Administrer et surveiller

NetApp Console setup and administration

NetApp
February 09, 2026

Sommaire

Administrer et surveiller . . . 1
- Comptes d’assistance NetApp associés . . . 1
  - Gérer les informations d’identification NSS associées à la NetApp Console . . . 1
  - Gérer les informations d’identification associées à votre connexion à la NetApp Console . . . 4
- Agents de console . . . 6
  - En savoir plus sur les agents de la NetApp Console . . . 6
  - Déployer un agent de console . . . 10
  - Agents de la console de maintenance . . . 166
  - Gérer les identifiants du fournisseur de cloud . . . 180
- Gestion des identités et des accès . . . 210
  - En savoir plus sur la gestion des identités et des accès de la NetApp Console . . . 210
  - Démarrer avec l’identité et l’accès dans la NetApp Console . . . 215
  - Configurez votre organisation de console . . . 216
  - Ajoutez des utilisateurs à votre organisation Console . . . 226
  - Gérer l’accès des utilisateurs et la sécurité . . . 229
  - Rôles d’accès à la NetApp Console . . . 236
  - API d’identité et d’accès . . . 257
- Sécurité et conformité . . . 258
  - Fédération d’identité . . . 258
  - Appliquer les autorisations ONTAP pour ONTAP Advanced View (ONTAP System Manager) . . . 271
  - Activer le mode lecture seule pour une organisation NetApp Console . . . 272
- Gérer les partenariats organisationnels . . . 274
  - Partenariats d’organisations dans la NetApp Console . . . 274
  - Gérer les partenariats dans la NetApp Console . . . 278
  - Gérer les membres d’une organisation partenaire . . . 280
  - Fournir un accès aux ressources aux utilisateurs du partenariat . . . 281
  - Travailler dans une organisation partenaire . . . 283
- Surveiller les opérations de la NetApp Console . . . 284
  - Auditer l’activité des utilisateurs à partir de la page Audit . . . 284
  - Surveiller les activités à l’aide du centre de notifications . . . 285

Administrer et surveiller

Comptes d’assistance NetApp associés

Gérer les informations d’identification NSS associées à la NetApp Console

Associez un compte de site de support NetApp à votre organisation de console pour activer les flux de travail clés pour la gestion du stockage. Ces informations d’identification NSS sont associées à l’ensemble de l’organisation.

La console prend également en charge l’association d’un compte NSS par compte utilisateur. "Apprenez à gérer les informations d’identification au niveau utilisateur" .

Aperçu

L’association des informations d’identification du site de support NetApp à votre numéro de série de compte de console spécifique est requise pour activer les tâches suivantes :

- Déploiement de Cloud Volumes ONTAP lorsque vous apportez votre propre licence (BYOL)

  Il est nécessaire de fournir votre compte NSS pour que la console puisse télécharger votre clé de licence et activer l’abonnement pour la durée que vous avez achetée. Cela inclut les mises à jour automatiques pour les renouvellements de mandat.

- Enregistrement des systèmes Cloud Volumes ONTAP à paiement à l’utilisation

  Fournir votre compte NSS est nécessaire pour activer le support de votre système et pour accéder aux ressources de support technique NetApp .

- Mise à niveau du logiciel Cloud Volumes ONTAP vers la dernière version

Ces informations d’identification sont associées au numéro de série de votre compte de console spécifique. Les utilisateurs peuvent accéder à ces informations d’identification depuis **Support > Gestion NSS**.

Ajouter un compte NSS

Vous pouvez ajouter et gérer vos comptes de site de support NetApp à utiliser avec la console à partir du tableau de bord de support dans la console.

Une fois que vous avez ajouté votre compte NSS, la console utilise ces informations pour des tâches telles que les téléchargements de licences, la vérification des mises à niveau logicielles et les futures inscriptions au support.

Vous pouvez associer plusieurs comptes NSS à votre organisation ; cependant, vous ne pouvez pas avoir de comptes clients et de comptes partenaires au sein de la même organisation.

NetApp utilise Microsoft Entra ID comme fournisseur d’identité pour les services d’authentification spécifiques au support et aux licences.

Étapes

1. Dans **Administration > Support**.

2. Sélectionnez **Gestion NSS**.
3. Sélectionnez **Ajouter un compte NSS**.
4. Sélectionnez **Continuer** pour être redirigé vers une page de connexion Microsoft.
5. Sur la page de connexion, indiquez votre adresse e-mail et votre mot de passe enregistrés sur le site de support NetApp .

   Une fois la connexion réussie, NetApp stockera le nom d'utilisateur NSS.

   Il s'agit d'un identifiant généré par le système qui correspond à votre e-mail. Sur la page **Gestion NSS**, vous pouvez afficher votre e-mail à partir du ••• menu.

   - Si vous avez besoin d'actualiser vos jetons d'identification de connexion, il existe également une option **Mettre à jour les informations d'identification** dans le ••• menu.

     L'utilisation de cette option vous invite à vous reconnecter. Notez que le jeton de ces comptes expire après 90 jours. Une notification sera publiée pour vous en informer.

Quelle est la prochaine étape ?

Les utilisateurs peuvent désormais sélectionner le compte lors de la création de nouveaux systèmes Cloud Volumes ONTAP et lors de l'enregistrement de systèmes Cloud Volumes ONTAP existants.

- "Lancement de Cloud Volumes ONTAP dans AWS"
- "Lancement de Cloud Volumes ONTAP dans Azure"
- "Lancement de Cloud Volumes ONTAP dans Google Cloud"
- "Enregistrement des systèmes de paiement à l'utilisation"

Mettre à jour les informations d'identification NSS

Pour des raisons de sécurité, vous devez mettre à jour vos informations d'identification NSS tous les 90 jours. Vous serez averti dans le centre de notifications de la console si vos informations d'identification NSS ont expiré. "En savoir plus sur le centre de notifications" .

Les informations d'identification expirées peuvent perturber les éléments suivants, sans toutefois s'y limiter :

- Mises à jour de licence, ce qui signifie que vous ne pourrez pas profiter de la capacité nouvellement achetée.
- Possibilité de soumettre et de suivre les cas d'assistance.

De plus, vous pouvez mettre à jour les informations d'identification NSS associées à votre organisation si vous souhaitez modifier le compte NSS associé à votre organisation. Par exemple, si la personne associée à votre compte NSS a quitté votre entreprise.

Étapes

1. Dans **Administration > Support**.
2. Sélectionnez **Gestion NSS**.
3. Pour le compte NSS que vous souhaitez mettre à jour, sélectionnez ••• puis sélectionnez **Mettre à jour les informations d'identification**.
4. Lorsque vous y êtes invité, sélectionnez **Continuer** pour être redirigé vers une page de connexion Microsoft.

NetApp utilise Microsoft Entra ID comme fournisseur d'identité pour les services d'authentification liés au support et aux licences.

5. Sur la page de connexion, indiquez votre adresse e-mail et votre mot de passe enregistrés sur le site de support NetApp .

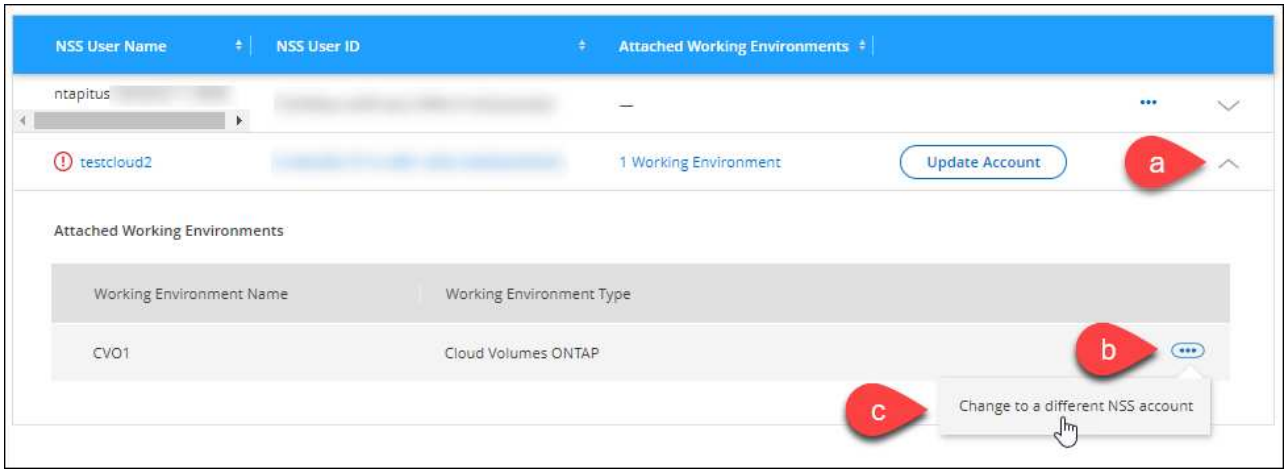
Attacher un système à un autre compte NSS

Si votre organisation dispose de plusieurs comptes de site de support NetApp , vous pouvez modifier le compte associé à un système Cloud Volumes ONTAP .

Vous devez d'abord avoir associé le compte à la Console.

Étapes

1. Dans **Administration > Support**.
2. Sélectionnez **Gestion NSS**.
3. Suivez les étapes suivantes pour modifier le compte NSS :
   a. Développez la ligne du compte du site de support NetApp auquel le système est actuellement associé.
   b. Pour le système pour lequel vous souhaitez modifier l'association, sélectionnez •••
   c. Sélectionnez **Changer de compte NSS**.



   d. Sélectionnez le compte puis sélectionnez **Enregistrer**.

Afficher l'adresse e-mail d'un compte NSS

Pour des raisons de sécurité, l'adresse e-mail associée à un compte NSS n'est pas affichée par défaut. Vous pouvez afficher l'adresse e-mail et le nom d'utilisateur associé à un compte NSS.

Lorsque vous accédez à la page de gestion NSS, la console génère un jeton pour chaque compte du tableau. Ce jeton inclut des informations sur l'adresse e-mail associée. Le jeton est supprimé lorsque vous quittez la page. Les informations ne sont jamais mises en cache, ce qui contribue à protéger votre vie privée.

Étapes

1. Dans **Administration > Support**.
2. Sélectionnez **Gestion NSS**.

3. Pour le compte NSS que vous souhaitez mettre à jour, sélectionnez••• puis sélectionnez **Afficher l'adresse e-mail**. Vous pouvez utiliser le bouton Copier pour copier l'adresse e-mail.

Supprimer un compte NSS

Supprimez tous les comptes NSS que vous ne souhaitez plus utiliser avec la console.

Vous ne pouvez pas supprimer un compte actuellement associé à un système Cloud Volumes ONTAP . Vous devez d'abordattacher ces systèmes à un autre compte NSS .

Étapes

1. Dans **Administration > Support**.
2. Sélectionnez **Gestion NSS**.
3. Pour le compte NSS que vous souhaitez supprimer, sélectionnez••• puis sélectionnez **Supprimer**.
4. Sélectionnez **Supprimer** pour confirmer.

Gérer les informations d'identification associées à votre connexion à la NetApp Console

Selon les actions que vous avez effectuées dans la console, vous avez peut-être associé les informations d'identification ONTAP et les informations d'identification du site de support NetApp (NSS) à votre connexion utilisateur. Vous pouvez afficher et gérer ces informations d'identification après les avoir associées. Par exemple, si vous modifiez le mot de passe de ces informations d'identification, vous devrez mettre à jour le mot de passe dans la console.

Informations d'identification ONTAP

Les utilisateurs ont besoin des informations d'identification d'administrateur ONTAP pour découvrir les clusters ONTAP dans la console. Cependant, l'accès à ONTAP System Manager dépend de l'utilisation ou non d'un agent de console.

Sans agent de console

Les utilisateurs sont invités à saisir leurs informations d'identification ONTAP pour accéder à ONTAP System Manager pour le cluster. Les utilisateurs peuvent choisir d'enregistrer ces informations d'identification dans la console, ce qui signifie qu'ils ne seront pas invités à les saisir à chaque fois. Les informations d'identification de l'utilisateur ne sont visibles que par l'utilisateur concerné et peuvent être gérées à partir de la page Informations d'identification de l'utilisateur.

Avec un agent de console

Par défaut, les utilisateurs ne sont pas invités à saisir leurs informations d'identification ONTAP pour accéder à ONTAP System Manager. Cependant, un administrateur de console (avec le rôle d'administrateur d'organisation) peut configurer la console pour inviter les utilisateurs à saisir leurs informations d'identification ONTAP . Lorsque ce paramètre est activé, les utilisateurs doivent saisir leurs informations d'identification ONTAP à chaque fois.

"Apprendre encore plus."

Informations d'identification NSS

Les informations d'identification NSS associées à votre connexion à la NetApp Console permettent l'enregistrement du support, la gestion des cas et l'accès à Digital Advisor.

- Lorsque vous accédez à **Support > Ressources** et que vous vous inscrivez à l'assistance, vous êtes invité à associer les informations d'identification NSS à votre connexion.

  Cela enregistre votre organisation ou votre compte pour l'assistance et active le droit à l'assistance. Un seul utilisateur de votre organisation doit associer un compte de site de support NetApp à sa connexion pour s'inscrire au support et activer le droit au support. Une fois cette opération terminée, la page **Ressources** indique que votre compte est enregistré pour l'assistance.

  "Apprenez comment vous inscrire pour bénéficier de l'assistance"

- Lorsque vous accédez à **Administration > Support > Gestion des cas**, vous êtes invité à saisir vos informations d'identification NSS, si vous ne l'avez pas déjà fait. Cette page vous permet de créer et de gérer les cas d'assistance associés à votre compte NSS et à votre entreprise.
- Lorsque vous accédez à Digital Advisor dans la console, vous êtes invité à vous connecter à Digital Advisor en saisissant vos informations d'identification NSS.

Notez les points suivants concernant le compte NSS associé à votre connexion :

- Le compte est géré au niveau de l'utilisateur, ce qui signifie qu'il n'est pas visible par les autres utilisateurs qui se connectent.
- Il ne peut y avoir qu'un seul compte NSS associé à Digital Advisor et à la gestion des cas d'assistance, par utilisateur.
- Si vous essayez d'associer un compte de site de support NetApp à un système Cloud Volumes ONTAP , vous ne pouvez choisir que parmi les comptes NSS qui ont été ajoutés à l'organisation dont vous êtes membre.

  Les informations d'identification au niveau du compte NSS sont différentes du compte NSS associé à votre connexion. Les informations d'identification au niveau du compte NSS vous permettent de déployer Cloud Volumes ONTAP avec BYOL, d'enregistrer les systèmes PAYGO et de mettre à niveau son logiciel.

  "En savoir plus sur l'utilisation des informations d'identification NSS avec votre organisation ou votre compte NetApp Console" .

Gérez vos identifiants d'utilisateur

Gérez vos informations d'identification utilisateur en mettant à jour le nom d'utilisateur et le mot de passe ou en supprimant les informations d'identification.

Étapes

1. Sélectionnez **Administration > Informations d'identification**.
2. Sélectionnez **Informations d'identification de l'utilisateur**.
3. Si vous ne disposez pas encore d'informations d'identification utilisateur, vous pouvez sélectionner **Ajouter des informations d'identification NSS** pour ajouter votre compte de site de support NetApp .
4. Gérez les informations d'identification existantes en choisissant les options suivantes dans le menu Actions :
   - **Mettre à jour les informations d'identification** : Mettez à jour le nom d'utilisateur et le mot de passe

du compte.

- **Supprimer les informations d'identification** : supprimez le compte NSS associé à votre connexion à la console.

Agents de console

En savoir plus sur les agents de la NetApp Console

Vous utilisez un agent Console pour connecter NetApp Console à votre infrastructure et orchestrer en toute sécurité des solutions de stockage sur AWS, Azure, Google Cloud ou des environnements sur site, ainsi que pour utiliser des services de protection des données.

Un agent Console vous permet de :

- Orchestrez les tâches de gestion du stockage depuis la NetApp Console, telles que le provisionnement de Cloud Volumes ONTAP, la configuration des volumes de stockage, l'utilisation de la classification des données, et bien plus encore.
- Authentifiez-vous à l'aide des rôles IAM de votre fournisseur de cloud pour l'intégration de la facturation des abonnements.
- Utilisez les services de données avancés (NetApp Backup and Recovery, NetApp Disaster Recovery, NetApp Ransomware Resilience et NetApp Cloud Tiering).
- Utilisez la console en mode restreint.

Si vous n'avez pas besoin d'orchestration avancée ni de protection des données, vous pouvez gérer de manière centralisée les clusters ONTAP sur site et les services de stockage natifs du cloud sans déployer d'agent. Des outils de surveillance et de mobilité des données sont également disponibles.

Le tableau suivant indique les fonctionnalités et services que vous pouvez utiliser avec et sans agent Console.

	Disponible avec agent	**Disponible sans agent**
Systèmes de stockage pris en charge :		
Amazon FSx pour ONTAP	Oui (fonctionnalités de découverte et de gestion)	Oui (découverte uniquement)
Stockage Amazon S3	Oui	Non
Stockage d'objets blob Azure	Oui	Oui
Azure NetApp Files	Oui	Oui
Cloud Volumes ONTAP	Oui	Non
Systèmes de la série E	Oui	Non
Google Cloud NetApp Volumes	Oui	Oui

	Disponible avec agent	Disponible sans agent
compartiments de stockage Google Cloud	Oui	Non
Systèmes StorageGRID	Oui	Non
Cluster ONTAP sur site (gestion et découverte avancées)	Oui (gestion et découverte avancées)	Non (découverte de base uniquement)
Services de gestion du stockage disponibles :		
Alertes	Oui	Non
Centre d'automatisation	Oui	Oui
Digital Advisor (Active IQ)	Oui	Non
Gestion des licences et des abonnements	Oui	Non
Efficacité économique	Oui	Non
Indicateurs du tableau de bord de la page d'accueil	Oui[2]	Non
Planification du cycle de vie	Oui	Non[1]
Durabilité	Oui	Non
Mises à jour logicielles	Oui	Oui
Charges de travail NetApp	Oui	Oui
Services de données disponibles :		
NetApp Backup and Recovery	Oui	Non
Classification des données	Oui	Non
NetApp Cloud Tiering	Oui	Non
NetApp Copy and Sync	Oui	Non
NetApp Disaster Recovery	Oui	Non
NetApp Ransomware Resilience	Oui	Non
NetApp Volume Caching	Oui	Non

[1] Vous pouvez consulter la planification du cycle de vie sans agent Console, mais un agent Console est nécessaire pour lancer des actions.

[2] Des indicateurs précis sur la page d'accueil nécessitent des agents de console correctement dimensionnés et configurés.

Les agents de console doivent être opérationnels à tout moment

Les agents de console sont un élément fondamental de la NetApp Console. Il est de votre responsabilité (en tant que client) de vous assurer que les agents concernés sont opérationnels et accessibles à tout moment. La console peut gérer de courtes pannes d'agent, mais vous devez corriger rapidement les pannes d'infrastructure.

Cette documentation est régie par le CLUF. L'utilisation du produit en dehors de la documentation peut avoir un impact sur ses fonctionnalités et sur vos droits CLUF.

Emplacements pris en charge

Vous pouvez installer des agents aux emplacements suivants :

- Amazon Web Services
- Microsoft Azure

  Déployez un agent de console dans Azure dans la même région que les systèmes Cloud Volumes ONTAP qu'il gère. Alternativement, déployez-le dans le "Paire de régions Azure" . Cela 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"

- Google Cloud

  Pour utiliser la console et les services de données avec Google Cloud, déployez votre agent dans Google Cloud.

- Dans vos locaux

Communication avec les fournisseurs de cloud

L'agent utilise TLS 1.3 pour toutes les communications avec AWS, Azure et Google Cloud.

Mode restreint

Pour utiliser la console en mode restreint, vous installez un agent de console et accédez à l'interface de la console qui s'exécute localement sur l'agent de console.

"En savoir plus sur les modes de déploiement de la NetApp Console" .

Comment installer un agent de console

Vous pouvez installer un agent de console directement depuis la console, depuis la place de marché de votre fournisseur de cloud ou en installant manuellement le logiciel sur votre propre hôte Linux ou dans votre environnement VCenter.

- "En savoir plus sur les modes de déploiement de la NetApp Console"
- "Démarrer avec la NetApp Console en mode standard"

- "Démarrer avec la NetApp Console en mode restreint"

Autorisations du fournisseur de cloud

Vous avez besoin d'autorisations spécifiques pour créer l'agent de console directement à partir de la NetApp Console et d'un autre ensemble d'autorisations pour l'agent de console lui-même. Si vous créez l'agent de console dans AWS ou Azure directement à partir de la console, la console crée l'agent de console avec les autorisations dont elle a besoin.

Lorsque vous utilisez la console en mode standard, la manière dont vous fournissez les autorisations dépend de la manière dont vous prévoyez de créer l'agent de la console.

Pour savoir comment configurer les autorisations, reportez-vous à ce qui suit :

- Mode standard
  - "Options d'installation de l'agent dans AWS"
  - "Options d'installation de l'agent dans Azure"
  - "Options d'installation de l'agent dans Google Cloud"
  - "Configurer les autorisations cloud pour les déploiements sur site"
- "Configurer les autorisations pour le mode restreint"

Pour afficher les autorisations exactes dont l'agent de la console a besoin pour les opérations quotidiennes, reportez-vous aux pages suivantes :

- "Découvrez comment l'agent de console utilise les autorisations AWS"
- "Découvrez comment l'agent de console utilise les autorisations Azure"
- "Découvrez comment l'agent de la console utilise les autorisations Google Cloud"

Il est de votre responsabilité de mettre à jour les stratégies de l'agent de la console à mesure que de nouvelles autorisations sont ajoutées dans les versions ultérieures. Les notes de publication répertorient les nouvelles autorisations.

Mises à niveau des agents

NetApp met à jour le logiciel de l'agent tous les mois pour ajouter des fonctionnalités et améliorer la stabilité. Certaines fonctionnalités de la console, telles que Cloud Volumes ONTAP et la gestion des clusters ONTAP sur site, dépendent de la version et des paramètres de l'agent de la console.

Lorsque vous installez votre agent dans le cloud, l'agent Console se met à jour automatiquement s'il dispose d'un accès Internet.

Maintenance du système d'exploitation et des machines virtuelles

La maintenance du système d'exploitation sur l'hôte de l'agent de console est votre responsabilité (celle du client). Par exemple, vous (client) devez appliquer les mises à jour de sécurité au système d'exploitation sur l'hôte de l'agent de console en suivant les procédures standard de votre entreprise pour la distribution du système d'exploitation.

Notez que vous (client) n'avez pas besoin d'arrêter les services sur l'hôte Console gent lors de l'application de mises à jour de sécurité mineures.

Si vous (client) devez arrêter puis démarrer la machine virtuelle de l'agent de console, vous devez le faire à

partir de la console de votre fournisseur de cloud ou en utilisant les procédures standard de gestion sur site.

L'agent de la console doit être opérationnel à tout moment .

Systèmes et agents multiples

Un agent peut gérer plusieurs systèmes et prendre en charge les services de données dans la console. Vous pouvez utiliser un seul agent pour gérer plusieurs systèmes en fonction de la taille du déploiement et des services de données que vous utilisez.

Pour les déploiements à grande échelle, travaillez avec votre représentant NetApp pour dimensionner votre environnement. Contactez le support NetApp si vous rencontrez des problèmes.

Voici quelques exemples de déploiements d'agents :

- Vous disposez d'un environnement multicloud (par exemple, AWS et Azure) et vous préférez avoir un agent dans AWS et un autre dans Azure. Chacun gère les systèmes Cloud Volumes ONTAP exécutés dans ces environnements.
- Un fournisseur de services peut utiliser une organisation de console pour fournir des services à ses clients, tout en utilisant une autre organisation pour assurer la reprise après sinistre de l'une de ses unités commerciales. Chaque organisation a besoin de son propre agent.

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 .

Points de terminaison	But
\ 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 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"
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 .

Points de terminaison	But
\ 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

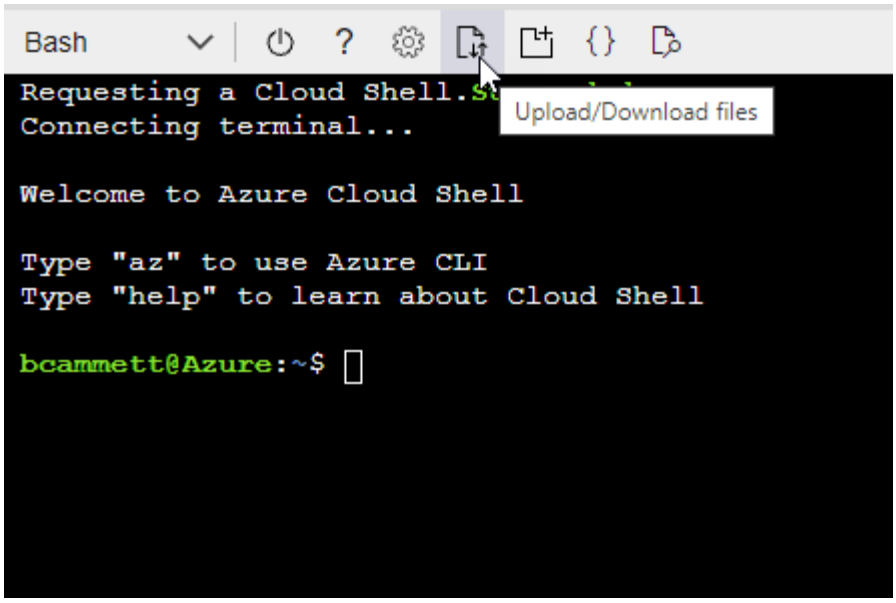
```
"AssignableScopes": [
"/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
]
```

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.

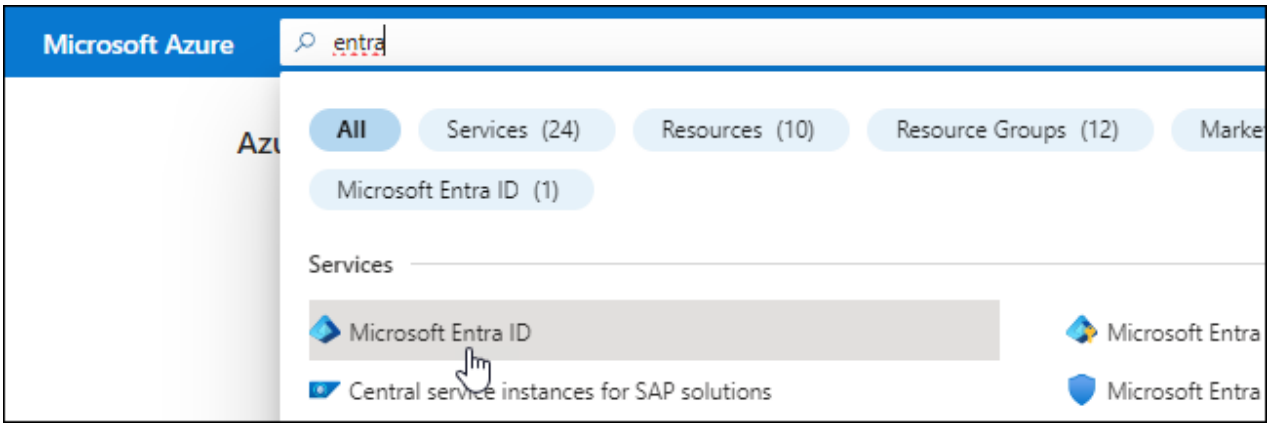
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont la console a besoin.

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**.



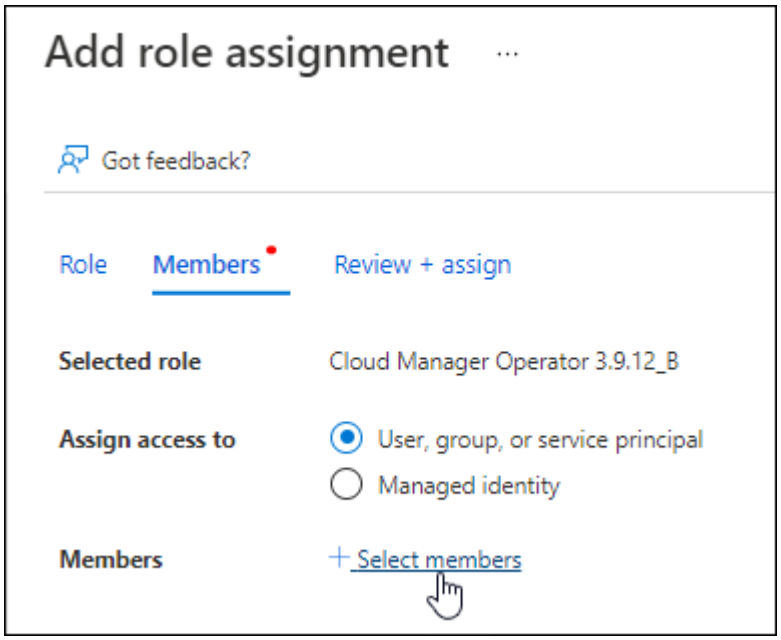
3. Dans le menu, sélectionnez **Inscriptions d'applications**.
4. Sélectionnez **Nouvelle inscription**.

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.

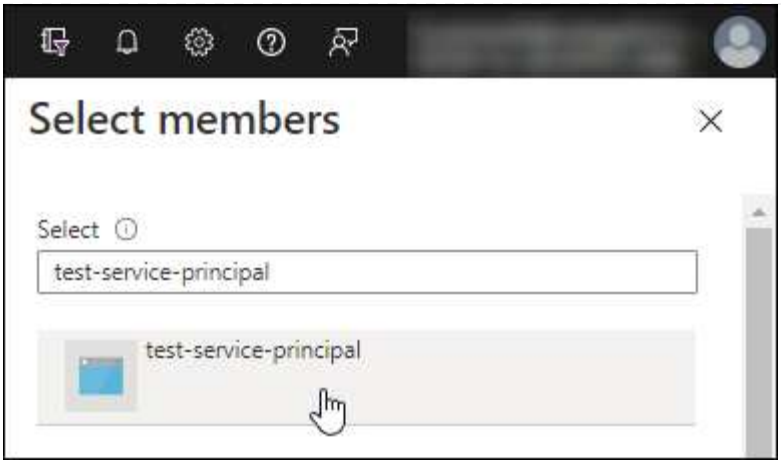
Attribuer le rôle personnalisé à l'application

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**.

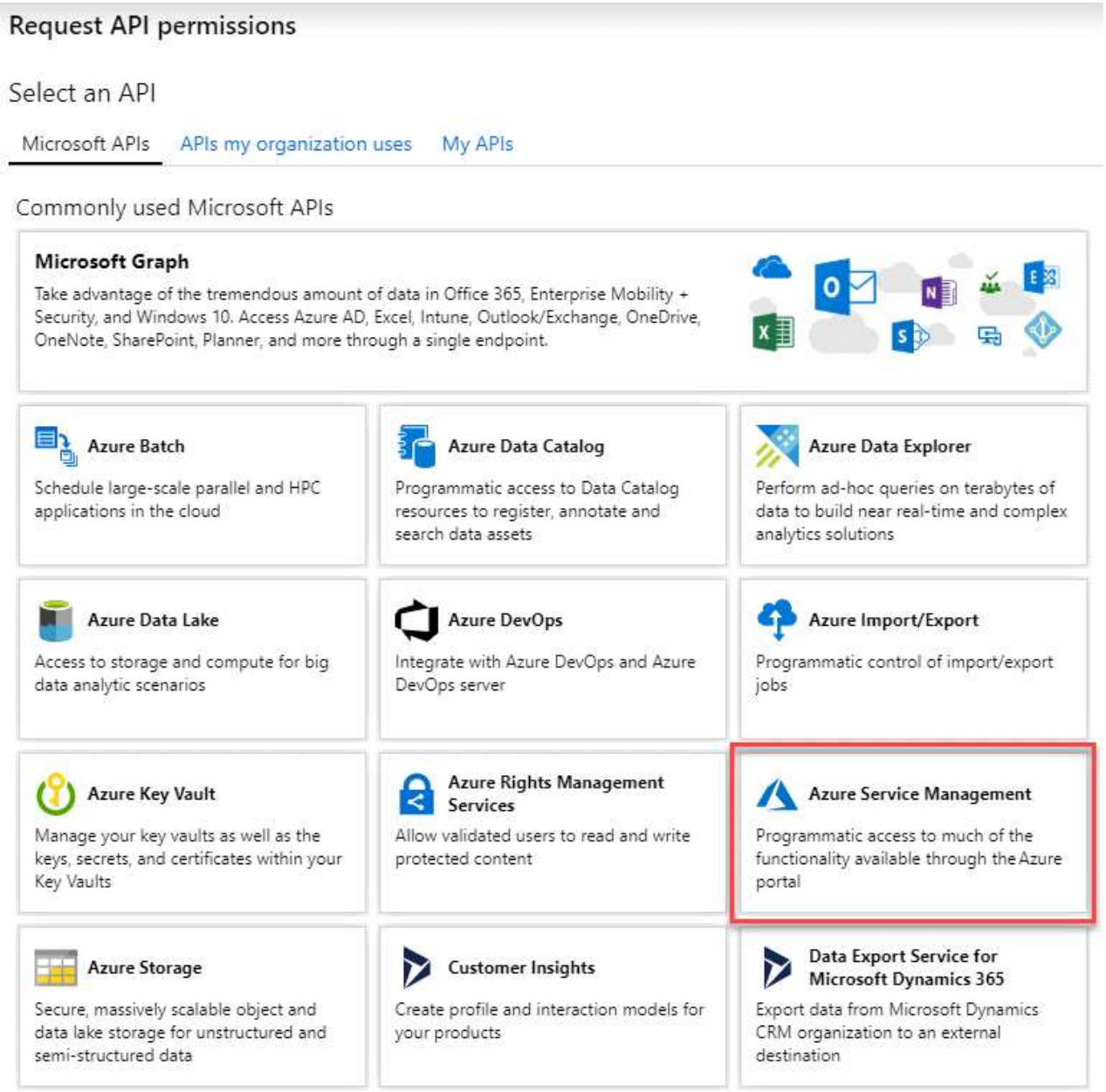
6. Cliquez sur **Réviser + attribuer**.

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

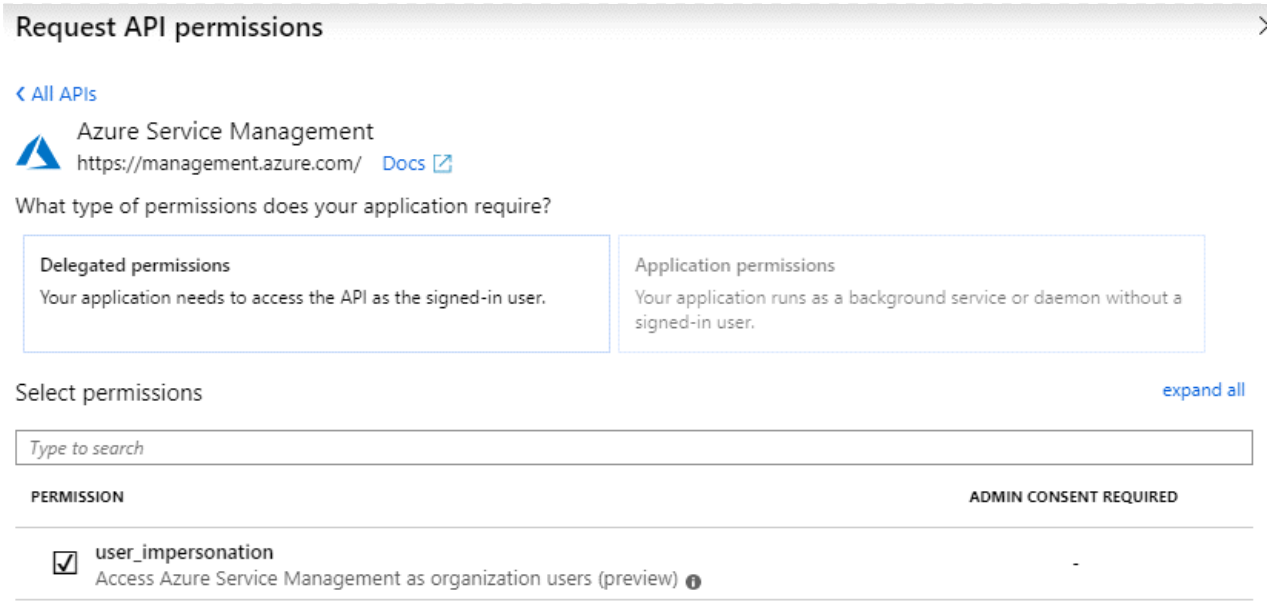
   Si vous souhaitez gérer des ressources dans plusieurs abonnements Azure, vous devez lier le principal de service à chacun de ces abonnements. Par exemple, la console vous permet de sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

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**.

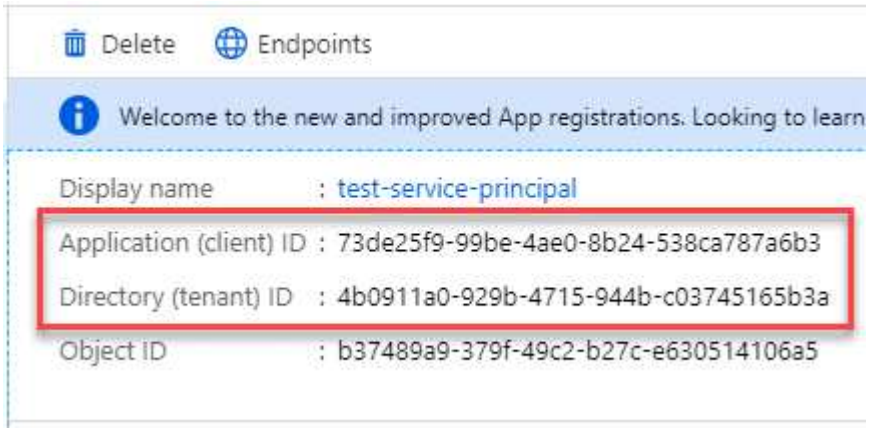


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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.

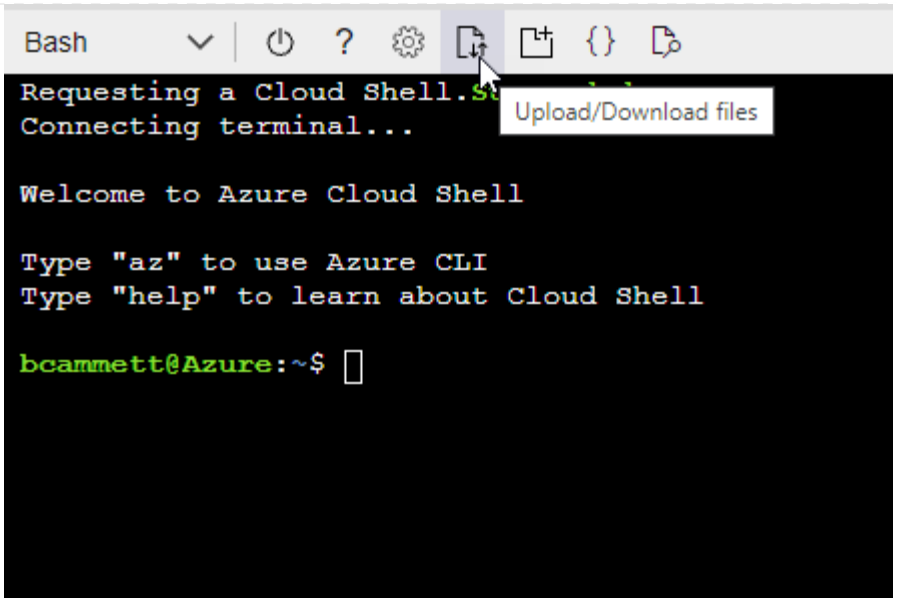
   Exemple

   ```
   "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

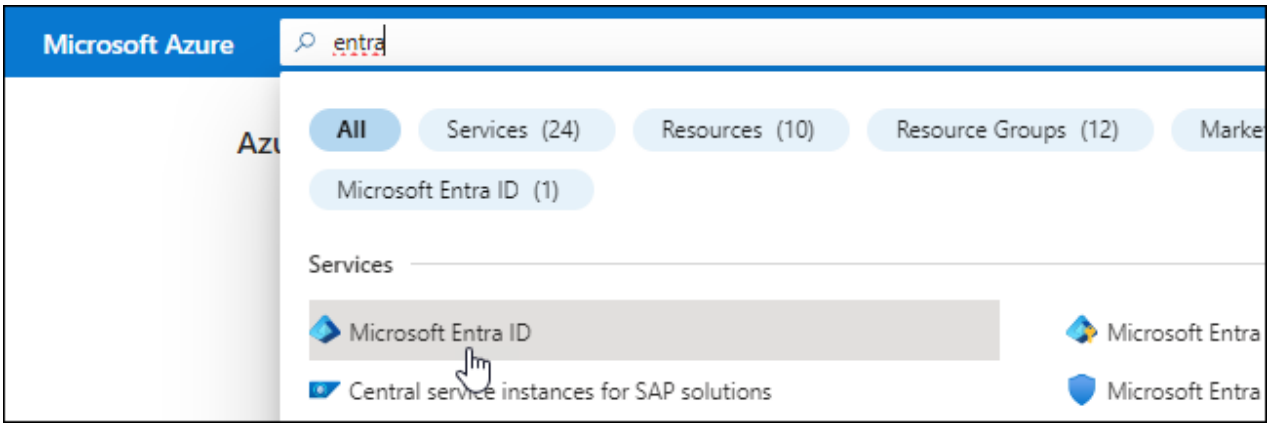
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont la console a besoin.

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 .

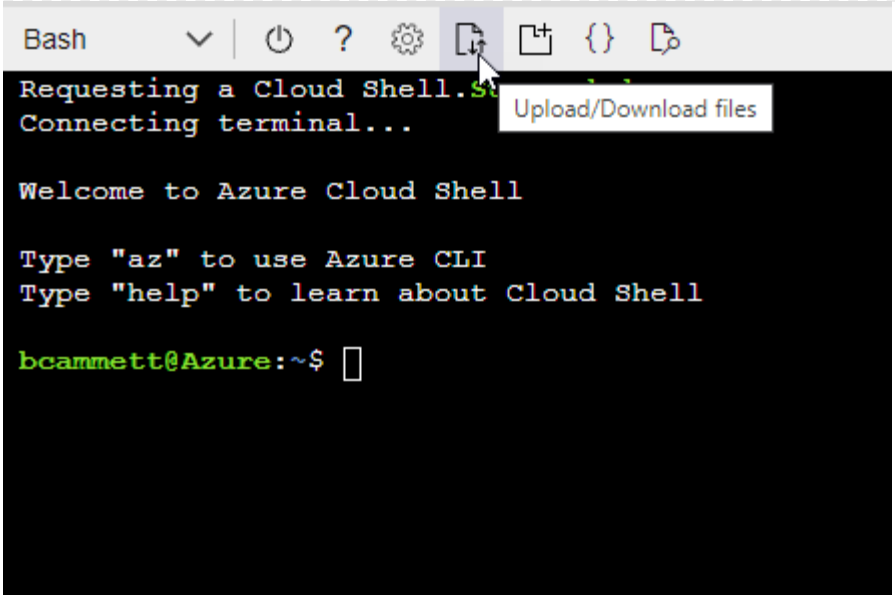
      Exemple

      ```
      "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**.

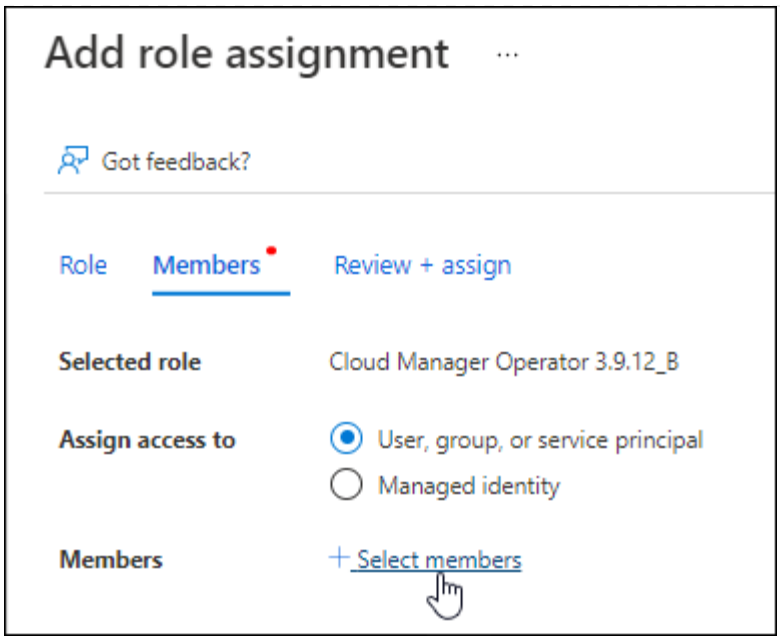
   b. Sélectionnez l'abonnement.

   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**.

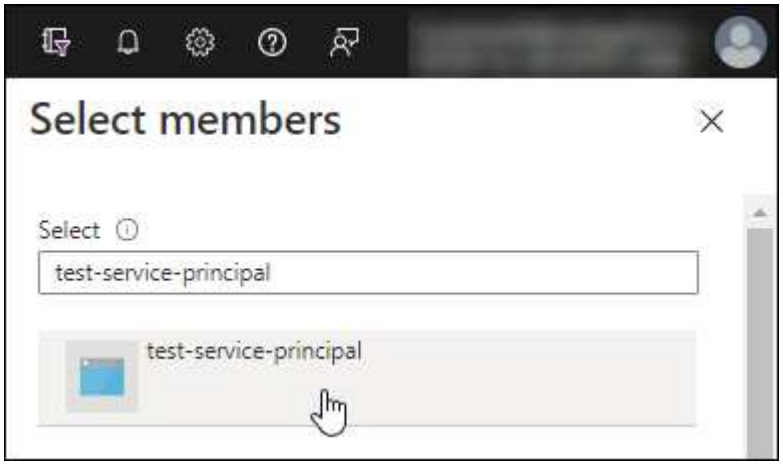
   e. Dans l'onglet **Membres**, procédez comme suit :

      - 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**.

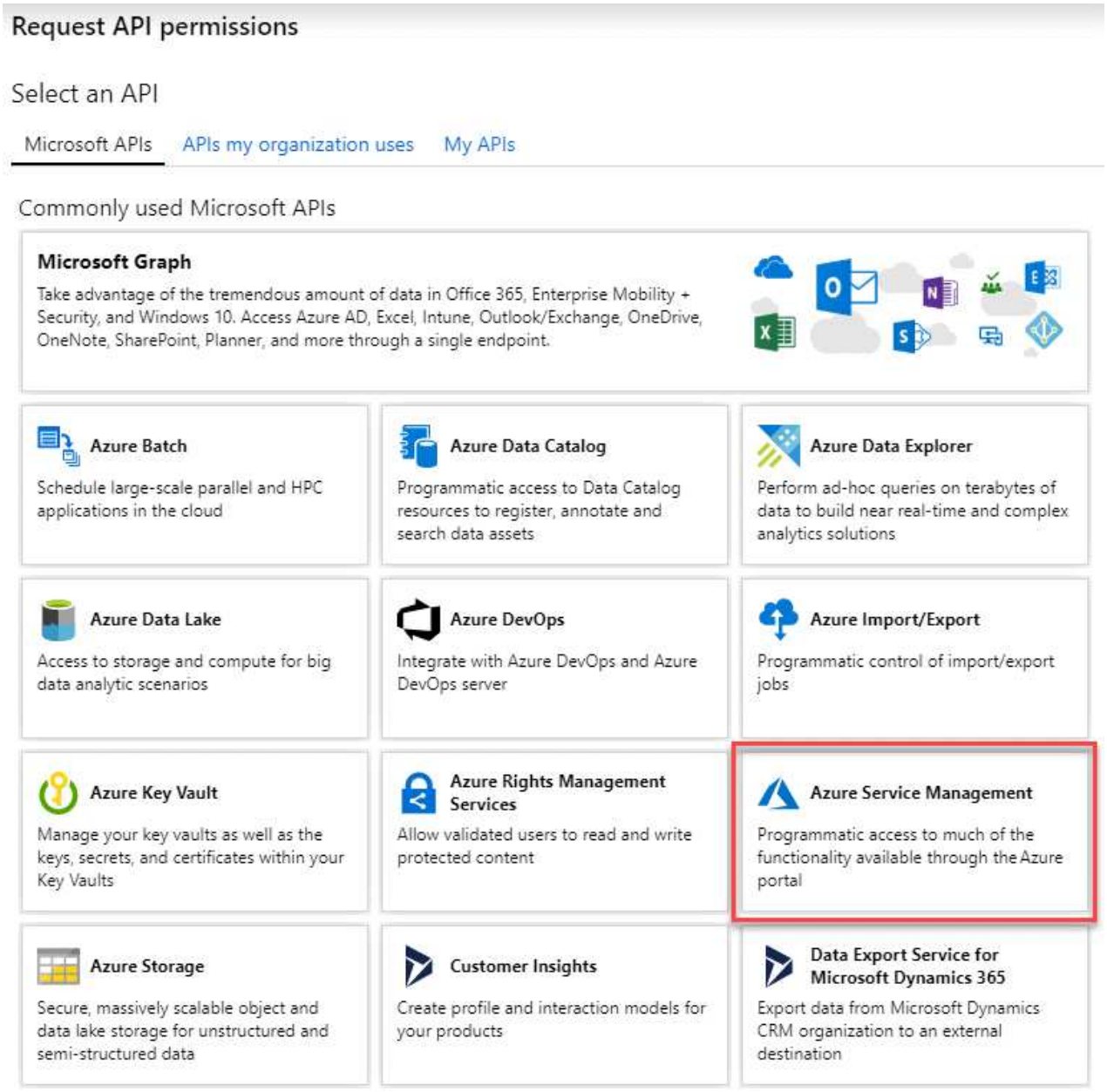
Le principal du service dispose désormais des autorisations Azure requises pour déployer l'agent de la console.

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.

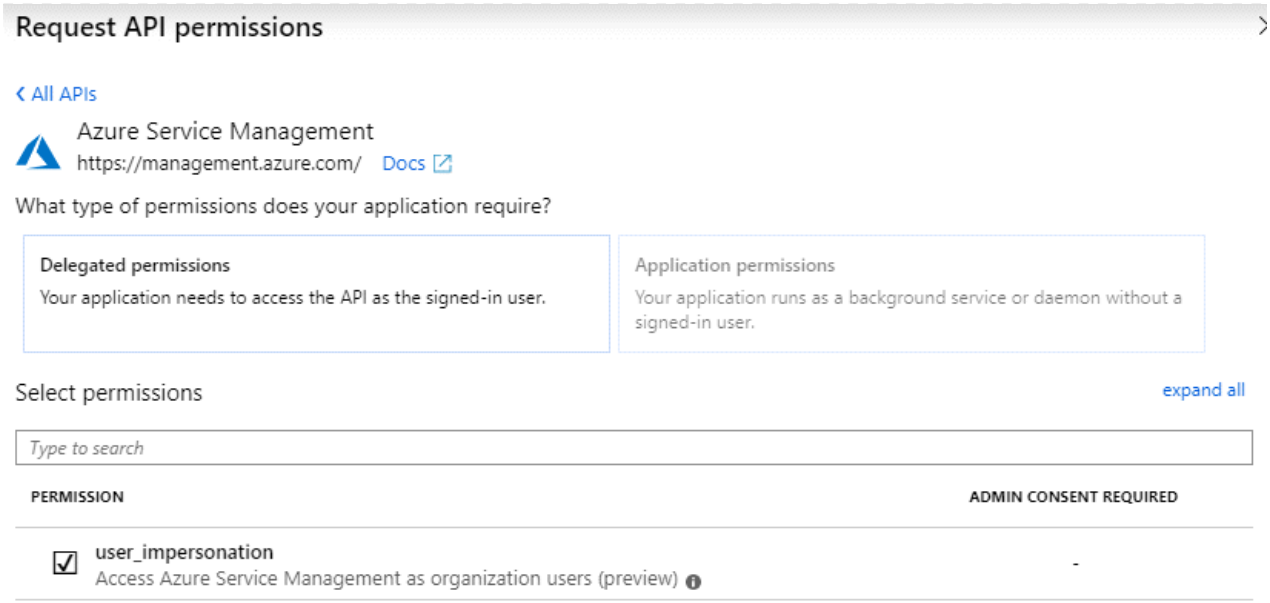
Ajouter des autorisations à l'API Windows Azure Service Management

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**.

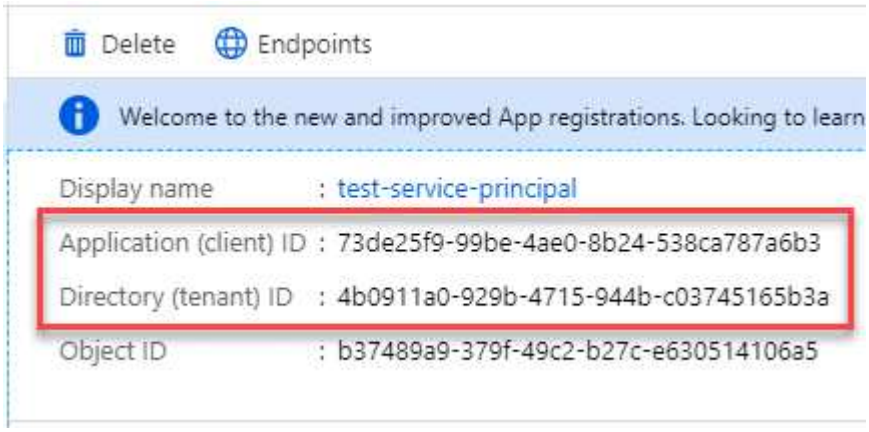


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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

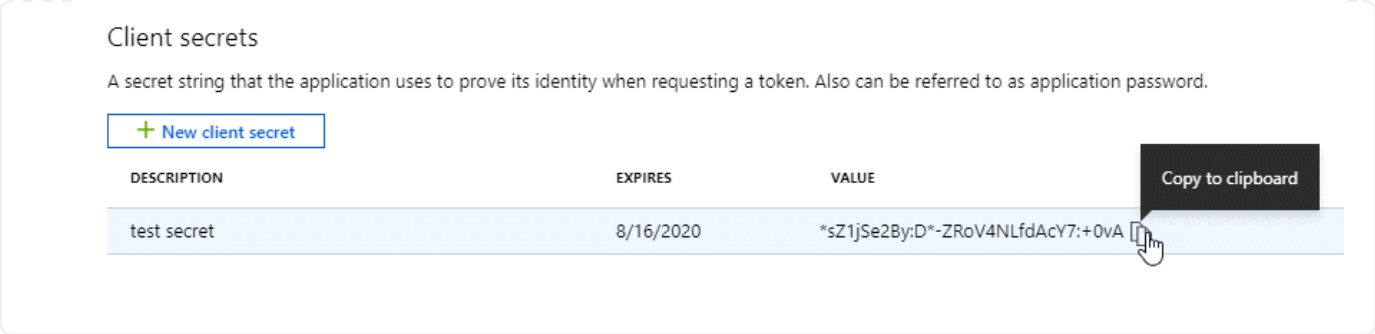
1. Dans le service **Microsoft Entra ID**, sélectionnez **Inscriptions d'applications** et sélectionnez l'application.
2. Copiez l'**ID d'application (client)** et l'**ID de répertoire (locataire)**.



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.

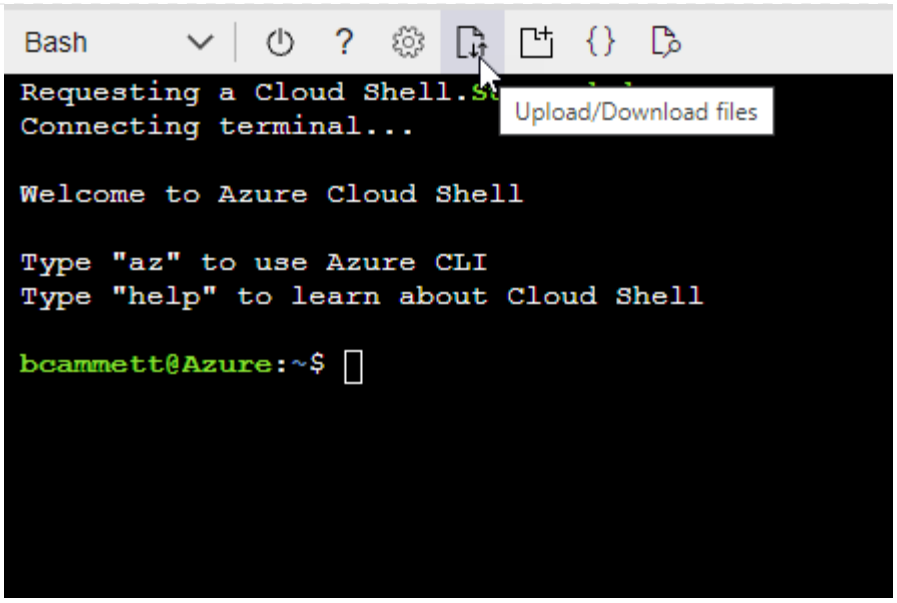
   Exemple

   ```
   "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

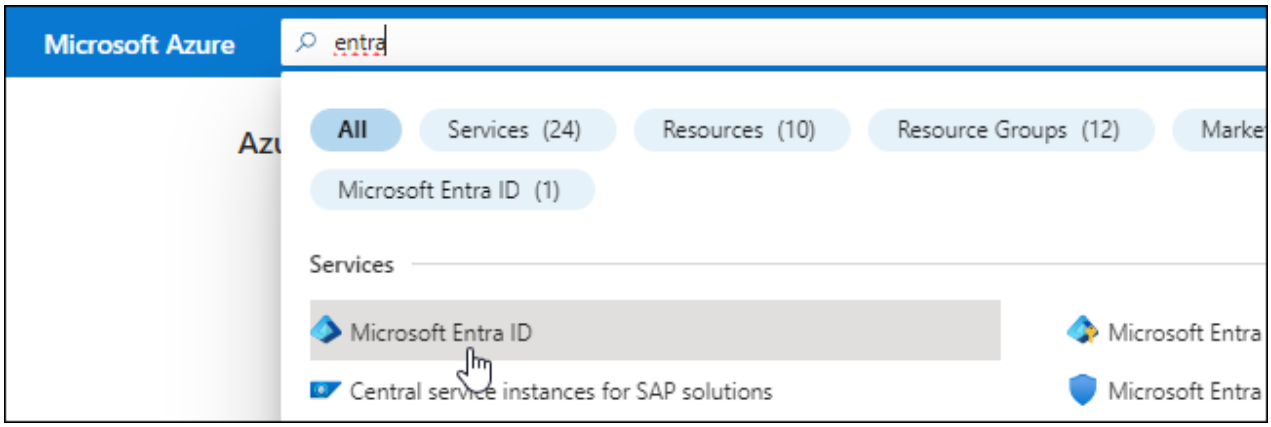
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont l'agent de la console a besoin.

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 .

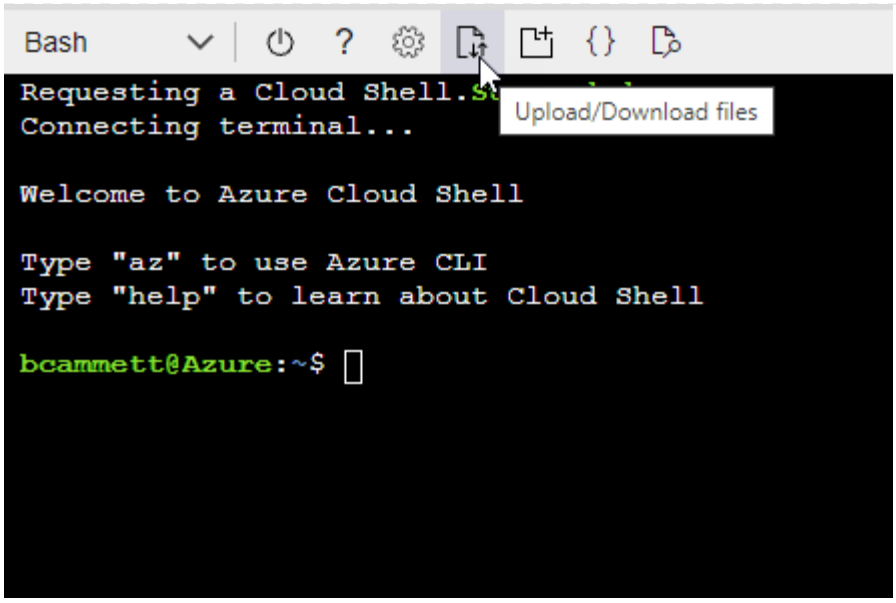
      Exemple

      ```
      "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**.

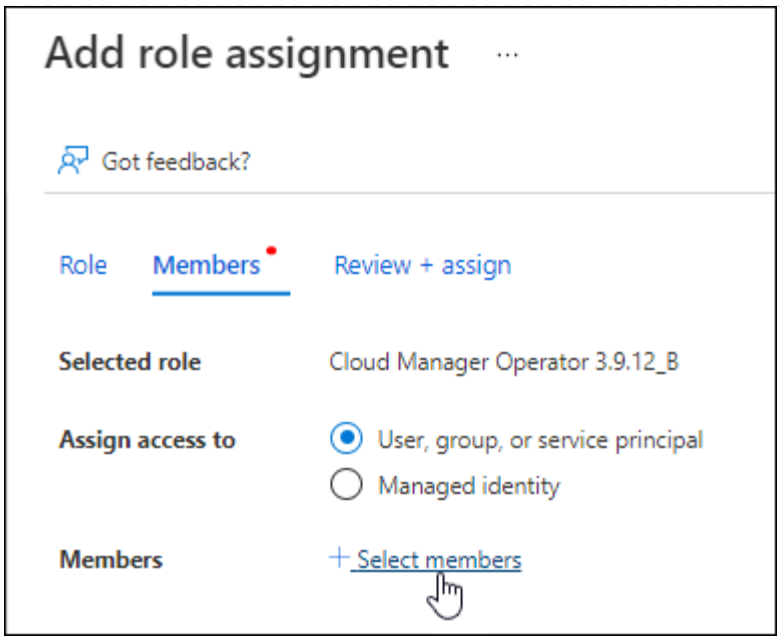
   b. Sélectionnez l'abonnement.

   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**.

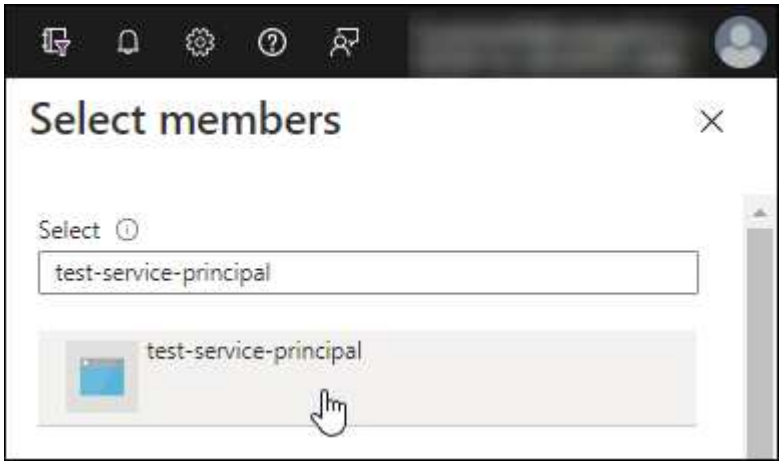
   e. Dans l'onglet **Membres**, procédez comme suit :

      - 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**.

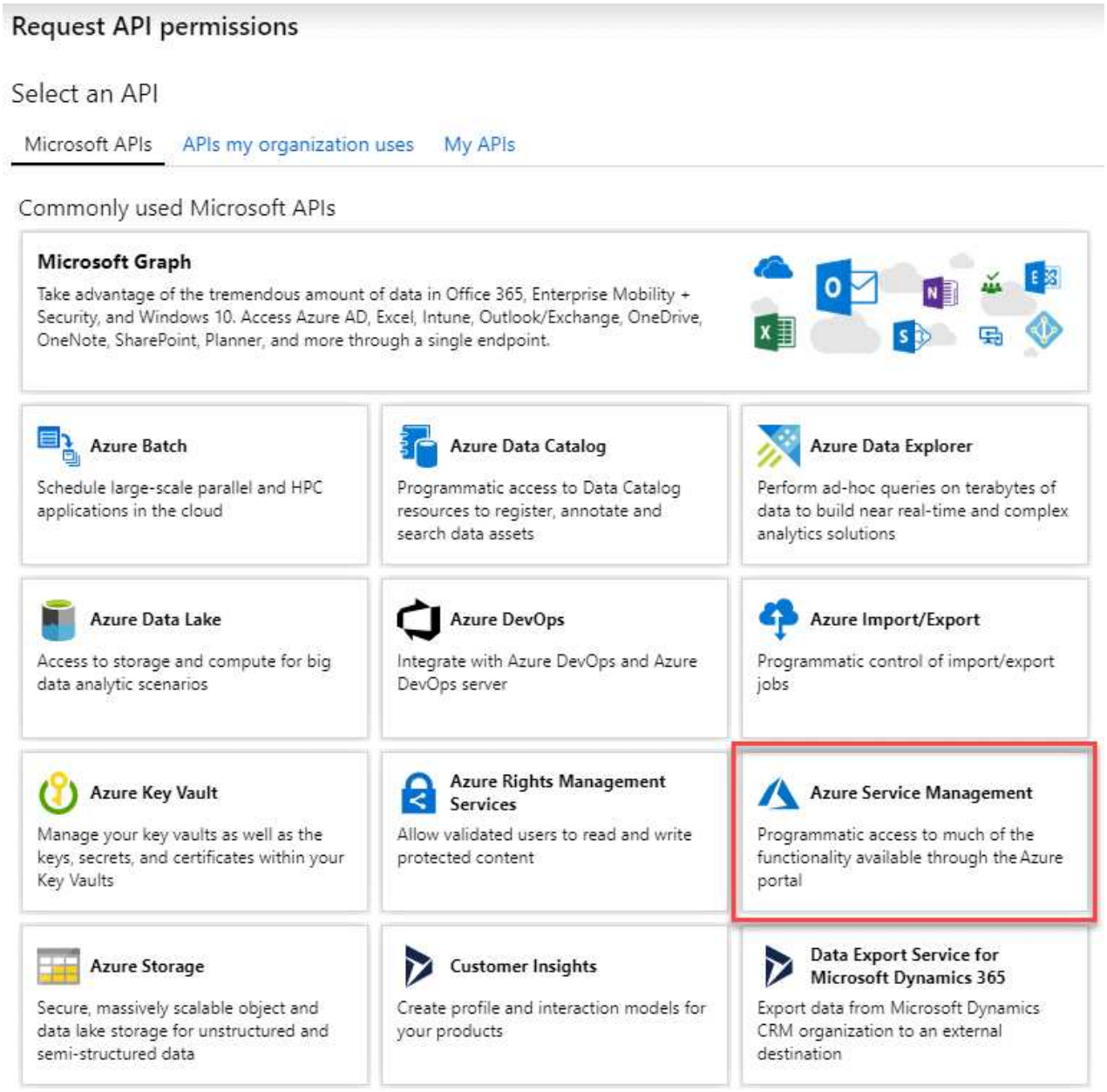
Le principal du service dispose désormais des autorisations Azure requises pour déployer l'agent de la console.

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.

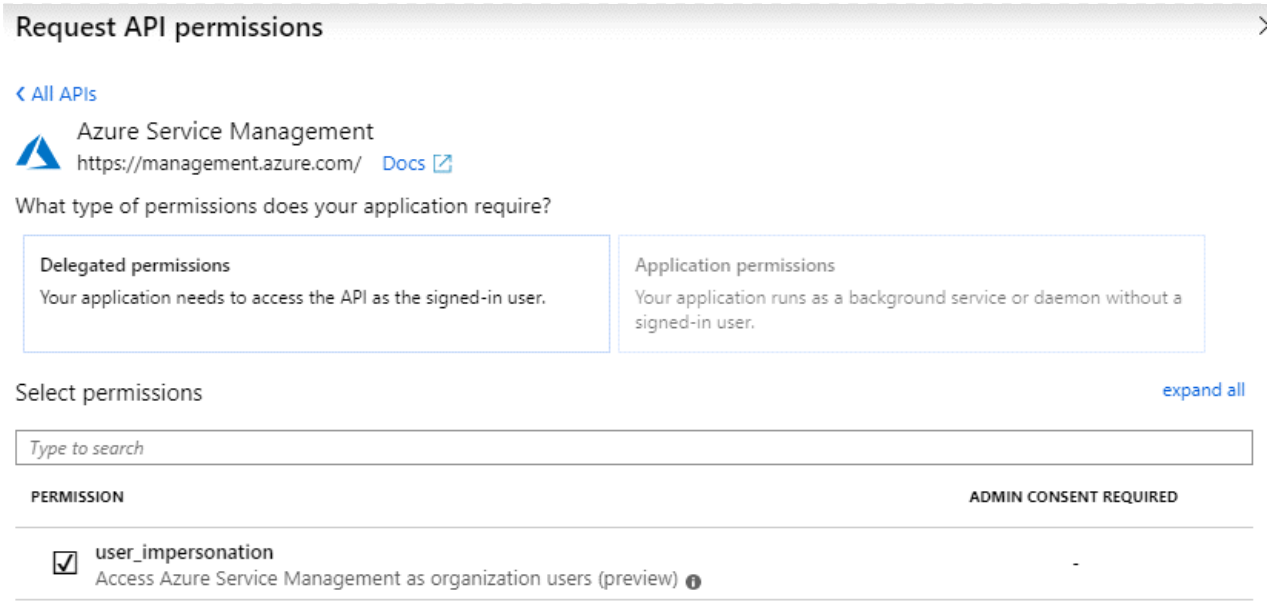
Ajouter des autorisations à l'API Windows Azure Service Management

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**.

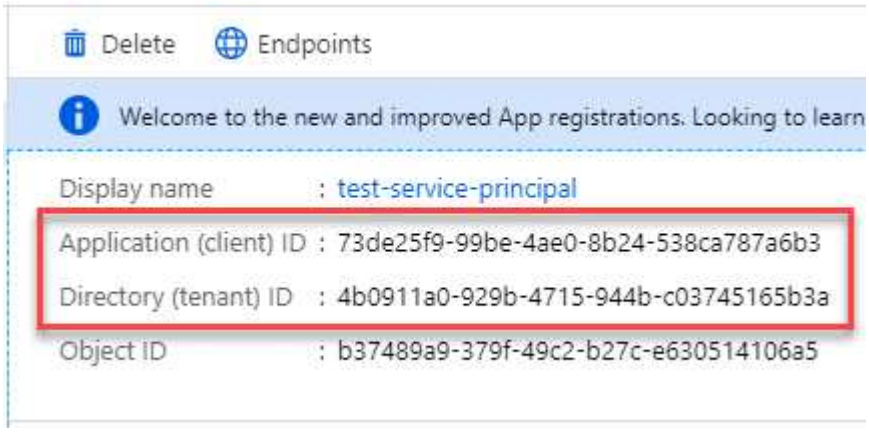


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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.
\ 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"

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"

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

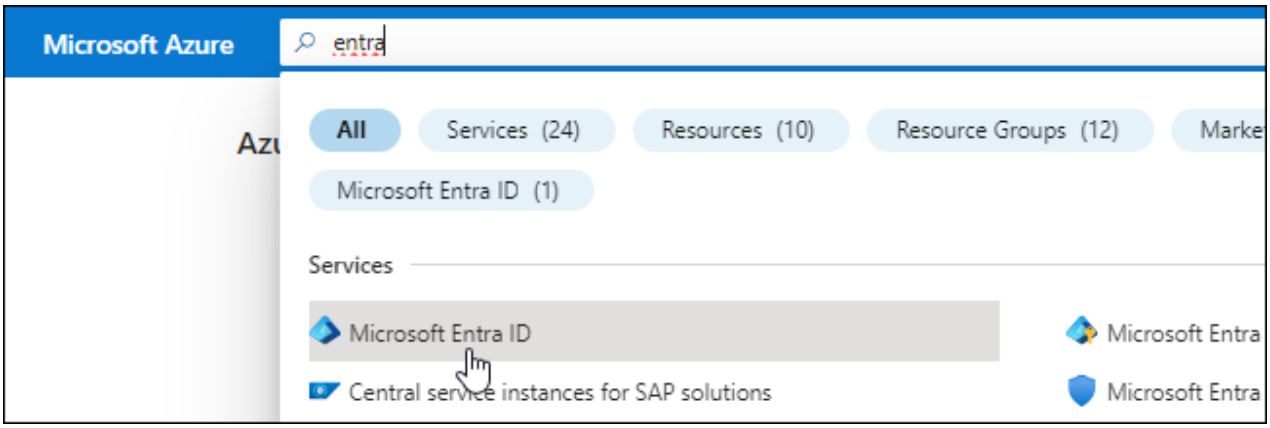
Lorsque l'agent de console est installé sur site, vous devez fournir à l'agent de console des autorisations Azure en configurant un principal de service dans Microsoft Entra ID et en obtenant les informations d'identification Azure dont l'agent de console a besoin.

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 .

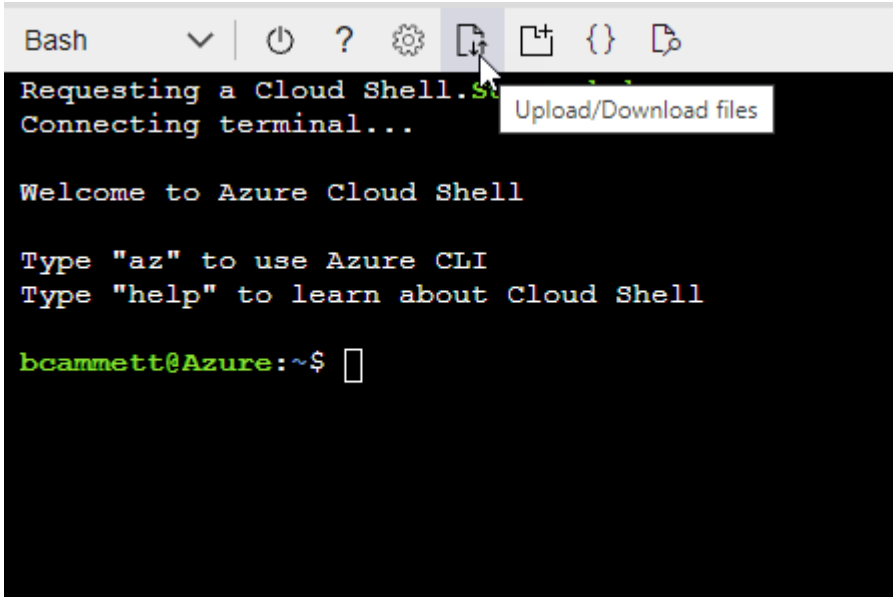
      Exemple

```
"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 :

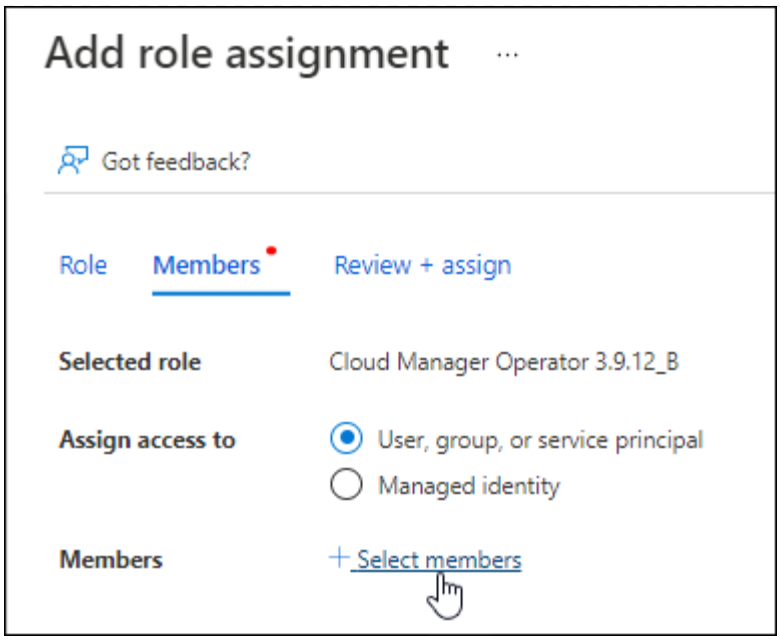
```
az role definition create --role-definition agent_Policy.json
```

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 :

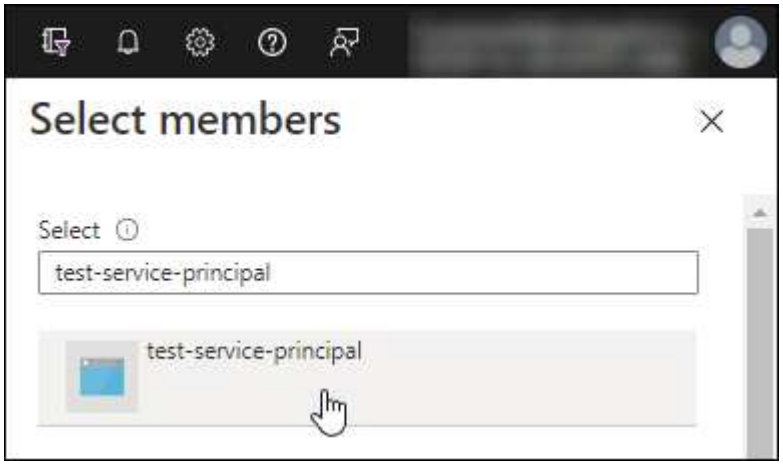
a. Depuis le portail Azure, ouvrez le service **Abonnements**.
b. Sélectionnez l'abonnement.
c. Sélectionnez **Contrôle d'accès (IAM) > Ajouter > Ajouter une attribution de rôle**.
d. Dans l'onglet **Rôle**, sélectionnez le rôle **Opérateur de console** et sélectionnez **Suivant**.
e. Dans l'onglet **Membres**,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

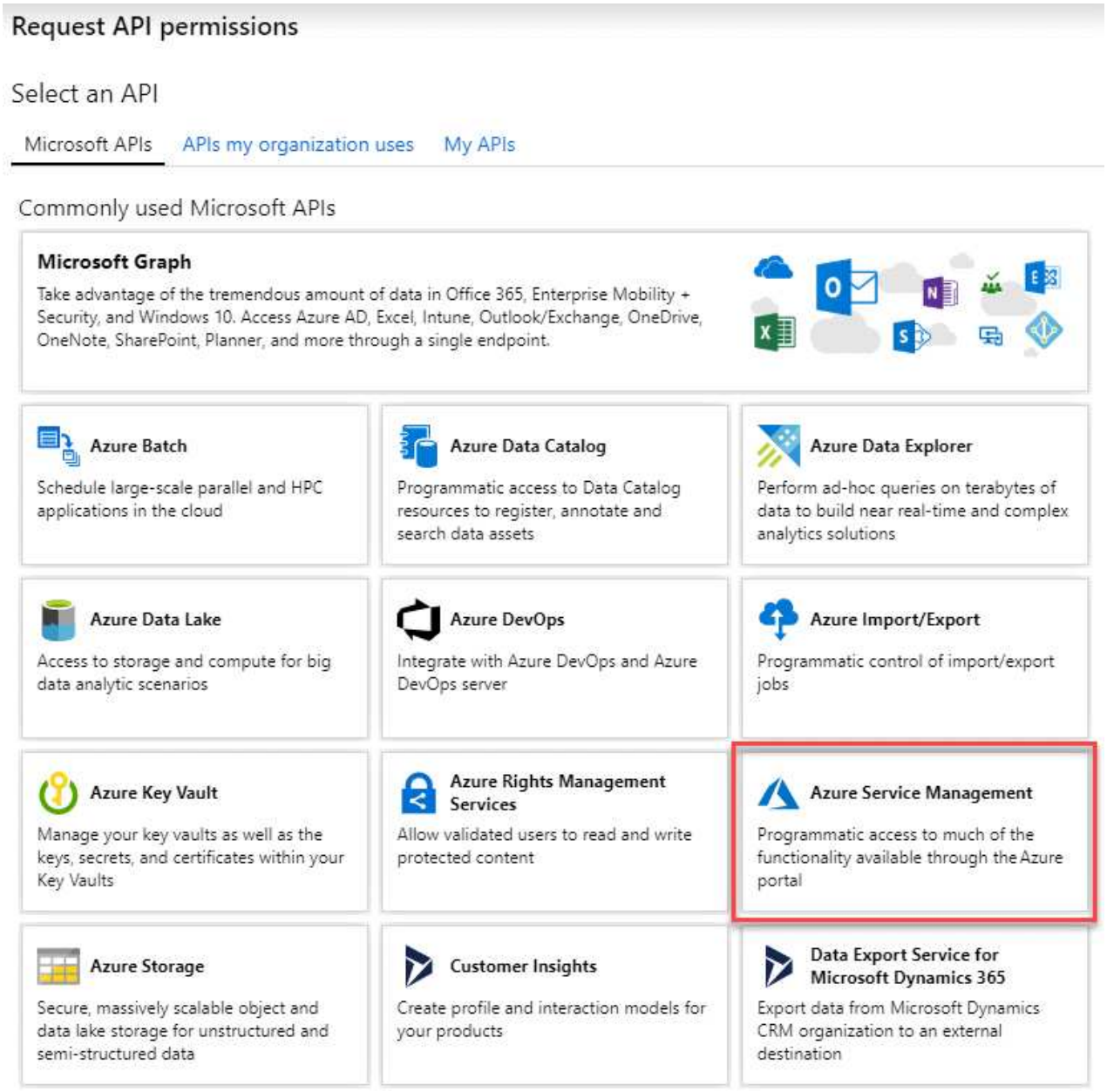
Le principal du service dispose désormais des autorisations Azure requises pour déployer l'agent de la console.

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.

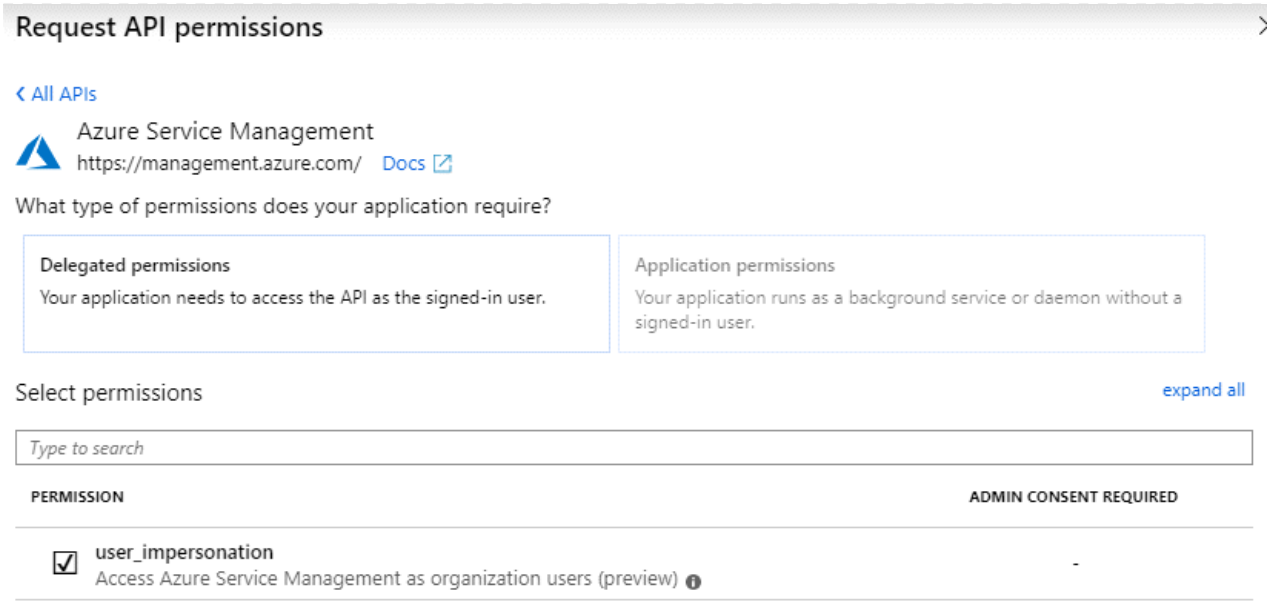
Ajouter des autorisations à l'API Windows Azure Service Management

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**.

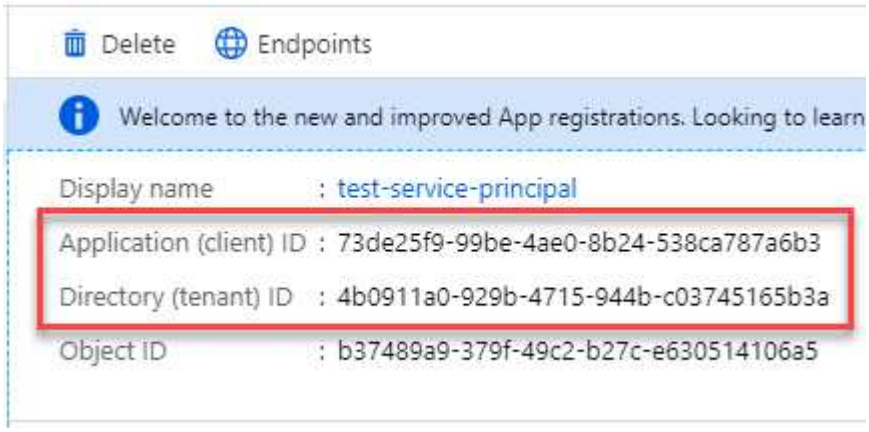


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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

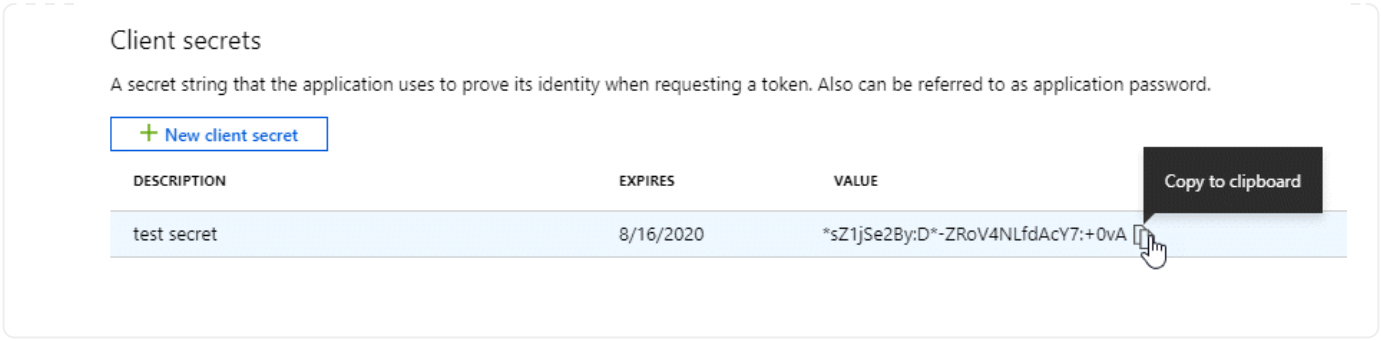
1. Dans le service **Microsoft Entra ID**, sélectionnez **Inscriptions d'applications** et sélectionnez l'application.
2. Copiez l'**ID d'application (client)** et l'**ID de répertoire (locataire)**.



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.

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

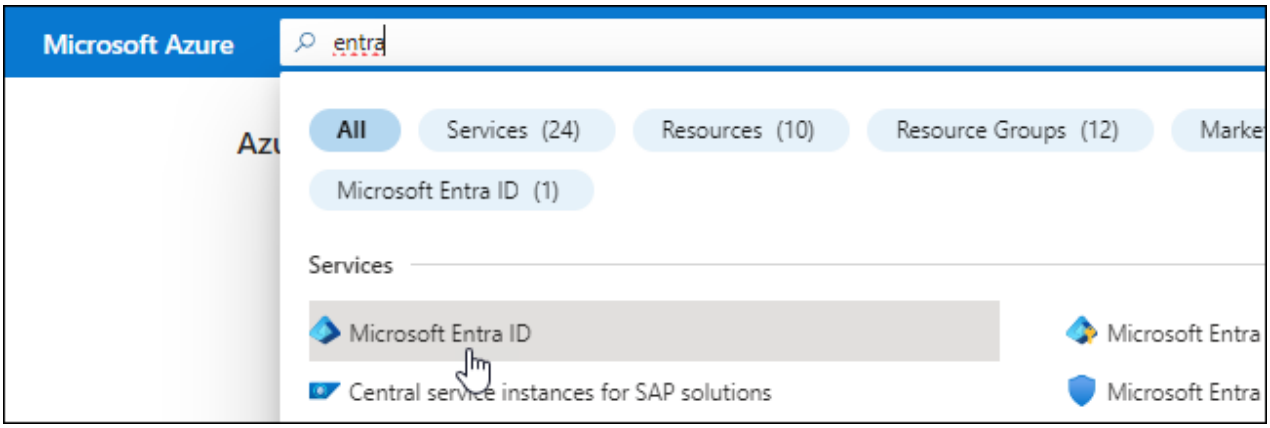
Lorsque l'agent de console est installé sur site, vous devez lui accorder des autorisations Azure en configurant un principal de service dans Microsoft Entra ID et en obtenant les informations d'identification Azure dont l'agent de console a besoin.

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 .

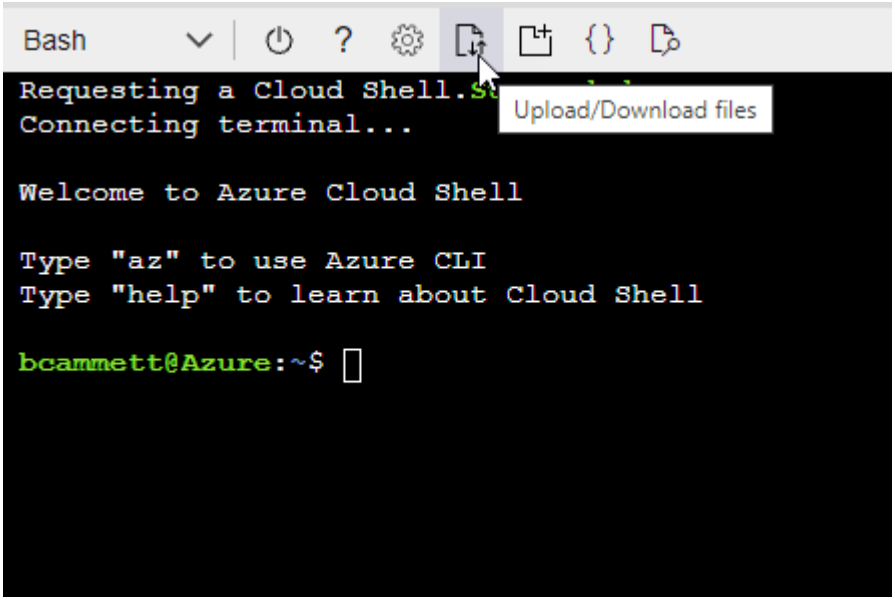
      Exemple

      ```
      "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 :

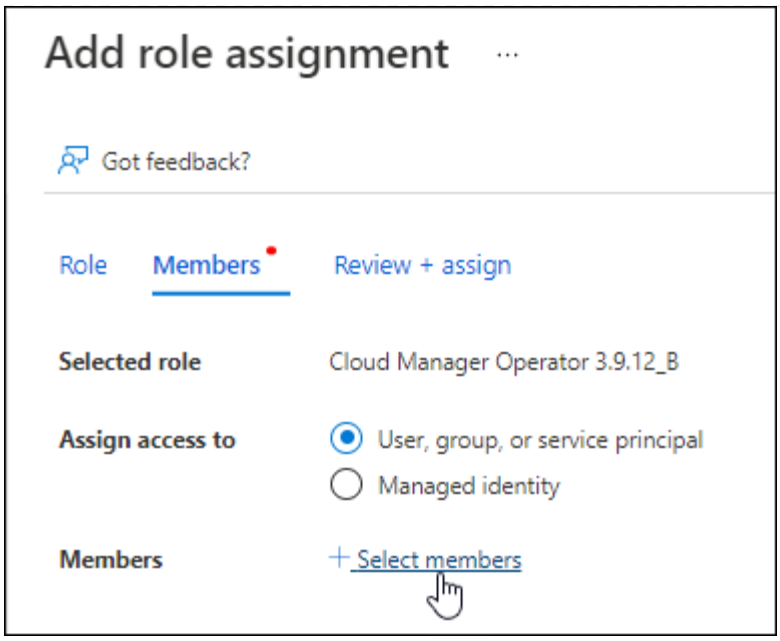
```
az role definition create --role-definition agent_Policy.json
```

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 :

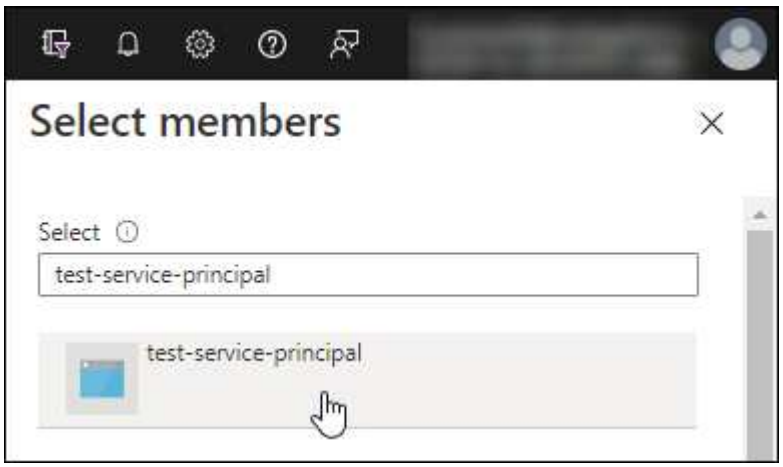
   a. Depuis le portail Azure, ouvrez le service **Abonnements**.
   b. Sélectionnez l'abonnement.
   c. Sélectionnez **Contrôle d'accès (IAM) > Ajouter > Ajouter une attribution de rôle**.
   d. Dans l'onglet **Rôle**, sélectionnez le rôle **Opérateur de console** et sélectionnez **Suivant**.
   e. Dans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

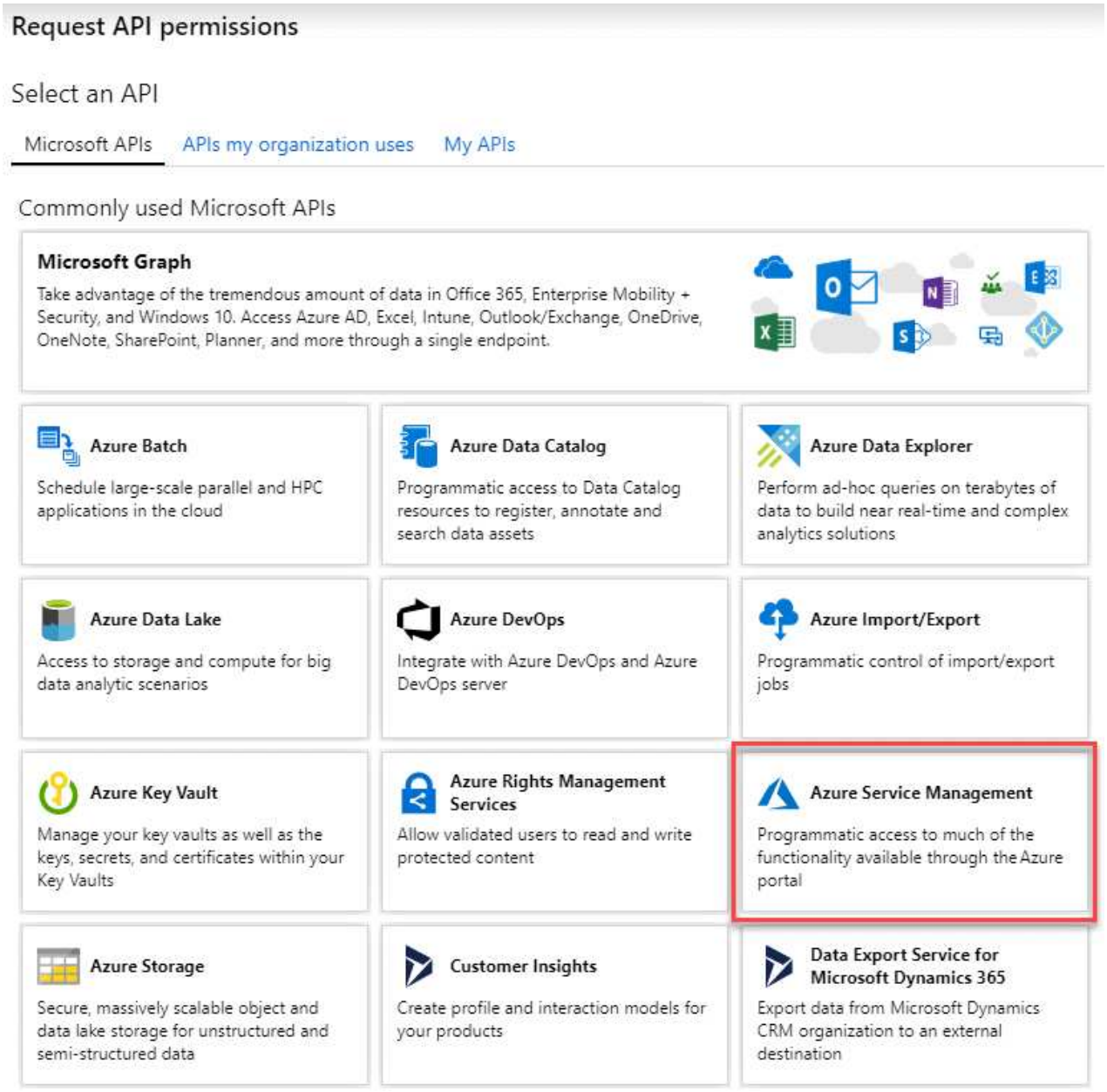
Le principal du service dispose désormais des autorisations Azure requises pour déployer l'agent de la console.

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.

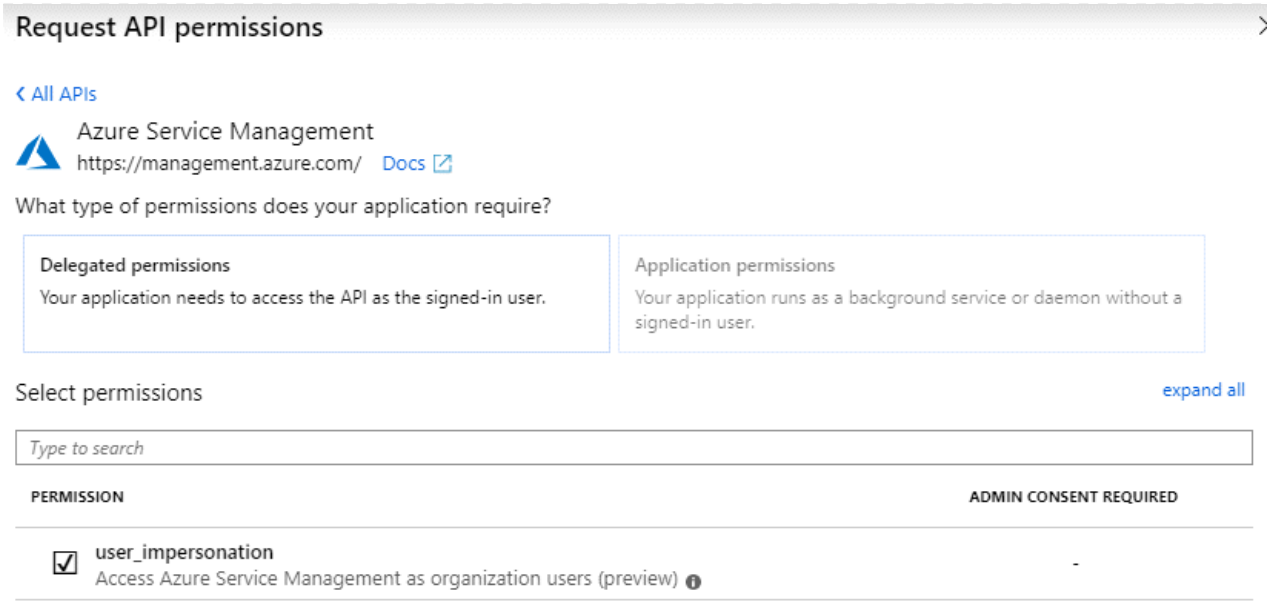
Ajouter des autorisations à l'API Windows Azure Service Management

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**.

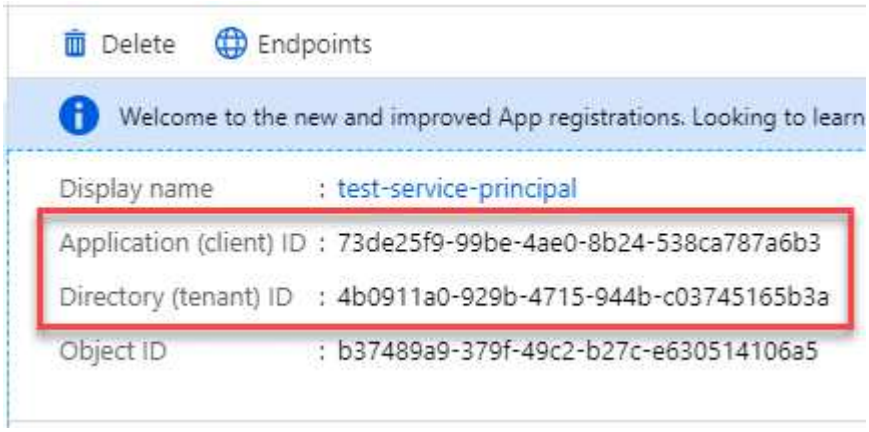


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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

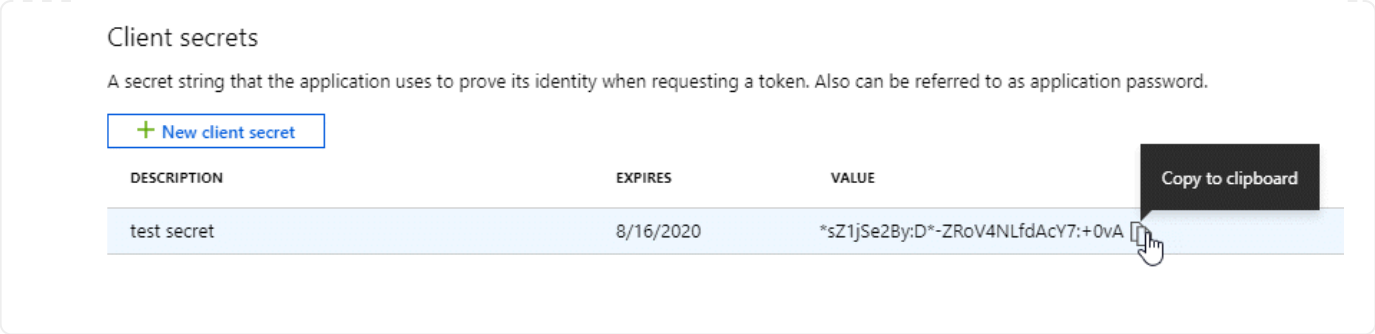
1. Dans le service **Microsoft Entra ID**, sélectionnez **Inscriptions d'applications** et sélectionnez l'application.
2. Copiez l'**ID d'application (client)** et l'**ID de répertoire (locataire)**.



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

Agents de la console de maintenance

Maintenir un hôte VCenter ou ESXi pour l'agent de console

Vous pouvez apporter des modifications à votre hôte VCenter ou ESXi existant après avoir déployé l'agent de console. Par exemple, vous pouvez augmenter la CPU ou la RAM de l'instance de machine virtuelle qui héberge l'agent de console.

Effectuez ces tâches de maintenance à l'aide de la console Web de la machine virtuelle :

- Augmenter la taille du disque
- Redémarrer l'agent
- Mettre à jour les routes statiques
- Mettre à jour les domaines de recherche

Limites

La mise à niveau de l'agent via la console n'est pas encore prise en charge. De plus, vous ne pouvez afficher que les informations sur l'adresse IP, le DNS et les passerelles.

Accéder à la console de maintenance de la machine virtuelle

Vous pouvez accéder à la console de maintenance à partir du client VSphere.

Étapes

1. Ouvrez le client VSphere et connectez-vous à votre VCenter.
2. Sélectionnez l'instance de machine virtuelle qui héberge l'agent de console.
3. Sélectionnez **Lancer la console Web**.
4. Connectez-vous à l'instance de machine virtuelle à l'aide du nom d'utilisateur et du mot de passe que vous avez spécifiés lors de la création de l'instance de machine virtuelle. Le nom d'utilisateur est `maint` et le mot de passe est celui que vous avez spécifié lors de la création de l'instance de VM.

Changer le mot de passe de l'utilisateur principal

Vous pouvez modifier le mot de passe pour le `maint` utilisateur.

Étapes

1. Ouvrez le client VSphere et connectez-vous à votre VCenter.
2. Sélectionnez l'instance de machine virtuelle qui héberge l'agent de console.
3. Sélectionnez **Lancer la console Web**.
4. Connectez-vous à l'instance de machine virtuelle à l'aide du nom d'utilisateur et du mot de passe que vous avez spécifiés lors de la création de l'instance de machine virtuelle. Le nom d'utilisateur est `maint` et le mot de passe est celui que vous avez spécifié lors de la création de l'instance de VM.
5. Entrer `1` pour voir le `System Configuration` menu.
6. Entrer `1` pour modifier le mot de passe de l'utilisateur de maintenance et suivre les instructions à l'écran.

Augmenter le CPU ou la RAM de l'instance VM

Vous pouvez augmenter la CPU ou la RAM de l'instance de machine virtuelle qui héberge l'agent de console.

Modifiez les paramètres de l'instance de machine virtuelle dans votre hôte VCenter ou ESXi, puis utilisez la console de maintenance pour appliquer les modifications.

Étapes du client VSphere

1. Ouvrez le client VSphere et connectez-vous à votre VCenter.
2. Sélectionnez l'instance de machine virtuelle qui héberge l'agent de console.
3. Cliquez avec le bouton droit sur l'instance de VM et sélectionnez **Modifier les paramètres**.
4. Augmentez l'espace disque dur utilisé pour la partition /opt ou /var.
   a. Sélectionnez **Disque dur 2** pour augmenter l'espace disque dur utilisé pour /opt.
   b. Sélectionnez **Disque dur 3** pour augmenter l'espace disque dur utilisé pour /var.
5. Enregistrez vos modifications.

Étapes de la console de maintenance

1. Ouvrez le client VSphere et connectez-vous à votre VCenter.
2. Sélectionnez l'instance de machine virtuelle qui héberge l'agent de console.
3. Sélectionnez **Lancer la console Web**.
4. Connectez-vous à l'instance de machine virtuelle à l'aide du nom d'utilisateur et du mot de passe que vous avez spécifiés lors de la création de l'instance de machine virtuelle. Le nom d'utilisateur est `maint` et le mot de passe est celui que vous avez spécifié lors de la création de l'instance de VM.
5. Entrer `1 to view the `System Configuration` menu.
6. Entrer `2` et suivez les instructions à l'écran. La console recherche de nouveaux paramètres et augmente la taille des partitions.

Afficher les paramètres réseau de la machine virtuelle de l'agent

Affichez les paramètres réseau de la machine virtuelle de l'agent dans le client VSphere pour confirmer ou résoudre les problèmes de réseau. Vous ne pouvez afficher (et non mettre à jour) que les paramètres réseau suivants : adresse IP et détails DNS.

Étapes

1. Ouvrez le client VSphere et connectez-vous à votre VCenter.
2. Sélectionnez l'instance de machine virtuelle qui héberge l'agent de console.
3. Sélectionnez **Lancer la console Web**.
4. Connectez-vous à l'instance de machine virtuelle à l'aide du nom d'utilisateur et du mot de passe que vous avez spécifiés lors de la création de l'instance de machine virtuelle. Le nom d'utilisateur est `maint` et le mot de passe est celui que vous avez spécifié lors de la création de l'instance de VM.
5. Entrer `2` pour voir le `Network Configuration` menu.
6. Saisissez un nombre compris entre 1 et 6 pour afficher les paramètres réseau correspondants.

Mettre à jour les routes statiques pour la machine virtuelle de l'agent

Ajoutez, mettez à jour ou supprimez des itinéraires statiques pour la machine virtuelle de l'agent selon les besoins.

Étapes

1. Ouvrez le client VSphere et connectez-vous à votre VCenter.
2. Sélectionnez l'instance de machine virtuelle qui héberge l'agent de console.
3. Sélectionnez **Lancer la console Web**.
4. Connectez-vous à l'instance de machine virtuelle à l'aide du nom d'utilisateur et du mot de passe que vous avez spécifiés lors de la création de l'instance de machine virtuelle. Le nom d'utilisateur est `maint` et le mot de passe est celui que vous avez spécifié lors de la création de l'instance de VM.
5. Entrer `2` pour voir le `Network Configuration` menu.
6. Entrer `7` pour mettre à jour les itinéraires statiques et suivre les invites à l'écran.
7. Appuyez sur Entrée.
8. Vous pouvez également apporter des modifications supplémentaires.
9. Entrer `9` pour valider vos modifications.

Mettre à jour les paramètres de recherche de domaine pour la machine virtuelle de l'agent

Vous pouvez mettre à jour les paramètres du domaine de recherche pour la machine virtuelle de l'agent.

Étapes

1. Ouvrez le client VSphere et connectez-vous à votre VCenter.
2. Sélectionnez l'instance de machine virtuelle qui héberge l'agent de console.
3. Sélectionnez **Lancer la console Web**.
4. Connectez-vous à l'instance de machine virtuelle à l'aide du nom d'utilisateur et du mot de passe que vous avez spécifiés lors de la création de l'instance de machine virtuelle. Le nom d'utilisateur est `maint` et le mot de passe est celui que vous avez spécifié lors de la création de l'instance de VM.
5. Entrer `2`` pour voir le `Network Configuration` menu.
6. Entrer `8` pour mettre à jour les paramètres de recherche de domaine et suivre les invites à l'écran.
7. Appuyez sur Entrée.
8. Vous pouvez également apporter des modifications supplémentaires.

9. Entrer `9` pour valider vos modifications.

Accéder aux outils de diagnostic de l'agent

Accédez aux outils de diagnostic pour résoudre les problèmes avec l'agent de la console. Le support NetApp peut vous demander de le faire lors du dépannage.

Étapes

1. Ouvrez le client VSphere et connectez-vous à votre VCenter.
2. Sélectionnez l'instance de machine virtuelle qui héberge l'agent de console.
3. Sélectionnez **Lancer la console Web**.
4. Connectez-vous à l'instance de machine virtuelle à l'aide du nom d'utilisateur et du mot de passe que vous avez spécifiés lors de la création de l'instance de machine virtuelle. Le nom d'utilisateur est `maint` et le mot de passe est celui que vous avez spécifié lors de la création de l'instance de VM.
5. Entrer `3` pour afficher le menu Support et Diagnostics.
6. Entrer `1` pour accéder aux outils de diagnostic et suivre les instructions à l'écran. + Par exemple, vous pouvez vérifier que tous les services d'agent sont en cours d'exécution. "Vérifiez l'état de l'agent de la console" .

Accéder aux outils de diagnostic de l'agent à distance

Vous pouvez accéder aux outils de diagnostic à distance avec un outil tel que Putty. Activez l'accès SSH à la machine virtuelle de l'agent en attribuant un mot de passe à usage unique.

L'accès SSH permet des fonctionnalités de terminal avancées telles que le copier-coller.

Étapes

1. Ouvrez le client VSphere et connectez-vous à votre VCenter.
2. Sélectionnez l'instance de machine virtuelle qui héberge l'agent de console.
3. Sélectionnez **Lancer la console Web**.
4. Connectez-vous à l'instance de machine virtuelle à l'aide du nom d'utilisateur et du mot de passe que vous avez spécifiés lors de la création de l'instance de machine virtuelle. Le nom d'utilisateur est `maint` et le mot de passe est celui que vous avez spécifié lors de la création de l'instance de VM.
5. Entrer `3` pour voir le `Support and Diagnostics` menu.
6. Entrer `2` pour accéder aux outils de diagnostic et suivre les invites à l'écran pour configurer un mot de passe à usage unique qui expire dans 24 heures.
7. Utilisez un outil SSH tel que Putty pour vous connecter à la machine virtuelle de l'agent à l'aide du nom d'utilisateur `diag` et le mot de passe à usage unique que vous avez configuré.

Installer un certificat signé par une autorité de certification pour l'accès à la console Web

Lorsque vous utilisez la NetApp Console en mode restreint, l'interface utilisateur est accessible à partir de la machine virtuelle de l'agent de console déployée dans votre région cloud ou sur site. Par défaut, la console utilise un certificat SSL auto-signé pour fournir un accès HTTPS sécurisé à la console Web exécutée sur l'agent de console.

Si votre entreprise l'exige, vous pouvez installer un certificat signé par une autorité de certification (CA), qui

offre une meilleure protection de sécurité qu'un certificat auto-signé. Une fois le certificat installé, la console utilise le certificat signé par une autorité de certification lorsque les utilisateurs accèdent à la console Web.

Installer un certificat HTTPS

Installez un certificat signé par une autorité de certification pour un accès sécurisé à la console Web exécutée sur l'agent de console.

À propos de cette tâche

Vous pouvez installer le certificat en utilisant l'une des options suivantes :

- Générez une demande de signature de certificat (CSR) à partir de la console, soumettez la demande de certificat à une autorité de certification, puis installez le certificat signé par l'autorité de certification sur l'agent de la console.

  La paire de clés utilisée par la console pour générer le CSR est stockée en interne sur l'agent de la console. La console récupère automatiquement la même paire de clés (clé privée) lorsque vous installez le certificat sur l'agent de la console.

- Installez un certificat signé par une autorité de certification que vous possédez déjà.

  Avec cette option, le CSR n'est pas généré via la console. Vous générez le CSR séparément et stockez la clé privée en externe. Vous fournissez la clé privée à la console lorsque vous installez le certificat.

Étapes

1. Sélectionnez **Administration > Agents**.
2. Sur la page **Aperçu**, sélectionnez le menu d'action pour un agent de console et sélectionnez **Configuration HTTPS**.

   L'agent Console doit être connecté pour pouvoir le modifier.

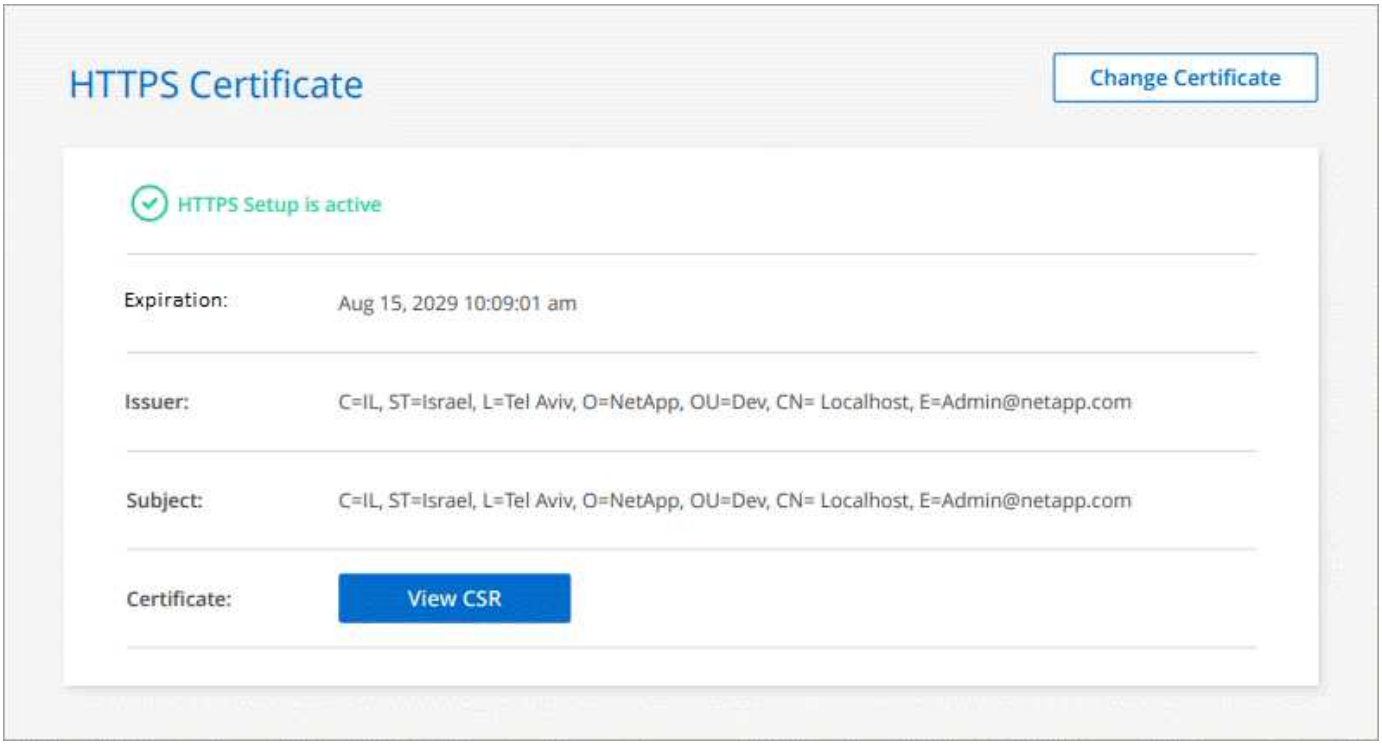
3. Dans la page de configuration HTTPS, installez un certificat en générant une demande de signature de certificat (CSR) ou en installant votre propre certificat signé par une autorité de certification :

Option	Description
Générer un CSR	a. Saisissez le nom d'hôte ou le DNS de l'hôte de l'agent de console (son nom commun), puis sélectionnez **Générer la CSR**. La console affiche une demande de signature de certificat. b. Utilisez le CSR pour soumettre une demande de certificat SSL à une autorité de certification. Le certificat doit utiliser le format X.509 codé en base 64 (Privacy Enhanced Mail) PEM. c. Téléchargez le fichier de certificat, puis sélectionnez **Installer**.

Option	Description
Installez votre propre certificat signé par une autorité de certification	a. Sélectionnez **Installer le certificat signé par une autorité de certification**. b. Chargez à la fois le fichier de certificat et la clé privée, puis sélectionnez **Installer**. Le certificat doit utiliser le format X.509 codé en base 64 (Privacy Enhanced Mail) PEM.

Résultat

L'agent de console utilise désormais le certificat signé par une autorité de certification pour fournir un accès HTTPS sécurisé. L'image suivante montre un agent configuré pour un accès sécurisé :



Renouveler le certificat HTTPS de la console

Vous devez renouveler le certificat HTTPS de l'agent avant son expiration pour garantir un accès sécurisé. Si vous ne renouvelez pas le certificat avant son expiration, un avertissement apparaît lorsque les utilisateurs accèdent à la console Web via HTTPS.

Étapes

1. Sélectionnez **Administration > Agents**.
2. Sur la page **Aperçu**, sélectionnez le menu d'action pour un agent de console et sélectionnez **Configuration HTTPS**.

   Les détails sur le certificat s'affichent, y compris la date d'expiration.

3. Sélectionnez **Modifier le certificat** et suivez les étapes pour générer un CSR ou installer votre propre certificat signé par une autorité de certification.

Configurer un agent de console pour utiliser un serveur proxy

Si vos politiques d'entreprise exigent que vous utilisiez un serveur proxy pour toutes les communications vers Internet, vous devez configurer vos agents pour qu'ils utilisent ce serveur proxy. Si vous n'avez pas configuré un agent de console pour utiliser un serveur proxy lors de l'installation, vous pouvez configurer l'agent de console pour utiliser ce serveur proxy à tout moment.

Le serveur proxy de l'agent permet l'accès Internet sortant sans IP publique ni passerelle NAT. Le serveur proxy fournit une connectivité sortante uniquement pour l'agent de console, et non pour les systèmes Cloud Volumes ONTAP .

Si les systèmes Cloud Volumes ONTAP ne disposent pas d'un accès Internet sortant, la console les configure pour utiliser le serveur proxy de l'agent de la console. Vous devez vous assurer que le groupe de sécurité de l'agent de console autorise les connexions entrantes sur le port 3128. Ouvrez ce port après avoir déployé l'agent de console.

Si l'agent de console lui-même ne dispose pas d'une connexion Internet sortante, les systèmes Cloud Volumes ONTAP ne peuvent pas utiliser le serveur proxy configuré.

Configurations prises en charge

- Les serveurs proxy transparents sont pris en charge pour les agents qui servent les systèmes Cloud Volumes ONTAP . Si vous utilisez les services de données NetApp avec Cloud Volumes ONTAP, créez un agent dédié pour Cloud Volumes ONTAP où vous pouvez utiliser un serveur proxy transparent.
- Les serveurs proxy explicites sont pris en charge avec tous les agents, y compris ceux qui gèrent les systèmes Cloud Volumes ONTAP et ceux qui gèrent les services de données NetApp .
- HTTP et HTTPS.
- Le serveur proxy peut résider dans le cloud ou dans votre réseau.

> Une fois que vous avez configuré un proxy, vous ne pouvez pas modifier le type de proxy. Si vous devez modifier le type de proxy, supprimez l'agent de console et ajoutez un nouvel agent avec le nouveau type de proxy.

Activer un proxy explicite sur un agent de console

Lorsque vous configurez un agent de console pour utiliser un serveur proxy, cet agent et les systèmes Cloud Volumes ONTAP qu'il gère (y compris les médiateurs HA) utilisent tous le serveur proxy.

Cette opération redémarre l'agent de la console. Vérifiez que l'agent de la console est inactif avant de continuer.

Étapes

1. Sélectionnez **Administration > Agents**.
2. Sur la page **Aperçu**, sélectionnez le menu d'action pour un agent de console et sélectionnez **Modifier l'agent**.

   L'agent de la console doit être actif pour pouvoir le modifier.

3. Sélectionnez **Configuration du proxy HTTP**.
4. Sélectionnez **Proxy explicite** dans le champ Type de configuration.

5. Sélectionnez **Activer le proxy**.
6. Spécifiez le serveur en utilisant la syntaxe http://address:port ou https://address:port
7. Spécifiez un nom d'utilisateur et un mot de passe si une authentification de base est requise pour le serveur.

   Notez ce qui suit :

   - L'utilisateur peut être un utilisateur local ou un utilisateur de domaine.
   - Pour un utilisateur de domaine, vous devez saisir le code ASCII du \ comme suit : nom-de-domaine%92nom-d'utilisateur

     Par exemple : netapp%92proxy

   - La console ne prend pas en charge les mots de passe qui incluent le caractère @.
8. Sélectionnez **Enregistrer**.

Activer un proxy transparent pour un agent de console

Seul Cloud Volumes ONTAP prend en charge l'utilisation d'un proxy transparent sur l'agent de la console. Si vous utilisez des services de données NetApp en plus de Cloud Volumes ONTAP, vous devez créer un agent distinct à utiliser pour les services de données ou pour Cloud Volumes ONTAP.

Avant d'activer un proxy transparent, assurez-vous que les exigences suivantes sont remplies :

- L'agent est installé sur le même réseau que le serveur proxy transparent.
- L'inspection TLS est activée sur le serveur proxy.
- Vous disposez d'un certificat au format PEM qui correspond à celui utilisé sur le serveur proxy transparent.
- Vous n'utilisez pas l'agent de console pour d'autres services de données NetApp que Cloud Volumes ONTAP.

Pour configurer un agent existant afin d'utiliser un serveur proxy transparent, utilisez l'outil de maintenance de l'agent de console disponible via la ligne de commande sur l'hôte de l'agent de console.

Lorsque vous configurez un serveur proxy, l'agent de la console redémarre. Vérifiez que l'agent de la console est inactif avant de continuer.

Étapes

Assurez-vous que vous disposez d'un fichier de certificat au format PEM pour le serveur proxy. Si vous ne disposez pas de certificat, contactez votre administrateur réseau pour en obtenir un.

1. Ouvrez une interface de ligne de commande sur l'hôte de l'agent de console.
2. Accédez au répertoire de l'outil de maintenance de l'agent de console : `/opt/application/netapp/service-manager-2/agent-maint-console`
3. Exécutez la commande suivante pour activer le proxy transparent, où `/home/ubuntu/<certificate-file>.pem` est le répertoire et le fichier de certificat de nom que vous avez pour le serveur proxy :

   ```
   ./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
   ```

Assurez-vous que le fichier de certificat est au format PEM et réside dans le même répertoire que la commande ou spécifiez le chemin d'accès complet au fichier de certificat.

```
./agent-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

Modifier le proxy transparent pour l'agent de la console

Vous pouvez mettre à jour le serveur proxy transparent existant d'un agent Console en utilisant le `proxy update` commande ou supprimer le serveur proxy transparent en utilisant la `proxy remove` commande. Pour plus d'informations, consultez la documentation relative à"Console de maintenance des agents" .

> Une fois que vous avez configuré un proxy, vous ne pouvez pas modifier le type de proxy. Si vous devez modifier le type de proxy, supprimez l'agent de console et ajoutez un nouvel agent avec le nouveau type de proxy.

Mettre à jour le proxy de l'agent de console s'il perd l'accès à Internet

Si la configuration proxy de votre réseau change, votre agent risque de perdre l'accès à Internet. Par exemple, si quelqu'un modifie le mot de passe du serveur proxy ou met à jour le certificat. Dans ce cas, vous devrez accéder directement à l'interface utilisateur depuis l'hôte de l'agent de la console et mettre à jour les paramètres. Assurez-vous que vous disposez d'un accès réseau à l'hôte de l'agent de la console et que vous pouvez vous connecter à la console.

Activer le trafic API direct

Si vous avez configuré un agent Console pour utiliser un serveur proxy, vous pouvez activer le trafic API direct sur l'agent Console afin d'envoyer des appels API directement aux services du fournisseur cloud sans passer par le proxy. Les agents exécutés sur AWS, Azure ou Google Cloud prennent en charge cette option.

Si vous désactivez Azure Private Links avec Cloud Volumes ONTAP et utilisez des points de terminaison de service, activez le trafic API direct. Sinon, le trafic ne sera pas acheminé correctement.

"En savoir plus sur l'utilisation d'un lien privé Azure ou de points de terminaison de service avec Cloud Volumes ONTAP"

Étapes

1. Sélectionnez **Administration > Agents**.
2. Sur la page **Aperçu**, sélectionnez le menu d'action pour un agent de console et sélectionnez **Modifier l'agent**.

   L'agent de la console doit être actif pour pouvoir le modifier.

3. Sélectionnez **Prendre en charge le trafic API direct**.
4. Cochez la case pour activer l'option, puis sélectionnez **Enregistrer**.

Dépanner l'agent de la console

Pour résoudre les problèmes avec un agent de console, vous pouvez vérifier les problèmes vous-même ou travailler avec le support NetApp qui peut vous demander votre ID système, la version de l'agent ou les derniers messages AutoSupport .

Si vous disposez d'un compte sur le site de support NetApp , vous pouvez également consulter le"Base de connaissances NetApp ."

Messages d'erreur courants et résolutions

Ce tableau répertorie les messages d'erreur courants et indique comment les corriger :

Message d'erreur	Explication	Ce qu'il faut faire
Impossible de charger l'interface utilisateur de l'agent de la console	L'installation de l'agent a échoué	• Vérifiez que le service Service Manager est actif. • Vérifiez que tous les conteneurs sont en cours d'exécution. • Assurez-vous que votre pare-feu autorise l'accès au service sur le port 8888. • Si vous rencontrez toujours des problèmes, contactez l'assistance.
Impossible d'accéder à l'interface utilisateur de l'agent NetApp	Ce message apparaît lorsque vous essayez d'accéder à l'adresse IP d'un agent. L'agent peut ne pas s'initialiser s'il ne dispose pas de l'accès réseau correct ou s'il est instable.	• Connectez-vous à l'agent de la console. • Vérifiez que le service Service Manager • Vérifiez que l'agent dispose de l'accès réseau dont il a besoin."En savoir plus sur les points de terminaison d'accès réseau requis."
Impossible de charger les paramètres de l'agent	La console affiche ce message lorsque vous essayez d'accéder à la page des paramètres de l'agent.	• Vérifiez si le conteneur OCCM est en cours d'exécution et fonctionne. • Si le problème persiste, contactez le support.
Impossible de charger les informations d'assistance pour l'agent.	Ce message s'affiche si l'agent ne peut pas accéder à votre compte d'assistance.	• Vérifiez que l'agent dispose d'un accès sortant aux points de terminaison requis."En savoir plus sur les points de terminaison d'accès réseau requis."

Vérifiez l'état de l'agent de la console

Utilisez l'une des commandes suivantes pour vérifier votre agent de console. Tous les services doivent avoir le statut *En cours d'exécution*. Si ce n'est pas le cas, contactez le support NetApp .

Pour plus d'informations sur l'accès aux diagnostics de l'agent de la console, consultez les rubriques suivantes :

- "Vérifier l'état de l'agent de la console (pour les déploiements d'hôtes Linux)"
- "Vérifier l'état de l'agent de la console (pour les déploiements VCenter)"

Docker (pour les déploiements Ubuntu et VCenter)

```
docker ps -a
```

Podman (pour les déploiements RedHat Enterprise Linux)

```
podman ps -a
```

Afficher la version de l'agent de la console

Affichez la version de l'agent de la console pour confirmer la mise à niveau ou partagez-la avec votre représentant NetApp .

Étapes

1. Sélectionnez **Administration > Support > Agents**.

   La console affiche la version en haut de la page.

Vérifier l'accès au réseau

Assurez-vous que l'agent de console dispose de l'accès réseau dont il a besoin."En savoir plus sur les points d'accès réseau requis."

Effectuez des vérifications de configuration sur l'agent de la console.

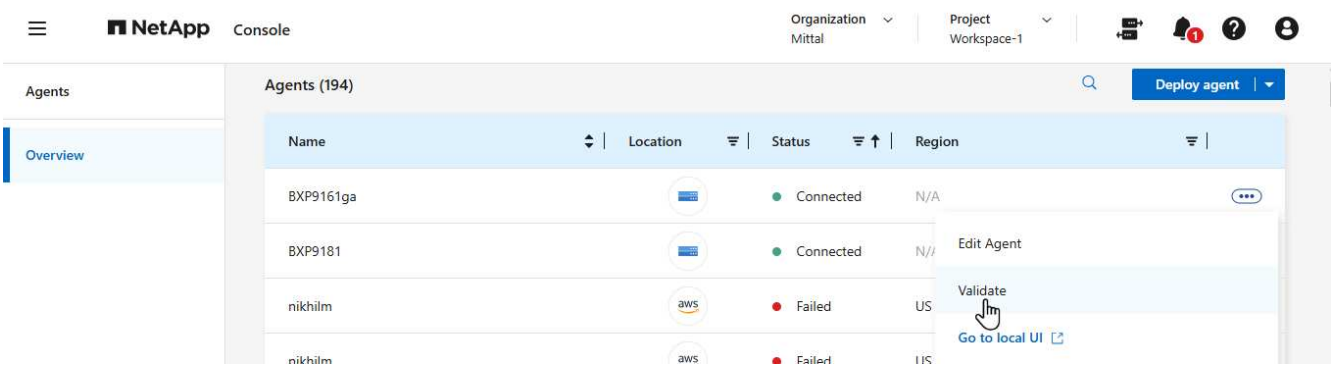
Effectuez des vérifications de configuration sur les agents de la console depuis la console ou la console de maintenance des agents pour vous assurer qu'ils sont connectés.

Vous pouvez également effectuer des vérifications de configuration à l'aide de la console de maintenance de l'agent."Apprenez-en davantage sur l'utilisation de la commande de validation de config-checker."

Vous ne pouvez valider que les agents dont le statut est **Connecté**.

Étapes depuis la console

1. Sélectionnez **Administration > Agents**.
2. Sélectionnez le menu d'actions de l'agent Console que vous souhaitez vérifier et choisissez **Valider**.



La validation peut prendre jusqu'à 15 minutes. Les résultats s'affichent une fois terminé.

Problèmes d'installation de l'agent de console

Si l'installation échoue, consultez le rapport et les journaux pour résoudre les problèmes.

Vous pouvez également accéder au rapport de validation au format JSON et aux journaux de configuration directement depuis l'hôte de l'agent de la console dans les répertoires suivants :

```
/tmp/netapp-console-agents/logs

/tmp/netapp-console-agents/results.json
```

- Pour les nouveaux déploiements d'agents, NetApp vérifie les points de terminaison suivants :"répertorié ici" . Cette vérification de configuration échoue avec une erreur si vous utilisez les points de terminaison précédents utilisés pour les mises à niveau,"répertorié ici" . NetApp recommande de mettre à jour vos règles de pare-feu pour autoriser l'accès aux points de terminaison actuels et bloquer l'accès aux points de terminaison précédents dès que possible."Apprenez à mettre à jour votre réseau" .
- Si vous mettez à jour les points de terminaison de votre pare-feu, vos agents existants continueront de fonctionner.

Désactiver les vérifications de configuration pour les installations manuelles

Il peut arriver que vous ayez besoin de désactiver les contrôles de configuration qui vérifient la connectivité sortante lors de l'installation. Par exemple, lors de l'installation manuelle d'un agent dans votre environnement Government Cloud, vous devez désactiver les vérifications de configuration, sinon l'installation échouera.

Étapes

Vous désactivez la vérification de configuration en définissant l'indicateur *skipConfigCheck* dans le fichier *com/opt/application/netapp/service-manager-2/config.json*. Par défaut, cet indicateur est défini sur faux et la vérification de configuration vérifie l'accès sortant pour l'agent. Définissez cet indicateur sur vrai pour désactiver la vérification. Familiarisez-vous avec la syntaxe JSON avant de passer à l'étape suivante.

Pour réactiver la vérification de configuration, procédez comme suit et définissez l'indicateur *skipConfigCheck* sur false.

Étapes

1. Accédez à l'hôte de l'agent de la console en tant que root ou avec les privilèges sudo.
2. Créez une copie de sauvegarde du fichier */opt/application/netapp/service-manager-2/config.json* pour vous assurer de pouvoir annuler vos modifications.
3. Arrêtez le service Service Manager 2 en exécutant la commande suivante :

```
systemctl stop netapp-service-manager.service
```

1. Modifiez le fichier */opt/application/netapp/service-manager-2/config.json* et remplacez la valeur de l'indicateur *skipConfigCheck* par true.

```
"skipConfigCheck": true
```

2. Enregistrez votre fichier.
3. Redémarrez le service Service Manager 2 en exécutant la commande suivante :

```
systemctl restart netapp-service-manager.service
```

Travailler avec le support NetApp

Si vous n'avez pas pu résoudre les problèmes avec votre agent de console, vous pouvez contacter le support NetApp . Le support NetApp peut vous demander l'ID de l'agent de console ou de lui envoyer les journaux de l'agent de console s'il ne les possède pas déjà.

Rechercher l'ID de l'agent de la console

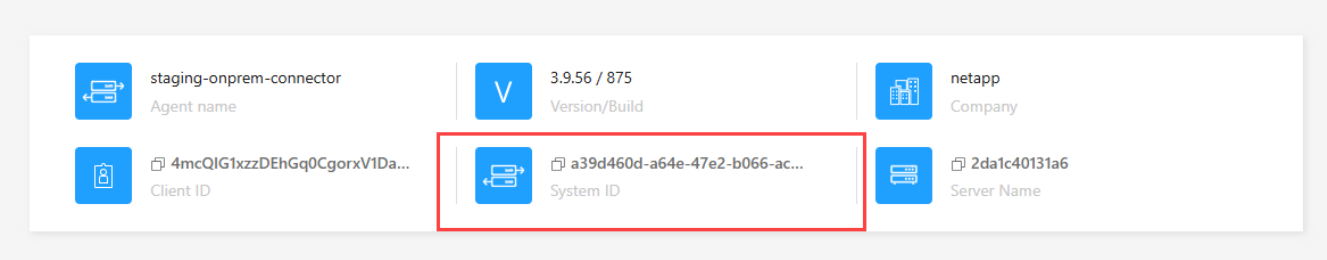
Pour vous aider à démarrer, vous aurez peut-être besoin de l'ID système de votre agent de console. L'ID est généralement utilisé à des fins de licence et de dépannage.

Étapes

1. Sélectionnez **Administration > Support > Agents**.

   Vous pouvez trouver l'ID système en haut de la page.

   Exemple



2. Survolez et cliquez sur l'ID pour le copier.

Téléchargez ou envoyez un message AutoSupport

Si vous rencontrez des problèmes, NetApp peut vous demander d'envoyer un message AutoSupport au support NetApp à des fins de dépannage.

> La NetApp Console prend jusqu'à cinq heures pour envoyer des messages AutoSupport en raison de l'équilibrage de charge. Pour une communication urgente, téléchargez le fichier et envoyez-le manuellement.

Étapes

1. Sélectionnez **Administration > Support > Agents**.
2. Selon la manière dont vous devez envoyer les informations au support NetApp , choisissez l'une des options suivantes :
   a. Sélectionnez l'option permettant de télécharger le message AutoSupport sur votre ordinateur local. Vous pouvez ensuite l'envoyer au support NetApp en utilisant la méthode de votre choix.
   b. Sélectionnez **Envoyer AutoSupport** pour envoyer directement le message au support NetApp .

Corriger les échecs de téléchargement lors de l'utilisation d'une passerelle Google Cloud NAT

L'agent de console télécharge automatiquement les mises à jour logicielles pour Cloud Volumes ONTAP. Votre configuration peut entraîner l'échec du téléchargement si elle utilise une passerelle NAT Google Cloud. Vous pouvez corriger ce problème en limitant le nombre de parties dans lesquelles l'image du logiciel est divisée. Cette étape doit être complétée en utilisant l'API.

Étape

1. Soumettez une requête PUT à /occm/config avec le JSON suivant comme corps :

```
{
  "maxDownloadSessions": 32
}
```

   La valeur de *maxDownloadSessions* peut être 1 ou tout entier supérieur à 1. Si la valeur est 1, l'image téléchargée ne sera pas divisée.

   Notez que 32 est une valeur d'exemple. La valeur dépend de votre configuration NAT et du nombre de sessions simultanées.

"En savoir plus sur l'appel API /occm/config"

Obtenez de l'aide auprès de la base de connaissances NetApp

"Consultez les informations de dépannage créées par l'équipe de support NetApp" .

Désinstaller et supprimer un agent de console

Désinstallez un agent de console pour résoudre les problèmes ou pour le supprimer définitivement de l'hôte. Les étapes à suivre dépendent du mode de déploiement que vous utilisez. Une fois que vous avez supprimé un agent de console de votre environnement, vous pouvez le supprimer de la console.

"En savoir plus sur les modes de déploiement de la NetApp Console" .

Désinstaller l'agent lors de l'utilisation du mode standard ou restreint

Si vous utilisez le mode standard ou le mode restreint (en d'autres termes, l'hôte de l'agent dispose d'une connectivité sortante), vous devez suivre les étapes ci-dessous pour désinstaller l'agent.

Étapes

1. Connectez-vous à la machine virtuelle Linux pour l'agent.
2. Depuis l'hôte Linux, exécutez le script de désinstallation :

```
/opt/application/netapp/service-manager-2/uninstall.sh [silent]
```

   silent exécute le script sans vous demander de confirmation.

Supprimer les agents de la console

Si vous avez supprimé une machine virtuelle d'agent ou désinstallé l'agent, vous devez la retirer de la liste des agents dans la console. Après la suppression d'une machine virtuelle d'agent ou la désinstallation du logiciel d'agent, l'agent affiche l'état **Déconnecté** dans la console.

Notez les points suivants concernant la suppression d'un agent de console :

- Cette action ne supprime pas la machine virtuelle.
- Cette action ne peut pas être annulée : une fois que vous avez supprimé un agent de console, vous ne pouvez pas le rajouter.

Étapes

1. Sélectionnez **Administration > Agents**.
2. Sur la page **Aperçu**, sélectionnez le menu d'actions d'un agent déconnecté et sélectionnez **Supprimer l'agent**.
3. Saisissez le nom de l'agent pour confirmer, puis sélectionnez **Supprimer**.

Gérer les identifiants du fournisseur de cloud

AWS

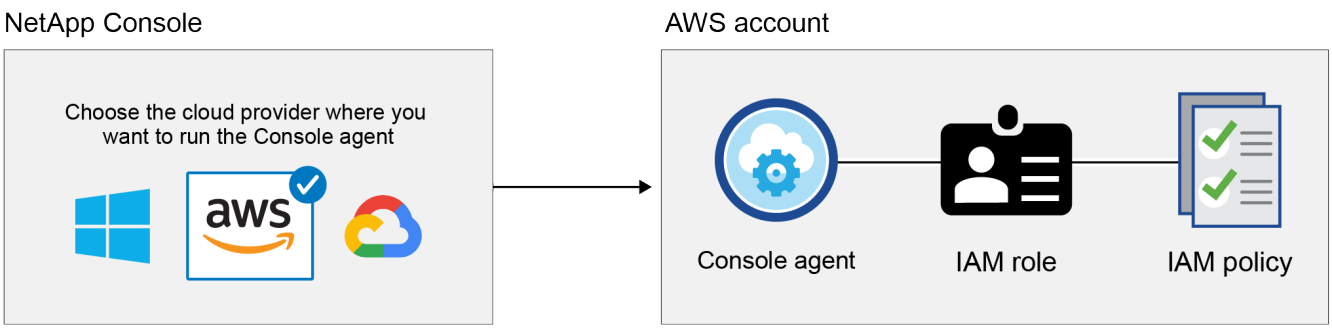
En savoir plus sur les informations d'identification et les autorisations AWS dans la NetApp Console

Vous gérez les informations d'identification AWS et les abonnements Marketplace directement depuis la NetApp Console pour garantir le déploiement sécurisé de Cloud Volumes ONTAP et d'autres services de données en fournissant les informations d'identification IAM appropriées lors du déploiement de l'agent de la console et en les associant aux abonnements AWS Marketplace pour la facturation.

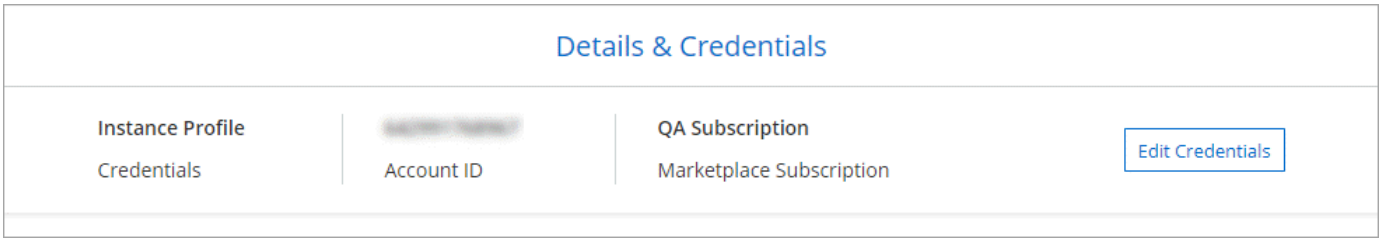
Informations d'identification AWS initiales

Lorsque vous déployez un agent de console à partir de la console, vous devez fournir l'ARN d'un rôle IAM ou des clés d'accès pour un utilisateur IAM. La méthode d'authentification doit disposer des autorisations nécessaires pour déployer l'agent Console dans AWS. Les autorisations requises sont listées dans le"Politique de déploiement d'agents pour AWS" .

Lorsque la console lance l'agent de console dans AWS, elle crée un rôle IAM et un profil pour l'agent. Il attache également une politique qui fournit à l'agent de la console des autorisations pour gérer les ressources et les processus au sein de ce compte AWS. "Vérifiez comment l'agent utilise les autorisations".



Si vous ajoutez un nouveau système Cloud Volumes ONTAP , la console sélectionne ces informations d'identification AWS par défaut :



Déployez tous vos systèmes Cloud Volumes ONTAP à l'aide des informations d'identification AWS initiales ou vous pouvez ajouter des informations d'identification supplémentaires.

Informations d'identification AWS supplémentaires

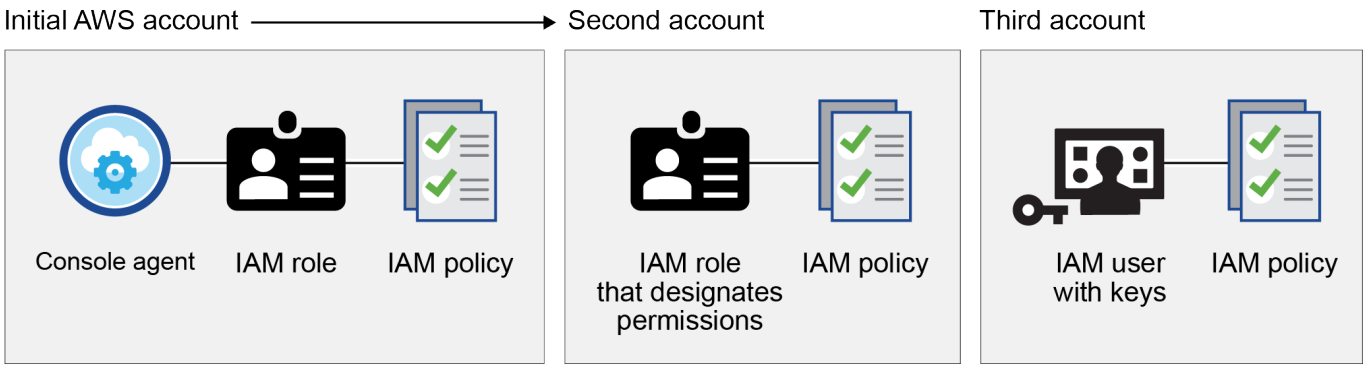
Vous pouvez ajouter des informations d'identification AWS supplémentaires à la console dans les cas suivants :

- Pour utiliser votre agent Console existant avec un compte AWS supplémentaire
- Pour créer un nouvel agent dans un compte AWS spécifique
- Pour créer et gérer les systèmes de fichiers FSx pour ONTAP

Consultez les sections ci-dessous pour plus de détails.

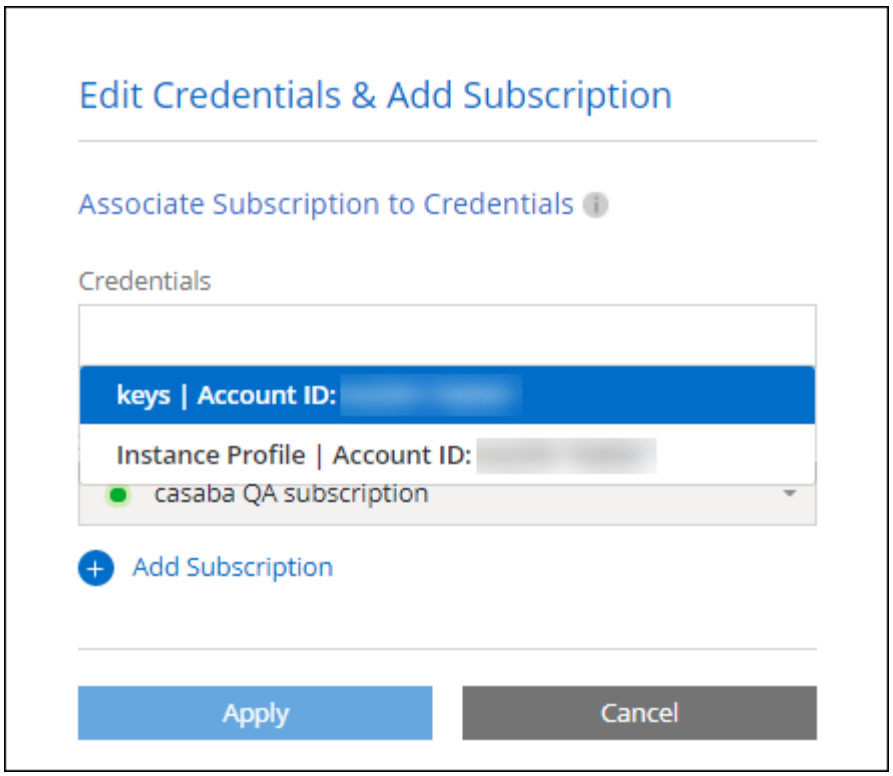
Ajoutez des informations d'identification AWS pour utiliser un agent de console avec un autre compte AWS

Pour utiliser la console avec des comptes AWS supplémentaires, fournissez des clés AWS ou l'ARN d'un rôle dans un compte de confiance. L'image suivante montre deux comptes supplémentaires, l'un fournissant des autorisations via un rôle IAM dans un compte approuvé et l'autre via les clés AWS d'un utilisateur IAM :



Vous ajoutez les informations d'identification du compte à la console en spécifiant le nom de ressource Amazon (ARN) du rôle IAM ou les clés AWS de l'utilisateur IAM.

Par exemple, vous pouvez basculer entre les informations d'identification lors de la création d'un nouveau système Cloud Volumes ONTAP :



"Découvrez comment ajouter des informations d'identification AWS à un agent existant."

Ajoutez les informations d'identification AWS pour créer un agent de console

L'ajout des identifiants AWS permet de créer un agent de console.

"Découvrez comment ajouter des informations d'identification AWS à la console pour créer un agent de console"

Ajouter les informations d'identification AWS pour FSx pour ONTAP

Ajoutez les informations d'identification AWS à la console pour fournir les autorisations nécessaires à la création et à la gestion d'un système FSx pour ONTAP .

"Découvrez comment ajouter des informations d'identification AWS à la console pour Amazon FSx for ONTAP"

Informations d'identification et abonnements à la place de marché

Vous devez associer les informations d'identification que vous ajoutez à un agent de console à un abonnement AWS Marketplace pour payer Cloud Volumes ONTAP à un tarif horaire (PAYGO) et d'autres services de données NetApp ou par le biais d'un contrat annuel. "Découvrez comment associer un abonnement AWS".

Notez les points suivants concernant les informations d'identification AWS et les abonnements à la place de marché :

- Vous ne pouvez associer qu'un seul abonnement AWS Marketplace à un ensemble d'informations d'identification AWS
- Vous pouvez remplacer un abonnement de marché existant par un nouvel abonnement

FAQ

Les questions suivantes concernent les informations d'identification et les abonnements.

Comment puis-je faire pivoter mes informations d'identification AWS en toute sécurité ?

Comme décrit dans les sections ci-dessus, la console vous permet de fournir des informations d'identification AWS de plusieurs manières : un rôle IAM associé à l'agent de la console, en assumant un rôle IAM dans un compte approuvé ou en fournissant des clés d'accès AWS.

Avec les deux premières options, la console utilise le service AWS Security Token pour obtenir des informations d'identification temporaires qui changent constamment. Ce processus représente la meilleure pratique : il est automatique et sécurisé.

Si vous fournissez à la console des clés d'accès AWS, vous devez faire tourner les clés en les mettant à jour dans la console à intervalles réguliers. Il s'agit d'un processus entièrement manuel.

Puis-je modifier l'abonnement AWS Marketplace pour les systèmes Cloud Volumes ONTAP ?

Oui, tu peux. Lorsque vous modifiez l'abonnement AWS Marketplace associé à un ensemble d'informations d'identification, tous les systèmes Cloud Volumes ONTAP existants et nouveaux sont facturés sur le nouvel abonnement.

"Découvrez comment associer un abonnement AWS" .

Puis-je ajouter plusieurs informations d'identification AWS, chacune avec des abonnements de marché différents ?

Toutes les informations d'identification AWS appartenant au même compte AWS seront associées au même abonnement AWS Marketplace.

Si vous disposez de plusieurs informations d'identification AWS appartenant à différents comptes AWS, ces informations d'identification peuvent être associées au même abonnement AWS Marketplace ou à des abonnements différents.

Puis-je déplacer des systèmes Cloud Volumes ONTAP existants vers un autre compte AWS ?

Non, il n'est pas possible de déplacer les ressources AWS associées à votre système Cloud Volumes ONTAP vers un autre compte AWS.

Comment fonctionnent les informations d'identification pour les déploiements sur le marché et les déploiements sur site ?

Les sections ci-dessus décrivent la méthode de déploiement recommandée pour l'agent de console, qui provient de la console. Vous pouvez également déployer un agent sur AWS depuis AWS Marketplace et installer manuellement le logiciel agent Console sur votre propre hôte Linux ou dans votre vCenter.

Si vous utilisez la Marketplace, les autorisations sont fournies de la même manière. Il vous suffit de créer et de configurer manuellement le rôle IAM, puis de fournir des autorisations pour tous les comptes supplémentaires.

Pour les déploiements sur site, vous ne pouvez pas configurer de rôle IAM pour la console, mais vous pouvez fournir des autorisations à l'aide de clés d'accès AWS.

Pour savoir comment configurer les autorisations, reportez-vous aux pages suivantes :

- Mode standard
  - "Configurer les autorisations pour un déploiement AWS Marketplace"
  - "Configurer les autorisations pour les déploiements sur site"
- Mode restreint
  - "Configurer les autorisations pour le mode restreint"

Gérer les informations d'identification AWS et les abonnements au marché pour NetApp Console

Ajoutez et gérez les informations d'identification AWS afin de déployer et de gérer les ressources cloud dans vos comptes AWS à partir de la NetApp Console. Si vous gérez plusieurs abonnements AWS Marketplace, vous pouvez attribuer chacun d'eux à différentes informations d'identification AWS à partir de la page Informations d'identification.

Aperçu

Vous pouvez ajouter des informations d'identification AWS à un agent de console existant ou directement à la console :

- Ajouter des informations d'identification AWS supplémentaires à un agent existant

  Ajoutez les informations d'identification AWS à un agent de console pour gérer les ressources cloud. Découvrez comment ajouter des informations d'identification AWS à un agent de console .

- Ajoutez les informations d'identification AWS à la console pour créer un agent de console

  L'ajout de nouvelles informations d'identification AWS à la console fournit les autorisations nécessaires pour créer un agent de console. Découvrez comment ajouter des informations d'identification AWS à la NetApp Console .

- Ajouter les informations d'identification AWS à la console pour FSx pour ONTAP

  Ajoutez de nouvelles informations d'identification AWS à la console pour créer et gérer FSx pour ONTAP. "Découvrez comment configurer les autorisations pour FSx pour ONTAP"

Comment faire tourner les informations d'identification

La NetApp Console vous permet de fournir des informations d'identification AWS de plusieurs manières : un rôle IAM associé à l'instance de l'agent, en assumant un rôle IAM dans un compte approuvé ou en fournissant des clés d'accès AWS. "En savoir plus sur les informations d'identification et les autorisations AWS" .

Avec les deux premières options, la console utilise le service AWS Security Token pour obtenir des informations d'identification temporaires qui changent constamment. Ce processus est la meilleure pratique car il est automatique et sécurisé.

Faites pivoter manuellement les clés d'accès AWS en les mettant à jour dans la console.

Ajouter des informations d'identification supplémentaires à un agent de console

Ajoutez des informations d'identification AWS supplémentaires à un agent de console afin qu'il dispose des autorisations nécessaires pour gérer les ressources et les processus au sein de votre environnement de cloud

public. Vous pouvez soit fournir l'ARN d'un rôle IAM dans un autre compte, soit fournir des clés d'accès AWS.

"Découvrez comment la NetApp Console utilise les informations d'identification et les autorisations AWS".

Accorder des autorisations

Accordez des autorisations avant d'ajouter des informations d'identification AWS à un agent de console. Les autorisations permettent à un agent de console de gérer les ressources et les processus au sein de ce compte AWS. Vous pouvez fournir les autorisations avec l'ARN d'un rôle dans un compte approuvé ou des clés AWS.

Si vous avez déployé un agent de console à partir de la console, les informations d'identification AWS pour le compte dans lequel vous avez déployé un agent de console ont été automatiquement ajoutées. Cela garantit que les autorisations nécessaires sont en place pour la gestion des ressources.

Choix

- Accorder des autorisations en assumant un rôle IAM dans un autre compte
- Accorder des autorisations en fournissant des clés AWS

Accorder des autorisations en assumant un rôle IAM dans un autre compte

Vous pouvez configurer une relation d'approbation entre le compte AWS source dans lequel vous avez déployé un agent de console et d'autres comptes AWS à l'aide de rôles IAM. Vous devez ensuite fournir à la console l'ARN des rôles IAM à partir des comptes approuvés.

Si un agent de console est installé sur site, vous ne pouvez pas utiliser cette méthode d'authentification. Vous devez utiliser des clés AWS.

Étapes

1. Accédez à la console IAM du compte cible dans lequel vous souhaitez fournir des autorisations à un agent de console.
2. Sous Gestion des accès, sélectionnez **Rôles > Créer un rôle** et suivez les étapes pour créer le rôle.

   Assurez-vous de faire ce qui suit :

   - Sous **Type d'entité approuvée**, sélectionnez **Compte AWS**.
   - Sélectionnez **Un autre compte AWS** et saisissez l'ID du compte sur lequel réside une instance d'agent de console.
   - Créez les politiques requises en copiant et en collant le contenu de"les politiques IAM pour un agent de console" .
3. Copiez l'ARN du rôle IAM afin de pouvoir le coller ultérieurement dans la console.

Résultat

Le compte dispose des autorisations requises. Vous pouvez désormais ajouter les informations d'identification à un agent de console .

Accorder des autorisations en fournissant des clés AWS

Si vous souhaitez fournir à la console des clés AWS pour un utilisateur IAM, vous devez accorder les autorisations requises à cet utilisateur. La politique IAM de la console définit les actions et ressources AWS que la console est autorisée à utiliser.

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

Étapes

1. Depuis la console IAM, créez des politiques en copiant et en collant le contenu de"les politiques IAM pour un agent de console" .

   "Documentation AWS : Création de politiques IAM"

2. Attachez les politiques à un rôle IAM ou à un utilisateur IAM.
   - "Documentation AWS : Création de rôles IAM"
   - "Documentation AWS : Ajout et suppression de stratégies IAM"

Ajouter les informations d'identification à un agent existant

Après avoir fourni à un compte AWS les autorisations requises, vous pouvez ajouter les informations d'identification de ce compte à un agent existant. Cela vous permet de lancer des systèmes Cloud Volumes ONTAP dans ce compte à l'aide du même agent.

Les nouvelles informations d'identification de votre fournisseur de cloud peuvent prendre quelques minutes pour être disponibles.

Étapes

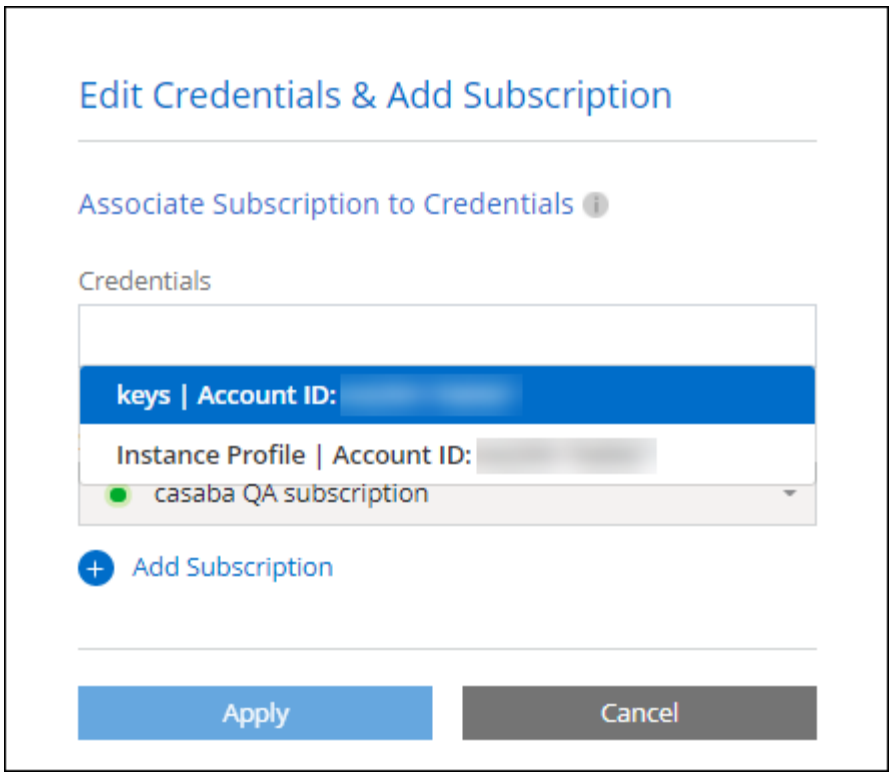
1. Utilisez la barre de navigation supérieure pour sélectionner un agent de console auquel vous souhaitez ajouter des informations d'identification.
2. Dans la barre de navigation de gauche, sélectionnez **Administration > Informations d'identification**.
3. Sur la page **Informations d'identification de l'organisation**, 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** : fournissez l'ARN (Amazon Resource Name) d'un rôle IAM approuvé ou 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.

      Pour payer les services à un tarif horaire (PAYGO) ou avec un contrat annuel, vous devez associer les informations d'identification AWS à votre abonnement AWS Marketplace.

   d. **Révision** : Confirmez les détails des nouvelles informations d'identification et sélectionnez **Ajouter**.

Résultat

Vous pouvez désormais passer à un autre ensemble d'informations d'identification à partir de la page Détails et informations d'identification lors de l'ajout d'un abonnement à la console.



Ajoutez des informations d'identification à la console pour créer un agent de console

Ajoutez les informations d'identification AWS en fournissant l'ARN d'un rôle IAM qui donne les autorisations nécessaires pour créer un agent de console. Vous pouvez choisir ces informations d'identification lors de la création d'un nouvel agent.

Configurer le rôle IAM

Configurez un rôle IAM qui permet à la couche logicielle en tant que service (SaaS) de la NetApp Console d'assumer le rôle.

Étapes

1. Accédez à la console IAM dans le compte cible.
2. Sous Gestion des accès, sélectionnez **Rôles > Créer un rôle** et suivez les étapes pour créer le rôle.

   Assurez-vous de faire ce qui suit :

   - Sous **Type d'entité approuvée**, sélectionnez **Compte AWS**.
   - Sélectionnez **Un autre compte AWS** et saisissez l'ID de la NetApp Console SaaS : 952013314444
   - Pour Amazon FSx for NetApp ONTAP en particulier, modifiez la politique **Relations de confiance** pour inclure « AWS » : « arn:aws:iam::952013314444:root ».

     Par exemple, la politique devrait ressembler à ceci :

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

+
Se référer à "Documentation AWS Identity and Access Management (IAM)" pour plus d'informations sur l'accès aux ressources inter-comptes dans IAM.

- Créez une politique qui inclut les autorisations requises pour créer un agent de console.
  - "Afficher les autorisations nécessaires pour FSx pour ONTAP"
  - "Afficher la politique de déploiement de l'agent"

3. Copiez l'ARN du rôle IAM afin de pouvoir le coller dans la console à l'étape suivante.

Résultat

Le rôle IAM dispose désormais des autorisations requises. Vous pouvez maintenant l'ajouter à la console.

Ajoutez les informations d'identification

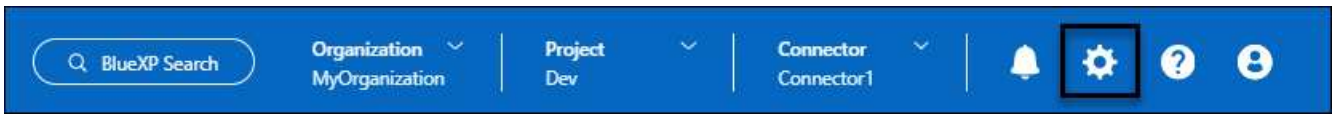
Après avoir fourni au rôle IAM les autorisations requises, ajoutez l'ARN du rôle à la console.

Avant de commencer

Si vous venez de créer le rôle IAM, il faudra peut-être quelques minutes avant qu'il soit disponible pour utilisation. Attendez quelques minutes avant d'ajouter les informations d'identification à la console.

Étapes

1. Sélectionnez **Administration > Informations d'identification**.



2. Sur la page **Informations d'identification de l'organisation**, sélectionnez **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
   a. **Emplacement des informations d'identification** : sélectionnez **Amazon Web Services > Console**.
   b. **Définir les informations d'identification** : indiquez l'ARN (Amazon Resource Name) du rôle IAM.
   c. **Révision** : Confirmez les détails des nouvelles informations d'identification et sélectionnez **Ajouter**.

Ajouter des informations d'identification à la console pour Amazon FSx for ONTAP

Pour plus de détails, reportez-vous à la "la documentation de la console pour Amazon FSx pour ONTAP"

Configurer un abonnement AWS

Après avoir ajouté vos informations d'identification AWS, vous pouvez configurer un abonnement AWS Marketplace avec ces informations d'identification. L'abonnement vous permet de payer les services de données NetApp et Cloud Volumes ONTAP à un tarif horaire (PAYGO) ou via un contrat annuel.

Il existe deux scénarios dans lesquels vous pouvez configurer un abonnement AWS Marketplace après avoir ajouté les informations d'identification :

- Vous n'avez pas configuré d'abonnement lorsque vous avez initialement ajouté les informations d'identification.
- Vous souhaitez modifier l'abonnement AWS Marketplace configuré avec les informations d'identification AWS.

  Le remplacement de l'abonnement actuel au marché par un nouvel abonnement modifie l'abonnement au marché pour tous les systèmes Cloud Volumes ONTAP existants et tous les nouveaux systèmes.

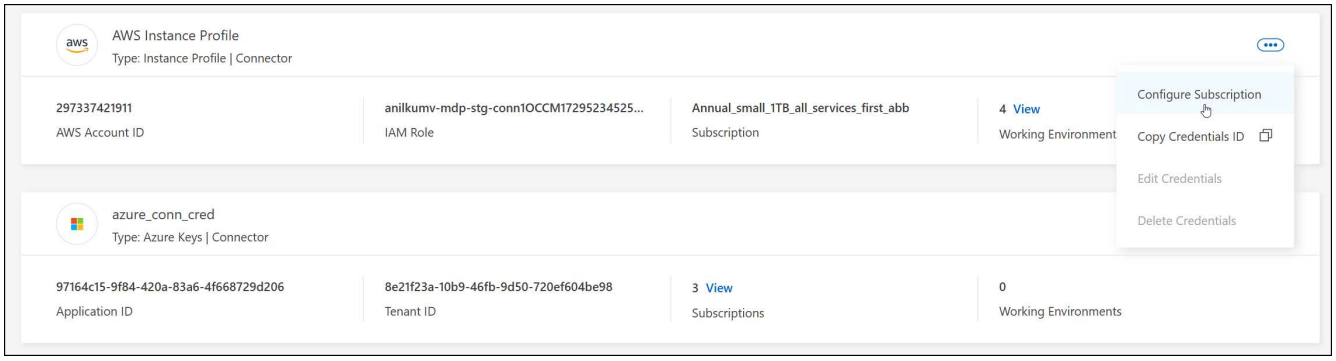
Avant de commencer

Vous devez créer un agent de console avant de pouvoir configurer un abonnement. "Apprenez à créer un agent de console" .

Étapes

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

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



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

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

b. Sélectionnez **S'abonner**.

c. Sélectionnez **Configurer votre compte**.

Vous serez redirigé vers la NetApp Console.

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

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

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

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

◦ Sélectionnez **Enregistrer**.

Associer un abonnement existant à votre organisation

Lorsque vous vous abonnez à partir d'AWS Marketplace, la dernière étape du processus consiste à associer l'abonnement à votre organisation. Si vous n'avez pas effectué cette étape, vous ne pourrez pas utiliser l'abonnement avec votre organisation.

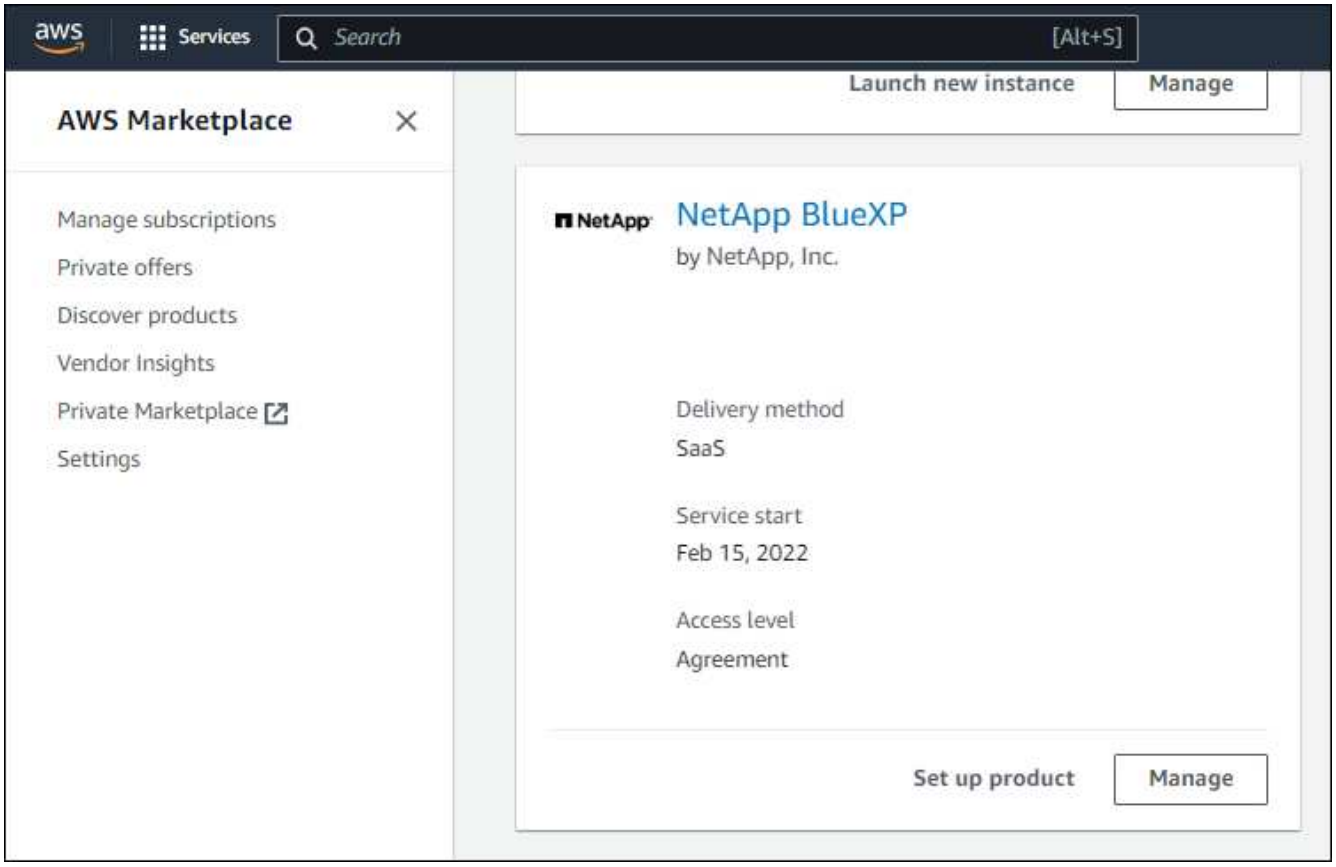
- "En savoir plus sur les modes de déploiement de la console"
- "En savoir plus sur la gestion des identités et des accès à la console"

Suivez les étapes ci-dessous si vous vous êtes abonné à NetApp Intelligent Services depuis AWS Marketplace, mais que vous avez manqué l'étape permettant d'associer l'abonnement à votre compte.

Étapes

1. Confirmez que vous n'avez pas associé votre abonnement à votre organisation Console.
   a. Dans le menu de navigation, sélectionnez **Administration > Licenses and subscriptions**.
   b. Sélectionnez **Abonnements**.
   c. Vérifiez que votre abonnement n'apparaît pas.

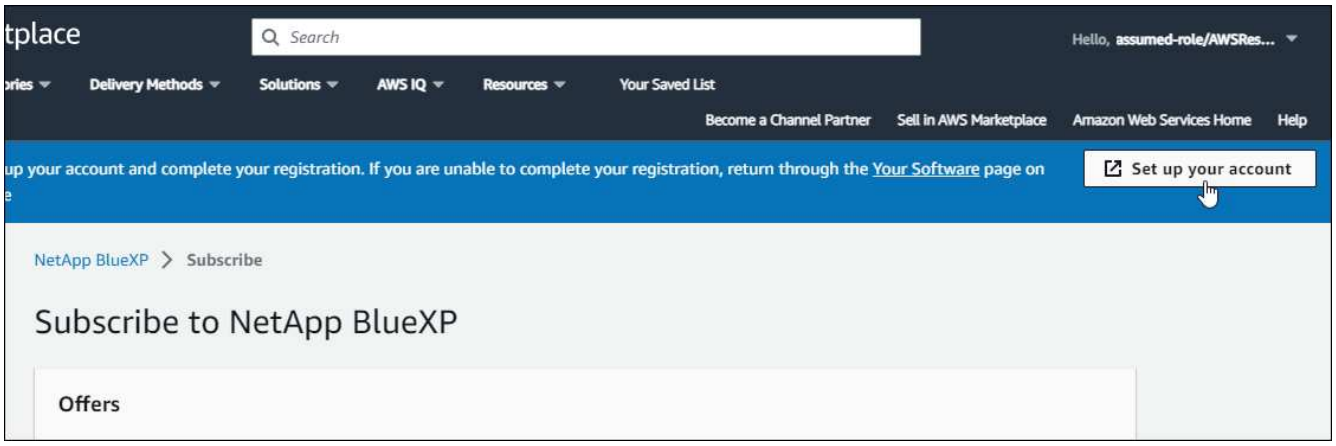
   Vous ne verrez que les abonnements associés à l'organisation ou au compte que vous consultez actuellement. Si vous ne voyez pas votre abonnement, procédez aux étapes suivantes.
2. Connectez-vous à la console AWS et accédez à **Abonnements AWS Marketplace**.
3. Trouver l'abonnement.



4. Sélectionnez **Configurer le produit**.

   La page de l'offre d'abonnement doit se charger dans un nouvel onglet ou une nouvelle fenêtre du navigateur.

5. Sélectionnez **Configurer votre compte**.



   La page **Affectation d'abonnement** sur netapp.com doit se charger dans un nouvel onglet ou une nouvelle fenêtre de navigateur.

   Notez que vous serez peut-être invité à vous connecter d'abord à la console.

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

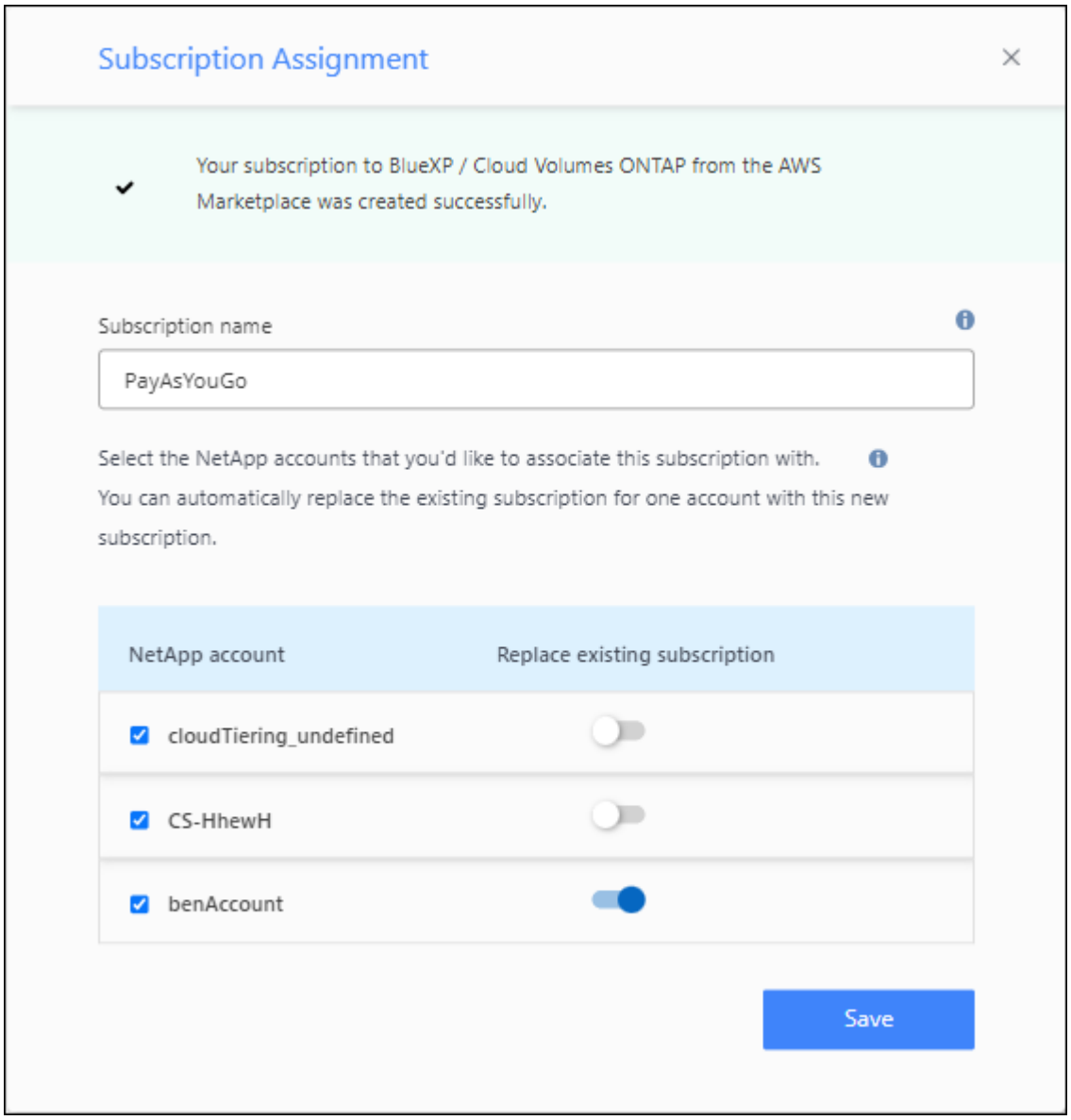
   - Sélectionnez les organisations ou les comptes de la console auxquels vous souhaitez associer cet

abonnement.

- Dans le champ **Remplacer l'abonnement existant**, choisissez si vous souhaitez remplacer automatiquement l'abonnement existant pour une organisation ou un compte par ce nouvel abonnement.

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

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



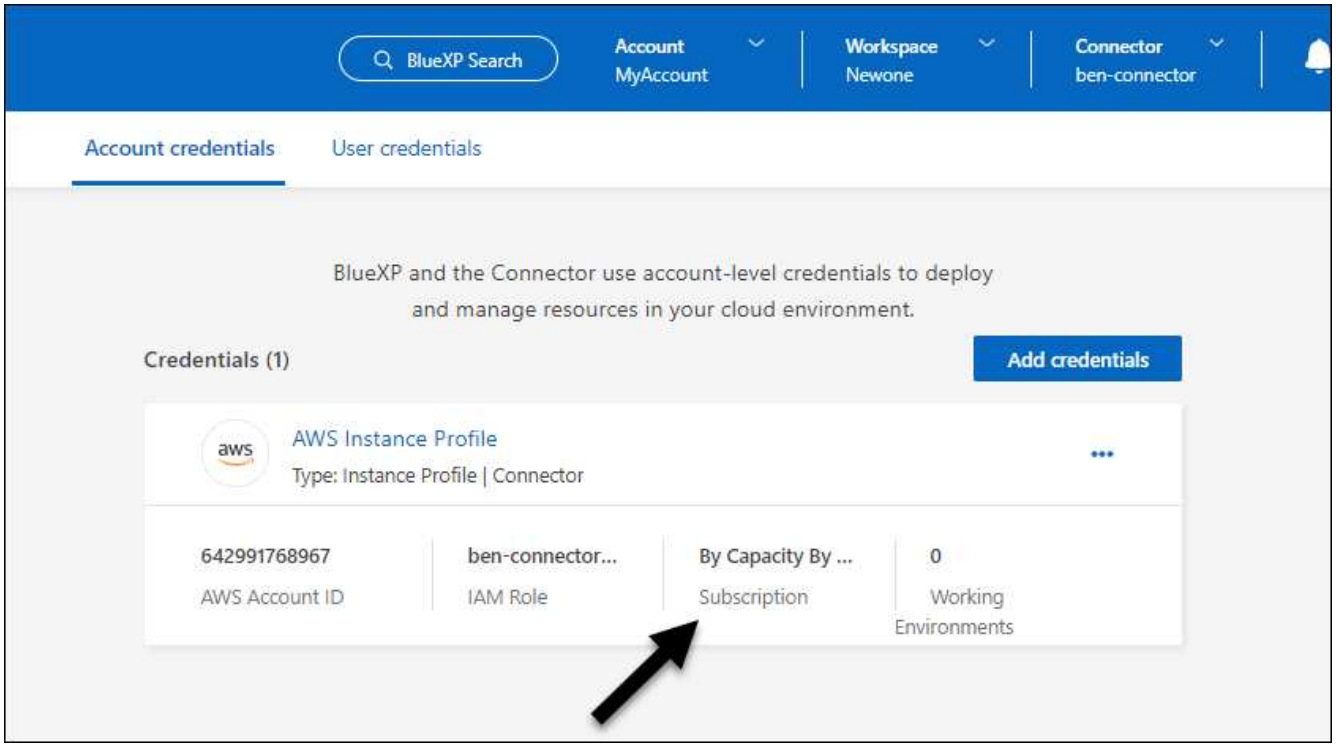
7. Confirmez que l'abonnement est associé à votre organisation.
   a. Dans le menu de navigation, sélectionnez **Administration > Licences et abonnements**.
   b. Sélectionnez **Abonnements**.
   c. Vérifiez que votre abonnement apparaît.

8. Confirmez que l'abonnement est associé à vos informations d'identification AWS.

   a. Sélectionnez **Administration > Informations d'identification**.

   b. Sur la page **Informations d'identification de l'organisation**, vérifiez que l'abonnement est associé à vos informations d'identification AWS.

      Voici un exemple.



Modifier les informations d'identification

Modifiez vos informations d'identification AWS en modifiant le type de compte (clés AWS ou rôle d'assumé), en modifiant le nom ou en mettant à jour les informations d'identification elles-mêmes (les clés ou l'ARN du rôle).

> Vous ne pouvez pas modifier les informations d'identification d'un profil d'instance associé à une instance d'agent de console ou à une instance Amazon FSx for ONTAP . Vous ne pouvez renommer les informations d'identification que pour une instance FSx for ONTAP .

Étapes

1. Sélectionnez **Administration > Informations d'identification**.
2. Sur la page **Informations d'identification de l'organisation**, sélectionnez le menu d'action pour un ensemble d'informations d'identification, puis sélectionnez **Modifier les informations d'identification**.
3. Apportez les modifications requises, puis sélectionnez **Appliquer**.

Supprimer les informations d'identification

Si vous n'avez plus besoin d'un ensemble d'informations d'identification, vous pouvez les supprimer. Vous ne pouvez supprimer que les informations d'identification qui ne sont pas associées à un système.

Vous ne pouvez pas supprimer les informations d'identification d'un profil d'instance associé à un agent de console.

Étapes

1. Sélectionnez **Administration > Informations d'identification**.
2. Sur la page **Informations d'identification de l'organisation** ou **Informations d'identification du compte**, sélectionnez le menu d'action pour un ensemble d'informations d'identification, puis sélectionnez **Supprimer les informations d'identification**.
3. Sélectionnez **Supprimer** pour confirmer.

Azuré

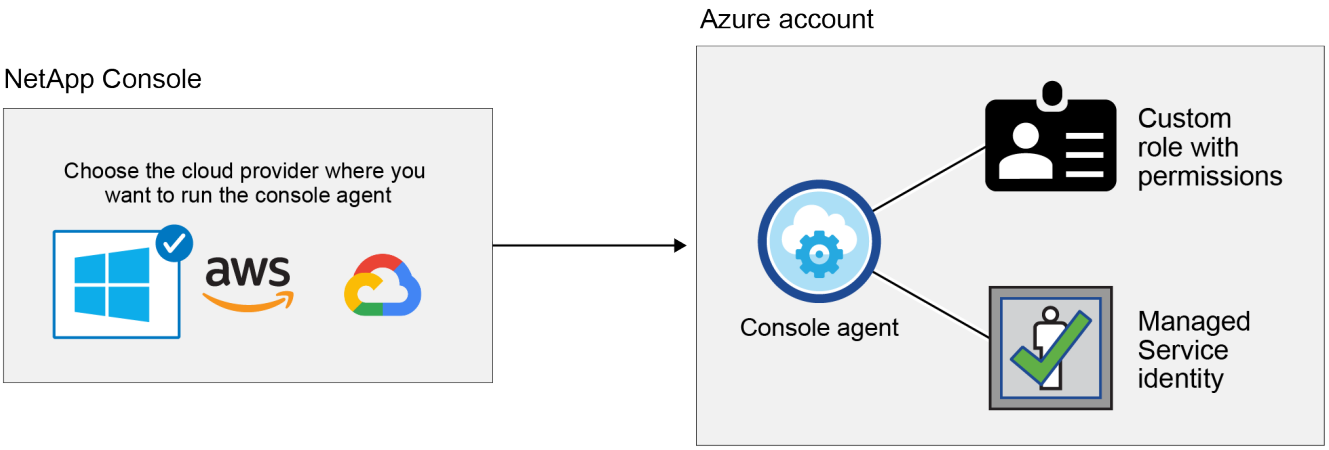
En savoir plus sur les informations d'identification et les autorisations Azure dans la NetApp Console

Découvrez comment la NetApp Console utilise les informations d'identification Azure pour effectuer des actions en votre nom et comment ces informations d'identification sont associées aux abonnements de la place de marché. Comprendre ces détails peut être utile lorsque vous gérez les informations d'identification d'un ou plusieurs abonnements Azure. Par exemple, vous souhaiterez peut-être savoir quand ajouter des informations d'identification Azure supplémentaires à la console.

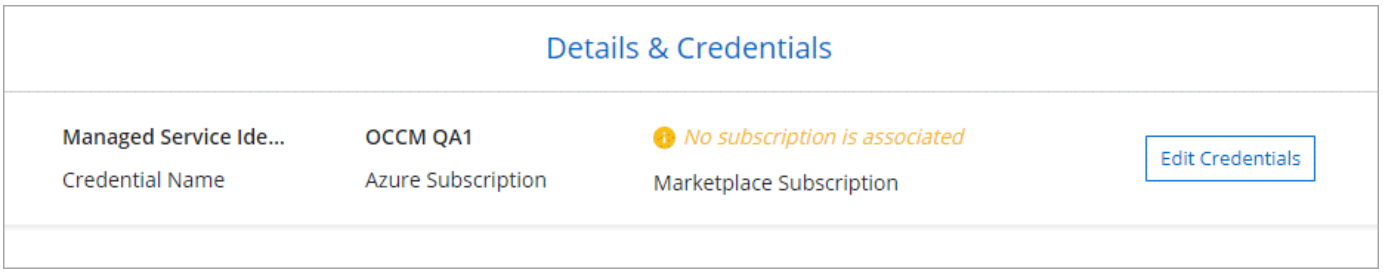
Informations d'identification Azure initiales

Lorsque vous déployez un agent de console à partir de la console, vous devez utiliser un compte Azure ou un principal de service disposant des autorisations nécessaires pour déployer la machine virtuelle de l'agent de console. Les autorisations requises sont répertoriées dans le"Politique de déploiement d'agent pour Azure" .

Lorsque la console déploie la machine virtuelle de l'agent de console dans Azure, elle active un "identité gérée attribuée par le système" sur la machine virtuelle, crée un rôle personnalisé et l'attribue à la machine virtuelle. Le rôle fournit à la console les autorisations requises pour gérer les ressources et les processus au sein de cet abonnement Azure. "Examiner comment la console utilise les autorisations" .



Si vous créez un nouveau système pour Cloud Volumes ONTAP, la console sélectionne ces informations d'identification Azure par défaut :



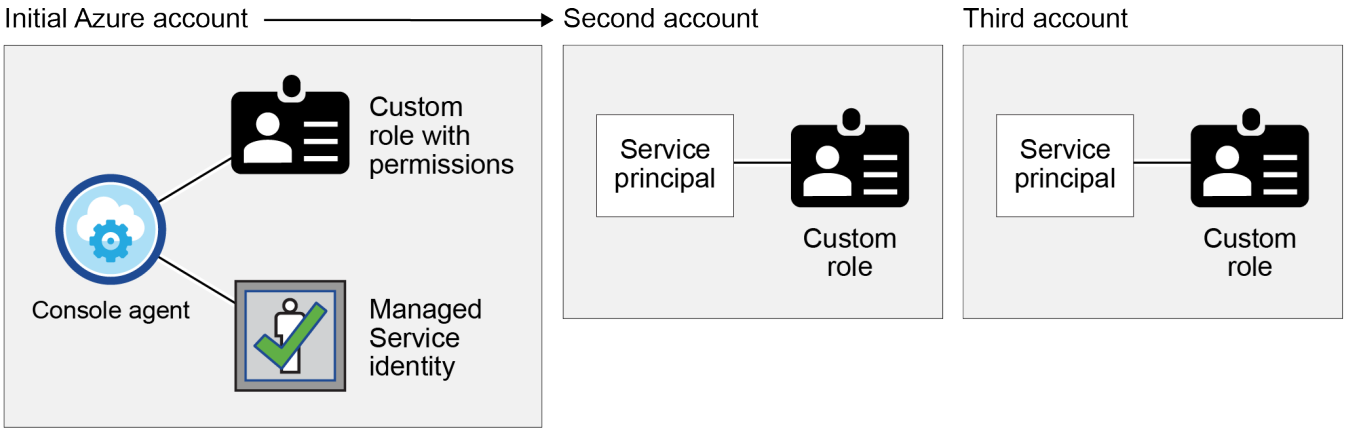
Vous pouvez déployer tous vos systèmes Cloud Volumes ONTAP à l'aide des informations d'identification Azure initiales ou ajouter des informations d'identification supplémentaires.

Abonnements Azure supplémentaires pour une identité gérée

L'identité gérée attribuée par le système à la machine virtuelle de l'agent de console est associée à l'abonnement dans lequel vous avez lancé l'agent de console. Si vous souhaitez sélectionner un autre abonnement Azure, vous devez"associer l'identité gérée à ces abonnements" .

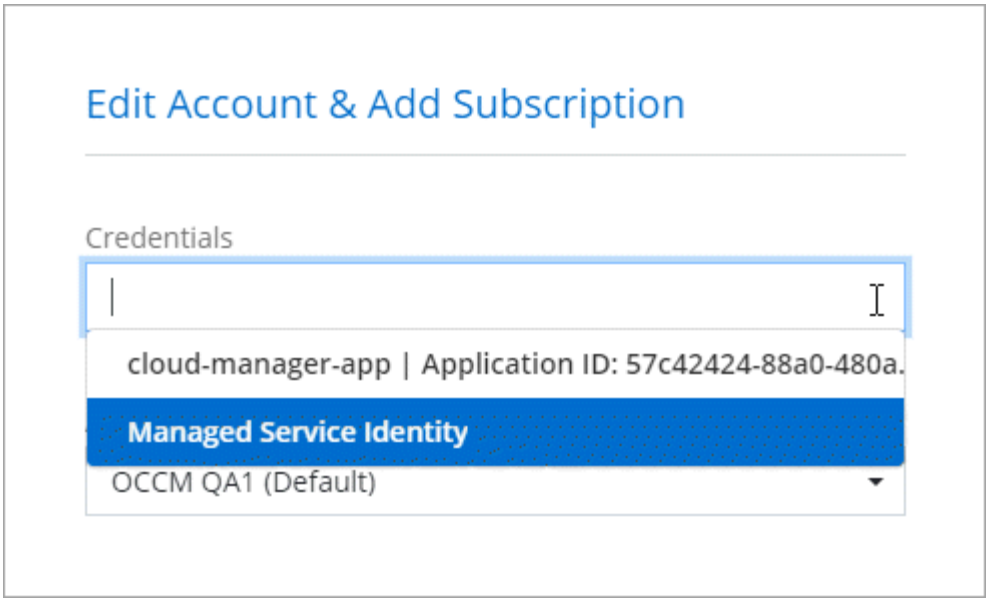
Informations d'identification Azure supplémentaires

Si vous souhaitez utiliser différentes informations d'identification Azure avec la console, vous devez accorder les autorisations requises en"création et configuration d'un principal de service dans Microsoft Entra ID" pour chaque compte Azure. L'image suivante montre deux comptes supplémentaires, chacun configuré avec un principal de service et un rôle personnalisé qui fournit des autorisations :



Vous voudriez alors"ajouter les informations d'identification du compte à la console" en fournissant des détails sur le principal du service AD.

Par exemple, vous pouvez basculer entre les informations d'identification lors de la création d'un nouveau système Cloud Volumes ONTAP :



Informations d'identification et abonnements à la place de marché

Les informations d'identification que vous ajoutez à un agent de console doivent être associées à un abonnement Azure Marketplace afin que vous puissiez payer Cloud Volumes ONTAP à un tarif horaire (PAYGO) ou des services de données NetApp ou via un contrat annuel.

"Découvrez comment associer un abonnement Azure" .

Notez les points suivants concernant les informations d'identification Azure et les abonnements à la place de marché :

- Vous ne pouvez associer qu'un seul abonnement Azure Marketplace à un ensemble d'informations d'identification Azure
- Vous pouvez remplacer un abonnement de marché existant par un nouvel abonnement

FAQ

La question suivante concerne les informations d'identification et les abonnements.

Puis-je modifier l'abonnement Azure Marketplace pour les systèmes Cloud Volumes ONTAP ?

Oui, tu peux. Lorsque vous modifiez l'abonnement Azure Marketplace associé à un ensemble d'informations d'identification Azure, tous les systèmes Cloud Volumes ONTAP existants et nouveaux seront facturés sur le nouvel abonnement.

"Découvrez comment associer un abonnement Azure" .

Puis-je ajouter plusieurs informations d'identification Azure, chacune avec des abonnements de marketplace différents ?

Toutes les informations d'identification Azure appartenant au même abonnement Azure seront associées au même abonnement Azure Marketplace.

Si vous disposez de plusieurs informations d'identification Azure appartenant à différents abonnements Azure, ces informations d'identification peuvent être associées au même abonnement Azure Marketplace ou à différents abonnements Marketplace.

Puis-je déplacer des systèmes Cloud Volumes ONTAP existants vers un autre abonnement Azure ?

Non, il n'est pas possible de déplacer les ressources Azure associées à votre système Cloud Volumes ONTAP vers un autre abonnement Azure.

Comment fonctionnent les informations d'identification pour les déploiements sur le marché et les déploiements sur site ?

Les sections ci-dessus décrivent la méthode de déploiement recommandée pour l'agent de console, qui provient de la console. Vous pouvez également déployer un agent de console dans Azure à partir de la Place de marché Azure et installer le logiciel de l'agent de console sur votre propre hôte Linux.

Si vous utilisez la Place de marché, vous pouvez fournir des autorisations en attribuant un rôle personnalisé à la machine virtuelle de l'agent de console et à une identité gérée attribuée par le système, ou vous pouvez utiliser un principal de service Microsoft Entra.

Pour les déploiements sur site, vous ne pouvez pas configurer une identité gérée pour l'agent de console, mais vous pouvez fournir des autorisations à l'aide d'un principal de service.

Pour savoir comment configurer les autorisations, reportez-vous aux pages suivantes :

- Mode standard
  - "Configurer les autorisations pour un déploiement Azure Marketplace"
  - "Configurer les autorisations pour les déploiements sur site"
- Mode restreint
  - "Configurer les autorisations pour le mode restreint"

Gérer les informations d'identification Azure et les abonnements à la place de marché pour la NetApp Console

Ajoutez et gérez les informations d'identification Azure afin que la NetApp Console dispose des autorisations nécessaires pour déployer et gérer les ressources cloud dans vos abonnements Azure. Si vous gérez plusieurs abonnements Azure Marketplace, vous pouvez attribuer chacun d'eux à différentes informations d'identification Azure à partir de la page Informations d'identification.

Aperçu

Il existe deux manières d'ajouter des abonnements et des informations d'identification Azure supplémentaires dans la console.

1. Associez des abonnements Azure supplémentaires à l'identité gérée Azure.
2. Pour déployer Cloud Volumes ONTAP à l'aide de différentes informations d'identification Azure, accordez des autorisations Azure à l'aide d'un principal de service et ajoutez ses informations d'identification à la console.

Associer des abonnements Azure supplémentaires à une identité gérée

La console vous permet de choisir les informations d'identification Azure et l'abonnement Azure dans lesquels vous souhaitez déployer Cloud Volumes ONTAP. Vous ne pouvez pas sélectionner un autre abonnement Azure pour le profil d'identité managée, sauf si vous l'associez "identité gérée" avec ces abonnements.

À propos de cette tâche

Une identité gérée est"le compte Azure initial" lorsque vous déployez un agent de console à partir de la console. Lorsque vous déployez l'agent de console, la console attribue le rôle d'opérateur de console à la machine virtuelle de l'agent de console.

Étapes

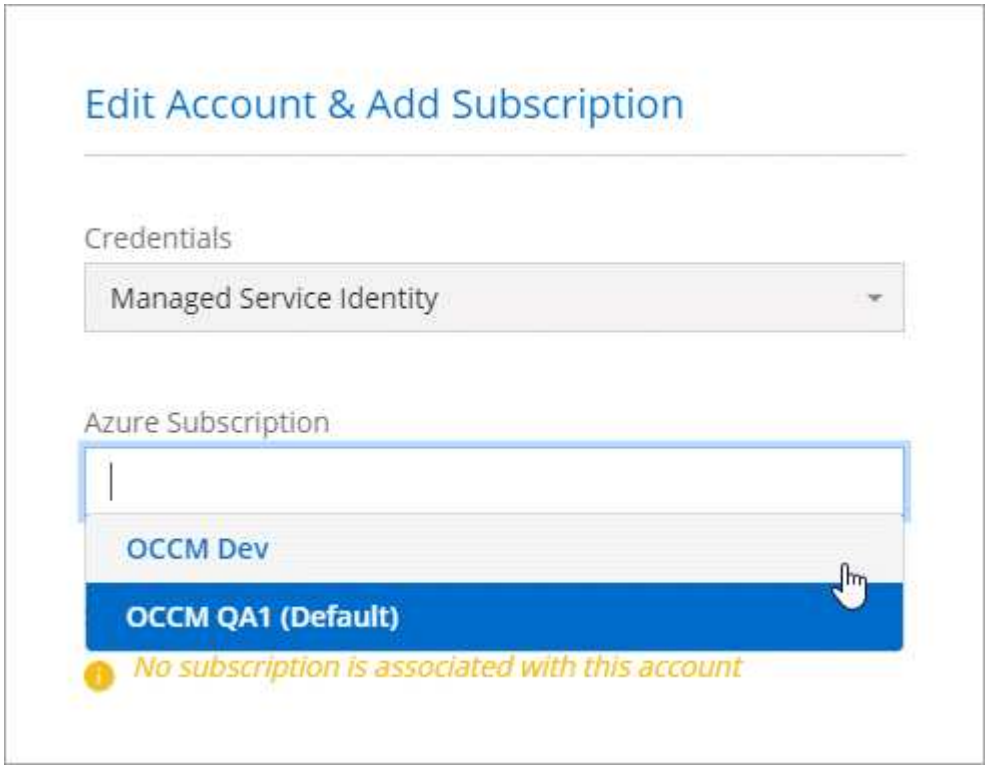
1. Connectez-vous au portail Azure.
2. Ouvrez le service **Abonnements**, puis sélectionnez l'abonnement dans lequel vous souhaitez déployer Cloud Volumes ONTAP.
3. Sélectionnez **Contrôle d'accès (IAM)**.
   a. Sélectionnez **Ajouter** > **Ajouter une attribution de rôle**, puis ajoutez les autorisations :
      - Sélectionnez le rôle **Opérateur de console**.

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

      - Attribuer l'accès à une **machine virtuelle**.
      - Sélectionnez l'abonnement dans lequel une machine virtuelle d'agent de console a été créée.
      - Sélectionnez une machine virtuelle d'agent de console.
      - Sélectionnez **Enregistrer**.
4. Répétez ces étapes pour des abonnements supplémentaires.

Résultat

Lors de la création d'un nouveau système, vous pouvez désormais choisir parmi plusieurs abonnements Azure pour le profil d'identité géré.



Ajouter des informations d'identification Azure supplémentaires à la NetApp Console

Lorsque vous déployez un agent de console à partir de la console, la console active une identité gérée attribuée par le système sur la machine virtuelle qui dispose des autorisations requises. La console sélectionne ces informations d'identification Azure par défaut lorsque vous créez un nouveau système pour Cloud Volumes ONTAP.

Un ensemble initial d'informations d'identification n'est pas ajouté si vous avez installé manuellement un logiciel d'agent de console sur un système existant. "En savoir plus sur les informations d'identification et les autorisations Azure" .

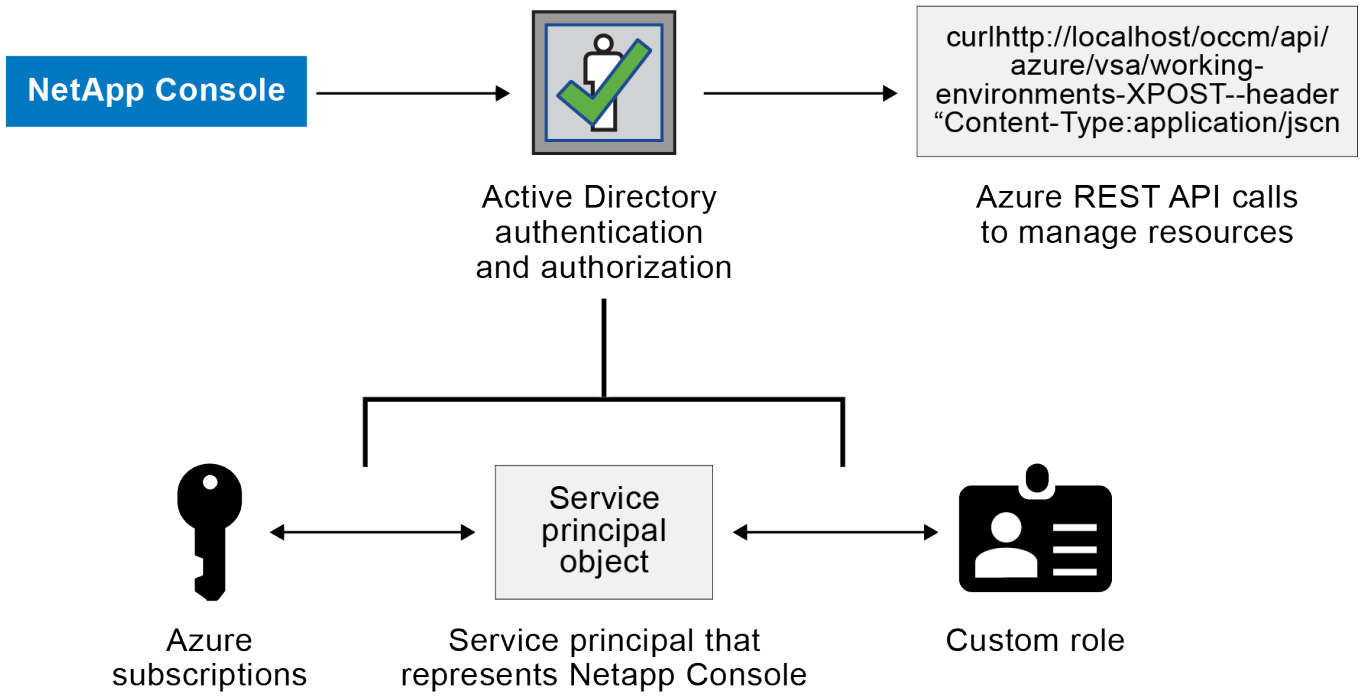
Si vous souhaitez déployer Cloud Volumes ONTAP à l'aide de *différentes* informations d'identification Azure, vous devez accorder les autorisations requises en créant et en configurant un principal de service dans Microsoft Entra ID pour chaque compte Azure. Vous pouvez ensuite ajouter les nouvelles informations d'identification à la console.

Accorder des autorisations Azure à l'aide d'un principal de service

La console a besoin d'autorisations pour effectuer des actions dans Azure. Vous pouvez accorder les autorisations requises à un compte Azure en créant et en configurant un principal de service dans Microsoft Entra ID et en obtenant les informations d'identification Azure dont la console a besoin.

À propos de cette tâche

L'image suivante illustre comment la console obtient les autorisations pour effectuer des opérations dans Azure. Un objet principal de service, lié à un ou plusieurs abonnements Azure, représente la console dans Microsoft Entra ID et est attribué à un rôle personnalisé qui autorise les autorisations requises.



Étapes

1. Créer une application Microsoft Entra .
2. Affecter l'application à un rôle .
3. Ajouter des autorisations à l'API Windows Azure Service Management .

4. Obtenir l'ID de l'application et l'ID du répertoire .
5. Créer un secret client .

Créer une application Microsoft Entra

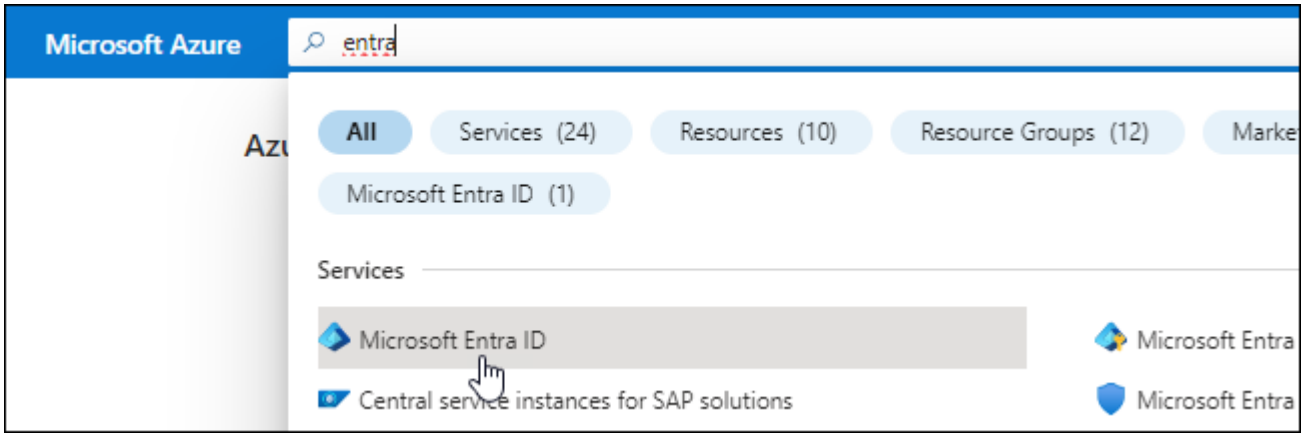
Créez une application Microsoft Entra et un principal de service que la console peut utiliser pour le contrôle d'accès basé sur les rôles.

Étapes

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

Vous devez lier le principal du service à un ou plusieurs abonnements Azure et lui attribuer le rôle personnalisé « Opérateur de console » afin que la console dispose d'autorisations dans Azure.

Étapes

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 .

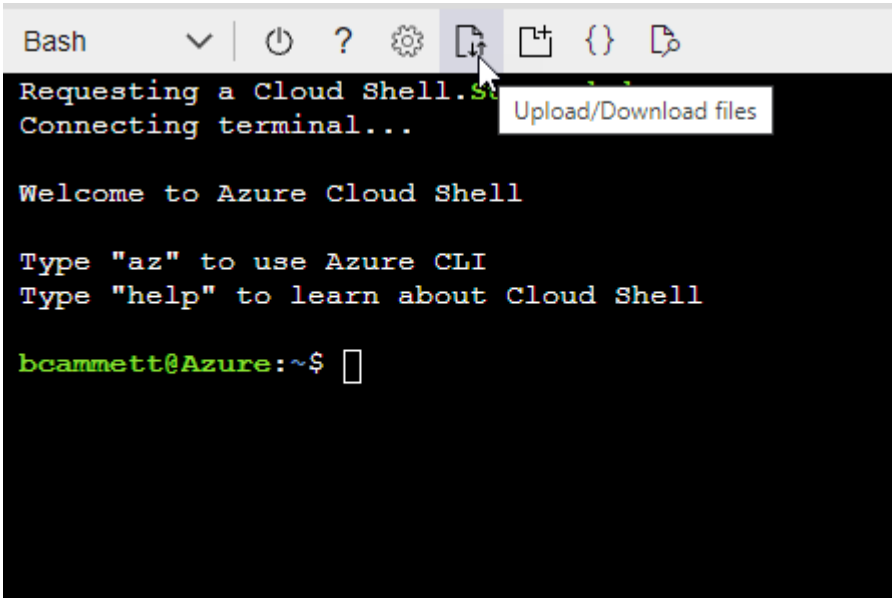
   Exemple

   ```
   "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**.

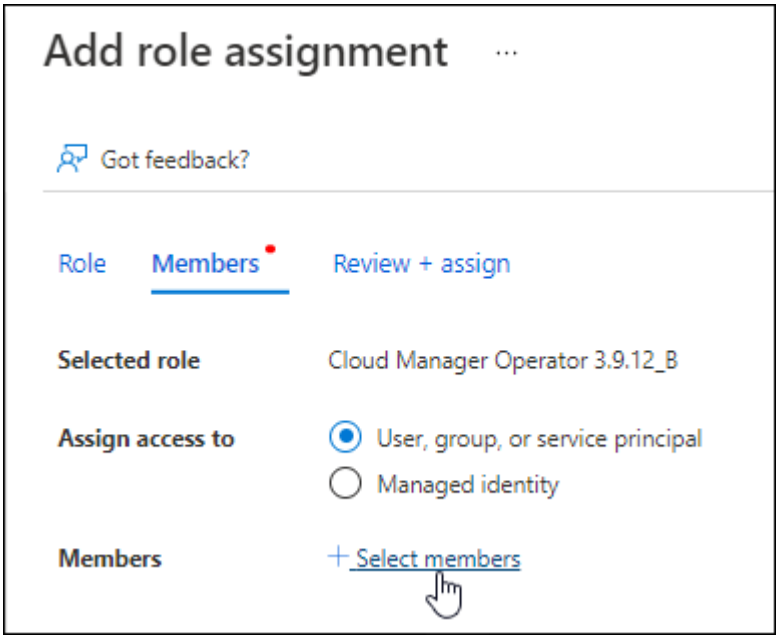
    b. Sélectionnez l'abonnement.

    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**.

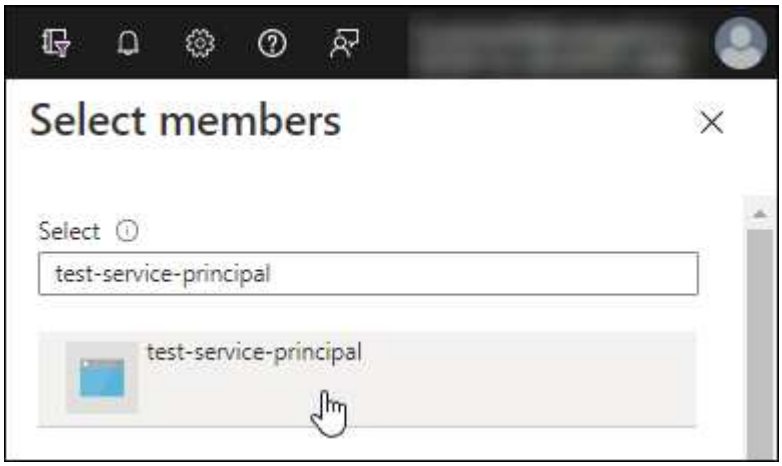
    e. Dans l'onglet **Membres**, procédez comme suit :

    - 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.

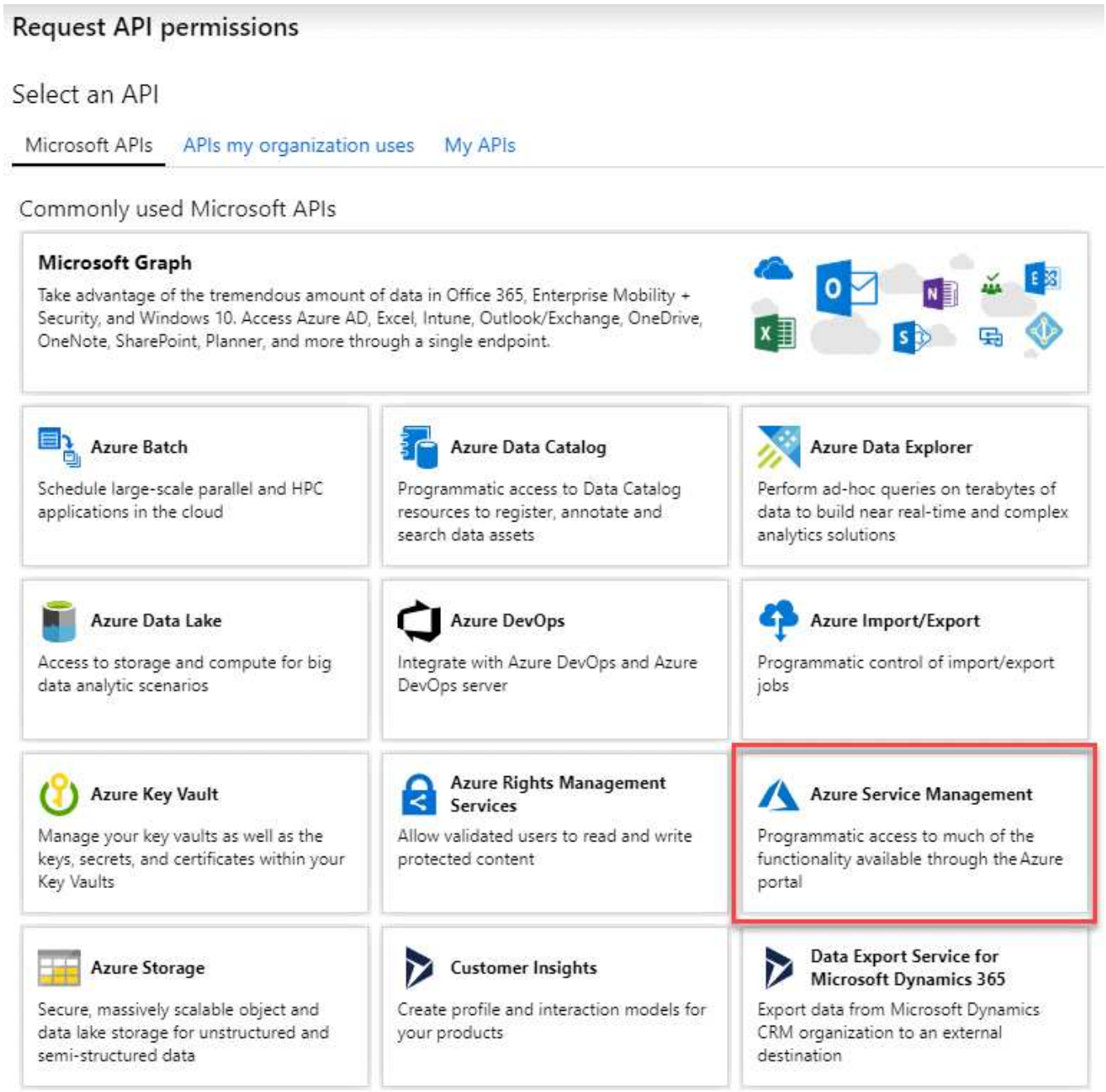
Si vous souhaitez déployer Cloud Volumes ONTAP à partir de plusieurs abonnements Azure, vous devez lier le principal de service à chacun de ces abonnements. Dans la NetApp Console, vous pouvez sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

Ajouter des autorisations à l'API Windows Azure Service Management

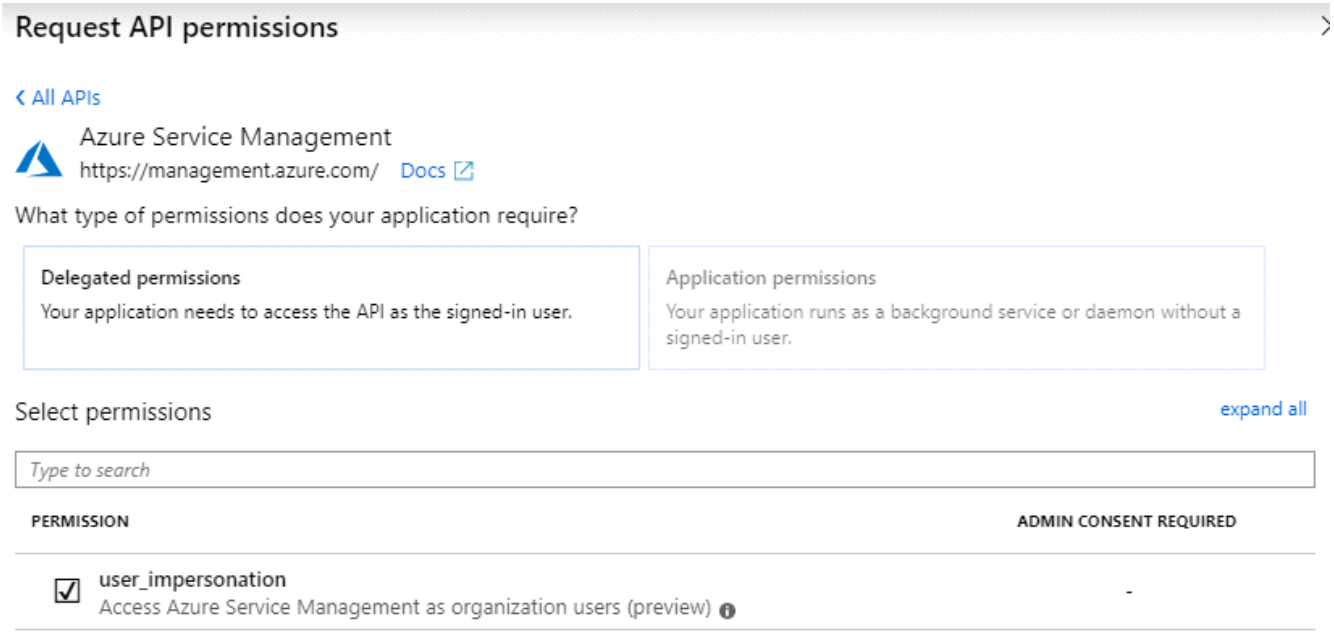
Vous devez attribuer les autorisations « API de gestion des services Windows Azure » au principal du service.

Étapes

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**.

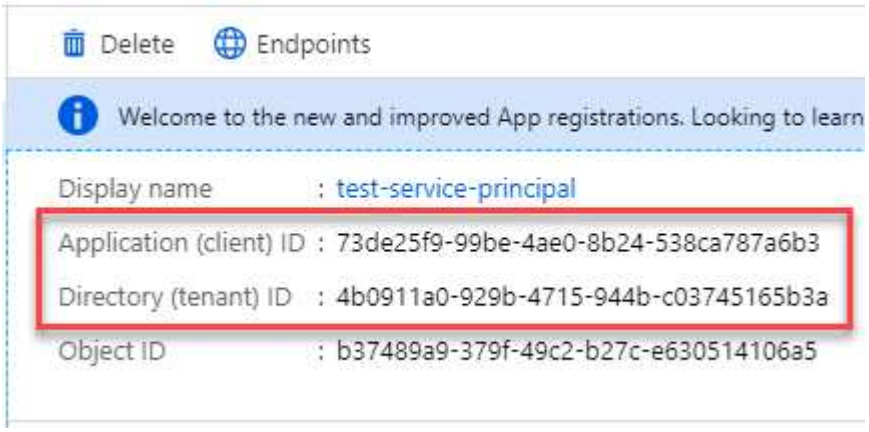


Obtenir l'ID de l'application et l'ID du répertoire

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.

Étapes

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

Créez un secret client et fournissez sa valeur à la console pour l'authentification avec Microsoft Entra ID.

Étapes

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.

Ajoutez les informations d'identification à la console

Après avoir fourni à un compte Azure les autorisations requises, vous pouvez ajouter les informations d'identification de ce compte à la console. Cette étape vous permet de lancer Cloud Volumes ONTAP à l'aide de différentes informations d'identification Azure.

Avant de commencer

Si vous venez de créer ces informations d'identification auprès de votre fournisseur de cloud, il faudra peut-être quelques minutes avant qu'elles soient disponibles pour utilisation. Attendez quelques minutes avant d'ajouter les informations d'identification à la console.

Avant de commencer

Vous devez créer un agent de console avant de pouvoir modifier les paramètres de la console. "Apprenez à créer un agent de console" .

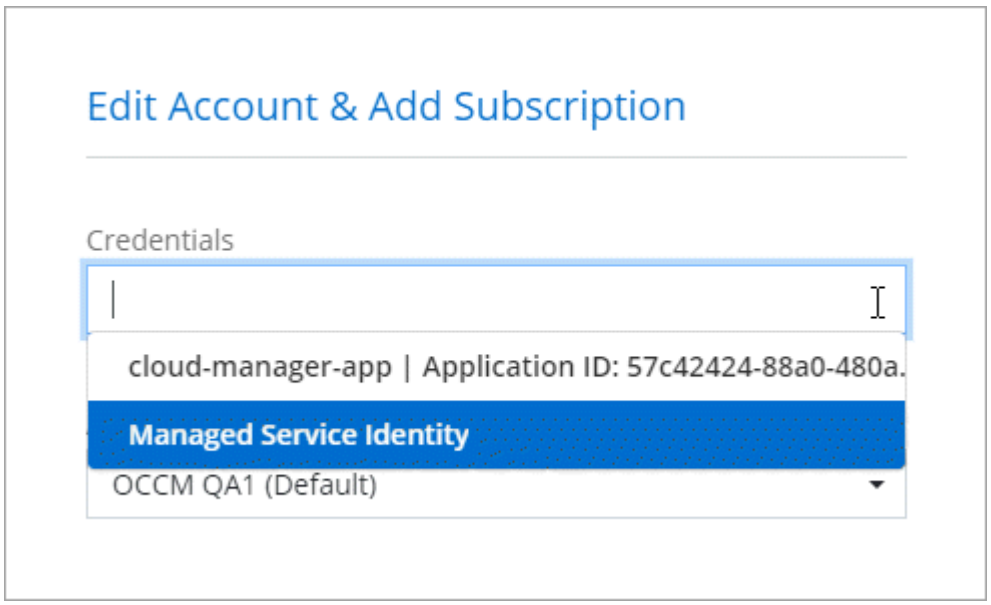
Étapes

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

Vous pouvez passer à un autre ensemble d'informations d'identification à partir de la page Détails et informations d'identification. "lors de l'ajout d'un système à la console"



Gérer les informations d'identification existantes

Gérez les informations d'identification Azure que vous avez déjà ajoutées à la console en associant un abonnement Marketplace, en modifiant les informations d'identification et en les supprimant.

Associer un abonnement Azure Marketplace aux informations d'identification

Après avoir ajouté vos informations d'identification Azure à la console, vous pouvez associer un abonnement Azure Marketplace à ces informations d'identification. Vous pouvez utiliser l'abonnement pour créer un système Cloud Volumes ONTAP à la carte et accéder aux services de données NetApp .

Il existe deux scénarios dans lesquels vous pouvez associer un abonnement Azure Marketplace après avoir ajouté les informations d'identification à la console :

- Vous n'avez pas associé d'abonnement lorsque vous avez initialement ajouté les informations d'identification à la console.
- Vous souhaitez modifier l'abonnement Azure Marketplace associé aux informations d'identification Azure.

  Le remplacement de l'abonnement actuel au marché le met à jour pour les systèmes Cloud Volumes ONTAP existants et nouveaux.

Étapes

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

   Vous devez sélectionner les informations d'identification associées à un agent de console. Vous ne pouvez

pas associer un abonnement au marché aux informations d'identification associées à la NetApp Console.

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

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

   b. Sélectionnez **S'abonner**.

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

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

      Vous serez redirigé vers la NetApp Console.

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

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

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

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

   ◦ Sélectionnez **Enregistrer**.

Modifier les informations d'identification

Modifiez vos informations d'identification Azure dans la console. Par exemple, vous pouvez mettre à jour le secret client si un nouveau secret a été créé pour l'application principale de service.

Étapes

1. Sélectionnez **Administration > Informations d'identification**.
2. Sélectionnez **Informations d'identification de l'organisation**.
3. Sélectionnez le menu d'action pour un ensemble d'informations d'identification, puis sélectionnez **Modifier les informations d'identification**.
4. Apportez les modifications requises, puis sélectionnez **Appliquer**.

Supprimer les informations d'identification

Si vous n'avez plus besoin d'un ensemble d'informations d'identification, vous pouvez les supprimer. Vous ne pouvez supprimer que les informations d'identification qui ne sont pas associées à un système.

Étapes

1. Sélectionnez **Administration > Informations d'identification**.

2. Sélectionnez **Informations d'identification de l'organisation**.
3. Sur la page **Informations d'identification de l'organisation**, sélectionnez le menu d'action pour un ensemble d'informations d'identification, puis sélectionnez **Supprimer les informations d'identification**.
4. Sélectionnez **Supprimer** pour confirmer.

Google Cloud

En savoir plus sur les projets et les autorisations Google Cloud

Découvrez comment la NetApp Console utilise les informations d'identification Google Cloud pour effectuer des actions en votre nom et comment ces informations d'identification sont associées aux abonnements de la place de marché. Comprendre ces détails peut être utile lorsque vous gérez les informations d'identification d'un ou plusieurs projets Google Cloud. Par exemple, vous souhaiterez peut-être en savoir plus sur le compte de service associé à la machine virtuelle de l'agent de console.

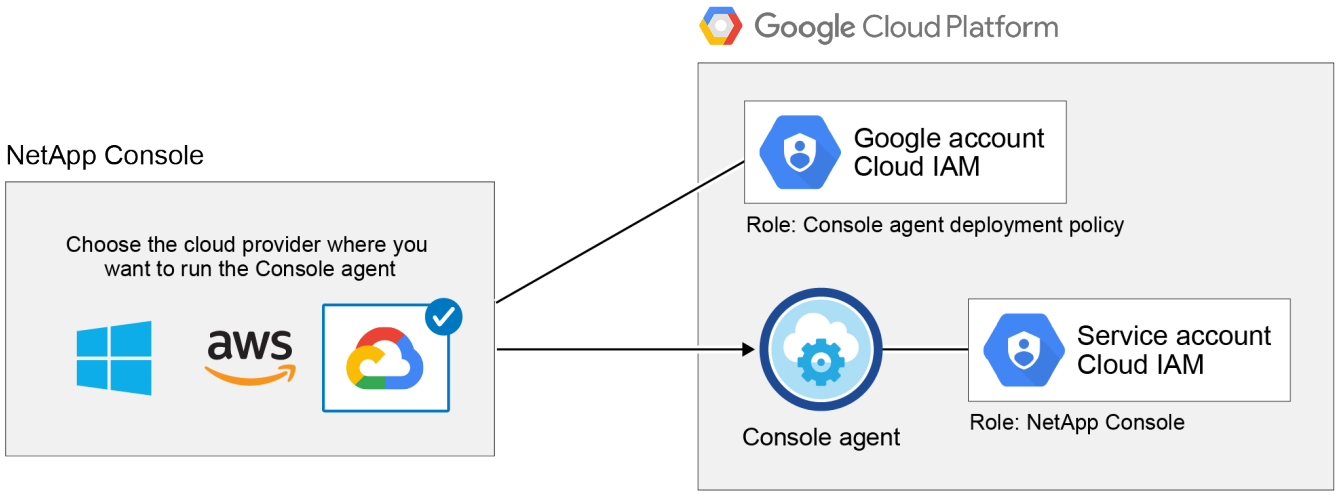
Projet et autorisations pour la NetApp Console

Avant de pouvoir utiliser la console pour gérer les ressources de votre projet Google Cloud, vous devez d'abord déployer un agent de console. L'agent ne peut pas être exécuté dans vos locaux ou chez un autre fournisseur de cloud.

Deux ensembles d'autorisations doivent être en place avant de déployer un agent de console directement à partir de la console :

1. Vous devez déployer un agent de console à l'aide d'un compte Google disposant des autorisations nécessaires pour lancer l'agent de console à partir de la console.
2. Lors du déploiement de l'agent de console, vous êtes invité à sélectionner un "compte de service" pour l'agent La console obtient des autorisations du compte de service pour créer et gérer les systèmes Cloud Volumes ONTAP , pour gérer les sauvegardes à l'aide de la sauvegarde et de la récupération NetApp , et bien plus encore. Les autorisations sont fournies en associant un rôle personnalisé au compte de service.

L'image suivante illustre les exigences d'autorisation décrites aux numéros 1 et 2 ci-dessus :



Pour savoir comment configurer les autorisations, reportez-vous aux pages suivantes :

- "Configurer les autorisations Google Cloud pour le mode standard"
- "Configurer les autorisations pour le mode restreint"

Informations d'identification et abonnements à la place de marché

Lorsque vous déployez un agent de console dans Google Cloud, la console crée un ensemble d'informations d'identification par défaut pour le compte de service Google Cloud dans le projet dans lequel réside l'agent de console. Ces informations d'identification doivent être associées à un abonnement Google Cloud Marketplace afin que vous puissiez payer les services de données Cloud Volumes ONTAP et NetApp .

"Découvrez comment associer un abonnement Google Cloud Marketplace" .

Notez les points suivants concernant les informations d'identification Google Cloud et les abonnements à la place de marché :

- Un seul ensemble d'informations d'identification Google Cloud peut être associé à un agent de console
- Vous ne pouvez associer qu'un seul abonnement Google Cloud Marketplace aux informations d'identification
- Vous pouvez remplacer un abonnement de marché existant par un nouvel abonnement

Projet pour Cloud Volumes ONTAP

Cloud Volumes ONTAP peut résider dans le même projet que l'agent de la console ou dans un projet différent. Pour déployer Cloud Volumes ONTAP dans un autre projet, vous devez d'abord ajouter le compte de service et le rôle de l'agent de console à ce projet.

- "Apprenez à configurer le compte de service"
- "Découvrez comment déployer Cloud Volumes ONTAP dans Google Cloud et sélectionner un projet"

Gestion des autorisations de l'agent de la console pour les déploiements Google Cloud

Il arrive que NetApp mette à jour les autorisations requises pour le compte de service utilisé par l'agent Console lorsqu'il est déployé sur Google Cloud.

"Vérifiez la liste des autorisations Google requises".

Utilisez la console Google Cloud pour mettre à jour le rôle IAM attribué au compte de service afin qu'il corresponde au nouvel ensemble d'autorisations.

"Documentation Google Cloud : Modifier un rôle personnalisé"

Gestion des identités et des accès

En savoir plus sur la gestion des identités et des accès de la NetApp Console

Utilisez la gestion des identités et des accès (IAM) de la console NetApp pour organiser vos ressources NetApp et contrôler l'accès en fonction de la structure de votre entreprise : par emplacement, département ou projet.

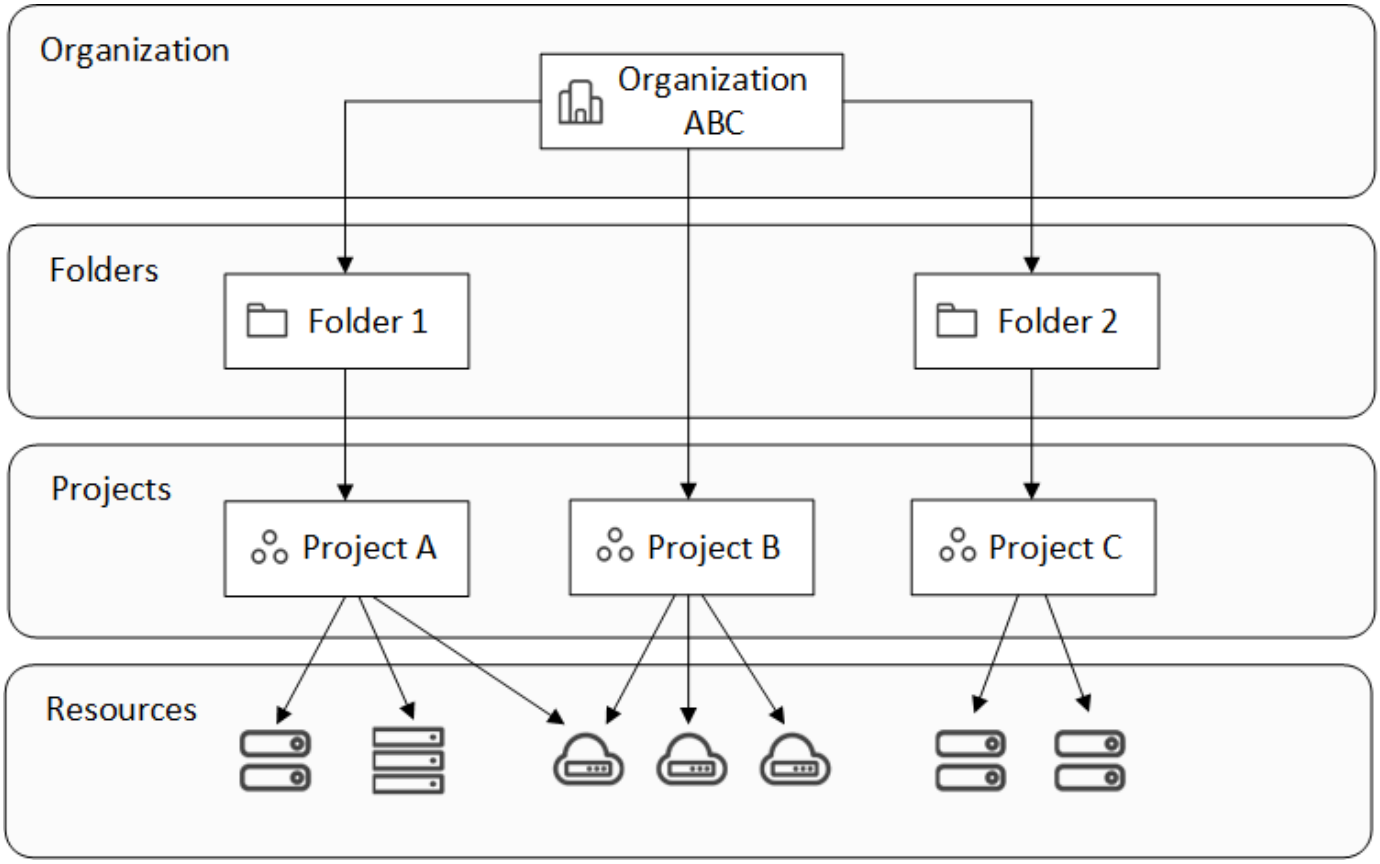
Les ressources sont organisées de manière hiérarchique : l'organisation se trouve au sommet, suivie des dossiers (qui peuvent contenir d'autres dossiers ou projets), puis des projets, qui contiennent des systèmes de

stockage, des charges de travail et des agents.

Attribuez des rôles d'accès au niveau de l'organisation, du dossier ou du projet afin que les utilisateurs disposent du bon accès aux ressources.

Vous devez disposer des rôles *Super administrateur*, *Administrateur d'organisation* ou *Administrateur de dossier ou de projet* pour gérer IAM dans la NetApp Console.

L'image suivante illustre cette hiérarchie à un niveau de base.



]

Composants de gestion des identités et des accès

Dans NetApp Console, vous organisez vos ressources de stockage à l'aide de trois composants principaux : les composants organisationnels, les composants de ressources et les composants d'accès utilisateur.

Projets et dossiers au sein de votre organisation

Au sein de votre structure IAM, vous travaillez avec trois composantes organisationnelles : les organisations, les projets et les dossiers. Vous pouvez accorder l'accès aux utilisateurs en leur attribuant des rôles à chacun de ces niveaux.

Organisation

Une *organisation* est le niveau supérieur du système IAM de la console et représente généralement votre entreprise. Votre organisation se compose de dossiers, de projets, de membres, de rôles et de ressources. Les agents sont associés à des projets spécifiques au sein de l'organisation.

Projets

Un *projet* est utilisé pour fournir un accès à une ressource de stockage. Vous devez affecter des ressources à un projet avant que quiconque puisse y accéder. Vous pouvez affecter plusieurs ressources à un seul projet et vous pouvez également avoir plusieurs projets. Vous attribuez ensuite aux utilisateurs des autorisations d'accès au projet afin de leur donner accès aux ressources qu'il contient.

Par exemple, vous pouvez associer un système ONTAP sur site à un seul projet ou à tous les projets de votre organisation, selon vos besoins.

"Découvrez comment ajouter des projets à votre organisation."

Dossiers

Regroupez les projets connexes dans des *dossiers* pour les organiser par emplacement, site ou unité commerciale. Il n'est pas possible d'associer directement des ressources à des dossiers, mais l'attribution d'un rôle à un utilisateur au niveau du dossier lui donne accès à tous les projets contenus dans ce dossier.

"Apprenez comment ajouter des dossiers à votre organisation."

Ressources

Une est une entité que la NetApp Console reconnaît et qui peut être affectée à un projet. comprennent les systèmes de stockage, les abonnements Keystone, certaines charges de travail NetApp Backup and Recovery, ainsi que les agents NetApp Console.

+ Vous devez associer une ressource à un projet avant que quiconque puisse y accéder.

+

Par exemple, vous pouvez associer un système Cloud Volumes ONTAP à un projet ou à tous les projets de votre organisation. La manière dont vous associez une ressource dépend des besoins de votre organisation.

+

"Apprenez à associer des ressources à des projets."

Systèmes de stockage et abonnements Keystone

Les systèmes de stockage sont les principales ressources que vous gérez dans NetApp Console. NetApp Console prend en charge la gestion des systèmes de stockage sur site et dans le cloud. Vous devez ajouter un système de stockage à un projet pour qu'il soit accessible aux personnes affectées à ce projet.

Systèmes de stockage

Les systèmes de stockage sont automatiquement associés au projet dans lequel ils sont ajoutés, mais vous pouvez les associer à d'autres projets ou dossiers depuis la page **Ressources**. Vous ne pouvez pas associer les systèmes de stockage FSx for NetApp ONTAP à des projets ou des dossiers, mais vous pouvez les consulter sur la page **Systèmes** ou depuis Workloads.

Abonnements Keystone

Les abonnements Keystone sont également des ressources que vous pouvez associer à des projets afin d'accorder aux utilisateurs l'accès à l'abonnement dans la NetApp Console.

Charges de travail de sauvegarde et de récupération (Oracle et Microsoft SQL Server)

Certaines charges de travail NetApp Backup and Recovery sont également considérées comme des ressources. Vous pouvez attribuer aux utilisateurs des autorisations d'accès à NetApp Backup and Recovery.

Agents de console

Les administrateurs de l'organisation créent des agents de console pour gérer les systèmes de stockage et activer les services de données NetApp . Les agents sont initialement liés au projet dans lequel ils sont créés, mais les administrateurs peuvent les ajouter à d'autres projets ou dossiers depuis la page Agents.

L'association d'un agent à un projet permet la gestion des ressources de ce projet, tandis que l'association d'un agent à un dossier permet aux administrateurs de dossier ou de projet de décider quels projets doivent utiliser l'agent. Les agents doivent être rattachés à des projets spécifiques pour assurer leurs capacités de gestion.

"Apprenez comment associer des agents à des projets."

Membres et rôles

Membres

Les membres de votre organisation sont des comptes d'utilisateurs ou des comptes de service. Un compte de service est généralement utilisé par une application pour effectuer des tâches spécifiques sans intervention humaine.

Vous devez ajouter des membres à votre organisation après leur inscription à NetApp Console. Une fois ajoutés, vous pouvez leur attribuer des rôles pour leur donner accès aux ressources. Vous pouvez ajouter manuellement des comptes de service depuis la console ou automatiser leur création et leur gestion via l'API IAM de la NetApp Console .

"Découvrez comment ajouter des membres à votre organisation."

Rôles d'accès

La console fournit des rôles d'accès que vous pouvez attribuer aux membres de votre organisation.

Lorsque vous associez un membre à un rôle, vous pouvez attribuer ce rôle à l'ensemble de l'organisation, à un dossier spécifique ou à un projet spécifique. Le rôle que vous sélectionnez confère à un membre des autorisations d'accès aux ressources de la partie sélectionnée de la hiérarchie.

La NetApp Console propose des rôles granulaires qui respectent le principe du « moindre privilège », ce qui signifie que les rôles d'accès sont conçus pour n'accorder aux utilisateurs que l'accès aux ressources dont ils ont besoin.

Cela signifie que les utilisateurs peuvent se voir attribuer plusieurs rôles à mesure que leurs responsabilités s'étendent.

"En savoir plus sur les rôles d'accès" .

Exemples de stratégie IAM

stratégie des petites organisations

Pour les organisations comptant moins de 50 utilisateurs et disposant d'une gestion centralisée du stockage, envisagez une approche simplifiée utilisant les rôles de super administrateur et de super visualiseur.

Exemple : Société ABC (équipe de 5 personnes)

- **Structure :** Une seule organisation avec 3 projets (Production, Développement, Sauvegarde)
- **Rôles :**

    - 2 membres seniors : rôle de **super administrateur** pour un accès administratif complet
    - 3 membres de l'équipe : rôle de **Super observateur** pour la surveillance sans droits de modification
- **Stratégie d'agent :** Un seul agent est associé à tous les projets pour l'accès aux ressources partagées.
- **Avantages :** Administration simplifiée, complexité des rôles réduite, adapté aux équipes nécessitant un accès étendu

Stratégie d'entreprise multirégionale

Pour les grandes organisations ayant des activités régionales et des équipes spécialisées, il convient de mettre en œuvre une approche hiérarchique avec des dossiers représentant les limites géographiques ou les limites des unités commerciales.

Exemple : Société XYZ (entreprise multinationale)

- **Structure :** Organisation > Dossiers régionaux (Amérique du Nord, Europe, Asie-Pacifique) > Dossiers de projet par région
- **Rôles de la plateforme :**
    - 1 **Administration de l'organisation** : Supervision globale et gestion des politiques
    - 3 **Administrateurs de dossiers ou de projets** : Contrôle régional (un par région)
    - 1 **Administrateur de la fédération** : Intégration du fournisseur d'identité d'entreprise
- **Rôles de stockage par région :**
    - 9 **Administration du stockage** : Découvrir et gérer les systèmes de stockage dans les régions attribuées
    - 2 **Visualiseur de stockage** : Surveillez les ressources de stockage dans différentes régions
    - 1 **Spécialiste de la santé du système** : Gérer la santé du stockage sans modifier le système
- **Rôles du service de données :**
    - Administration des sauvegardes et des restaurations : par projet, selon les responsabilités liées aux sauvegardes.
    - **Administrateur de la résilience aux ransomwares** : Supervision de l'équipe de sécurité sur l'ensemble des projets
- **Stratégie d'agents :** Agents régionaux associés à des projets géographiques appropriés
- **Avantages :** Sécurité renforcée grâce à la séparation des rôles, à l'autonomie régionale et au respect des réglementations locales

stratégie de spécialisation départementale

Pour les organisations disposant d'équipes spécialisées nécessitant un accès spécifique aux services de données, utilisez des attributions de rôles ciblées basées sur les responsabilités fonctionnelles.

Exemple : TechCorp (entreprise technologique de taille moyenne)

- **Structure :** Organisation > Dossiers de département (Informatique, Sécurité, Développement) > Ressources spécifiques au projet
- **Rôles spécialisés :**
    - Équipe de sécurité : rôles d'administrateur de la résilience aux ransomwares et de consultant en classification.

- Équipe de sauvegarde : **Super administrateur de sauvegarde et de restauration** pour des opérations de sauvegarde complètes
- Équipe de développement : **Administrateur du stockage** pour la gestion de l'environnement de test
- Équipe de conformité : **Analyste de soutien aux opérations** pour le suivi et la gestion des cas de soutien

- **Stratégie relative aux agents :** Les agents sont rattachés aux projets départementaux en fonction de la propriété des ressources.
- **Avantages :** Contrôle d'accès personnalisé, efficacité opérationnelle accrue et responsabilisation claire pour les tâches spécialisées

Prochaines étapes avec IAM dans la NetApp Console

- "Démarrer avec IAM dans la NetApp Console"
- "Surveiller ou auditer l'activité IAM"
- "En savoir plus sur l'API pour NetApp Console IAM"

Démarrer avec l'identité et l'accès dans la NetApp Console

Lorsque vous vous inscrivez à la NetApp Console, vous êtes invité à créer une nouvelle organisation. L'organisation comprend un membre (un administrateur d'organisation) et un projet par défaut. Pour configurer la gestion des identités et des accès (IAM) afin de répondre aux besoins de votre entreprise, vous devrez personnaliser la hiérarchie de votre organisation, ajouter des membres supplémentaires, ajouter ou découvrir des ressources et associer ces ressources à l'ensemble de votre hiérarchie.

Vous avez besoin des autorisations d'**administrateur d'organisation** ou de **super administrateur** pour gérer l'identité et l'accès de votre organisation. Avec les autorisations d'**administrateur de dossier ou de projet**, vous ne pouvez gérer que les dossiers et les projets auxquels vous avez accès.

Suivez ces étapes pour créer une nouvelle organisation. L'ordre peut varier en fonction des besoins de votre organisation.

Modifiez le projet par défaut ou ajoutez-le à la hiérarchie de votre organisation

Utilisez le projet par défaut ou créez des projets et des dossiers supplémentaires correspondant à la hiérarchie de votre entreprise.

"Apprenez à organiser vos ressources avec des dossiers et des projets" .

Membres associés à votre organisation

Une fois que les utilisateurs se sont inscrits à NetApp Console, vous devez les ajouter explicitement à votre organisation Console. Vous avez également la possibilité d'ajouter des comptes de service à votre organisation.

"Apprenez à gérer les membres et leurs autorisations" .

3 Ajouter ou découvrir des ressources

Ajoutez ou découvrez des ressources (systèmes) dans la console. Les membres de l'organisation gèrent les systèmes au sein d'un projet.

Apprenez à créer ou à découvrir des ressources :

- "Amazon FSx for NetApp ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes ONTAP"
- "Systèmes de la série E"
- "Clusters ONTAP sur site"
- "StorageGRID"

4 Associer des ressources à des projets supplémentaires

L'ajout ou la découverte d'un système dans la console associe automatiquement la ressource au projet actuellement sélectionné. Pour rendre cette ressource disponible pour un autre projet de votre organisation, associez-la au projet concerné. Si un agent de console est utilisé pour gérer la ressource, associez l'agent de console au projet correspondant.

- "Apprenez à gérer la hiérarchie des ressources de votre organisation" .
- "Découvrez comment associer un agent de console à un dossier ou à un projet" .

Informations connexes

- "En savoir plus sur la gestion des identités et des accès dans la NetApp Console"
- "En savoir plus sur l'API pour l'identité et l'accès"

Configurez votre organisation de console

Ajoutez des dossiers et des projets à votre organisation NetApp Console

Ajoutez des dossiers et des projets en fonction de la structure de votre entreprise. Une fois les dossiers et les projets créés, vous pouvez leur associer des ressources et gérer l'accès des membres à ces projets.

La console crée automatiquement un projet pour vous lorsque vous créez une nouvelle organisation. La plupart des organisations ont besoin de gérer plusieurs projets, ainsi que de dossiers pour bien les organiser. "Découvrez la hiérarchie des ressources dans la NetApp Console.".

Utiliser des dossiers et des projets pour organiser les ressources

Dans NetApp Console, une organisation contient des dossiers et des projets qui vous aident à organiser vos ressources. Les dossiers vous permettent de regrouper les projets connexes, et les projets vous aident à gérer les ressources et l'accès des membres.

Dossiers

Les dossiers vous aident à organiser les projets connexes. Vous pouvez créer des dossiers imbriqués pour représenter les différents niveaux de la structure de votre organisation. Par exemple, vous pouvez créer un dossier principal pour chaque unité commerciale, puis créer des sous-dossiers pour les différentes équipes au sein de cette unité commerciale. Vous créez ensuite des projets dans des dossiers.

Les dossiers permettent également de gérer plus efficacement l'accès des membres grâce à l'héritage des rôles. Lorsque vous attribuez des rôles aux membres au niveau du dossier, ils héritent des autorisations pour tous les sous-projets et dossiers.

Les dossiers sont un outil d'organisation et ne sont pas visibles pour les membres qui ne disposent pas des autorisations IAM telles que les rôles d'administrateur d'organisation, d'administrateur de dossier ou de projet, ou de super administrateur. Les membres accèdent aux projets, pas aux dossiers.

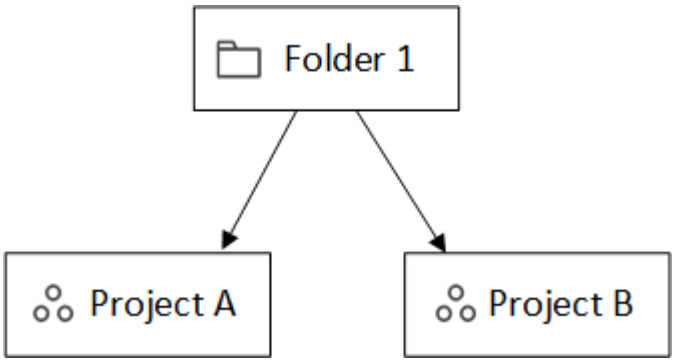
Les administrateurs de l'organisation peuvent déléguer les responsabilités administratives en créant des dossiers. Après avoir créé un dossier, un administrateur de l'organisation peut attribuer à un membre les rôles d'administrateur de dossier ou de projet pour des dossiers spécifiques. Ces membres peuvent alors gérer tous les projets contenus dans ce dossier sans avoir accès à l'ensemble de l'organisation.

Les dossiers peuvent contenir d'autres dossiers ou projets comme enfants, mais ils ne peuvent pas avoir de ressources directement associées à eux. Les ressources doivent être associées à un projet.

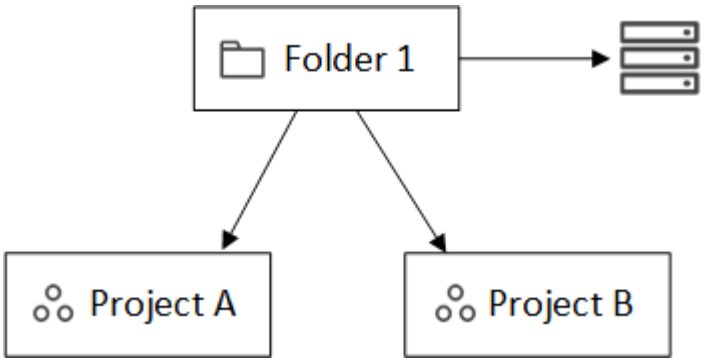
Quand associer une ressource à un dossier

Un *administrateur d'organisation* peut associer une ressource à un dossier afin qu'un *administrateur de dossier ou de projet* puisse la lier aux projets appropriés dans le dossier.

Par exemple, disons que vous avez un dossier qui contient deux projets :

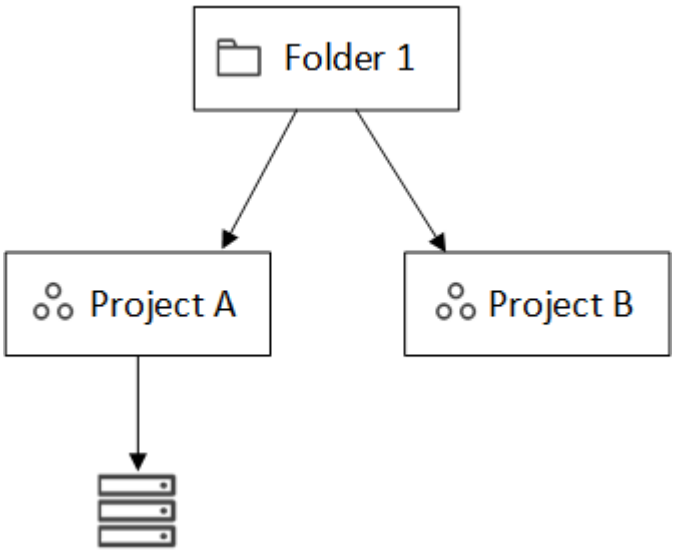


L'administrateur de l'organisation peut associer une ressource au dossier :



Associer une ressource à un dossier ne la rend pas accessible à tous les projets ; seul l'administrateur du dossier ou du projet peut la voir. L'administrateur du dossier ou du projet décide quels projets peuvent y accéder et associe la ressource aux projets appropriés.

Dans cet exemple, l'administrateur associe la ressource au projet A :



Les membres disposant d'autorisations pour le projet A peuvent désormais accéder à la ressource.

Projets

Associer les ressources aux projets pour permettre aux membres de les gérer. Les ressources doivent être associées à un projet pour la gestion et l'accès des utilisateurs.

Une organisation peut avoir un ou plusieurs projets. Un projet peut se trouver directement sous l'organisation ou dans un dossier. Si un agent est utilisé pour découvrir des ressources au sein d'un projet, vous devez également associer cet agent à ce projet.

Les utilisateurs naviguent entre les projets qui leur sont assignés sur la page **Systèmes** pour gérer les ressources associées à chaque projet.

Ajouter un dossier ou un projet

Ajoutez des projets pour gérer les ressources et des dossiers pour regrouper les projets associés. Lorsque vous créez une nouvelle organisation, la console inclut un projet.

Vous pouvez créer jusqu'à sept niveaux de dossiers et de projets dans la structure des ressources de votre organisation. Créez des dossiers imbriqués pour organiser vos ressources selon vos besoins.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Organisation**.
3. Depuis la page **Organisation**, sélectionnez **Ajouter un dossier ou un projet**.
4. Sélectionnez **Dossier** ou **Projet**.
5. Saisissez les détails du dossier ou du projet :

- **Nom et emplacement** : Saisissez un nom et choisissez un emplacement pour le dossier ou le projet. Vous pouvez placer des dossiers ou des projets sous l'organisation ou dans un autre dossier.
- **Ressources** : Sélectionnez les ressources que vous souhaitez associer à ce dossier ou à ce projet. Si vous n'avez pas encore ajouté de systèmes de stockage à la console, vous pouvez effectuer cette étape ultérieurement.

> Les membres ne peuvent accéder aux ressources d'un dossier que lorsque ces ressources sont affectées à un projet. Utilisez des dossiers pour stocker temporairement les ressources en attendant de créer les projets nécessaires. Cela peut aider l'administrateur de l'organisation à déléguer l'allocation des ressources à un administrateur de dossier ou de projet, qui affectera ensuite les ressources aux projets au sein du dossier.

- **Accès** : Sélectionnez **Ajouter un membre** pour attribuer un accès et un rôle. Vous pouvez ajouter ou supprimer des membres du projet ou du dossier à tout moment.

  "En savoir plus sur les rôles d'accès" .

6. Sélectionnez **Ajouter**.

Renommer un dossier ou un projet

Renommez un dossier ou un projet selon vos besoins. Le changement de nom n'affecte pas les ressources associées ni l'accès des membres.

Étapes

1. Depuis la page **Organisation**, accédez à un projet ou à un dossier dans le tableau, sélectionnez ••• puis sélectionnez **Modifier le dossier** ou **Modifier le projet**.
2. Sur la page **Modifier**, saisissez un nouveau nom et sélectionnez **Appliquer**.

Supprimer un dossier ou un projet

Supprimez les dossiers et les projets dont vous n'avez plus besoin, par exemple après une restructuration d'équipe ou la fin d'un projet.

Avant de supprimer un dossier ou un projet, assurez-vous qu'il ne contient aucune ressource. Apprenez comment supprimer des ressources.

Étapes

1. Depuis la page **Organisation**, accédez à un projet ou à un dossier dans le tableau, sélectionnez ••• puis sélectionnez **Supprimer**.
2. Confirmez que vous souhaitez supprimer le dossier ou le projet.

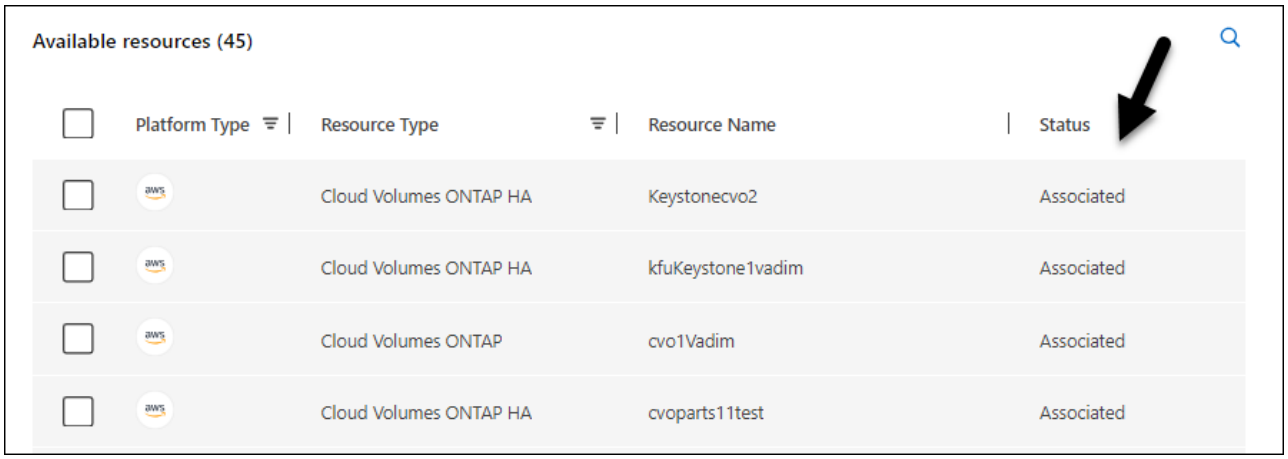
Afficher les ressources associées à un dossier ou à un projet

Afficher les ressources et les membres associés à un dossier ou à un projet.

Étapes

1. Depuis la page **Organisation**, accédez à un projet ou à un dossier dans le tableau, sélectionnez ••• puis sélectionnez **Modifier le dossier** ou **Modifier le projet**.

2. Sur la page **Modifier**, vous pouvez afficher les détails du dossier ou du projet sélectionné en développant les sections **Ressources** ou **Accès**.
   - Sélectionnez **Ressources** pour afficher les ressources associées. Dans le tableau, la colonne **Statut** identifie les ressources associées au dossier ou au projet.



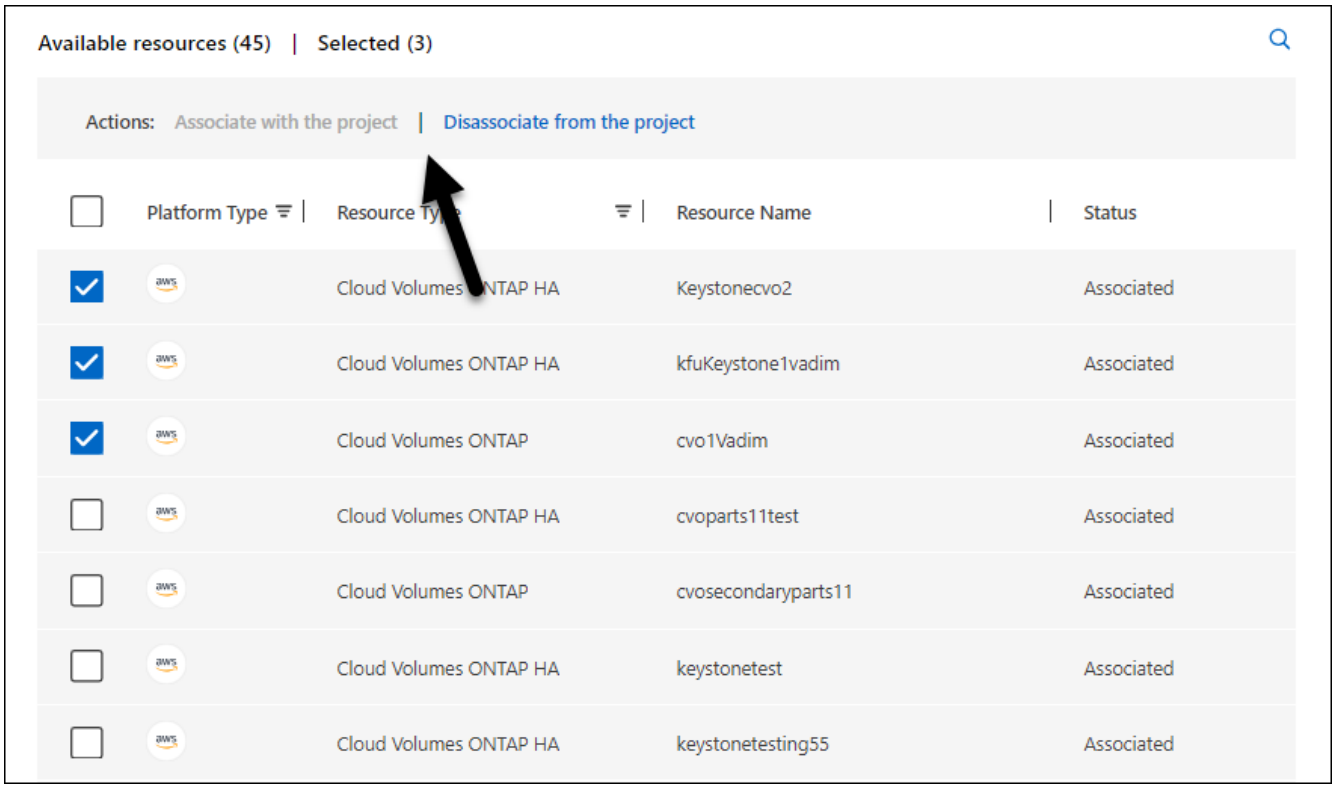
Modifier les ressources associées à un dossier ou à un projet

Vous pouvez modifier les ressources associées à un dossier ou à un projet en fonction de l'évolution des besoins de votre organisation.

Étapes

1. Depuis la page **Organisation**, accédez à un projet ou à un dossier dans le tableau, sélectionnez ••• puis sélectionnez **Modifier le dossier** ou **Modifier le projet**.
2. Sur la page **Modifier**, sélectionnez **Ressources**.

   Dans le tableau, la colonne **Statut** identifie les ressources associées au dossier ou au projet.
3. Sélectionnez les ressources que vous souhaitez associer ou dissocier.
4. En fonction des ressources que vous avez sélectionnées, choisissez **S'associer au projet** ou **Se dissocier du projet**.



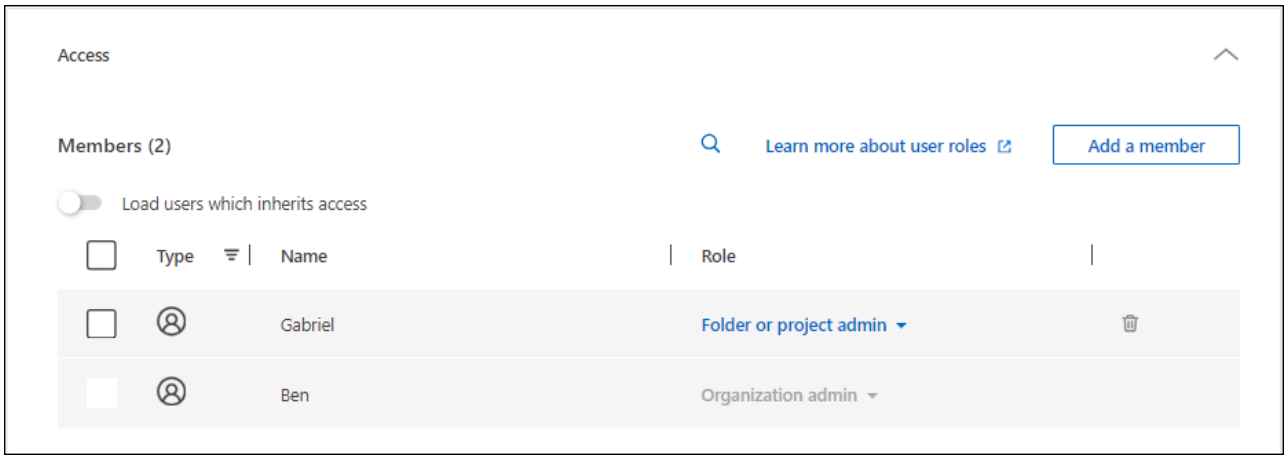
5. Sélectionnez **Appliquer**.

Afficher les membres associés à un dossier ou à un projet

Vous pouvez consulter les membres associés à un dossier ou à un projet depuis la page **Organisation**.

Étapes

1. Depuis la page **Organisation**, accédez à un projet ou à un dossier dans le tableau, sélectionnez ••• puis sélectionnez **Modifier le dossier** ou **Modifier le projet**.
2. Sur la page **Modifier**, sélectionnez **Accès** pour afficher la liste des membres qui ont accès au dossier ou au projet sélectionné.
   - Sélectionnez **Accès** pour afficher les membres qui ont accès au dossier ou au projet.



Modifier l’accès des membres à un dossier ou à un projet

Modifier les droits d’accès des membres pour contrôler l’accès aux ressources. N’oubliez pas que les rôles attribués au niveau du dossier sont hérités par tous les projets et dossiers enfants.

Vous ne pouvez pas modifier les droits d’accès des membres aux niveaux inférieurs s’ils sont hérités du niveau du dossier ou de l’organisation. Modifiez les autorisations du membre au niveau hiérarchique supérieur pour changer son accès. Vous pouvez également : "gérer les autorisations depuis la page Membres".

Étapes

1. Depuis la page **Organisation**, accédez à un projet ou à un dossier dans le tableau, sélectionnez ••• puis sélectionnez **Modifier le dossier** ou **Modifier le projet**.
2. Sur la page **Modifier**, sélectionnez **Accès** pour afficher la liste des membres qui ont accès au dossier ou au projet sélectionné.
3. Modifier l’accès des membres :
   - **Ajouter un membre** : Sélectionnez le membre que vous souhaitez ajouter au dossier ou au projet et attribuez-lui un rôle.
   - **Modifier le rôle d’un membre** : Pour tous les membres ayant un rôle autre qu’Administrateur de l’organisation, sélectionnez leur rôle existant, puis choisissez un nouveau rôle.
   - **Supprimer l’accès des membres** : pour les membres qui ont un rôle défini dans le dossier ou le projet que vous consultez, vous pouvez supprimer leur accès.
4. Sélectionnez **Appliquer**.

Informations connexes

- "En savoir plus sur l’identité et l’accès dans la NetApp Console"
- "Démarrer avec l’identité et l’accès"
- "En savoir plus sur l’API d’identité et d’accès"

Ajoutez des ressources aux dossiers et aux projets dans la NetApp Console.

Contrôlez l’accès des utilisateurs aux ressources en les ajoutant aux projets et aux dossiers de votre organisation NetApp Console . Accorder l’accès aux utilisateurs au niveau du projet.

Une *ressource* est une entité dont la console a connaissance, telle qu’une ressource de stockage, un agent de console ou une charge de travail de sauvegarde et de restauration.

Vous pouvez consulter et gérer les ressources depuis la page **Ressources** de la console.

types de ressources de la console

Vous pouvez associer plusieurs types de ressources aux projets de votre organisation NetApp Console :

Ressources de stockage

Les ressources de stockage sont le type de ressource le plus courant dans votre organisation et comprennent à la fois les systèmes de stockage sur site et les systèmes de stockage dans le cloud. Lorsque vous ajoutez un système de stockage à la console, vous pouvez l’ajouter à un dossier ou à un projet. En attendant, la console le considère comme non découvert et ne l’affiche pas sur la page **Ressources**.

Agents de console

Si vous avez utilisé un agent Console pour découvrir les systèmes de stockage, ajoutez cet agent au même dossier ou projet. Cela permet aux utilisateurs d'effectuer des fonctions activées par l'agent, telles que les services de données ou la gestion du stockage native de la console. Vous pouvez ajouter des agents à des dossiers ou à des projets depuis la page **Agents** de la Console. "Découvrez comment associer un agent de console à un dossier ou à un projet".

Abonnements Keystone

Si votre organisation dispose d'abonnements Keystone , vous pouvez les consulter sur la page **Ressources**. Vous pouvez associer des abonnements Keystone à des dossiers ou des projets afin de donner accès aux membres qui disposent des autorisations nécessaires pour ces dossiers ou projets.

Consultez les ressources de votre organisation

Vous pouvez afficher les ressources découvertes et non découvertes associées à votre organisation. Le système détecte les ressources de stockage et les marque comme non découvertes jusqu'à ce que vous les ajoutiez à la console.

> La console exclut les ressources Amazon FSx for NetApp ONTAP de la page Ressources car les utilisateurs ne peuvent pas les associer à un rôle. Vous pouvez consulter ces ressources sur la page **Systèmes** ou depuis la section Charges de travail.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Ressources**.
3. Sélectionnez **Recherche avancée et filtrage**.
4. Utilisez les options disponibles pour trouver une ressource :
   - **Rechercher par nom de ressource** : saisissez une chaîne de texte et sélectionnez **Ajouter**.
   - **Plateforme** : Sélectionnez une ou plusieurs plateformes, telles qu'Amazon Web Services.
   - **Ressources** : sélectionnez une ou plusieurs ressources, telles que Cloud Volumes ONTAP.
   - **Organisation, dossier ou projet** : sélectionnez l'organisation entière, un dossier spécifique ou un projet spécifique.
5. Sélectionnez **Rechercher**.

Associer une ressource à des dossiers et des projets

Associez une ressource à un dossier ou à un projet pour la rendre accessible aux membres disposant des autorisations nécessaires pour ce dossier ou ce projet.

Étapes

1. Depuis la page **Ressources**, accédez à une ressource dans le tableau, sélectionnez ••• puis sélectionnez **Associer à des dossiers ou des projets**.
2. Sélectionnez un dossier ou un projet, puis sélectionnez **Accepter**.
3. Pour associer un dossier ou un projet supplémentaire, sélectionnez **Ajouter un dossier ou un projet**, puis sélectionnez le dossier ou le projet.

   Notez que vous ne pouvez sélectionner que les dossiers et les projets pour lesquels vous disposez des autorisations d'administrateur.

4. Sélectionnez **Associer les ressources**.
    - Si vous avez associé la ressource à des projets, les membres disposant d'autorisations pour ces projets ont désormais la possibilité d'accéder à la ressource depuis la console.
    - Si vous avez associé la ressource à un dossier, un *administrateur de dossier ou de projet* peut désormais accéder à la ressource et l'associer à un projet dans le dossier. "En savoir plus sur l'association d'une ressource à un dossier".

Après avoir terminé

Si vous découvrez une ressource à l'aide d'un agent de console, associez l'agent de console au projet pour accorder l'accès. Dans le cas contraire, l'agent de console et sa ressource associée ne sont pas accessibles aux membres sans le rôle *Organization admin*.

"Découvrez comment associer un agent de console à un dossier ou à un projet".

Afficher les dossiers et les projets associés à une ressource

Vous pouvez afficher les dossiers et les projets associés à une ressource particulière.

Si vous avez besoin de savoir quels membres de l'organisation ont accès à la ressource, vous pouvez"afficher les membres qui ont accès aux dossiers et projets associés à la ressource" .

Étapes

1. Depuis la page **Ressources**, accédez à une ressource dans le tableau, sélectionnez••• puis sélectionnez **Afficher les détails**.

L'exemple suivant montre une ressource associée à un projet.

Pour voir quels membres de l'organisation ont accès à la ressource,"Afficher les membres ayant accès aux dossiers et projets associés" .

Supprimer une ressource d'un dossier ou d'un projet

Pour supprimer une ressource d'un dossier ou d'un projet, supprimez son association. Cela empêche les membres de gérer la ressource dans ce dossier ou ce projet.

Pour supprimer une ressource détectée de l'ensemble de l'organisation, accédez à la page **Systèmes** et supprimez le système.

Étapes

1. Depuis la page **Ressources**, accédez à une ressource dans le tableau, sélectionnez••• puis sélectionnez **Afficher les détails**.

2. Pour supprimer une ressource d'un dossier ou d'un projet, sélectionnez à côté du dossier ou du projet.
3. Sélectionnez **Supprimer** pour supprimer l'association.

Informations connexes

- "En savoir plus sur l'identité et l'accès dans la NetApp Console"
- "Démarrer avec l'identité et l'accès dans la NetApp Console"
- "En savoir plus sur l'API pour l'identité et l'accès"

Associer un agent de console à d'autres dossiers et projets

Associez les agents de la console à des projets spécifiques pour permettre la gestion des ressources et l'accès aux services de données. Pour que l'accès par l'équipe soit possible, les ressources découvertes via un agent de console doivent être associées à la fois à la ressource et à l'agent, et appartenir aux mêmes projets respectifs.

Les super administrateurs et les administrateurs d'organisation peuvent créer des agents et associer n'importe quel agent à n'importe quel projet ou dossier. Les administrateurs de dossiers ou de projets ne peuvent associer des agents existants qu'aux dossiers et projets pour lesquels ils disposent des autorisations nécessaires. "En savoir plus sur les actions qu'un *administrateur de dossier ou de projet* peut effectuer".

Étapes

1. Sélectionnez **Administration > Identité et accès** > **Agents**.
2. Dans le tableau, recherchez l'agent de console que vous souhaitez associer.

   Utilisez la recherche au-dessus du tableau pour trouver un agent de console spécifique ou filtrez le tableau par hiérarchie de ressources.

3. Pour afficher les dossiers et les projets liés à l'agent de la console, sélectionnez puis sélectionnez **Afficher les détails**.

   La page affiche les détails sur les dossiers et les projets associés à l'agent de console.

4. Sélectionnez **Associer au dossier ou au projet**.
5. Sélectionnez un dossier ou un projet, puis sélectionnez **Accepter**.
6. Pour associer l'agent de console à un dossier ou un projet supplémentaire, sélectionnez **Ajouter un dossier ou un projet**, puis sélectionnez le dossier ou le projet.
7. Sélectionnez **Agent associé**.

Après avoir terminé

Associez les ressources de l'agent de console aux mêmes dossiers et projets à partir de la page **Ressources**.

"Apprenez à associer une ressource à des dossiers et des projets" .

Informations connexes

- "En savoir plus sur les agents de la NetApp Console"
- "En savoir plus sur la gestion des identités et des accès de la NetApp Console"
- "Démarrer avec l'identité et l'accès"

- "En savoir plus sur l'API pour la gestion des identités et des accès"

Ajoutez des utilisateurs à votre organisation Console

Ajouter des utilisateurs à une organisation NetApp Console

Dans la console, vous accordez aux utilisateurs l'accès aux projets ou aux dossiers en fonction d'un rôle d'accès. Un *rôle d'accès* contient un ensemble d'autorisations qui permet à un membre (compte utilisateur ou compte de service) d'effectuer des actions spécifiques au niveau assigné de la hiérarchie des ressources.

Rôles d'accès requis

Super administrateur, administrateur d'organisation ou administrateur de dossier ou de projet (pour les dossiers et les projets qu'ils administrent). "En savoir plus sur les rôles d'accès".

Comprendre comment l'accès est accordé dans la NetApp Console

La NetApp Console utilise le contrôle d'accès basé sur les rôles (RBAC) pour gérer les autorisations. Attribuer des rôles aux utilisateurs individuellement ou par le biais de groupes fédérés. Chaque rôle définit les actions autorisées pour des ressources spécifiques.

Veuillez noter les points suivants concernant l'octroi d'accès dans la NetApp Console:

- Tous les utilisateurs doivent d'abord s'inscrire à la NetApp Console avant de pouvoir accéder aux ressources.
- Vous devez attribuer explicitement un rôle à chaque utilisateur dans la console avant qu'il puisse accéder aux ressources, même s'il est membre d'un groupe fédéré auquel un rôle a été attribué.
- Vous pouvez ajouter des comptes de service directement depuis la console et leur attribuer des rôles.

Ajoutez des membres à votre organisation

La NetApp Console prend en charge trois types de membres : les comptes d'utilisateurs, les comptes de service et les groupes fédérés.

Les utilisateurs doivent s'inscrire à la NetApp Console avant que vous puissiez les ajouter et leur attribuer un rôle, même s'ils font partie d'un groupe fédéré. Créez des comptes de service directement dans la console.

Pour accéder aux ressources, tous les membres doivent se voir attribuer au moins un rôle explicite.

Lors de l'ajout d'un membre, choisissez le niveau de ressource (organisation, dossier ou projet) et attribuez-lui un ou plusieurs rôles avec les autorisations nécessaires.

Ajouter un utilisateur

Les utilisateurs s'inscrivent à la NetApp Console, mais un administrateur d'organisation, de dossier ou de projet doit les ajouter à une organisation, un dossier ou un projet pour qu'ils puissent accéder aux ressources.

Avant de commencer :

L'utilisateur doit déjà s'être inscrit à la NetApp Console. S'ils ne se sont pas encore inscrits, dirigez-les vers "Inscrivez-vous à la NetApp Console."

Si vous ajoutez un utilisateur faisant partie d'un groupe fédéré, assurez-vous que cet utilisateur s'est déjà inscrit à la NetApp Console et qu'un rôle lui a été explicitement attribué dans la console. NetApp recommande d'attribuer un rôle d'accès minimal tel que celui de lecteur de l'organisation.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Membres**.
3. Sélectionnez **Ajouter un membre**.
4. Pour **Type de membre**, gardez **Utilisateur** sélectionné.
5. Pour **E-mail de l'utilisateur**, saisissez l'adresse e-mail de l'utilisateur associée à la connexion qu'il a créée.
6. Utilisez la section **Sélectionnez une organisation, un dossier ou un projet** pour choisir le niveau de votre hiérarchie de ressources pour lequel le membre doit disposer d'autorisations.

   Notez ce qui suit :

   - Vous pouvez sélectionner uniquement les dossiers et les projets pour lesquels vous disposez des autorisations.
   - Lorsque vous sélectionnez une organisation ou un dossier, vous accordez au membre l'autorisation d'accéder à tout son contenu.
   - Vous ne pouvez attribuer le rôle **Administrateur de l'organisation** qu'au niveau de l'organisation.
7. **Sélectionnez une catégorie** puis sélectionnez un **Rôle** qui fournit au membre des autorisations pour les ressources associées à l'organisation, au dossier ou au projet que vous avez sélectionné.

   "En savoir plus sur les rôles d'accès" .
8. Pour donner accès à davantage de dossiers, de projets ou de rôles, sélectionnez **Ajouter un rôle**, choisissez le dossier, le projet ou la catégorie de rôle, puis sélectionnez un rôle.
9. Sélectionnez **Ajouter**.

   La console envoie des instructions par courriel à l'utilisateur.

Ajouter un compte de service

Les comptes de service vous permettent d'automatiser les tâches et de vous connecter en toute sécurité aux API de la console. Choisissez un ID client et un secret pour les configurations simples, ou un JWT (JSON Web Token) pour une sécurité renforcée dans les environnements automatisés ou natifs du cloud. Choisissez la méthode qui répond à vos exigences de sécurité.

Avant de commencer :

Pour l'authentification JWT, préparez votre clé publique ou votre certificat.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Membres**.
3. Sélectionnez **Ajouter un membre**.

4. Pour **Type de membre**, sélectionnez **Compte de service**.
5. Saisissez un nom pour le compte de service.
6. Pour utiliser l'authentification JWT, sélectionnez **Utiliser l'authentification JWT par clé privée** et téléchargez votre clé ou certificat RSA public. Ignorez cette étape si vous utilisez un ID client et un secret.

   Votre certificat X.509. Il doit être au format PEM, CRT ou CER.

   a. Configurez les notifications d'expiration de votre certificat. Choisissez entre sept jours ou 30 jours. Les notifications d'expiration sont envoyées par e-mail et affichées dans la console aux utilisateurs ayant le rôle de super administrateur ou d'administrateur d'organisation.
7. Utilisez la section **Sélectionnez une organisation, un dossier ou un projet** pour choisir le niveau de votre hiérarchie de ressources pour lequel le membre doit disposer d'autorisations.

   Notez ce qui suit :

   - Vous ne pouvez sélectionner que les dossiers et les projets pour lesquels vous disposez d'autorisations.
   - La sélection d'une organisation ou d'un dossier accorde au membre des autorisations sur tout son contenu.
   - Vous ne pouvez attribuer le rôle **Administrateur de l'organisation** qu'au niveau de l'organisation.
8. Sélectionnez une **Catégorie**, puis un **Rôle** qui confère au membre les autorisations nécessaires pour accéder aux ressources de l'organisation, du dossier ou du projet que vous avez sélectionné.

   "En savoir plus sur les rôles d'accès" .
9. Pour donner accès à davantage de dossiers, de projets ou de rôles, sélectionnez **Ajouter un rôle**, choisissez le dossier, le projet ou la catégorie de rôle, puis sélectionnez un rôle.
10. Si vous n'avez pas choisi d'utiliser l'authentification JWT, téléchargez ou copiez l'ID client et le secret client.

    La console n'affiche le secret client qu'une seule fois. Copiez-le en lieu sûr ; vous pourrez le recréer plus tard si vous le perdez.
11. Si vous avez choisi l'authentification JWT, téléchargez ou copiez l'ID client et l'audience JWT. La console n'affiche ces informations qu'une seule fois et ne permet pas de les récupérer ultérieurement.
12. Sélectionnez **Fermer**.

Ajoutez un groupe fédéré à votre organisation

Vous pouvez ajouter un groupe fédéré de votre fournisseur d'identité (IdP) à votre organisation et lui attribuer un ou plusieurs rôles. Les membres du groupe fédéré héritent des rôles que vous attribuez au groupe dans la console.

Avant d'attribuer un rôle à un groupe fédéré, assurez-vous des points suivants :

- Configurez la fédération entre votre fournisseur d'identité et la console. "Apprenez à configurer une fédération."
- Le groupe doit déjà exister dans votre fournisseur d'identité et avoir un accès applicatif à la console.
- Les utilisateurs appartenant au groupe doivent déjà s'être inscrits à la NetApp Console et s'être vu attribuer explicitement un rôle dans la console. NetApp recommande d'attribuer un rôle d'accès minimal tel que celui de lecteur de l'organisation.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Membres**.
3. Sélectionnez **Ajouter un membre**.
4. Pour **Type de membre**, sélectionnez **Groupe fédéré**.
5. Sélectionnez la fédération dont le groupe est membre.
6. Pour **Nom du groupe**, veuillez saisir le nom exact du groupe dans votre fournisseur d'identité.
7. Utilisez la section **Sélectionnez une organisation, un dossier ou un projet** pour choisir le niveau de votre hiérarchie de ressources pour lequel le membre doit disposer d'autorisations.

   Notez ce qui suit :

   - Vous ne pouvez sélectionner que les dossiers et les projets pour lesquels vous disposez d'autorisations.
   - La sélection d'une organisation ou d'un dossier accorde au membre des autorisations sur tout son contenu.
   - Vous ne pouvez attribuer le rôle **Administrateur de l'organisation** qu'au niveau de l'organisation.
8. Sélectionnez une **Catégorie**, puis un **Rôle** qui confère au membre les autorisations nécessaires pour accéder aux ressources de l'organisation, du dossier ou du projet que vous avez sélectionné.

   "En savoir plus sur les rôles d'accès" .
9. Pour donner accès à davantage de dossiers, de projets ou de rôles, sélectionnez **Ajouter un rôle**, choisissez le dossier, le projet ou la catégorie de rôle, puis sélectionnez un rôle.

Informations connexes

- "En savoir plus sur la gestion des identités et des accès dans la NetApp Console"
- "Démarrer avec l'identité et l'accès"
- "Rôles d'accès à la NetApp Console"
- "En savoir plus sur l'API pour l'identité et l'accès"

Gérer l'accès des utilisateurs et la sécurité

Découvrez le contrôle d'accès basé sur les rôles (RBAC) de NetApp Console

Gérez l'accès des utilisateurs à la NetApp Console grâce au contrôle d'accès basé sur les rôles (RBAC), en attribuant des rôles prédéfinis au niveau de l'organisation, du dossier ou du projet. Chaque rôle octroie des autorisations spécifiques qui définissent les actions que les utilisateurs peuvent effectuer dans le cadre de leur rôle.

NetApp conçoit les rôles de console selon le principe du moindre privilège, de sorte que chaque rôle n'inclut que les autorisations nécessaires à ses tâches. Cette approche renforce la sécurité en limitant l'accès à ce dont chaque membre a besoin.

Après avoir organisé les ressources en dossiers et projets, attribuez aux membres de l'organisation un ou plusieurs rôles pour des dossiers ou projets spécifiques, leur permettant ainsi d'exercer uniquement leurs responsabilités.

Par exemple, vous pouvez attribuer à un membre le rôle d'administrateur de résilience aux ransomwares pour un niveau de projet spécifique, lui permettant d'effectuer des opérations de résilience aux ransomwares pour les ressources de ce projet, sans lui accorder un accès plus large à l'ensemble de l'organisation. Ce même utilisateur peut se voir attribuer ce rôle pour plusieurs projets au sein de votre organisation.

Vous pouvez attribuer aux utilisateurs plusieurs rôles pour un même périmètre ou pour des périmètres différents, en fonction de leurs responsabilités. Par exemple, une petite organisation pourrait confier la gestion de la résilience aux ransomwares et des tâches de sauvegarde et de restauration à un même utilisateur au niveau de l'organisation, tandis qu'une plus grande organisation pourrait affecter des utilisateurs différents à chaque rôle au niveau du projet.

Types de membres de l'organisation Console

Il existe trois types de membres dans une organisation NetApp Console : * *Comptes utilisateurs* : Utilisateurs individuels qui se connectent à la NetApp Console pour gérer les ressources. Les utilisateurs doivent s'inscrire à la NetApp Console avant de pouvoir être ajoutés à une organisation. * *Comptes de service* : Comptes non humains utilisés par les applications ou les services pour interagir avec la NetApp Console via des API. Vous pouvez ajouter des comptes de service directement à votre organisation Console. * *Groupes fédérés* : Groupes synchronisés depuis votre fournisseur d'identité (IdP) qui vous permettent de gérer collectivement l'accès de plusieurs utilisateurs. Chaque utilisateur d'un groupe fédéré doit s'être inscrit à la NetApp Console et avoir été ajouté à votre organisation avec un rôle d'accès avant de pouvoir accéder aux ressources accordées au groupe.

"Découvrez comment ajouter des membres à votre organisation."

Rôles prédéfinis dans la NetApp Console

La NetApp Console inclut des rôles prédéfinis que vous pouvez attribuer aux membres de l'organisation. Chaque rôle comprend des autorisations qui spécifient les actions qu'un membre peut effectuer dans le cadre qui lui est assigné (organisation, dossier ou projet).

Les rôles de la NetApp Console utilisent le principe du moindre privilège, qui garantit que les membres ne disposent que des autorisations nécessaires à leurs tâches, et catégorisent les rôles selon le type d'accès qu'ils fournissent :

- Rôles de la plateforme : Fournir les autorisations d'administration de la console
- Rôles des services de données : octroient des autorisations pour la gestion de services de données spécifiques, tels que la résilience aux ransomwares et la sauvegarde et la restauration.
- Rôles de l'application : Fournir les autorisations de gestion du stockage ainsi que d'audit des événements et alertes de la console.

Vous pouvez attribuer plusieurs rôles à un membre en fonction de ses responsabilités. Par exemple, vous pouvez attribuer à un membre à la fois le rôle d'administrateur de la résilience aux ransomwares et le rôle d'administrateur de la sauvegarde et de la récupération pour un projet spécifique.

"Découvrez les rôles prédéfinis disponibles dans la NetApp Console.".

Gérer l'accès des membres dans la NetApp Console

Gérez l'accès des membres dans votre organisation Console. Attribuer des rôles pour définir les autorisations. Supprimez les membres lorsqu'ils quittent l'entreprise.

Rôles d'accès requis

Super administrateur, administrateur d'organisation ou administrateur de dossier ou de projet (pour les dossiers et les projets qu'ils administrent). Lien : reference-iam-predefined-roles.html [En savoir plus sur les rôles d'accès].

Vous pouvez attribuer des rôles d'accès par projet ou par dossier. Par exemple, attribuez un rôle à un utilisateur pour deux projets spécifiques ou attribuez le rôle au niveau du dossier pour donner à un utilisateur le rôle d'administrateur de résilience aux ransomwares pour tous les projets d'un dossier.

Ajoutez vos dossiers et projets avant d'attribuer l'accès aux utilisateurs. "Apprenez à ajouter des dossiers et des projets."

Comprendre comment l'accès est accordé dans la NetApp Console

La NetApp Console utilise un modèle de contrôle d'accès basé sur les rôles (RBAC) pour gérer les autorisations des utilisateurs. Vous pouvez attribuer des rôles prédéfinis aux membres individuellement ou par le biais de groupes fédérés. Vous pouvez ajouter et attribuer des rôles aux comptes de service, ainsi qu'aux groupes fédérés. Chaque rôle définit les actions qu'un membre peut effectuer sur les ressources associées.

Veuillez noter les points suivants concernant l'octroi d'accès dans la NetApp Console:

- Tous les utilisateurs doivent d'abord s'inscrire à la NetApp Console avant de pouvoir accéder aux ressources.
- Vous devez attribuer explicitement un rôle à chaque utilisateur dans la console avant qu'il puisse accéder aux ressources, même s'il est membre d'un groupe fédéré auquel un rôle a été attribué.
- Vous pouvez ajouter des comptes de service directement depuis la console et leur attribuer des rôles.

Utilisation de l'héritage de rôles

Lorsque vous attribuez un rôle au niveau de l'organisation, du dossier ou du projet dans NetApp Console, ce rôle est automatiquement hérité par toutes les ressources du périmètre sélectionné. Par exemple, les rôles au niveau d'un dossier s'appliquent à tous les projets qu'il contient, tandis que les rôles au niveau d'un projet s'appliquent à toutes les ressources de ce projet.

Afficher les membres de l'organisation

Pour comprendre quelles ressources et autorisations sont disponibles pour un membre, vous pouvez afficher les rôles attribués au membre à différents niveaux de la hiérarchie des ressources de votre organisation."Découvrez comment utiliser les rôles pour contrôler l'accès aux ressources de la console."

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Membres**.

   Le tableau **Membres** répertorie les membres de votre organisation.

3. Depuis la page **Membres**, accédez à un membre dans le tableau, sélectionnez ••• puis sélectionnez **Afficher les détails**.

Afficher les rôles attribués à un membre

Vous pouvez vérifier les rôles qui leur sont actuellement attribués.

Si vous disposez du rôle *Administrateur de dossier ou de projet*, la page affiche tous les membres de

l'organisation. Cependant, vous ne pouvez afficher et gérer les autorisations des membres que pour les dossiers et les projets pour lesquels vous disposez d'autorisations. "En savoir plus sur les actions qu'un *administrateur de dossier ou de projet* peut effectuer" .

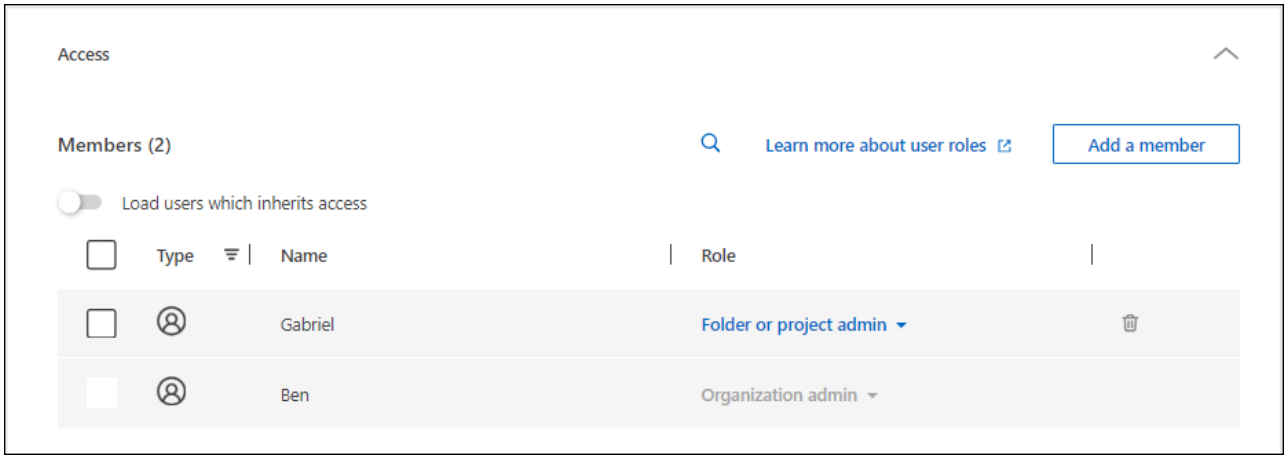
1. Depuis la page **Membres**, accédez à un membre dans le tableau, sélectionnez ••• puis sélectionnez **Afficher les détails**.
2. Dans le tableau, développez la ligne correspondante pour l'organisation, le dossier ou le projet dans lequel vous souhaitez afficher le rôle attribué au membre et sélectionnez **Afficher** dans la colonne **Rôle**.

Afficher les membres associés à un dossier ou à un projet

Vous pouvez consulter la liste des membres qui ont accès à un dossier ou à un projet spécifique.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Organisation**.
3. Depuis la page **Organisation**, accédez à un projet ou à un dossier dans le tableau, sélectionnez••• puis sélectionnez **Modifier le dossier** ou **Modifier le projet**.
   - Sélectionnez **Accès** pour afficher les membres qui ont accès au dossier ou au projet.



Attribuer ou modifier l'accès des membres

Une fois qu'un utilisateur s'inscrit à NetApp Console, vous pouvez l'ajouter à votre organisation et lui attribuer un rôle pour lui donner accès aux ressources. "Découvrez comment ajouter des membres à votre organisation."

Vous pouvez ajuster l'accès d'un membre en ajoutant ou en supprimant des rôles selon les besoins.

Ajouter un rôle d'accès à un membre

Vous attribuez généralement un rôle lorsque vous ajoutez un membre à votre organisation, mais vous pouvez le mettre à jour à tout moment en supprimant ou en ajoutant des rôles.

Vous pouvez attribuer à un utilisateur un rôle d'accès pour votre organisation, votre dossier ou votre projet.

Les membres peuvent occuper plusieurs rôles au sein d'un même projet et dans différents projets. Par exemple, les petites organisations peuvent attribuer tous les rôles d'accès disponibles au même utilisateur, tandis que les grandes organisations peuvent confier des tâches plus spécialisées à certains utilisateurs. Vous

pouvez également attribuer à un utilisateur le rôle d'administrateur de la résilience aux ransomwares au niveau de l'organisation. Dans cet exemple, l'utilisateur pourrait effectuer des tâches de résilience aux ransomwares sur tous les projets de votre organisation.

Votre stratégie de rôle d'accès doit s'aligner sur la manière dont vous avez organisé vos ressources NetApp .

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Membres**.
3. Sélectionnez l'un des onglets membres : **Utilisateurs**, **Comptes de service** ou **Groupes fédérés**.
4. Sélectionnez le menu actions ••• à côté du membre auquel vous souhaitez attribuer un rôle et sélectionnez **Ajouter un rôle**.
5. Pour ajouter un rôle, suivez les étapes dans la boîte de dialogue :
   - **Sélectionnez une organisation, un dossier ou un projet** : Choisissez le niveau de votre hiérarchie de ressources pour lequel le membre doit disposer d'autorisations.

     Si vous sélectionnez l'organisation ou un dossier, le membre aura des autorisations sur tout ce qui se trouve dans l'organisation ou le dossier.

   - **Sélectionnez une catégorie** : Choisissez une catégorie de rôle. "En savoir plus sur les rôles d'accès" .
   - Sélectionnez un **rôle** : choisissez un rôle qui fournit au membre des autorisations pour les ressources associées à l'organisation, au dossier ou au projet que vous avez sélectionné.
   - **Ajouter un rôle** : si vous souhaitez fournir l'accès à des dossiers ou projets supplémentaires au sein de votre organisation, sélectionnez **Ajouter un rôle**, spécifiez un autre dossier, projet ou catégorie de rôle, puis sélectionnez une catégorie de rôle et un rôle correspondant.
6. Sélectionnez **Ajouter de nouveaux rôles**.

Modifier le rôle attribué à un membre

Modifier les rôles d'un membre pour mettre à jour son accès.

> Les utilisateurs doivent avoir au moins un rôle qui leur est attribué. Vous ne pouvez pas supprimer tous les rôles d'un utilisateur. Si vous devez supprimer tous les rôles, vous devez supprimer l'utilisateur de votre organisation.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Membres**.
3. Sélectionnez l'un des onglets membres : **Utilisateurs**, **Comptes de service** ou **Groupes fédérés**.
4. Depuis la page **Membres**, accédez à un membre dans le tableau, sélectionnez ••• puis sélectionnez **Afficher les détails**.
5. Dans le tableau, développez la ligne correspondante pour l'organisation, le dossier ou le projet pour lequel vous souhaitez modifier le rôle attribué au membre et sélectionnez **Afficher** dans la colonne **Rôle** pour afficher les rôles attribués à ce membre.
6. Vous pouvez modifier un rôle existant pour un membre ou supprimer un rôle.
   a. Pour modifier le rôle d'un membre, sélectionnez **Modifier** à côté du rôle que vous souhaitez modifier. Vous ne pouvez modifier un rôle que pour un rôle appartenant à la même catégorie de rôle. Par

exemple, vous pouvez passer d'un rôle de service de données à un autre. Confirmer le changement.

b. Pour retirer le rôle d'un membre, sélectionnez à côté du rôle pour supprimer le rôle correspondant du membre. Il vous sera demandé de confirmer la suppression.

Supprimer un membre de votre organisation

Supprimez un membre s'il quitte votre organisation.

Lorsque vous supprimez un membre, le système révoque ses autorisations de console mais conserve ses comptes de console et de site de support NetApp .

membres fédérés

- Les utilisateurs fédérés perdent automatiquement l'accès à la NetApp Console lorsqu'ils sont supprimés de votre fournisseur d'identité. Mais vous devriez tout de même les supprimer de votre organisation Console pour que votre liste de membres reste à jour.
- Si vous supprimez un utilisateur d'un groupe fédéré dans votre fournisseur d'identité, il perd l'accès à la console associé à ce groupe. Ils conservent toutefois tous les accès associés à un rôle explicite qui leur est attribué dans la console.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Membres**.
3. Sélectionnez l'un des onglets membres : **Utilisateurs**, **Comptes de service** ou **Groupes fédérés**.
4. Depuis la page **Membres**, accédez à un membre dans le tableau, sélectionnez puis sélectionnez **Supprimer l'utilisateur**.
5. Confirmez que vous souhaitez supprimer le membre de votre organisation.

Sécurité des utilisateurs

Sécurisez l'accès des utilisateurs à votre organisation NetApp Console en gérant les paramètres de sécurité des membres. Vous pouvez réinitialiser les mots de passe des utilisateurs, gérer l'authentification multifacteurs (MFA) et recréer les informations d'identification des comptes de service.

Rôles d'accès requis

Super administrateur, administrateur d'organisation ou administrateur de dossier ou de projet (pour les dossiers et les projets qu'ils administrent). Lien : reference-iam-predefined-roles.html [En savoir plus sur les rôles d'accès].

Réinitialiser les mots de passe des utilisateurs (utilisateurs locaux uniquement)

Les administrateurs de l'organisation ne peuvent pas réinitialiser les mots de passe des utilisateurs locaux. Ils peuvent toutefois demander aux utilisateurs de réinitialiser eux-mêmes leurs mots de passe.

Indiquez à l'utilisateur de réinitialiser son mot de passe depuis la page de connexion de la console en sélectionnant **Mot de passe oublié ?**.

Cette option n'est pas disponible pour les utilisateurs appartenant à une organisation fédérée.

Gérer l’authentification multifacteur (MFA) d’un utilisateur

Si un utilisateur perd l’accès à son périphérique MFA, vous pouvez supprimer ou désactiver sa configuration MFA.

> L’authentification multifacteurs est uniquement disponible pour les utilisateurs locaux. Les utilisateurs fédérés ne peuvent pas activer l’authentification multifacteur.

Les utilisateurs doivent configurer à nouveau l’authentification multifacteur (MFA) lorsqu’ils se connectent après sa suppression. Si l’utilisateur perd temporairement l’accès à son dispositif MFA, il peut utiliser son code de récupération enregistré pour se connecter.

S’ils ne disposent pas de leur code de récupération, désactivez temporairement MFA pour autoriser la connexion. Lorsque vous désactivez l’authentification multifacteur pour un utilisateur, elle est désactivée pendant huit heures seulement, puis réactivée automatiquement. L’utilisateur est autorisé à se connecter une fois pendant cette période sans MFA. Après les huit heures, l’utilisateur doit utiliser MFA pour se connecter.

> Pour gérer l’authentification multifacteur d’un utilisateur, vous devez disposer d’une adresse e-mail dans le même domaine que l’utilisateur concerné.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Membres**.

   Le tableau **Membres** répertorie les membres de votre organisation.

3. Depuis la page **Membres**, accédez à un membre dans le tableau, sélectionnez ••• puis sélectionnez **Gérer l’authentification multifacteur**.
4. Choisissez de supprimer ou de désactiver la configuration MFA de l’utilisateur.

Recréer les informations d’identification pour un compte de service

Vous pouvez créer de nouveaux identifiants pour un service si vous les perdez ou si vous devez les mettre à jour.

La création de nouveaux identifiants supprime les anciens. Vous ne pouvez pas utiliser les anciens identifiants.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Membres**.
3. Dans le tableau **Membres**, accédez à un compte de service, sélectionnez ••• puis sélectionnez **Recréer les secrets**.
4. Sélectionnez **Recréer**.
5. Téléchargez ou copiez l’ID client et le secret client.

   La console n’affiche le secret client qu’une seule fois. Veillez à le copier ou à le télécharger et à le conserver en lieu sûr.

Rôles d’accès à la NetApp Console

En savoir plus sur les rôles d’accès à la NetApp Console

La gestion des identités et des accès (IAM) dans la NetApp Console fournit des rôles prédéfinis que vous pouvez attribuer aux membres de votre organisation à différents niveaux de votre hiérarchie de ressources. Avant d’attribuer ces rôles, vous devez comprendre les autorisations incluses dans chaque rôle. Les rôles se répartissent dans les catégories suivantes : plateforme, application et service de données.

Rôles de la plateforme

Les rôles de plate-forme accordent des autorisations d’administration à la NetApp Console , y compris l’attribution de rôles et la gestion des utilisateurs. La console a plusieurs rôles de plate-forme.

Rôle de la plateforme	Responsabilités
"Administrateur de l’organisation"	Permet à un utilisateur d’accéder sans restriction à tous les projets et dossiers au sein d’une organisation, d’ajouter des membres à n’importe quel projet ou dossier, ainsi que d’effectuer n’importe quelle tâche et d’utiliser n’importe quel service de données qui n’a pas de rôle explicite associé. Les utilisateurs dotés de ce rôle gèrent votre organisation en créant des dossiers et des projets, en attribuant des rôles, en ajoutant des utilisateurs et en gérant des systèmes s’ils disposent des informations d’identification appropriées. Il s’agit du seul rôle d’accès qui peut créer des agents de console.
"Administrateur de dossier ou de projet"	Permet à un utilisateur un accès illimité aux projets et dossiers attribués. Ils peuvent ajouter des membres aux dossiers ou aux projets qu’ils gèrent, ainsi qu’effectuer n’importe quelle tâche et utiliser n’importe quel service de données ou application sur les ressources du dossier ou du projet qui leur est attribué. Les administrateurs de dossier ou de projet ne peuvent pas créer d’agents de console.
"Administrateur de la fédération"	Permet à un utilisateur de créer et de gérer des fédérations avec la console, ce qui permet l’authentification unique (SSO).
"Téléspectateur de la Fédération"	Permet à un utilisateur de visualiser les fédérations existantes avec la console. Impossible de créer ou de gérer des fédérations.
"Administrateur de partenariat"	Permet à un utilisateur de créer et de gérer des partenariats.
"Visionneuse de partenariat"	Permet à un utilisateur de visualiser les partenariats existants. Impossible de créer ou de gérer des partenariats.
"Super administrateur"	Donne à l’utilisateur un sous-ensemble de rôles d’administrateur. Ce rôle est conçu pour les petites organisations qui n’ont peut-être pas besoin de répartir les responsabilités de la console entre plusieurs utilisateurs.
"Super spectateur"	Donne à l’utilisateur un sous-ensemble de rôles de spectateur. Ce rôle est conçu pour les petites organisations qui n’ont peut-être pas besoin de répartir les responsabilités de la console entre plusieurs utilisateurs.

Rôles d’application

Voici une liste des rôles dans la catégorie d’application. Chaque rôle accorde des autorisations spécifiques

dans le cadre de son périmètre désigné. Les utilisateurs sans le rôle d'application ou de plateforme requis ne peuvent pas accéder à l'application correspondante.

Rôle de l'application	Responsabilités
"Administrateur Google Cloud NetApp Volumes"	Les utilisateurs disposant du rôle Google Cloud NetApp Volumes peuvent découvrir et gérer Google Cloud NetApp Volumes.
"Visionneuse de Google Cloud NetApp Volumes"	Les utilisateurs disposant du rôle utilisateur Google Cloud NetApp Volumes peuvent consulter Google Cloud NetApp Volumes.
"Administrateur Keystone"	Les utilisateurs disposant du rôle d'administrateur Keystone peuvent créer des demandes de service. Permet aux utilisateurs de surveiller et d'afficher l'utilisation, les ressources et les détails d'administration au sein du locataire Keystone auquel ils accèdent.
"Visionneuse Keystone"	Les utilisateurs disposant du rôle de visualiseur Keystone NE PEUVENT PAS créer de demandes de service. Permet aux utilisateurs de surveiller et d'afficher la consommation, les actifs et les informations administratives au sein du locataire Keystone auquel ils accèdent.
Rôle de configuration du médiateur ONTAP	Les comptes de service dotés du rôle de configuration de médiateur ONTAP peuvent créer des demandes de service. Ce rôle est requis dans un compte de service pour configurer une instance du"Médiateur cloud ONTAP" .
"Analyste de soutien aux opérations"	Fournit un accès aux alertes et aux outils de surveillance et la possibilité de saisir et de gérer les cas d'assistance.
"Administrateur de stockage"	Administrez les fonctions de santé et de gouvernance du stockage, découvrez les ressources de stockage, ainsi que modifiez et supprimez les systèmes existants.
"Visionneuse de stockage"	Affichez l'état du stockage et les fonctions de gouvernance, ainsi que les ressources de stockage précédemment découvertes. Impossible de découvrir, de modifier ou de supprimer les systèmes de stockage existants.
"Spécialiste de la santé du système"	Administrer les fonctions de stockage, de santé et de gouvernance, toutes les autorisations de l'administrateur de stockage, sauf l'impossibilité de modifier ou de supprimer les systèmes existants.

Rôles des services de données

Voici une liste des rôles dans la catégorie de service de données. Chaque rôle accorde des autorisations spécifiques dans le cadre de son périmètre désigné. Les utilisateurs qui ne disposent pas du rôle de service de données requis ou d'un rôle de plateforme ne pourront pas accéder au service de données.

Rôle du service de données	Responsabilités
"Super administrateur de sauvegarde et de récupération"	Effectuez toutes les actions dans NetApp Backup and Recovery.
"Administrateur de sauvegarde et de récupération"	Effectuez des sauvegardes sur des snapshots locaux, répliquez-les sur un stockage secondaire et sauvegardez-les sur un stockage d'objets.
"Administrateur de restauration de sauvegarde et de récupération"	Restaurer les charges de travail dans la sauvegarde et la récupération.

Rôle du service de données	Responsabilités
"Administrateur de clone de sauvegarde et de récupération"	Cloner des applications et des données dans la sauvegarde et la récupération.
"Visionneuse de sauvegarde et de récupération"	Afficher les informations de sauvegarde et de récupération.
"Administrateur de reprise après sinistre"	Effectuez toutes les actions dans le service NetApp Disaster Recovery .
"Administrateur de basculement de reprise après sinistre"	Effectuer des basculements et des migrations.
"Administrateur d'application de reprise après sinistre"	Créez des plans de réplication, modifiez les plans de réplication et démarrez les basculements de test.
"Visionneuse de reprise après sinistre"	Afficher uniquement les informations.
Visionneuse de classification	Permet aux utilisateurs d'afficher les résultats de l'analyse de NetApp Data Classification . Les utilisateurs disposant de ce rôle peuvent afficher les informations de conformité et générer des rapports pour les ressources auxquelles ils sont autorisés à accéder. Ces utilisateurs ne peuvent pas activer ou désactiver l'analyse des volumes, des buckets ou des schémas de base de données. La classification ne comporte pas de rôle d'administrateur.
"Administrateur de la résilience aux ransomwares"	Gérez les actions sur les onglets Protéger, Alertes, Récupérer, Paramètres et Rapports de NetApp Ransomware Resilience.
"Visionneuse de résilience aux ransomwares"	Affichez les données de charge de travail, affichez les données d'alerte, téléchargez les données de récupération et téléchargez les rapports dans Ransomware Resilience.
"Comportement utilisateur de Ransomware Resilience administrateur"	Configurez, gérez et affichez la détection, les alertes et la surveillance des comportements suspects des utilisateurs dans Ransomware Resilience.
"Visualiseur de comportement utilisateur de Ransomware Resilience"	Affichez les alertes et les informations sur les comportements suspects des utilisateurs dans Ransomware Resilience.
Administrateur SnapCenter	Offre la possibilité de sauvegarder des instantanés à partir de clusters ONTAP sur site à l'aide de NetApp Backup and Recovery pour les applications. Un membre disposant de ce rôle peut effectuer les actions suivantes : * Effectuer n'importe quelle action à partir de Sauvegarde et récupération > Applications * Gérer tous les systèmes dans les projets et dossiers pour lesquels il dispose d'autorisations * Utiliser tous les services de la NetApp Console SnapCenter n'a pas de rôle de visualiseur.

Liens connexes

- "En savoir plus sur la gestion des identités et des accès de la NetApp Console"
- "Démarrer avec NetApp Console IAM"
- "Gérer les membres de la NetApp Console et leurs autorisations"
- "En savoir plus sur l'API pour NetApp Console IAM"

Rôles d’accès à la plateforme NetApp Console

Attribuez des rôles de plateforme aux utilisateurs pour accorder des autorisations de gestion de la NetApp Console, attribuer des rôles, ajouter des utilisateurs, créer des agents de console et gérer les fédérations.

Exemple de rôles organisationnels pour une grande organisation multinationale

XYZ Corporation organise l’accès au stockage des données par région (Amérique du Nord, Europe et Asie-Pacifique), offrant un contrôle régional avec une surveillance centralisée.

L'**administrateur de l’organisation** dans la console de la société XYZ crée une organisation initiale et des dossiers distincts pour chaque région. L'**administrateur de dossier ou de projet** de chaque région organise les projets (avec les ressources associées) dans le dossier de la région.

Les administrateurs régionaux dotés du rôle **Administrateur de dossier ou de projet** gèrent activement leurs dossiers en ajoutant des ressources et des utilisateurs. Ces administrateurs régionaux peuvent également ajouter, supprimer ou renommer les dossiers et les projets qu’ils gèrent. L'**administrateur de l’organisation** hérite des autorisations pour toutes les nouvelles ressources, maintenant ainsi la visibilité de l’utilisation du stockage dans l’ensemble de l’organisation.

Au sein de la même organisation, un utilisateur se voit attribuer le rôle **Administrateur de la fédération** pour gérer la fédération de l’organisation avec son IdP d’entreprise. Cet utilisateur peut ajouter ou supprimer des organisations fédérées, mais ne peut pas gérer les utilisateurs ou les ressources au sein de l’organisation. L'**administrateur de l’organisation** attribue à un utilisateur le rôle de **spectateur de fédération** pour vérifier l’état de la fédération et afficher les organisations fédérées.

Les tableaux suivants indiquent les actions que chaque rôle de plate-forme de console peut effectuer.

Rôles d’administration de l’organisation

Tâche	Administrateur de l’organisation	Administrateur de dossier ou de projet
Créer des agents	Oui	Non
Créer, modifier ou supprimer des systèmes depuis la console (ajouter ou découvrir des systèmes)	Oui	Oui
Créer des dossiers et des projets, y compris la suppression	Oui	Non
Renommer les dossiers et projets existants	Oui	Oui
Attribuer des rôles et ajouter des utilisateurs	Oui	Oui
Associer des ressources à des dossiers et des projets	Oui	Oui
Associer des agents à des dossiers et des projets	Oui	Non
Supprimer les agents des dossiers et des projets	Oui	Non
Gérer les agents (modifier les certificats, les paramètres, etc.)	Oui	Non
Gérer les informations d’identification depuis Administration > Informations d’identification	Oui	Oui
Créer, gérer et afficher les fédérations	Oui	Non

Tâche	Administrateur de l'organisation	Administrateur de dossier ou de projet
Inscrivez-vous au support et soumettez des cas via la console	Oui	Oui
Utiliser des services de données qui ne sont pas associés à un rôle d'accès explicite	Oui	Oui
Afficher la page d'audit et les notifications	Oui	Oui

Rôles de la Fédération

Tâche	Administrateur de la fédération	Téléspectateur de la Fédération
Créer une fédération	Oui	Non
Vérifier un domaine	Oui	Non
Ajouter un domaine à une fédération	Oui	Non
Désactiver et supprimer les fédérations	Oui	Non
Fédérations de tests	Oui	Non
Voir les fédérations et leurs coordonnées	Oui	Oui

Rôles de partenariat

Tâche	Administrateur de partenariat	Visionneuse de partenariat
Peut créer un partenariat	Oui	Non
Attribuer des rôles aux membres partenaires	Oui	Non
Peut ajouter des membres à un partenariat	Oui	Non
Peut afficher les détails du partenariat de l'organisation	Oui	Oui

Rôles de super administrateur et de spectateur

Le rôle **Super administrateur** offre un accès complet pour gérer les fonctionnalités de la console, le stockage et les services de données. Ce rôle convient à ceux qui supervisent l'administration et la gouvernance. En revanche, le rôle **Super spectateur** offre un accès en lecture seule, idéal pour les auditeurs ou les parties prenantes qui ont besoin de visibilité sans apporter de modifications.

Les organisations doivent utiliser l'accès **Super administrateur** avec parcimonie afin de minimiser les risques de sécurité et de se conformer au principe du moindre privilège. La plupart des organisations devraient attribuer des rôles précis avec uniquement les autorisations nécessaires pour réduire les risques et améliorer l'auditabilité.

Exemple de super rôles

ABC Corporation dispose d'une petite équipe de cinq personnes qui utilisent la NetApp Console pour les services de données et la gestion du stockage. Au lieu de distribuer plusieurs rôles, ils attribuent le rôle de **Super administrateur** à deux membres seniors de l'équipe qui gèrent toutes les tâches administratives, y

compris la gestion des utilisateurs et la configuration des ressources. Les trois membres restants de l'équipe se voient attribuer le rôle de **Super visualiseur**, leur permettant de surveiller l'état du stockage et l'état du service de données sans pouvoir modifier les paramètres.

Rôle	Rôles hérités
Super administrateur	• Administrateur de l'organisation • Administrateur de dossier ou de projet • Administrateur de la fédération • Administrateur de partenariat • Administrateur de la résilience aux ransomwares • Administrateur de reprise après sinistre • Super administrateur de sauvegarde • Administrateur de stockage • Administrateur Keystone • Administrateur Google Cloud NetApp Volumes
Super spectateur	• Visionneuse d'organisation • Téléspectateur de la Fédération • Visionneuse de partenariat • Visionneuse de résilience aux ransomwares • Visionneuse de reprise après sinistre • Visionneuse de sauvegarde • Visionneuse de stockage • Visionneuse Keystone • Visionneuse de Google Cloud NetApp Volumes

Rôles d'application

Rôles Google Cloud NetApp Volumes dans la NetApp Console

Vous pouvez attribuer le rôle suivant aux utilisateurs pour leur donner accès aux Google Cloud NetApp Volumes dans la NetApp Console.

Google Cloud NetApp Volumes utilise le rôle suivant :

- * Administrateur Google Cloud NetApp Volumes * : découvrez et gérez les Google Cloud NetApp Volumes dans la console.
- * Visionneuse de Google Cloud NetApp Volumes * : Affichez les Google Cloud NetApp Volumes dans la console.

Rôles d'accès Keystone dans la NetApp Console

Les rôles Keystone donnent accès aux tableaux de bord Keystone et permettent aux utilisateurs de visualiser et de gérer leur abonnement Keystone . Il existe deux rôles Keystone : administrateur Keystone et visualiseur Keystone . La principale différence entre les deux rôles réside dans les actions qu'ils peuvent entreprendre dans Keystone. Le rôle d'administrateur Keystone est le seul rôle autorisé à créer des demandes de service ou à modifier des abonnements.

Exemple de rôles Keystone dans la NetApp Console

La société XYZ dispose de quatre ingénieurs de stockage de différents départements qui consultent les informations d'abonnement Keystone . Bien que tous ces utilisateurs doivent surveiller l'abonnement Keystone , seul le chef d'équipe est autorisé à faire des demandes de service. Trois membres de l'équipe se voient attribuer le rôle de * visualiseur Keystone **, tandis que le chef d'équipe se voit attribuer le rôle d'** administrateur Keystone * afin qu'il existe un point de contrôle sur les demandes de service pour l'entreprise.

Le tableau suivant indique les actions que chaque rôle Keystone peut effectuer.

Fonctionnalité et action	Administrateur Keystone	Visionneuse Keystone
Afficher les onglets suivants : Abonnement, Ressources, Surveillance et Administration	Oui	Oui
* Page d'abonnement Keystone * :		
Voir les abonnements	Oui	Oui
Modifier ou renouveler les abonnements	Oui	Non
* Page des ressources Keystone * :		
Afficher les actifs	Oui	Oui
Gérer les actifs	Oui	Non
* Page d'alertes Keystone * :		
Afficher les alertes	Oui	Oui
Gérer les alertes	Oui	Non
Créer des alertes pour soi-même	Oui	Oui
* Licenses and subscriptions*:		

Fonctionnalité et action	Administrateur Keystone	Visionneuse Keystone
Peut afficher les licences et les abonnements	Oui	Oui
* Page des rapports Keystone * :		
Télécharger les rapports	Oui	Oui
Gérer les rapports	Oui	Oui
Créer des rapports pour soi-même	Oui	Oui
Demandes de service:		
Créer des demandes de service	Oui	Non
Afficher les demandes de service créées par n'importe quel utilisateur au sein de l'organisation	Oui	Oui

Rôle d'accès d'analyste de support opérationnel pour la NetApp Console

Vous pouvez attribuer le rôle d'analyste de support opérationnel aux utilisateurs afin de leur donner accès aux alertes et à la surveillance. Les utilisateurs disposant de ce rôle peuvent également ouvrir des cas d'assistance.

Analyste de soutien opérationnel

Tâche	Peut effectuer
Gérez vos propres informations d'identification utilisateur depuis Paramètres > Informations d'identification	Oui
Voir les ressources découvertes	Oui
Inscrivez-vous au support et soumettez des cas via la console	Oui
Afficher la page d'audit et les notifications	Oui
Afficher, télécharger et configurer les alertes	Oui

Rôles d'accès au stockage pour la NetApp Console

Vous pouvez attribuer les rôles suivants aux utilisateurs pour leur donner accès aux fonctionnalités de gestion du stockage dans la NetApp Console. Vous pouvez attribuer aux utilisateurs un rôle administratif pour gérer le stockage ou un rôle de spectateur pour la surveillance.

Ces rôles ne sont pas disponibles à partir de l'API de partenariat de la NetApp Console .

Les administrateurs peuvent attribuer des rôles de stockage aux utilisateurs pour les ressources et fonctionnalités de stockage suivantes :

Ressources de stockage :

- Clusters ONTAP sur site
- StorageGRID
- E-Series

Services et fonctionnalités de la console :

- Conseiller numérique
- Mises à jour logicielles
- Planification du cycle de vie
- Durabilité

Exemple de rôles de stockage dans la NetApp Console

XYZ Corporation, une société multinationale, dispose d'une grande équipe d'ingénieurs et d'administrateurs de stockage. Ils permettent à cette équipe de gérer les actifs de stockage pour leurs régions tout en limitant l'accès aux tâches principales de la console telles que la gestion des utilisateurs, la création d'agents et la gestion des licences.

Au sein d'une équipe de 12 personnes, deux utilisateurs se voient attribuer le rôle **Storage viewer** qui leur permet de surveiller les ressources de stockage associées aux projets de console auxquels ils sont affectés. Les neuf autres se voient attribuer le rôle **Administrateur de stockage** qui inclut la possibilité de gérer les mises à jour logicielles, d'accéder à ONTAP System Manager via la console, ainsi que de découvrir les ressources de stockage (ajouter des systèmes). Une personne de l'équipe se voit attribuer le rôle de **Spécialiste de l'état du système** afin qu'elle puisse gérer l'état des ressources de stockage dans sa région, mais pas modifier ni supprimer de systèmes. Cette personne peut également effectuer des mises à jour logicielles sur les ressources de stockage pour les projets qui lui sont attribués.

L'organisation dispose de deux utilisateurs supplémentaires avec le rôle **Administrateur de l'organisation** qui peuvent gérer tous les aspects de la console, y compris la gestion des utilisateurs, la création d'agents et la gestion des licences, ainsi que de plusieurs utilisateurs avec le rôle **Administrateur de dossier ou de projet** qui peuvent effectuer des tâches d'administration de la console pour les dossiers et les projets auxquels ils sont affectés.

Le tableau suivant présente les actions effectuées par chaque rôle de stockage.

Fonctionnalité et action	Administrateur de stockage	Spécialiste de la santé du système	Visionneuse de stockage
Gestion du stockage:			
Découvrir de nouvelles ressources (créer des systèmes)	Oui	Oui	Non
Afficher les systèmes découverts	Oui	Oui	Non

Fonctionnalité et action	Administrateur de stockage	Spécialiste de la santé du système	Visionneuse de stockage
Supprimer les systèmes de la console	Oui	Non	Non
Modifier les systèmes	Oui	Non	Non
Créer des agents	Non	Non	Non
Conseiller numérique			
Afficher toutes les pages et fonctions	Oui	Oui	Oui
* Licenses and subscriptions*			
Afficher toutes les pages et fonctions	Non	Non	Non
Mises à jour logicielles			
Afficher la page de destination et les recommandations	Oui	Oui	Oui
Examiner les recommandations de versions potentielles et les principaux avantages	Oui	Oui	Oui
Afficher les détails de mise à jour d'un cluster	Oui	Oui	Oui
Exécutez les vérifications préalables à la mise à jour et téléchargez le plan de mise à niveau	Oui	Oui	Oui
Installer les mises à jour logicielles	Oui	Oui	Non
Planification du cycle de vie			
Examiner l'état de la planification des capacités	Oui	Oui	Oui
Choisissez l'action suivante (meilleure pratique, niveau)	Oui	Non	Non
Hiérarchisez les données froides vers le stockage cloud et libérez de l'espace de stockage	Oui	Oui	Non
Configurer des rappels	Oui	Oui	Oui
Durabilité			
Afficher le tableau de bord et les recommandations	Oui	Oui	Oui
Télécharger les données du rapport	Oui	Oui	Oui

Fonctionnalité et action	Administrateur de stockage	Spécialiste de la santé du système	Visionneuse de stockage
Modifier le pourcentage d'atténuation du carbone	Oui	Oui	Non
Recommandations de correction	Oui	Oui	Non
Reporter les recommandations	Oui	Oui	Non
Accès du gestionnaire système			
Peut saisir des informations d'identification	Oui	Oui	Non
Informations d'identification			
Informations d'identification de l'utilisateur	Oui	Oui	Non

Rôles des services de données

Rôles de NetApp Backup and Recovery dans la NetApp Console

Vous pouvez attribuer les rôles suivants aux utilisateurs pour leur donner accès à NetApp Backup and Recovery dans la console. Les rôles de sauvegarde et de récupération vous offrent la flexibilité d'attribuer aux utilisateurs un rôle spécifique aux tâches qu'ils doivent accomplir au sein de votre organisation. La manière dont vous attribuez les rôles dépend de votre propre entreprise et de vos pratiques de gestion du stockage.

Le service utilise les rôles suivants qui sont spécifiques à NetApp Backup and Recovery.

- **Super administrateur de sauvegarde et de récupération** : effectuez toutes les actions dans NetApp Backup and Recovery.
- **Administrateur de sauvegarde et de récupération de sauvegarde** : effectuez des sauvegardes sur des snapshots locaux, répliquez sur un stockage secondaire et sauvegardez sur des actions de stockage d'objets dans NetApp Backup and Recovery.
- **Administrateur de restauration de sauvegarde et de récupération** : Restaurez les charges de travail à l'aide de NetApp Backup and Recovery.
- **Administrateur de clonage de sauvegarde et de récupération** : Clonez des applications et des données à l'aide de NetApp Backup and Recovery.
- **Visionneuse de sauvegarde et de récupération** : affichez les informations dans NetApp Backup and Recovery, mais n'effectuez aucune action.

Pour plus de détails sur tous les rôles d'accès à la NetApp Console , consultez "la documentation de configuration et d'administration de la console" .

Rôles utilisés pour les actions courantes

Le tableau suivant indique les actions que chaque rôle de NetApp Backup and Recovery peut effectuer pour toutes les charges de travail.

Fonctionnalité et action	Super administrateur de sauvegarde et de récupération	Sauvegarde et récupération de l'administrateur de sauvegarde	Administrateur de restauration de sauvegarde et de récupération	Administrateur de clone de sauvegarde et de récupération	Visionneuse de sauvegarde et de récupération
Ajouter, modifier ou supprimer des hôtes	Oui	Non	Non	Non	Non
Installer des plugins	Oui	Non	Non	Non	Non
Ajouter des informations d'identification (hôte, instance, vCenter)	Oui	Non	Non	Non	Non
Afficher le tableau de bord et tous les onglets	Oui	Oui	Oui	Oui	Oui
Démarrer un essai gratuit	Oui	Non	Non	Non	Non
Lancer la découverte des charges de travail	Non	Oui	Oui	Oui	Non
Afficher les informations de licence	Oui	Oui	Oui	Oui	Oui
Activer la licence	Oui	Non	Non	Non	Non
Voir les hôtes	Oui	Oui	Oui	Oui	Oui
Horaires:					
Activer les horaires	Oui	Oui	Oui	Oui	Non
Suspendre les horaires	Oui	Oui	Oui	Oui	Non
Politiques et protection:					
Voir les plans de protection	Oui	Oui	Oui	Oui	Oui
Créer, modifier ou supprimer des plans de protection	Oui	Oui	Non	Non	Non
Restaurer les charges de travail	Oui	Non	Oui	Non	Non

Fonctionnalité et action	Super administrateur de sauvegarde et de récupération	Sauvegarde et récupération de l'administrateur de sauvegarde	Administrateur de restauration de sauvegarde et de récupération	Administrateur de clone de sauvegarde et de récupération	Visionneuse de sauvegarde et de récupération
Créer, diviser ou supprimer des clones	Oui	Non	Non	Oui	Non
Créer, modifier ou supprimer une politique	Oui	Oui	Non	Non	Non
Rapports:					
Afficher les rapports	Oui	Oui	Oui	Oui	Oui
Créer des rapports	Oui	Oui	Oui	Oui	Non
Supprimer les rapports	Oui	Non	Non	Non	Non
Importer depuis SnapCenter et gérer l'hôte:					
Afficher les données SnapCenter importées	Oui	Oui	Oui	Oui	Oui
Importer des données depuis SnapCenter	Oui	Oui	Non	Non	Non
Gérer (migrer) l'hôte	Oui	Oui	Non	Non	Non
Configurer les paramètres:					
Configurer le répertoire des journaux	Oui	Oui	Oui	Non	Non
Associer ou supprimer les informations d'identification d'instance	Oui	Oui	Oui	Non	Non
Seaux:					
Afficher les seaux	Oui	Oui	Oui	Oui	Oui
Créer, modifier ou supprimer un bucket	Oui	Oui	Non	Non	Non

Rôles utilisés pour les actions spécifiques à la charge de travail

Le tableau suivant indique les actions que chaque rôle NetApp Backup and Recovery peut effectuer pour des charges de travail spécifiques.

Charges de travail Kubernetes

Ce tableau indique les actions que chaque rôle de NetApp Backup and Recovery peut effectuer pour les actions spécifiques aux charges de travail Kubernetes.

Fonctionnalité et action	Super administrateur de sauvegarde et de récupération	Sauvegarde et récupération de l'administrateur de sauvegarde	Administrateur de restauration de sauvegarde et de récupération	Visionneuse de sauvegarde et de récupération
Afficher les clusters, les espaces de noms, les classes de stockage et les ressources API	Oui	Oui	Oui	Oui
Ajouter de nouveaux clusters Kubernetes	Oui	Oui	Non	Non
Mettre à jour les configurations de cluster	Oui	Non	Non	Non
Supprimer les clusters de la gestion	Oui	Non	Non	Non
Voir les candidatures	Oui	Oui	Oui	Oui
Créer et définir de nouvelles applications	Oui	Oui	Non	Non
Mettre à jour les configurations des applications	Oui	Oui	Non	Non
Supprimer les applications de la gestion	Oui	Oui	Non	Non
Afficher les ressources protégées et l'état de la sauvegarde	Oui	Oui	Oui	Oui
Créez des sauvegardes et protégez les applications avec des politiques	Oui	Oui	Non	Non
Déprotégez les applications et supprimez les sauvegardes	Oui	Oui	Non	Non

Fonctionnalité et action	Super administrateur de sauvegarde et de récupération	Sauvegarde et récupération de l'administrateur de sauvegarde	Administrateur de restauration de sauvegarde et de récupération	Visionneuse de sauvegarde et de récupération
Afficher les points de récupération et les résultats de la visionneuse de ressources	Oui	Oui	Oui	Oui
Restaurer les applications à partir des points de récupération	Oui	Non	Oui	Non
Afficher les politiques de sauvegarde Kubernetes	Oui	Oui	Oui	Oui
Créer des politiques de sauvegarde Kubernetes	Oui	Oui	Oui	Non
Mettre à jour les politiques de sauvegarde	Oui	Oui	Oui	Non
Supprimer les politiques de sauvegarde	Oui	Oui	Oui	Non
Afficher les hooks d'exécution et les sources des hooks	Oui	Oui	Oui	Oui
Créer des hooks d'exécution et des sources de hook	Oui	Oui	Oui	Non
Mettre à jour les hooks d'exécution et les sources des hooks	Oui	Oui	Oui	Non
Supprimer les hooks d'exécution et les sources de hook	Oui	Oui	Oui	Non
Afficher les modèles de hook d'exécution	Oui	Oui	Oui	Oui
Créer des modèles de hook d'exécution	Oui	Oui	Oui	Non
Mettre à jour les modèles de hook d'exécution	Oui	Oui	Oui	Non
Supprimer les modèles de hook d'exécution	Oui	Oui	Oui	Non

Fonctionnalité et action	Super administrateur de sauvegarde et de récupération	Sauvegarde et récupération de l'administrateur de sauvegarde	Administrateur de restauration de sauvegarde et de récupération	Visionneuse de sauvegarde et de récupération
Afficher les tableaux de bord récapitulatifs et analytiques de la charge de travail	Oui	Oui	Oui	Oui
Afficher les buckets et les cibles de stockage StorageGRID	Oui	Oui	Oui	Oui

Rôles de NetApp Disaster Recovery dans la NetApp Console

Vous pouvez attribuer les rôles suivants aux utilisateurs pour leur donner accès à NetApp Disaster Recovery dans la console. Les rôles de reprise après sinistre vous offrent la flexibilité d'attribuer aux utilisateurs un rôle spécifique aux tâches qu'ils doivent accomplir au sein de votre organisation. La manière dont vous attribuez les rôles dépend de votre propre entreprise et de vos pratiques de gestion du stockage.

La reprise après sinistre utilise les rôles suivants :

- **Administrateur de reprise après sinistre** : Effectuez toutes les actions.
- **Administrateur de basculement de reprise après sinistre** : Effectuer le basculement et les migrations.
- **Administrateur d'application de récupération après sinistre** : Créer des plans de réplication. Modifier les plans de réplication. Démarrer les tests de basculement.
- **Visionneuse de récupération après sinistre** : Afficher uniquement les informations.

Le tableau suivant indique les actions que chaque rôle peut effectuer.

Fonctionnalité et action	Administrateur de reprise après sinistre	Administrateur de basculement de reprise après sinistre	Administrateur d'application de reprise après sinistre	Visionneuse de reprise après sinistre
Afficher le tableau de bord et tous les onglets	Oui	Oui	Oui	Oui
Démarrer un essai gratuit	Oui	Non	Non	Non
Lancer la découverte des charges de travail	Oui	Non	Non	Non
Afficher les informations de licence	Oui	Oui	Oui	Oui
Activer la licence	Oui	Non	Oui	Non
Dans l'onglet Sites :				

Fonctionnalité et action	Administrateur de reprise après sinistre	Administrateur de basculement de reprise après sinistre	Administrateur d'application de reprise après sinistre	Visionneuse de reprise après sinistre
Voir les sites	Oui	Oui	Oui	Oui
Ajouter, modifier ou supprimer des sites	Oui	Non	Non	Non
Dans l'onglet Plans de réplication :				
Afficher les plans de réplication	Oui	Oui	Oui	Oui
Afficher les détails du plan de réplication	Oui	Oui	Oui	Oui
Créer ou modifier des plans de réplication	Oui	Oui	Oui	Non
Créer des rapports	Oui	Non	Non	Non
Voir les instantanés	Oui	Oui	Oui	Oui
Effectuer des tests de basculement	Oui	Oui	Oui	Non
Effectuer des basculements	Oui	Oui	Non	Non
Effectuer des restaurations automatiques	Oui	Oui	Non	Non
Effectuer des migrations	Oui	Oui	Non	Non
Dans l'onglet Groupes de ressources :				
Afficher les groupes de ressources	Oui	Oui	Oui	Oui
Créer, modifier ou supprimer des groupes de ressources	Oui	Non	Oui	Non
Dans l'onglet Suivi des tâches :				
Voir les offres d'emploi	Oui	Non	Oui	Oui
Annuler les emplois	Oui	Oui	Oui	Non

Rôles d'accès à la résilience contre les ransomwares pour la NetApp Console

Les rôles Ransomware Resilience permettent aux utilisateurs d'accéder à NetApp Ransomware Resilience. Ransomware Resilience prend en charge les rôles suivants :

Rôles de base

- Administrateur de la résilience aux ransomwares : configurez les paramètres de résilience aux ransomwares ; examinez et répondez aux alertes de chiffrement.
- Visionneuse de résilience aux ransomwares : affichez les incidents de chiffrement, les rapports et les paramètres de découverte

Rôles d'activité de comportement de l'utilisateur"Détection d'activité utilisateur suspecte" les alertes offrent une visibilité sur les données telles que les événements d'activité des fichiers ; ces alertes incluent les noms de fichiers et les actions de fichiers (telles que la lecture, l'écriture, la suppression, le renommage) effectuées par l'utilisateur. Pour limiter la visibilité de ces données, seuls les utilisateurs disposant de ces rôles peuvent gérer ou visualiser ces alertes.

- Administrateur du comportement utilisateur de Ransomware Resilience - Activez la détection d'activité utilisateur suspecte, enquêtez et répondez aux alertes d'activité utilisateur suspecte
- Visualiseur de comportement utilisateur Ransomware Resilience : affichez les alertes d'activité utilisateur suspecte

> Les rôles de comportement utilisateur ne sont pas des rôles autonomes ; ils sont conçus pour être ajoutés aux rôles d'administrateur ou de spectateur de Ransomware Resilience. Pour plus d'informations, voir Rôles de comportement des utilisateurs.

Consultez les tableaux suivants pour des descriptions détaillées de chaque rôle.

Rôles de base

Le tableau suivant décrit les actions disponibles pour les rôles d'administrateur et de visualiseur de Ransomware Resilience.

Fonctionnalité et action	Administrateur de la résilience aux ransomwares	Visionneuse de résilience aux ransomwares
Afficher le tableau de bord et tous les onglets	Oui	Oui
Sur le tableau de bord, mettre à jour le statut de la recommandation	Oui	Non
Démarrer un essai gratuit	Oui	Non
Lancer la découverte des charges de travail	Oui	Non
Initier la redécouverte des charges de travail	Oui	Non
Dans l'onglet Protéger :		
Ajouter, modifier ou supprimer des plans de protection pour les politiques de *chiffrement*	Oui	Non
Protéger les charges de travail	Oui	Non
Identifier l'exposition aux données sensibles grâce à la classification des données	Oui	Non

Fonctionnalité et action	Administrateur de la résilience aux ransomwares	Visionneuse de résilience aux ransomwares
Liste des plans de protection et des détails	Oui	Oui
Liste des groupes de protection	Oui	Oui
Afficher les détails du groupe de protection	Oui	Oui
Créer, modifier ou supprimer des groupes de protection	Oui	Non
Télécharger les données	Oui	Oui
Dans l'onglet Alertes :		
Afficher les alertes de chiffrement et les détails des alertes	Oui	Oui
Modifier le statut de l'incident de chiffrement	Oui	Non
Marquer l'alerte de chiffrement pour la récupération	Oui	Non
Afficher les détails de l'incident de chiffrement	Oui	Oui
Ignorer ou résoudre les incidents de chiffrement	Oui	Non
Obtenez la liste complète des fichiers impactés par l'événement de chiffrement	Oui	Non
Télécharger les données d'alertes d'événements de chiffrement	Oui	Oui
Bloquer l'utilisateur (avec la configuration de l'agent Workload Security)	Oui	Non
Dans l'onglet Récupérer :		
Télécharger les fichiers impactés par l'événement de chiffrement	Oui	Non
Restaurer la charge de travail à partir d'un événement de chiffrement	Oui	Non
Télécharger les données de récupération à partir de l'événement de chiffrement	Oui	Oui
Télécharger les rapports d'événements de chiffrement	Oui	Oui
Dans l'onglet Paramètres :		
Ajouter ou modifier des destinations de sauvegarde	Oui	Non

Fonctionnalité et action	Administrateur de la résilience aux ransomwares	Visionneuse de résilience aux ransomwares
Lister les destinations de sauvegarde	Oui	Oui
Afficher les cibles SIEM connectées	Oui	Oui
Ajouter ou modifier des cibles SIEM	Oui	Non
Configurer l'exercice de préparation	Oui	Non
Démarrer, réinitialiser ou modifier l'exercice de préparation	Oui	Non
Examen de l'état de préparation de l'exercice	Oui	Oui
Mettre à jour la configuration de la découverte	Oui	Non
Afficher la configuration de la découverte	Oui	Oui
Dans l'onglet Rapports :		
Télécharger les rapports	Oui	Oui

Rôles de comportement des utilisateurs

Pour configurer les paramètres de comportement utilisateur suspect et répondre aux alertes, un utilisateur doit disposer du rôle d'administrateur du comportement utilisateur Ransomware Resilience. Pour afficher uniquement les alertes de comportement utilisateur suspect, un utilisateur doit disposer du rôle d'observateur de comportement utilisateur Ransomware Resilience.

Les rôles de comportement des utilisateurs doivent être conférés aux utilisateurs disposant de privilèges d'administrateur ou de spectateur Ransomware Resilience existants qui ont besoin d'accéder à"paramètres et alertes d'activité utilisateur suspecte" . Un utilisateur disposant du rôle d'administrateur Ransomware Resilience, par exemple, doit recevoir le rôle d'administrateur du comportement utilisateur Ransomware Resilience pour configurer les agents d'activité utilisateur et bloquer ou débloquer les utilisateurs. Le rôle d'administrateur du comportement utilisateur de Ransomware Resilience ne doit pas être conféré à un visualiseur de Ransomware Resilience.

Pour activer la détection d'activité utilisateur suspecte, vous devez disposer du rôle d'administrateur de l'organisation de la console.

Le tableau suivant décrit les actions disponibles pour les rôles d'administrateur et de spectateur du comportement utilisateur de Ransomware Resilience.

Fonctionnalité et action	Comportement utilisateur de Ransomware Resilience administrateur	Visualiseur de comportement utilisateur de Ransomware Resilience
Dans l'onglet Paramètres :		
Créer, modifier ou supprimer un agent d'activité utilisateur	Oui	Non
Créer ou supprimer un connecteur d'annuaire utilisateur	Oui	Non
Mettre en pause ou reprendre la collecte de données	Oui	Non
Exécuter un exercice de préparation aux violations de données	Oui	Non
Dans l'onglet Protéger :		
Ajouter, modifier ou supprimer des plans de protection pour les politiques de *comportement utilisateur suspect*	Oui	Non
Dans l'onglet Alertes :		
Afficher les alertes d'activité des utilisateurs et les détails des alertes	Oui	Oui
Modifier le statut de l'incident d'activité de l'utilisateur	Oui	Non
Marquer l'alerte d'activité de l'utilisateur pour la récupération	Oui	Non
Afficher les détails des incidents liés à l'activité de l'utilisateur	Oui	Oui
Rejeter ou résoudre les incidents d'activité des utilisateurs	Oui	Non
Obtenez la liste complète des fichiers impactés par l'utilisateur suspect	Oui	Oui
Télécharger les données d'alertes d'événements d'activité utilisateur	Oui	Oui
Bloquer ou débloquer l'utilisateur	Oui	Non
Dans l'onglet Récupérer :		
Télécharger les fichiers impactés par l'événement d'activité utilisateur	Oui	Non
Restaurer la charge de travail à partir d'un événement d'activité utilisateur	Oui	Non
Télécharger les données de récupération à partir de l'événement d'activité de l'utilisateur	Oui	Oui

Fonctionnalité et action	Comportement utilisateur de Ransomware Resilience administrateur	Visualiseur de comportement utilisateur de Ransomware Resilience
Télécharger les rapports d'événements d'activité utilisateur	Oui	Oui

API d'identité et d'accès

ID d'organisation et de projet

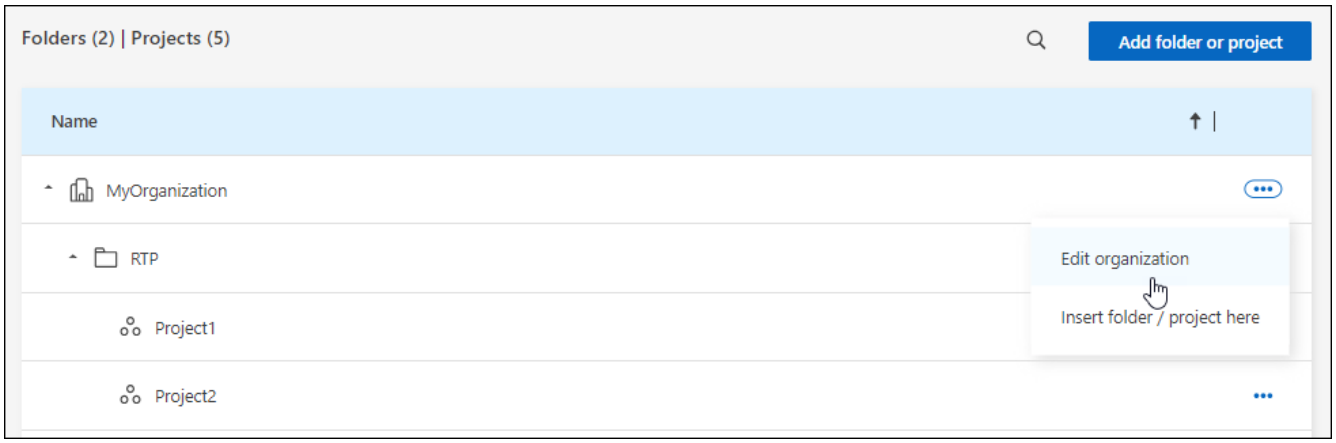
Votre organisation NetApp Console possède un nom et un ID. Vous pouvez choisir un nom pour votre organisation afin de l'identifier. Vous devrez peut-être également récupérer l'ID de l'organisation pour certaines intégrations.

Renommez votre organisation

Vous pouvez renommer votre organisation. Ceci est utile si vous soutenez plus d'une organisation.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Organisation**.
3. Depuis la page **Organisation**, accédez à la première ligne du tableau, sélectionnez ••• puis sélectionnez **Modifier l'organisation**.



4. Saisissez un nouveau nom d'organisation et sélectionnez **Appliquer**.

Obtenir l'ID de l'organisation

L'ID d'organisation est utilisé pour certaines intégrations avec la console.

Vous pouvez afficher l'ID de l'organisation à partir de la page Organisations et le copier dans le presse-papiers selon vos besoins.

Étapes

1. Sélectionnez **Administration > Identité et accès** > **Organisation**.
2. Sur la page **Organisation**, recherchez l'ID de votre organisation dans la barre de résumé et copiez-le dans

le presse-papiers. Vous pouvez l'enregistrer pour une utilisation ultérieure ou le copier directement à l'endroit où vous en avez besoin.

Obtenir l'ID d'un projet

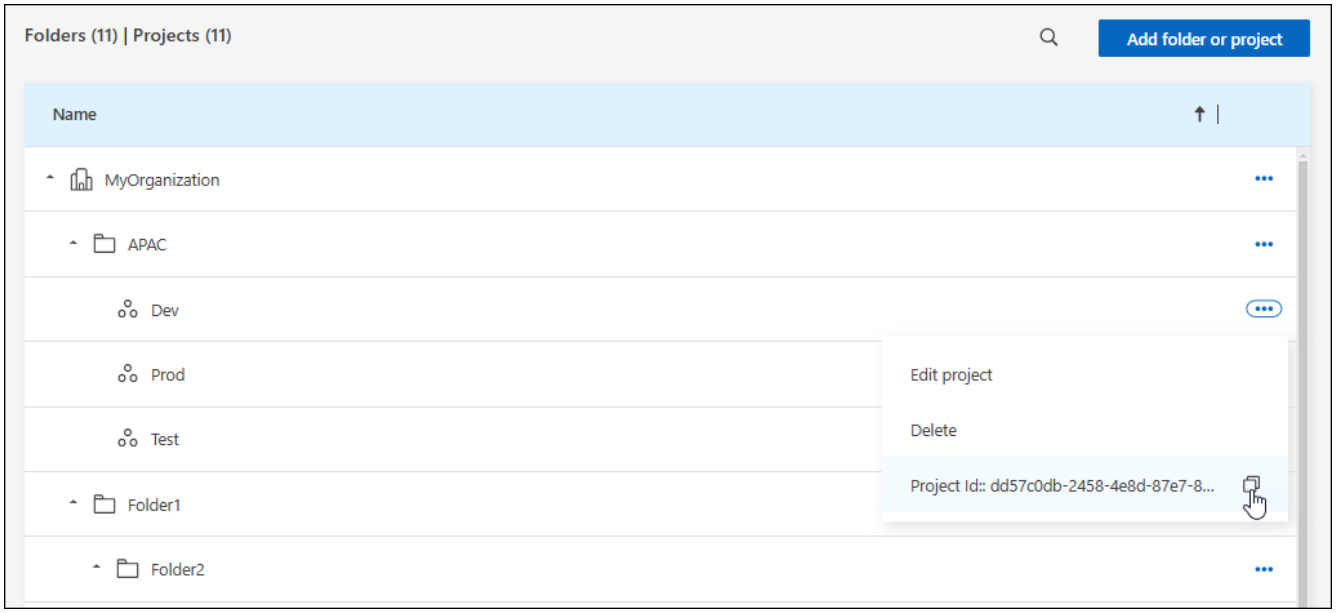
Vous devrez obtenir l'ID d'un projet si vous utilisez l'API. Par exemple, lors de la création d'un système Cloud Volumes ONTAP .

Étapes

1. Depuis la page **Organisation**, accédez à un projet dans le tableau et sélectionnez •••

   L'ID du projet s'affiche.

2. Pour copier l'ID, sélectionnez le bouton Copier.



Informations connexes

- "En savoir plus sur la gestion des identités et des accès"
- "Démarrer avec l'identité et l'accès"
- "En savoir plus sur l'API pour l'identité et l'accès"

Sécurité et conformité

Fédération d'identité

Activer l'authentification unique en utilisant la fédération d'identité avec la NetApp Console

L'authentification unique (fédération) simplifie le processus de connexion et améliore la sécurité en permettant aux utilisateurs de se connecter à la NetApp Console à l'aide de leurs informations d'identification d'entreprise. Vous pouvez activer l'authentification unique (SSO) avec votre fournisseur d'identité (IdP) ou avec le site de support NetApp .

Rôle requis

Administrateur d'organisation, administrateur de fédération, visualiseur de fédération."En savoir plus sur les rôles d'accès."

Authentification unique avec le site d'assistance NetApp

La fédération avec le site de support NetApp permet aux utilisateurs de se connecter à la console, à Active IQ Digital Advisor et à d'autres applications associées à l'aide des mêmes informations d'identification.

> Si vous vous fédérez avec le site de support NetApp , vous ne pouvez pas également vous fédérer avec votre fournisseur de gestion des identités d'entreprise. Choisissez celui qui convient le mieux à votre organisation.

Étapes

1. Téléchargez et complétez le "Formulaire de demande de fédération NetApp" .
2. Soumettez le formulaire à l'adresse e-mail indiquée dans le formulaire.

   L'équipe de support NetApp examine et traite votre demande.

Authentification unique avec votre fournisseur d'identité

Vous pouvez configurer une connexion fédérée avec votre fournisseur d'identité pour activer l'authentification unique (SSO) pour la console. Le processus implique la configuration de votre fournisseur d'identité pour qu'il approuve NetApp en tant que fournisseur de services, puis la création de la connexion dans la console.

> Si vous avez précédemment configuré la fédération à l'aide de NetApp Cloud Central (une application externe à la console), vous devez importer votre fédération à l'aide de la page Fédération pour la gérer dans la console."Apprenez à importer votre fédération."

Fournisseurs d'identité pris en charge

NetApp prend en charge les protocoles et fournisseurs d'identité suivants pour la fédération :

Protocoles

- Fournisseurs d'identité SAML (Security Assertion Markup Language)
- Services de fédération Active Directory (AD FS)

Fournisseurs d'identité

- Identifiant Microsoft Entra
- PingFédéré

Fédération avec le flux de travail de la NetApp Console

NetApp prend uniquement en charge l'authentification unique initiée par le fournisseur de services (SP). Vous devez d'abord configurer le fournisseur d'identité pour qu'il approuve NetApp en tant que fournisseur de services. Ensuite, vous pouvez créer une connexion dans la console qui utilise la configuration du fournisseur d'identité.

Vous pouvez fédérer avec votre domaine de messagerie ou avec un autre domaine que vous possédez. Pour fédérer avec un domaine différent de votre domaine de messagerie, vérifiez d'abord que vous êtes propriétaire du domaine.

1 Vérifiez votre domaine (si vous n'utilisez pas votre domaine de messagerie)

Pour fédérer avec un domaine différent de votre domaine de messagerie, vérifiez que vous en êtes propriétaire. Vous pouvez fédérer votre domaine de messagerie sans aucune étape supplémentaire.

2 Configurez votre IdP pour faire confiance à NetApp en tant que fournisseur de services

Configurez votre fournisseur d'identité pour qu'il fasse confiance à NetApp en créant une nouvelle application et en fournissant des détails tels que l'URL ACS, l'ID d'entité ou d'autres informations d'identification. Les informations sur le fournisseur de services varient selon le fournisseur d'identité. Reportez-vous donc à la documentation de votre fournisseur d'identité spécifique pour plus de détails. Vous devrez travailler avec votre administrateur IdP pour terminer cette étape.

3 Créer la connexion fédérée dans la console

Fournissez l'URL ou le fichier de métadonnées SAML de votre fournisseur d'identité pour créer la connexion. Ces informations sont utilisées pour établir la relation de confiance entre la console et votre fournisseur d'identité. Les informations que vous fournissez dépendent de l'IdP que vous utilisez. Par exemple, si vous utilisez Microsoft Entra ID, vous devez fournir l'ID client, le secret et le domaine.

4 Testez votre fédération dans la console

Testez votre connexion fédérée avant de l'activer. Utilisez l'option de test sur la page Fédération dans la console pour vérifier que votre utilisateur de test peut s'authentifier avec succès. Si le test réussit, vous pouvez activer la connexion.

5 Activez votre connexion dans la console

Une fois la connexion activée, les utilisateurs peuvent se connecter à la console à l'aide de leurs informations d'identification d'entreprise.

Consultez le sujet de votre protocole ou IdP respectif pour commencer :

- "Configurer une connexion fédérée avec AD FS"
- "Configurer une connexion fédérée avec Microsoft Entra ID"
- "Configurer une connexion fédérée avec PingFederate"
- "Configurer une connexion fédérée avec un fournisseur d'identité SAML"

Vérification de domaine

Vérifiez le domaine de messagerie pour votre connexion fédérée

Si vous souhaitez vous fédérer avec un domaine différent de votre domaine de messagerie, vous devez d'abord vérifier que vous êtes propriétaire du domaine. Vous ne pouvez utiliser que des domaines vérifiés pour la fédération.

Rôles requis

Le rôle d'administrateur de fédération est requis pour créer et gérer des fédérations. Le spectateur de la

Fédération peut voir la page de la Fédération."En savoir plus sur les rôles d'accès."

La vérification de votre domaine implique l'ajout d'un enregistrement TXT aux paramètres DNS de votre domaine. Cet enregistrement est utilisé pour prouver que vous êtes propriétaire du domaine et permet à la NetApp Console d'approuver le domaine pour la fédération. Vous devrez peut-être vous coordonner avec votre administrateur informatique ou réseau pour terminer cette étape.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Fédération** pour afficher la page **Fédérations**.
3. Sélectionnez **Configurer une nouvelle fédération**.
4. Sélectionnez **Vérifier la propriété du domaine**.
5. Saisissez le domaine que vous souhaitez vérifier et sélectionnez **Continuer**.
6. Copiez l'enregistrement TXT fourni.
7. Accédez aux paramètres DNS de votre domaine et configurez la valeur TXT qui a été fournie en tant qu'enregistrement TXT pour votre domaine. Travaillez avec votre administrateur informatique ou réseau si nécessaire.
8. Une fois l'enregistrement TXT ajouté, revenez à la console et sélectionnez **Vérifier**.

Configurer les fédérations

Fédérer la NetApp Console avec les services de fédération Active Directory (AD FS)

Fédérez vos services de fédération Active Directory (AD FS) avec la NetApp Console pour activer l'authentification unique (SSO) pour la NetApp Console. Cela permet aux utilisateurs de se connecter à la console en utilisant leurs identifiants d'entreprise.

Rôles requis

Le rôle d'administrateur de fédération est requis pour créer et gérer des fédérations. Le spectateur de la Fédération peut voir la page de la Fédération."En savoir plus sur les rôles d'accès."

Vous pouvez vous fédérer avec votre IdP d'entreprise ou avec le site de support NetApp . NetApp recommande de choisir l'un ou l'autre, mais pas les deux.

NetApp prend uniquement en charge l'authentification unique initiée par le fournisseur de services (SP). Tout d'abord, configurez le fournisseur d'identité pour qu'il approuve la NetApp Console en tant que fournisseur de services. Ensuite, créez une connexion dans la console en utilisant la configuration de votre fournisseur d'identité.

Vous pouvez configurer la fédération avec votre serveur AD FS pour activer l'authentification unique (SSO) pour la NetApp Console. Le processus implique la configuration de votre AD FS pour approuver la console en tant que fournisseur de services, puis la création de la connexion dans la NetApp Console.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Fédération** pour afficher la page **Fédérations**.
3. Sélectionnez **Configurer une nouvelle fédération**.
4. Entrez les détails de votre domaine :

a. Choisissez si vous souhaitez utiliser un domaine vérifié ou votre domaine de messagerie. Le domaine de messagerie est le domaine associé au compte avec lequel vous êtes connecté.

b. Entrez le nom de la fédération que vous configurez.

c. Si vous choisissez un domaine vérifié, sélectionnez le domaine dans la liste.

5. Sélectionnez **Suivant**.
6. Pour votre méthode de connexion, choisissez **Protocole** puis sélectionnez **Active Directory Federation Services (AD FS)**.
7. Sélectionnez **Suivant**.
8. Créez une approbation de partie de confiance sur votre serveur AD FS. Vous pouvez utiliser PowerShell ou le configurer manuellement sur votre serveur AD FS. Consultez la documentation AD FS pour plus de détails sur la création d'une approbation de partie de confiance.

   a. Créez la confiance à l'aide de PowerShell en utilisant le script suivant :

   ```
   (new-object Net.WebClient -property @{Encoding = [Text.Encoding]
   ::UTF8}).DownloadString("https://raw.github.com/auth0/AD FS-
   auth0/master/AD FS.ps1") | iex
   AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-
   cloud-account.auth0.com/login/callback"
   ```

   b. Vous pouvez également créer l'approbation manuellement dans la console de gestion AD FS. Utilisez les valeurs suivantes de la NetApp Console lors de la création de l'approbation :

      - Lors de la création de l'identifiant de confiance de confiance, utilisez la valeur **YOUR_TENANT** : `netapp-cloud-account`
      - Lorsque vous sélectionnez **Activer la prise en charge de WS-Federation**, utilisez la valeur **YOUR_AUTH0_DOMAIN** : `netapp-cloud-account.auth0.com`

   c. Après avoir créé l'approbation, copiez l'URL des métadonnées à partir de votre serveur AD FS ou téléchargez le fichier de métadonnées de fédération. Vous aurez besoin de cette URL ou de ce fichier pour terminer la connexion dans la console.

   NetApp recommande d'utiliser l'URL des métadonnées pour permettre à la NetApp Console de récupérer automatiquement la dernière configuration AD FS. Si vous téléchargez le fichier de métadonnées de fédération, vous devrez le mettre à jour manuellement dans la NetApp Console chaque fois que des modifications sont apportées à votre configuration AD FS.

9. Revenez à la console et sélectionnez **Suivant** pour créer la connexion.
10. Créez la connexion avec AD FS.

    a. Saisissez l'**URL AD FS** que vous avez copiée à partir de votre serveur AD FS à l'étape précédente ou téléchargez le fichier de métadonnées de fédération que vous avez téléchargé à partir de votre serveur AD FS.

11. Sélectionnez **Créer une connexion**. La création de la connexion peut prendre quelques secondes.
12. Sélectionnez **Suivant**.
13. Sélectionnez **Tester la connexion** pour tester votre connexion. Vous êtes dirigé vers une page de connexion pour votre serveur IdP. Connectez-vous avec vos identifiants IdP. Une fois connecté, retournez à la console pour activer la connexion.

Lorsque vous utilisez la console en mode restreint, copiez l'URL dans une fenêtre de navigateur incognito ou dans un navigateur distinct pour vous connecter à votre fournisseur d'identité.

14. Dans la console, sélectionnez **Suivant** pour consulter la page récapitulative.
15. Configurer les notifications.

    Choisissez entre sept jours ou 30 jours. Le système envoie par courriel des notifications d'expiration et les affiche dans la console à tout utilisateur ayant les rôles suivants : super administrateur, administrateur d'organisation, administrateur de fédération et visionneur de fédération.

16. Vérifiez les détails de la fédération, puis sélectionnez **Activer la fédération**.
17. Sélectionnez **Terminer** pour terminer le processus.

Une fois la fédération activée, les utilisateurs se connectent à la NetApp Console à l'aide de leurs identifiants d'entreprise.

Fédérer la NetApp Console avec Microsoft Entra ID

Fédérez-vous avec votre fournisseur IdP Microsoft Entra ID pour activer l'authentification unique (SSO) pour la NetApp Console. Cela permet aux utilisateurs de se connecter en utilisant leurs identifiants d'entreprise.

Rôles requis

Le rôle d'administrateur de fédération est requis pour créer et gérer des fédérations. Le spectateur de la Fédération peut voir la page de la Fédération."En savoir plus sur les rôles d'accès."

Vous pouvez vous fédérer avec votre IdP d'entreprise ou avec le site de support NetApp . NetApp recommande de choisir l'un ou l'autre, mais pas les deux.

NetApp prend uniquement en charge l'authentification unique initiée par le fournisseur de services (SP). Vous devez d'abord configurer le fournisseur d'identité pour qu'il approuve NetApp en tant que fournisseur de services. Ensuite, vous pouvez créer une connexion dans la console qui utilise la configuration du fournisseur d'identité.

Vous pouvez configurer une connexion fédérée avec Microsoft Entra ID pour activer l'authentification unique (SSO) pour la console. Le processus implique la configuration de votre identifiant Microsoft Entra pour approuver la console en tant que fournisseur de services, puis la création de la connexion dans la console.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Fédération** pour afficher la page **Fédérations**.
3. Sélectionnez **Configurer une nouvelle fédération**.

Détails du domaine

1. Entrez les détails de votre domaine :
   a. Choisissez si vous souhaitez utiliser un domaine vérifié ou votre domaine de messagerie. Le domaine de messagerie est le domaine associé au compte avec lequel vous êtes connecté.
   b. Entrez le nom de la fédération que vous configurez.

c. Si vous choisissez un domaine vérifié, sélectionnez le domaine dans la liste.

2. Sélectionnez **Suivant**.

Méthode de connexion

1. Pour votre méthode de connexion, choisissez **Fournisseur** puis sélectionnez **Microsoft Entra ID**.
2. Sélectionnez **Suivant**.

Instructions de configuration

1. Configurez votre identifiant Microsoft Entra pour faire confiance à NetApp en tant que fournisseur de services. Vous devez effectuer cette étape sur votre serveur Microsoft Entra ID.
   a. Utilisez les valeurs suivantes lors de l'enregistrement de votre application Microsoft Entra ID pour faire confiance à la console :
      - Pour l'**URL de redirection**, utilisez `https://services.cloud.netapp.com`
      - Pour l'**URL de réponse**, utilisez `https://netapp-cloud-account.auth0.com/login/callback`
   b. Créez un secret client pour votre application Microsoft Entra ID. Vous devrez fournir l'ID client, le secret client et le nom de domaine Entra ID pour terminer la fédération.
2. Revenez à la console et sélectionnez **Suivant** pour créer la connexion.

Créer une connexion

1. Créer la connexion avec Microsoft Entra ID
   a. Saisissez l'ID client et le secret client que vous avez créés à l'étape précédente.
   b. Saisissez le nom de domaine Microsoft Entra ID.
2. Sélectionnez **Créer une connexion**. Le système crée la connexion en quelques secondes.

Tester et activer la connexion

1. Sélectionnez **Suivant**.
2. Sélectionnez **Tester la connexion** pour tester votre connexion. Vous êtes dirigé vers une page de connexion pour votre serveur IdP. Connectez-vous avec vos identifiants IdP. Une fois connecté, retournez à la console pour activer la connexion.

   Lorsque vous utilisez la console en mode restreint, copiez l'URL dans une fenêtre de navigateur incognito ou dans un navigateur distinct pour vous connecter à votre fournisseur d'identité.

3. Dans la console, sélectionnez **Suivant** pour consulter la page récapitulative.
4. Configurer les notifications.

   Choisissez entre sept jours ou 30 jours. Le système envoie par courriel des notifications d'expiration et les affiche dans la console à tout utilisateur ayant les rôles suivants : super administrateur, administrateur d'organisation, administrateur de fédération et visionneur de fédération.

5. Vérifiez les détails de la fédération, puis sélectionnez **Activer la fédération**.

6. Sélectionnez **Terminer** pour terminer le processus.

Une fois la fédération activée, les utilisateurs se connectent à la NetApp Console à l'aide de leurs identifiants d'entreprise.

Fédérer la NetApp Console avec PingFederate

Fédérez-vous avec votre fournisseur IdP PingFederate pour activer l'authentification unique (SSO) pour la NetApp Console. Cela permet aux utilisateurs de se connecter en utilisant leurs identifiants d'entreprise.

Rôles requis

Le rôle d'administrateur de fédération est requis pour créer et gérer des fédérations. Le spectateur de la Fédération peut voir la page de la Fédération."En savoir plus sur les rôles d'accès."

Vous pouvez vous fédérer avec votre IdP d'entreprise ou avec le site de support NetApp . NetApp recommande de choisir l'un ou l'autre, mais pas les deux.

NetApp prend uniquement en charge l'authentification unique initiée par le fournisseur de services (SP). Vous devez d'abord configurer le fournisseur d'identité pour qu'il approuve NetApp en tant que fournisseur de services. Ensuite, vous pouvez créer une connexion dans la console qui utilise la configuration du fournisseur d'identité.

Vous pouvez configurer une connexion fédérée avec PingFederate pour activer l'authentification unique (SSO) pour la console. Le processus implique la configuration de votre serveur PingFederate pour faire confiance à la console en tant que fournisseur de services, puis la création de la connexion dans la console.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Fédération** pour afficher la page **Fédérations**.
3. Sélectionnez **Configurer une nouvelle fédération**.
4. Entrez les détails de votre domaine :
   a. Choisissez si vous souhaitez utiliser un domaine vérifié ou votre domaine de messagerie. Le domaine de messagerie est le domaine associé au compte avec lequel vous êtes connecté.
   b. Entrez le nom de la fédération que vous configurez.
   c. Si vous choisissez un domaine vérifié, sélectionnez le domaine dans la liste.
5. Sélectionnez **Suivant**.
6. Pour votre méthode de connexion, choisissez **Fournisseur** puis sélectionnez **PingFederate**.
7. Sélectionnez **Suivant**.
8. Configurez votre serveur PingFederate pour faire confiance à NetApp en tant que fournisseur de services. Vous devez effectuer cette étape sur votre serveur PingFederate.
   a. Utilisez les valeurs suivantes lors de la configuration de PingFederate pour approuver la NetApp Console:
      - Pour l'**URL de réponse** ou l'**URL du service client d'assertion (ACS)**, utilisez `https://netapp-cloud-account.auth0.com/login/callback`
      - Pour l'**URL de déconnexion**, utilisez `https://netapp-cloud-account.auth0.com/logout`

- Pour **ID d'audience/d'entité**, utilisez `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` où <fed-domain-name-pingfederate> est le nom de domaine de la fédération. Par exemple, si votre domaine est `example.com` , l'ID d'audience/d'entité serait `urn:auth0:netappcloud-account:fed-example-com-pingfederate` .

b. Copiez l'URL du serveur PingFederate. Vous aurez besoin de cette URL lors de la création de la connexion dans la console.

c. Téléchargez le certificat X.509 depuis votre serveur PingFederate. Il doit être au format PEM codé en Base64 (.pem, .crt, .cer).

9. Revenez à la console et sélectionnez **Suivant** pour créer la connexion.
10. Créer la connexion avec PingFederate
    a. Saisissez l'URL du serveur PingFederate que vous avez copiée à l'étape précédente.
    b. Téléchargez le certificat de signature X.509. Le certificat doit être au format PEM, CER ou CRT.
11. Sélectionnez **Créer une connexion**. Le système crée la connexion en quelques secondes.
12. Sélectionnez **Suivant**.
13. Sélectionnez **Tester la connexion** pour tester votre connexion. Vous êtes dirigé vers une page de connexion pour votre serveur IdP. Connectez-vous avec vos identifiants IdP. Une fois connecté, retournez à la console pour activer la connexion.

> Lorsque vous utilisez la console en mode restreint, copiez l'URL dans une fenêtre de navigateur incognito ou dans un navigateur distinct pour vous connecter à votre fournisseur d'identité.

14. Dans la console, sélectionnez **Suivant** pour consulter la page récapitulative.
15. Configurer les notifications.

    Choisissez entre sept jours ou 30 jours. Le système envoie par courriel des notifications d'expiration et les affiche dans la console à tout utilisateur ayant les rôles suivants : super administrateur, administrateur d'organisation, administrateur de fédération et visionneur de fédération.

16. Vérifiez les détails de la fédération, puis sélectionnez **Activer la fédération**.
17. Sélectionnez **Terminer** pour terminer le processus.

Une fois la fédération activée, les utilisateurs se connectent à la NetApp Console à l'aide de leurs identifiants d'entreprise.

Fédérer avec un fournisseur d'identité SAML

Fédérez-vous avec votre fournisseur IdP SAML 2.0 pour activer l'authentification unique (SSO) pour la console NEtApp. Cela permet aux utilisateurs de se connecter en utilisant leurs identifiants d'entreprise.

Rôle requis

Le rôle d'administrateur de fédération est requis pour créer et gérer des fédérations. Le spectateur de la Fédération peut voir la page de la Fédération."En savoir plus sur les rôles d'accès."

> Vous pouvez vous fédérer avec votre IdP d'entreprise ou avec le site de support NetApp . Vous ne pouvez pas vous fédérer avec les deux.

NetApp prend uniquement en charge l'authentification unique initiée par le fournisseur de services (SP). Vous devez d'abord configurer le fournisseur d'identité pour qu'il approuve NetApp en tant que fournisseur de services. Ensuite, vous pouvez créer une connexion dans la console qui utilise la configuration du fournisseur d'identité.

Vous pouvez configurer une connexion fédérée avec votre fournisseur SAML 2.0 pour activer l'authentification unique (SSO) pour la console. Le processus implique la configuration de votre fournisseur pour qu'il fasse confiance à NetApp en tant que fournisseur de services, puis la création de la connexion dans la console.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Fédération** pour afficher la page **Fédérations**.
3. Sélectionnez **Configurer une nouvelle fédération**.
4. Entrez les détails de votre domaine :
   a. Choisissez si vous souhaitez utiliser un domaine vérifié ou votre domaine de messagerie. Le domaine de messagerie est le domaine associé au compte avec lequel vous êtes connecté.
   b. Entrez le nom de la fédération que vous configurez.
   c. Si vous choisissez un domaine vérifié, sélectionnez le domaine dans la liste.
5. Sélectionnez **Suivant**.
6. Pour votre méthode de connexion, choisissez **Protocole** puis sélectionnez **Fournisseur d'identité SAML**.
7. Sélectionnez **Suivant**.
8. Configurez votre fournisseur d'identité SAML pour faire confiance à NetApp en tant que fournisseur de services. Vous devez effectuer cette étape sur votre serveur fournisseur SAML.
   a. Assurez-vous que votre IdP possède l'attribut `email` définir sur l'adresse e-mail de l'utilisateur. Ceci est nécessaire pour que la console identifie correctement les utilisateurs :

```
<saml:AttributeStatement
xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="email"
NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
        <saml:AttributeValue
xsi:type="xs:string">email@domain.com</saml:AttributeValue>
    </saml:Attribute>
</saml:AttributeStatement>
```

1. Utilisez les valeurs suivantes lors de l'enregistrement de votre application SAML auprès de la console :
   - Pour l'**URL de réponse** ou l'**URL du service client d'assertion (ACS)**, utilisez `https://netapp-cloud-account.auth0.com/login/callback`
   - Pour l'**URL de déconnexion**, utilisez `https://netapp-cloud-account.auth0.com/logout`
   - Pour **ID d'audience/d'entité**, utilisez `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` où <fed-domain-name-saml> est le nom de domaine que vous souhaitez utiliser pour la fédération. Par exemple, si votre domaine est `example.com` , l'ID d'audience/d'entité serait

`urn:auth0:netapp-cloud-account:fed-example-com-samlp` .

2. Après avoir créé la confiance, copiez les valeurs suivantes à partir de votre serveur fournisseur SAML :
   - URL de connexion
   - URL de déconnexion (facultatif)
3. Téléchargez le certificat X.509 depuis le serveur de votre fournisseur SAML. Il doit être au format PEM, CER ou CRT.
   a. Revenez à la console et sélectionnez **Suivant** pour créer la connexion.
   b. Créez la connexion avec SAML.
4. Saisissez l'**URL de connexion** de votre serveur SAML.
5. Téléchargez le certificat X.509 que vous avez téléchargé depuis le serveur de votre fournisseur SAML.
6. Si vous le souhaitez, saisissez l'**URL de déconnexion** de votre serveur SAML.
   a. Sélectionnez **Créer une connexion**. Le système crée la connexion en quelques secondes.
   b. Sélectionnez **Suivant**.
   c. Sélectionnez **Tester la connexion** pour tester votre connexion. Vous êtes dirigé vers une page de connexion pour votre serveur IdP. Connectez-vous avec vos identifiants IdP. Une fois connecté, retournez à la console pour activer la connexion.

      Lorsque vous utilisez la console en mode restreint, copiez l'URL dans une fenêtre de navigateur incognito ou dans un navigateur distinct pour vous connecter à votre fournisseur d'identité.

   d. Dans la console, sélectionnez **Suivant** pour consulter la page récapitulative.
   e. Configurer les notifications.

      Choisissez entre sept jours ou 30 jours. Le système envoie par courriel des notifications d'expiration et les affiche dans la console à tout utilisateur ayant les rôles suivants : super administrateur, administrateur d'organisation, administrateur de fédération et visionneur de fédération.

   f. Vérifiez les détails de la fédération, puis sélectionnez **Activer la fédération**.
   g. Sélectionnez **Terminer** pour terminer le processus.

Une fois la fédération activée, les utilisateurs se connectent à la NetApp Console à l'aide de leurs identifiants d'entreprise.

Gérer les fédérations

Gérer les fédérations dans la NetApp Console

Vous pouvez gérer votre fédération dans la NetApp Console. Vous pouvez le désactiver, mettre à jour les informations d'identification expirées, ainsi que le désactiver si vous n'en avez plus besoin.

Rôles requis

Le rôle d'administrateur de fédération est requis pour créer et gérer des fédérations. Le spectateur de la Fédération peut voir la page de la Fédération."En savoir plus sur les rôles d'accès."

Vous pouvez également ajouter un domaine vérifié supplémentaire à une fédération existante, ce qui vous

permet d'utiliser plusieurs domaines pour votre connexion fédérée.

- Si vous avez configuré la fédération à l'aide de NetApp Cloud Central, importez-la via la page **Fédération** pour la gérer dans la console."Apprenez à importer votre fédération"
- Vous pouvez consulter les événements de gestion des fédérations, tels que l'activation, la désactivation et la mise à jour des fédérations, sur la page Audit. "En savoir plus sur les opérations de surveillance dans la NetApp Console."

Activer une fédération

Si vous avez créé une fédération mais qu'elle n'est pas activée, vous pouvez l'activer via la page **Fédération**. L'activation d'une fédération permet aux utilisateurs associés à la fédération de se connecter à la console à l'aide de leurs informations d'identification d'entreprise. Créez et testez la fédération avec succès avant de l'activer.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez l'onglet **Fédération**.
3. Sélectionnez le menu actions ••• à côté de la fédération que vous souhaitez activer et sélectionnez **Activer**.

Ajouter un domaine vérifié à une fédération existante

Vous pouvez ajouter un domaine vérifié à une fédération existante dans la console pour utiliser plusieurs domaines avec le même fournisseur d'identité (IdP).

Vous devez déjà avoir vérifié le domaine dans la console avant de pouvoir l'ajouter à une fédération. Si vous n'avez pas encore vérifié le domaine, vous pouvez le faire en suivant les étapes décrites dans"Vérifiez votre domaine dans la console" .

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez l'onglet **Fédération**.
3. Sélectionnez le menu actions ⋮ à côté de la fédération à laquelle vous souhaitez ajouter un domaine vérifié et sélectionnez **Mettre à jour les domaines**. La boîte de dialogue **Mettre à jour les domaines** affiche le domaine déjà associé à cette fédération.
4. Sélectionnez un domaine vérifié dans la liste des domaines disponibles.
5. Sélectionnez **Mettre à jour**. Les nouveaux utilisateurs de domaine peuvent obtenir un accès à la console fédérée dans un délai de 30 secondes.

Mise à jour d'une connexion fédérée expirant

Vous pouvez mettre à jour les détails d'une fédération dans la console. Par exemple, vous devrez mettre à jour la fédération si les informations d'identification telles qu'un certificat ou un secret client expirent. Si nécessaire, mettez à jour la date de notification pour vous rappeler de mettre à jour la connexion avant son expiration.

Mettez d'abord à jour la console avant de mettre à jour votre IdP pour éviter les problèmes de connexion. Restez connecté à la console pendant le processus.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez l'onglet **Fédération**.
3. Sélectionnez le menu actions (trois points verticaux) à côté de la fédération que vous souhaitez mettre à jour et sélectionnez **Mettre à jour la fédération**.
4. Mettez à jour les détails de la fédération si nécessaire.
5. Sélectionnez **Mettre à jour**.

Tester une fédération existante

Testez la connexion d'une fédération existante pour vérifier qu'elle fonctionne. Cela peut vous aider à identifier les problèmes liés à la fédération et à les résoudre.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez l'onglet **Fédération**.
3. Sélectionnez le menu actions ⋮ à côté de la fédération à laquelle vous souhaitez ajouter un domaine vérifié et sélectionnez **Tester la connexion**.
4. Sélectionnez **Test**. Le système vous invite à vous connecter avec vos identifiants d'entreprise. Si la connexion réussit, vous êtes redirigé vers la NetApp Console. Si la connexion échoue, vous voyez un message d'erreur indiquant le problème avec la fédération.
5. Sélectionnez **Terminé** pour revenir à l'onglet **Fédération**.

Désactiver une fédération

Si vous n'avez plus besoin d'une fédération, vous pouvez la désactiver. Cela empêche les utilisateurs associés à la fédération de se connecter à la console à l'aide de leurs informations d'identification d'entreprise. Vous pouvez réactiver la fédération plus tard si nécessaire.

Désactivez une fédération avant de la supprimer, par exemple lors de la mise hors service de l'IdP ou de l'arrêt de la fédération. Cela vous permet de le réactiver ultérieurement si nécessaire.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez l'onglet **Fédération**.
3. Sélectionnez le menu actions ⋮ à côté de la fédération à laquelle vous souhaitez ajouter un domaine vérifié et sélectionnez **Désactiver**.

Supprimer une fédération

Si vous n'avez plus besoin d'une fédération, vous pouvez la supprimer. Cela supprime la fédération et empêche tous les utilisateurs associés à la fédération de se connecter à la console à l'aide de leurs informations d'identification d'entreprise. Par exemple, si l'IdP est en cours de mise hors service ou si la fédération n'est plus nécessaire.

Vous ne pouvez pas récupérer une fédération après l'avoir supprimée. Vous devez créer une nouvelle fédération.

ⓘ Vous devez désactiver une fédération avant de pouvoir la supprimer. Vous ne pouvez pas annuler la suppression d'une fédération après l'avoir supprimée.

Étapes

1. Sélectionnez **Administration > Identité et accès** .
2. Sélectionnez **Fédérations** pour afficher la page **Fédérations**.
3. Sélectionnez le menu actions ⋮ à côté de la fédération à laquelle vous souhaitez ajouter un domaine vérifié et sélectionnez **Supprimer**.

Importez votre fédération dans la NetApp Console

Si vous avez déjà configuré la fédération via NetApp Cloud Central (une application externe à la NetApp Console), la page Fédération vous invite à importer votre connexion fédérée existante vers la console afin que vous puissiez la gérer dans la nouvelle interface. Vous pourrez alors profiter des dernières améliorations sans avoir à recréer votre connexion fédérée.

ⓘ Après avoir importé votre fédération existante, vous pouvez gérer la fédération à partir de la page **Fédérations**."En savoir plus sur la gestion des fédérations."

Rôle requis

Administrateur d'organisation ou administrateur de fédération."En savoir plus sur les rôles d'accès."

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez l'onglet **Fédération**.
3. Sélectionnez **Importer la Fédération**.

Appliquer les autorisations ONTAP pour ONTAP Advanced View (ONTAP System Manager)

Par défaut, les informations d'identification de l'agent de console permettent aux utilisateurs d'accéder à la vue avancée (ONTAP System Manager). Vous pouvez demander aux utilisateurs leurs informations d'identification ONTAP à la place. Cela garantit que les autorisations ONTAP d'un utilisateur sont appliquées lorsqu'il travaille avec des clusters ONTAP dans les clusters Cloud Volumes ONTAP et ONTAP sur site.

ⓘ Vous devez disposer du rôle d'administrateur d'organisation pour modifier les paramètres de l'agent de la console.

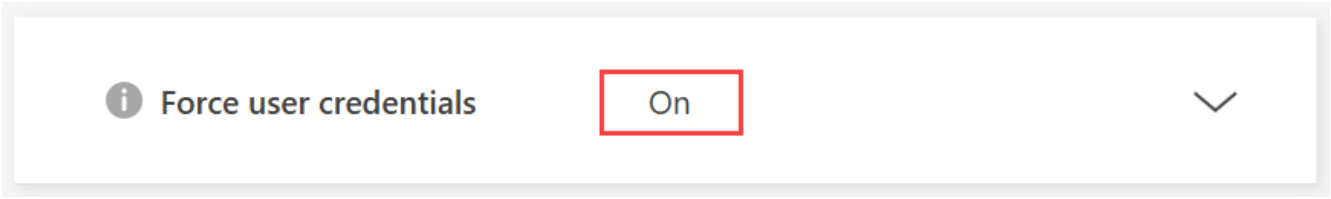
Étapes

1. Sélectionnez **Administration > Agents**.
2. Sur la page **Aperçu**, sélectionnez le menu d'action pour un agent de console et sélectionnez **Modifier l'agent**.

   L'agent de la console doit être actif pour pouvoir le modifier.

3. Développez l'option **Forcer les informations d'identification**.
4. Cochez la case pour activer l'option **Forcer les informations d'identification**, puis sélectionnez **Enregistrer**.

5. Vérifiez que l'option **Forcer les informations d'identification** est activée.



Activer le mode lecture seule pour une organisation NetApp Console

Par mesure de sécurité, vous pouvez activer le mode lecture seule pour votre organisation NetApp Console . En mode lecture seule, les utilisateurs peuvent consulter les ressources et les paramètres, mais ne peuvent apporter aucune modification.

En mode lecture seule, les utilisateurs disposant de rôles d'administrateur doivent élever manuellement leurs autorisations pour effectuer des modifications, ce qui garantit que ces modifications sont intentionnelles.

Rôles d'accès requis

Super administrateur ou administrateur d'organisation.

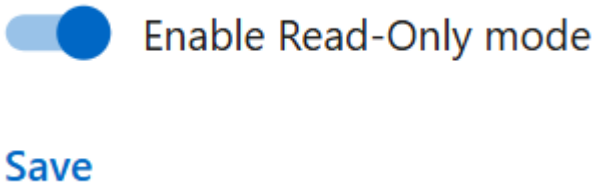
Activez le mode lecture seule pour votre organisation Console

Activez le mode lecture seule pour limiter les modifications apportées à l'organisation de votre console. Tous les utilisateurs peuvent toujours consulter les ressources. Les utilisateurs disposant de rôles d'administrateur ne peuvent effectuer aucune action dans la console sans élever manuellement leurs autorisations.

Lorsque le mode lecture seule est activé, les utilisateurs voient une bannière les informant que l'organisation est en mode lecture seule. Les utilisateurs doivent se rendre dans les paramètres utilisateur pour modifier leur rôle.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Dans l'onglet **Organisations**, sélectionnez **Modifier les paramètres de l'organisation** pour l'organisation que vous souhaitez passer en mode lecture seule.
3. Dans la section **Mode lecture seule**, activez le mode lecture seule en déplaçant le commutateur sur la position **Activé** puis sélectionnez **Enregistrer**.



Inscrivez-vous à NetApp Console en tant qu'administrateur initial de l'organisation

Si votre entreprise ne dispose pas d'une organisation NetApp Console , inscrivez-vous pour en créer une. Le premier utilisateur est l'administrateur et gère les comptes et les autorisations. Vous pourrez modifier les rôles et ajouter des administrateurs ultérieurement.

Étapes

1. Ouvrez un navigateur Web et accédez à la "NetApp Console"
2. Si vous possédez un compte sur le site d'assistance NetApp , saisissez directement l'adresse électronique associée à votre compte sur la page **Connexion**.

   La console vous inscrit automatiquement lors de cette première connexion avec vos identifiants du site d'assistance NetApp .

3. Si vous souhaitez vous inscrire en créant une connexion à la console, sélectionnez **S'inscrire**.
   a. Sur la page **Inscription**, saisissez les informations requises et sélectionnez **Suivant**.

      Seuls les caractères anglais sont autorisés dans le formulaire d'inscription.

   b. Consultez votre boîte de réception pour obtenir un e-mail de NetApp contenant des instructions pour vérifier votre adresse e-mail.

      Vérifiez votre adresse e-mail pour finaliser votre inscription.

4. Après vous être connecté, veuillez lire et accepter le contrat de licence utilisateur final.
5. Sur la page **Bienvenue**, créez une organisation.
6. Sélectionnez **Commençons**.

+ En tant qu'administrateur novice, suivez la procédure guidée pour ajouter du stockage, créer un agent de console, et plus encore. "Découvrez comment utiliser l'assistant de console."

Prochaines étapes

En tant qu'administrateur, une fois que vous avez suivi les étapes indiquées dans l'Assistant de console, vous devez planifier votre stratégie d'identité et d'accès, ajouter des utilisateurs à votre organisation et leur attribuer des rôles. "Découvrez la gestion des identités et des accès pour la NetApp Console."

Inscrivez-vous ou connectez-vous à la NetApp Console lorsqu'une organisation existe déjà.

Si votre entreprise possède déjà une organisation NetApp Console , inscrivez-vous ou connectez-vous pour y accéder. Votre méthode d'inscription ou de connexion dépend de si votre entreprise utilise la fédération d'identités ou possède des identifiants pour le site de support NetApp . Sinon, créez un compte de connexion à la NetApp Console .

Étapes

1. Ouvrez un navigateur Web et accédez à la "NetApp Console"
2. Si vous possédez un compte sur le site d'assistance NetApp ou si votre entreprise a configuré l'authentification unique (SSO), saisissez votre adresse e-mail associée ou vos identifiants SSO sur la page **Connexion**. Suivez les instructions pour terminer la connexion.

   Dans les deux cas, vous êtes inscrit à la console dans le cadre de cette connexion initiale.

3. Si vous souhaitez vous inscrire en créant une connexion à la console, sélectionnez **S'inscrire**.
   a. Sur la page **Inscription**, saisissez les informations requises et sélectionnez **Suivant**.

      Seuls les caractères anglais sont autorisés dans le formulaire d'inscription.

b. Consultez votre boîte de réception pour obtenir un e-mail de NetApp contenant des instructions pour vérifier votre adresse e-mail.

   Vérifiez votre adresse e-mail pour finaliser votre inscription.

4. Après vous être connecté, veuillez lire et accepter le contrat de licence utilisateur final.
5. Si le système vous invite à créer une organisation, fermez la boîte de dialogue et informez-en un administrateur de la console afin qu'il puisse vous ajouter à votre organisation et vous donner accès. "Apprenez comment contacter un administrateur de l'organisation."

Prochaines étapes

Une fois que vous aurez accès à votre organisation, vous pourrez commencer à gérer le stockage et à utiliser les services de données qui vous sont attribués.

Gérer les partenariats organisationnels

Partenariats d'organisations dans la NetApp Console

La création de partenariats entre organisations dans la NetApp Console permet aux partenaires de gérer en toute sécurité les ressources NetApp au-delà des frontières organisationnelles, rationalisant ainsi la collaboration et renforçant la sécurité.

Rôles requis

Administrateur de partenariat"En savoir plus sur les rôles d'accès."

Les partenariats permettent une gestion sécurisée des ressources NetApp dans toutes les organisations à l'aide de relations basées sur les rôles dans la console. L'organisation initiatrice accorde l'accès à ses ressources, tandis que l'organisation acceptante fournit les utilisateurs ou les comptes de service auxquels l'accès doit être accordé. Les partenariats sont établis via un flux de travail en libre-service, donnant à l'organisation initiatrice un contrôle total sur les ressources partagées, les rôles attribués et la possibilité d'intégrer, de gérer ou de révoquer l'accès des partenaires selon les besoins.

Les clients peuvent autoriser les MSP ou les revendeurs à gérer les environnements NetApp sans nécessiter de configurations compliquées. Les clients peuvent contrôler les clusters auxquels les partenaires peuvent accéder et les rôles dont ils disposent, et peuvent révoquer l'accès à tout moment pour maintenir la sécurité et la conformité.

En tant que partenaire, vous bénéficiez d'une visibilité et d'un contrôle centralisés sur les environnements clients. Vous pouvez facilement basculer vers l'organisation d'un client pour gérer les ressources, exécuter des services de données et surveiller l'état dans des limites définies, réduisant ainsi les outils personnalisés et garantissant l'alignement avec les politiques de chaque client.

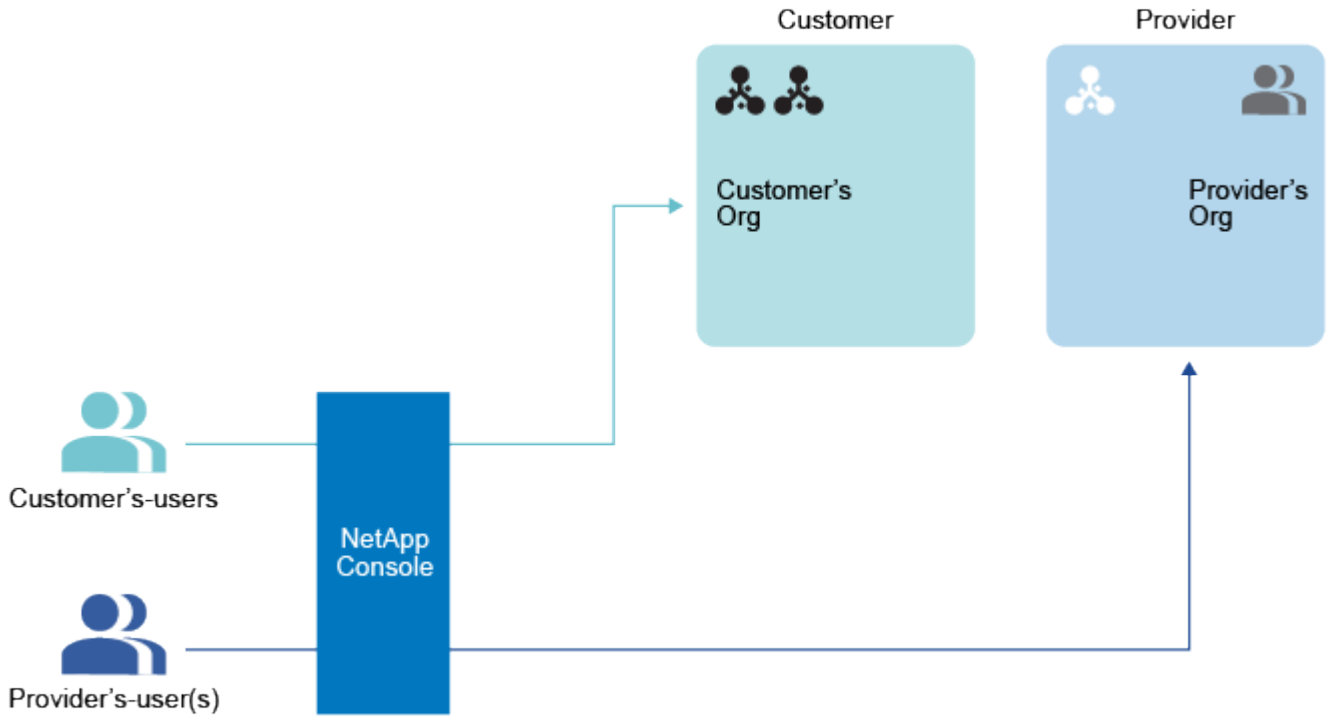
Attribuer à un ou plusieurs utilisateurs le rôle d'administrateur de partenariat

Attribuez le rôle d'administrateur de partenariat à un ou plusieurs utilisateurs des organisations initiatrice et destinataire afin de créer et de gérer les partenariats. Vous pouvez attribuer le rôle de lecteur de partenariat aux utilisateurs qui ont uniquement besoin de consulter les partenariats et non de les gérer.

Partagez l'identifiant de votre organisation avec l'organisation initiatrice

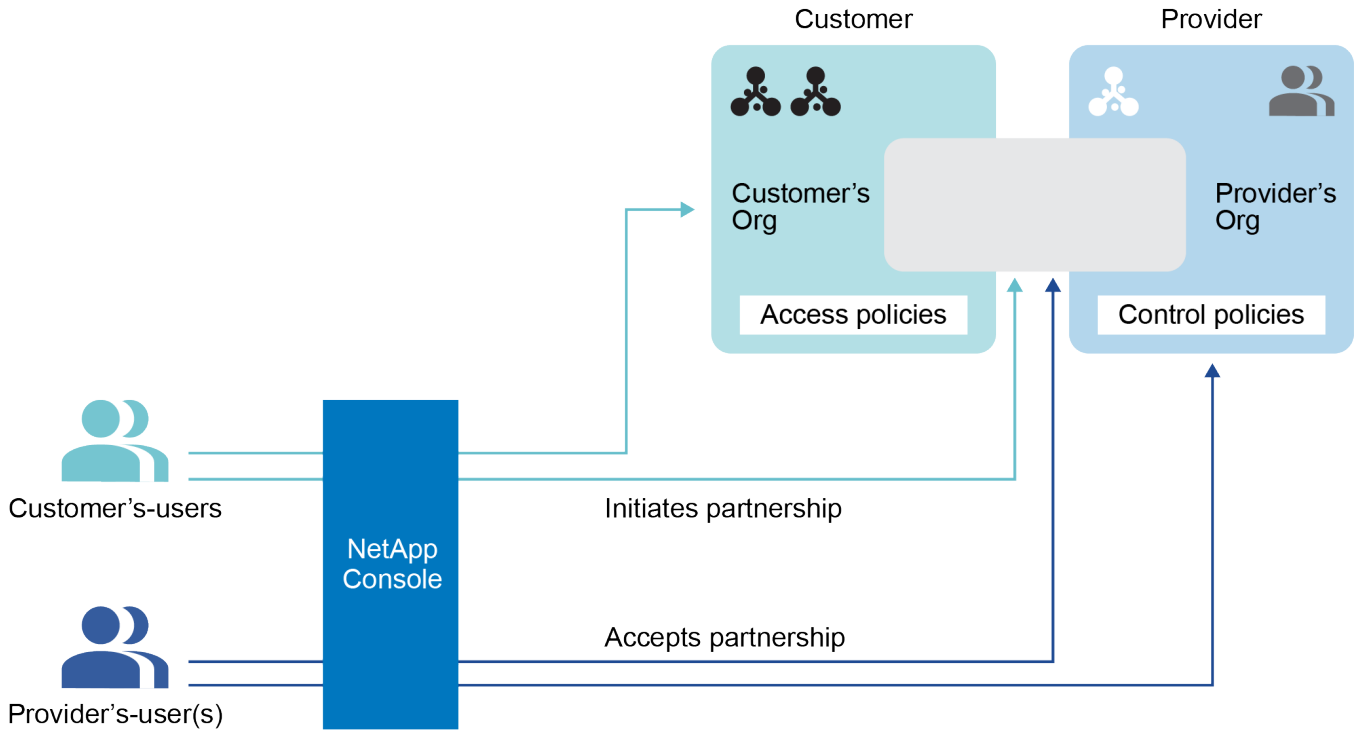
Pour initier un partenariat, l'initiateur doit connaître l'ID de l'organisation cible. Seule l'organisation concernée peut accéder à cet ID d'organisation. Partagez-le directement avec l'organisation initiatrice en dehors de la NetApp Console par courrier électronique ou par une autre méthode.

L'organisation initiatrice est l'organisation qui accorde l'accès à ses ressources.



3 Initier le partenariat au sein de la NetApp Console

L'organisation qui initie le partenariat le fait depuis la NetApp Console en envoyant une demande de partenariat.



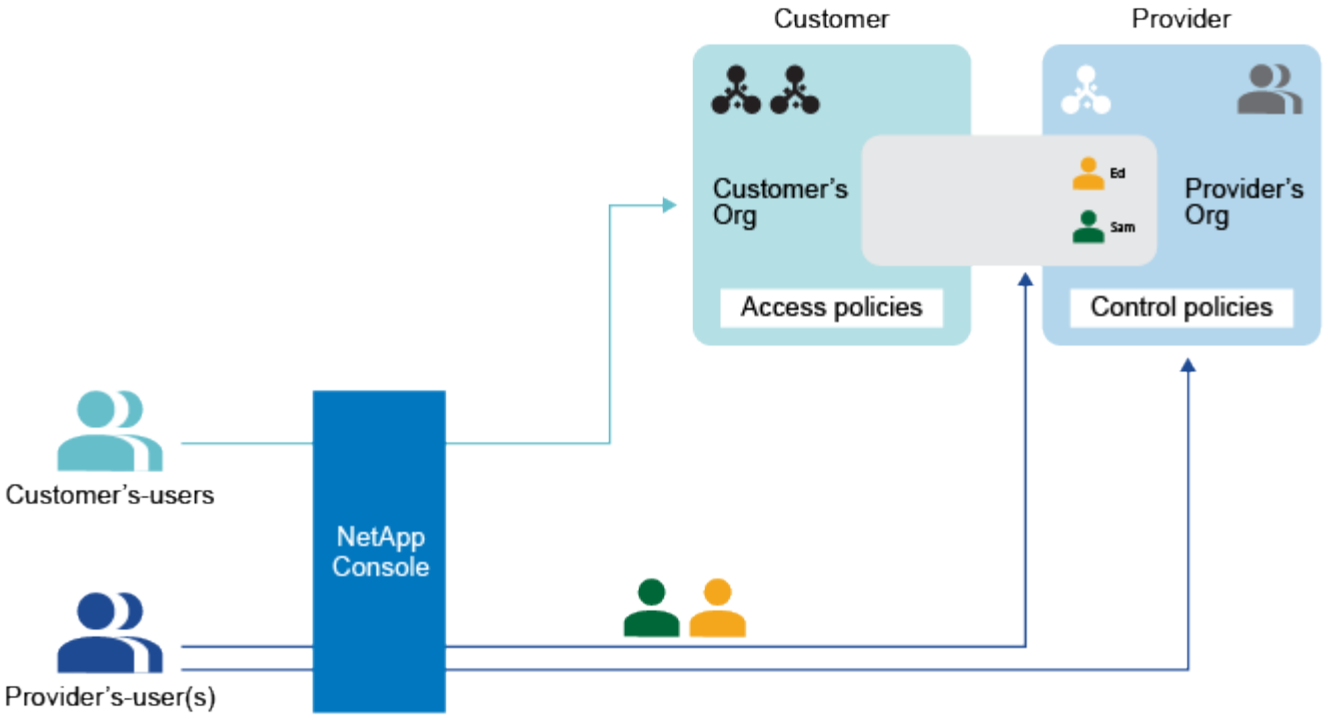
4 Approuver le partenariat

L'organisme récepteur doit accepter la demande.

L'organisation réceptrice est l'organisation à laquelle l'accès aux ressources est accordé.

5 Affecter des utilisateurs au partenariat

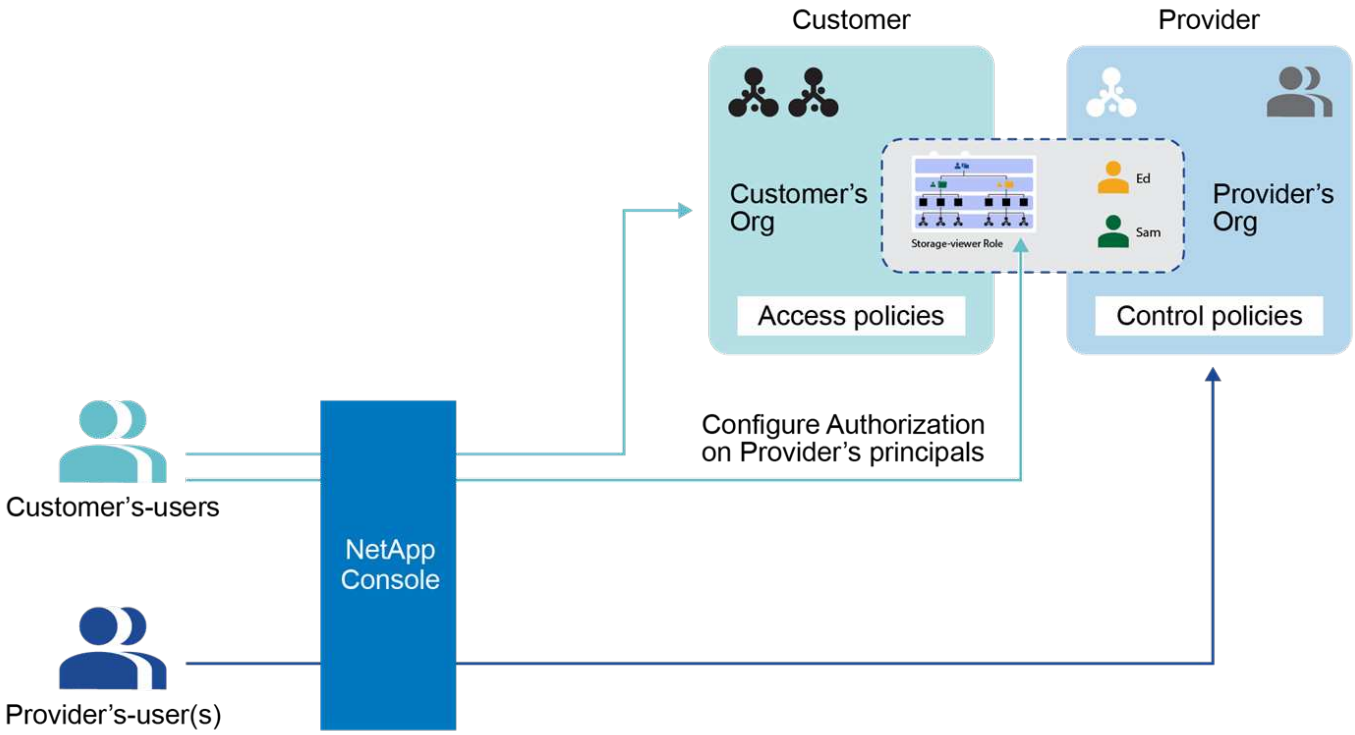
L'organisation réceptrice attribue des utilisateurs ou des comptes de service spécifiques de votre organisation au partenariat. L'organisation initiatrice attribue des rôles à ces utilisateurs.



6 **Accorder aux utilisateurs assignés l'accès aux ressources**

Si vous êtes l'organisation initiatrice, vous pouvez accorder l'accès à des ressources spécifiques aux utilisateurs qui ont été affectés au partenariat. Vous pouvez révoquer l'accès à tout moment.

Vous pouvez le faire en attribuant des rôles à des projets ou des dossiers particuliers au sein de votre organisation.



Gérer les partenariats dans la NetApp Console

Créez des partenariats pour établir des connexions sécurisées et gérées entre votre organisation et des partenaires de confiance pour une gestion collaborative des ressources NetApp .

Les partenariats vous permettent de gérer en toute sécurité les ressources NetApp au-delà des frontières avec des relations basées sur les rôles dans la console. L'organisation initiatrice accorde l'accès à ses ressources, tandis que l'organisation acceptante fournit les utilisateurs ou les comptes de service auxquels l'accès doit être accordé. Les partenariats sont établis via un flux de travail en libre-service, donnant à l'organisation initiatrice un contrôle total sur les ressources partagées, les rôles attribués et la possibilité d'intégrer, de gérer ou de révoquer l'accès des partenaires selon les besoins.

Rôles requis

Le rôle **Administrateur de partenariat** est requis pour créer et gérer des partenariats. Le **spectateur de partenariats** peut consulter la page Partenariats."En savoir plus sur les rôles d'accès."

Initier un partenariat organisationnel

Vous pouvez demander un partenariat avec une autre organisation si vous connaissez son identifiant d'organisation. L'organisme récepteur approuve la demande avant que le partenariat puisse se poursuivre.

Avant de commencer, assurez-vous de disposer de l'ID d'organisation de l'organisation partenaire et que le rôle **Administrateur du partenariat** vous a été attribué.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez l'onglet **Partenariats**.

3. Sélectionnez **Ajouter un partenariat**.
4. Dans la boîte de dialogue **Créer un partenariat**, saisissez l'ID de l'organisation partenaire du partenaire demandé et sélectionnez **Ajouter**.

   La demande de partenariat est envoyée à l'organisme partenaire pour approbation. Vous pouvez consulter l'état de la demande de partenariat sur la page **Partenariats**.

Approuver un partenariat d'organisation

Une demande de partenariat d'organisation doit être acceptée par l'organisation réceptrice avant que le partenariat puisse se poursuivre. Vous devez disposer du rôle **Administrateur de partenariat** pour approuver et gérer les partenariats.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Partenariats**.
3. Sélectionnez l'onglet **Partenariat reçu**.
4. Accédez au partenariat reçu que vous souhaitez approuver et sélectionnez ••• puis sélectionnez **Approuver**.
5. Vérifiez les détails du partenariat, y compris le nom et l'ID de l'organisation qui a demandé le partenariat et sélectionnez **Suivant**.
6. Facultatif, ajoutez les membres de l'organisation au partenariat et sélectionnez **Appliquer**.

   Vous pouvez ajouter des membres supplémentaires via la page **Partenariat** à tout moment.

   > Tous les membres que vous ajoutez deviennent visibles dans l'organisation du partenaire où le partenaire peut les affecter à des ressources.

Résultat

Le partenariat que vous avez approuvé affiche désormais le statut **Établi**. Les utilisateurs disposant des rôles **Administrateur de partenariat** ou **Observateur de partenariat** dans l'une ou l'autre organisation peuvent consulter le partenariat.

Afficher le statut du partenariat

Consultez l'état de vos partenariats.

Rôle requis

Administrateur de partenariat, visualiseur de partenariat."En savoir plus sur les rôles d'accès."

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez les **Partenariats**.
3. Sélectionnez soit l'onglet **Partenariats initiés** soit l'onglet **Partenariats reçus**.
4. Consultez le tableau correspondant qui affiche les partenariats et leurs statuts.

Désactiver un partenariat d'organisation

Vous devez être membre de l'organisation initiatrice pour désactiver un partenariat. La désactivation d'un partenariat révoque immédiatement l'accès à toutes les ressources de votre organisation qui ont été partagées avec l'organisation partenaire.

Rôle requis

Administrateur de partenariat"En savoir plus sur les rôles d'accès."

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez les **Partenariats**.
3. Sélectionnez soit l'onglet **Partenariats initiés**.
4. Consultez le tableau correspondant qui affiche les partenariats et leurs statuts.
5. Accédez au partenariat initié que vous souhaitez désactiver et sélectionnez ••• puis sélectionnez **Désactiver**.

Gérer les membres d'une organisation partenaire

Vous pouvez ajouter des utilisateurs à un partenariat en les ajoutant à l'organisation partenaire. Une fois que vous avez ajouté des utilisateurs, l'organisation partenaire est chargée de leur attribuer des rôles pour des ressources particulières au sein de son organisation.

Rôles requis

Le rôle **Administrateur de partenariat** est requis pour créer et gérer des partenariats. Le **spectateur de partenariats** peut consulter la page Partenariats."En savoir plus sur les rôles d'accès."

Vous pouvez supprimer des utilisateurs d'un partenariat à tout moment. La suppression d'un utilisateur d'un partenariat révoque immédiatement son accès à toutes les ressources de l'organisation partenaire.

Ajouter des membres à un partenariat

Lorsque vous ajoutez des membres à un partenariat, l'**administrateur du partenariat** de l'organisation partenaire doit leur attribuer des rôles pour des ressources particulières de son organisation avant qu'ils puissent accéder à ces ressources.

Une fois que vous avez ajouté des membres à un partenariat, les membres s'affichent en tant que membres de l'organisation partenaire où le partenaire peut les affecter à des ressources.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Partenariats**.
3. Sélectionnez l'onglet **Partenariat reçu**.
4. Sélectionnez le menu actions ••• à côté du partenariat établi auquel vous souhaitez adhérer et sélectionnez **Ajouter des membres**.
5. Choisissez un ou plusieurs membres à ajouter au partenariat et sélectionnez **Ajouter**.

Supprimer des membres d'un partenariat

Vous pouvez supprimer des membres d'un partenariat à tout moment. La suppression d'un utilisateur d'un partenariat révoque immédiatement son accès à toutes les ressources de l'organisation partenaire.

Si vous souhaitez modifier le rôle d'un membre ou les ressources auxquelles il peut accéder, l'administrateur du partenariat de l'organisation partenaire doit effectuer ces modifications.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Partenariats**.
3. Sélectionnez l'onglet **Partenariat reçu**.
4. Sélectionnez le menu actions ••• à côté du membre que vous souhaitez supprimer et sélectionnez **Supprimer l'association**.
5. Confirmez l'action en sélectionnant **Supprimer** dans la boîte de dialogue.

Afficher les informations de rôle d'un utilisateur

Vous pouvez afficher le rôle qui a été attribué à un utilisateur et les ressources associées.

Vous ne pouvez pas modifier le rôle associé à un utilisateur. Si vous avez des questions sur les ressources ou le rôle fourni, contactez l'administrateur de l'organisation partenaire.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Partenariats**.
3. Sélectionnez l'onglet **Partenariat reçu**.
4. Depuis la page **Membres**, accédez à un membre dans le tableau, sélectionnez ••• puis sélectionnez **Afficher les détails**.
5. Dans le tableau, développez la ligne correspondante pour l'organisation, le dossier ou le projet dans lequel vous souhaitez afficher le rôle attribué au membre et sélectionnez le numéro dans la colonne **Rôle**.

Fournir un accès aux ressources aux utilisateurs du partenariat

Vous pouvez accorder l'accès aux utilisateurs du partenariat en leur attribuant des rôles spécifiques pour les dossiers et les projets au sein de votre organisation.

Rôles requis

Administrateur de partenariat"En savoir plus sur les rôles d'accès."

Une organisation partenaire doit d'abord ajouter des membres au partenariat avant que vous puissiez leur attribuer des rôles pour les ressources de votre organisation."Découvrez comment ajouter des membres à un partenariat."

Comprendre les rôles des utilisateurs du partenariat

Vous pouvez gérer les rôles des membres des organisations partenaires de la même manière que vous le faites pour les vôtres. Cependant, tous les rôles ne sont pas disponibles pour les utilisateurs du partenariat. En particulier, vous ne pouvez pas accorder aux utilisateurs partenaires un rôle autorisant les mises à jour logicielles. La mise à jour du logiciel ONTAP nécessite généralement un accès direct au réseau.

Vous pouvez attribuer les rôles suivants aux utilisateurs partenaires :

- "Administrateur de l'organisation"
- "Administrateur de dossier ou de projet"
- "Administrateur de la fédération"
- "Téléspectateur de la Fédération"
- "Administrateur de sauvegarde et de récupération"
- "Visionneuse de sauvegarde"
- "Restaurer l'administrateur"
- "Cloner l'administrateur"
- "Administrateur de reprise après sinistre"
- "Administrateur de basculement de reprise après sinistre"
- "Administrateur d'application de reprise après sinistre"
- "Visionneuse de reprise après sinistre"
- "Analyste de soutien aux opérations"
- "Visionneuse de classification"

"En savoir plus sur les rôles prédéfinis"

Ajouter un rôle à un utilisateur partenaire

Vous donnez accès aux ressources de votre organisation en ajoutant un rôle à un membre. Lorsque vous attribuez un rôle, vous spécifiez une ressource et un rôle. Vous pouvez attribuer plusieurs rôles à un utilisateur.

Par exemple, si vous aviez deux projets et que vous souhaitiez que le même utilisateur ait le rôle d'administrateur de sauvegarde et de récupération pour les deux, vous devrez fournir le rôle à l'utilisateur pour chaque projet. De même, si vous souhaitez attribuer à un utilisateur deux rôles différents pour le même projet, vous devrez attribuer chaque rôle séparément.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Partenariats**.
3. Sélectionnez l'onglet **Partenariat initié**.
4. Sélectionnez le menu actions ••• à côté du partenariat établi que vous souhaitez afficher et sélectionnez **Afficher les détails**.

   La liste **Membre** affiche les membres que l'organisation partenaire a ajoutés au partenariat.

5. Sélectionnez le menu actions ••• à côté du membre auquel vous souhaitez attribuer un rôle et sélectionnez **Ajouter un rôle**.
6. Pour ajouter un rôle, suivez les étapes dans la boîte de dialogue :
   - **Sélectionnez une organisation, un dossier ou un projet** : Choisissez le niveau de votre hiérarchie de ressources pour lequel le membre doit disposer d'autorisations.

     Si vous sélectionnez l'organisation ou un dossier, le membre aura des autorisations sur tout ce qui se trouve dans l'organisation ou le dossier.

- **Sélectionnez une catégorie** : Choisissez une catégorie de rôle. "En savoir plus sur les rôles d'accès" .
- Sélectionnez un **rôle** : choisissez un rôle qui fournit au membre des autorisations pour les ressources associées à l'organisation, au dossier ou au projet que vous avez sélectionné.
- **Ajouter un rôle** : si vous souhaitez fournir l'accès à des dossiers ou projets supplémentaires au sein de votre organisation, sélectionnez **Ajouter un rôle**, spécifiez un autre dossier, projet ou catégorie de rôle, puis sélectionnez une catégorie de rôle et un rôle correspondant.

7. Sélectionnez **Ajouter de nouveaux rôles**.

Modifier ou supprimer un rôle d'un utilisateur partenaire

Vous pouvez modifier ou supprimer un rôle que vous avez attribué à un membre d'une organisation partenaire.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Partenariats**.
3. Sélectionnez l'onglet **Partenariat initié**.
4. Sélectionnez le menu actions ••• à côté du partenariat établi que vous souhaitez afficher et sélectionnez **Afficher les détails**.

   La liste **Membre** affiche les membres que l'organisation partenaire a ajoutés au partenariat.

5. Depuis la page **Membres**, accédez à un membre dans le tableau, sélectionnez ••• puis sélectionnez **Afficher les détails**.
6. Dans le tableau, développez la ligne correspondante pour l'organisation, le dossier ou le projet pour lequel vous souhaitez modifier le rôle attribué au membre et sélectionnez **Afficher** dans la colonne **Rôle** pour afficher les rôles attribués à ce membre.
7. Vous pouvez modifier un rôle existant pour un membre ou supprimer un rôle.
   a. Pour modifier le rôle d'un membre, sélectionnez **Modifier** à côté du rôle que vous souhaitez modifier. Vous ne pouvez modifier un rôle que pour un rôle appartenant à la même catégorie de rôle. Par exemple, vous pouvez passer d'un rôle de service de données à un autre. Confirmer le changement.
   b. Pour retirer le rôle d'un membre, sélectionnez 🗑 à côté du rôle pour supprimer le rôle correspondant du membre. Il vous sera demandé de confirmer la suppression.

Travailler dans une organisation partenaire

Une fois qu'un rôle vous a été attribué dans une organisation partenaire, vous pouvez basculer vers cette organisation et effectuer les actions pour lesquelles vous êtes autorisé à effectuer.

Utilisez le menu Organisation pour basculer entre vos organisations et toutes les organisations partenaires auxquelles vous avez accès."Apprenez-en davantage sur le changement d'organisation et de projet."

Vous pourrez voir les ressources qui ont été partagées avec vous dans l'organisation partenaire et effectuer des actions en fonction du rôle qui vous a été attribué. Travaillez avec votre administrateur de partenariat pour vous assurer que vous disposez du rôle approprié pour les ressources auxquelles vous devez accéder.

Surveiller les opérations de la NetApp Console

Vous pouvez surveiller l'état des opérations effectuées par la console pour voir s'il existe des problèmes que vous devez résoudre. Vous pouvez afficher l'état à partir de la page Audit, du Centre de notifications ou recevoir des notifications par e-mail.

Le tableau met en évidence les fonctionnalités de la page Audit et du Centre de notifications en les comparant.

Centre de notifications	Page d'audit
Affiche le statut de haut niveau des événements et des actions	Fournit des détails sur chaque événement ou action pour une enquête plus approfondie
Affiche l'état de la session de connexion en cours (les informations n'apparaissent pas dans le centre de notifications après la déconnexion)	Conserve le statut du dernier mois
Affiche uniquement les actions initiées dans l'interface utilisateur	Affiche toutes les actions de l'interface utilisateur ou des API
Affiche les actions initiées par l'utilisateur	Affiche toutes les actions, qu'elles soient initiées par l'utilisateur ou par le système
Filtrer les résultats par importance	Filtrer par service, action, utilisateur, statut, etc.
Offre la possibilité d'envoyer des notifications par courrier électronique aux utilisateurs et à d'autres personnes	Aucune capacité de courrier électronique

Auditer l'activité des utilisateurs à partir de la page Audit

Utilisez la page Audit pour identifier qui a effectué une action ou son statut.

La page Audit affiche les actions que les utilisateurs ont effectuées pour gérer votre organisation ou votre compte. Cela inclut des actions de gestion telles que l'association d'utilisateurs, la création de systèmes, la création d'agents, etc.

Vous pouvez également vérifier qui a ajouté un membre à une organisation ou qu'un projet a été supprimé avec succès.

Étapes

1. Sélectionnez **Administration > Audit**.
2. Utilisez les filtres au-dessus du tableau pour modifier les actions affichées dans le tableau.

   Par exemple, vous pouvez utiliser le filtre **Service** pour afficher les actions liées à un service spécifique, ou vous pouvez utiliser le filtre **Utilisateur** pour afficher les actions liées à un compte utilisateur spécifique.

Téléchargez les journaux d'audit depuis la page Audit

Vous pouvez télécharger les journaux d'audit de la page Audit dans un fichier CSV. Cela vous permet de conserver un enregistrement des actions effectuées par les utilisateurs dans votre organisation. Le fichier CSV inclut toutes les colonnes du fichier CSV téléchargé, quels que soient les filtres ou les colonnes affichées sur la page Audit.

Étapes

1. Dans la page **Audit**, sélectionnez l'icône de téléchargement dans le coin supérieur droit du tableau.

Surveiller les activités à l'aide du centre de notifications

Les notifications suivent les opérations de la console pour confirmer le succès. Ils vous permettent d'afficher l'état de nombreuses actions de la console que vous avez lancées au cours de votre session de connexion actuelle. Tous les services de la console ne signalent pas d'informations au centre de notifications.

Vous pouvez afficher les notifications en sélectionnant la cloche de notification () dans la barre de menu. La couleur de la petite bulle dans la cloche indique le niveau de gravité de notification le plus élevé qui est actif. Donc, si vous voyez une bulle rouge, cela signifie qu'il y a une notification importante que vous devez consulter.

Vous pouvez également configurer la console pour envoyer certains types de notifications par e-mail afin d'être informé des activités importantes du système même lorsque vous n'êtes pas connecté au système. Les e-mails peuvent être envoyés à tous les utilisateurs faisant partie de votre organisation ou à tout autre destinataire devant être informé de certains types d'activité du système. Découvrez commentdéfinir les paramètres de notification par e-mail .

Comparaison du centre de notifications avec les alertes

Le centre de notifications vous permet d'afficher l'état des opérations que vous avez lancées et de configurer des notifications d'alerte pour certains types d'activités système. Parallèlement, les alertes vous permettent de visualiser les problèmes ou les risques potentiels dans votre environnement de stockage ONTAP liés à la capacité, à la disponibilité, aux performances, à la protection et à la sécurité.

"En savoir plus sur les alertes de la NetApp Console"

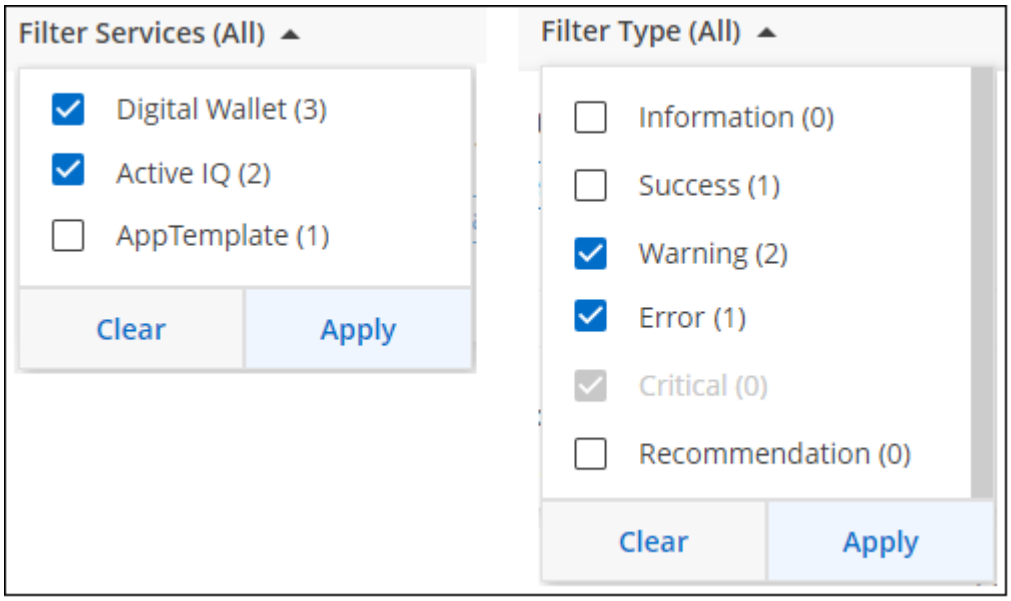
Types de notifications

La console classe les notifications dans les catégories suivantes :

Type de notification	Description
Primordial	Un problème est survenu qui pourrait entraîner une interruption de service si des mesures correctives ne sont pas prises immédiatement.
Erreur	Une action ou un processus s'est terminé par un échec, ou pourrait conduire à un échec si aucune mesure corrective n'est prise.
Avertissement	Un problème dont vous devez être conscient pour vous assurer qu'il n'atteigne pas une gravité critique. Les notifications de cette gravité n'entraînent pas d'interruption de service et une action corrective immédiate peut ne pas être nécessaire.
Recommandation	Une recommandation système vous invitant à prendre une mesure pour améliorer le système ou un certain service ; par exemple : réduction des coûts, suggestion de nouveaux services, configuration de sécurité recommandée, etc.
Information	Un message qui fournit des informations supplémentaires sur une action ou un processus.
Succès	Une action ou un processus terminé avec succès.

Filtrer les notifications

Par défaut, vous verrez toutes les notifications actives dans le centre de notifications. Vous pouvez filtrer les notifications que vous voyez pour afficher uniquement celles qui sont importantes pour vous. Vous pouvez filtrer par « Service » et par « Type » de notification.



Par exemple, si vous souhaitez voir uniquement les notifications « Erreur » et « Avertissement » pour les opérations de la console, sélectionnez ces entrées et vous ne verrez que ces types de notifications.

Ignorer les notifications

Vous pouvez supprimer les notifications de la page si vous n'avez plus besoin de les voir. Vous pouvez ignorer les notifications individuellement ou toutes à la fois.

Pour ignorer toutes les notifications, dans le centre de notifications, sélectionnez ⋮ et sélectionnez **Tout rejeter**.

Pour ignorer des notifications individuelles, passez votre curseur sur la notification et sélectionnez **Ignorer**.

Définir les paramètres de notification par e-mail

Vous pouvez envoyer des types spécifiques de notifications par e-mail afin d'être informé des activités importantes du système, même lorsque vous n'êtes pas connecté. Les e-mails peuvent être envoyés à tous les utilisateurs qui font partie de votre organisation ou de votre compte, ou à tout autre destinataire qui doit être informé de certains types d'activité du système.

- La console envoie des notifications par e-mail pour l'agent, les licences et les abonnements, NetApp Copy and Sync et NetApp Backup and Recovery.
- L'envoi de notifications par e-mail n'est pas pris en charge lorsque l'agent de console est installé sur un site sans accès Internet.

Les filtres que vous définissez dans le Centre de notifications ne déterminent pas les types de notifications que vous recevez par e-mail. Par défaut, tout administrateur d'organisation recevra des e-mails pour toutes les notifications « Critiques » et « Recommandation ». Ces notifications s'appliquent à tous les services : vous ne pouvez pas choisir de recevoir des notifications uniquement pour certains services, par exemple les agents ou NetApp Backup and Recovery.

Tous les autres utilisateurs et destinataires sont configurés pour ne recevoir aucun e-mail de notification. Vous devrez donc configurer les paramètres de notification pour tous les utilisateurs supplémentaires.

Vous devez disposer du rôle d'administrateur de l'organisation pour personnaliser les paramètres de notifications.

Étapes

1. Sélectionnez **Administration > Paramètres de notifications**.
2. Sélectionnez **Utilisateurs de l'organisation** ou **Destinataires supplémentaires**.

   La page **Destinataires supplémentaires** vous permet de configurer la console pour notifier les personnes membres de votre organisation Console.

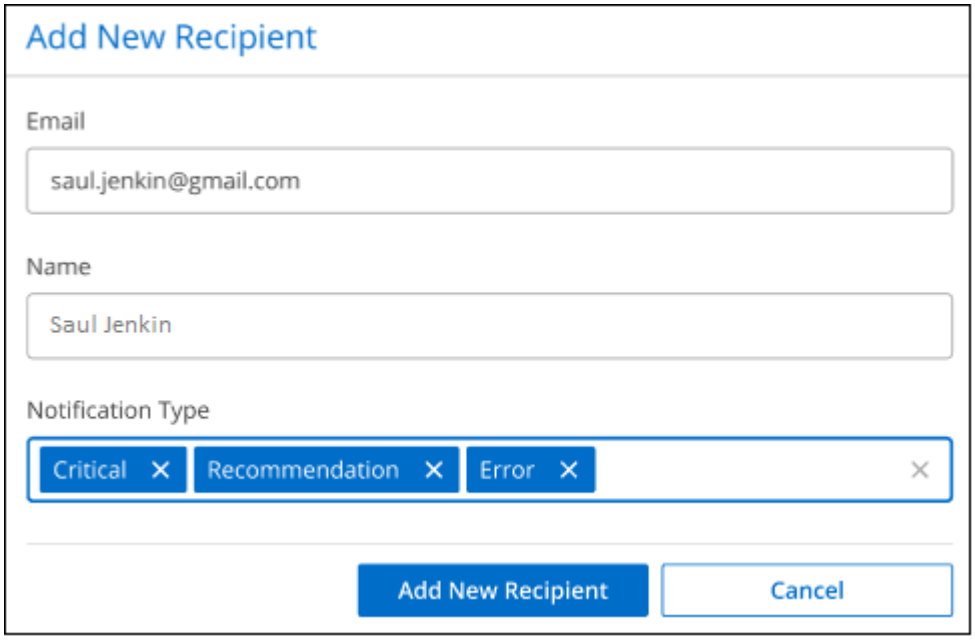
3. Sélectionnez un ou plusieurs utilisateurs à partir de la page *Utilisateurs de l'organisation* ou de la page *Destinataires supplémentaires* et choisissez le type de notifications à envoyer :
   - Pour apporter des modifications à un seul utilisateur, sélectionnez le menu dans la colonne Notifications pour cet utilisateur, cochez les types de notifications à envoyer et sélectionnez **Appliquer**.
   - Pour apporter des modifications à plusieurs utilisateurs, cochez la case correspondant à chaque utilisateur, sélectionnez **Gérer les notifications par e-mail**, cochez les types de notifications à envoyer et sélectionnez **Appliquer**.

Ajouter des destinataires de courrier électronique supplémentaires

Les utilisateurs qui apparaissent sur la page *Utilisateurs de l'organisation* sont renseignés automatiquement à partir des utilisateurs de votre organisation ou de votre compte. Vous pouvez ajouter des adresses e-mail dans la page *Destinataires supplémentaires* pour d'autres personnes ou groupes qui n'ont pas accès à la console, mais qui doivent être informés de certains types d'alertes et de notifications.

Étapes

1. Depuis la page **Paramètres de notifications**, sélectionnez **Ajouter de nouveaux destinataires**.



2. Saisissez le nom, l'adresse e-mail et sélectionnez les types de notifications que le destinataire recevra, puis sélectionnez **Ajouter un nouveau destinataire**.

Informations sur le copyright

Informations sur les marques commerciales