Déployer un agent de console

NetApp Console setup and administration

NetApp
February 09, 2026

Sommaire

Déployer un agent de console

AWS

Options d’installation de l’agent de console dans AWS

Il existe plusieurs manières différentes de créer un agent de console dans AWS. Le moyen le plus courant est d’accéder directement à partir de la NetApp Console .

Les options d’installation suivantes sont disponibles :

- "Créez l’agent de console directement depuis la console"(c’est l’option standard)

  Cette action lance une instance EC2 exécutant Linux et le logiciel agent de console dans un VPC de votre choix.

- "Créer un agent de console à partir d’AWS Marketplace"

  Cette action lance également une instance EC2 exécutant Linux et le logiciel agent de la console, mais le déploiement est lancé directement à partir d’AWS Marketplace, plutôt qu’à partir de la console.

- "Téléchargez et installez manuellement le logiciel sur votre propre hôte Linux"

L’option d’installation que vous choisissez a un impact sur la manière dont vous vous préparez à l’installation. Cela inclut la manière dont vous fournissez à la console les autorisations requises dont elle a besoin pour authentifier et gérer les ressources dans AWS.

Créer un agent de console dans AWS à partir de la NetApp Console

Vous pouvez créer un agent de console dans AWS directement à partir de la NetApp Console. Avant de créer un agent de console dans AWS à partir de la console, vous devez configurer votre réseau et préparer les autorisations AWS.

Avant de commencer

- Vous devriez avoir un"compréhension des agents de console" .
- Vous devriez revoir"Limitations de l’agent de console" .

Étape 1 : Configurer la mise en réseau pour déployer un agent de console dans AWS

Assurez-vous que l’emplacement réseau où vous prévoyez d’installer l’agent de console prend en charge les exigences suivantes. Ces exigences permettent à l’agent de console de gérer les ressources et les processus dans votre cloud hybride.

VPC et sous-réseau

Lorsque vous créez l’agent de console, vous devez spécifier le VPC et le sous-réseau où il doit résider.

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 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.

Points de terminaison contactés depuis la console NetApp

Lorsque vous utilisez la NetApp Console Web fournie via la couche SaaS, elle contacte plusieurs points de terminaison pour effectuer des tâches de gestion des données. Cela inclut les points de terminaison contactés pour déployer l'agent de console à partir de la console.

"Afficher la liste des points de terminaison contactés depuis la console NetApp" .

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"

Vous devrez implémenter cette exigence de mise en réseau après avoir créé l'agent de console.

Étape 2 : configurer les autorisations AWS pour l'agent de la console

La console doit s'authentifier auprès d'AWS avant de pouvoir déployer l'agent de console dans votre VPC. Vous pouvez choisir l'une de ces méthodes d'authentification :

- Laissez la console assumer un rôle IAM disposant des autorisations requises
- Fournissez une clé d'accès AWS et une clé secrète pour un utilisateur IAM disposant des autorisations requises

Quelle que soit l'option choisie, la première étape consiste à créer une politique IAM. Cette politique contient uniquement les autorisations nécessaires pour lancer l'agent de console dans AWS à partir de la console.

Si nécessaire, vous pouvez restreindre la politique IAM en utilisant l'IAM `Condition` élément. "Documentation AWS : élément de condition"

Étapes

1. Accédez à la console AWS IAM.
2. Sélectionnez **Politiques > Créer une politique**.
3. Sélectionnez **JSON**.
4. Copiez et collez la politique suivante :

   Cette politique contient uniquement les autorisations nécessaires pour lancer l'agent de console dans AWS à partir de la console. Lorsque la console crée l'agent de console, elle applique un nouvel ensemble d'autorisations à l'agent de console qui permet à l'agent de console de gérer les ressources AWS. "Afficher

les autorisations requises pour l'agent de la console lui-même".

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "iam:PassRole",
        "iam:ListRoles",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
```

```
            "cloudformation:DescribeStackEvents",
            "cloudformation:ValidateTemplate",
            "ec2:AssociateIamInstanceProfile",
            "ec2:DescribeIamInstanceProfileAssociations",
            "ec2:DisassociateIamInstanceProfile",
            "iam:GetRole",
            "iam:TagRole",
            "kms:ListAliases",
            "cloudformation:ListStacks"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:TerminateInstances"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/OCCMInstance": "*"
            }
        },
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ]
    }
  ]
}
```

5. Sélectionnez **Suivant** et ajoutez des balises, si nécessaire.
6. Sélectionnez **Suivant** et entrez un nom et une description.
7. Sélectionnez **Créer une politique**.
8. Attachez la politique à un rôle IAM que la console peut assumer ou à un utilisateur IAM afin de pouvoir fournir à la console des clés d'accès :
   - (Option 1) Configurez un rôle IAM que la console peut assumer :
     i. Accédez à la console AWS IAM dans le compte cible.
     ii. Sous Gestion des accès, sélectionnez **Rôles > Créer un rôle** et suivez les étapes pour créer le rôle.
     iii. Sous **Type d'entité approuvée**, sélectionnez **Compte AWS**.
     iv. Sélectionnez **Un autre compte AWS** et saisissez l'ID du compte SaaS de la console : 952013314444
     v. Sélectionnez la politique que vous avez créée dans la section précédente.
     vi. Après avoir créé le rôle, copiez l'ARN du rôle afin de pouvoir le coller dans la console lorsque vous créez l'agent de console.

- (Option 2) Configurez les autorisations pour un utilisateur IAM afin de pouvoir fournir à la console des clés d'accès :
  i. Depuis la console AWS IAM, sélectionnez **Utilisateurs**, puis sélectionnez le nom d'utilisateur.
  ii. Sélectionnez **Ajouter des autorisations > Joindre directement les politiques existantes**.
  iii. Sélectionnez la politique que vous avez créée.
  iv. Sélectionnez **Suivant** puis sélectionnez **Ajouter des autorisations**.
  v. Assurez-vous que vous disposez de la clé d'accès et de la clé secrète de l'utilisateur IAM.

Résultat

Vous devriez maintenant avoir un rôle IAM disposant des autorisations requises ou un utilisateur IAM disposant des autorisations requises. Lorsque vous créez l'agent de console à partir de la console, vous pouvez fournir des informations sur le rôle ou les clés d'accès.

Étape 3 : Créer l'agent de console

Créez l'agent de console directement à partir de la console Web.

À propos de cette tâche

- La création de l'agent de console à partir de la console déploie une instance EC2 dans AWS à l'aide d'une configuration par défaut. Ne passez pas à une instance EC2 plus petite avec moins de processeurs ou moins de RAM après avoir créé l'agent de console. "En savoir plus sur la configuration par défaut de l'agent de console" .
- Lorsque la console crée l'agent de console, elle crée un rôle IAM et un profil pour l'agent. Ce rôle inclut des autorisations qui permettent à l'agent de la console de gérer les ressources AWS. Assurez-vous que le rôle est mis à jour à mesure que de nouvelles autorisations sont ajoutées dans les versions futures. "En savoir plus sur la politique IAM pour l'agent de console".

Avant de commencer

Vous devriez avoir les éléments suivants :

- Une méthode d'authentification AWS : soit un rôle IAM, soit des clés d'accès pour un utilisateur IAM avec les autorisations requises.
- Un VPC et un sous-réseau qui répondent aux exigences de mise en réseau.
- Une paire de clés pour l'instance EC2.
- Détails sur un serveur proxy, si un proxy est requis pour l'accès Internet à partir de l'agent de la console.
- Installation"exigences de mise en réseau" .
- Installation"Autorisations AWS" .

Étapes

1. Sélectionnez **Administration > Agents**.
2. Sur la page **Aperçu**, sélectionnez **Déployer l'agent > AWS**
3. Suivez les étapes de l'assistant pour créer l'agent de console :
4. Sur la page **Introduction**, vous trouverez un aperçu du processus
5. Sur la page **Informations d'identification AWS**, spécifiez votre région AWS, puis choisissez une méthode d'authentification, qui est soit un rôle IAM que la console peut assumer, soit une clé d'accès AWS et une clé secrète.

Si vous choisissez **Assumer le rôle**, vous pouvez créer le premier ensemble d'informations d'identification à partir de l'assistant de déploiement de l'agent de console. Tout ensemble d'informations d'identification supplémentaire doit être créé à partir de la page Informations d'identification. Ils seront ensuite disponibles depuis l'assistant dans une liste déroulante. "Apprenez à ajouter des informations d'identification supplémentaires" .

6. Sur la page **Détails**, fournissez des détails sur l'agent de la console.
   - Entrez un nom.
   - Ajouter des balises personnalisées (métadonnées).
   - Choisissez si vous souhaitez que la console crée un nouveau rôle doté des autorisations requises ou si vous souhaitez sélectionner un rôle existant que vous avez configuré avec"les autorisations requises" .
   - Choisissez si vous souhaitez crypter les disques EBS de l'agent de console. Vous avez la possibilité d'utiliser la clé de chiffrement par défaut ou d'utiliser une clé personnalisée.
7. Sur la page **Réseau**, spécifiez un VPC, un sous-réseau et une paire de clés pour l'agent, choisissez d'activer ou non une adresse IP publique et spécifiez éventuellement une configuration de proxy.

   Assurez-vous que vous disposez de la paire de clés correcte pour accéder à la machine virtuelle de l'agent de console. Sans une paire de clés, vous ne pouvez pas y accéder.

8. Sur la page **Groupe de sécurité**, choisissez de créer un nouveau groupe de sécurité ou de sélectionner un groupe de sécurité existant qui autorise les règles entrantes et sortantes requises.

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

9. Vérifiez vos sélections pour vérifier que votre configuration est correcte.

   a. La case à cocher **Valider la configuration de l'agent** est cochée par défaut pour que la console valide les exigences de connectivité réseau lors du déploiement. Si la console ne parvient pas à déployer l'agent, elle fournit un rapport pour vous aider à résoudre le problème. Si le déploiement réussit, aucun rapport n'est fourni.

   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, décochez la case pour ignorer la vérification de validation.

10. Sélectionnez **Ajouter**.

    La console déploie l'agent en 10 minutes environ. Restez sur la page jusqu'à ce que le processus soit terminé.

Résultat

Une fois le processus terminé, l'agent de la console peut être utilisé à partir de la console.

Si le déploiement échoue, vous pouvez télécharger un rapport et des journaux depuis la console pour vous aider à résoudre les problèmes."Découvrez comment résoudre les problèmes d'installation."

Si vous avez des compartiments Amazon S3 dans le même compte AWS où vous avez créé l'agent de console, vous verrez un environnement de travail Amazon S3 apparaître automatiquement sur la page **Systèmes**. "Apprenez à gérer les buckets S3 depuis la NetApp Console"

Créer un agent de console à partir d'AWS Marketplace

Vous créez un agent de console dans AWS directement à partir d'AWS Marketplace. Pour créer un agent de console à partir d'AWS Marketplace, vous devez configurer votre réseau, préparer les autorisations AWS, vérifier les exigences de l'instance, puis créer l'agent de console.

Avant de commencer

- Vous devriez avoir un"compréhension des agents de console" .
- Vous devriez revoir"Limitations de l'agent de console" .

Étape 1 : Configurer le réseau

Assurez-vous que l'emplacement réseau de l'agent de console répond aux exigences suivantes pour gérer les ressources de cloud hybride.

VPC et sous-réseau

Lorsque vous créez l'agent de console, vous devez spécifier le VPC et le sous-réseau où il doit résider.

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 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"

Points de terminaison	But
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.
\ 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"

Implémentez cet accès réseau après avoir créé l'agent de console.

Étape 2 : configurer les autorisations AWS

Pour préparer un déploiement sur une place de marché, créez des stratégies IAM dans AWS et attachez-les à un rôle IAM. Lorsque vous créez l'agent de console à partir d'AWS Marketplace, vous êtes invité à sélectionner ce 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.

      Vous devrez peut-être créer une deuxième stratégie en fonction des services de données NetApp que vous prévoyez d'utiliser. 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. 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 que vous pouvez associer à l'instance EC2 lors du déploiement à partir d'AWS Marketplace.

Étape 3 : Examiner les exigences de l'instance

Lorsque vous créez l'agent de console, vous devez choisir un type d'instance EC2 qui répond aux exigences suivantes.

processeur

8 cœurs ou 8 vCPU

BÉLIER
32 Go

Type d'instance AWS EC2
Un type d'instance qui répond aux exigences de CPU et de RAM. NetApp recommande t3.2xlarge.

Étape 4 : Créer l'agent de console

Créez l'agent de console directement à partir d'AWS Marketplace.

À propos de cette tâche

La création de l'agent de console à partir d'AWS Marketplace déploie une instance EC2 dans AWS à l'aide d'une configuration par défaut. "En savoir plus sur la configuration par défaut de l'agent de console" .

Avant de commencer

Vous devriez avoir les éléments suivants :

- Un VPC et un sous-réseau qui répondent aux exigences de mise en réseau.
- Un rôle IAM avec une politique attachée qui inclut les autorisations requises pour l'agent de la console.
- 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'instance.
- 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**.

  AWS lance l'agent de console avec les paramètres spécifiés et l'agent de console s'exécute en environ dix minutes.

  Si l'installation échoue, vous pouvez consulter les journaux et un rapport pour vous aider à résoudre le problème."Découvrez comment résoudre les problèmes d'installation."

8. Ouvrez un navigateur Web à partir d'un hôte disposant d'une connexion à la machine virtuelle de l'agent de console et à l'URL de l'agent de console.
9. Après vous être connecté, configurez l'agent de 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.

      Gardez le mode restreint désactivé pour utiliser la console en mode standard. Vous devez activer le mode restreint uniquement si vous disposez d'un environnement sécurisé et souhaitez déconnecter ce compte des services backend de la console. Si c'est le cas,"suivez les étapes pour démarrer avec la NetApp Console en mode restreint" .
   d. Sélectionnez **Commençons**.

Résultat

L'agent de console est maintenant installé et configuré avec votre organisation de console.

Ouvrez un navigateur Web et accédez à la "NetApp Console" pour commencer à utiliser l'agent Console avec la Console.

Si vous avez des compartiments Amazon S3 dans le même compte AWS où vous avez créé l'agent de console, vous verrez un environnement de travail Amazon S3 apparaître automatiquement sur la page **Systèmes**. "Apprenez à gérer les buckets S3 depuis la NetApp Console"

Installer manuellement l'agent de console dans AWS

Vous pouvez installer manuellement un agent de console sur un hôte Linux exécuté dans

AWS. Pour installer manuellement l'agent de console sur votre propre hôte Linux, vous devez vérifier les exigences de l'hôte, configurer votre réseau, préparer les autorisations AWS, installer l'agent de console, puis fournir les autorisations que vous avez préparées.

Avant de commencer

- Vous devriez avoir un"compréhension des agents de console" .
- Vous devriez revoir"Limitations de l'agent de console" .

Étape 1 : Examiner les exigences de l'hôte

Assurez-vous que l'hôte exécutant le logiciel agent Console respecte les exigences en matière de système d'exploitation, de RAM et de ports.

> 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.

Type d'instance AWS EC2

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

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 .
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 .

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		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
Docker Engine 23.06 à 28.0.0.	Non pris en charge		22,04 LTS	3.9.50 ou version ultérieure

Paire de clés

Lorsque vous créez l'agent de console, vous devez sélectionner une paire de clés EC2 à utiliser avec l'instance.

Limite de saut de réponse PUT lors de l'utilisation d'IMDSv2

Si IMDSv2 est activé (paramètre par défaut pour les nouvelles instances EC2), définissez la limite de sauts de réponse PUT sur 3. Sinon, le système affichera une erreur d'initialisation de l'interface utilisateur lors de la configuration de l'agent.

- "Exiger l'utilisation d'IMDSv2 sur les instances Amazon EC2"
- "Documentation AWS : Modifier la limite de saut de réponse PUT"

Étape 2 : 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
```

Étape 3 : Configurer le réseau

Assurez-vous que l'emplacement réseau réponde aux exigences suivantes afin que l'agent de la console puisse gérer les ressources de votre cloud hybride.

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.

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 .

Points de terminaison	But
\ 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.
\ 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"

Étape 4 : configurer les autorisations AWS pour la console

Accordez les autorisations AWS à la NetApp Console en utilisant l'une de ces options :

- Option 1 : créez des stratégies IAM et attachez-les à un rôle IAM que vous pouvez associer à l'instance EC2.
- Option 2 : fournissez à la console la clé d'accès AWS pour un utilisateur IAM disposant des autorisations requises.

Suivez les étapes pour préparer les autorisations pour la console.

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 politique. 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. 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 que vous pouvez associer à l'instance EC2 après avoir installé l'agent de console.

Clé d'accès AWS

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 disposez désormais d'un utilisateur IAM disposant des autorisations requises et d'une clé d'accès que vous pouvez fournir à la console.

Étape 5 : Installer l'agent de console

Une fois les prérequis remplis, installez manuellement le logiciel sur votre hôte Linux.

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.

2. Attendez que l'installation soit terminée.

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

   Si l'installation échoue, vous pouvez consulter le rapport d'installation et les journaux pour vous aider à résoudre les problèmes."Découvrez comment résoudre les problèmes d'installation."

1. Ouvrez un navigateur Web à partir d'un hôte disposant d'une connexion à la machine virtuelle de l'agent de console et entrez l'URL suivante :

   https://ipaddress

2. Après vous être connecté, configurez l'agent de la console :

   a. Spécifiez l'organisation 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.

      Vous devez garder le mode restreint désactivé car ces étapes décrivent comment utiliser la console en mode standard. Vous devez activer le mode restreint uniquement si vous disposez d'un environnement sécurisé et souhaitez déconnecter ce compte des services backend. Si c'est le cas,"suivez les étapes pour démarrer avec la NetApp Console en mode restreint" .

   d. Sélectionnez **Commençons**.

Si vous avez des compartiments Amazon S3 dans le même compte AWS où vous avez créé l'agent de console, vous verrez un système de stockage Amazon S3 apparaître automatiquement sur la page **Systèmes**.

"Découvrez comment gérer les buckets S3 à partir de NetApp ConsoleP"

Étape 6 : Accorder des autorisations à la NetApp Console

Après avoir installé l'agent Console, accordez-lui les autorisations AWS que vous avez configurées afin qu'il puisse gérer vos données et votre infrastructure de stockage sur AWS.

Rôle IAM

Associez le rôle IAM que vous créez à l'instance EC2 de l'agent de console.

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**.

Aller à la "NetApp Console" pour commencer à utiliser l'agent de console.

Clé d'accès AWS

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

Étapes

1. Assurez-vous que l'agent de console correct est actuellement sélectionné dans la console.
2. Sélectionnez **Administration > Informations d'identification**.
3. Sélectionnez **Informations d'identification de l'organisation**.
4. 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**.

Aller à la "NetApp Console" pour commencer à utiliser l'agent de console.

Azuré

Options d'installation de l'agent de console dans Azure

Il existe plusieurs manières différentes de créer un agent de console dans Azure. Le moyen le plus courant est d'accéder directement à partir de la NetApp Console .

Les options d'installation suivantes sont disponibles :

- "Créer un agent de console directement à partir de la NetApp Console"(c'est l'option standard)

  Cette action lance une machine virtuelle exécutant Linux et le logiciel agent de console dans un réseau virtuel de votre choix.

- "Créer un agent de console à partir de la place de marché Azure"

  Cette action lance également une machine virtuelle exécutant Linux et le logiciel agent de la console, mais le déploiement est lancé directement à partir de la Place de marché Azure, plutôt qu'à partir de la console.

- "Téléchargez et installez manuellement le logiciel sur votre propre hôte Linux"

L'option d'installation que vous choisissez a un impact sur la manière dont vous vous préparez à l'installation. Cela inclut la manière dont vous fournissez à l'agent de console les autorisations requises dont il a besoin pour authentifier et gérer les ressources dans Azure.

Créer un agent de console dans Azure à partir de la NetApp Console

Pour créer un agent de console dans Azure à partir de la NetApp Console, vous devez configurer votre réseau, préparer les autorisations Azure, puis créer l'agent de console.

Avant de commencer

- Vous devriez avoir un"compréhension des agents de console" .
- Vous devriez revoir"Limitations de l'agent de console" .

Étape 1 : Configurer le réseau

Assurez-vous que l'emplacement réseau où vous prévoyez d'installer l'agent de console prend en charge les exigences suivantes. Ces exigences permettent à l'agent de console de gérer les ressources du cloud hybride.

région Azure

Si vous utilisez Cloud Volumes ONTAP, l'agent de console doit être déployé dans la même région Azure que les systèmes Cloud Volumes ONTAP qu'il gère, ou dans la "Paire de régions Azure" pour les systèmes Cloud Volumes ONTAP . Cette exigence garantit qu'une connexion Azure Private Link est utilisée entre Cloud Volumes ONTAP et ses comptes de stockage associés.

"Découvrez comment Cloud Volumes ONTAP utilise un lien privé Azure"

VNet et sous-réseau

Lorsque vous créez l'agent de console, vous devez spécifier le réseau virtuel et le sous-réseau sur lesquels il doit résider.

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 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
\ 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.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.

Points de terminaison contactés depuis la console NetApp

Lorsque vous utilisez la NetApp Console Web fournie via la couche SaaS, elle contacte plusieurs points de terminaison pour effectuer des tâches de gestion des données. Cela inclut les points de terminaison contactés pour déployer l'agent de console à partir de la console.

"Afficher la liste des points de terminaison contactés depuis la console NetApp" .

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"

Vous devez implémenter cette exigence de mise en réseau après avoir créé l'agent de console.

Étape 2 : Créer une stratégie de déploiement d'agent de console (rôle personnalisé)

Vous devez créer un rôle personnalisé disposant des autorisations nécessaires pour déployer l'agent de console dans Azure.

Créez un rôle personnalisé Azure que vous pouvez attribuer à votre compte Azure ou à un principal de service Microsoft Entra. La console s'authentifie auprès d'Azure et utilise ces autorisations pour créer l'agent de console en votre nom.

La console déploie la machine virtuelle de l'agent de console dans Azure, active un "identité gérée attribuée par le système" , crée le rôle requis et l'attribue à la machine virtuelle. "Examiner comment la console utilise les autorisations" .

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. Copiez les autorisations requises pour un nouveau rôle personnalisé dans Azure et enregistrez-les dans un fichier JSON.

   Ce rôle personnalisé contient uniquement les autorisations nécessaires pour lancer la machine virtuelle de l'agent de console dans Azure à partir de la console. N'utilisez pas cette politique pour d'autres situations. Lorsque la console crée l'agent de console, elle applique un nouvel ensemble d'autorisations à la machine virtuelle de l'agent de console qui permet à l'agent de console de gérer les ressources Azure.

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
```

```
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/read",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/rea
d",
    "Microsoft.Network/networkInterfaces/ipConfigurations/read",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Resources/deployments/validate/action",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/operationresults/read",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
```

```
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Authorization/roleDefinitions/write",
    "Microsoft.Authorization/roleAssignments/write",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Authorization/roleAssignments/read"
  ],
  "NotActions": [],
  "AssignableScopes": [],
  "Description": "Azure SetupAsService",
  "IsCustom": "true"
}
```

2. Modifiez le JSON en ajoutant votre ID d'abonnement Azure à l'étendue attribuable.

   Exemple

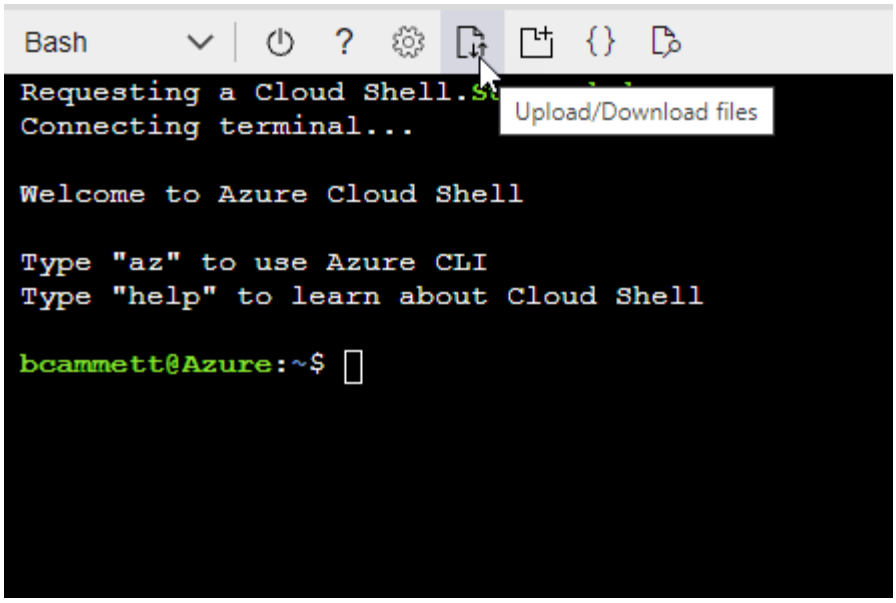
```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
]
```

3. 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. Entrez la commande Azure CLI suivante :

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

Vous disposez désormais d'un rôle personnalisé appelé *Azure SetupAsService*. Vous pouvez appliquer ce rôle personnalisé à votre compte utilisateur ou à un principal de service.

Étape 3 : Configurer l'authentification

Lors de la création de l'agent de console à partir de la console, vous devez fournir une connexion qui permet à la console de s'authentifier auprès d'Azure et de déployer la machine virtuelle. Vous avez deux options :

1. Sign in avec votre compte Azure lorsque vous y êtes invité. Ce compte doit disposer d'autorisations Azure spécifiques. Il s'agit de l'option par défaut.
2. Fournissez des détails sur un principal de service Microsoft Entra. Ce principal de service nécessite également des autorisations spécifiques.

Suivez les étapes pour préparer l'une de ces méthodes d'authentification à utiliser avec la console.

Compte Azure

Attribuez le rôle personnalisé à l'utilisateur qui déploiera l'agent de la console à partir de la console.

Étapes

1. Dans le portail Azure, ouvrez le service **Abonnements** et sélectionnez l'abonnement de l'utilisateur.
2. Cliquez sur **Contrôle d'accès (IAM)**.
3. Cliquez sur **Ajouter** > **Ajouter une attribution de rôle**, puis ajoutez les autorisations :
   a. Sélectionnez le rôle **Azure SetupAsService** et cliquez sur **Suivant**.

      Azure SetupAsService est le nom par défaut fourni dans la stratégie de déploiement de l'agent de console pour Azure. Si vous avez choisi un nom différent pour le rôle, sélectionnez plutôt ce nom.

   b. Gardez **Utilisateur, groupe ou principal du service** sélectionné.
   c. Cliquez sur **Sélectionner les membres**, choisissez votre compte utilisateur et cliquez sur **Sélectionner**.
   d. Cliquez sur **Suivant**.
   e. Cliquez sur **Réviser + attribuer**.

Principal de service

Au lieu de vous connecter avec votre compte Azure, vous pouvez fournir à la console les informations d'identification d'un principal de service Azure disposant des autorisations requises.

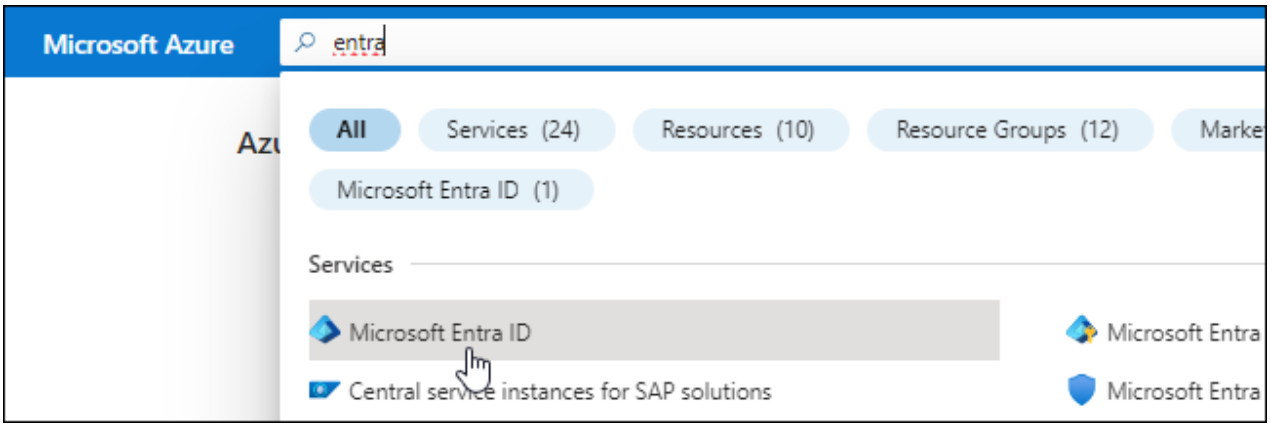
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont la console a besoin.

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**.



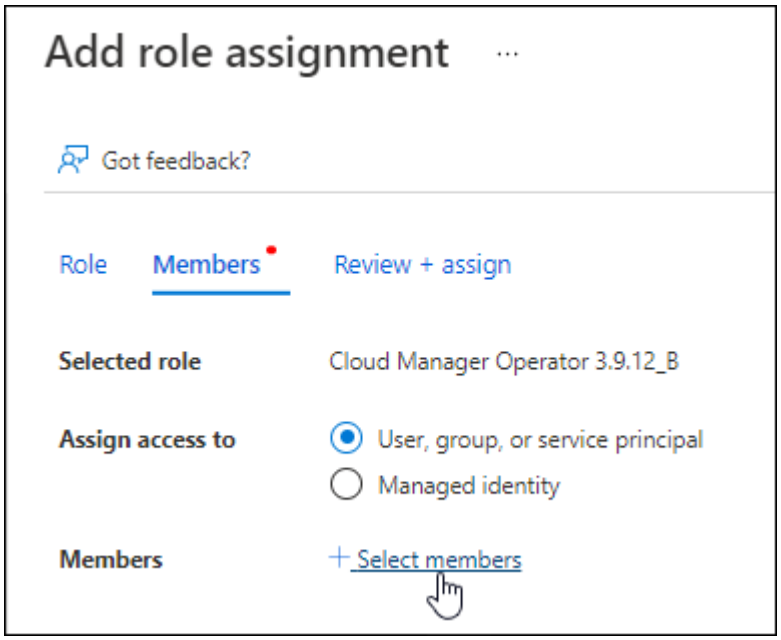
3. Dans le menu, sélectionnez **Inscriptions d'applications**.
4. Sélectionnez **Nouvelle inscription**.

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.

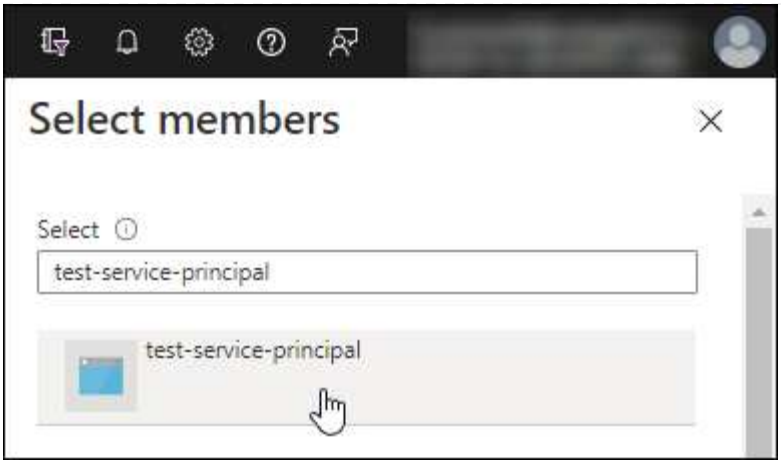
Attribuer le rôle personnalisé à l'application

1. Depuis le portail Azure, ouvrez le service **Abonnements**.
2. Sélectionnez l'abonnement.
3. Cliquez sur **Contrôle d'accès (IAM) > Ajouter > Ajouter une attribution de rôle**.
4. Dans l'onglet **Rôle**, sélectionnez le rôle **Opérateur de console** et cliquez sur **Suivant**.
5. Dans l'onglet **Membres**, procédez comme suit :
   a. Gardez **Utilisateur, groupe ou principal du service** sélectionné.
   b. Cliquez sur **Sélectionner les membres**.



   c. Recherchez le nom de l'application.

      Voici un exemple :



a. Sélectionnez l'application et cliquez sur **Sélectionner**.

b. Cliquez sur **Suivant**.

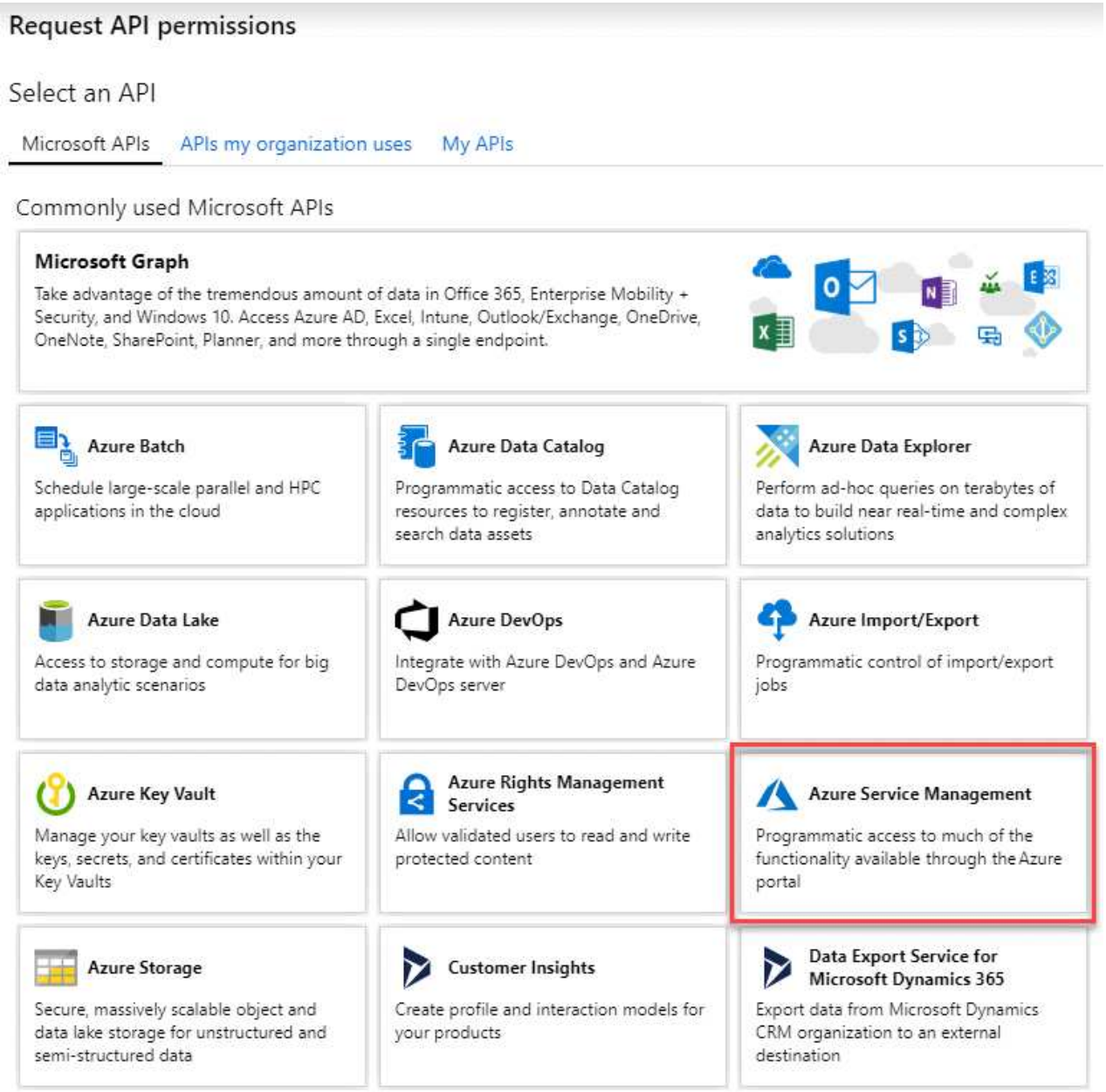
6. Cliquez sur **Réviser + attribuer**.

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

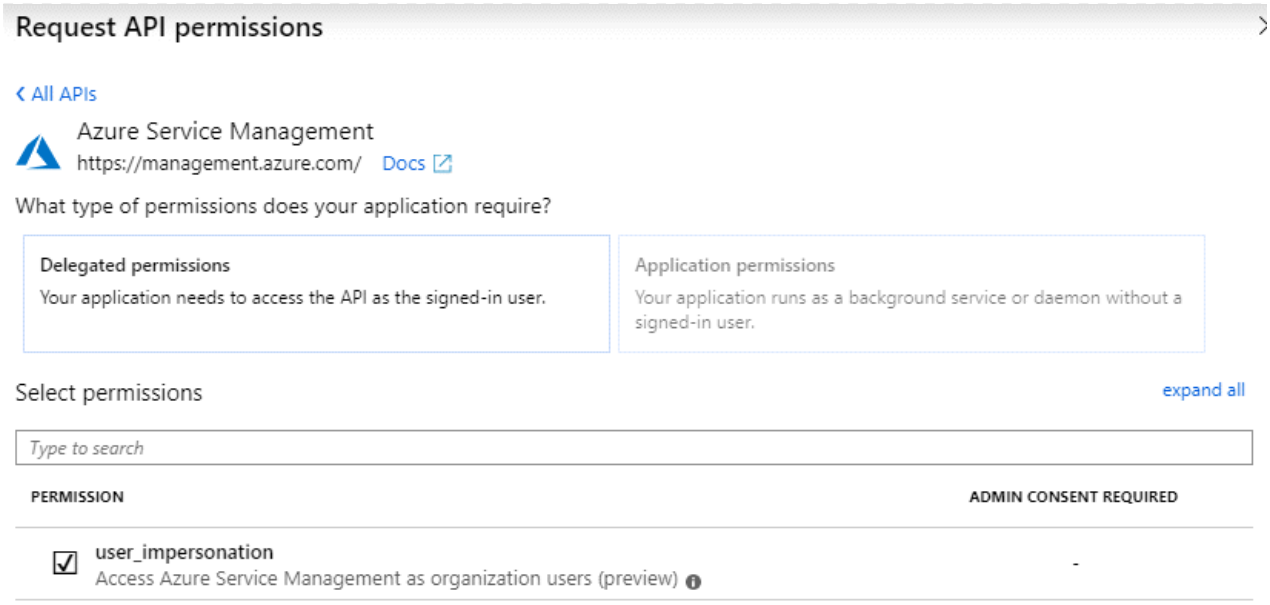
   Si vous souhaitez gérer des ressources dans plusieurs abonnements Azure, vous devez lier le principal de service à chacun de ces abonnements. Par exemple, la console vous permet de sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

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**.

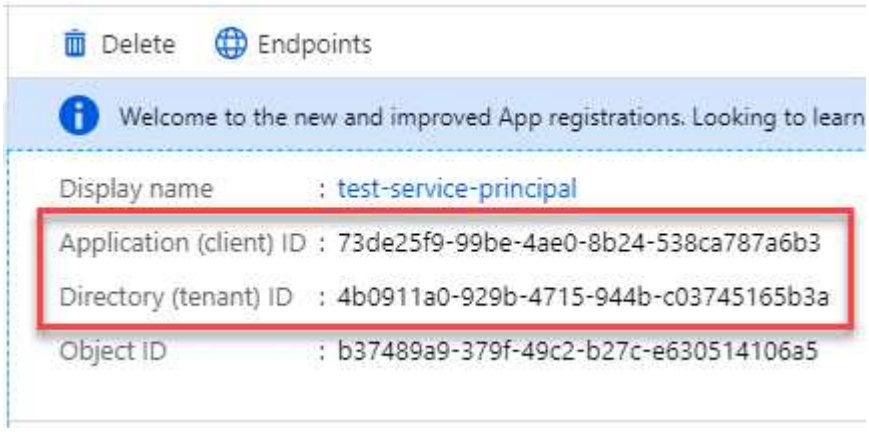


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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 créez l'agent de console.

Étape 4 : Créer l'agent de console

Créez l'agent de console directement à partir de la NetApp Console.

À propos de cette tâche

- La création de l'agent de console à partir de la console déploie une machine virtuelle dans Azure à l'aide d'une configuration par défaut. Ne passez pas à une instance de machine virtuelle plus petite avec moins de processeurs ou moins de RAM après avoir créé l'agent de console. "En savoir plus sur la configuration par défaut de l'agent de console" .
- Lorsque la console déploie l'agent de console, elle crée un rôle personnalisé et l'attribue à la machine virtuelle de l'agent de console. Ce rôle inclut des autorisations qui permettent à l'agent de la console de gérer les ressources Azure. Vous devez vous assurer que le rôle est maintenu à jour à mesure que de nouvelles autorisations sont ajoutées dans les versions ultérieures. "En savoir plus sur le rôle personnalisé de l'agent de console" .

Avant de commencer

Vous devriez avoir les éléments suivants :

- Un abonnement Azure.
- Un réseau virtuel et un sous-réseau dans la région Azure de votre choix.
- Détails sur un serveur proxy, si votre organisation a besoin d'un proxy pour tout le trafic Internet sortant :
  - adresse IP
  - Informations d'identification
  - Certificat HTTPS
- Une clé publique SSH, si vous souhaitez utiliser cette méthode d'authentification pour la machine virtuelle de l'agent de console. L'autre option pour la méthode d'authentification est d'utiliser un mot de passe.

  "En savoir plus sur la connexion à une machine virtuelle Linux dans Azure"

- Si vous ne souhaitez pas que la console crée automatiquement un rôle Azure pour l'agent de la console, vous devrez créer le vôtre."en utilisant la politique sur cette page" .

  Ces autorisations concernent l'agent de console lui-même. Il s'agit d'un ensemble d'autorisations différent de celui que vous avez précédemment configuré pour déployer la machine virtuelle de l'agent de console.

Étapes

1. Sélectionnez **Administration > Agents**.
2. Sur la page **Aperçu**, sélectionnez **Déployer l'agent > Azure**
3. Sur la page **Révision**, examinez les exigences de déploiement d'un agent. Ces exigences sont également détaillées ci-dessus sur cette page.
4. Sur la page **Authentification de la machine virtuelle**, sélectionnez l'option d'authentification qui correspond à la façon dont vous configurez les autorisations Azure :

   - Sélectionnez **Connexion** pour vous connecter à votre compte Microsoft, qui devrait disposer des autorisations requises.

     Le formulaire est détenu et hébergé par Microsoft. Vos informations d'identification ne sont pas fournies à NetApp.

     Si vous êtes déjà connecté à un compte Azure, la console utilise automatiquement ce compte. Si vous possédez plusieurs comptes, vous devrez peut-être d'abord vous déconnecter pour vous assurer que vous utilisez le bon compte.

   - Sélectionnez **Principal du service Active Directory** pour saisir des informations sur le principal du service Microsoft Entra qui accorde les autorisations requises :
     - ID de l'application (client)
     - ID du répertoire (locataire)
     - Secret client

   Découvrez comment obtenir ces valeurs pour un principal de service .

5. Sur la page **Authentification de la machine virtuelle**, choisissez un abonnement Azure, un emplacement, un nouveau groupe de ressources ou un groupe de ressources existant, puis choisissez une méthode d'authentification pour la machine virtuelle de l'agent de console que vous créez.

   La méthode d'authentification de la machine virtuelle peut être un mot de passe ou une clé publique SSH.

   "En savoir plus sur la connexion à une machine virtuelle Linux dans Azure"

6. Sur la page **Détails**, saisissez un nom pour l'agent, spécifiez les balises et choisissez si vous souhaitez que la console crée un nouveau rôle doté des autorisations requises ou si vous souhaitez sélectionner un rôle existant que vous avez configuré avec"les autorisations requises" .

   Notez que vous pouvez choisir les abonnements Azure associés à ce rôle. Chaque abonnement que vous choisissez fournit à l'agent de la console des autorisations pour gérer les ressources de cet abonnement (par exemple, Cloud Volumes ONTAP).

7. Sur la page **Réseau**, choisissez un réseau virtuel et un sous-réseau, activez ou non une adresse IP publique et spécifiez éventuellement une configuration proxy.

   - Sur la page **Groupe de sécurité**, choisissez de créer un nouveau groupe de sécurité ou de sélectionner un groupe de sécurité existant qui autorise les règles entrantes et sortantes requises.

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

8. Vérifiez vos sélections pour vérifier que votre configuration est correcte.

   a. La case à cocher **Valider la configuration de l'agent** est cochée par défaut pour que la console valide

les exigences de connectivité réseau lors du déploiement. Si la console ne parvient pas à déployer l'agent, elle fournit un rapport pour vous aider à résoudre le problème. Si le déploiement réussit, aucun rapport n'est fourni.

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, décochez la case pour ignorer la vérification de validation.

9. Sélectionnez **Ajouter**.

   La console prépare l'agent en 10 minutes environ. Restez sur la page jusqu'à ce que le processus soit terminé.

Résultat

Une fois le processus terminé, l'agent de la console peut être utilisé à partir de la console.

Si le déploiement échoue, vous pouvez télécharger un rapport et des journaux depuis la console pour vous aider à résoudre les problèmes."Découvrez comment résoudre les problèmes d'installation."

Si vous disposez d'un stockage Blob Azure dans le même compte Azure où vous avez créé l'agent de console, vous verrez le stockage Blob Azure apparaître automatiquement sur la page **Systèmes**. "Découvrez comment gérer le stockage Azure Blob depuis la NetApp Console"

Créer un agent de console à partir de la place de marché Azure

Vous pouvez créer un agent de console dans Azure directement à partir de la Place de marché Azure. Pour créer un agent de console à partir de la Place de marché Azure, vous devez configurer votre réseau, préparer les autorisations Azure, examiner les exigences de l'instance, puis créer l'agent de console.

Avant de commencer

- Vous devriez avoir un"compréhension des agents de console" .
- Revoir"Limitations de l'agent de console" .

Étape 1 : Configurer le réseau

Assurez-vous que l'emplacement réseau où vous prévoyez d'installer l'agent de console prend en charge les exigences suivantes. Ces exigences permettent à l'agent de console de gérer les ressources dans votre cloud hybride.

région Azure

Si vous utilisez Cloud Volumes ONTAP, l'agent de console doit être déployé dans la même région Azure que les systèmes Cloud Volumes ONTAP qu'il gère, ou dans la "Paire de régions Azure" pour les systèmes Cloud Volumes ONTAP . Cette exigence garantit qu'une connexion Azure Private Link est utilisée entre Cloud Volumes ONTAP et ses comptes de stockage associés.

"Découvrez comment Cloud Volumes ONTAP utilise un lien privé Azure"

VNet et sous-réseau

Lorsque vous créez l'agent de console, vous devez spécifier le réseau virtuel et le sous-réseau sur lesquels il doit résider.

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 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
\ 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.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"

Implémentez les exigences de mise en réseau après avoir créé l'agent de console.

Étape 2 : Examiner les exigences de la machine virtuelle

Lorsque vous créez l'agent de console, choisissez un type de machine virtuelle qui répond aux exigences suivantes.

processeur

8 cœurs ou 8 vCPU

BÉLIER

32 Go

Taille de la machine virtuelle Azure

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

Étape 3 : Configurer les autorisations

Vous pouvez accorder des autorisations des manières suivantes :

- Option 1 : attribuez un rôle personnalisé à la machine virtuelle Azure à l'aide d'une identité managée attribuée par le système.
- Option 2 : fournissez à la console les informations d'identification d'un principal de service Azure disposant des autorisations requises.

Suivez ces étapes pour configurer les autorisations pour la console.

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"

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.

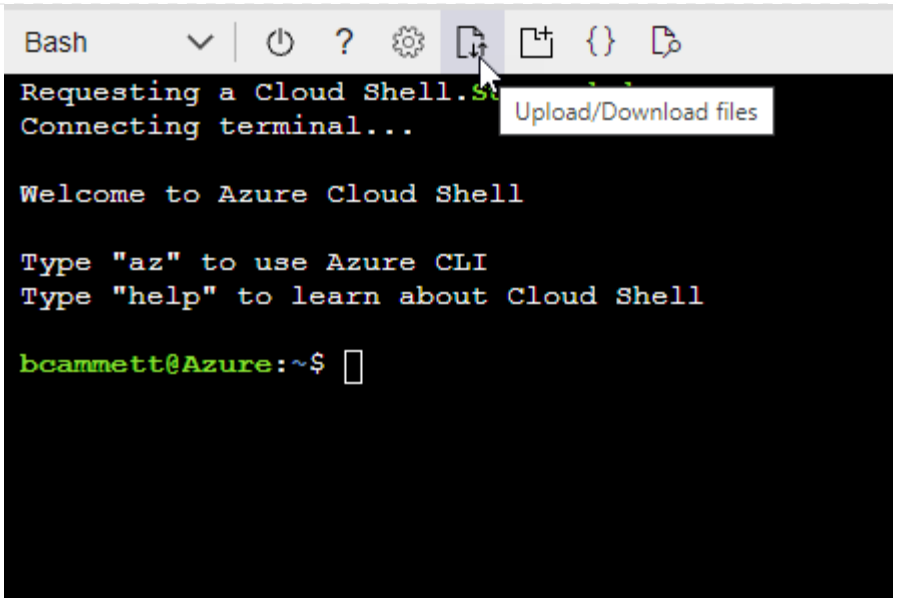
   Exemple

   ```
   "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

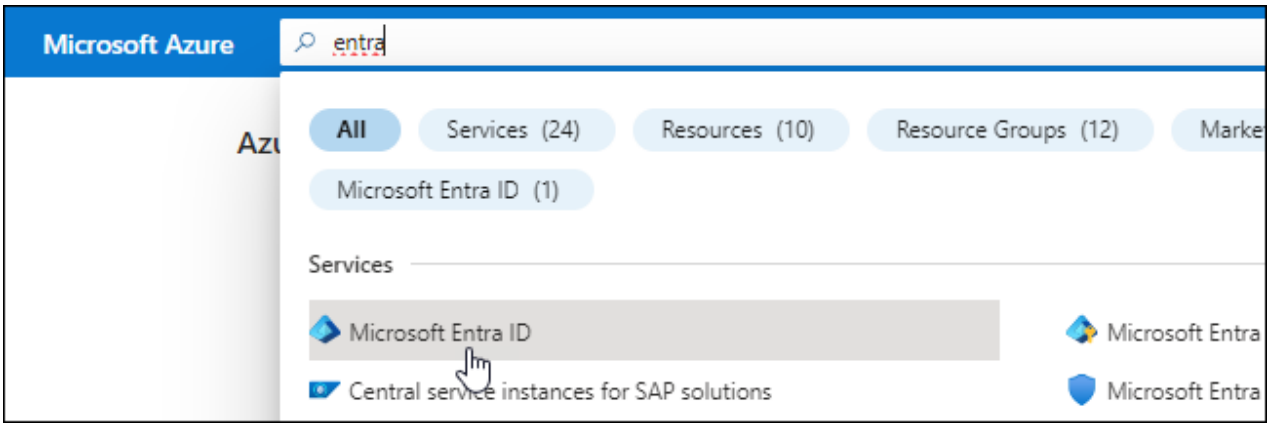
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont la console a besoin.

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 .

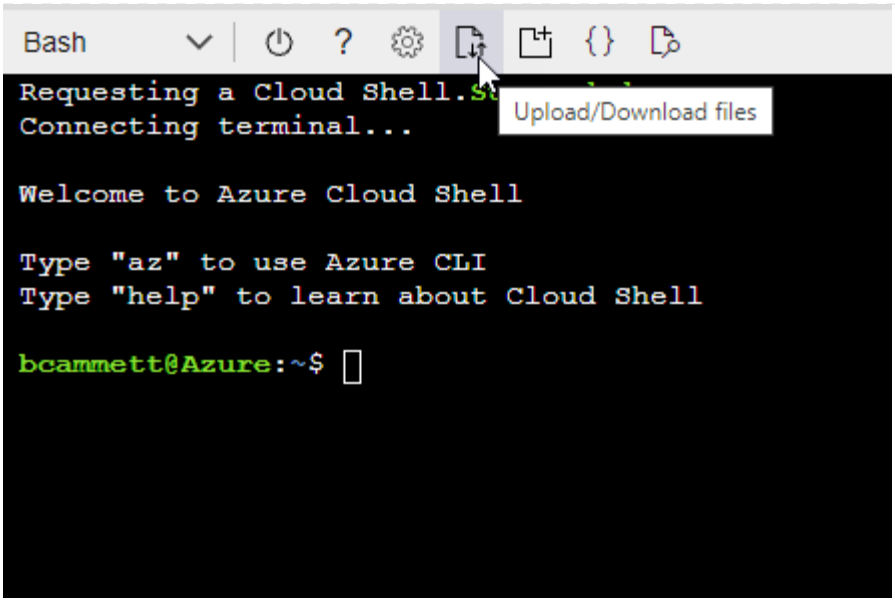
      Exemple

      ```
      "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**.

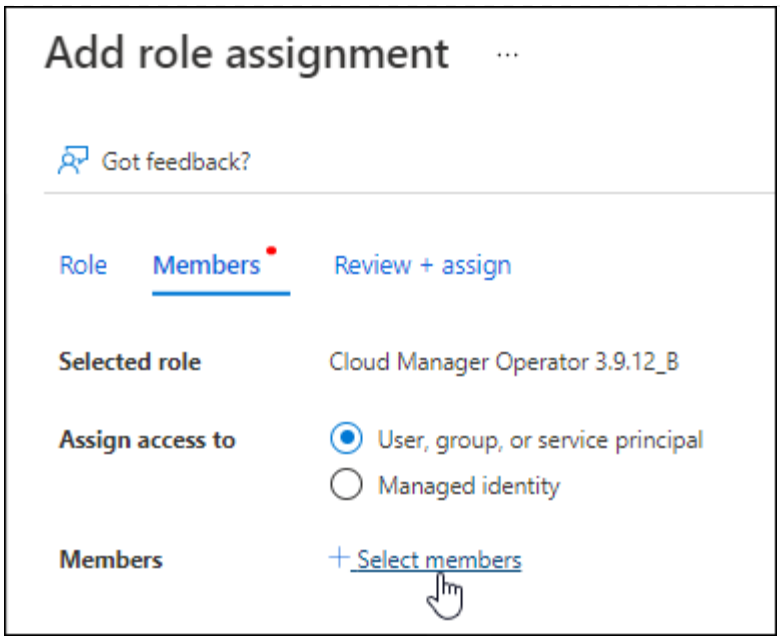
   b. Sélectionnez l'abonnement.

   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**.

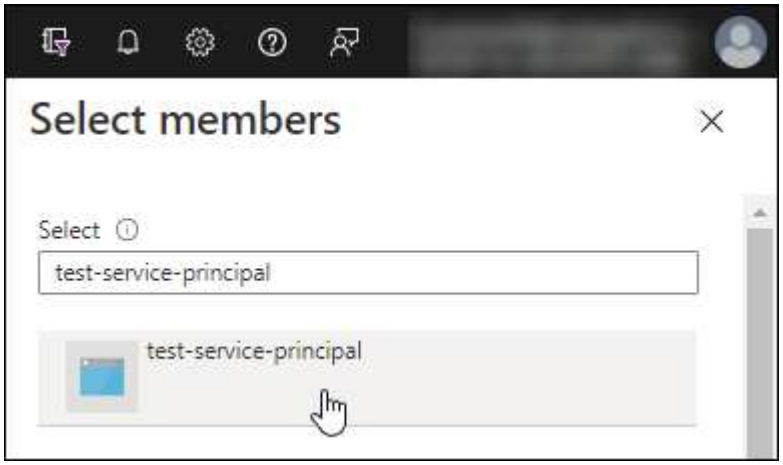
   e. Dans l'onglet **Membres**, procédez comme suit :

      - 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**.

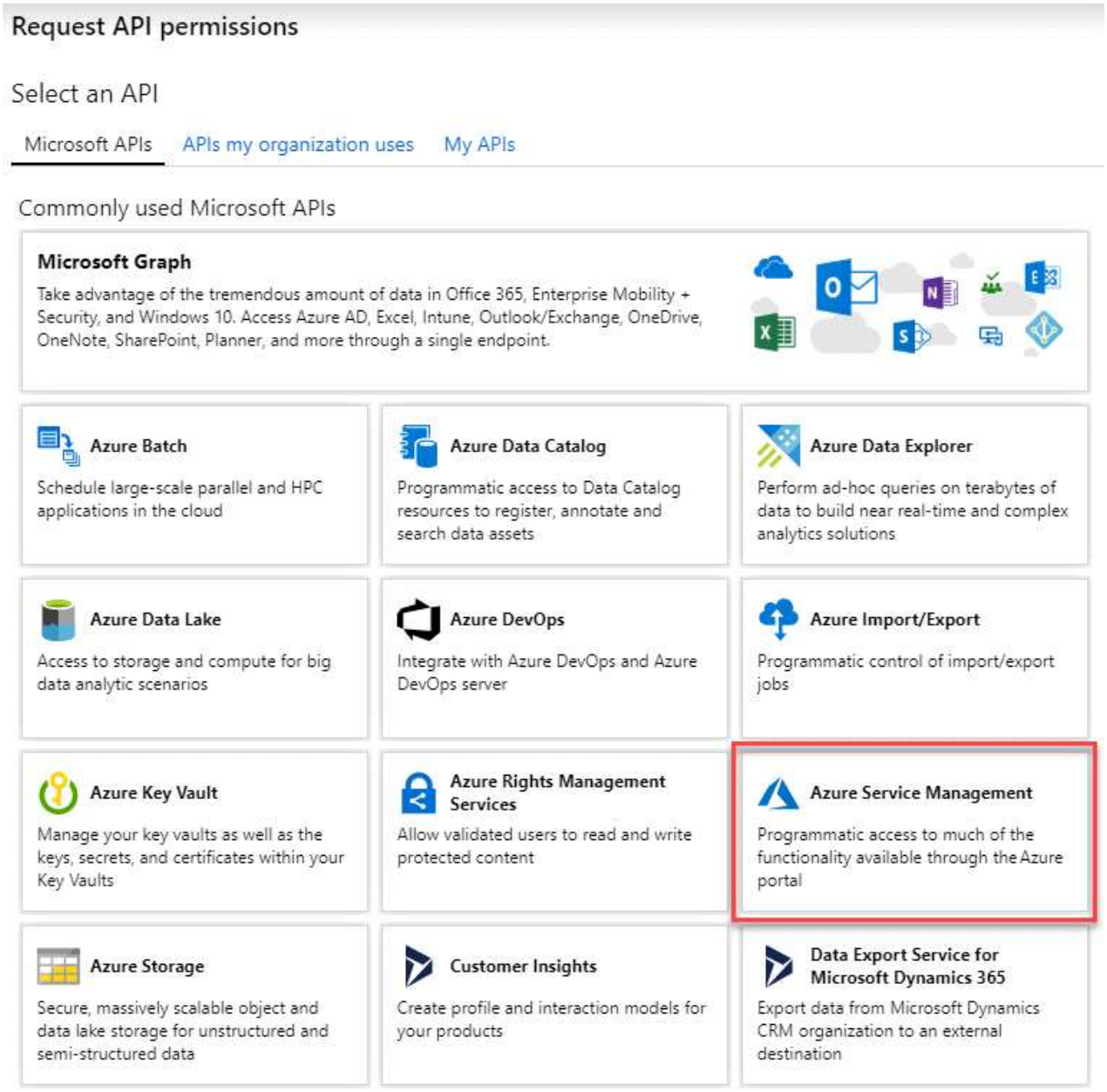
Le principal du service dispose désormais des autorisations Azure requises pour déployer l'agent de la console.

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.

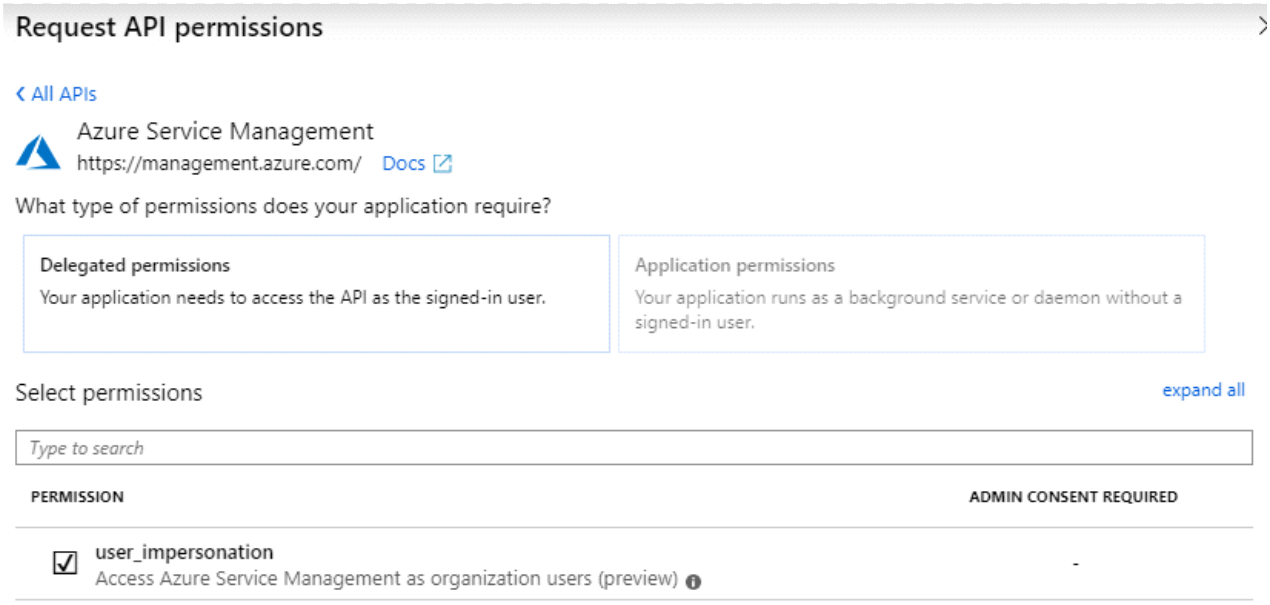
Ajouter des autorisations à l'API Windows Azure Service Management

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**.

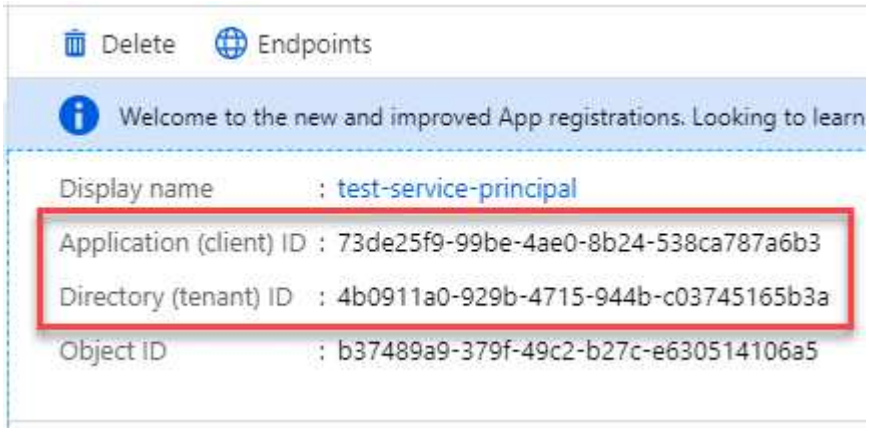


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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

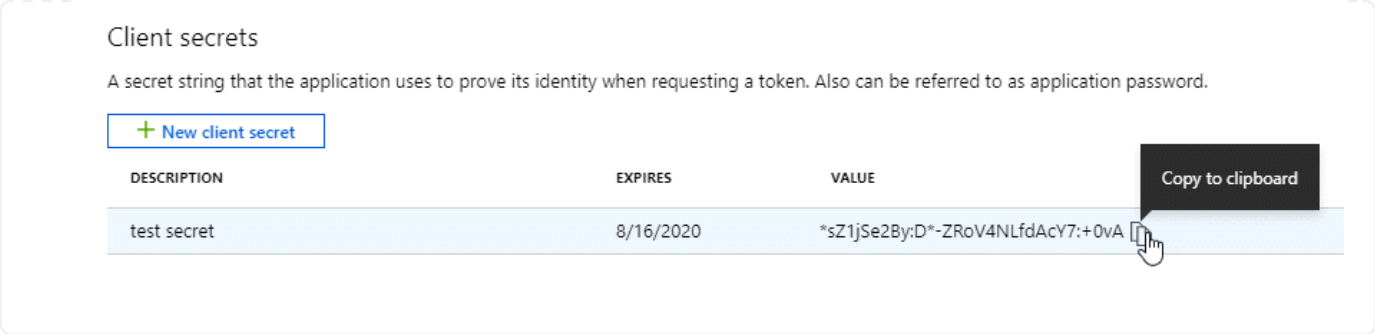
1. Dans le service **Microsoft Entra ID**, sélectionnez **Inscriptions d'applications** et sélectionnez l'application.
2. Copiez l'**ID d'application (client)** et l'**ID de répertoire (locataire)**.



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.



Étape 4 : Créer l'agent de console

Lancez l'agent de console directement depuis la Place de marché Azure.

À propos de cette tâche

La création de l'agent de console à partir de la Place de marché Azure configure une machine virtuelle avec une configuration par défaut. "En savoir plus sur la configuration par défaut de l'agent de console" .

Avant de commencer

Vous devriez avoir les éléments suivants :

- Un abonnement Azure.
- Un réseau virtuel et un sous-réseau dans la région Azure de votre choix.
- Détails sur un serveur proxy, si votre organisation a besoin d'un proxy pour tout le trafic Internet sortant :
  - adresse IP
  - Informations d'identification
  - Certificat HTTPS
- Une clé publique SSH, si vous souhaitez utiliser cette méthode d'authentification pour la machine virtuelle de l'agent de console. L'autre option pour la méthode d'authentification est d'utiliser un mot de passe.

  "En savoir plus sur la connexion à une machine virtuelle Linux dans Azure"

- Si vous ne souhaitez pas que la console crée automatiquement un rôle Azure pour l'agent de la console, vous devrez créer le vôtre."en utilisant la politique sur cette page" .

  Ces autorisations concernent l'instance de l'agent de console elle-même. Il s'agit d'un ensemble d'autorisations différent de celui que vous avez précédemment configuré pour déployer la machine virtuelle de l'agent de console.

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"

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.
- **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**.

  Ce paramètre est important car une identité gérée permet à la machine virtuelle de l'agent de console de s'identifier auprès de Microsoft Entra ID sans fournir 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.

   Azure déploie la machine virtuelle avec les paramètres spécifiés. Vous devriez voir la machine virtuelle et le logiciel de l'agent de console s'exécuter dans environ dix minutes.

   Si l'installation échoue, vous pouvez consulter les journaux et un rapport pour vous aider à résoudre le problème."Découvrez comment résoudre les problèmes d'installation."

5. Ouvrez un navigateur Web à partir d'un hôte disposant d'une connexion à la machine virtuelle de l'agent de console et entrez l'URL suivante :

   https://ipaddress

6. Après vous être connecté, configurez l'agent de 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.

      Gardez le mode restreint désactivé pour utiliser la console en mode standard. Vous devez activer le mode restreint uniquement si vous disposez d'un environnement sécurisé et souhaitez déconnecter ce compte des services backend de la console. Si c'est le cas,"suivez les étapes pour démarrer avec la console en mode restreint" .

   d. Sélectionnez **Commençons**.

Résultat

Vous avez maintenant installé l'agent de console et l'avez configuré avec votre organisation de console.

Si vous disposez d'un stockage Blob Azure dans le même abonnement Azure où vous avez créé l'agent de console, vous verrez un système de stockage Blob Azure apparaître automatiquement sur la page **Systèmes**. "Découvrez comment gérer le stockage Azure Blob depuis la console"

Étape 5 : Accorder des autorisations à l'agent de la console

Maintenant que vous avez créé l'agent de console, vous devez lui fournir les autorisations que vous avez précédemment configurées. L'octroi des autorisations permet à l'agent de la console de gérer vos données et votre infrastructure de stockage dans Azure.

Rôle personnalisé

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.

Quelle est la prochaine étape ?

Aller à la "NetApp Console" pour commencer à utiliser l'agent de console.

Principal de service

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 console dispose désormais des autorisations nécessaires pour effectuer des actions dans Azure en votre nom.

Installer manuellement l'agent de console dans Azure

Pour installer manuellement l'agent de console sur votre propre hôte Linux, vous devez vérifier les exigences de l'hôte, configurer votre réseau, préparer les autorisations Azure, installer l'agent de console, puis fournir les autorisations que vous avez préparées.

Avant de commencer

- Vous devriez avoir un"compréhension des agents de console" .
- Vous devriez revoir"Limitations de l'agent de console" .

Étape 1 : Examiner les exigences de l'hôte

Le logiciel de l'agent de console doit s'exécuter sur un hôte qui répond aux exigences spécifiques du système d'exploitation, de la RAM, des ports, etc.

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.

Taille de la machine virtuelle Azure

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

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 2 : 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 2. 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 3 : Configurer le réseau

Assurez-vous que l'emplacement réseau où vous prévoyez d'installer l'agent de console prend en charge les exigences suivantes. La satisfaction de ces exigences permet à l'agent de console de gérer les ressources et les processus au sein de votre environnement de cloud hybride.

région Azure

Si vous utilisez Cloud Volumes ONTAP, l'agent de console doit être déployé dans la même région Azure que les systèmes Cloud Volumes ONTAP qu'il gère, ou dans la "Paire de régions Azure" pour les systèmes Cloud Volumes ONTAP . Cette exigence garantit qu'une connexion Azure Private Link est utilisée entre Cloud Volumes ONTAP et ses comptes de stockage associés.

"Découvrez comment Cloud Volumes ONTAP utilise un lien privé Azure"

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.

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.
\ 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.

Points de terminaison	But
\ 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.
\ 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"

Étape 4 : Configurer les autorisations de déploiement de l'agent de console

Vous devez fournir des autorisations Azure à l'agent de la console en utilisant l'une des options suivantes :

- Option 1 : attribuez un rôle personnalisé à la machine virtuelle Azure à l'aide d'une identité managée attribuée par le système.
- Option 2 : fournissez à l'agent de la console les informations d'identification d'un principal de service Azure disposant des autorisations requises.

Suivez les étapes pour préparer les autorisations pour l'agent de la console.

Créer un rôle personnalisé pour le déploiement 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.

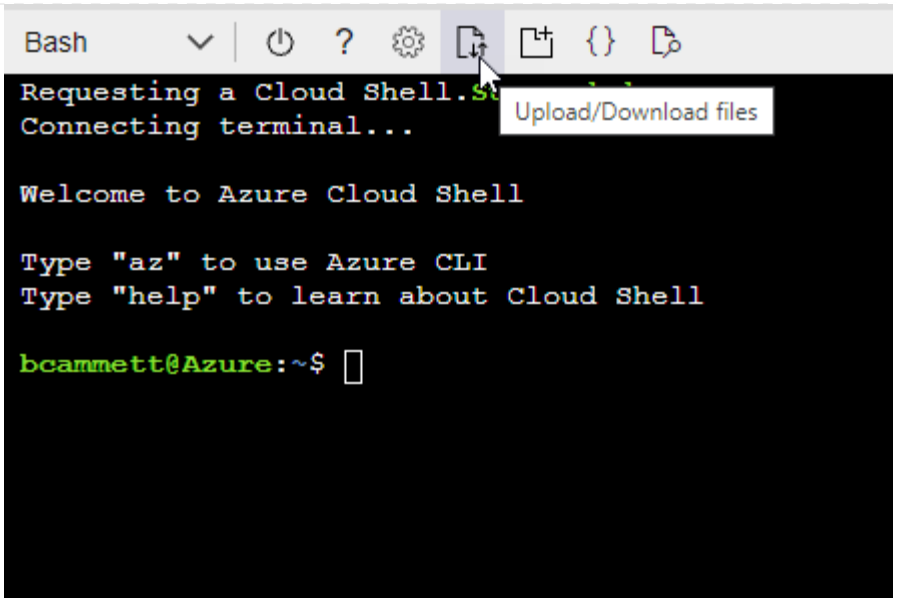
   Exemple

   ```
   "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

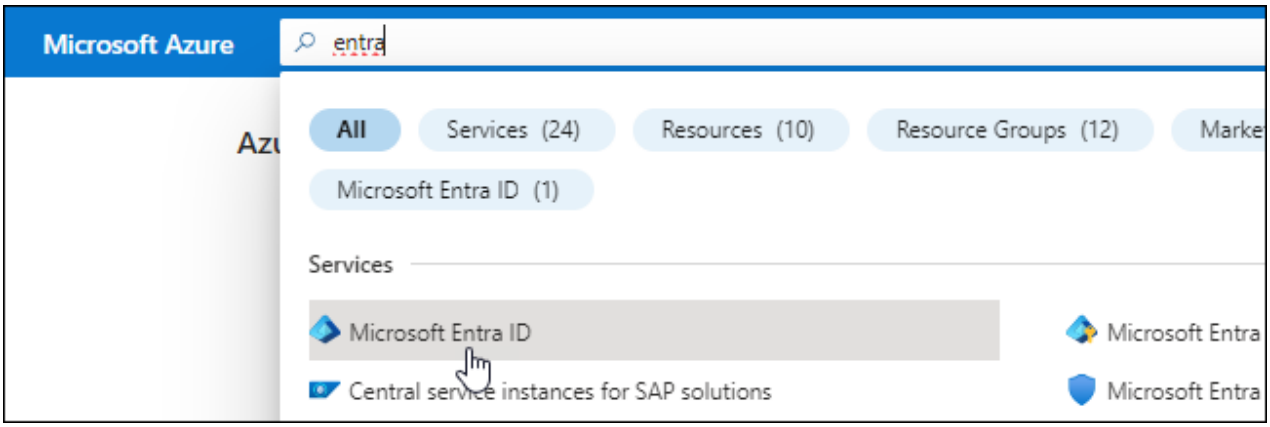
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont l'agent de la console a besoin.

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 .

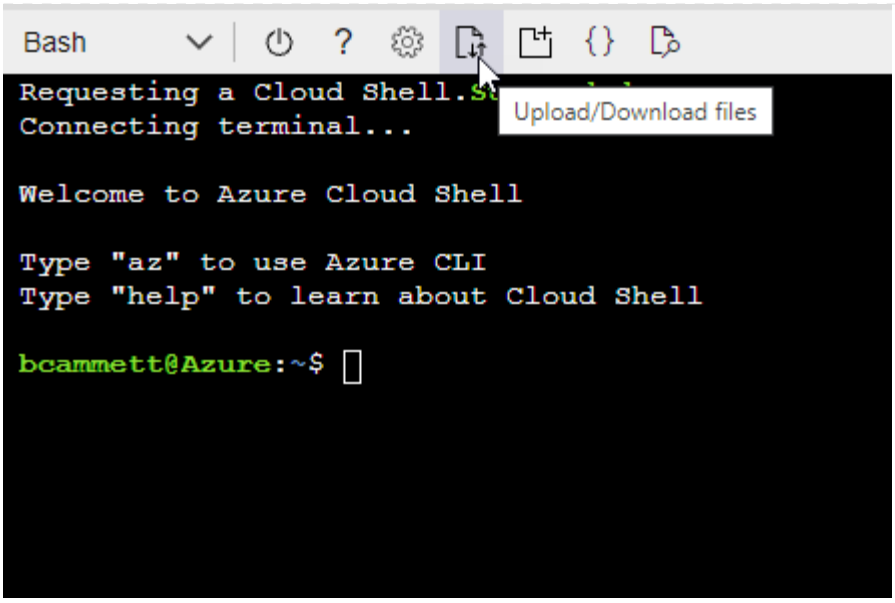
      Exemple

      ```
      "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**.

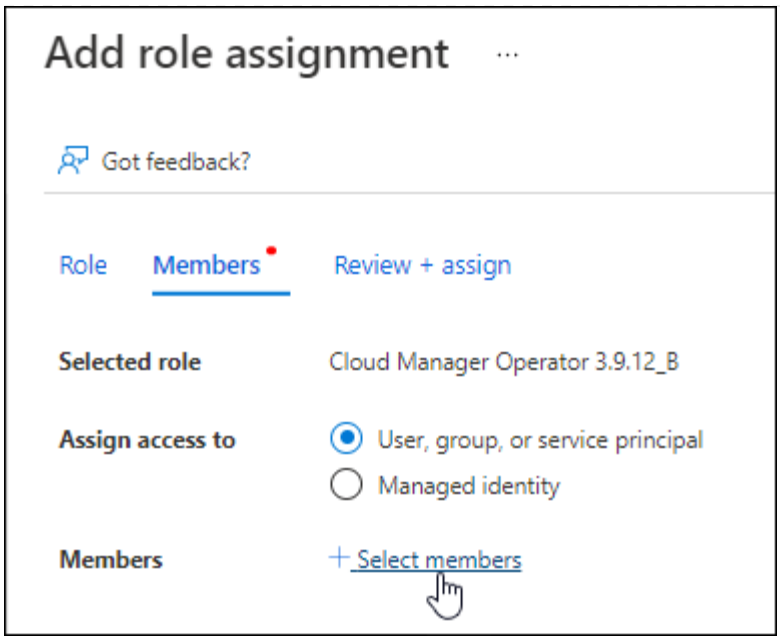
   b. Sélectionnez l'abonnement.

   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**.

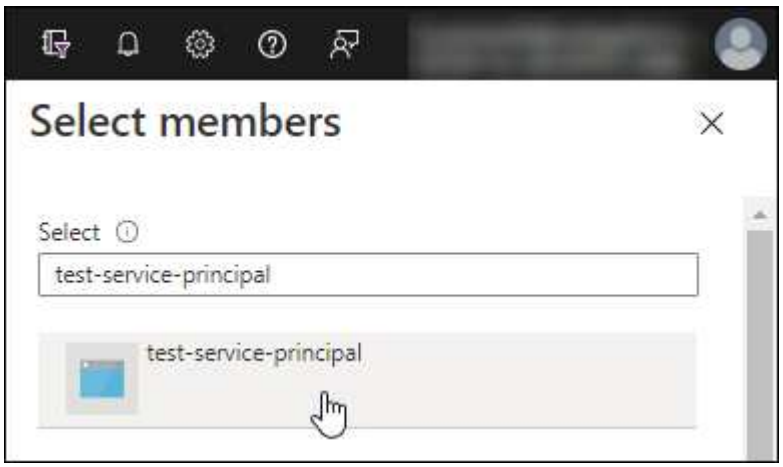
   e. Dans l'onglet **Membres**, procédez comme suit :

      - 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**.

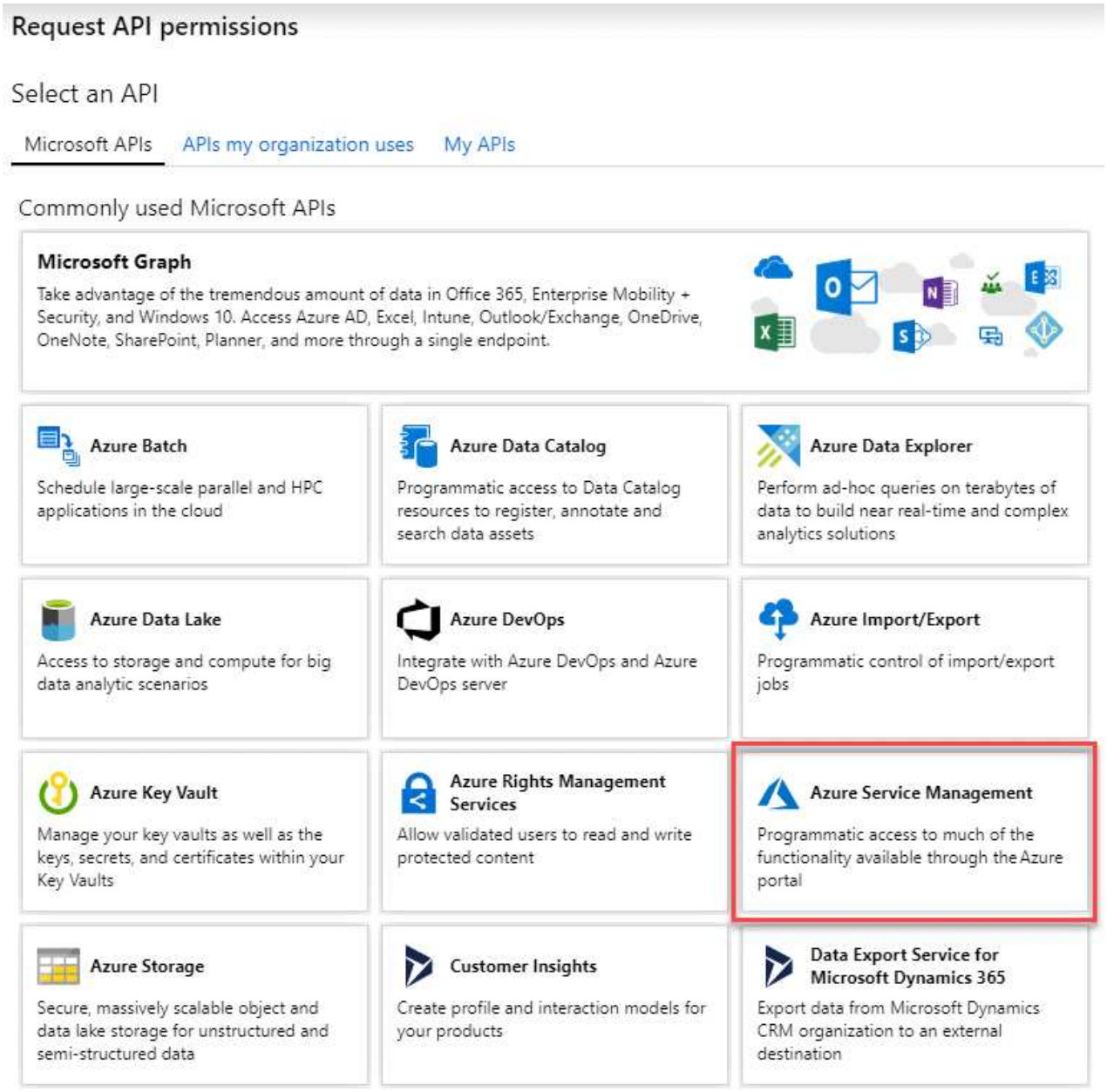
Le principal du service dispose désormais des autorisations Azure requises pour déployer l'agent de la console.

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.

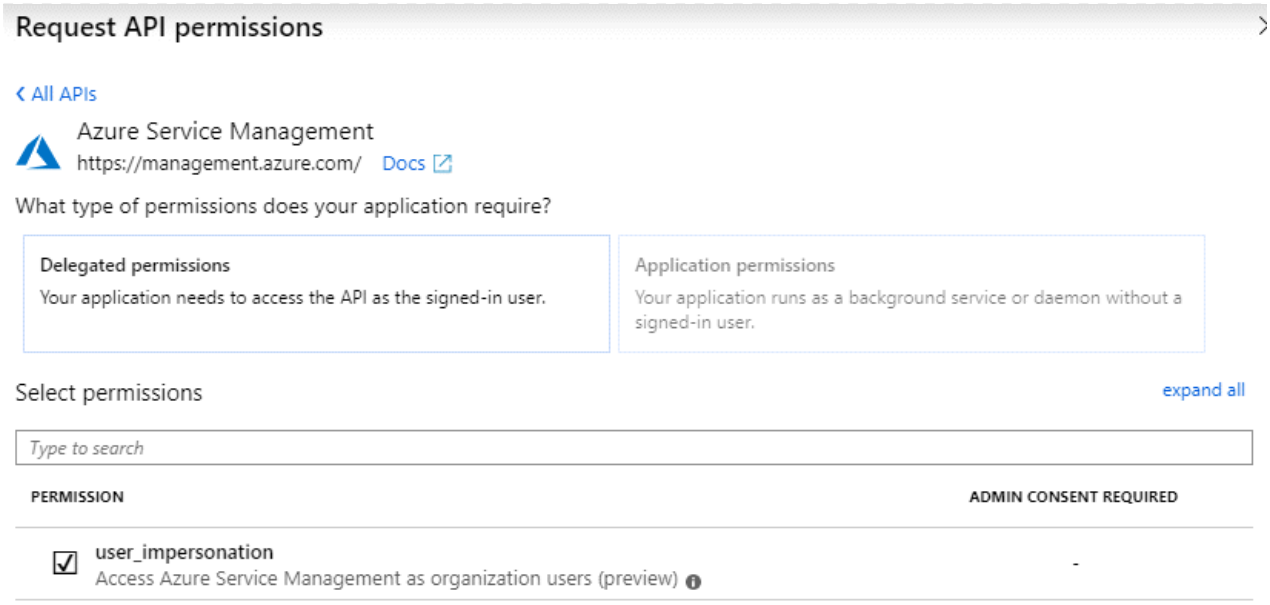
Ajouter des autorisations à l'API Windows Azure Service Management

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**.

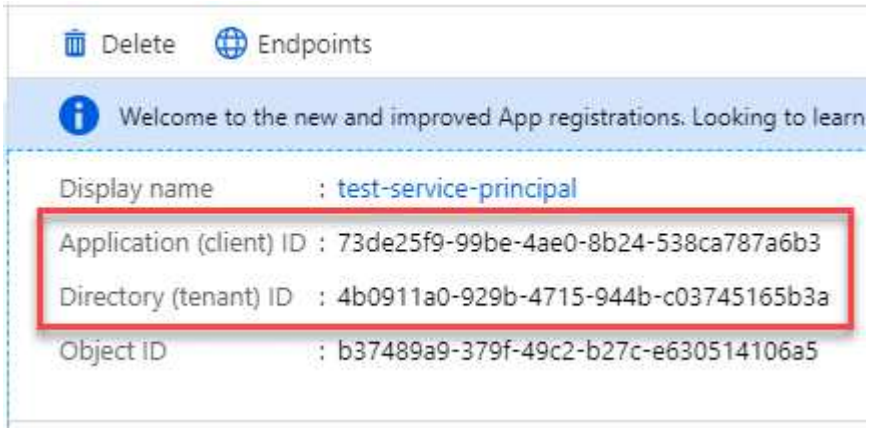


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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.

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.

Étape 5 : Installer l'agent de console

Une fois les prérequis terminés, vous pouvez installer manuellement le logiciel sur votre propre hôte Linux.

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" .

- Une identité gérée activée sur la machine virtuelle dans Azure afin que vous puissiez 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"

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.

2. Attendez que l'installation soit terminée.

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

   Si l'installation échoue, vous pouvez consulter le rapport d'installation et les journaux pour vous aider à résoudre les problèmes."Découvrez comment résoudre les problèmes d'installation."

1. Ouvrez un navigateur Web à partir d'un hôte disposant d'une connexion à la machine virtuelle de l'agent de console et entrez l'URL suivante :

   https://ipaddress

2. Après vous être connecté, configurez l'agent de la console :

a. Spécifiez l’organisation 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.

   Vous devez garder le mode restreint désactivé car ces étapes décrivent comment utiliser la console en mode standard. Vous devez activer le mode restreint uniquement si vous disposez d’un environnement sécurisé et souhaitez déconnecter ce compte des services backend. Si c’est le cas,"suivez les étapes pour démarrer avec la NetApp Console en mode restreint" .

d. Sélectionnez **Commençons**.

Si vous disposez d’un stockage Blob Azure dans le même abonnement Azure où vous avez créé l’agent de console, vous verrez un système de stockage Blob Azure apparaître automatiquement sur la page **Systèmes**. "Découvrez comment gérer le stockage Azure Blob depuis la NetApp Console"

Étape 6 : Accorder des autorisations à la NetApp Console

Maintenant que vous avez installé l’agent de console, vous devez fournir à l’agent de console les autorisations Azure que vous avez précédemment configurées. L’octroi des autorisations permet à la console de gérer vos données et votre infrastructure de stockage dans Azure.

Rôle personnalisé

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.

Quelle est la prochaine étape ?

Aller à la "NetApp Console" pour commencer à utiliser l'agent de console.

Principal de service

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.

Google Cloud

Options d'installation de l'agent de console dans Google Cloud

Il existe plusieurs manières différentes de créer un agent de console dans Google Cloud. Le moyen le plus courant est d'accéder directement à partir de la NetApp Console .

Les options d'installation suivantes sont disponibles :

- "Créez l'agent de console directement depuis la console"(c'est l'option standard)

  Cette action lance une instance de machine virtuelle exécutant Linux et le logiciel agent de console dans un VPC de votre choix.

- "Créer l'agent de console à l'aide de Google Platform"

  Cette action lance également une instance de machine virtuelle exécutant Linux et le logiciel de l'agent de la console, mais le déploiement est lancé directement depuis Google Cloud, plutôt que depuis la console.

- "Téléchargez et installez manuellement le logiciel sur votre propre hôte Linux"

L'option d'installation que vous choisissez a un impact sur la manière dont vous vous préparez à l'installation. Cela inclut la manière dont vous fournissez à la console les autorisations requises dont elle a besoin pour authentifier et gérer les ressources dans Google Cloud.

Créer un agent de console dans Google Cloud à partir de la NetApp Console

Vous pouvez créer un agent de console dans Google Cloud à partir de la console. Vous devez configurer votre réseau, préparer les autorisations Google Cloud, activer les API Google Cloud, puis créer l'agent de la console.

Avant de commencer

- Vous devriez avoir un"compréhension des agents de console" .
- Vous devriez revoir"Limitations de l'agent de console" .

Étape 1 : Configurer le réseau

Configurez la mise en réseau pour garantir que l'agent de la console peut gérer les ressources, avec des connexions aux réseaux cibles et un accès Internet sortant.

VPC et sous-réseau

Lorsque vous créez l'agent de console, vous devez spécifier le VPC et le sous-réseau où il doit résider.

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 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
\ 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.
\ 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.

Points de terminaison contactés depuis la console NetApp

Lorsque vous utilisez la NetApp Console Web fournie via la couche SaaS, elle contacte plusieurs points de terminaison pour effectuer des tâches de gestion des données. Cela inclut les points de terminaison contactés pour déployer l'agent de console à partir de la console.

"Afficher la liste des points de terminaison contactés depuis la console NetApp" .

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"

Implémentez cette exigence de mise en réseau après avoir créé l'agent de console.

Étape 2 : Configurer les autorisations pour créer l'agent de console

Avant de pouvoir déployer un agent de console à partir de la console, vous devez configurer des autorisations pour l'utilisateur Google Platform qui déploie la machine virtuelle de l'agent de console.

Étapes

1. Créer un rôle personnalisé dans Google Platform :

   a. Créez un fichier YAML qui inclut les autorisations suivantes :

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
```

```
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
```

```
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. Depuis Google Cloud, activez Cloud Shell.

c. Téléchargez le fichier YAML qui inclut les autorisations requises.

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

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

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

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

2. Attribuez ce rôle personnalisé à l'utilisateur qui déploiera l'agent de la console à partir de la console ou à l'aide de gcloud.

"Documentation Google Cloud : Attribuer un rôle unique"

Étape 3 : Créez un compte de service Google Cloud à utiliser avec l'agent.

Un compte de service Google Cloud est requis pour fournir à l'agent de la console les autorisations dont la console a besoin pour gérer les ressources dans Google Cloud. Lorsque vous créez l'agent de console, vous devez associer ce compte de service à la machine virtuelle de l'agent de console.

Il est de votre responsabilité de mettre à jour le rôle personnalisé à mesure que de nouvelles autorisations sont

ajoutées dans les versions ultérieures. Si de nouvelles autorisations sont requises, elles seront répertoriées dans les notes de version.

Étapes

1. Créer un rôle personnalisé dans Google Cloud :

   a. Créez un fichier YAML qui inclut le contenu du"autorisations de compte de service pour l'agent de console" .

   b. Depuis Google Cloud, activez Cloud Shell.

   c. Téléchargez le fichier YAML qui inclut les autorisations requises.

   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 connector --project=myproject --file=agent.yaml
      ```

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

2. Créez un compte de service dans Google Cloud et attribuez le rôle au compte de service :

   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"

3. Si vous prévoyez de déployer des systèmes Cloud Volumes ONTAP dans des projets différents de celui dans lequel réside l'agent de console, vous devrez fournir au compte de service de l'agent de console un accès à ces projets.

   Par exemple, disons que l'agent de console se trouve dans le projet 1 et que vous souhaitez créer des systèmes Cloud Volumes ONTAP dans le projet 2. Vous devrez accorder l'accès au compte de service dans le projet 2.

   a. Depuis le service IAM & Admin, sélectionnez le projet Google Cloud dans lequel vous souhaitez créer des systèmes Cloud Volumes ONTAP .

   b. Sur la page **IAM**, sélectionnez **Accorder l'accès** et fournissez les détails requis.

      - Saisissez l'e-mail du compte de service de l'agent de la console.
      - Sélectionnez le rôle personnalisé de l'agent de console.
      - Sélectionnez **Enregistrer**.

   Pour plus de détails, reportez-vous à "Documentation Google Cloud"

Étape 4 : Configurer les autorisations VPC partagées

Si vous utilisez un VPC partagé pour déployer des ressources dans un projet de service, vous devrez préparer vos autorisations.

Ce tableau est fourni à titre de référence et votre environnement doit refléter le tableau des autorisations une fois la configuration IAM terminée.

Afficher les autorisations VPC partagées

Identité	Créateur	Hébergé dans	Autorisations du projet de service	Autorisations du projet hôte	But
Compte Google pour déployer l'agent	Coutume	Projet de service	"Politique de déploiement des agents"	compute.networkUser	Déploiement de l'agent dans le projet de service
compte de service d'agent	Coutume	Projet de service	"Politique de compte de service d'agent"	compute.networkUser deploymentmanager.editor	Déploiement et maintenance de Cloud Volumes ONTAP et des services dans le projet de service
Compte de service Cloud Volumes ONTAP	Coutume	Projet de service	Membre storage.admin : compte de service de la NetApp Console en tant que serviceAccount.user	S/O	(Facultatif) Pour NetApp Cloud Tiering et NetApp Backup and Recovery
Agent de service des API Google	Google Cloud	Projet de service	Éditeur (par défaut)	compute.networkUser	Interagit avec les API Google Cloud au nom du déploiement. Permet à la console d'utiliser le réseau partagé.
Compte de service par défaut de Google Compute Engine	Google Cloud	Projet de service	Éditeur (par défaut)	compute.networkUser	Déploie des instances Google Cloud et une infrastructure de calcul pour le compte du déploiement. Permet à la console d'utiliser le réseau partagé.

Remarques :

1. deploymentmanager.editor n'est requis au niveau du projet hôte que si vous ne transmettez pas de règles de pare-feu au déploiement et que vous choisissez de laisser la console les créer pour vous. La NetApp Console crée un déploiement dans le projet hôte qui contient la règle de pare-feu VPC0 si aucune règle n'est spécifiée.
2. firewall.create et firewall.delete ne sont requis que si vous ne transmettez pas de règles de pare-feu au déploiement et que vous choisissez de laisser la console les créer pour vous. Ces autorisations résident dans le fichier .yaml du compte de console. Si vous déployez une paire HA à l'aide d'un VPC partagé, ces autorisations seront utilisées pour créer les règles de pare-feu pour VPC1, 2 et 3. Pour tous les autres déploiements, ces autorisations seront également utilisées pour créer des règles pour VPC0.
3. Pour la hiérarchisation du cloud, le compte de service de hiérarchisation doit avoir le rôle serviceAccount.user sur le compte de service, pas seulement au niveau du projet. Actuellement, si vous attribuez serviceAccount.user au niveau du projet, les autorisations ne s'affichent pas lorsque vous interrogez le compte de service avec getIAMPolicy.

Étape 5 : Activer les API Google Cloud

Vous devez activer plusieurs API Google Cloud avant de déployer l'agent de console et Cloud Volumes ONTAP.

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)

"Documentation Google Cloud : Activation des API"

Étape 6 : Créer l'agent de console

Créez un agent de console directement depuis la console.

La création de l'agent de console déploie une instance de machine virtuelle dans Google Cloud à l'aide d'une configuration par défaut. Ne passez pas à une instance de machine virtuelle plus petite avec moins de processeurs ou moins de RAM après avoir créé l'agent de console. "En savoir plus sur la configuration par défaut de l'agent de console" .

Lorsque vous déployez un agent dans Google Cloud, celui-ci crée un compartiment pour stocker les fichiers de déploiement.

Avant de commencer

Vous devriez avoir les éléments suivants :

- Les autorisations Google Cloud requises pour créer l'agent de console et un compte de service pour la machine virtuelle de l'agent de console.
- Un VPC et un sous-réseau qui répondent aux exigences de mise en réseau.
- Détails sur un serveur proxy, si un proxy est requis pour l'accès Internet à partir de l'agent de la console.

Étapes

1. Sélectionnez **Administration > Agents**.
2. Sur la page **Aperçu**, sélectionnez **Déployer l'agent > Google Cloud**
3. Sur la page **Déploiement d'un agent**, examinez les détails concernant ce dont vous aurez besoin. Vous avez deux options :
    a. Sélectionnez **Continuer** pour préparer le déploiement à l'aide du guide intégré au produit. Chaque étape du guide intégré au produit inclut les informations contenues sur cette page de la documentation.

b. Sélectionnez **Passer au déploiement** si vous avez déjà préparé en suivant les étapes sur cette page.

4. Suivez les étapes de l'assistant pour créer l'agent de console :
   - Si vous y êtes invité, connectez-vous à votre compte Google, qui devrait disposer des autorisations requises pour créer l'instance de machine virtuelle.

     Le formulaire appartient et est hébergé par Google. Vos informations d'identification ne sont pas fournies à NetApp.

   - **Détails**: Saisissez un nom pour l'instance de machine virtuelle, spécifiez les balises, sélectionnez un projet, puis sélectionnez le compte de service disposant des autorisations requises (reportez-vous à la section ci-dessus pour plus de détails).
   - **Emplacement** : spécifiez une région, une zone, un VPC et un sous-réseau pour l'instance.
   - **Réseau** : Choisissez si vous souhaitez activer une adresse IP publique et spécifiez éventuellement une configuration proxy.
   - **Balises réseau** : ajoutez une balise réseau à l'instance de l'agent de console si vous utilisez un proxy transparent. Les balises réseau doivent commencer par une lettre minuscule et peuvent contenir des lettres minuscules, des chiffres et des traits d'union. Les balises doivent se terminer par une lettre minuscule ou un chiffre. Par exemple, vous pouvez utiliser la balise « console-agent-proxy ».
   - **Politique de pare-feu** : choisissez de créer une nouvelle politique de pare-feu ou de sélectionner une politique de pare-feu existante qui autorise les règles entrantes et sortantes requises.

     "Règles de pare-feu dans Google Cloud"

5. Vérifiez vos sélections pour vérifier que votre configuration est correcte.

   a. La case à cocher **Valider la configuration de l'agent** est cochée par défaut pour que la console valide les exigences de connectivité réseau lors du déploiement. Si la console ne parvient pas à déployer l'agent, elle fournit un rapport pour vous aider à résoudre le problème. Si le déploiement réussit, aucun rapport n'est fourni.

   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, décochez la case pour ignorer la vérification de validation.

6. Sélectionnez **Ajouter**.

   L'agent est prêt dans environ 10 minutes ; restez sur la page jusqu'à ce que le processus soit terminé.

Résultat

Une fois le processus terminé, l'agent de console est disponible pour utilisation.

Si le déploiement échoue, vous pouvez télécharger un rapport et des journaux depuis la console pour vous aider à résoudre les problèmes."Découvrez comment résoudre les problèmes d'installation."

Si vous disposez de buckets Google Cloud Storage dans le même compte Google Cloud où vous avez créé l'agent de la console, vous verrez un système Google Cloud Storage apparaître automatiquement sur la page **Systèmes**. "Découvrez comment gérer Google Cloud Storage depuis la console"

Créer un agent de console à partir de Google Cloud

Pour créer un agent de console dans Google Cloud à l'aide de Google Cloud, vous devez configurer votre réseau, préparer les autorisations Google Cloud, activer les API Google Cloud, puis créer l'agent de console.

Avant de commencer

- Vous devriez avoir un"compréhension des agents de console" .
- Vous devriez revoir"Limitations de l'agent de console" .

Étape 1 : Configurer le réseau

Configurez la mise en réseau pour permettre à l'agent de la console de gérer les ressources et de se connecter aux réseaux cibles et à Internet.

VPC et sous-réseau

Lorsque vous créez l'agent de console, vous devez spécifier le VPC et le sous-réseau où il doit résider.

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 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
\ 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.
\ https://mysupport.netapp.com	Pour obtenir des informations de licence et envoyer des messages AutoSupport au support NetApp .

Points de terminaison	But
\ 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.
\ 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.

Points de terminaison contactés depuis la console NetApp

Lorsque vous utilisez la NetApp Console Web fournie via la couche SaaS, elle contacte plusieurs points de terminaison pour effectuer des tâches de gestion des données. Cela inclut les points de terminaison contactés pour déployer l'agent de console à partir de la console.

"Afficher la liste des points de terminaison contactés depuis la console NetApp" .

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"

Implémentez cette exigence de mise en réseau après avoir créé l'agent de console.

Étape 2 : Configurer les autorisations pour créer l'agent de console

Configurez les autorisations pour que l'utilisateur Google Cloud puisse déployer la machine virtuelle de l'agent de la console à partir de Google Cloud.

Étapes

1. Créer un rôle personnalisé dans Google Platform :

   a. Créez un fichier YAML qui inclut les autorisations suivantes :

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console
agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
```

```
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

b. Depuis Google Cloud, activez Cloud Shell.

c. Téléchargez le fichier YAML qui inclut les autorisations requises.

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

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

rôles gcloud iam créer un connecteurDéploiement --project=myproject --file=connector
-deployment.yaml

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

2. Attribuez ce rôle personnalisé à l'utilisateur qui déploie l'agent de console à partir de Google Cloud.

"Documentation Google Cloud : Attribuer un rôle unique"

Étape 3 : Configurer les autorisations pour les opérations de l'agent de console

Un compte de service Google Cloud est requis pour fournir à l'agent de la console les autorisations dont la console a besoin pour gérer les ressources dans Google Cloud. Lorsque vous créez l'agent de console, vous devez associer ce compte de service à la machine virtuelle de l'agent de console.

Il est de votre responsabilité de mettre à jour le rôle personnalisé à mesure que de nouvelles autorisations sont ajoutées dans les versions ultérieures. Si de nouvelles autorisations sont requises, elles seront répertoriées dans les notes de version.

Étapes

1. Créer un rôle personnalisé dans Google Cloud :

   a. Créez un fichier YAML qui inclut le contenu du"autorisations de compte de service pour l'agent de console" .

   b. Depuis Google Cloud, activez Cloud Shell.

   c. Téléchargez le fichier YAML qui inclut les autorisations requises.

   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 connector --project=myproject --file=agent.yaml
   ```

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

2. Créez un compte de service dans Google Cloud et attribuez le rôle au compte de service :

   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"

3. Si vous prévoyez de déployer des systèmes Cloud Volumes ONTAP dans des projets différents de celui dans lequel réside l'agent de console, vous devrez fournir au compte de service de l'agent de console un accès à ces projets.

   Par exemple, disons que l'agent de console se trouve dans le projet 1 et que vous souhaitez créer des systèmes Cloud Volumes ONTAP dans le projet 2. Vous devrez accorder l'accès au compte de service dans le projet 2.

   a. Depuis le service IAM & Admin, sélectionnez le projet Google Cloud dans lequel vous souhaitez créer

des systèmes Cloud Volumes ONTAP .

b. Sur la page **IAM**, sélectionnez **Accorder l'accès** et fournissez les détails requis.
   - Saisissez l'e-mail du compte de service de l'agent de la console.
   - Sélectionnez le rôle personnalisé de l'agent de console.
   - Sélectionnez **Enregistrer**.

Pour plus de détails, reportez-vous à "Documentation Google Cloud"

Étape 4 : Configurer les autorisations VPC partagées

Si vous utilisez un VPC partagé pour déployer des ressources dans un projet de service, vous devrez préparer vos autorisations.

Ce tableau est fourni à titre de référence et votre environnement doit refléter le tableau des autorisations une fois la configuration IAM terminée.

Afficher les autorisations VPC partagées

Identité	Créateur	Hébergé dans	Autorisations du projet de service	Autorisations du projet hôte	But
Compte Google pour déployer l'agent	Coutume	Projet de service	"Politique de déploiement des agents"	compute.networkUser	Déploiement de l'agent dans le projet de service
compte de service d'agent	Coutume	Projet de service	"Politique de compte de service d'agent"	compute.networkUser deploymentmanager.editor	Déploiement et maintenance de Cloud Volumes ONTAP et des services dans le projet de service
Compte de service Cloud Volumes ONTAP	Coutume	Projet de service	Membre storage.admin : compte de service de la NetApp Console en tant que serviceAccount.user	S/O	(Facultatif) Pour NetApp Cloud Tiering et NetApp Backup and Recovery
Agent de service des API Google	Google Cloud	Projet de service	Éditeur (par défaut)	compute.networkUser	Interagit avec les API Google Cloud au nom du déploiement. Permet à la console d'utiliser le réseau partagé.
Compte de service par défaut de Google Compute Engine	Google Cloud	Projet de service	Éditeur (par défaut)	compute.networkUser	Déploie des instances Google Cloud et une infrastructure de calcul pour le compte du déploiement. Permet à la console d'utiliser le réseau partagé.

Remarques :

1. deploymentmanager.editor n'est requis au niveau du projet hôte que si vous ne transmettez pas de règles de pare-feu au déploiement et que vous choisissez de laisser la console les créer pour vous. La NetApp Console crée un déploiement dans le projet hôte qui contient la règle de pare-feu VPC0 si aucune règle n'est spécifiée.
2. firewall.create et firewall.delete ne sont requis que si vous ne transmettez pas de règles de pare-feu au déploiement et que vous choisissez de laisser la console les créer pour vous. Ces autorisations résident dans le fichier .yaml du compte de console. Si vous déployez une paire HA à l'aide d'un VPC partagé, ces autorisations seront utilisées pour créer les règles de pare-feu pour VPC1, 2 et 3. Pour tous les autres déploiements, ces autorisations seront également utilisées pour créer des règles pour VPC0.
3. Pour la hiérarchisation du cloud, le compte de service de hiérarchisation doit avoir le rôle serviceAccount.user sur le compte de service, pas seulement au niveau du projet. Actuellement, si vous attribuez serviceAccount.user au niveau du projet, les autorisations ne s'affichent pas lorsque vous interrogez le compte de service avec getIAMPolicy.

Étape 5 : Activer les API Google Cloud

Activez plusieurs API Google Cloud avant de déployer l'agent de console et Cloud Volumes ONTAP.

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)

"Documentation Google Cloud : Activation des API"

Étape 6 : Créer l'agent de console

Créez un agent de console à l'aide de Google Cloud.

La création de l'agent de console déploie une instance de machine virtuelle dans Google Cloud avec la configuration par défaut. Ne passez pas à une instance de machine virtuelle plus petite avec moins de processeurs ou moins de RAM après avoir créé l'agent de console. "En savoir plus sur la configuration par défaut de l'agent de console" .

Avant de commencer

Vous devriez avoir les éléments suivants :

- Les autorisations Google Cloud requises pour créer l'agent de console et un compte de service pour la machine virtuelle de l'agent de console.
- Un VPC et un sous-réseau qui répondent aux exigences de mise en réseau.
- Une compréhension des exigences des instances de VM.
    - **CPU** : 8 cœurs ou 8 vCPU
    - **RAM** : 32 Go
    - **Type de machine** : Nous recommandons 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 les fonctionnalités de machine virtuelle protégée.

Étapes

1. Connectez-vous au SDK Google Cloud en utilisant votre méthode préférée.

   Cet exemple utilise un shell local avec le SDK gcloud installé, mais vous pouvez également utiliser Google Cloud Shell.

Pour plus d'informations sur le SDK Google Cloud, visitez le"Page de documentation du SDK Google Cloud" .

2. Vérifiez que vous êtes connecté en tant qu'utilisateur disposant des autorisations requises définies dans la section ci-dessus :

```
gcloud auth list
```

La sortie doit afficher ce qui suit, où le compte utilisateur * est le compte utilisateur sous lequel vous souhaitez vous connecter :

```
Credentialed Accounts
ACTIVE  ACCOUNT
     some_user_account@domain.com
*    desired_user_account@domain.com
To set the active account, run:
 $ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install them,
please run:
$ gcloud components update
```

3. Exécutez le `gcloud compute instances create` commande:

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-8
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

nom d'instance
: Le nom d'instance souhaité pour l'instance de machine virtuelle.

projet
: (Facultatif) Le projet dans lequel vous souhaitez déployer la machine virtuelle.

compte de service
Le compte de service spécifié dans la sortie de l'étape 2.

zone
La zone où vous souhaitez déployer la VM

sans adresse
(Facultatif) Aucune adresse IP externe n'est utilisée (vous avez besoin d'un NAT cloud ou d'un proxy pour acheminer le trafic vers l'Internet public)

balise réseau
(Facultatif) Ajoutez un balisage réseau pour lier une règle de pare-feu utilisant des balises à l'instance de l'agent de console

chemin réseau
(Facultatif) Ajoutez le nom du réseau dans lequel déployer l'agent de console (pour un VPC partagé, vous avez besoin du chemin complet)

chemin de sous-réseau
(Facultatif) Ajoutez le nom du sous-réseau dans lequel déployer l'agent de console (pour un VPC partagé, vous avez besoin du chemin complet)

kms-key-path
(Facultatif) Ajoutez une clé KMS pour crypter les disques de l'agent de console (les autorisations IAM doivent également être appliquées)

Pour plus d'informations sur ces drapeaux, visitez le"Documentation du SDK de calcul Google Cloud" .

L'exécution de la commande déploie l'agent de la console. L'instance de l'agent de console et le logiciel devraient être exécutés dans environ cinq minutes.

4. 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.

5. Après vous être connecté, configurez l'agent de la console :
   a. Spécifiez l'organisation de la console à associer à l'agent de la console.

      "En savoir plus sur la gestion des identités et des accès" .

   b. Entrez un nom pour le système.

Résultat

L'agent de console est maintenant installé et configuré avec votre organisation de console.

Ouvrez un navigateur Web et accédez à la "NetApp Console" pour commencer à utiliser l'agent de console.

Installer manuellement l’agent de console dans Google Cloud

Pour installer manuellement l’agent de console sur votre propre hôte Linux, vous devez vérifier les exigences de l’hôte, configurer votre réseau, préparer les autorisations Google Cloud, activer les API Google Cloud, installer la console, puis fournir les autorisations que vous avez préparées.

Avant de commencer

- Vous devriez avoir un"compréhension des agents de console" .
- Vous devriez revoir"Limitations de l’agent de console" .

Étape 1 : Examiner les exigences de l’hôte

Le logiciel de l’agent de console doit s’exécuter sur un hôte qui répond aux exigences spécifiques du système d’exploitation, de la RAM, des ports, etc.

> 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.

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 .
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 .

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		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
Docker Engine 23.06 à 28.0.0.	Non pris en charge		22,04 LTS	3.9.50 ou version ultérieure

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"

Étape 2 : 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 3. 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 3 : Configurer le réseau

Configurez votre réseau afin que l'agent de la console puisse gérer les ressources et les processus au sein de votre environnement cloud hybride. Par exemple, vous devez vous assurer que les connexions sont disponibles pour les réseaux cibles et que l'accès Internet sortant est disponible.

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.

Points de terminaison	But
\ 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.
\ 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.

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"

Étape 4 : Configurer les autorisations pour l'agent de la console

Un compte de service Google Cloud est requis pour fournir à l'agent de la console les autorisations dont la console a besoin pour gérer les ressources dans Google Cloud. Lorsque vous créez l'agent de console, vous devez associer ce compte de service à la machine virtuelle de l'agent de console.

Il est de votre responsabilité de mettre à jour le rôle personnalisé à mesure que de nouvelles autorisations sont ajoutées dans les versions ultérieures. Si de nouvelles autorisations sont requises, elles seront répertoriées dans les notes de version.

Étapes

1. Créer un rôle personnalisé dans Google Cloud :

   a. Créez un fichier YAML qui inclut le contenu du"autorisations de compte de service pour l'agent de console" .

   b. Depuis Google Cloud, activez Cloud Shell.

   c. Téléchargez le fichier YAML qui inclut les autorisations requises.

   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 connector --project=myproject --file=agent.yaml
      ```

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

2. Créez un compte de service dans Google Cloud et attribuez le rôle au compte de service :

   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"

3. Si vous prévoyez de déployer des systèmes Cloud Volumes ONTAP dans des projets différents de celui dans lequel réside l'agent de console, vous devrez fournir au compte de service de l'agent de console un accès à ces projets.

   Par exemple, disons que l'agent de console se trouve dans le projet 1 et que vous souhaitez créer des systèmes Cloud Volumes ONTAP dans le projet 2. Vous devrez accorder l'accès au compte de service dans le projet 2.

   a. Depuis le service IAM & Admin, sélectionnez le projet Google Cloud dans lequel vous souhaitez créer des systèmes Cloud Volumes ONTAP .
   b. Sur la page **IAM**, sélectionnez **Accorder l'accès** et fournissez les détails requis.
      - Saisissez l'e-mail du compte de service de l'agent de la console.
      - Sélectionnez le rôle personnalisé de l'agent de console.
      - Sélectionnez **Enregistrer**.

   Pour plus de détails, reportez-vous à "Documentation Google Cloud"

Étape 5 : Configurer les autorisations VPC partagées

Si vous utilisez un VPC partagé pour déployer des ressources dans un projet de service, vous devrez préparer vos autorisations.

Ce tableau est fourni à titre de référence et votre environnement doit refléter le tableau des autorisations une fois la configuration IAM terminée.

Afficher les autorisations VPC partagées

Identité	Créateur	Hébergé dans	Autorisations du projet de service	Autorisations du projet hôte	But
Compte Google pour déployer l'agent	Coutume	Projet de service	"Politique de déploiement des agents"	compute.networkUser	Déploiement de l'agent dans le projet de service
compte de service d'agent	Coutume	Projet de service	"Politique de compte de service d'agent"	compute.networkUser deploymentmanager.editor	Déploiement et maintenance de Cloud Volumes ONTAP et des services dans le projet de service
Compte de service Cloud Volumes ONTAP	Coutume	Projet de service	Membre storage.admin : compte de service de la NetApp Console en tant que serviceAccount.user	S/O	(Facultatif) Pour NetApp Cloud Tiering et NetApp Backup and Recovery
Agent de service des API Google	Google Cloud	Projet de service	Éditeur (par défaut)	compute.networkUser	Interagit avec les API Google Cloud au nom du déploiement. Permet à la console d'utiliser le réseau partagé.
Compte de service par défaut de Google Compute Engine	Google Cloud	Projet de service	Éditeur (par défaut)	compute.networkUser	Déploie des instances Google Cloud et une infrastructure de calcul pour le compte du déploiement. Permet à la console d'utiliser le réseau partagé.

Remarques :

1. deploymentmanager.editor n'est requis au niveau du projet hôte que si vous ne transmettez pas de règles de pare-feu au déploiement et que vous choisissez de laisser la console les créer pour vous. La NetApp Console crée un déploiement dans le projet hôte qui contient la règle de pare-feu VPC0 si aucune règle n'est spécifiée.
2. firewall.create et firewall.delete ne sont requis que si vous ne transmettez pas de règles de pare-feu au déploiement et que vous choisissez de laisser la console les créer pour vous. Ces autorisations résident dans le fichier .yaml du compte de console. Si vous déployez une paire HA à l'aide d'un VPC partagé, ces autorisations seront utilisées pour créer les règles de pare-feu pour VPC1, 2 et 3. Pour tous les autres déploiements, ces autorisations seront également utilisées pour créer des règles pour VPC0.
3. Pour la hiérarchisation du cloud, le compte de service de hiérarchisation doit avoir le rôle serviceAccount.user sur le compte de service, pas seulement au niveau du projet. Actuellement, si vous attribuez serviceAccount.user au niveau du projet, les autorisations ne s'affichent pas lorsque vous interrogez le compte de service avec getIAMPolicy.

Étape 6 : Activer les API Google Cloud

Plusieurs API Google Cloud doivent être activées avant de pouvoir déployer un agent Console 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)

"Documentation Google Cloud : Activation des API"

Étape 7 : Installer l'agent de console

Une fois les prérequis terminés, vous pouvez installer manuellement le logiciel sur votre propre hôte Linux.

Lors du déploiement d'un agent, le système crée également un bucket Google Cloud pour stocker les fichiers de déploiement.

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.
2. Attendez que l'installation soit terminée.

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

   Si l'installation échoue, vous pouvez consulter le rapport d'installation et les journaux pour vous aider à résoudre les problèmes."Découvrez comment résoudre les problèmes d'installation."

1. Ouvrez un navigateur Web à partir d'un hôte disposant d'une connexion à la machine virtuelle de l'agent de console et entrez l'URL suivante :

https://ipaddress

2. Après vous être connecté, configurez l'agent de la console :

   a. Spécifiez l'organisation 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.

      Vous devez garder le mode restreint désactivé car ces étapes décrivent comment utiliser la console en mode standard. Vous devez activer le mode restreint uniquement si vous disposez d'un environnement sécurisé et souhaitez déconnecter ce compte des services backend. Si c'est le cas,"suivez les étapes pour démarrer avec la NetApp Console en mode restreint" .

   d. Sélectionnez **Commençons**.

   Si l'installation échoue, vous pouvez consulter les journaux et un rapport pour vous aider à résoudre le problème."Découvrez comment résoudre les problèmes d'installation."

Si vous disposez de buckets Google Cloud Storage dans le même compte Google Cloud où vous avez créé l'agent de la console, vous verrez un système Google Cloud Storage apparaître automatiquement sur la page **Systèmes**. "Découvrez comment gérer Google Cloud Storage depuis la NetApp Console"

Étape 8 : Accorder des autorisations à l'agent de console

Vous devez fournir à l'agent de la console les autorisations Google Cloud que vous avez précédemment configurées. L'octroi des autorisations permet à l'agent de la console de gérer vos données et votre infrastructure de stockage dans Google Cloud.

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 des ressources dans d'autres projets Google Cloud, 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.

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 .
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 .

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		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
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

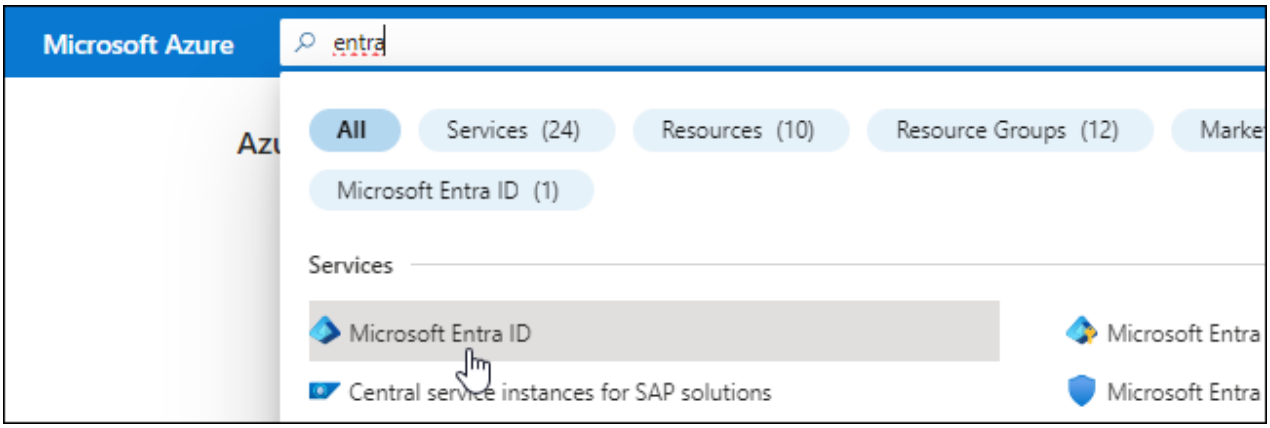
Lorsque l'agent de console est installé sur site, vous devez fournir à l'agent de console des autorisations Azure en configurant un principal de service dans Microsoft Entra ID et en obtenant les informations d'identification Azure dont l'agent de console a besoin.

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 .

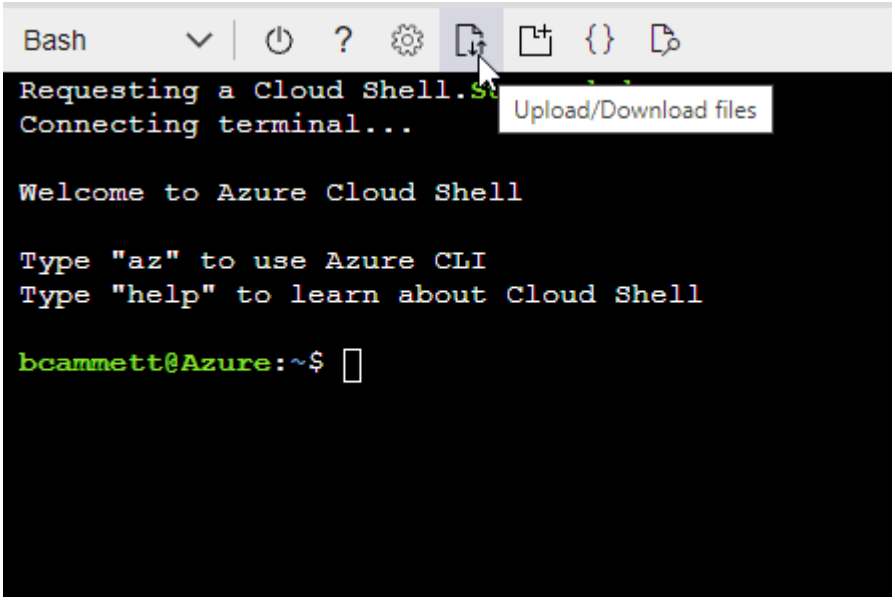
      Exemple

```
"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 :

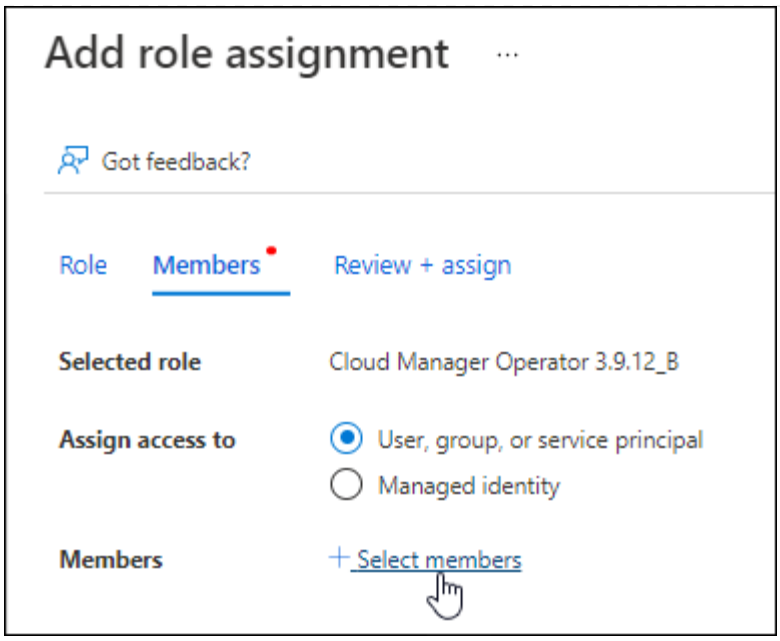
```
az role definition create --role-definition agent_Policy.json
```

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 :

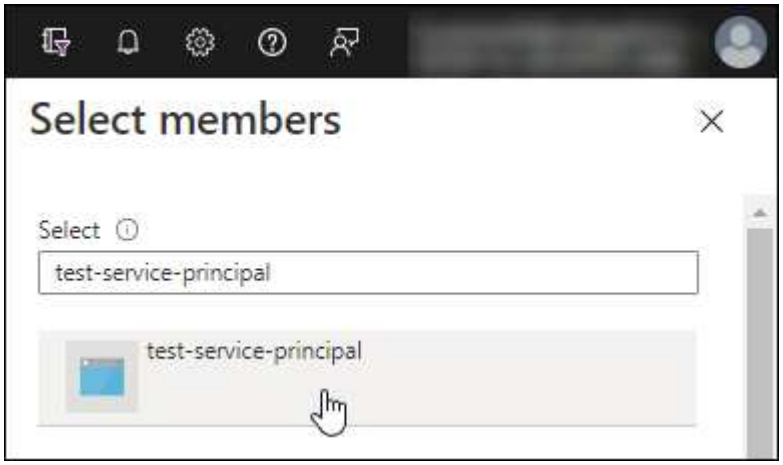
a. Depuis le portail Azure, ouvrez le service **Abonnements**.
b. Sélectionnez l'abonnement.
c. Sélectionnez **Contrôle d'accès (IAM) > Ajouter > Ajouter une attribution de rôle**.
d. Dans l'onglet **Rôle**, sélectionnez le rôle **Opérateur de console** et sélectionnez **Suivant**.
e. Dans l'onglet **Membres**,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

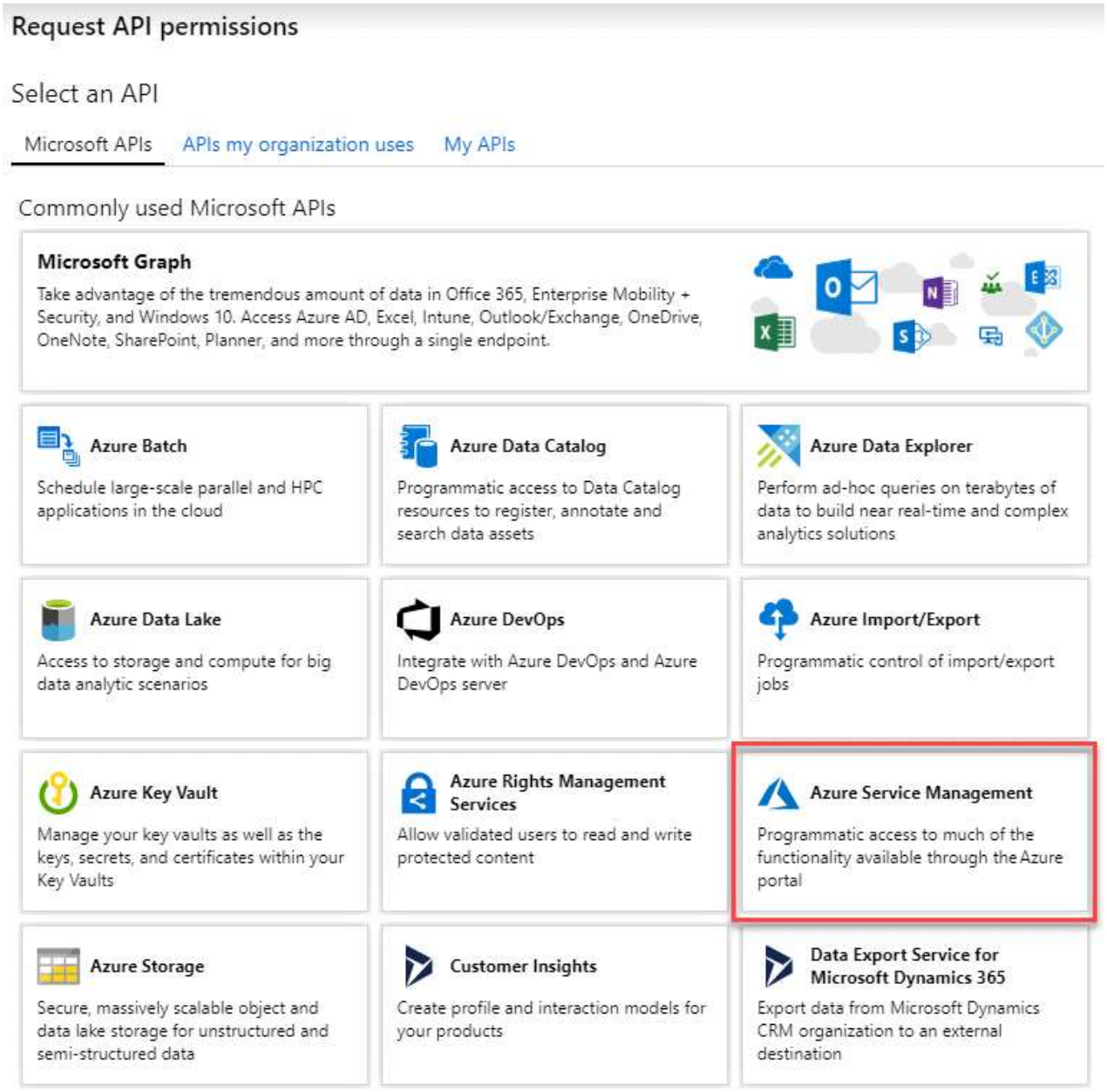
Le principal du service dispose désormais des autorisations Azure requises pour déployer l'agent de la console.

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.

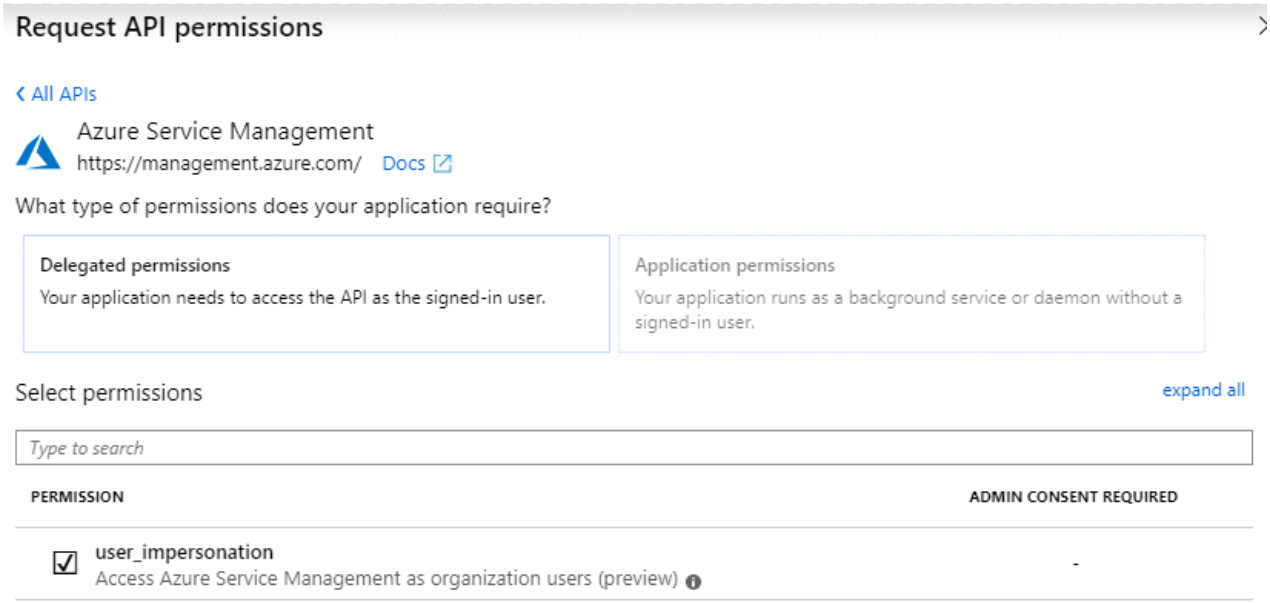
Ajouter des autorisations à l'API Windows Azure Service Management

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**.

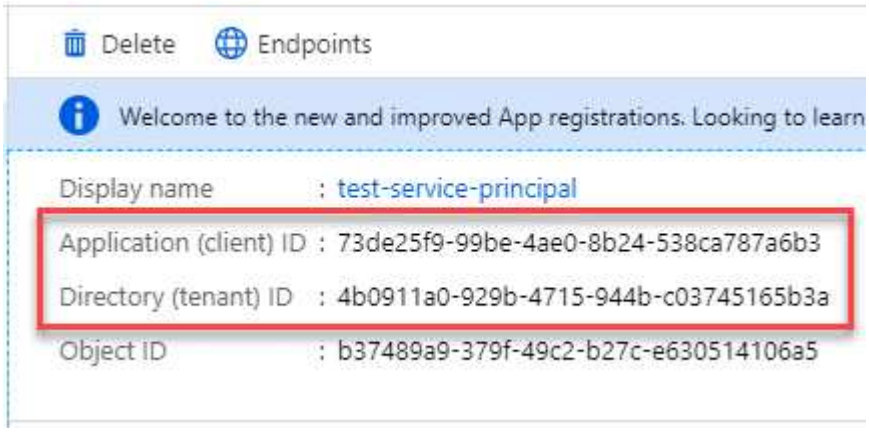


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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

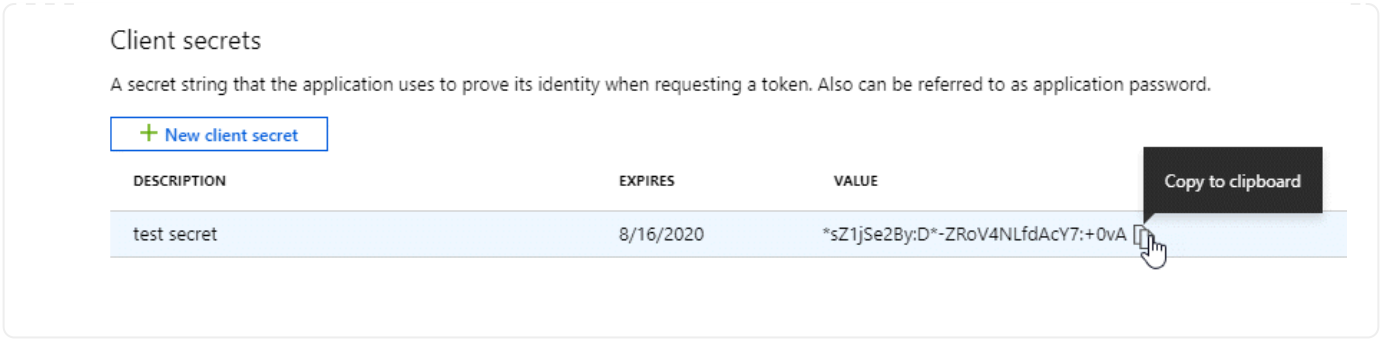
1. Dans le service **Microsoft Entra ID**, sélectionnez **Inscriptions d'applications** et sélectionnez l'application.
2. Copiez l'**ID d'application (client)** et l'**ID de répertoire (locataire)**.



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 4. 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

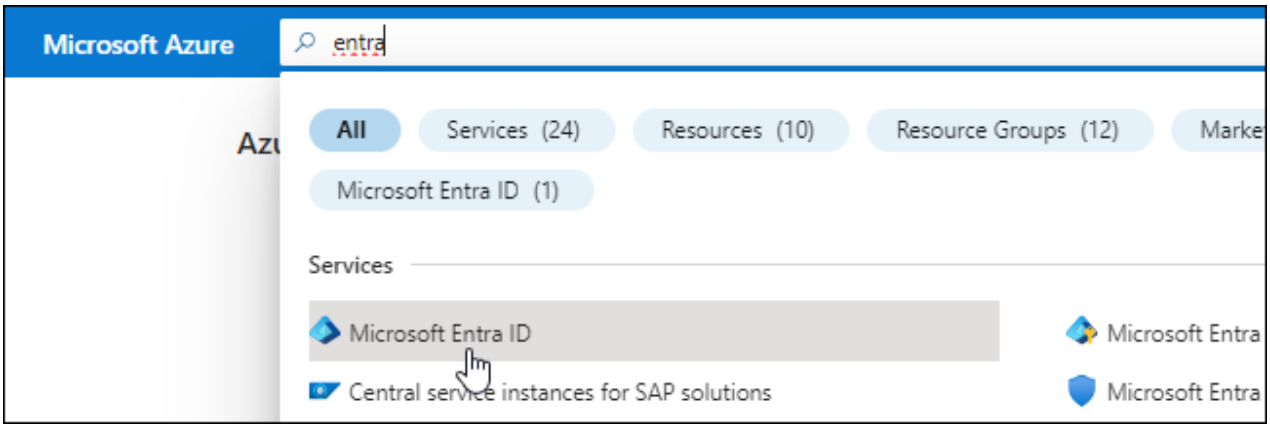
Lorsque l'agent de console est installé sur site, vous devez lui accorder des autorisations Azure en configurant un principal de service dans Microsoft Entra ID et en obtenant les informations d'identification Azure dont l'agent de console a besoin.

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 .

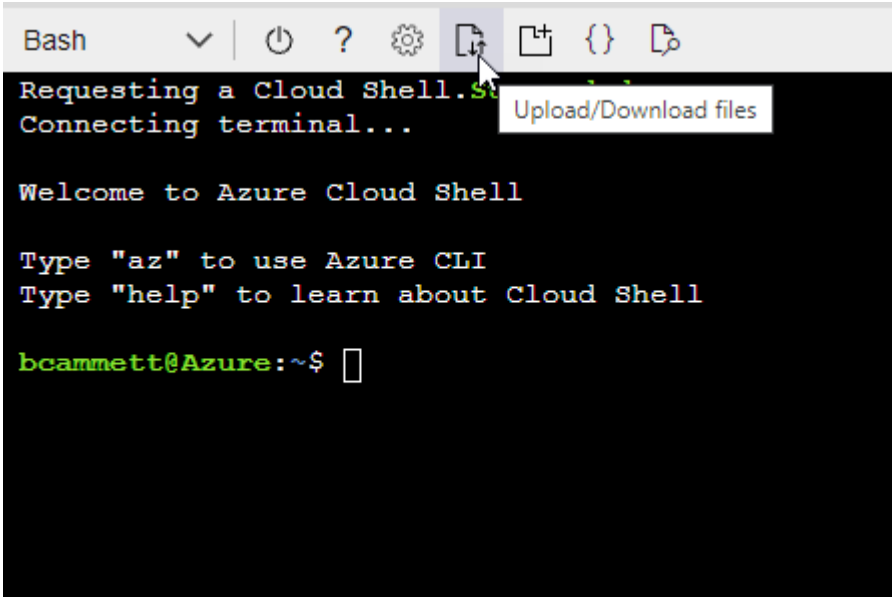
      Exemple

```
"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 :

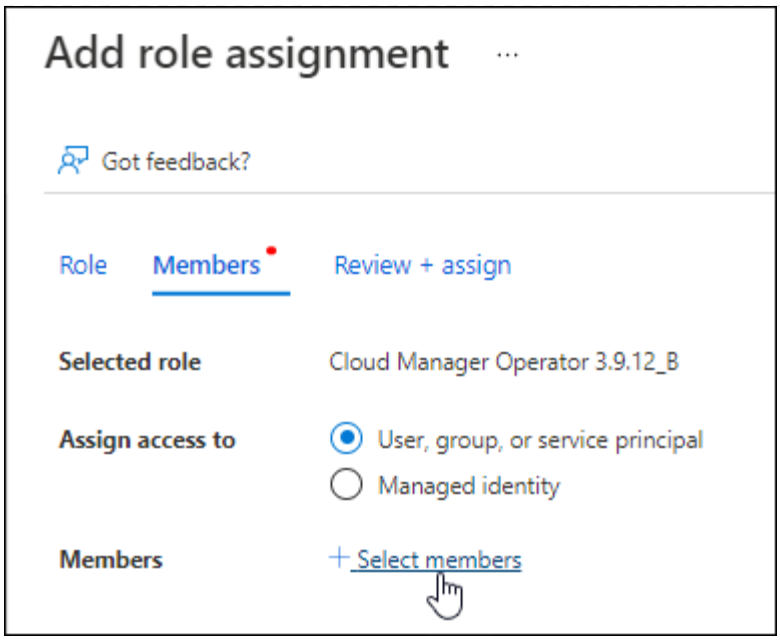
```
az role definition create --role-definition agent_Policy.json
```

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 :

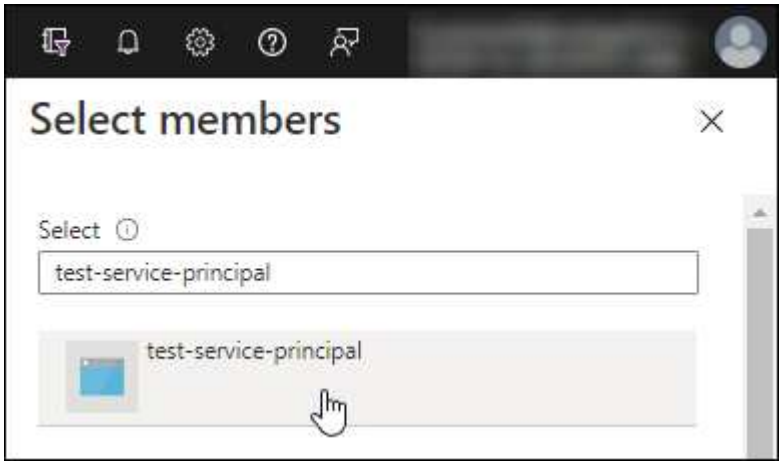
a. Depuis le portail Azure, ouvrez le service **Abonnements**.
b. Sélectionnez l'abonnement.
c. Sélectionnez **Contrôle d'accès (IAM) > Ajouter > Ajouter une attribution de rôle**.
d. Dans l'onglet **Rôle**, sélectionnez le rôle **Opérateur de console** et sélectionnez **Suivant**.
e. Dans l'onglet **Membres**,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

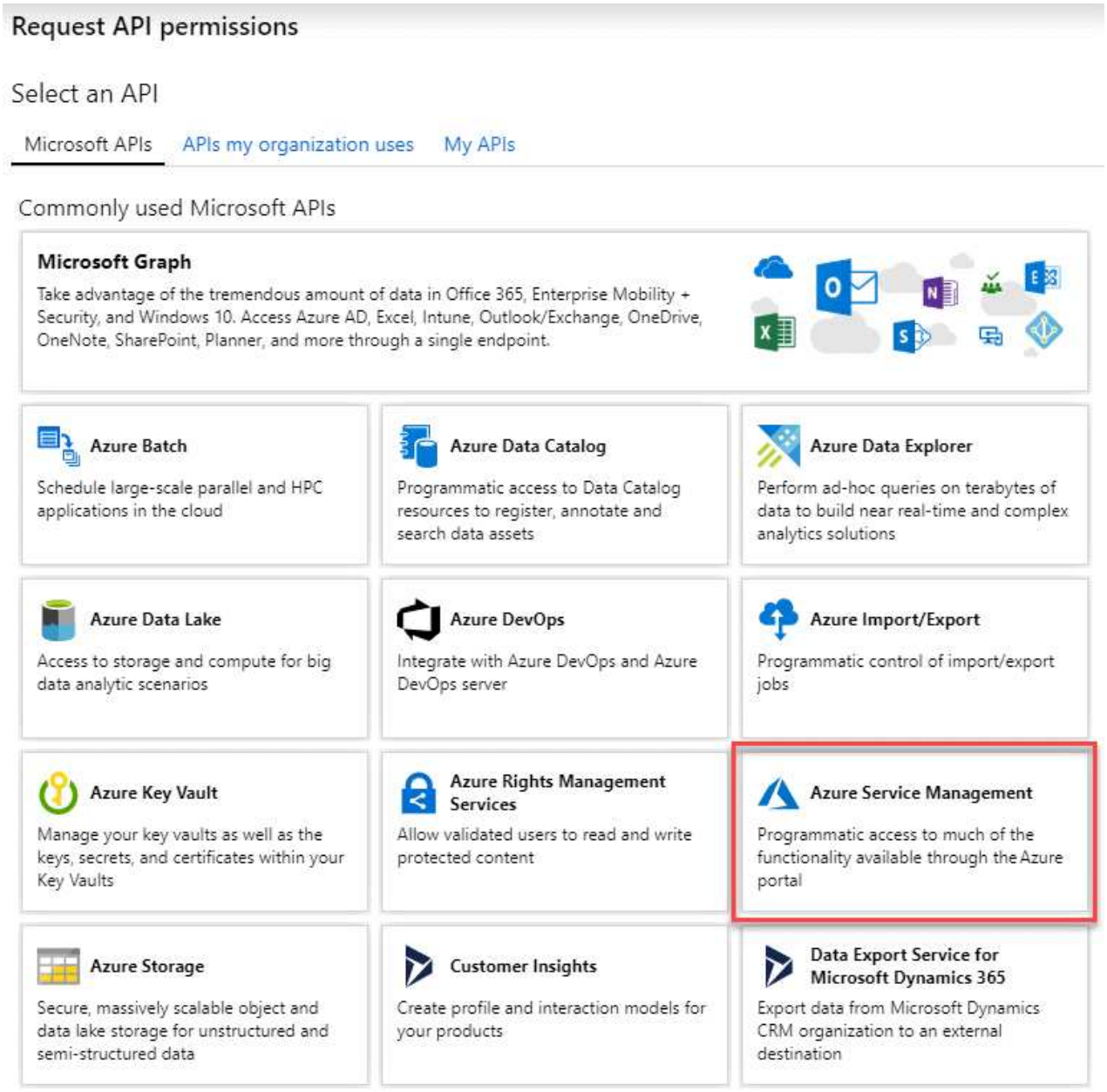
Le principal du service dispose désormais des autorisations Azure requises pour déployer l'agent de la console.

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.

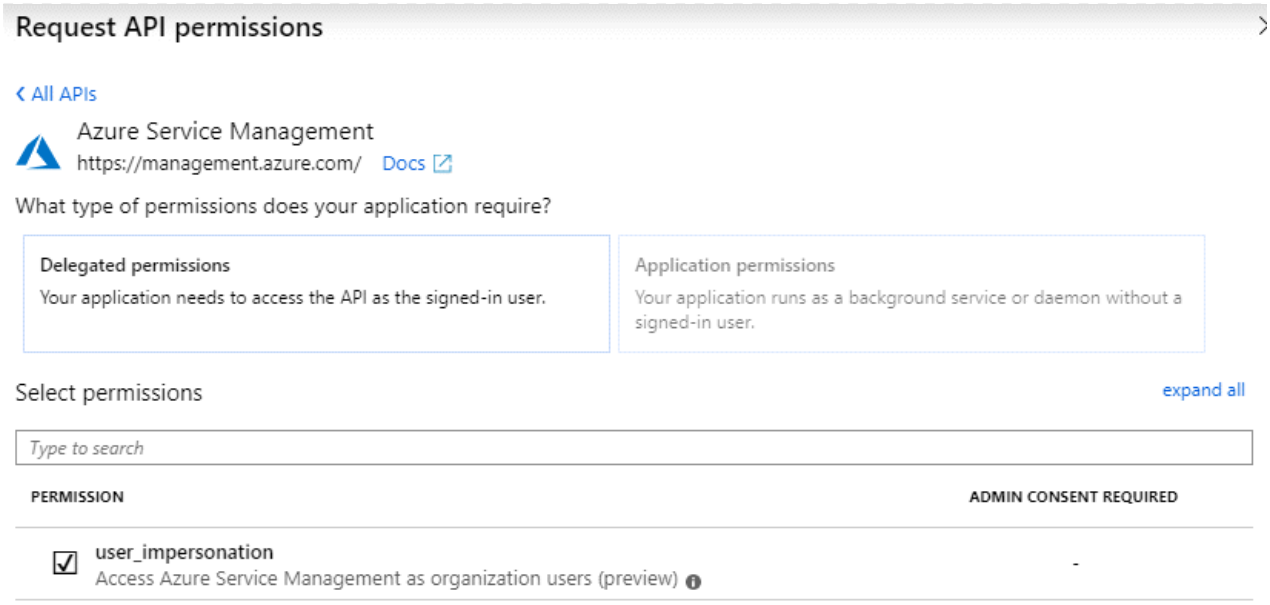
Ajouter des autorisations à l'API Windows Azure Service Management

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**.

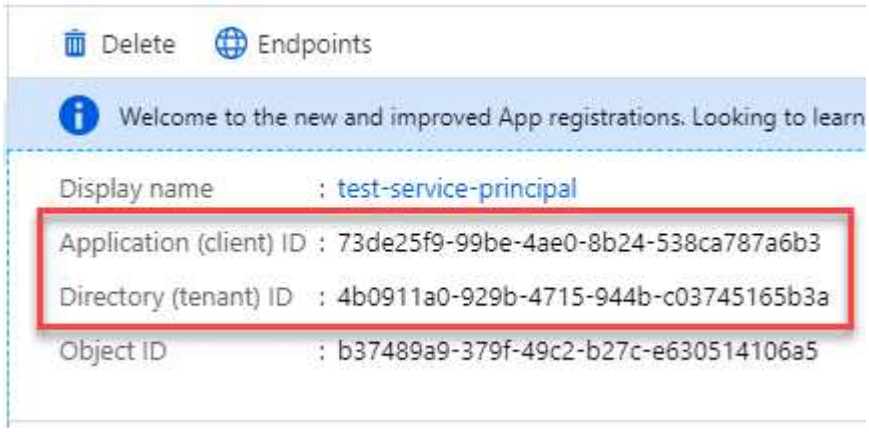


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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

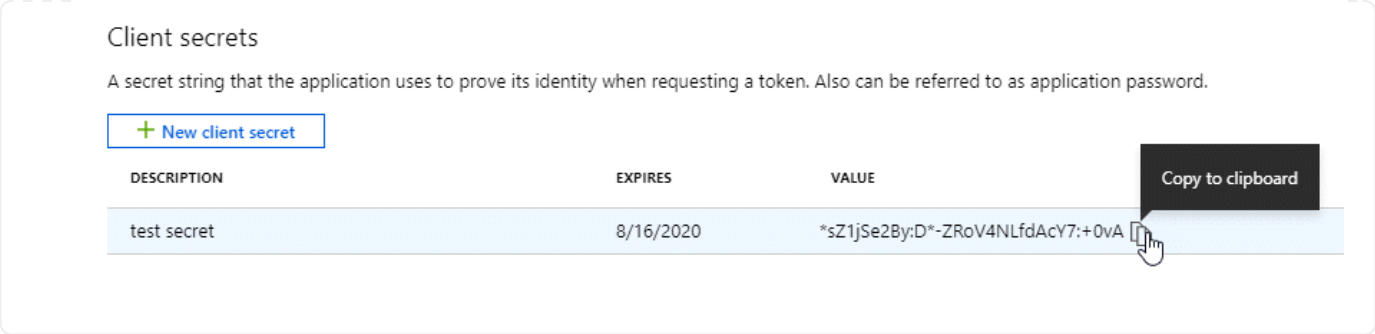
1. Dans le service **Microsoft Entra ID**, sélectionnez **Inscriptions d'applications** et sélectionnez l'application.
2. Copiez l'**ID d'application (client)** et l'**ID de répertoire (locataire)**.



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