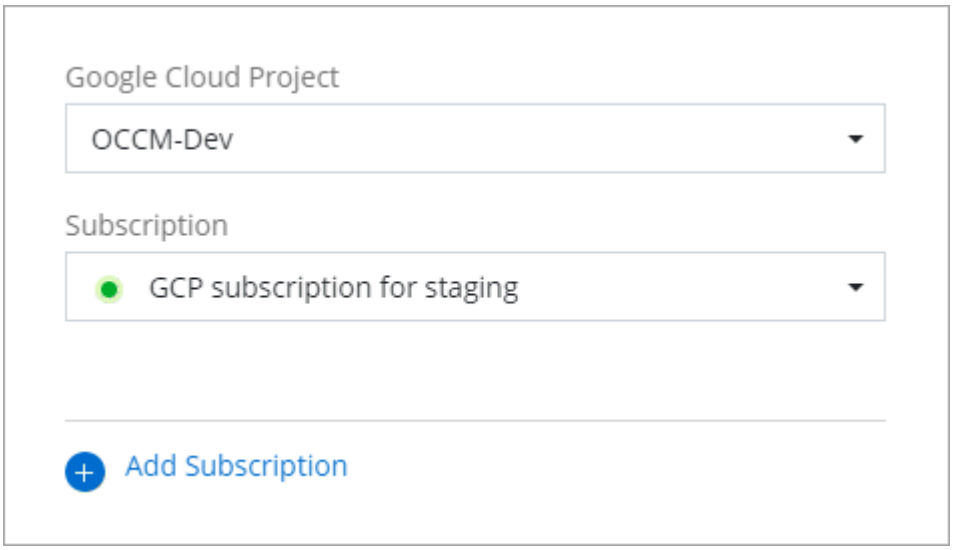
Google Cloud

Étapes

1. Sélectionnez **Administration > Informations d'identification**.
2. Sélectionnez **Informations d'identification de l'organisation**.
3. Sélectionnez le menu d'action pour un ensemble d'informations d'identification associées à un agent de console, puis sélectionnez **Configurer l'abonnement**.



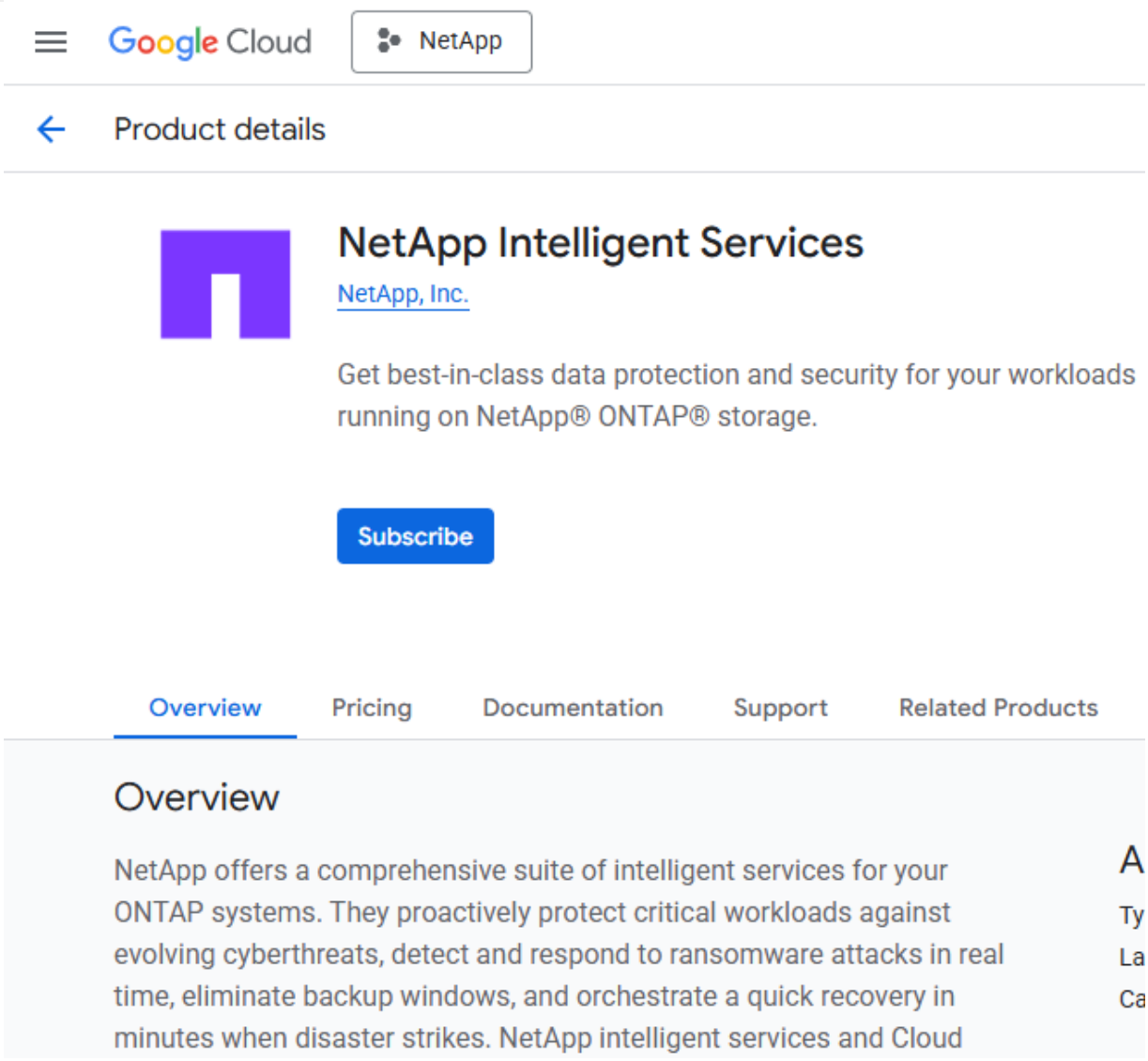
1. Pour configurer un abonnement existant avec les informations d'identification sélectionnées, sélectionnez un projet et un abonnement Google Cloud dans la liste déroulante, puis sélectionnez **Configurer**.



2. Si vous n'avez pas encore d'abonnement, sélectionnez **Ajouter un abonnement > Continuer** et suivez les étapes dans Google Cloud Marketplace.

Avant d'effectuer les étapes suivantes, assurez-vous que vous disposez des privilèges d'administrateur de facturation dans votre compte Google Cloud ainsi que d'une connexion à la NetApp Console .

a. Après avoir été redirigé vers le "Page des NetApp Intelligent Services sur Google Cloud Marketplace" , assurez-vous que le bon projet est sélectionné dans le menu de navigation supérieur.

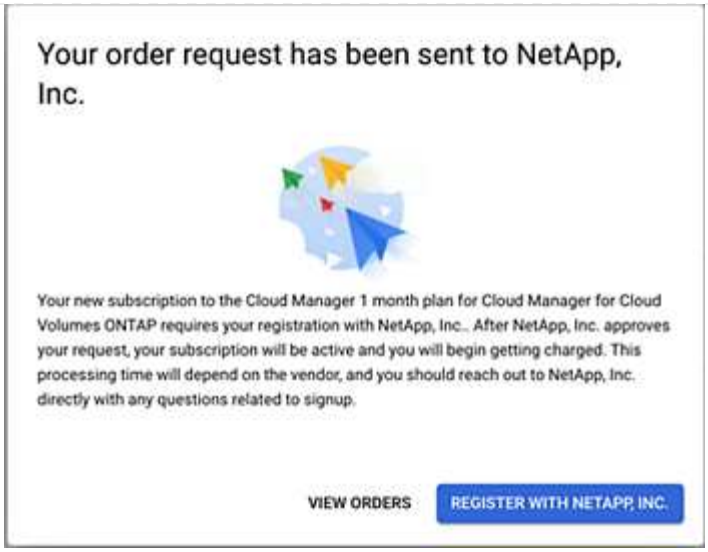


b. Sélectionnez **S'abonner**.
c. Sélectionnez le compte de facturation approprié et acceptez les conditions générales.
d. Sélectionnez **S'abonner**.

   Cette étape envoie votre demande de transfert à NetApp.

e. Dans la boîte de dialogue contextuelle, sélectionnez **S'inscrire auprès de NetApp, Inc.**

   Cette étape doit être effectuée pour lier l'abonnement Google Cloud à votre organisation ou compte Console. Le processus de liaison d'un abonnement n'est pas terminé tant que vous n'êtes pas redirigé depuis cette page et que vous ne vous connectez pas à la console.



f. Suivez les étapes sur la page **Affectation d'abonnement** :

> Si quelqu'un de votre organisation possède déjà un abonnement au marché à partir de votre compte de facturation, vous serez redirigé vers "la page Cloud Volumes ONTAP dans la NetApp Console" plutôt. Si cela est inattendu, contactez votre équipe commerciale NetApp . Google n'autorise qu'un seul abonnement par compte de facturation Google.

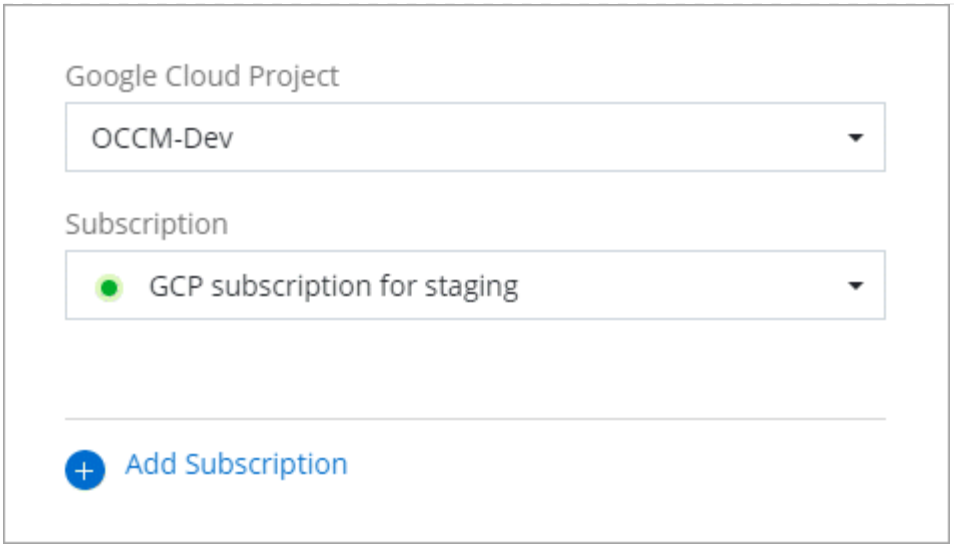
- Sélectionnez l'organisation de la console à laquelle vous souhaitez associer cet abonnement.
- Dans le champ **Remplacer l'abonnement existant**, choisissez si vous souhaitez remplacer automatiquement l'abonnement existant d'une organisation par ce nouvel abonnement.

  La console remplace l'abonnement existant pour toutes les informations d'identification de l'organisation par ce nouvel abonnement. Si un ensemble d'informations d'identification n'a jamais été associé à un abonnement, ce nouvel abonnement ne sera pas associé à ces informations d'identification.

Pour toutes les autres organisations ou comptes, vous devrez associer manuellement l'abonnement en répétant ces étapes.

- Sélectionnez **Enregistrer**.

3. Une fois ce processus terminé, revenez à la page Informations d'identification dans la console et sélectionnez ce nouvel abonnement.



Informations connexes

- "Gérer les licences basées sur la capacité BYOL pour Cloud Volumes ONTAP"
- "Gérer les licences BYOL pour les services de données"
- "Gérer les informations d'identification et les abonnements AWS"
- "Gérer les informations d'identification et les abonnements Azure"
- "Gérer les informations d'identification et les abonnements Google Cloud"

Ce que vous pouvez faire ensuite (mode restreint)

Une fois que vous êtes opérationnel avec NetApp Console en mode restreint, vous pouvez commencer à utiliser les services pris en charge par le mode restreint.

Pour obtenir de l'aide, reportez-vous à la documentation de ces services :

- "Documentation Azure NetApp Files"
- "Documents de sauvegarde et de récupération"
- "Documents de classification"
- "Documentation Cloud Volumes ONTAP"
- "Documents sur le portefeuille numérique"
- "Documentation du cluster ONTAP sur site"
- "Documents de réplication"

Informations connexes

"Modes de déploiement de la NetApp Console"

Informations sur le copyright

Informations sur les marques commerciales