Documentation de configuration et d’administration de la console NetApp

NetApp Console setup and administration

NetApp
October 07, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/console-setup-admin/index.html on October 07, 2025. Always check docs.netapp.com for the latest.

Sommaire

Documentation de configuration et d'administration de la console NetApp . . . 1
Notes de version . . . 2
Quoi de neuf . . . 2
6 octobre 2025 . . . 2
BlueXP est désormais NetApp Console . . . 2
Agent de console 4.0.0 . . . 8
Console NetApp . . . 9
11 août 2025 . . . 10
31 juillet 2025 . . . 11
21 juillet 2025 . . . 11
14 juillet 2025 . . . 12
9 juin 2025 . . . 13
29 mai 2025 . . . 14
12 mai 2025 . . . 14
14 avril 2025 . . . 16
28 mars 2025 . . . 16
10 mars 2025 . . . 17
6 mars 2025 . . . 17
18 février 2025 . . . 18
10 février 2025 . . . 19
13 janvier 2025 . . . 21
16 décembre 2024 . . . 21
9 décembre 2024 . . . 22
26 novembre 2024 . . . 23
11 novembre 2024 . . . 23
10 octobre 2024 . . . 24
7 octobre 2024 . . . 24
30 septembre 2024 . . . 26
9 septembre 2024 . . . 26
22 août 2024 . . . 28
8 août 2024 . . . 28
31 juillet 2024 . . . 29
15 juillet 2024 . . . 30
8 juillet 2024 . . . 30
12 juin 2024 . . . 30
4 juin 2024 . . . 31
17 mai 2024 . . . 31
Limitations connues de la console NetApp . . . 32
Limitations de l'agent de console . . . 32
Modifications apportées aux systèmes d'exploitation Linux pris en charge . . . 33
Systèmes d'exploitation pris en charge . . . 33
Prise en charge de RHEL 8 et 9 . . . 34
Fin du support pour RHEL 7 et CentOS 7 . . . 35

Informations connexes . . . 35
Commencer . . . 37
Apprendre les bases . . . 37
En savoir plus sur la console NetApp . . . 37
En savoir plus sur les agents de la console NetApp . . . 40
En savoir plus sur les modes de déploiement de la console NetApp . . . 44
Démarrer avec l'assistant NetApp . . . 51
Commencer à utiliser l'assistant de console NetApp . . . 51
Démarrer avec le mode standard . . . 52
Démarrage du flux de travail (mode standard) . . . 52
Préparer l'accès réseau pour la console NetApp . . . 53
Inscrivez-vous ou connectez-vous à la console NetApp . . . 55
Créer un agent de console . . . 56
Abonnez-vous aux services intelligents NetApp (mode standard) . . . 205
Ce que vous pouvez faire ensuite (mode standard) . . . 211
Démarrer avec le mode restreint . . . 211
Démarrage du flux de travail (mode restreint) . . . 211
Préparez-vous au déploiement en mode restreint . . . 212
Déployer l'agent de console en mode restreint . . . 232
S'abonner aux services intelligents NetApp (mode restreint) . . . 244
Ce que vous pouvez faire ensuite (mode restreint) . . . 250
Démarrer avec l'interface héritée de BlueXP (mode privé) . . . 250
Démarrage du flux de travail (mode privé BlueXP) . . . 251
Utiliser la console NetApp . . . 253
Connectez-vous à la console NetApp . . . 253
Afficher les métriques sur la page d'accueil de la console NetApp . . . 255
Rôles de la console NetApp requis . . . 255
Activer l'affichage des métriques sur la page d'accueil . . . 257
Afficher la capacité de stockage globale . . . 257
Afficher les alertes ONTAP . . . 258
Afficher la capacité de performance de stockage . . . 259
Afficher les licences et les abonnements dont vous disposez . . . 259
Afficher l'état de résilience aux ransomwares . . . 260
Afficher l'état de la sauvegarde et de la récupération . . . 260
Gérez les paramètres utilisateur de votre console NetApp . . . 260
Changer votre nom d'affichage . . . 261
Configurer l'authentification multifacteur . . . 261
Régénérez votre code de récupération MFA . . . 261
Supprimez votre configuration MFA . . . 262
Contactez l'administrateur de votre organisation . . . 262
Configurer le mode sombre (thème sombre) . . . 262
Administrer la console NetApp . . . 264
Gestion des identités et des accès . . . 264
En savoir plus sur la gestion des identités et des accès de la console NetApp . . . 264
Démarrer avec l'identité et l'accès dans la console NetApp . . . 271

Organisez vos ressources de la console NetApp avec des dossiers et des projets . . . 272
Ajouter des membres et des comptes de service à la console NetApp . . . 276
Utiliser des rôles pour gérer l'accès des utilisateurs aux ressources de la console NetApp . . . 280
Gérer la hiérarchie des ressources dans votre organisation NetApp Console . . . 282
Associer un agent de console à d'autres dossiers et projets . . . 284
Basculer entre les organisations, les projets et les agents de la console . . . 285
ID d'organisation et de projet . . . 288
Surveiller ou auditer l'activité IAM . . . 289
Rôles d'accès à la console NetApp . . . 290
Organisations partenaires . . . 309
Partenariats dans la console NetApp . . . 309
Gérer les partenariats dans la console NetApp . . . 313
Gérer les membres d'une organisation partenaire . . . 315
Fournir un accès aux ressources aux utilisateurs du partenariat . . . 316
Travailler dans une organisation partenaire . . . 318
Fédération d'identité . . . 319
Activer l'authentification unique en utilisant la fédération d'identité avec la console NetApp . . . 319
Vérification de domaine . . . 321
Configurer les fédérations . . . 321
Gérer les fédérations dans la console NetApp . . . 329
Importez votre fédération dans la console NetApp . . . 331
Agents de console . . . 331
Maintenir la machine virtuelle de l'agent de console et le système d'exploitation . . . 331
Maintenir un hôte VCenter ou ESXi pour l'agent de console . . . 335
Installer un certificat signé par une autorité de certification pour l'accès à la console Web . . . 338
Configurer un agent de console pour utiliser un serveur proxy . . . 340
Exiger l'utilisation d'IMDSv2 sur les instances Amazon EC2 . . . 343
Gérer les mises à niveau de l'agent de la console . . . 345
Travailler avec plusieurs agents de console . . . 347
Dépanner l'agent de la console . . . 349
Désinstaller et supprimer un agent de console . . . 353
Configuration par défaut de l'agent de console . . . 354
Appliquer les autorisations ONTAP pour ONTAP Advanced View (ONTAP System Manager) . . . 356
Informations d'identification et abonnements . . . 357
AWS . . . 357
Azuré . . . 371
Google Cloud . . . 386
Gérer les informations d'identification NSS associées à la console NetApp . . . 392
Gérer les informations d'identification associées à votre connexion à la console NetApp . . . 395
Surveiller les opérations de la console NetApp . . . 397
Auditer l'activité des utilisateurs à partir de la page Audit . . . 397
Surveiller les activités à l'aide du centre de notifications . . . 398
Référence . . . 401
Console de maintenance des agents . . . 401
Console de maintenance de l'agent de console . . . 401

Autorisations . . . 402
Résumé des autorisations pour la console NetApp . . . 402
Autorisations AWS pour l'agent de la console . . . 407
Autorisations Azure pour l'agent de console . . . 437
Autorisations Google Cloud pour l'agent de la console . . . 457
Ports . . . 462
Règles du groupe de sécurité de l'agent de console dans AWS . . . 462
Règles du groupe de sécurité de l'agent de console dans Azure . . . 464
Règles de pare-feu d'agent dans Google Cloud . . . 465
Ports pour l'agent de console sur site . . . 466
Points d'accès réseau requis pour la version 3.9.55 et les versions antérieures . . . 467
Mettez à jour votre liste de points de terminaison vers la liste révisée pour la version 4.0.0 et supérieure . . . 467
Points de terminaison contactés par la console NetApp . . . 468
Points de terminaison contactés par l'agent de la console . . . 469
Points de terminaison d'agent sur site . . . 472
Connaissances et soutien . . . 473
Inscrivez-vous pour obtenir de l'aide . . . 473
Présentation de l'enregistrement de l'assistance . . . 473
Enregistrez BlueXP pour le support NetApp . . . 473
Associer les informations d'identification NSS pour la prise en charge de Cloud Volumes ONTAP . . . 476
Obtenir de l'aide . . . 477
Obtenir de l'aide pour un service de fichiers d'un fournisseur cloud . . . 477
Utiliser les options d'auto-assistance . . . 478
Créer un dossier auprès du support NetApp . . . 478
Gérez vos cas d'assistance . . . 480
Mentions légales . . . 482
Copyright . . . 482
Marques de commerce . . . 482
Brevets . . . 482
Politique de confidentialité . . . 482
Open source . . . 482

Documentation de configuration et d’administration de la console NetApp

Notes de version

Quoi de neuf

Découvrez les nouveautés des fonctionnalités d'administration de la console NetApp : gestion des identités et des accès (IAM), agents de console, informations d'identification du fournisseur de cloud, etc.

6 octobre 2025

BlueXP est désormais NetApp Console

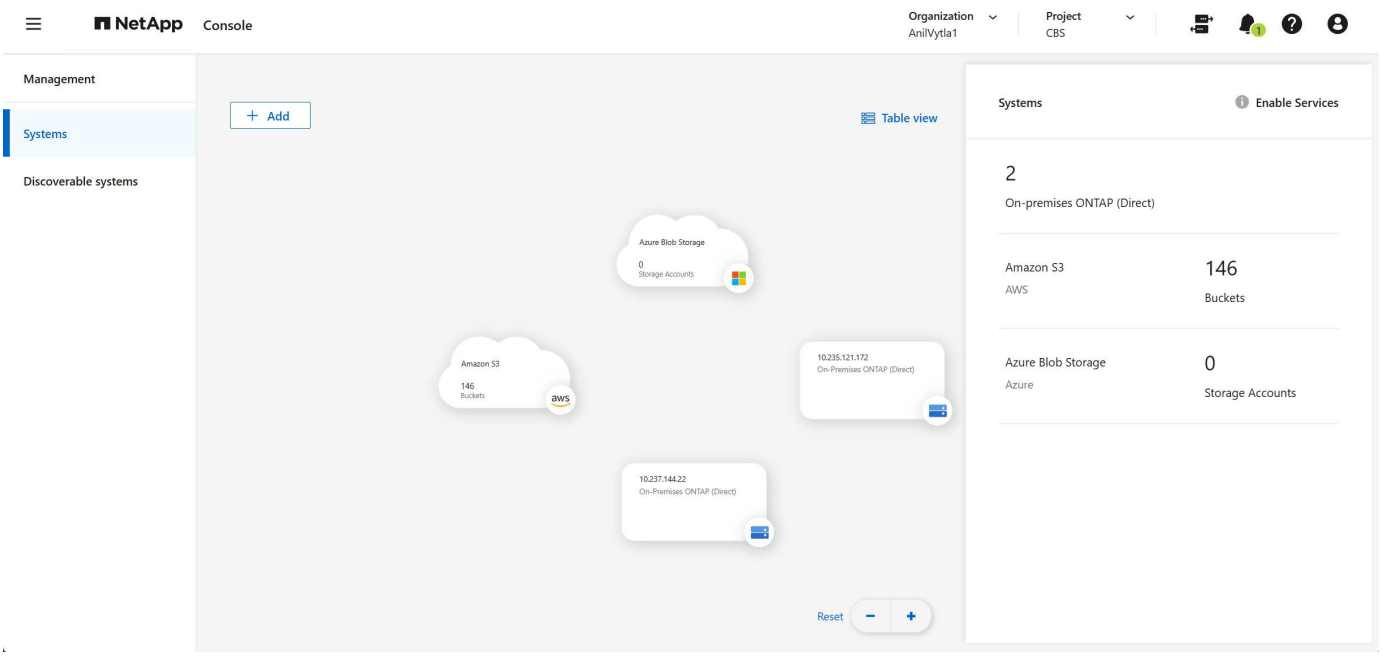
La console NetApp , construite sur la base BlueXP améliorée et restructurée, fournit une gestion centralisée du stockage NetApp et des services de données NetApp dans les environnements sur site et cloud à l'échelle de l'entreprise, offrant des informations en temps réel, des flux de travail plus rapides et une administration simplifiée, hautement sécurisée et conforme.

Menus et pages de navigation

NetApp a déplacé la plupart des options de menu vers le volet de navigation de gauche et a réorganisé les menus pour faciliter la navigation dans la console NetApp .

Canvas est remplacé par la page Systèmes

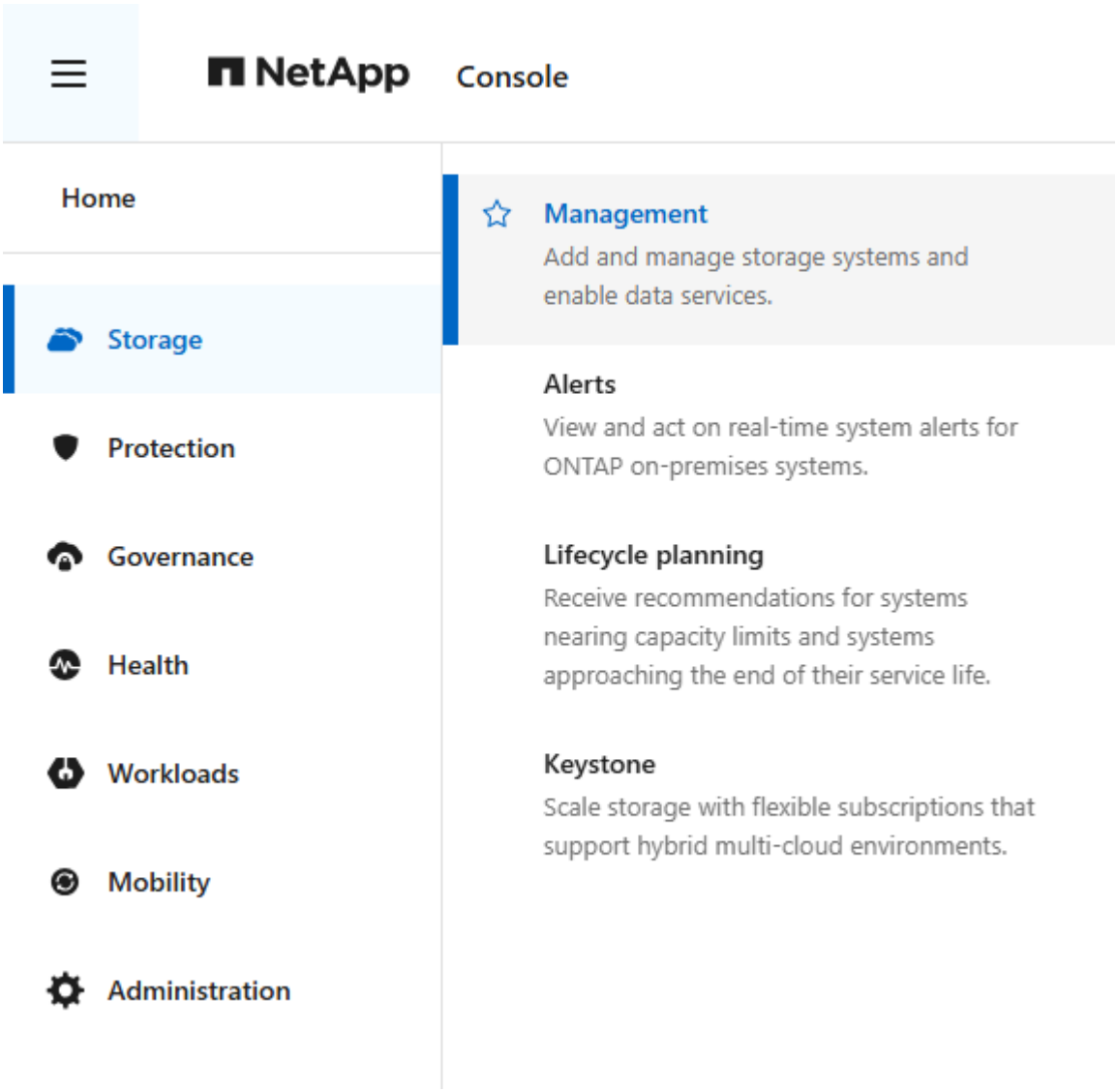
NetApp a renommé le Canvas en page **Systèmes**. Accédez à la page **Système** à partir du menu **Stockage > Gestion**.



Menu de stockage étendu

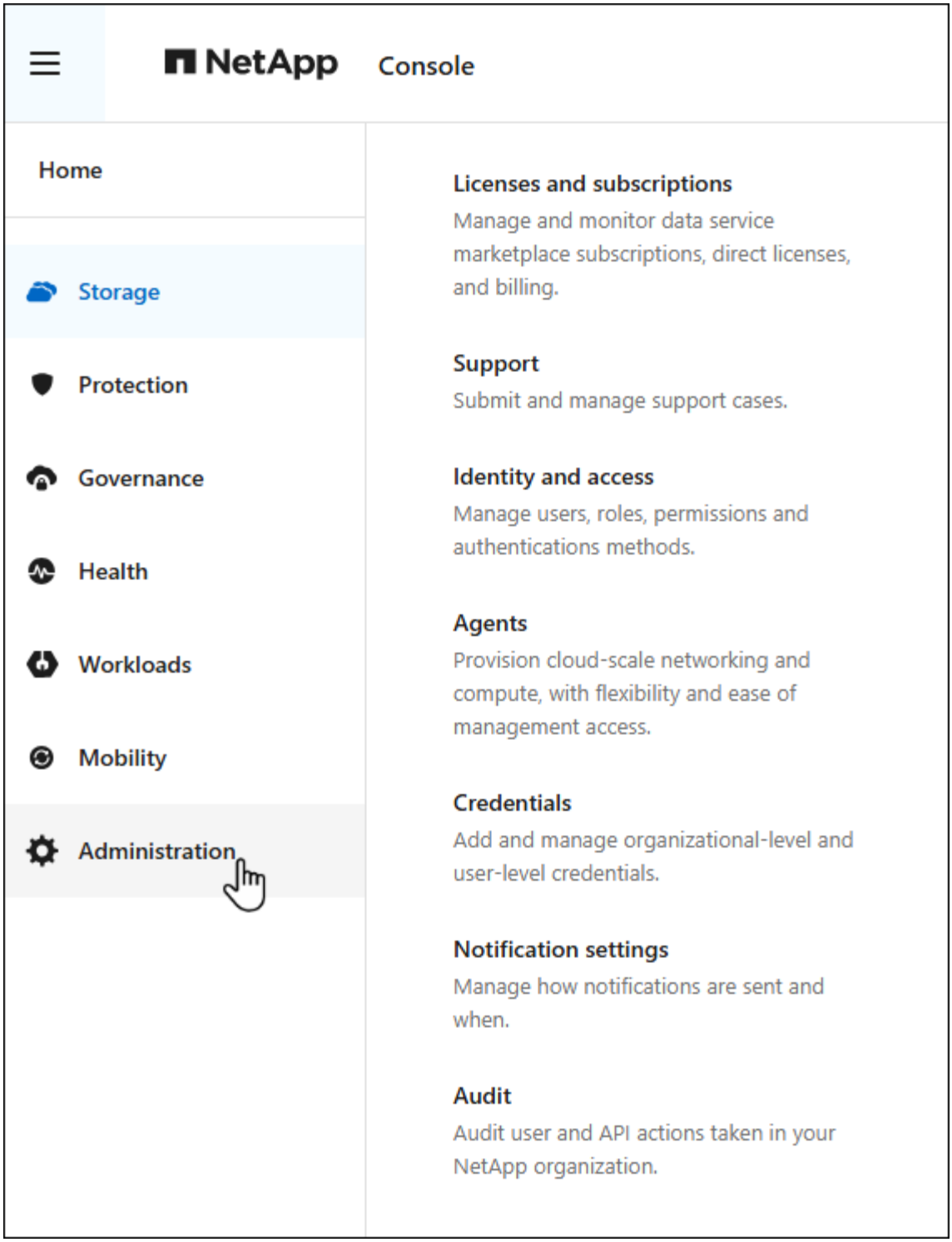
Le menu **Stockage** inclut les **Alertes** pour afficher les alertes du système ONTAP et la **Planification du cycle de vie** (anciennement **Efficacité économique**) pour identifier les ressources inutilisées ou sous-utilisées.

NetApp a déplacé Keystone vers le menu **Stockage**, où vous pouvez gérer vos abonnements NetApp Keystone et afficher votre utilisation.



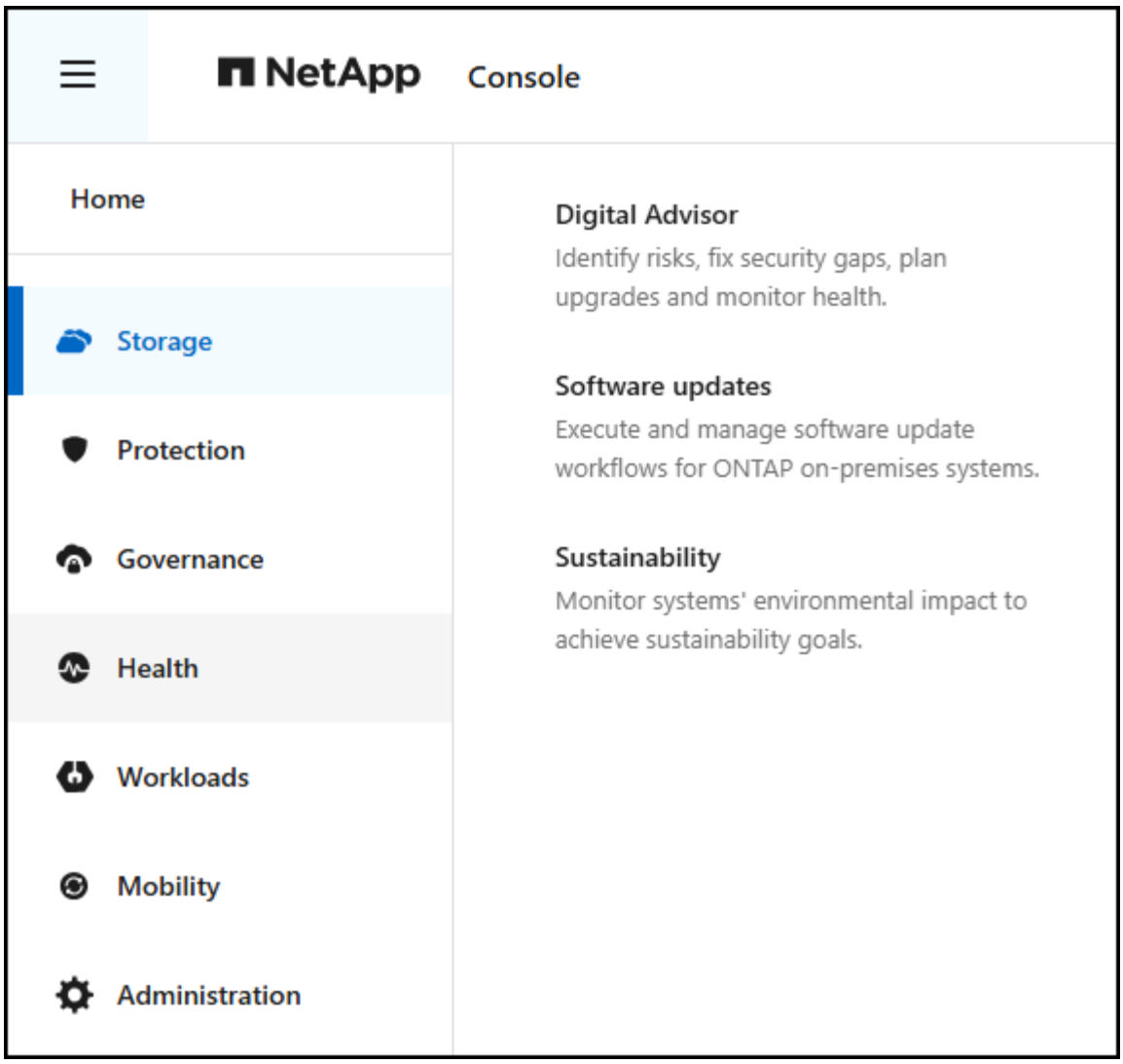
Menu d'administration

Utilisez le menu **Administration** centralisé pour gérer la console NetApp , les cas d'assistance, les licences et les abonnements (anciennement appelé portefeuille numérique).



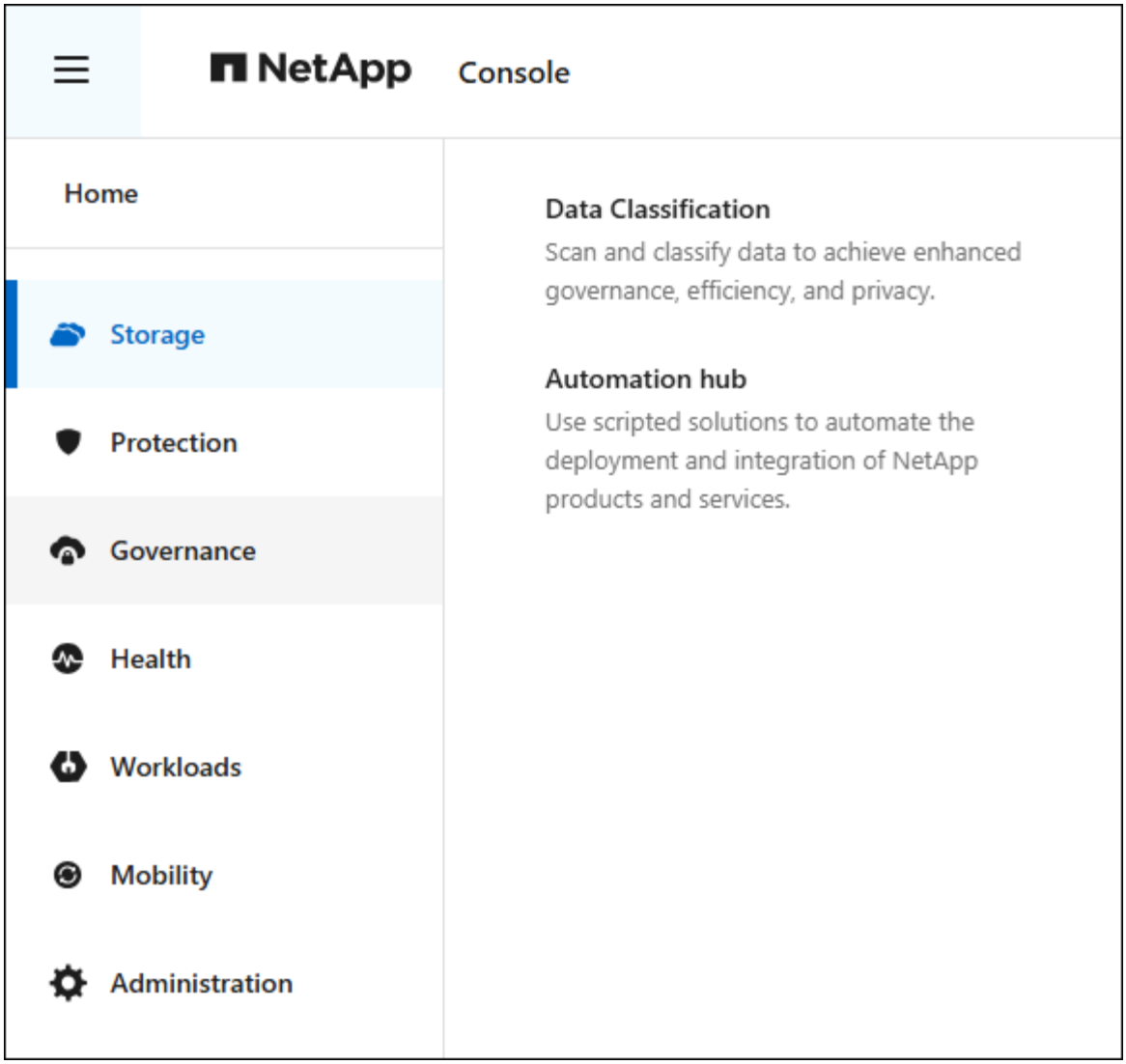
Menu santé

Un menu **Santé** efficace comprend les **Mises à jour logicielles** où vous pouvez gérer les mises à jour du logiciel ONTAP , la **Durabilité** où vous pouvez surveiller votre impact environnemental et le * Digital Advisor* où vous pouvez obtenir des recommandations proactives pour optimiser votre environnement de stockage.



Menu de gouvernance

Le menu **Gouvernance** inclut la **Classification des données** où vous pouvez gérer la classification et la conformité des données et le **Hub d'automatisation** où vous pouvez créer et gérer des flux de travail d'automatisation.



Nommage plus intuitif des éléments, des services de données et des fonctionnalités

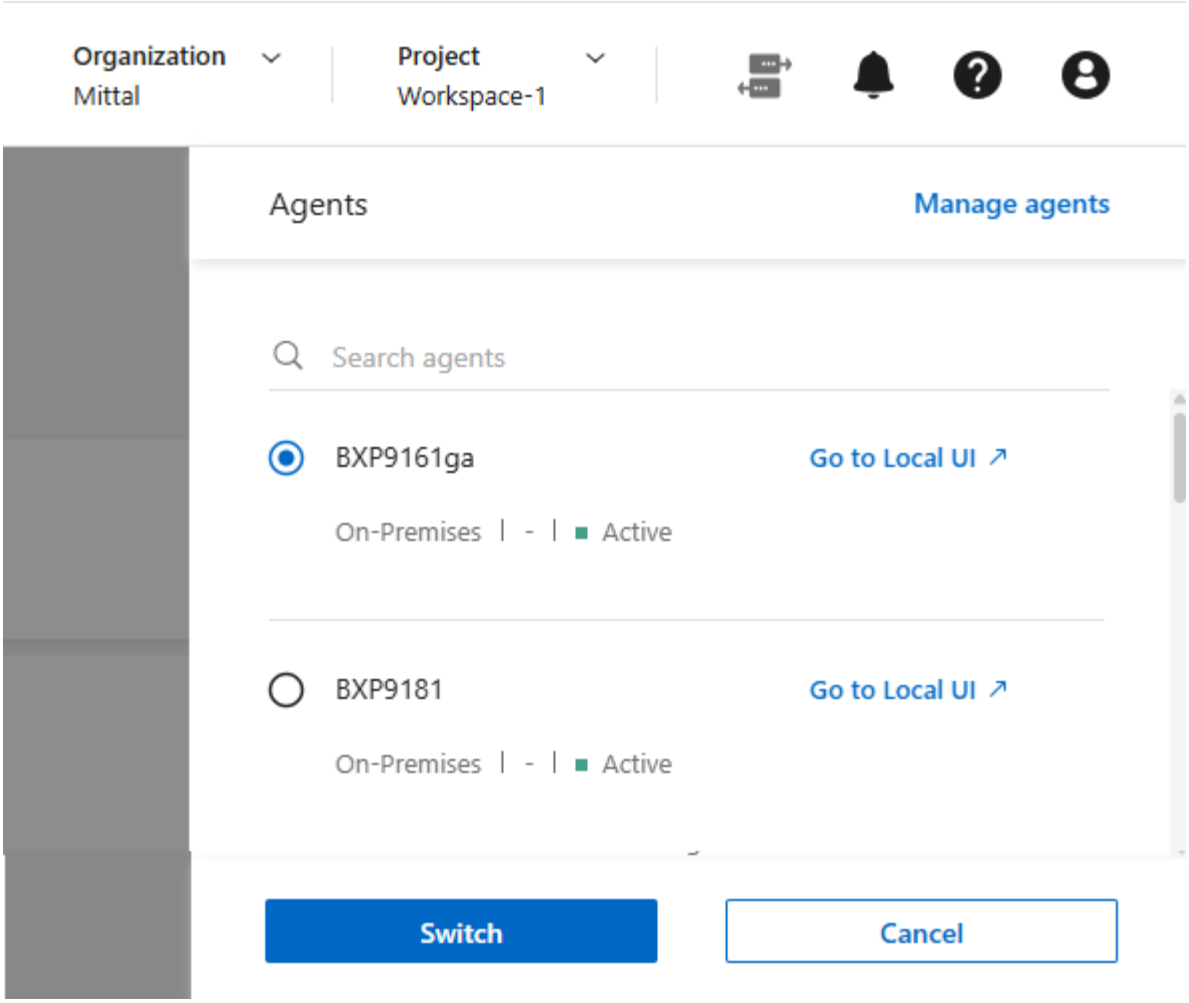
NetApp a renommé plusieurs éléments, services de données et fonctionnalités pour clarifier leur objectif. Les principaux changements incluent :

Nom précédent	* Nom de la console NetApp *
Connecteurs	Agents de console. Affichez, ajoutez et gérez vos agents à partir du menu **Administration > Agents**.
Page de chronologie	Page d'audit Afficher l'activité de la console d'audit à partir du menu **Administration > Audit**.

Nom précédent	* Nom de la console NetApp *
Environnements de travail	Systèmes Affichez, ajoutez et gérez vos systèmes à partir du menu **Stockage > Gestion**.
Protection contre les ransomwares BlueXP	Résilience aux ransomwares NetApp . Ransomware Resilience vous aide à protéger vos données et à récupérer rapidement après une attaque de ransomware.
Efficacité économique de BlueXP	Planification du cycle de vie. La planification du cycle de vie vous aide à optimiser vos coûts de stockage en identifiant les ressources inutilisées et sous-utilisées. Accédez à la planification du cycle de vie à partir du menu **Stockage > Planification du cycle de vie**.
BlueXP digital wallet	Licences et abonnements Accédez à vos licences et abonnements depuis le menu **Administration > Licences et abonnements**.

Agents de console

Accédez et gérez vos agents de console à partir du menu **Administration > Agents**. NetApp a modifié la manière de sélectionner un agent de console pour la page **Systèmes** (anciennement le Canevas). NetApp a remplacé le nom du menu Connecteur par une icône , vous permettant de sélectionner l'agent de console pour lequel vous souhaitez afficher les systèmes.



Vous pouvez également gérer vos agents depuis le menu **Administration > Agents**.

Agent de console 4.0.0

Cette version de l'agent de console inclut des améliorations de sécurité, des corrections de bogues et les nouvelles fonctionnalités suivantes.

La version 4.0.0 est disponible pour le mode standard et le mode restreint.

Consolidation et réduction des points de terminaison réseau requis

NetApp a réduit les points de terminaison réseau requis pour la console et les agents de console, améliorant ainsi la sécurité et simplifiant le déploiement. Il est important de noter que tous les déploiements antérieurs à la version 4.0.0 continuent d'être entièrement pris en charge. Bien que les points de terminaison précédents restent disponibles pour les agents existants, NetApp recommande fortement de mettre à jour les règles de pare-feu vers les points de terminaison actuels après avoir confirmé la réussite des mises à niveau des agents.

- "Apprenez à mettre à jour votre liste de points de terminaison" .
- "En savoir plus sur les points de terminaison requis."

Prise en charge du déploiement VCenter des agents de console

Vous pouvez déployer des agents de console dans des environnements VMware à l'aide d'un fichier OVA. Le fichier OVA inclut une image de machine virtuelle préconfigurée avec un logiciel d'agent de console et des paramètres pour se connecter à la console NetApp . Un téléchargement de fichier ou un déploiement d'URL est disponible directement depuis la console NetApp ."Découvrez comment déployer un agent de console dans les environnements VMware."

L'agent de console OVA pour VMware offre une image VM préconfigurée pour un déploiement rapide.

Rapports de validation pour les déploiements d'agents ayant échoué

Lorsque vous déployez un agent de console à partir de la console NetApp , vous avez désormais la possibilité de valider la configuration de l'agent. Si la console ne parvient pas à déployer l'agent, elle fournit un rapport téléchargeable pour vous aider à résoudre le problème.

Dépannage amélioré pour les agents de console

L'agent de console a amélioré les messages d'erreur qui vous aident à mieux comprendre les problèmes."Découvrez comment dépanner les agents de la console."

Console NetApp

L'administration de la console NetApp inclut les nouvelles fonctionnalités suivantes :

Tableau de bord de la page d'accueil

Le tableau de bord de la page d'accueil de la console NetApp offre une visibilité en temps réel sur l'infrastructure de stockage avec des mesures de santé, de capacité, d'état de licence et de services de données."En savoir plus sur la page d'accueil."

Assistant NetApp

Les nouveaux utilisateurs dotés du rôle d'administrateur d'organisation peuvent utiliser l'assistant NetApp pour configurer la console, notamment pour ajouter un agent, lier un compte de support NetApp et ajouter un système de stockage."En savoir plus sur l'assistant NetApp ."

Authentification du compte de service

La console NetApp prend en charge l'authentification du compte de service à l'aide d'un ID client généré par le système et d'un secret ou de JWT gérés par le client, permettant aux organisations de sélectionner l'approche la mieux adaptée à leurs exigences de sécurité et à leurs flux de travail d'intégration. L'authentification client JWT par clé privée utilise une cryptographie asymétrique, offrant une sécurité plus forte que l'ID client traditionnel et les méthodes secrètes. L'authentification client JWT par clé privée utilise une cryptographie asymétrique, gardant la clé privée sécurisée dans l'environnement du client, réduisant les risques de vol d'informations d'identification et améliorant la sécurité de votre pile d'automatisation et de vos applications clientes."Découvrez comment ajouter un compte de service."

Délais d'expiration de session

Le système déconnecte les utilisateurs après 24 heures ou lorsqu'ils ferment leur navigateur Web.

Soutien aux partenariats entre organisations

Vous pouvez créer des partenariats dans la console NetApp qui permettent aux partenaires de gérer en toute sécurité les ressources NetApp au-delà des frontières organisationnelles, ce qui facilite la collaboration et renforce la sécurité. "Apprenez à gérer les partenariats" .

Rôles de super administrateur et de super spectateur

Ajout des rôles **Super administrateur** et **Super spectateur**. **Super administrateur** accorde un accès de gestion complet aux fonctionnalités de la console, au stockage et aux services de données. **Super viewer** offre une visibilité en lecture seule aux auditeurs et aux parties prenantes. Ces rôles sont utiles pour les petites équipes de membres seniors où un accès large est courant. Pour une sécurité et une auditabilité améliorées, les organisations sont encouragées à utiliser l'accès **Super administrateur** avec parcimonie et à attribuer des rôles précis lorsque cela est possible."En savoir plus sur les rôles d'accès."

Rôle supplémentaire de la résilience aux ransomwares

Ajout du rôle **Administrateur du comportement utilisateur de Ransomware Resilience** et du rôle **Observateur du comportement utilisateur de Ransomware Resilience**. Ces rôles permettent aux utilisateurs de configurer et d'afficher respectivement le comportement des utilisateurs et les données d'analyse."En savoir plus sur les rôles d'accès."

Chat d'assistance supprimé

NetApp a supprimé la fonctionnalité de chat d'assistance de la console NetApp . Utilisez la page **Administration > Support** pour créer et gérer des cas d'assistance.

11 août 2025

Connecteur 3.9.55

Cette version du connecteur BlueXP inclut des améliorations de sécurité et des corrections de bogues.

La version 3.9.55 est disponible pour le mode standard et le mode restreint.

Prise en charge de la langue japonaise

L'interface utilisateur BlueXP est désormais disponible en japonais. Si la langue de votre navigateur est le japonais, BlueXP s'affiche en japonais. Pour accéder à la documentation en japonais, utilisez le menu de langue sur le site Web de documentation.

Fonctionnalité de résilience opérationnelle

La fonctionnalité de résilience opérationnelle a été supprimée de BlueXP. Contactez le support NetApp si vous rencontrez des problèmes.

Gestion des identités et des accès BlueXP (IAM)

La gestion des identités et des accès dans BlueXP fournit désormais la fonctionnalité suivante.

Nouveau rôle d'accès pour le support opérationnel

BlueXP prend désormais en charge un rôle d'analyste de support opérationnel. Ce rôle accorde à un utilisateur les autorisations nécessaires pour surveiller les alertes de stockage, afficher la chronologie d'audit BlueXP et

saisir et suivre les cas de support NetApp .

"En savoir plus sur l'utilisation des rôles d'accès."

31 juillet 2025

Version du mode privé (3.9.54)

Une nouvelle version du mode privé est désormais disponible en téléchargement à partir du "Site de support NetApp"

La version 3.9.54 inclut des mises à jour des composants et services BlueXP suivants.

Composant ou service	Version incluse dans cette version	Modifications depuis la version précédente du mode privé
Connecteur	3.9.54, 3.9.53	Aller à la "Quoi de neuf dans la page BlueXP" et reportez-vous aux modifications incluses pour les versions 3.9.54 et 3.9.53.
Sauvegarde et récupération	28 juillet 2025	Aller à la "Quoi de neuf dans la page de BlueXP backup and recovery ?" et se référer aux modifications incluses dans la version de juillet 2025.
Classification	14 juillet 2025 (version 1.45)	Aller à la "Quoi de neuf dans la page de BlueXP classification" .

Pour plus de détails sur le mode privé, y compris comment effectuer une mise à niveau, reportez-vous à ce qui suit :

- "En savoir plus sur le mode privé"
- "Découvrez comment démarrer avec BlueXP en mode privé"
- "Découvrez comment mettre à niveau le connecteur lors de l'utilisation du mode privé"

21 juillet 2025

Prise en charge des Google Cloud NetApp Volumes

Vous pouvez désormais afficher les Google Cloud NetApp Volumes dans BlueXP."En savoir plus sur Google Cloud NetApp Volumes."

Gestion des identités et des accès BlueXP (IAM)

Nouveau rôle d'accès pour Google Cloud NetApp Volumes

BlueXP prend désormais en charge l'utilisation d'un rôle d'accès pour le système de stockage suivant :

- Google Cloud NetApp Volumes

"En savoir plus sur l'utilisation des rôles d'accès."

14 juillet 2025

Connecteur 3.9.54

Cette version du connecteur BlueXP inclut des améliorations de sécurité, des corrections de bogues et les nouvelles fonctionnalités suivantes :

- Prise en charge des proxys transparents pour les connecteurs dédiés à la prise en charge des services Cloud Volumes ONTAP ."En savoir plus sur la configuration d'un proxy transparent."
- Possibilité d'utiliser des balises réseau pour aider à acheminer le trafic du connecteur lorsque le connecteur est déployé dans un environnement Google Cloud.
- Notifications supplémentaires intégrées au produit pour la surveillance de l'état du connecteur, y compris l'utilisation du processeur et de la RAM.

À l'heure actuelle, la version 3.9.54 est disponible pour le mode standard et le mode restreint.

Gestion des identités et des accès BlueXP (IAM)

La gestion des identités et des accès dans BlueXP offre désormais les fonctionnalités suivantes :

- Prise en charge d'IAM en mode privé, vous permettant de gérer l'accès et les autorisations des utilisateurs pour les services et applications BlueXP .
- Gestion simplifiée des fédérations d'identité, incluant une navigation plus facile, des options plus claires pour la configuration des connexions fédérées et une visibilité améliorée sur les fédérations existantes.
- Rôles d'accès pour la BlueXP backup and recovery, la BlueXP disaster recovery et la gestion de la fédération.

Prise en charge d'IAM en mode privé

BlueXP prend désormais en charge IAM en mode privé, vous permettant de gérer l'accès et les autorisations des utilisateurs pour les services et applications BlueXP . Cette amélioration permet aux clients en mode privé de tirer parti du contrôle d'accès basé sur les rôles (RBAC) pour une meilleure sécurité et conformité.

"En savoir plus sur IAM dans BlueXP."

Gestion simplifiée des fédérations d'identité

BlueXP propose désormais une interface plus intuitive pour la gestion de la fédération d'identité. Cela inclut une navigation plus facile, des options plus claires pour la configuration des connexions fédérées et une meilleure visibilité sur les fédérations existantes.

L'activation de l'authentification unique (SSO) via la fédération d'identité permet aux utilisateurs de se connecter à BlueXP avec leurs informations d'identification d'entreprise. Cela améliore la sécurité, réduit l'utilisation des mots de passe et simplifie l'intégration.

Vous serez invité à importer toutes les connexions fédérées existantes vers la nouvelle interface pour accéder aux nouvelles fonctionnalités de gestion. Cela vous permet de profiter des dernières améliorations sans avoir à recréer vos connexions fédérées."En savoir plus sur l'importation de votre connexion fédérée existante vers BlueXP."

Une gestion améliorée de la fédération vous permet de :

- Ajoutez plusieurs domaines vérifiés à une connexion fédérée, ce qui vous permet d'utiliser plusieurs

domaines avec le même fournisseur d'identité (IdP).

- Désactivez ou supprimez les connexions fédérées lorsque cela est nécessaire, ce qui vous donne le contrôle de l'accès et de la sécurité des utilisateurs.
- Contrôlez l'accès à la gestion de la fédération avec les rôles IAM.

"En savoir plus sur la fédération d'identité dans BlueXP."

Nouveaux rôles d'accès pour la BlueXP backup and recovery, la BlueXP disaster recovery et la gestion de la fédération

BlueXP prend désormais en charge l'utilisation des rôles IAM pour les fonctionnalités et services de données suivants :

- BlueXP backup and recovery
- BlueXP disaster recovery
- Fédération

"En savoir plus sur l'utilisation des rôles d'accès."

9 juin 2025

Connecteur 3.9.53

Cette version du connecteur BlueXP inclut des améliorations de sécurité et des corrections de bogues.

La version 3.9.53 est disponible pour le mode standard et le mode restreint.

Alertes d'utilisation de l'espace disque

Le centre de notifications inclut désormais des alertes sur l'utilisation de l'espace disque sur le connecteur."Apprendre encore plus."

Améliorations de l'audit

La chronologie inclut désormais les événements de connexion et de déconnexion des utilisateurs. Vous pouvez voir l'activité de connexion, ce qui peut aider à l'audit et à la surveillance de la sécurité. Les utilisateurs de l'API qui ont le rôle d'administrateur de l'organisation peuvent afficher l'adresse e-mail de l'utilisateur qui s'est connecté en incluant le `includeUserData=true` paramètre comme dans ce qui suit : `/audit/<account_id>?includeUserData=true` .

Gestion des abonnements Keystone disponible dans BlueXP

Vous pouvez gérer votre abonnement NetApp Keystone depuis BlueXP.

"Découvrez la gestion des abonnements Keystone dans BlueXP."

Gestion des identités et des accès BlueXP (IAM)

Authentification multifacteur (MFA)

Les utilisateurs non fédérés peuvent activer MFA pour leurs comptes BlueXP afin d'améliorer la sécurité. Les administrateurs peuvent gérer les paramètres MFA, notamment la réinitialisation ou la désactivation de MFA pour les utilisateurs selon les besoins. Ceci est pris en charge uniquement en mode standard.

"Découvrez comment configurer l'authentification multifacteur pour vous-même." "Découvrez comment administrer l'authentification multifacteur pour les utilisateurs."

Charges de travail

Vous pouvez désormais afficher et supprimer les informations d'identification Amazon FSx for NetApp ONTAP à partir de la page Informations d'identification dans BlueXP.

29 mai 2025

Version du mode privé (3.9.52)

Une nouvelle version du mode privé est désormais disponible en téléchargement à partir du "Site de support NetApp"

La version 3.9.52 inclut des mises à jour des composants et services BlueXP suivants.

Composant ou service	Version incluse dans cette version	Modifications depuis la version précédente du mode privé
Connecteur	3.9.52, 3.9.51	Aller à la "Quoi de neuf dans la page du connecteur BlueXP" et reportez-vous aux modifications incluses pour les versions 3.9.52 et 3.9.50.
Sauvegarde et récupération	12 mai 2025	Aller à la "Quoi de neuf dans la page de BlueXP backup and recovery ?" et reportez-vous aux modifications incluses dans la version de mai 2025.
Classification	12 mai 2025 (version 1.43)	Aller à la "Quoi de neuf dans la page de BlueXP classification" et reportez-vous aux modifications incluses dans les versions 1.38 à 1.371.41.

Pour plus de détails sur le mode privé, y compris comment effectuer une mise à niveau, reportez-vous à ce qui suit :

- "En savoir plus sur le mode privé"
- "Découvrez comment démarrer avec BlueXP en mode privé"
- "Découvrez comment mettre à niveau le connecteur lors de l'utilisation du mode privé"

12 mai 2025

Connecteur 3.9.52

Cette version du connecteur BlueXP inclut des améliorations de sécurité mineures et des corrections de bogues, ainsi que quelques mises à jour supplémentaires.

À l'heure actuelle, la version 3.9.52 est disponible pour le mode standard et le mode restreint.

Prise en charge de Docker 27 et Docker 28

Docker 27 et Docker 28 sont désormais pris en charge avec le connecteur.

Cloud Volumes ONTAP

Les nœuds Cloud Volumes ONTAP ne s'arrêtent plus lorsque le connecteur n'est plus conforme ou hors service pendant plus de 14 jours. Cloud Volumes ONTAP envoie toujours des messages de gestion des événements lorsqu'il perd l'accès au connecteur. Cette modification vise à garantir que Cloud Volumes ONTAP peut continuer à fonctionner même si le connecteur est en panne pendant une période prolongée. Cela ne modifie pas les exigences de conformité du connecteur.

Administration Keystone disponible dans BlueXP

La version bêta de NetApp Keystone dans BlueXP a ajouté l'accès à l'administration de Keystone . Vous pouvez accéder à la page d'inscription pour la version bêta de NetApp Keystone à partir de la barre de navigation de gauche de BlueXP.

Gestion des identités et des accès BlueXP (IAM)

Nouveaux rôles de gestion du stockage

Les rôles d'administrateur de stockage, de spécialiste de l'état du système et de visualiseur de stockage sont disponibles et peuvent être attribués aux utilisateurs.

Ces rôles vous permettent de gérer qui dans votre organisation peut découvrir et gérer les ressources de stockage, ainsi que d'afficher les informations sur l'état du stockage et d'effectuer des mises à jour logicielles.

Ces rôles sont pris en charge pour contrôler l'accès aux ressources de stockage suivantes :

- Systèmes de la série E
- Systèmes StorageGRID
- Systèmes ONTAP sur site

Vous pouvez également utiliser ces rôles pour contrôler l'accès aux services BlueXP suivants :

- Mises à jour logicielles
- Conseiller numérique
- Résilience opérationnelle
- Efficacité économique
- Durabilité

Les rôles suivants ont été ajoutés :

- **Administrateur de stockage**

  Administrer l'état du stockage, la gouvernance et la découverte des ressources de stockage de l'organisation. Ce rôle peut également effectuer des mises à jour logicielles sur les ressources de stockage.

- **Spécialiste de la santé du système**

  Administrer la santé du stockage et la gouvernance des ressources de stockage de l'organisation. Ce rôle

peut également effectuer des mises à jour logicielles sur les ressources de stockage. Ce rôle ne peut pas modifier ou supprimer les environnements de travail.

- **Visionneuse de stockage**

  Afficher les informations sur l'état du stockage et les données de gouvernance.

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

14 avril 2025

Connecteur 3.9.51

Cette version du connecteur BlueXP inclut des améliorations de sécurité mineures et des corrections de bogues.

À l'heure actuelle, la version 3.9.51 est disponible pour le mode standard et le mode restreint.

Les points de terminaison sécurisés pour les téléchargements de connecteurs sont désormais pris en charge pour la sauvegarde et la récupération et la protection contre les ransomwares

Si vous utilisez la sauvegarde et la récupération ou la protection contre les ransomwares, vous pouvez désormais utiliser des points de terminaison sécurisés pour les téléchargements de connecteurs."Découvrez les points de terminaison sécurisés pour les téléchargements de connecteurs."

Gestion des identités et des accès BlueXP (IAM)

- Les utilisateurs sans administrateur d'organisation ou de dossier ou de projet doivent se voir attribuer un rôle de protection contre les ransomwares pour avoir accès à la protection contre les ransomwares. Vous pouvez attribuer à un utilisateur l'un des deux rôles suivants : administrateur de la protection contre les ransomwares ou visualiseur de la protection contre les ransomwares.
- Les utilisateurs sans administrateur d'organisation ou de dossier ou de projet doivent se voir attribuer un rôle Keystone pour avoir accès à Keystone. Vous pouvez attribuer à un utilisateur l'un des deux rôles suivants : administrateur Keystone ou visualiseur Keystone .

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

- Si vous disposez du rôle d'administrateur d'organisation, de dossier ou de projet, vous pouvez désormais associer un abonnement Keystone à un projet IAM. L'association d'un abonnement Keystone à un projet IAM vous permet de contrôler l'accès à Keystone dans BlueXP.

28 mars 2025

Version du mode privé (3.9.50)

Une nouvelle version du mode privé est désormais disponible en téléchargement à partir du "Site de support NetApp"

La version 3.9.50 inclut des mises à jour des composants et services BlueXP suivants.

Composant ou service	Version incluse dans cette version	Modifications depuis la version précédente du mode privé
Connecteur	3.9.50, 3.9.49	Aller à la "Quoi de neuf dans la page du connecteur BlueXP" et reportez-vous aux modifications incluses pour les versions 3.9.50 et 3.9.49.
Sauvegarde et récupération	17 mars 2025	Aller à la "Quoi de neuf dans la page de BlueXP backup and recovery ?" et reportez-vous aux modifications incluses dans la version de mars 2024.
Classification	10 mars 2025 (version 1.41)	Aller à la "Quoi de neuf dans la page de BlueXP classification" et reportez-vous aux modifications incluses dans les versions 1.38 à 1.371.41.

Pour plus de détails sur le mode privé, y compris comment effectuer une mise à niveau, reportez-vous à ce qui suit :

- "En savoir plus sur le mode privé"
- "Découvrez comment démarrer avec BlueXP en mode privé"
- "Découvrez comment mettre à niveau le connecteur lors de l'utilisation du mode privé"

10 mars 2025

Connecteur 3.9.50

Cette version du connecteur BlueXP inclut des améliorations de sécurité mineures et des corrections de bogues.

- La gestion des systèmes Cloud Volumes ONTAP est désormais prise en charge par les connecteurs sur lesquels SELinux est activé sur le système d'exploitation.

  "En savoir plus sur SELinux"

À l'heure actuelle, la version 3.9.50 est disponible pour le mode standard et le mode restreint.

NetApp Keystone bêta disponible dans BlueXP

NetApp Keystone sera bientôt disponible sur BlueXP et est désormais en version bêta. Vous pouvez accéder à la page d'inscription pour la version bêta de NetApp Keystone à partir de la barre de navigation de gauche de BlueXP.

6 mars 2025

Mise à jour du connecteur 3.9.49

Accès à ONTAP System Manager lorsque BlueXP utilise un connecteur

Un administrateur BlueXP (utilisateurs avec le rôle d'administrateur d'organisation) peut configurer BlueXP pour inviter les utilisateurs à saisir leurs informations d'identification ONTAP afin d'accéder au gestionnaire système ONTAP . Lorsque ce paramètre est activé, les utilisateurs doivent saisir leurs informations d'identification ONTAP à chaque fois car elles ne sont pas stockées dans BlueXP.

Cette fonctionnalité est disponible dans la version 3.9.49 et supérieure de Connector. "Découvrez comment configurer les paramètres d'identification." .

Mise à jour du connecteur 3.9.48

Possibilité de désactiver le paramètre de mise à niveau automatique pour le connecteur

Vous pouvez désactiver la fonction de mise à niveau automatique du connecteur.

Lorsque vous utilisez BlueXP en mode standard ou en mode restreint, BlueXP met automatiquement à niveau votre connecteur vers la dernière version, à condition que le connecteur dispose d'un accès Internet sortant pour obtenir la mise à jour du logiciel. Si vous devez gérer manuellement le moment de la mise à niveau du connecteur, vous pouvez désormais désactiver les mises à niveau automatiques pour le mode standard ou le mode restreint.

Ce changement n'a pas d'impact sur le mode privé BlueXP où vous devez toujours mettre à niveau le connecteur vous-même.

Cette fonctionnalité est disponible dans la version 3.9.48 et supérieure de Connector.

"Découvrez comment désactiver la mise à niveau automatique du connecteur."

18 février 2025

Version du mode privé (3.9.48)

Une nouvelle version du mode privé est désormais disponible en téléchargement à partir du "Site de support NetApp"

La version 3.9.48 inclut des mises à jour des composants et services BlueXP suivants.

Composant ou service	Version incluse dans cette version	Modifications depuis la version précédente du mode privé
Connecteur	3.9.48	Aller à la "Quoi de neuf dans la page du connecteur BlueXP" et reportez-vous aux modifications incluses pour les versions 3.9.48.
Sauvegarde et récupération	21 février 2025	Aller à la "Quoi de neuf dans la page de BlueXP backup and recovery ?" et reportez-vous aux modifications incluses dans la version de février 2025.

Composant ou service	Version incluse dans cette version	Modifications depuis la version précédente du mode privé
Classification	22 janvier 2025 (version 1.39)	Aller à la "Quoi de neuf dans la page de BlueXP classification" et reportez-vous aux modifications incluses dans la version 1.39.

10 février 2025

Connecteur 3.9.49

Cette version du connecteur BlueXP inclut des améliorations de sécurité mineures et des corrections de bogues.

À l'heure actuelle, la version 3.9.49 est disponible pour le mode standard et le mode restreint.

Gestion des identités et des accès BlueXP (IAM)

- Prise en charge de l'attribution de plusieurs rôles à un utilisateur BlueXP .
- Prise en charge de l'attribution d'un rôle sur plusieurs ressources de l'organisation BlueXP (Org/dossier/projet)
- Les rôles sont désormais associés à l'une des deux catégories : plate-forme et service de données.

Le mode restreint utilise désormais BlueXP IAM

La gestion des identités et des accès BlueXP (IAM) est désormais utilisée en mode restreint.

La gestion des identités et des accès BlueXP (IAM) est un modèle de gestion des ressources et des accès qui remplace et améliore les fonctionnalités précédentes fournies par les comptes BlueXP lors de l'utilisation de BlueXP en mode standard et restreint.

Informations connexes

- "En savoir plus sur BlueXP IAM"
- "Démarrer avec BlueXP IAM"

BlueXP IAM offre une gestion plus granulaire des ressources et des autorisations :

- Une *organisation* de niveau supérieur vous permet de gérer l'accès à vos différents *projets*.
- Les *dossiers* vous permettent de regrouper des projets liés.
- La gestion améliorée des ressources vous permet d'associer une ressource à un ou plusieurs dossiers ou projets.

  Par exemple, vous pouvez associer un système Cloud Volumes ONTAP à plusieurs projets.

- La gestion améliorée des accès vous permet d'attribuer un rôle aux membres à différents niveaux de la hiérarchie de l'organisation.

Ces améliorations offrent un meilleur contrôle sur les actions que les utilisateurs peuvent effectuer et sur les ressources auxquelles ils peuvent accéder.

Comment BlueXP IAM affecte votre compte existant en mode restreint

Lorsque vous vous connectez à BlueXP, vous remarquerez ces changements :

- Votre *compte* s'appelle désormais une *organisation*
- Vos *espaces de travail* s'appellent désormais *projets*
- Les noms des rôles d'utilisateur ont changé :
  - *Administrateur du compte* est désormais *Administrateur de l'organisation*
  - *Administrateur de l'espace de travail* est désormais *Administrateur du dossier ou du projet*
  - *Visionneuse de conformité* est désormais *Visionneuse de classification*
- Sous Paramètres, vous pouvez accéder à la gestion des identités et des accès BlueXP pour profiter de ces améliorations

Notez ce qui suit :

- Aucun changement n'est apporté à vos utilisateurs ou environnements de travail existants.
- Bien que les noms des rôles aient changé, il n'y a aucune différence du point de vue des autorisations. Les utilisateurs continueront d'avoir accès aux mêmes environnements de travail qu'auparavant.
- Il n'y a aucun changement dans la façon dont vous vous connectez à BlueXP. BlueXP IAM fonctionne avec les connexions cloud NetApp , les informations d'identification du site de support NetApp et les connexions fédérées, tout comme les comptes BlueXP .
- Si vous aviez plusieurs comptes BlueXP , vous avez désormais plusieurs organisations BlueXP .

API pour BlueXP IAM

Cette modification introduit une nouvelle API pour BlueXP IAM, mais elle est rétrocompatible avec l'API de location précédente. "En savoir plus sur l'API pour BlueXP IAM"

Modes de déploiement pris en charge

BlueXP IAM est pris en charge lors de l'utilisation de BlueXP en mode standard et restreint. Si vous utilisez BlueXP en mode privé, vous continuerez à utiliser un *compte* BlueXP pour gérer les espaces de travail, les utilisateurs et les ressources.

Version du mode privé (3.9.48)

Une nouvelle version du mode privé est désormais disponible en téléchargement à partir du "Site de support NetApp"

La version 3.9.48 inclut des mises à jour des composants et services BlueXP suivants.

Composant ou service	Version incluse dans cette version	Modifications depuis la version précédente du mode privé
Connecteur	3.9.48	Aller à la "Quoi de neuf dans la page du connecteur BlueXP" et reportez-vous aux modifications incluses pour les versions 3.9.48.
Sauvegarde et récupération	21 février 2025	Aller à la "Quoi de neuf dans la page de BlueXP backup and recovery ?" et reportez-vous aux modifications incluses dans la version de février 2025.

Composant ou service	Version incluse dans cette version	Modifications depuis la version précédente du mode privé
Classification	22 janvier 2025 (version 1.39)	Aller à la "Quoi de neuf dans la page de BlueXP classification" et reportez-vous aux modifications incluses dans la version 1.39.

13 janvier 2025

Connecteur 3.9.48

Cette version du connecteur BlueXP inclut des améliorations de sécurité mineures et des corrections de bogues.

À l'heure actuelle, la version 3.9.48 est disponible pour le mode standard et le mode restreint.

Gestion des identités et des accès BlueXP

- La page Ressources affiche désormais les ressources non découvertes. Les ressources non découvertes sont des ressources de stockage que BlueXP connaît mais pour lesquelles vous n'avez pas créé d'environnements de travail. Par exemple, les ressources qui s'affichent dans le conseiller numérique et qui n'ont pas encore d'environnement de travail s'affichent sur la page Ressources en tant que ressources non découvertes.
- Les ressources Amazon FSx for NetApp ONTAP ne s'affichent pas sur la page des ressources IAM car vous ne pouvez pas les associer à un rôle IAM. Vous pouvez afficher ces ressources sur leur toile respective ou à partir des charges de travail.

Créer un dossier d'assistance pour des services BlueXP supplémentaires

Après avoir enregistré BlueXP pour l'assistance, vous pouvez créer un cas d'assistance directement à partir de la console Web BlueXP . Lorsque vous créez le dossier, vous devez sélectionner le service auquel le problème est associé.

À partir de cette version, vous pouvez désormais créer un dossier d'assistance et l'associer à des services BlueXP supplémentaires :

- BlueXP disaster recovery
- BlueXP ransomware protection

"En savoir plus sur la création d'un dossier d'assistance" .

16 décembre 2024

Nouveaux points de terminaison sécurisés pour obtenir des images de connecteur

Lorsque vous installez le connecteur ou lorsqu'une mise à niveau automatique se produit, le connecteur contacte les référentiels pour télécharger des images pour l'installation ou la mise à niveau. Par défaut, le connecteur a toujours contacté les points de terminaison suivants :

- https://*.blob.core.windows.net
- \ https://cloudmanagerinfraprod.azurecr.io

Le premier point de terminaison inclut un caractère générique car nous ne pouvons pas fournir un emplacement définitif. L'équilibrage de charge du référentiel est géré par le fournisseur de services, ce qui signifie que les téléchargements peuvent s'effectuer à partir de différents points de terminaison.

Pour une sécurité accrue, le connecteur peut désormais télécharger les images d'installation et de mise à niveau à partir de points de terminaison dédiés :

- \ https://bluexpinfraprod.eastus2.data.azurecr.io
- \ https://bluexpinfraprod.azurecr.io

Nous vous recommandons de commencer à utiliser ces nouveaux points de terminaison en supprimant les points de terminaison existants de vos règles de pare-feu et en autorisant les nouveaux points de terminaison.

Ces nouveaux points de terminaison sont pris en charge à partir de la version 3.9.47 du connecteur. Il n'y a pas de compatibilité descendante avec les versions précédentes du connecteur.

Notez ce qui suit :

- Les points de terminaison existants sont toujours pris en charge. Si vous ne souhaitez pas utiliser les nouveaux points de terminaison, aucune modification n'est requise.
- Le connecteur contacte d'abord les points de terminaison existants. Si ces points de terminaison ne sont pas accessibles, le connecteur contacte automatiquement les nouveaux points de terminaison.
- Les nouveaux points de terminaison ne sont pas pris en charge dans les scénarios suivants :
  - Si le connecteur est installé dans une région gouvernementale.
  - Si vous utilisez le connecteur avec la BlueXP backup and recovery ou la BlueXP ransomware protection.

  Pour ces deux scénarios, vous pouvez continuer à utiliser les points de terminaison existants.

9 décembre 2024

Connecteur 3.9.47

Cette version du connecteur BlueXP inclut des corrections de bogues et une modification des points de terminaison contactés lors de l'installation du connecteur.

À l'heure actuelle, la version 3.9.47 est disponible pour le mode standard et le mode restreint.

Point de terminaison pour contacter le support NetApp pendant l'installation

Lorsque vous installez manuellement le connecteur, le programme d'installation ne contacte plus \ https://support.netapp.com.

L'installateur contacte toujours \ https://mysupport.netapp.com.

Gestion des identités et des accès BlueXP

La page Connecteurs répertorie uniquement les connecteurs actuellement disponibles. Il n'affiche plus les connecteurs que vous avez supprimés.

26 novembre 2024

Version du mode privé (3.9.46)

Une nouvelle version du mode privé est désormais disponible en téléchargement à partir du "Site de support NetApp"

La version 3.9.46 inclut des mises à jour des composants et services BlueXP suivants.

Composant ou service	Version incluse dans cette version	Modifications depuis la version précédente du mode privé
Connecteur	3.9.46	Améliorations mineures de sécurité et corrections de bugs
Sauvegarde et récupération	22 novembre 2024	Aller à la "Quoi de neuf dans la page de BlueXP backup and recovery ?" et se référer aux modifications incluses dans la version de novembre 2024
Classification	4 novembre 2024 (version 1.37)	Aller à la "Quoi de neuf dans la page de BlueXP classification" et se référer aux modifications incluses dans les versions 1.32 à 1.37
Gestion des Cloud Volumes ONTAP	11 novembre 2024	Aller à la "Quoi de neuf avec la page de gestion de Cloud Volumes ONTAP" et se référer aux modifications incluses dans les versions d'octobre 2024 et de novembre 2024
Gestion des clusters ONTAP sur site	26 novembre 2024	Aller à la "Quoi de neuf avec la page de gestion des clusters ONTAP sur site ?" et se référer aux modifications incluses dans la version de novembre 2024

Bien que le BlueXP digital wallet et la BlueXP replication soient également inclus dans le mode privé, il n'y a aucun changement par rapport à la version précédente du mode privé.

Pour plus de détails sur le mode privé, y compris comment effectuer une mise à niveau, reportez-vous à ce qui suit :

- "En savoir plus sur le mode privé"
- "Découvrez comment démarrer avec BlueXP en mode privé"
- "Découvrez comment mettre à niveau le connecteur lors de l'utilisation du mode privé"

11 novembre 2024

Connecteur 3.9.46

Cette version du connecteur BlueXP inclut des améliorations de sécurité mineures et des corrections de bogues.

À l'heure actuelle, la version 3.9.46 est disponible pour le mode standard et le mode restreint.

ID pour les projets IAM

Vous pouvez désormais afficher l'ID d'un projet à partir de la gestion des identités et des accès BlueXP . Vous devrez peut-être utiliser l'ID lors d'un appel API.

"Apprenez comment obtenir l'ID d'un projet" .

10 octobre 2024

Patch du connecteur 3.9.45

Ce patch inclut des corrections de bugs.

7 octobre 2024

Gestion des identités et des accès BlueXP

La gestion des identités et des accès BlueXP (IAM) est un nouveau modèle de gestion des ressources et des accès qui remplace et améliore les fonctionnalités précédentes fournies par les comptes BlueXP lors de l'utilisation de BlueXP en mode standard.

BlueXP IAM offre une gestion plus granulaire des ressources et des autorisations :

- Une *organisation* de niveau supérieur vous permet de gérer l'accès à vos différents *projets*.
- Les *dossiers* vous permettent de regrouper des projets liés.
- La gestion améliorée des ressources vous permet d'associer une ressource à un ou plusieurs dossiers ou projets.

  Par exemple, vous pouvez associer un système Cloud Volumes ONTAP à plusieurs projets.

- La gestion améliorée des accès vous permet d'attribuer un rôle aux membres à différents niveaux de la hiérarchie de l'organisation.

Ces améliorations offrent un meilleur contrôle sur les actions que les utilisateurs peuvent effectuer et sur les ressources auxquelles ils peuvent accéder.

Comment BlueXP IAM affecte votre compte existant

Lorsque vous vous connectez à BlueXP, vous remarquerez ces changements :

- Votre *compte* s'appelle désormais une *organisation*
- Vos *espaces de travail* s'appellent désormais *projets*
- Les noms des rôles d'utilisateur ont changé :
  - *Administrateur du compte* est désormais *Administrateur de l'organisation*
  - *Administrateur de l'espace de travail* est désormais *Administrateur du dossier ou du projet*

    - *Visionneuse de conformité* est désormais *Visionneuse de classification*
- Sous Paramètres, vous pouvez accéder à la gestion des identités et des accès BlueXP pour profiter de ces améliorations

Notez ce qui suit :

- Aucun changement n'est apporté à vos utilisateurs ou environnements de travail existants.
- Bien que les noms des rôles aient changé, il n'y a aucune différence du point de vue des autorisations. Les utilisateurs continueront d'avoir accès aux mêmes environnements de travail qu'auparavant.
- Il n'y a aucun changement dans la façon dont vous vous connectez à BlueXP. BlueXP IAM fonctionne avec les connexions cloud NetApp , les informations d'identification du site de support NetApp et les connexions fédérées, tout comme les comptes BlueXP .
- Si vous aviez plusieurs comptes BlueXP , vous avez désormais plusieurs organisations BlueXP .

API pour BlueXP IAM

Cette modification introduit une nouvelle API pour BlueXP IAM, mais elle est rétrocompatible avec l'API de location précédente. "En savoir plus sur l'API pour BlueXP IAM"

Modes de déploiement pris en charge

BlueXP IAM est pris en charge lors de l'utilisation de BlueXP en mode standard. Si vous utilisez BlueXP en mode restreint ou en mode privé, vous continuerez à utiliser un *compte* BlueXP pour gérer les espaces de travail, les utilisateurs et les ressources.

Où aller ensuite

- "En savoir plus sur BlueXP IAM"
- "Démarrer avec BlueXP IAM"

Connecteur 3.9.45

Cette version inclut une prise en charge étendue du système d'exploitation et des corrections de bogues.

La version 3.9.45 est disponible pour le mode standard et le mode restreint.

Prise en charge d'Ubuntu 24.04 LTS

À partir de la version 3.9.45, BlueXP prend désormais en charge les nouvelles installations du connecteur sur les hôtes Ubuntu 24.04 LTS lors de l'utilisation de BlueXP en mode standard ou en mode restreint.

"Afficher les exigences de l'hôte du connecteur" .

Prise en charge de SELinux avec les hôtes RHEL

BlueXP prend désormais en charge le connecteur avec les hôtes Red Hat Enterprise Linux sur lesquels SELinux est activé en mode d'application ou en mode permissif.

La prise en charge de SELinux commence avec la version 3.9.40 pour le mode standard et le mode restreint et avec la version 3.9.42 pour le mode privé.

Veuillez noter les limitations suivantes :

- BlueXP ne prend pas en charge SELinux avec les hôtes Ubuntu.
- La gestion des systèmes Cloud Volumes ONTAP n'est pas prise en charge par les connecteurs sur

lesquels SELinux est activé sur le système d'exploitation.

"En savoir plus sur SELinux"

30 septembre 2024

Version du mode privé (3.9.44)

Une nouvelle version du mode privé est désormais disponible en téléchargement à partir du site de support NetApp .

Cette version inclut les versions suivantes des composants et services BlueXP pris en charge avec le mode privé.

Service	Version incluse
Connecteur	3.9.44
Sauvegarde et récupération	27 septembre 2024
Classification	15 mai 2024 (version 1.31)
Gestion des Cloud Volumes ONTAP	9 septembre 2024
Portefeuille numérique	30 juillet 2023
Gestion des clusters ONTAP sur site	22 avril 2024
Réplication	18 septembre 2022

Pour le connecteur, la version 3.9.44 en mode privé inclut les mises à jour introduites dans les versions d'août 2024 et de septembre 2024. Notamment, la prise en charge de Red Hat Enterprise Linux 9.4.

Pour en savoir plus sur ce qui est inclus dans les versions de ces composants et services BlueXP , reportez-vous aux notes de version de chaque service BlueXP :

- "Quoi de neuf dans la version de septembre 2024 du Connecteur"
- "Quoi de neuf dans la version d'août 2024 du Connecteur"
- "Quoi de neuf avec la BlueXP backup and recovery"
- "Quoi de neuf avec la BlueXP classification"
- "Nouveautés de la gestion Cloud Volumes ONTAP dans BlueXP"

Pour plus de détails sur le mode privé, y compris comment effectuer une mise à niveau, reportez-vous à ce qui suit :

- "En savoir plus sur le mode privé"
- "Découvrez comment démarrer avec BlueXP en mode privé"
- "Découvrez comment mettre à niveau le connecteur lors de l'utilisation du mode privé"

9 septembre 2024

Connecteur 3.9.44

Cette version inclut la prise en charge de Docker Engine 26, une amélioration des certificats SSL et des

corrections de bogues.

La version 3.9.44 est disponible pour le mode standard et le mode restreint.

Prise en charge de Docker Engine 26 avec les nouvelles installations

À partir de la version 3.9.44 du connecteur, Docker Engine 26 est désormais pris en charge avec les *nouvelles* installations du connecteur sur les hôtes Ubuntu.

Si vous disposez d'un connecteur existant créé avant la version 3.9.44, Docker Engine 25.0.5 est toujours la version maximale prise en charge sur les hôtes Ubuntu.

"En savoir plus sur les exigences de Docker Engine" .

Certificat SSL mis à jour pour l'accès à l'interface utilisateur locale

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

Dans cette version, nous avons apporté des modifications au certificat SSL pour les connecteurs nouveaux et existants :

- Le nom commun du certificat correspond désormais au nom d'hôte court
- Le nom alternatif du sujet du certificat est le nom de domaine complet (FQDN) de la machine hôte

Prise en charge de RHEL 9.4

BlueXP prend désormais en charge l'installation du connecteur sur un hôte Red Hat Enterprise Linux 9.4 lors de l'utilisation de BlueXP en mode standard ou en mode restreint.

La prise en charge de RHEL 9.4 commence avec la version 3.9.40 du connecteur.

La liste mise à jour des versions RHEL prises en charge pour le mode standard et le mode restreint inclut désormais les éléments suivants :

- 8,6 à 8,10
- 9,1 à 9,4

"En savoir plus sur la prise en charge de RHEL 8 et 9 avec le connecteur" .

Prise en charge de Podman 4.9.4 avec toutes les versions de RHEL

Podman 4.9.4 est désormais pris en charge par toutes les versions prises en charge de Red Hat Enterprise Linux. La version 4.9.4 était auparavant prise en charge uniquement avec RHEL 8.10.

La liste mise à jour des versions Podman prises en charge inclut 4.6.1 et 4.9.4 avec les hôtes Red Hat Enterprise Linux.

Podman est requis pour les hôtes RHEL à partir de la version 3.9.40 du connecteur.

"En savoir plus sur la prise en charge de RHEL 8 et 9 avec le connecteur" .

Autorisations AWS et Azure mises à jour

Nous avons mis à jour les politiques AWS et Azure du connecteur afin de supprimer les autorisations qui ne

sont plus nécessaires. Les autorisations étaient liées à la mise en cache Edge BlueXP et à la découverte et à la gestion des clusters Kubernetes, qui ne sont plus pris en charge depuis août 2024.

- "Découvrez ce qui a changé dans la politique AWS" .
- "Découvrez ce qui a changé dans la politique Azure" .

22 août 2024

Patch du connecteur 3.9.43

Nous avons mis à jour le connecteur pour prendre en charge la version Cloud Volumes ONTAP 9.15.1.

La prise en charge de cette version inclut une mise à jour de la stratégie de connecteur pour Azure. La politique inclut désormais les autorisations suivantes :

```
"Microsoft.Compute/virtualMachineScaleSets/write",
"Microsoft.Compute/virtualMachineScaleSets/read",
"Microsoft.Compute/virtualMachineScaleSets/delete"
```

Ces autorisations sont requises pour la prise en charge des ensembles de machines virtuelles identiques par Cloud Volumes ONTAP . Si vous disposez de connecteurs existants et que vous souhaitez utiliser cette nouvelle fonctionnalité, vous devrez ajouter ces autorisations aux rôles personnalisés associés à vos informations d'identification Azure.

- "En savoir plus sur la version 9.15.1 de Cloud Volumes ONTAP"
- "Afficher les autorisations Azure pour le connecteur" .

8 août 2024

Connecteur 3.9.43

Cette version inclut des améliorations mineures et des corrections de bugs.

La version 3.9.43 est disponible pour le mode standard et le mode restreint.

Mise à jour des exigences en matière de CPU et de RAM

Pour offrir une plus grande fiabilité et améliorer les performances de BlueXP et du connecteur, nous avons désormais besoin de CPU et de RAM supplémentaires pour la machine virtuelle du connecteur :

- CPU : 8 cœurs ou 8 vCPU (l'exigence précédente était de 4)
- RAM : 32 Go (l'exigence précédente était de 14 Go)

Suite à ce changement, le type d'instance de machine virtuelle par défaut lors du déploiement du connecteur à partir de BlueXP ou de la place de marché du fournisseur de cloud est le suivant :

- AWS : t3.2xlarge
- Azure : Standard_D8s_v3
- Google Cloud : n2-standard-8

Les exigences mises à jour en matière de CPU et de RAM s'appliquent à tous les nouveaux connecteurs. Pour les connecteurs existants, il est recommandé d'augmenter le CPU et la RAM pour améliorer les performances et la fiabilité.

Prise en charge de Podman 4.9.4 avec RHEL 8.10

La version 4.9.4 de Podman est désormais prise en charge lors de l'installation du connecteur sur un hôte Red Hat Enterprise Linux 8.10.

Validation des utilisateurs pour la fédération d'identité

Si vous utilisez la fédération d'identité avec BlueXP, chaque utilisateur qui se connecte à BlueXP pour la première fois devra remplir un formulaire rapide pour valider son identité.

31 juillet 2024

Version du mode privé (3.9.42)

Une nouvelle version du mode privé est désormais disponible en téléchargement à partir du site de support NetApp .

Prise en charge de RHEL 8 et 9

Cette version inclut la prise en charge de l'installation du connecteur sur un hôte Red Hat Enterprise Linux 8 ou 9 lors de l'utilisation de BlueXP en mode privé. Les versions suivantes de RHEL sont prises en charge :

- 8,6 à 8,10
- 9,1 à 9,3

Podman est requis comme outil d'orchestration de conteneurs pour ces systèmes d'exploitation.

Vous devez connaître les exigences de Podman, les limitations connues, un résumé de la prise en charge du système d'exploitation, ce qu'il faut faire si vous avez un hôte RHEL 7, comment démarrer, et plus encore.

"En savoir plus sur la prise en charge de RHEL 8 et 9 avec le connecteur" .

Versions incluses dans cette version

Cette version inclut les versions suivantes des services BlueXP qui sont pris en charge avec le mode privé.

Service	Version incluse
Connecteur	3.9.42
Sauvegarde et récupération	18 juillet 2024
Classification	1er juillet 2024 (version 1.33)
Gestion des Cloud Volumes ONTAP	10 juin 2024
Portefeuille numérique	30 juillet 2023
Gestion des clusters ONTAP sur site	30 juillet 2023
Réplication	18 septembre 2022

Pour en savoir plus sur ce qui est inclus dans les versions de ces services BlueXP , reportez-vous aux notes de version de chaque service BlueXP .

- "En savoir plus sur le mode privé"
- "Découvrez comment démarrer avec BlueXP en mode privé"
- "Découvrez comment mettre à niveau le connecteur lors de l'utilisation du mode privé"
- "Découvrez les nouveautés de la BlueXP backup and recovery"
- "Découvrez les nouveautés de la BlueXP classification"
- "Découvrez les nouveautés de la gestion Cloud Volumes ONTAP dans BlueXP"

15 juillet 2024

Prise en charge de RHEL 8.10

BlueXP prend désormais en charge l'installation du connecteur sur un hôte Red Hat Enterprise Linux 8.10 lors de l'utilisation du mode standard ou du mode restreint.

La prise en charge de RHEL 8.10 commence avec la version 3.9.40 du connecteur.

"En savoir plus sur la prise en charge de RHEL 8 et 9 avec le connecteur" .

8 juillet 2024

Connecteur 3.9.42

Cette version inclut des améliorations mineures, des corrections de bogues et la prise en charge du connecteur dans la région AWS Canada Ouest (Calgary).

La version 3.9.42 est disponible pour le mode standard et le mode restreint.

Mise à jour des exigences du moteur Docker

Lorsque le connecteur est installé sur un hôte Ubuntu, la version minimale prise en charge de Docker Engine est désormais 23.0.6. C'était auparavant le 19.3.1.

La version maximale prise en charge est toujours la 25.0.5.

"Afficher les exigences de l'hôte du connecteur" .

La vérification de l'e-mail est désormais requise

Les nouveaux utilisateurs qui s'inscrivent à BlueXP doivent désormais vérifier leur adresse e-mail avant de pouvoir se connecter.

12 juin 2024

Connecteur 3.9.41

Cette version du connecteur BlueXP inclut des améliorations de sécurité mineures et des corrections de bogues.

La version 3.9.41 est disponible pour le mode standard et le mode restreint.

4 juin 2024

Version du mode privé (3.9.40)

Une nouvelle version du mode privé est désormais disponible en téléchargement à partir du site de support NetApp . Cette version inclut les versions suivantes des services BlueXP qui sont pris en charge avec le mode privé.

Notez que cette version en mode privé n'inclut pas la prise en charge du connecteur avec Red Hat Enterprise Linux 8 et 9.

Service	Version incluse
Connecteur	3.9.40
Sauvegarde et récupération	17 mai 2024
Classification	15 mai 2024 (version 1.31)
Gestion des Cloud Volumes ONTAP	17 mai 2024
Portefeuille numérique	30 juillet 2023
Gestion des clusters ONTAP sur site	30 juillet 2023
Réplication	18 septembre 2022

Pour en savoir plus sur ce qui est inclus dans les versions de ces services BlueXP , reportez-vous aux notes de version de chaque service BlueXP .

- "En savoir plus sur le mode privé"
- "Découvrez comment démarrer avec BlueXP en mode privé"
- "Découvrez comment mettre à niveau le connecteur lors de l'utilisation du mode privé"
- "Découvrez les nouveautés de la BlueXP backup and recovery"
- "Découvrez les nouveautés de la BlueXP classification"
- "Découvrez les nouveautés de la gestion Cloud Volumes ONTAP dans BlueXP"

17 mai 2024

Connecteur 3.9.40

Cette version du connecteur BlueXP inclut la prise en charge de systèmes d'exploitation supplémentaires, des améliorations de sécurité mineures et des corrections de bogues.

À l'heure actuelle, la version 3.9.40 est disponible pour le mode standard et le mode restreint.

Prise en charge de RHEL 8 et 9

Le connecteur est désormais pris en charge sur les hôtes exécutant les versions suivantes de Red Hat Enterprise Linux avec de *nouvelles* installations de connecteur lors de l'utilisation de BlueXP en mode standard ou en mode restreint :

- 8,6 à 8,9
- 9,1 à 9,3

Podman est requis comme outil d'orchestration de conteneurs pour ces systèmes d'exploitation.

Vous devez connaître les exigences de Podman, les limitations connues, un résumé de la prise en charge du système d'exploitation, ce qu'il faut faire si vous avez un hôte RHEL 7, comment démarrer, et plus encore.

"En savoir plus sur la prise en charge de RHEL 8 et 9 avec le connecteur" .

Fin du support pour RHEL 7 et CentOS 7

Le 30 juin 2024, RHEL 7 atteindra la fin de maintenance (EOM), tandis que CentOS 7 atteindra la fin de vie (EOL). NetApp continuera à prendre en charge le connecteur sur ces distributions Linux jusqu'au 30 juin 2024.

"Découvrez ce qu'il faut faire si vous disposez d'un connecteur existant exécuté sur RHEL 7 ou CentOS 7" .

Mise à jour des autorisations AWS

Dans la version 3.9.38, nous avons mis à jour la politique de connecteur pour AWS pour inclure l'autorisation « ec2:DescribeAvailabilityZones ». Cette autorisation est désormais requise pour prendre en charge les zones locales AWS avec Cloud Volumes ONTAP.

- "Afficher les autorisations AWS pour le connecteur" .
- "En savoir plus sur la prise en charge des zones locales AWS"

Limitations connues de la console NetApp

Les limitations connues identifient les plates-formes, les appareils ou les fonctions qui ne sont pas pris en charge par cette version du produit ou qui n'interagissent pas correctement avec elle. Examinez attentivement ces limitations.

Ces limitations sont spécifiques à la configuration de la console NEtApp et à l'administration : l'agent, la plateforme SaaS (logiciel en tant que service), etc.

Limitations de l'agent de console

Conflit possible avec les adresses IP dans la plage 172

La console NetApp déploie un agent avec deux interfaces dont les adresses IP sont comprises dans les plages 172.17.0.0/16 et 172.18.0.0/16.

Si votre réseau dispose d'un sous-réseau configuré avec l'une de ces plages, vous risquez de rencontrer des échecs de connectivité depuis la console. Par exemple, la découverte de clusters ONTAP sur site dans la console peut échouer.

Voir l'article de la base de connaissances"Conflit IP de l'agent avec le réseau existant" pour obtenir des instructions sur la façon de modifier l'adresse IP des interfaces de l'agent.

Le décryptage SSL n'est pas pris en charge

La console ne prend pas en charge les configurations de pare-feu pour lesquelles le décryptage SSL est activé. Si le décryptage SSL est activé, des messages d'erreur s'affichent dans la console et l'instance de l'agent s'affiche comme inactive.

Pour une sécurité renforcée, vous avez la possibilité de"installer un certificat HTTPS signé par une autorité de certification (CA)" .

Page blanche lors du chargement de l'interface utilisateur locale

Si vous chargez la console Web exécutée sur un agent, l'interface peut parfois ne pas s'afficher et vous obtenez simplement une page vierge.

Ce problème est lié à un problème de mise en cache. La solution de contournement consiste à utiliser une session de navigateur Web privée ou en mode navigation privée.

Les hôtes Linux partagés ne sont pas pris en charge

L'agent n'est pas pris en charge sur une machine virtuelle partagée avec d'autres applications. La VM doit être dédiée au logiciel agent.

Agents et extensions tiers

Les agents tiers ou les extensions de machine virtuelle ne sont pas pris en charge sur la machine virtuelle de l'agent.

Modifications apportées aux systèmes d'exploitation Linux pris en charge

NetApp ajoute et supprime parfois la prise en charge de l'agent de console sur des systèmes d'exploitation Linux spécifiques. Découvrez comment cette prise en charge affecte vos agents de console existants.

Systèmes d'exploitation pris en charge

NetApp prend en charge l'agent avec les systèmes d'exploitation Linux suivants.

Mode standard

Installation manuelle

- Ubuntu 24.04 LTS
- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8,6 à 8,10
  - 9,1 à 9,4

Déploiement à partir de la console NetApp

Ubuntu 22.04 LTS

Déploiement depuis AWS Marketplace

Ubuntu 22.04 LTS

Déploiement depuis la place de marché Azure

Ubuntu 22.04 LTS

Mode restreint

Installation manuelle

- Ubuntu 24.04 LTS
- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8,6 à 8,10
  - 9,1 à 9,4

Déploiement depuis AWS Marketplace

Ubuntu 22.04 LTS

Déploiement depuis la place de marché Azure

Ubuntu 22.04 LTS

Mode privé

Installation manuelle

- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8,6 à 8,10
  - 9,1 à 9,4

Prise en charge de RHEL 8 et 9

Notez les points suivants concernant la prise en charge de RHEL 8 et 9 :

Limites

La classification des données NetApp est prise en charge si vous installez l'agent sur un hôte RHEL 8 ou 9 résidant sur site. Cette option n'est pas prise en charge si l'hôte RHEL 8 ou 9 réside dans AWS, Azure ou

Google Cloud.

Outil d'orchestration de conteneurs

Vous devez utiliser l'outil Podman comme outil d'orchestration de conteneur lors de l'installation de l'agent de console sur un hôte RHEL 8 ou 9. Docker Engine n'est pas pris en charge avec RHEL 8 et 9.

Mode de déploiement

RHEL 8 et 9 sont pris en charge lors de l'utilisation de la console en mode standard et en mode restreint.

Versions d'agent de console prises en charge

NetApp prend en charge RHEL 8 et 9 à partir des versions suivantes de l'agent de console :

- 3.9.40 lors de l'utilisation de la console en mode standard ou en mode restreint

Nouvelles installations manuelles uniquement

RHEL 8 et 9 sont pris en charge avec les *nouvelles* installations d'agents lors de l'installation manuelle d'agents sur des hôtes exécutés sur vos locaux ou dans le cloud.

Mises à niveau RHEL

Si vous disposez d'un agent existant exécuté sur un hôte RHEL 7, NetApp ne prend pas en charge la mise à niveau du système d'exploitation RHEL 7 vers RHEL 8 ou 9. En savoir plus sur les agents de console existants sur RHEL 7 ou CentOS 7 .

Fin du support pour RHEL 7 et CentOS 7

Le 30 juin 2024, RHEL 7 a atteint la fin de maintenance (EOM), tandis que CentOS 7 a atteint la fin de vie (EOL). NetApp a interrompu la prise en charge des agents sur ces distributions Linux le 30 juin 2024.

"Red Hat : Ce qu'il faut savoir sur la fin de la maintenance de Red Hat Enterprise Linux 7"

Agents de console existants sur RHEL 7 ou CentOS 7

Si vous disposez d'un agent existant exécuté sur RHEL 7 ou CentOS 7, NetApp ne prend pas en charge la mise à niveau ou la conversion du système d'exploitation vers RHEL 8 ou 9. Vous devez créer un nouvel agent sur un système d'exploitation pris en charge.

1. Configurer un hôte RHEL 8 ou 9.
2. Installez Podman.
3. Installer un *nouvel* agent.
4. Configurez l'agent pour découvrir les systèmes que l'agent précédent gérait.

Informations connexes

Comment démarrer avec RHEL 8 et 9

Reportez-vous aux pages suivantes pour plus de détails sur les exigences de l'hôte, les exigences de Podman et les étapes d'installation de Podman et de Cagent :

Mode standard

- "Installer et configurer un agent de console sur site"
- "Installer manuellement l'agent de console dans AWS"
- "Installer manuellement l'agent de console dans Azure"
- "Installer manuellement l'agent de console dans Google Cloud"

Mode restreint

"Préparez-vous au déploiement en mode restreint"

Comment redécouvrir vos systèmes

Reportez-vous aux pages suivantes pour redécouvrir vos systèmes après avoir déployé un nouvel agent de console.

- "Ajouter des systèmes Cloud Volumes ONTAP existants"
- "Découvrez les clusters ONTAP sur site"
- "Créer ou découvrir un système FSx pour ONTAP"
- "Créer un système de Azure NetApp Files"
- "Découvrez les systèmes de la série E"
- "Découvrez les systèmes StorageGRID"

Commencer

Apprendre les bases

En savoir plus sur la console NetApp

La console NetApp offre une gestion centralisée du stockage NetApp et des services de données NetApp dans les environnements locaux et cloud à l'échelle de l'entreprise, offrant des informations en temps réel, des flux de travail plus rapides et une administration simplifiée, hautement sécurisée et conforme.

Il s'agit d'une plate-forme disponible en tant que service (SaaS) qui fournit la gestion du stockage, la mobilité des données, la protection des données, ainsi que l'analyse et le contrôle des données. Les capacités de gestion sont fournies via une console Web et des API.

Caractéristiques

La console unifie la gestion et la protection du stockage sur un multicloud hybride avec des services de données intégrés pour protéger et optimiser les données.

Gestion centralisée du stockage

Découvrez, déployez et gérez le stockage cloud et sur site avec la console.

Stockage cloud et sur site pris en charge

Vous pouvez gérer les types de stockage suivants depuis la console :

Solutions de stockage en nuage

- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Google Cloud NetApp Volumes

Stockage flash et objet sur site

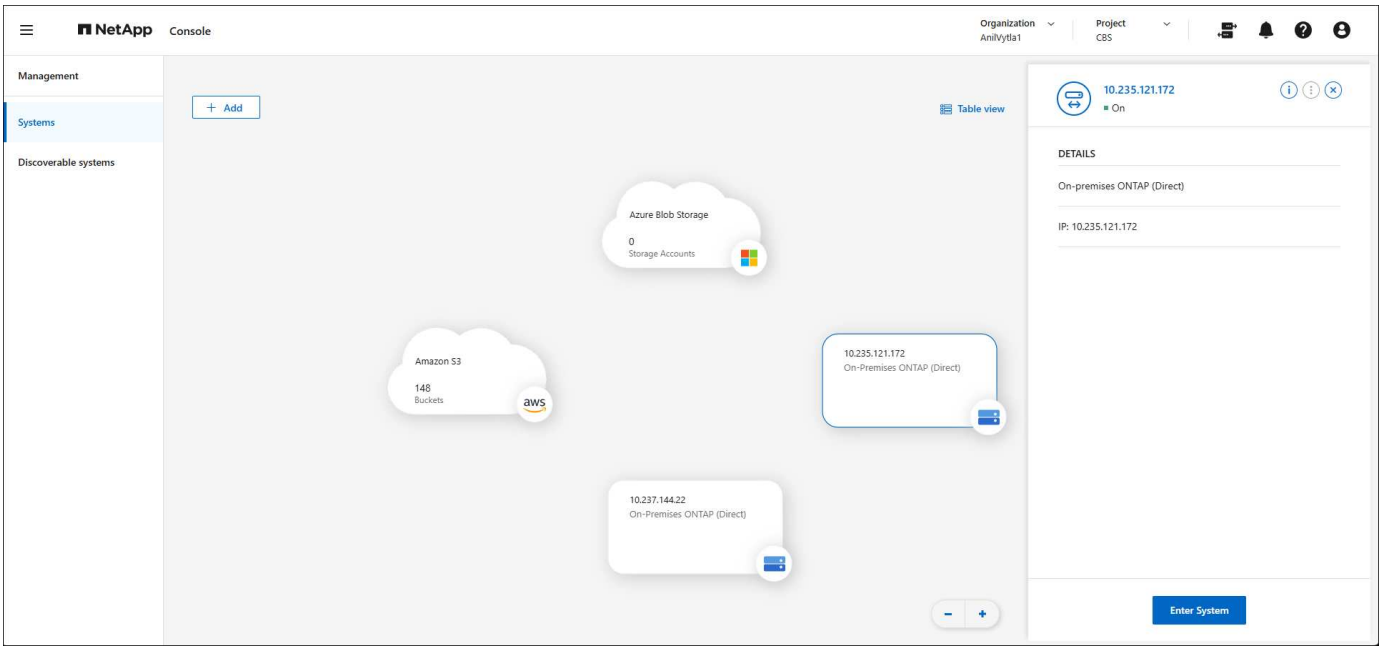
- Systèmes de la série E
- Clusters ONTAP
- Systèmes StorageGRID

Stockage d'objets dans le cloud

- Stockage Amazon S3
- Stockage d'objets blob Azure
- Stockage Google Cloud

Gestion du stockage

Dans la console, les *systèmes* représentent le stockage découvert ou déployé. Vous pouvez sélectionner un *système* pour l'intégrer aux services de données NetApp ou gérer le stockage, comme l'ajout de volumes.



Services de données intégrés et gestion du stockage pour protéger, sécuriser et optimiser les données

La console fournit des services de données pour sécuriser et maintenir la disponibilité du stockage.

Alertes de stockage

Affichez les problèmes liés à la capacité, à la disponibilité, aux performances, à la protection et à la sécurité dans votre environnement ONTAP .

Centre d'automatisation

Utilisez des solutions scriptées pour automatiser le déploiement et l'intégration des produits et services NetApp .

Sauvegarde et récupération NetApp

Sauvegardez et restaurez les données dans le cloud et sur site.

Classification des données NetApp

Préparez vos données d'application et vos environnements cloud à la confidentialité.

Copie et synchronisation NetApp

Synchronisez les données entre les magasins de données sur site et dans le cloud.

Conseiller numérique NetApp (Active IQ)

Utilisez l'analyse prédictive et le support proactif pour optimiser votre infrastructure de données.

Licences et abonnements

Gérez et surveillez vos licences et abonnements.

Reprise après sinistre NetApp

Protégez les charges de travail VMware sur site à l'aide de VMware Cloud sur Amazon FSx for ONTAP comme site de reprise après sinistre.

Planification du cycle de vie

Identifiez les clusters présentant une faible capacité actuelle ou prévue et mettez en œuvre une hiérarchisation des données ou des recommandations de capacité supplémentaires.

Résilience aux ransomwares NetApp

Détectez les anomalies pouvant entraîner des attaques de ransomware. Protégez et récupérez les charges de travail.

Réplication NetApp

Répliquez les données entre les systèmes de stockage pour prendre en charge la sauvegarde et la reprise après sinistre.

Mises à jour logicielles

Automatisez l'évaluation, la planification et l'exécution des mises à niveau ONTAP .

Tableau de bord de durabilité

Analysez la durabilité de vos systèmes de stockage.

Hiérarchisation du cloud NetApp

Étendez votre stockage ONTAP sur site au cloud.

Mise en cache des volumes NetApp

Créez un volume de cache inscriptible pour accélérer l'accès aux données ou décharger le trafic des volumes fortement consultés.

Charges de travail NetApp

Concevez, configurez et exploitez des charges de travail clés à l'aide d' Amazon FSx for NetApp ONTAP.

"En savoir plus sur la console NetApp et les services de données disponibles"

Fournisseurs de cloud pris en charge

La console vous permet de gérer le stockage cloud et d'utiliser les services cloud dans Amazon Web Services, Microsoft Azure et Google Cloud.

Coût

L'utilisation de la console NetApp est gratuite. Vous encourez des frais si vous déployez des agents de console dans le cloud ou si vous utilisez le mode restreint déployé dans le cloud. Certains services de données NetApp entraînent des coûts.https://bluexp.netapp.com/pricing["En savoir plus sur les tarifs des services de données NetApp"^]

Comment fonctionne la console NetApp

La console NetApp est une console Web fournie via la couche SaaS, un système de gestion des ressources et des accès, des agents de console qui gèrent les systèmes de stockage et activent les services de données NetApp , ainsi que différents modes de déploiement pour répondre aux besoins de votre entreprise.

Logiciel en tant que service

Vous accédez à la console via un "interface Web" et API. Cette expérience SaaS vous permet d'accéder automatiquement aux dernières fonctionnalités dès leur sortie.

Gestion des identités et des accès (IAM)

La console fournit une gestion des identités et des accès (IAM) pour la gestion des ressources et des accès. Ce modèle IAM fournit une gestion granulaire des ressources et des autorisations :

- Une *organisation* de niveau supérieur vous permet de gérer l'accès à vos différents *projets*
- Les *dossiers* vous permettent de regrouper des projets liés
- La gestion des ressources vous permet d'associer une ressource à un ou plusieurs dossiers ou projets
- La gestion des accès vous permet d'attribuer un rôle aux membres à différents niveaux de la hiérarchie de l'organisation
- "En savoir plus sur IAM dans la console NetApp"

Agents de console

Un agent de console est nécessaire pour certaines fonctionnalités et services de données supplémentaires. Il vous permet de gérer les ressources et les processus dans vos environnements sur site et dans le cloud. Vous en avez besoin pour gérer certains systèmes (par exemple, Cloud Volumes ONTAP) et pour utiliser certains services de données NetApp .

"En savoir plus sur les agents de console" .

Modes de déploiement

NetApp propose deux modes de déploiement pour la console NetApp : le *mode standard* utilise une couche de logiciel en tant que service (SaaS) pour une fonctionnalité complète, tandis que le *mode restreint* limite la connectivité sortante.

NetApp continue de proposer BlueXP pour les sites qui n'ont pas besoin de connectivité sortante. BlueXP est disponible uniquement en mode privé."Découvrez BlueXP (mode privé) pour les sites sans connexion Internet."

"En savoir plus sur les modes de déploiement" .

Certification SOC 2 Type 2

Un cabinet d'expertise comptable et d'auditeur de services indépendant a examiné la console et a affirmé qu'elle avait obtenu les rapports SOC 2 Type 2 sur la base des critères applicables des services de confiance.

"Consultez les rapports SOC 2 de NetApp"

En savoir plus sur les agents de la console NetApp

Un *agent de console* s'exécute sur votre réseau cloud ou sur votre réseau local. Vous utilisez un agent de console pour connecter les services de console NetApp à vos environnements de stockage.

Ce que vous pouvez faire sans agent de console

Certaines fonctionnalités et services de la console sont disponibles si vous ne déployez pas d'agent de console :

- Amazon FSx for NetApp ONTAP

Certaines actions nécessitent un agent de console ou un lien NetApp Workloads. "Découvrez quelles actions nécessitent un agent ou un lien de console"

- Centre d'automatisation
- Azure NetApp Files

  Vous n'avez pas besoin d'un agent de console pour gérer Azure NetApp Files, mais un agent est requis pour utiliser la classification des données NetApp pour analyser Azure NetApp Files.

- Google Cloud NetApp Volumes
- Copie et synchronisation NetApp
- Conseiller numérique
- Surveiller l'utilisation des licences, la surveillance des abonnements nécessite un agent de console

  Vous pouvez généralement ajouter une licence à la console NetApp sans agent de console.

  Un agent est requis pour ajouter des licences Cloud Volumes ONTAP *basées sur les nœuds* car les données proviennent des licences installées sur les systèmes Cloud Volumes ONTAP .

- Découverte directe des clusters ONTAP sur site

  Vous n'avez pas besoin d'un agent de console pour ajouter un cluster ONTAP local à la console, mais un agent est requis pour des fonctionnalités de console et des services de données supplémentaires.

  "En savoir plus sur les options de découverte et de gestion des clusters ONTAP sur site"

- Mises à jour logicielles
- Durabilité
- Charges de travail NetApp

Lorsqu'un agent de console est requis

En mode standard, la console nécessite un agent de console pour :

- Alertes
- Fonctionnalités de gestion Amazon FSx pour ONTAP
- Stockage Amazon S3
- Stockage d'objets blob Azure
- Sauvegarde et récupération NetApp
- Classification des données
- Cloud Volumes ONTAP
- Reprise après sinistre NetApp
- Systèmes de la série E
- Efficacité économique [1]
- Compartiments de stockage Google Cloud
- Intégration du cluster ONTAP sur site avec les services de données NetApp
- Résilience aux ransomwares NetApp

- Systèmes StorageGRID
- Hiérarchisation du cloud NetApp
- Mise en cache des volumes NetApp

[1] Vous pouvez accéder à ces services sans agent de console, mais un agent de console est requis pour lancer des actions.

Vous avez toujours besoin d'un agent de console pour utiliser la console en mode restreint.

Les agents de console doivent être opérationnels à tout moment

Les agents de console sont un élément fondamental de la console NetApp . 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 console NetApp" .

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. La façon de commencer dépend du fait que vous utilisez la console en mode

standard ou en mode restreint.

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

Autorisations Cloud

Vous avez besoin d'autorisations spécifiques pour créer l'agent de console directement à partir de la console NetApp et d'un autre ensemble d'autorisations pour l'instance de l'agent de console elle-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.

En mode standard ou restreint, l'agent de la 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.

En savoir plus sur les modes de déploiement de la console NetApp

La console NetApp propose plusieurs *modes de déploiement* qui vous permettent de répondre à vos exigences commerciales et de sécurité.

- Le *mode standard* s'appuie sur une couche de logiciel en tant que service (SaaS) pour fournir toutes les fonctionnalités. Les utilisateurs accèdent à la console via une interface hébergée basée sur le Web
- Le *mode restreint* est disponible pour les organisations qui ont des restrictions de connectivité et qui souhaitent installer la console NetApp dans leur propre cloud public. Les utilisateurs accèdent à la console via une interface Web hébergée sur un agent de console dans leur environnement cloud.

  La console NetApp restreint le trafic, la communication et les données en mode restreint, et vous devez vous assurer que votre environnement (sur site et dans le cloud) est conforme aux réglementations requises.

Aperçu

Chaque mode de déploiement diffère en termes de connectivité sortante, d'emplacement, d'installation, d'authentification, de services de données et de méthodes de facturation.

Mode standard

Vous utilisez un service SaaS depuis la console Web. Selon les services de données et les fonctionnalités que vous prévoyez d'utiliser, un administrateur d'organisation de console crée un ou plusieurs agents de console pour gérer les données dans votre environnement de cloud hybride.

Ce mode utilise la transmission de données cryptées sur l'Internet public.

Mode restreint

Vous installez un agent de console dans le cloud (dans une région gouvernementale, souveraine ou commerciale) et sa connectivité sortante vers la couche SaaS de la console NetApp est limitée.

Ce mode est généralement utilisé par les gouvernements étatiques et locaux et par les entreprises réglementées.

En savoir plus sur la connectivité sortante vers la couche SaaS .

Mode privé BlueXP (interface BlueXP héritée uniquement)

Le mode privé BlueXP (interface BlueXP héritée) est généralement utilisé avec des environnements locaux qui n'ont pas de connexion Internet et avec des régions cloud sécurisées, notamment AWS Secret Cloud, AWS Top Secret Cloud et Azure IL6. NetApp continue de prendre en charge ces environnements avec l'interface BlueXP héritée."Documentation PDF pour le mode privé BlueXP"

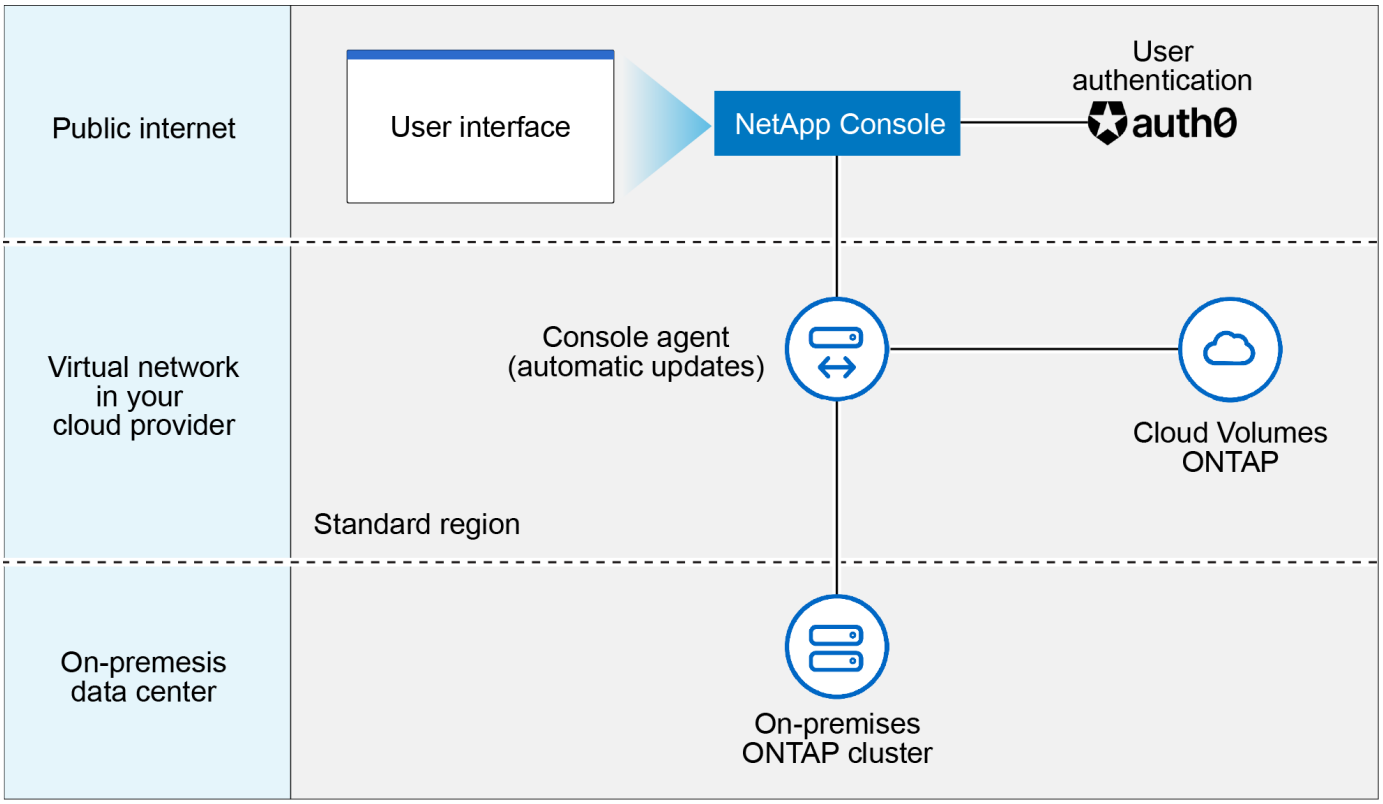
Le tableau suivant fournit une comparaison de la console NetApp .

	Mode standard	Mode restreint
Connexion requise à la couche SaaS de la console NetApp ?	Oui	Sortie uniquement
Connexion requise à votre fournisseur cloud ?	Oui	Oui, dans la région
Installation de l'agent de console	Depuis la console, la place de marché cloud ou l'installation manuelle	Place de marché cloud ou installation manuelle
Mises à niveau de l'agent de console	Mises à niveau automatiques	Mises à niveau automatiques
Accès UI	Depuis la couche SaaS de la console	Localement à partir d'une machine virtuelle d'agent
Point de terminaison de l'API	La couche SaaS de la console	Un agent de console
Authentification	Via SaaS en utilisant auth0, la connexion NSS ou la fédération d'identité	Via SaaS en utilisant auth0 ou la fédération d'identité
Authentification multifacteur	Disponible pour les utilisateurs locaux	Non disponible
Services de stockage et de données	Tous sont pris en charge	Beaucoup sont soutenus
Options de licence de service de données	Abonnements Marketplace et BYOL	Abonnements Marketplace et BYOL

Lisez les sections suivantes pour en savoir plus sur ces modes, notamment les fonctionnalités et services de la console NetApp pris en charge.

Mode standard

L'image suivante est un exemple de déploiement en mode standard.



La console fonctionne comme suit en mode standard :

Communication sortante

La connectivité est requise entre un agent de console et la couche SaaS de la console, les ressources accessibles au public de votre fournisseur de cloud et d'autres composants essentiels aux opérations quotidiennes.

- "Points de terminaison qu'un agent contacte dans AWS"
- "Points de terminaison qu'un agent contacte dans Azure"
- "Points de terminaison qu'un agent contacte dans Google Cloud"

Emplacement pris en charge pour un agent

En mode standard, un agent est pris en charge dans le cloud ou dans vos locaux.

Installation de l'agent de console

Vous pouvez installer un agent en utilisant l'une des méthodes suivantes :

- Depuis la console
- Depuis AWS ou Azure Marketplace
- Depuis le SDK Google Cloud
- Manuellement à l'aide d'un installateur sur un hôte Linux dans votre centre de données ou votre cloud
- Utilisez l'OVA fourni dans votre environnement VCenter.

Mises à niveau de l'agent de console

NetApp met automatiquement à niveau votre agent tous les mois.p.

Accès à l'interface utilisateur

L'interface utilisateur est accessible depuis la console Web fournie via la couche SaaS.

Point de terminaison de l'API

Les appels API sont effectués vers le point de terminaison suivant : \ https://api.bluexp.netapp.com

Authentification

Authentification avec les connexions auth0 ou NetApp Support Site (NSS). La fédération d'identité est disponible.

Services de données pris en charge

Tous les services de données NetApp sont pris en charge. "En savoir plus sur les services de données NetApp" .

Options de licence prises en charge

Les abonnements Marketplace et BYOL sont pris en charge avec le mode standard ; toutefois, les options de licence prises en charge dépendent du service de données NetApp que vous utilisez. Consultez la documentation de chaque service pour en savoir plus sur les options de licence disponibles.

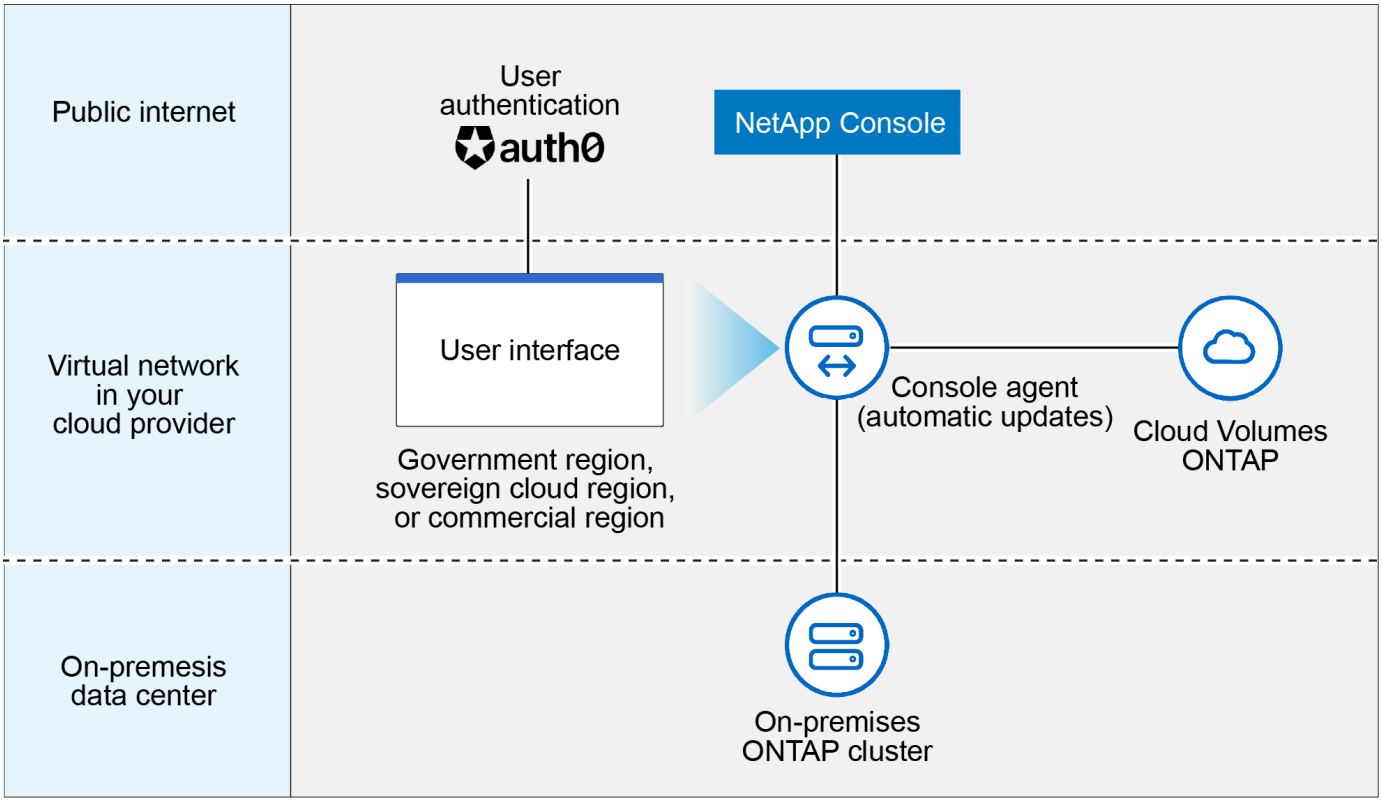
Comment démarrer avec le mode standard

Aller à la "Console NetApp" et inscrivez-vous.

"Découvrez comment démarrer avec le mode standard" .

Mode restreint

L'image suivante est un exemple de déploiement en mode restreint.



La console fonctionne comme suit en mode restreint :

Communication sortante

Un agent nécessite une connectivité sortante vers la couche SaaS de la console pour les services de données, les mises à niveau logicielles, l'authentification et la transmission de métadonnées.

La couche SaaS de la console n'initie pas de communication avec un agent. Les agents initient toutes les communications avec la couche SaaS de la console, en extrayant ou en poussant les données selon les besoins.

Une connexion est également requise aux ressources du fournisseur cloud de la région.

Emplacement pris en charge pour un agent

En mode restreint, un agent est pris en charge dans le cloud : dans une région gouvernementale, une région souveraine ou une région commerciale.

Installation de l'agent de console

Vous pouvez installer à partir d'AWS ou d'Azure Marketplace ou une installation manuelle sur votre propre hôte Linux ou utiliser un OVA téléchargeable dans votre environnement VCenter.

Mises à niveau de l'agent de console

NetApp met automatiquement à niveau votre logiciel agent avec des mises à jour mensuelles.

Accès à l'interface utilisateur

L'interface utilisateur est accessible à partir d'une machine virtuelle agent déployée dans votre région cloud.

Point de terminaison de l'API

Les appels API sont effectués vers la machine virtuelle de l'agent.

Authentification

L'authentification est fournie via auth0. La fédération d'identité est également disponible.

Gestion du stockage et services de données pris en charge

Les services de stockage et de données suivants avec mode restreint :

Services pris en charge	Remarques
Azure NetApp Files	Support complet
Sauvegarde et récupération	Pris en charge dans les régions gouvernementales et les régions commerciales avec mode restreint. Non pris en charge dans les régions souveraines avec mode restreint. En mode restreint, NetApp Backup and Recovery prend en charge la sauvegarde et la restauration des données de volume ONTAP uniquement. "Afficher la liste des destinations de sauvegarde prises en charge pour les données ONTAP" La sauvegarde et la restauration des données d'application et des données de machine virtuelle ne sont pas prises en charge.

Services pris en charge	Remarques
Classification des données NetApp	Pris en charge dans les régions gouvernementales avec mode restreint. Non pris en charge dans les régions commerciales ou dans les régions souveraines avec mode restreint.
Cloud Volumes ONTAP	Support complet
Licences et abonnements	Vous pouvez accéder aux informations de licence et d'abonnement avec les options de licence prises en charge répertoriées ci-dessous pour le mode restreint.
Clusters ONTAP sur site	La découverte avec un agent de console et la découverte sans agent de console (découverte directe) sont toutes deux prises en charge. Lorsque vous découvrez un cluster local sans agent de console, la vue avancée (Gestionnaire système) n'est pas prise en charge.
Réplication	Pris en charge dans les régions gouvernementales avec mode restreint. Non pris en charge dans les régions commerciales ou dans les régions souveraines avec mode restreint.

Options de licence prises en charge

Les options de licence suivantes sont prises en charge avec le mode restreint :

- Abonnements Marketplace (contrats horaires et annuels)

  Notez ce qui suit :

  - Pour Cloud Volumes ONTAP, seules les licences basées sur la capacité sont prises en charge.
  - Dans Azure, les contrats annuels ne sont pas pris en charge avec les régions gouvernementales.
- Apportez votre propre vin

  Pour Cloud Volumes ONTAP, les licences basées sur la capacité et les licences basées sur les nœuds sont prises en charge avec BYOL.

Comment démarrer avec le mode restreint

Vous devez activer le mode restreint lorsque vous créez votre organisation NetApp Console.

Si vous n'avez pas encore d'organisation, vous êtes invité à créer votre organisation et à activer le mode restreint lorsque vous vous connectez à la console pour la première fois à partir d'un agent de console que vous avez installé manuellement ou que vous avez créé à partir de la place de marché de votre fournisseur de cloud.

Vous ne pouvez pas modifier le paramètre du mode restreint après avoir créé l'organisation.

"Découvrez comment démarrer avec le mode restreint" .

Comparaison des services et des fonctionnalités

Le tableau suivant peut vous aider à identifier rapidement les services et fonctionnalités pris en charge par le mode restreint.

Notez que certains services peuvent être pris en charge avec des limitations. Pour plus de détails sur la manière dont ces services sont pris en charge avec le mode restreint, reportez-vous aux sections ci-dessus.

Domaine de produits	Service ou fonctionnalité de données NetApp	Mode restreint
Stockage Cette partie du tableau répertorie la prise en charge de la gestion des systèmes de stockage à partir de la console. Il n'indique pas les destinations de sauvegarde prises en charge pour NetApp Backup and Recovery.	Amazon FSx pour ONTAP	Non
	Amazon S3	Non
	Azure Blob	Non
	Azure NetApp Files	Oui
	Cloud Volumes ONTAP	Oui
	Google Cloud NetApp Volumes	Non
	Stockage Google Cloud	Non
	Clusters ONTAP sur site	Oui
	E-Series	Non
	StorageGRID	Non
Services de données	Sauvegarde et récupération NetApp	Ouihttps://docs.netapp.com/us-en/bluexp-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-limited-internet-connectivity["Afficher la liste des destinations de sauvegarde prises en charge pour les données de volume ONTAP"^]
	Classification des données NetApp	Oui
	Copie et synchronisation NetApp	Non
	Reprise après sinistre NetApp	Non
	Résilience aux ransomwares NetApp	Non
	Réplication NetApp	Oui
	Hiérarchisation du cloud NetApp	Non
	Mise en cache des volumes NetApp	Non
	Usine de charges de travail NetApp	Non

Domaine de produits	Service ou fonctionnalité de données NetApp	Mode restreint
Caractéristiques	Alertes	Non
	Digital Advisor	Non
	Gestion des licences et des abonnements	Oui
	Gestion des identités et des accès	Oui
	Informations d'identification	Oui
	Fédération	Oui
	Planification du cycle de vie	Non
	Authentification multifacteur	Oui
	Comptes NSS	Oui
	Notifications	Oui
	Recherche	Oui
	Mises à jour logicielles	Non
	Durabilité	Non
	Audit	Oui

Démarrer avec l'assistant NetApp

Commencer à utiliser l'assistant de console NetApp

Si vous utilisez la console NetApp pour la première fois avec le rôle d'administrateur d'organisation, vous pouvez utiliser l'assistant de console pour vous guider tout au long du processus de configuration initiale. L'assistant vous aide à ajouter un compte de site de support NetApp (NSS), à ajouter un agent de console, à ajouter un cluster et à ajouter une licence ou un abonnement, ce qui facilite la prise en main de la gestion de vos données.

Rôles requis pour accéder à l'assistant de console

L'assistant de console est uniquement disponible pour les utilisateurs disposant du rôle d'administrateur d'organisation.

Quand l'assistant de console apparaît-il ?

L'assistant de console est disponible sur la page d'accueil de la console NetApp jusqu'à ce que les tâches de configuration obligatoires soient terminées.

Utilisez l'Assistant pour effectuer ces tâches, dont certaines sont obligatoires :

- Ajoutez un compte de site de support NetApp (NSS).
- Connectez-vous à votre parc de stockage en déployant un agent de console (étape obligatoire).

- Gérez votre système en ajoutant ou en découvrant un cluster (étape obligatoire).
- Ajoutez un abonnement au marketplace ou une licence PAYGO.
- Liens vers les services de données ouvertes.

Activer l'assistant de console

Par défaut, la console NetApp affiche l'assistant de console sur la page d'accueil pour les nouveaux utilisateurs disposant du rôle d'administrateur d'organisation.

Vous ne pouvez fermer l'assistant que lorsque vous ou quelqu'un d'autre avez terminé les éléments obligatoires. Une fois les éléments obligatoires terminés, l'Assistant est fermé pour tous les utilisateurs de votre organisation et n'apparaît plus.

Utilisez l'assistant de console pour commencer

L'assistant de console vous guide dans la configuration de votre environnement de console NetApp avec ces tâches :

- Ajoutez un compte de site de support NetApp (NSS).
- Connectez-vous à votre parc de stockage en déployant un agent de console, sur site ou dans le cloud. Vous pouvez le déployer manuellement ou en téléchargeant un OVA. Cette étape est obligatoire.
- Gérez votre système en ajoutant ou en découvrant un cluster. Cette étape est obligatoire.
- Ajoutez un abonnement au marketplace ou une licence PAYGO.
- En savoir plus sur les services de données NetApp .

Démarrer avec le mode standard

Démarrage du flux de travail (mode standard)

Commencez à utiliser la console NetApp en mode standard en préparant la mise en réseau pour la console, en vous inscrivant et en créant un compte, et éventuellement en créant un agent de console.

En mode standard, vous accédez à une console Web hébergée en tant que produit SaaS (Software-as-a-service) de NetApp. Avant de commencer, assurez-vous de bien comprendre"modes de déploiement" et"Agents de console" .

1 **"Préparer le réseau pour l'utilisation de la console NetApp"**

Les ordinateurs qui accèdent à la console NetApp doivent disposer de connexions à des points de terminaison spécifiques. Si votre réseau restreint l'accès sortant, vous devez vous assurer que ces points de terminaison sont autorisés.

2 **"Inscrivez-vous et créez une organisation"**

Aller à la "Console NetApp" et inscrivez-vous. Vous aurez la possibilité de créer une organisation, mais vous devez ignorer cette étape si votre entreprise possède déjà une organisation existante.

À ce stade, vous êtes connecté et pouvez commencer à gérer le stockage et à utiliser des services tels que Digital Advisor, Amazon FSx for ONTAP, Azure NetApp Files, etc. "Découvrez ce que vous pouvez faire sans agent de console" .

3 Créer un agent de console

Les fonctionnalités avancées de gestion du stockage et certains services de données NetApp nécessitent l'installation d'un agent de console. L'agent de console permet à la console de gérer les ressources et les processus au sein de votre environnement cloud hybride.

Vous pouvez créer un agent de console dans votre réseau cloud ou sur site.

- "En savoir plus sur les cas où les agents de console sont requis et leur fonctionnement"
- "Découvrez comment créer un agent de console dans AWS"
- "Découvrez comment créer un agent de console dans Azure"
- "Découvrez comment créer un agent de console dans Google Cloud"
- "Découvrez comment créer un agent de console sur site"

Pour utiliser NetApp Intelligent Data Services pour la gestion du stockage et des données dans Google Cloud, assurez-vous que l'agent de la console s'exécute dans Google Cloud.

4 "Abonnez-vous aux services intelligents NetApp (facultatif)"

Inscrivez-vous aux services intelligents NetApp via votre fournisseur de cloud pour payer à l'heure (PAYGO) ou via un contrat annuel. Les services intelligents NetApp incluent NetApp Backup and Recovery, Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience et NetApp Disaster Recovery. La classification des données NetApp est incluse dans votre abonnement sans frais supplémentaires.

Préparer l'accès réseau pour la console NetApp

La console NetApp , l'agent de la console NetApp et les services de données NetApp nécessitent un accès Internet sortant et la possibilité de contacter les points de terminaison nécessaires.

Vous devrez configurer l'accès au réseau pour les éléments suivants :

- Ordinateurs qui accèdent à la console NetApp en tant que logiciel en tant que service (SaaS)
- Emplacements réseau où vous déployez les agents de console que vous installez sur site ou dans le cloud.
- Points de terminaison supplémentaires pour certains services de données NetApp , notamment Cloud Volumes ONTAP.

> NetApp a réduit les points de terminaison réseau requis pour la console et les agents de console, améliorant ainsi la sécurité et simplifiant le déploiement. Il est important de noter que tous les déploiements antérieurs à la version 4.0.0 continuent d'être entièrement pris en charge. Bien que les points de terminaison précédents restent disponibles pour les agents existants, NetApp recommande fortement de mettre à jour les règles de pare-feu vers les points de terminaison actuels après avoir confirmé la réussite des mises à niveau des agents."Découvrez comment mettre à jour votre liste de points de terminaison."

Points de terminaison contactés par la console NetApp

Chaque ordinateur qui accède à la console NetApp doit disposer de connexions aux points de terminaison répertoriés ci-dessous.

Le système contacte ces points de terminaison dans deux scénarios :

- À partir d'un ordinateur accédant au "Console NetApp" en tant que logiciel en tant que service (SaaS).
- Depuis un ordinateur accédant directement à un hôte d'agent de console, soit pour se connecter et le configurer, soit pour accéder à la console à partir de l'hôte de l'agent.

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

Préparer la mise en réseau pour l'agent de la console

Vous installez l'agent de console sur site ou dans le cloud, et il contacte les points de terminaison pour effectuer les actions initiées par la console.

Les agents de console doivent avoir accès aux mêmes points de terminaison que la console NetApp , ainsi qu'à des points de terminaison supplémentaires en fonction de l'endroit où vous installez l'agent.

Configurez l'accès au point de terminaison réseau avant d'installer l'agent de la console.

- "Configurer l'accès au réseau AWS pour un agent de console"
- "Configurer l'accès au réseau Azure pour un agent de console"
- "Configurer l'accès au réseau Google Cloud pour un agent de console"
- "Configurer l'accès au réseau local pour un agent de console"

Préparer la mise en réseau pour Cloud Volumes ONTAP

Certains services de données NetApp ainsi que Cloud Volumes ONTAP nécessitent que l'agent dispose d'un accès Internet sortant supplémentaire.

Points de terminaison pour Cloud Volumes ONTAP

- "Points de terminaison pour Cloud Volumes ONTAP dans AWS"
- "Points de terminaison pour Cloud Volumes ONTAP dans Azure"
- "Points de terminaison pour Cloud Volumes ONTAP dans Google Cloud"

"Reportez-vous à la documentation des services de données NetApp respectifs."

Inscrivez-vous ou connectez-vous à la console NetApp

La console NetApp est accessible à partir d'une console Web. Pour commencer à utiliser la console, votre première étape consiste à vous inscrire ou à vous connecter à l'aide de vos informations d'identification du site de support NetApp ou en créant une connexion à la console NetApp .

À propos de cette tâche

Lorsque vous accédez à la console pour la première fois, vous pouvez vous inscrire ou vous connecter en utilisant l'une des options suivantes :

Connexion à la console NetApp

Vous pouvez vous inscrire en créant un identifiant. Cette méthode d'authentification nécessite de spécifier votre adresse email et un mot de passe. Après avoir vérifié votre adresse e-mail, vous pouvez vous connecter puis créer une organisation, si vous n'en appartenez pas déjà une.

Informations d'identification du site de support NetApp (NSS)

Si vous disposez déjà d'informations d'identification du site de support NetApp , vous n'avez pas besoin de vous inscrire à la console. Vous vous connectez à l'aide de vos informations d'identification NSS, puis la console vous invite à créer une organisation, si vous n'en appartenez pas déjà à une.

Un code d'accès à usage unique (OTP) vous sera envoyé à l'adresse e-mail enregistrée. Un nouvel OTP est généré à chaque tentative de connexion.

Connexion fédérée

Si votre entreprise dispose déjà d'une instance de console NetApp , votre administrateur de console a peut-être configuré l'authentification unique pour se connecter à l'aide des informations d'identification de votre annuaire d'entreprise (identité fédérée).

"Découvrez comment utiliser la fédération d'identité avec la console NetApp" .

Étapes

1. Ouvrez un navigateur Web et accédez à la "Console NetApp"
2. Si vous disposez d'un compte sur le site de support NetApp ou si vous avez déjà configuré la fédération d'identité, saisissez l'adresse e-mail associée à votre compte directement sur la page **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**.

      Veuillez noter que 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.

      Cette étape est nécessaire avant de pouvoir vous connecter à la console.

4. Après vous être connecté, consultez le contrat de licence utilisateur final et acceptez les conditions.

   Si votre compte utilisateur n'appartient pas déjà à une organisation de la console, vous serez invité à en créer une.

5. Sur la page **Bienvenue**, saisissez un nom pour votre organisation Console.

   La console définit une organisation comme l'élément de niveau supérieur dans la gestion des identités et des accès (IAM) de la console. "En savoir plus sur IAM" .

   Si votre entreprise possède déjà une organisation et que vous souhaitez la rejoindre, fermez la console et demandez à l'administrateur de l'organisation de vous associer à l'organisation. Une fois ajouté, vous pouvez vous connecter et vous aurez accès à l'organisation de la console. "Apprenez à ajouter des membres à une organisation existante" .

6. Sélectionnez **Commençons**.

Créer 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 console NetApp .

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 console NetApp

Vous pouvez créer un agent de console dans AWS directement à partir de la console NetApp . 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"
\ https://mysupport.netapp.com	Pour obtenir des informations de licence et envoyer des messages AutoSupport au support NetApp .
\ https://support.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 console NetApp .
\ 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 console NetApp .

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 console NetApp 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'instance de 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'instance de 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'instance de 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'instance de l'agent de console qui permet à l'agent de console de gérer les ressources AWS. "Afficher les autorisations requises pour l'instance de l'agent de console elle-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 de confiance**, 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 d'instance pour l'instance. 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 pour l'instance.
   - Ajoutez des balises personnalisées (métadonnées) à l'instance.
   - 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'instance, 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 prépare l'instance 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 console NetApp"

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

Points de terminaison	But
\ https://support.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 console NetApp .
\ 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 console NetApp .
\ 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 ci-dessus. Nous recommandons 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 console NetApp 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 console NetApp 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 "Console NetApp" 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 console NetApp"

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

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 de console n'est pas pris en charge sur un hôte partagé avec d'autres applications. L'hôte doit être un hôte dédié. L'hôte peut être de n'importe quelle architecture répondant 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 de console nécessite cet espace dans `/var` car Docker ou Podman sont architecturés pour créer les conteneurs dans ce répertoire. Plus précisément, ils créeront des conteneurs dans le `/var/lib/containers/storage` annuaire. 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.

Configuration requise pour le système d'exploitation et les 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 a
Red Hat Enterprise Linux	9,1 à 9,4 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 Afficher les exigences de configuration de Podman .	Pris en charge en mode d'application ou en mode permissif • La gestion des systèmes Cloud Volumes ONTAP n'est PAS prise en charge par les agents sur lesquels SELinux est activé sur le système d'exploitation.
Ubuntu	24,04 LTS	3.9.45 ou version ultérieure avec la console NetApp en mode standard ou en mode restreint	Docker Engine 23.06 à 28.0.0.	Non pris en charge

Type d'instance AWS EC2

Un type d'instance qui répond aux exigences de CPU et de RAM ci-dessus. Nous recommandons t3.2xlarge.

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 sur l'instance EC2 (il s'agit du paramètre par défaut pour les nouvelles instances EC2), vous devez modifier la limite de saut de réponse PUT sur l'instance à 3. Si vous ne modifiez pas la limite sur l'instance EC2, vous recevrez une erreur d'initialisation de l'interface utilisateur lorsque vous tenterez de configurer l'agent.

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

Espace disque dans /opt

100 Go d'espace doivent être disponibles

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

Espace disque dans /var

20 Go d'espace doivent être disponibles

L'agent de console nécessite cet espace dans `/var` car Docker ou Podman sont architecturés pour créer les conteneurs dans ce répertoire. Plus précisément, ils créeront des conteneurs dans le `/var/lib/containers/storage` annuaire. Les montages externes ou les liens symboliques ne fonctionnent pas pour cet espace.

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 8, vérifiez que votre version Podman utilise 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 Red Hat Enterprise Linux.

   Pour Red Hat Enterprise Linux 9 :

```
sudo dnf install podman-2:<version>
```

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

   Pour Red Hat Enterprise Linux 8 :

```
sudo dnf install podman-3:<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.
6. Si vous utilisez Red Hat Enterprise :

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

   Pour Red Hat Enterprise Linux 9 :

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

   Pour Red Hat Enterprise Linux 8 :

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

7. 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.

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

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

      ```
      podman info | grep networkBackend
      ```

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

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

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

   d. 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` .

9. Redémarrez podman.

```
systemctl restart podman
```

10. 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.

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 console Web NetApp

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

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"

Étape 4 : configurer les autorisations AWS pour la console

Vous devez fournir des autorisations AWS à la console NetApp en utilisant l'une des options suivantes :

- 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 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. 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 console NetApp 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 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" .

À propos de cette tâche

Le programme d'installation disponible sur le site de support NetApp peut être une version antérieure. 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 de l'agent de la console à partir du "Site de support NetApp" , puis copiez-le sur l'hôte Linux.

   Vous devez télécharger le programme d'installation de l'agent « en ligne » destiné à être utilisé sur votre réseau ou dans le cloud.

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 des informations de proxy si votre réseau nécessite un proxy pour l'accès à Internet. Vous pouvez ajouter un proxy transparent ou explicite. Les paramètres --proxy et --cacert sont facultatifs et vous ne serez pas invité à les ajouter. Si vous disposez d'un serveur proxy, vous devrez saisir les paramètres comme indiqué.

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 console pour utiliser un serveur proxy HTTP ou HTTPS en utilisant l'un des formats suivants :

- http://adresse:port
- http://nom-d'utilisateur:mot-de-passe@adresse:port
- http://nom-de-domaine%92nom-d'utilisateur:mot-de-passe@adresse:port
- https://adresse:port
- https://nom-d'utilisateur:mot-de-passe@adresse:port
- https://nom-de-domaine%92nom-d'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 un \ comme indiqué ci-dessus.
  - L'agent de console ne prend pas en charge les noms d'utilisateur ou 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 préfixant d'une barre oblique inverse : & ou !

    Par exemple:

http://bxpproxyuser:netapp1\!@adresse:3128

`--cacert`spécifie un certificat signé par une autorité de certification à utiliser pour l'accès HTTPS entre l'agent de console et le serveur proxy. Ce paramètre est requis pour les serveurs proxy HTTPS, les serveurs proxy

d’interception et les serveurs proxy transparents.

+ Voici un exemple de configuration d’un serveur proxy transparent. Lorsque vous configurez un proxy transparent, vous n’avez pas besoin de définir le serveur proxy. Vous ajoutez uniquement un certificat signé par une autorité de certification à votre hôte d’agent de console :

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

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
      ...
      # 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
      ...
      Esc:wq
      ```

   c. 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 ne devez activer le mode restreint que si vous disposez d'un environnement sécurisé et que vous souhaitez déconnecter ce compte des services backend. Si c'est le cas,"suivez les étapes pour démarrer avec la console NetApp 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 console NetApp

Maintenant que vous avez installé l'agent de console, vous devez fournir à la console les autorisations AWS 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 AWS.

Rôle IAM

Attachez le rôle IAM que vous avez précédemment créé 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 "Console NetApp" 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 "Console NetApp" 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 console NetApp .

Les options d'installation suivantes sont disponibles :

- "Créer un agent de console directement à partir de la console NetApp"(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 console NetApp

Pour créer un agent de console dans Azure à partir de la console NetApp , 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://support.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 console NetApp .
\ 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 console NetApp .

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 console NetApp 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'instance de l'agent de la 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/agreem
ents/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreem
ents/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.

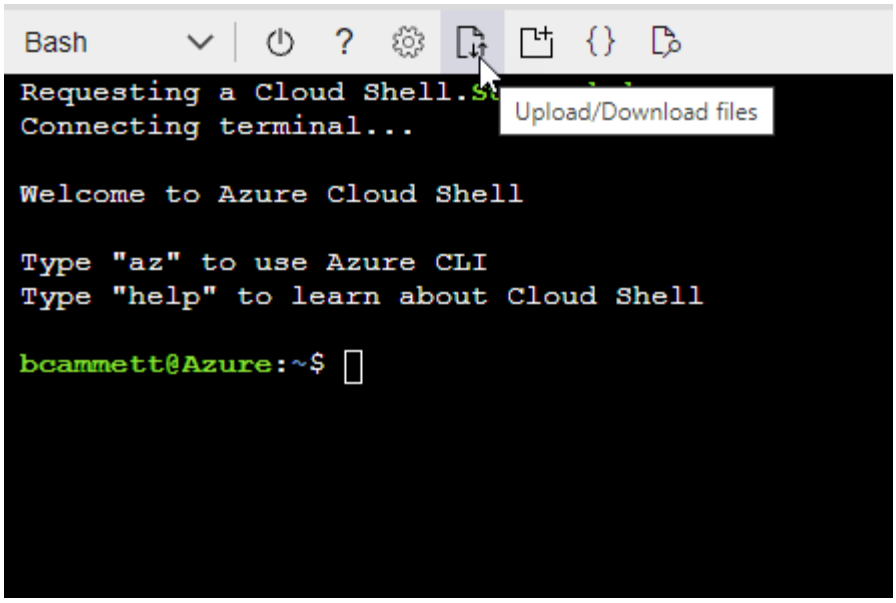
   Exemple

```
"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.

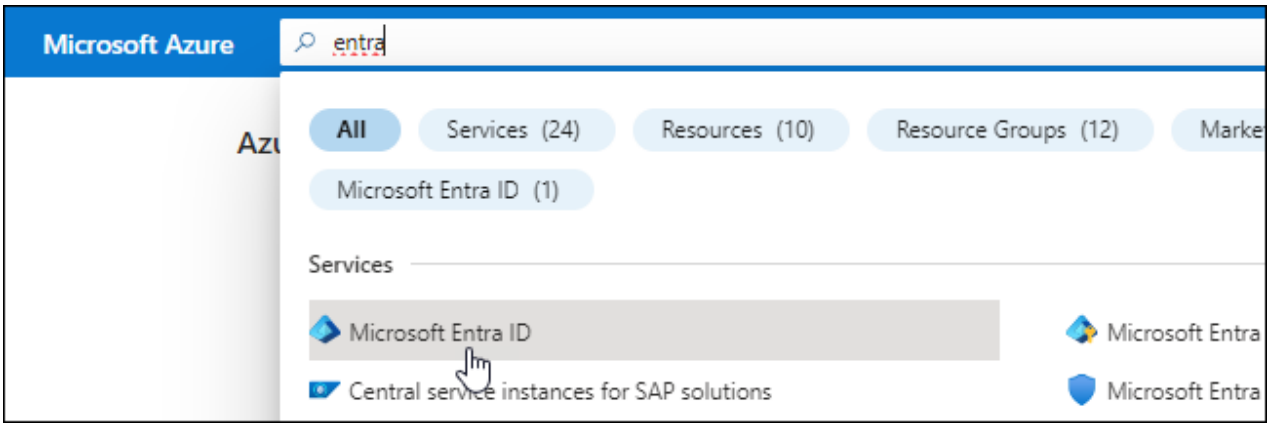
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont la console a besoin.

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**.



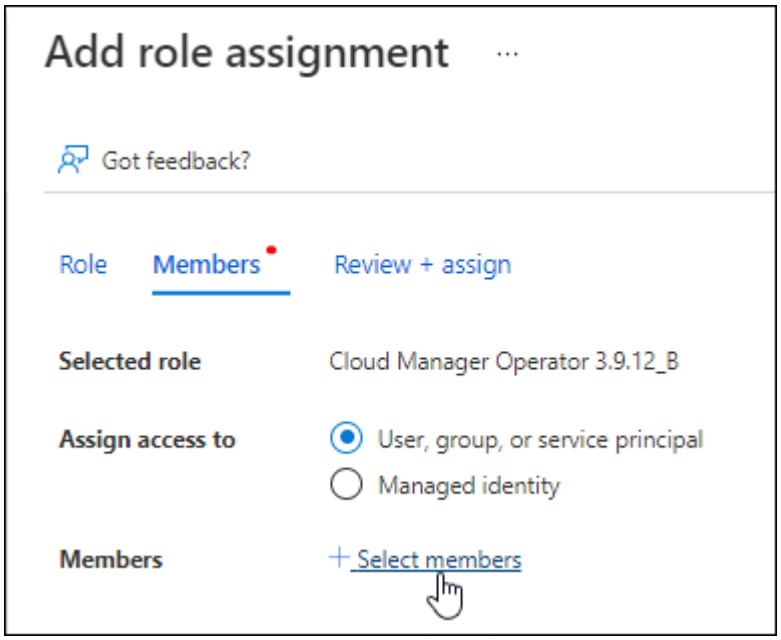
3. Dans le menu, sélectionnez **Inscriptions d'applications**.
4. Sélectionnez **Nouvelle inscription**.

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 console NetApp).
   - **URI de redirection**: Vous pouvez laisser ce champ vide.
6. Sélectionnez **S'inscrire**.

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

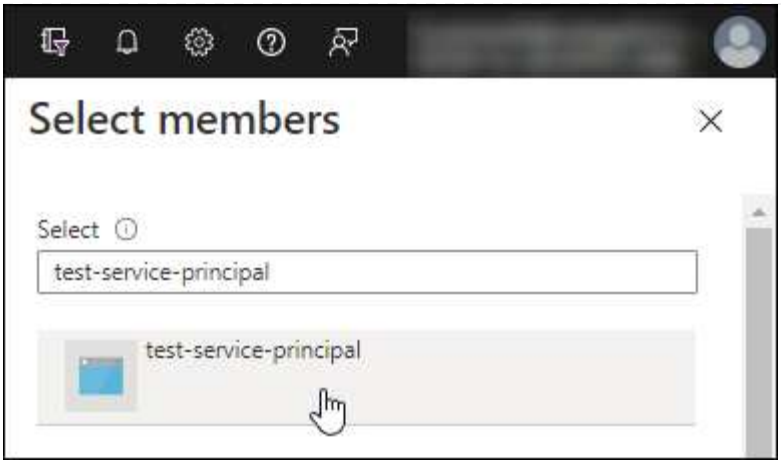
Attribuer le rôle personnalisé à l'application

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**.

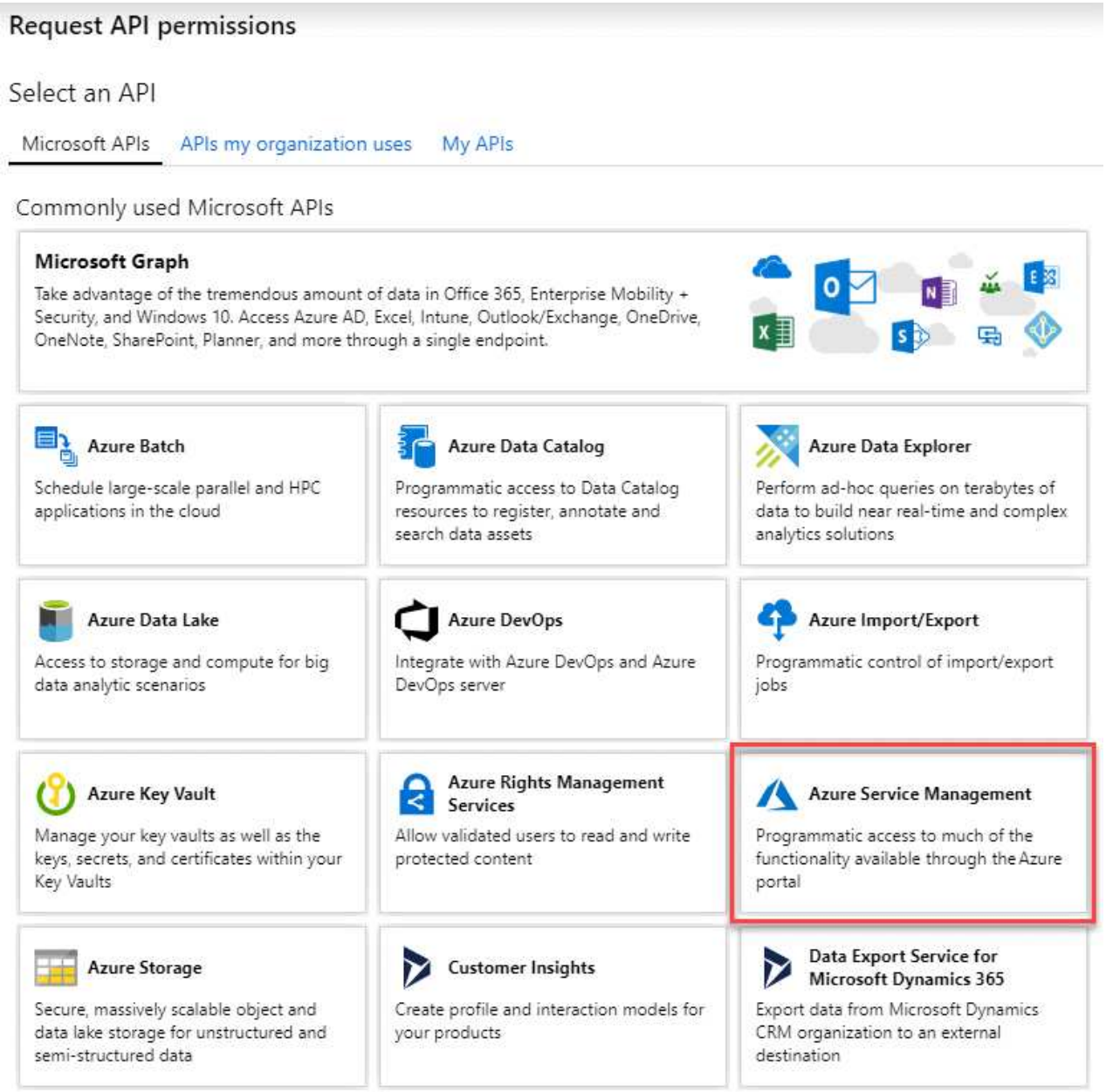
6. Cliquez sur **Réviser + attribuer**.

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

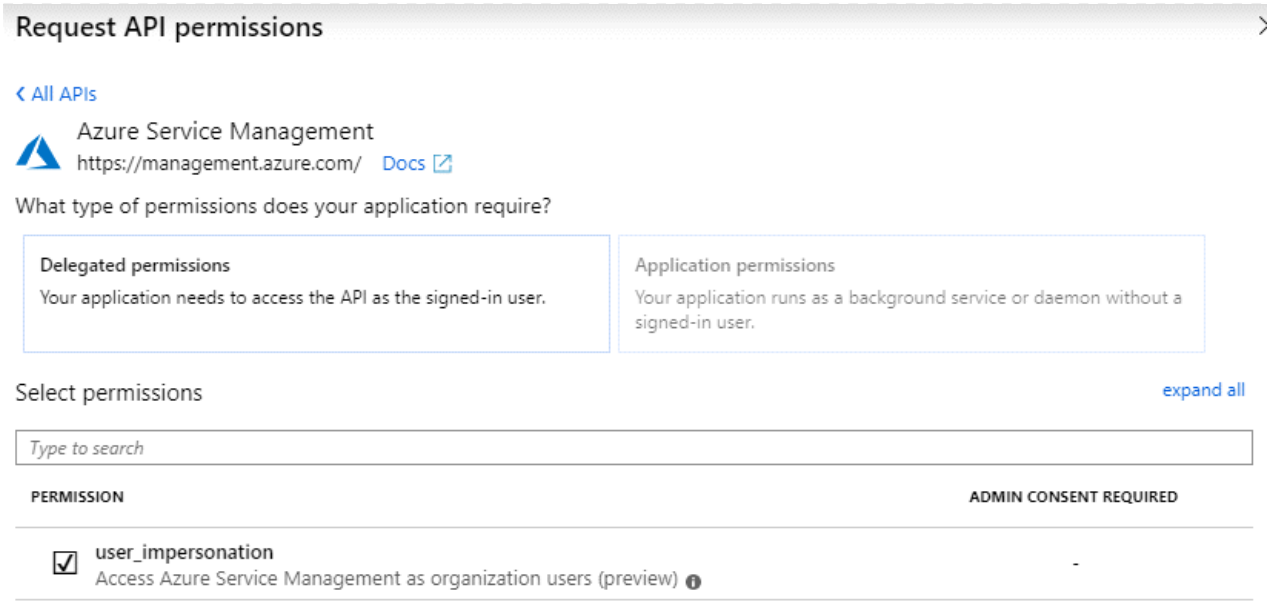
   Si vous souhaitez gérer des ressources dans plusieurs abonnements Azure, vous devez lier le principal de service à chacun de ces abonnements. Par exemple, la console vous permet de sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

Ajouter des autorisations à l'API de gestion des services Windows Azure

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**.

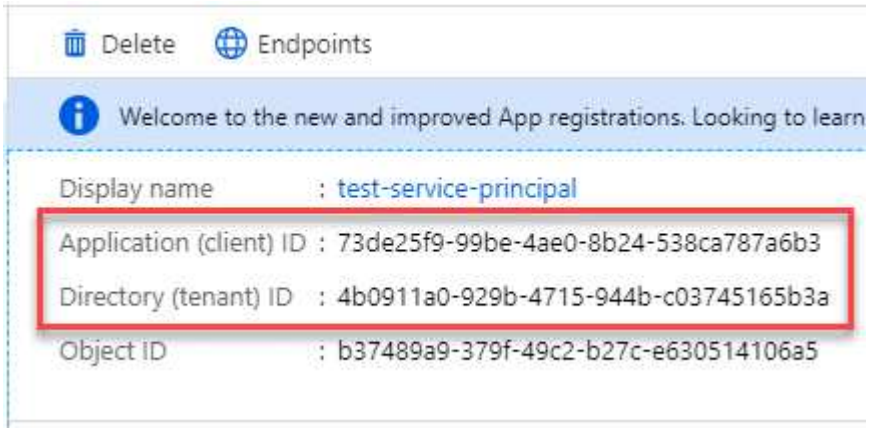


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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

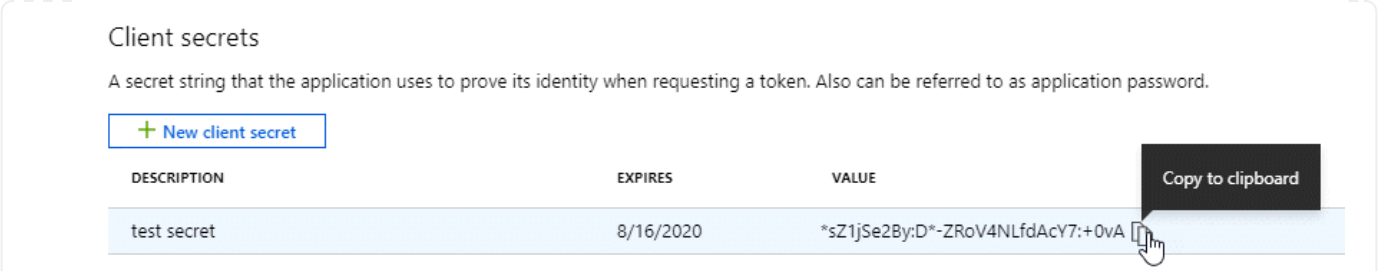
1. Dans le service **Microsoft Entra ID**, sélectionnez **Inscriptions d'applications** et sélectionnez l'application.
2. Copiez l'**ID d'application (client)** et l'**ID de répertoire (locataire)**.



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 console NetApp .

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'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. 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'instance, 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'instance 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 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 NetApp"

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://support.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 console NetApp .
\ 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 console NetApp .

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 ci-dessus. Nous recommandons 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 console NetApp .

   Exemple

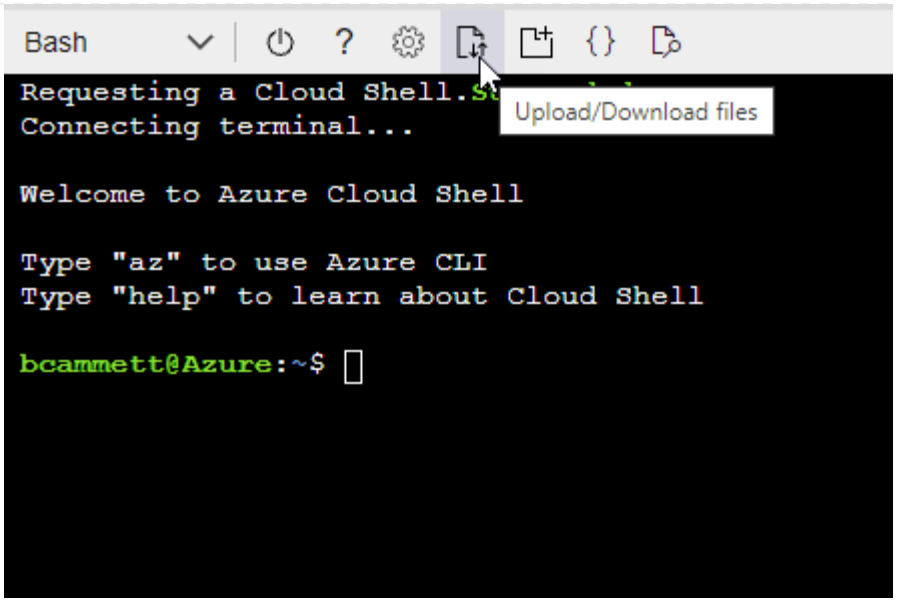
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

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 Connector_Policy.json
```

Principal de service

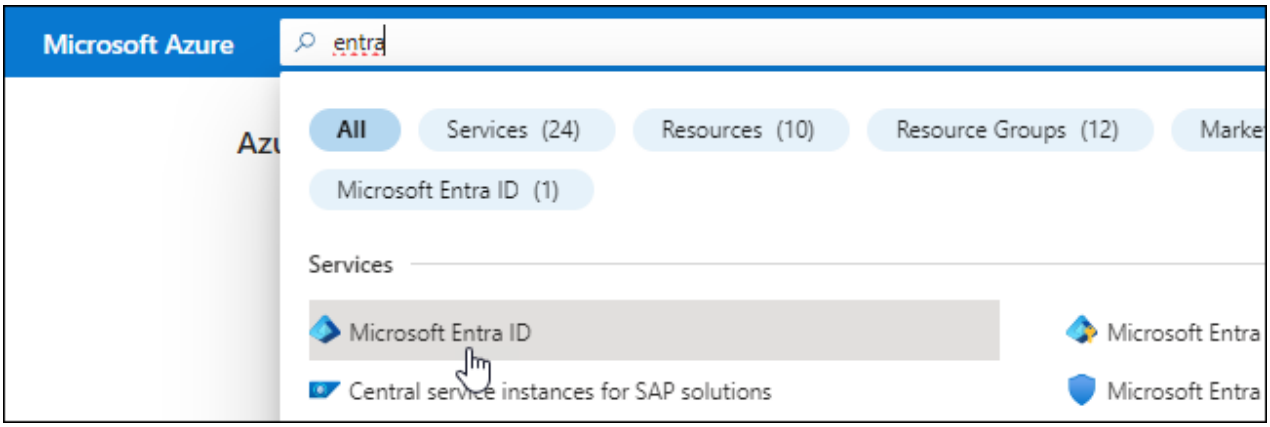
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont la console a besoin.

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 console NetApp).
- **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 .

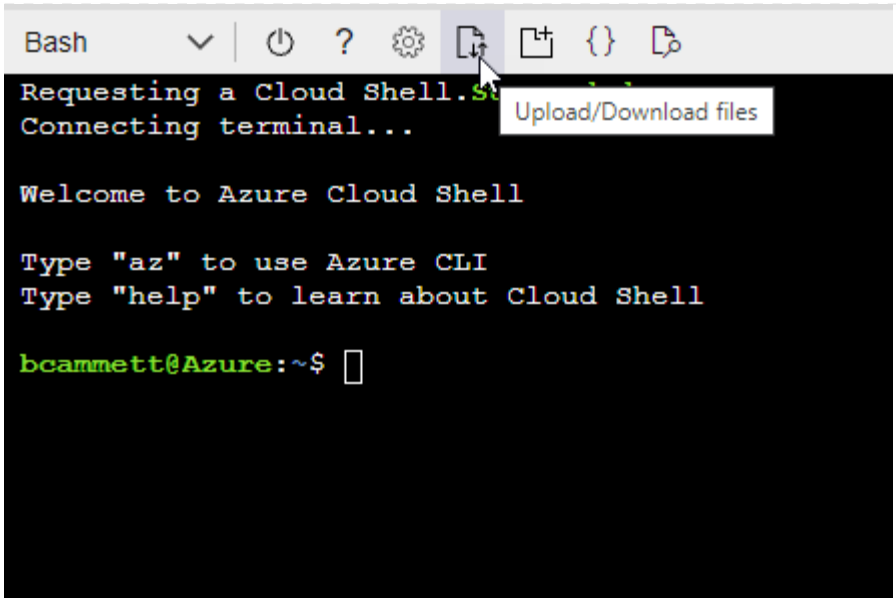
      Exemple

      ```
      "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 :

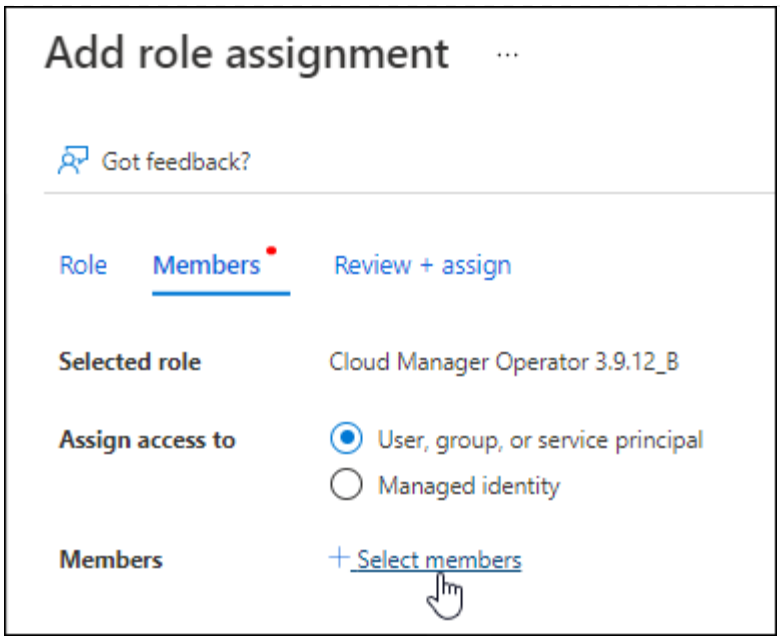
```
az role definition create --role-definition
Connector_Policy.json
```

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 :

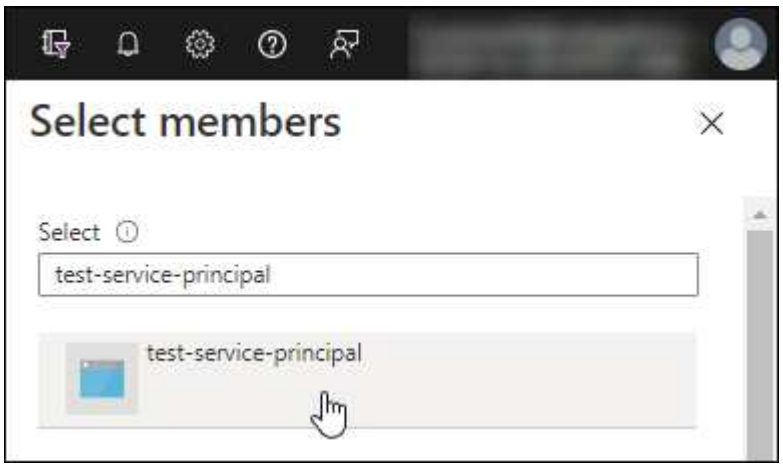
   a. Depuis le portail Azure, ouvrez le service **Abonnements**.
   b. Sélectionnez l'abonnement.
   c. Sélectionnez **Contrôle d'accès (IAM) > Ajouter > Ajouter une attribution de rôle**.
   d. Dans l'onglet **Rôle**, sélectionnez le rôle **Opérateur de console** et sélectionnez **Suivant**.
   e. Dans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

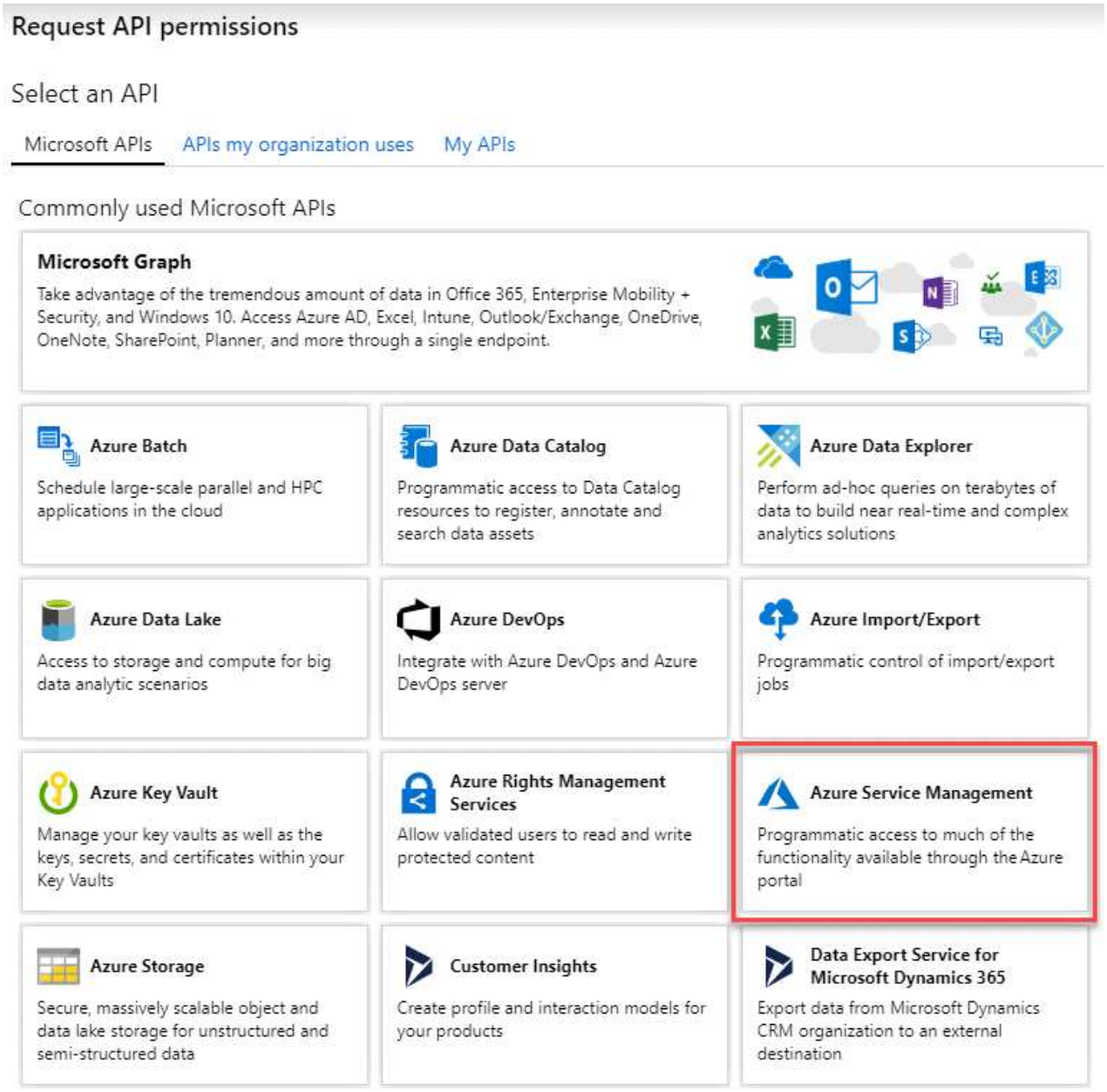
Le principal du service dispose désormais des autorisations Azure requises pour déployer l'agent de la console.

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 console NetApp , vous pouvez sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

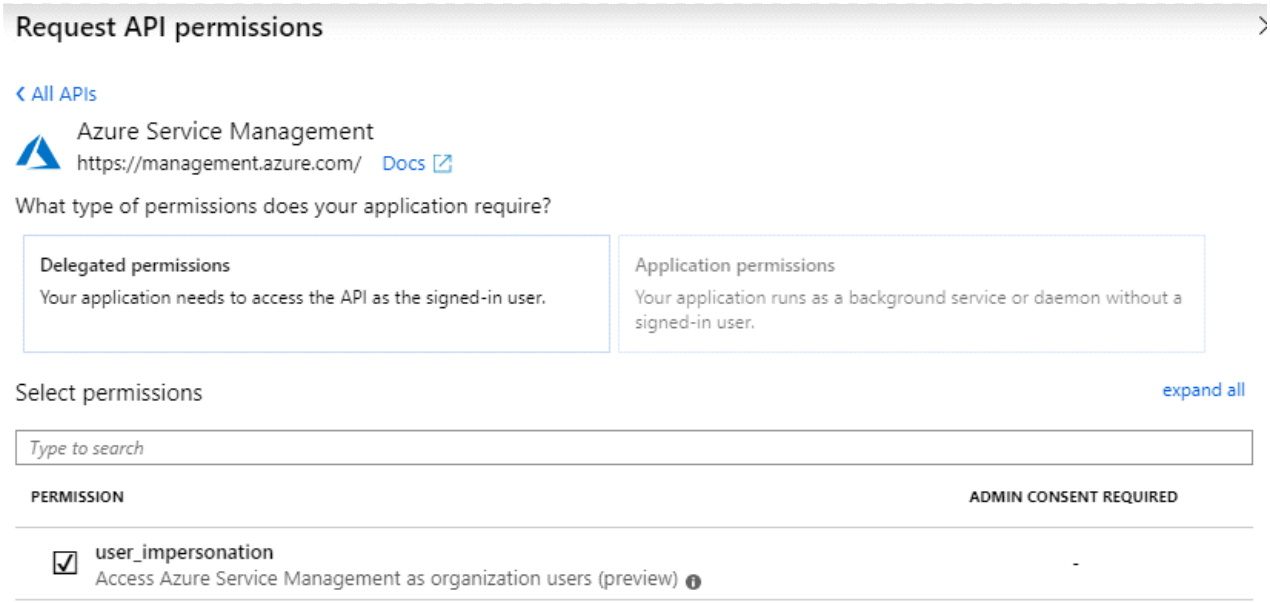
Ajouter des autorisations à l'API de gestion des services Windows Azure

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**.

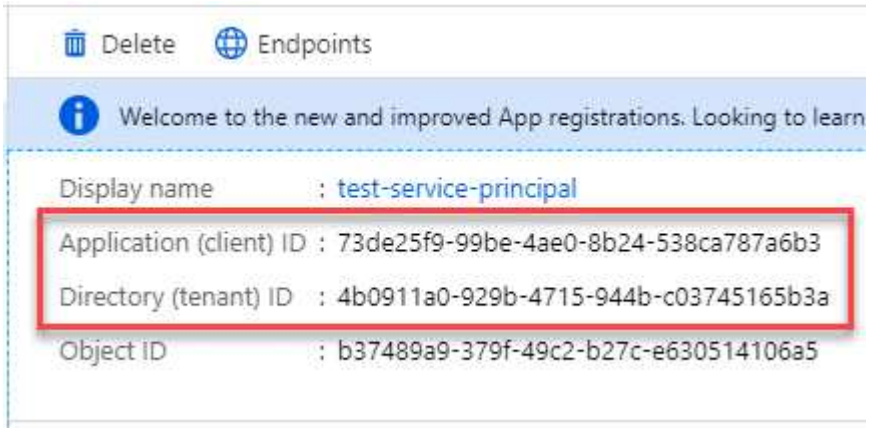


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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

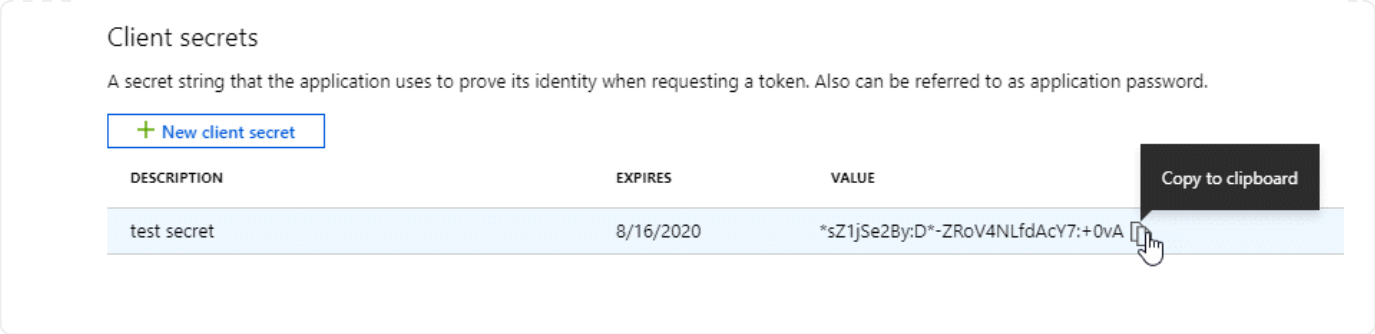
1. Dans le service **Microsoft Entra ID**, sélectionnez **Inscriptions d'applications** et sélectionnez l'application.
2. Copiez l'**ID d'application (client)** et l'**ID de répertoire (locataire)**.



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 console NetApp 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 console NetApp 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 "Console NetApp" 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 de console n'est pas pris en charge sur un hôte partagé avec d'autres applications. L'hôte doit être un hôte dédié. L'hôte peut être de n'importe quelle architecture répondant 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 de console nécessite cet espace dans `/var` car Docker ou Podman sont architecturés pour créer les conteneurs dans ce répertoire. Plus précisément, ils créeront des conteneurs dans le `/var/lib/containers/storage` annuaire. 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.

Configuration requise pour le système d'exploitation et les 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 a
Red Hat Enterprise Linux	9,1 à 9,4 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 Afficher les exigences de configuration de Podman .	Pris en charge en mode d'application ou en mode permissif • La gestion des systèmes Cloud Volumes ONTAP n'est PAS prise en charge par les agents sur lesquels SELinux est activé sur le système d'exploitation.
Ubuntu	24,04 LTS	3.9.45 ou version ultérieure avec la console NetApp en mode standard ou en mode restreint	Docker Engine 23.06 à 28.0.0.	Non pris en charge

Taille de la machine virtuelle Azure

Un type d'instance qui répond aux exigences de CPU et de RAM ci-dessus. Nous recommandons Standard_D8s_v3.

Espace disque dans /opt

100 Go d'espace doivent être disponibles

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

Espace disque dans /var

20 Go d'espace doivent être disponibles

L'agent de console nécessite cet espace dans `/var` car Docker ou Podman sont architecturés pour créer les conteneurs dans ce répertoire. Plus précisément, ils créeront des conteneurs dans le `/var/lib/containers/storage` annuaire. Les montages externes ou les liens symboliques ne fonctionnent pas pour cet espace.

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 8, vérifiez que votre version Podman utilise 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 Red Hat Enterprise Linux.

   Pour Red Hat Enterprise Linux 9 :

```
sudo dnf install podman-2:<version>
```

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

   Pour Red Hat Enterprise Linux 8 :

```
sudo dnf install podman-3:<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.
6. Si vous utilisez Red Hat Enterprise :

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

   Pour Red Hat Enterprise Linux 9 :

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

   Pour Red Hat Enterprise Linux 8 :

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

7. 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.

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

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

      ```
      podman info | grep networkBackend
      ```

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

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

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

   d. 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` .

9. Redémarrez podman.

```
systemctl restart podman
```

10. 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 console Web NetApp

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://support.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 console NetApp .
\ 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 console NetApp .

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"

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 console NetApp .

   Exemple

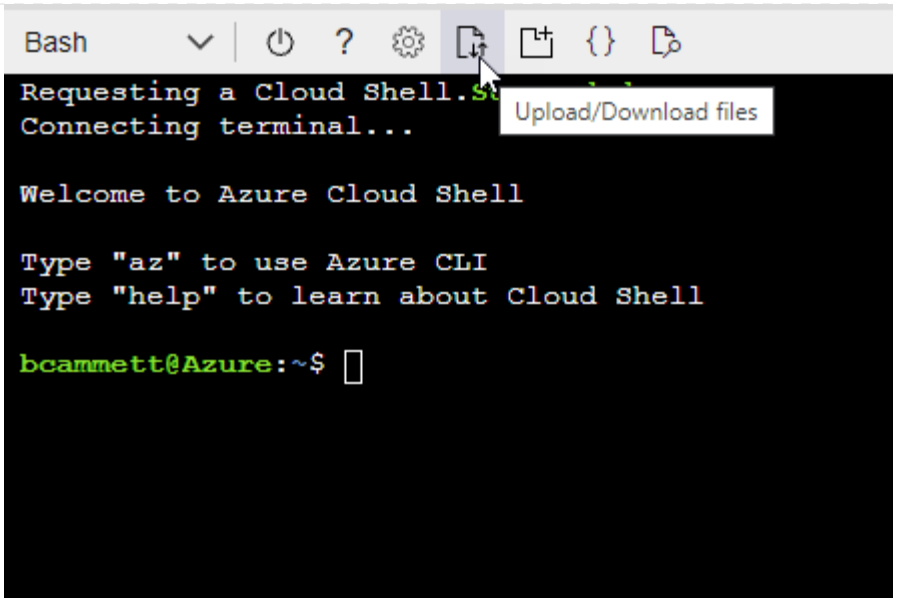
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ```

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 Connector_Policy.json
```

Principal de service

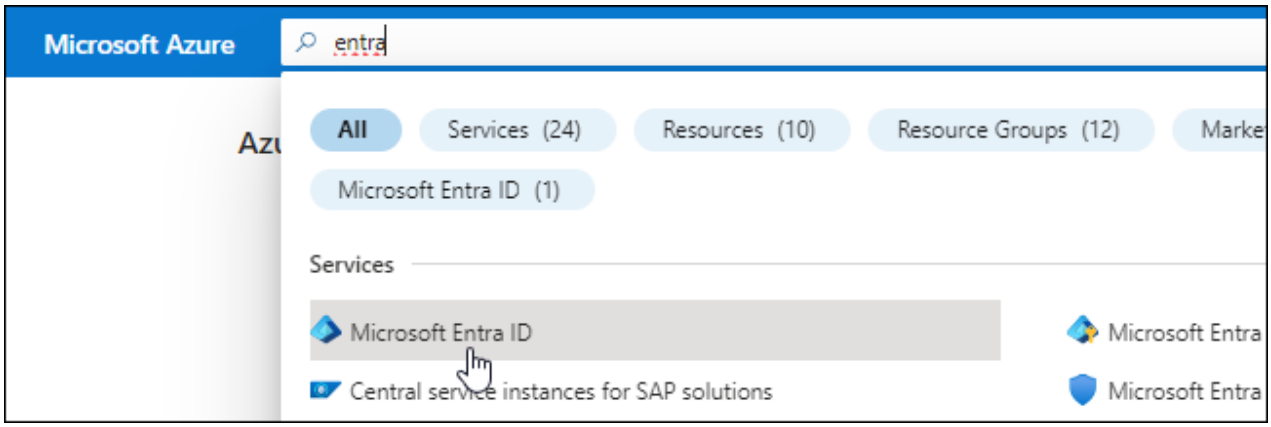
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont l'agent de la console a besoin.

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 console NetApp).
- **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 .

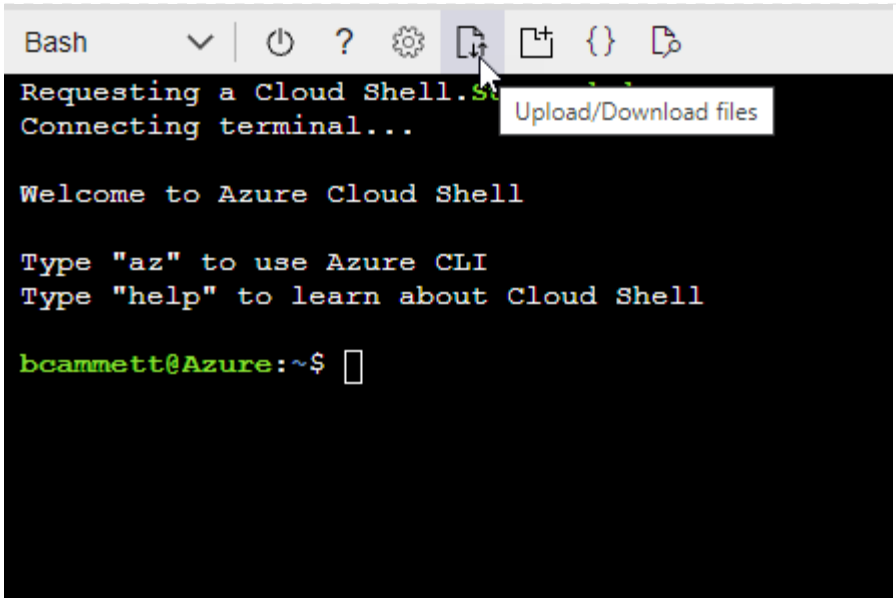
      Exemple

      ```
      "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 :

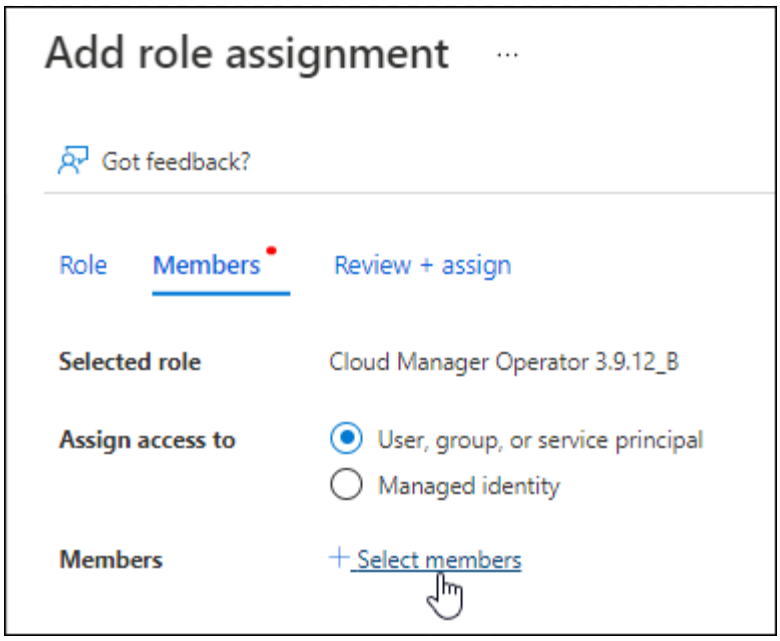
```
az role definition create --role-definition
Connector_Policy.json
```

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 :

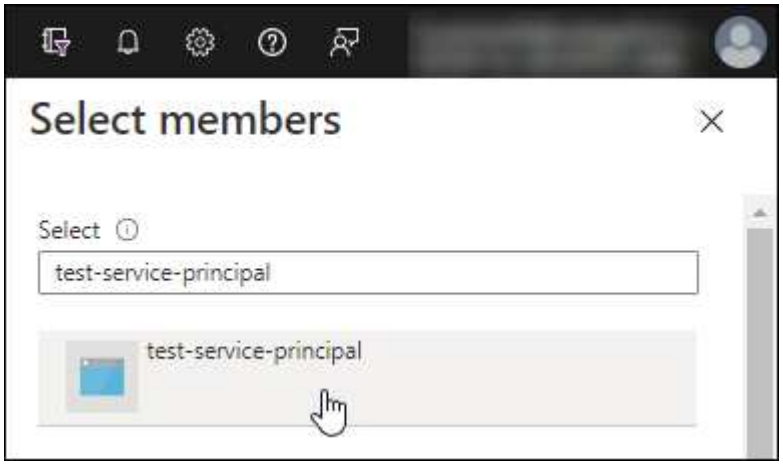
   a. Depuis le portail Azure, ouvrez le service **Abonnements**.
   b. Sélectionnez l'abonnement.
   c. Sélectionnez **Contrôle d'accès (IAM) > Ajouter > Ajouter une attribution de rôle**.
   d. Dans l'onglet **Rôle**, sélectionnez le rôle **Opérateur de console** et sélectionnez **Suivant**.
   e. Dans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

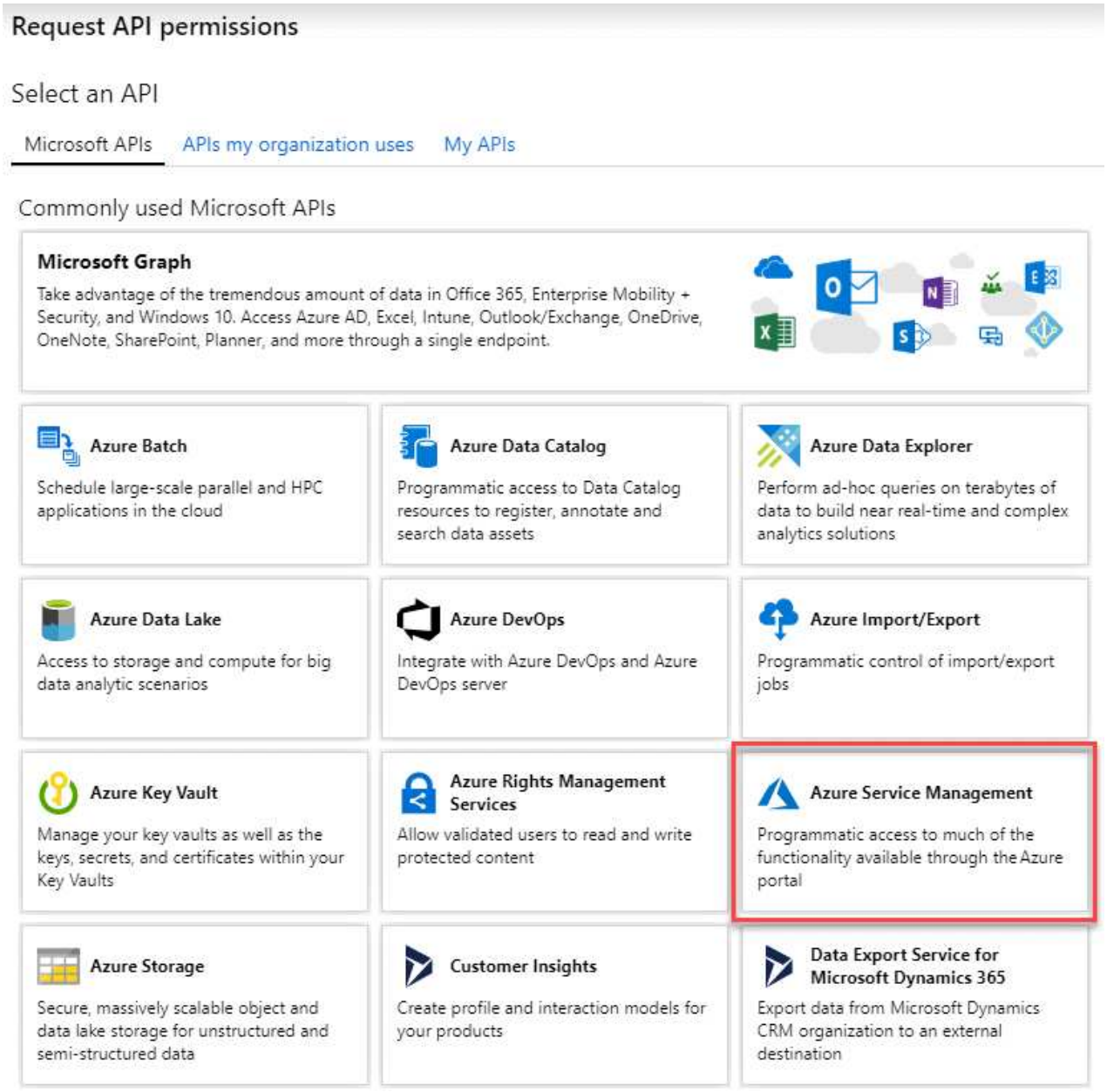
Le principal du service dispose désormais des autorisations Azure requises pour déployer l'agent de la console.

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 console NetApp , vous pouvez sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

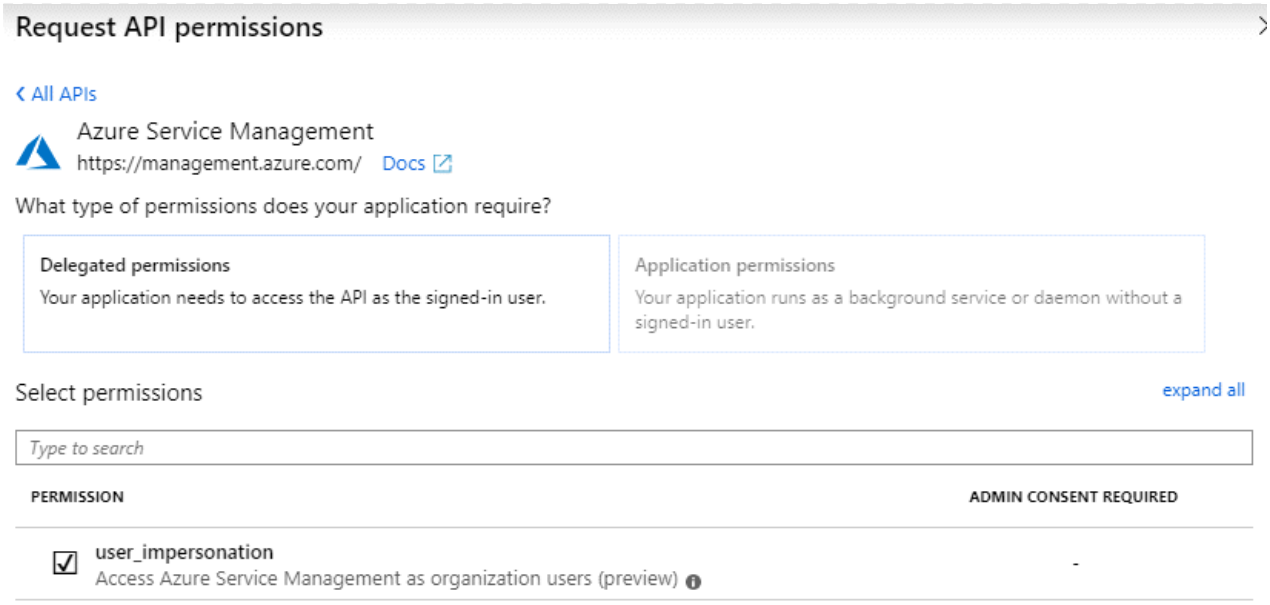
Ajouter des autorisations à l'API de gestion des services Windows Azure

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**.

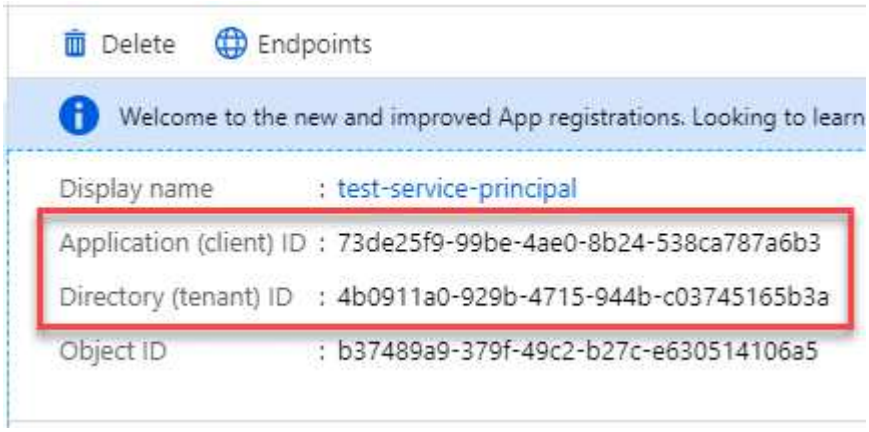


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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

Le programme d'installation disponible sur le site de support NetApp peut être une version antérieure. 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 de l'agent de la console à partir du "Site de support NetApp" , puis copiez-le sur l'hôte Linux.

   Vous devez télécharger le programme d'installation de l'agent « en ligne » destiné à être utilisé sur votre réseau ou dans le cloud.

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 des informations de proxy si votre réseau nécessite un proxy pour l'accès à Internet. Vous pouvez ajouter un proxy transparent ou explicite. Les paramètres --proxy et --cacert sont facultatifs et vous ne serez pas invité à les ajouter. Si vous disposez d'un serveur proxy, vous devrez saisir les paramètres comme indiqué.

   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 console pour utiliser un serveur proxy HTTP ou HTTPS en utilisant l'un des formats suivants :

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

- https://nom-d'utilisateur:mot-de-passe@adresse:port
- https://nom-de-domaine%92nom-d'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 un \ comme indiqué ci-dessus.
  - L'agent de console ne prend pas en charge les noms d'utilisateur ou 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 préfixant d'une barre oblique inverse : & ou !

    Par exemple:

http://bxpproxyuser:netapp1\!@adresse:3128

`--cacert`spécifie un certificat signé par une autorité de certification à utiliser pour l'accès HTTPS entre l'agent de console et le serveur proxy. Ce paramètre est requis pour les serveurs proxy HTTPS, les serveurs proxy d'interception et les serveurs proxy transparents.

+ Voici un exemple de configuration d'un serveur proxy transparent. Lorsque vous configurez un proxy transparent, vous n'avez pas besoin de définir le serveur proxy. Vous ajoutez uniquement un certificat signé par une autorité de certification à votre hôte d'agent de console :

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

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
      ...
      # 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
      ...
      Esc:wq
      ```

c. 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 ne devez activer le mode restreint que si vous disposez d'un environnement sécurisé et que vous souhaitez déconnecter ce compte des services backend. Si c'est le cas,"suivez les étapes pour démarrer avec la console NetApp 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 console NetApp"

Étape 6 : Accorder des autorisations à la console NetApp

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 console NetApp 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 "Console NetApp" 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 console NetApp . ---

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 console NetApp

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://www.googleapis.com/deploymentmanager/v2/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://support.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 console NetApp .
\ 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 console NetApp .

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 console NetApp 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:
- 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
- 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.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 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 : 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 « connecteur » au niveau du projet :

      ```
      gcloud iam roles create connector --project=myproject --file=connector.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 de l'agent"	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 console NetApp 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 console NetApp 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 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)

      (Requis uniquement si vous prévoyez d'utiliser NetApp Backup and Recovery avec des clés de chiffrement gérées par le client (CMEK))

"Documentation Google Cloud : Activation des API"

Étape 6 : Créer l'agent de console

Créez un agent de console directement depuis la console.

À propos de cette tâche

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" .

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

Résultat

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

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

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

Créer un agent de console à partir de Google Cloud

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

Cloud, puis créer l'agent de console.

Avant de commencer

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

Étape 1 : Configurer le réseau

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

VPC et sous-réseau

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

Connexions aux réseaux cibles

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

Accès Internet sortant

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

Points de terminaison contactés depuis l'agent de la console

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

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

Points de terminaison	But
\ https://www.googleapis.com/compute/v1/ \ https://compute.googleapis.com/compute/v1 \ https://cloudresourcemanager.googleapis.com/v1/projects \ https://www.googleapis.com/compute/beta \ https://storage.googleapis.com/storage/v1 \ https://www.googleapis.com/storage/v1 \ https://iam.googleapis.com/v1 \ https://cloudkms.googleapis.com/v1 \ https://www.googleapis.com/deploymentmanager/v2/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://support.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 console NetApp .
\ 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 console NetApp .
\ 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 console NetApp 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 NetApp Console
agent
stage: GA
includedPermissions:
- 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
- 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.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 « connecteur » au niveau du projet :

```
gcloud iam roles create connector --project=myproject --file=connector.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 de l'agent"	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 console NetApp 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 console NetApp 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 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)

      (Requis uniquement si vous prévoyez d'utiliser NetApp Backup and Recovery avec des clés de chiffrement gérées par le client (CMEK))

"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 "Console NetApp" 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 de console n'est pas pris en charge sur un hôte partagé avec d'autres applications. L'hôte doit être un hôte dédié. L'hôte peut être de n'importe quelle architecture répondant 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 de console nécessite cet espace dans `/var` car Docker ou Podman sont architecturés pour créer les conteneurs dans ce répertoire. Plus précisément, ils créeront des conteneurs dans le `/var/lib/containers/storage` annuaire. 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.

Configuration requise pour le système d'exploitation et les 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 a
Red Hat Enterprise Linux	9,1 à 9,4 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 Afficher les exigences de configuration de Podman .	Pris en charge en mode d'application ou en mode permissif • La gestion des systèmes Cloud Volumes ONTAP n'est PAS prise en charge par les agents sur lesquels SELinux est activé sur le système d'exploitation.
Ubuntu	24,04 LTS	3.9.45 ou version ultérieure avec la console NetApp en mode standard ou en mode restreint	Docker Engine 23.06 à 28.0.0.	Non pris en charge

Type de machine Google Cloud

Un type d'instance qui répond aux exigences de CPU et de RAM ci-dessus. 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 "Fonctionnalités de la machine virtuelle blindée"

Espace disque dans /opt

100 Go d'espace doivent être disponibles

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

Espace disque dans /var

20 Go d'espace doivent être disponibles

L'agent de console nécessite cet espace dans `/var` car Docker ou Podman sont architecturés pour créer les conteneurs dans ce répertoire. Plus précisément, ils créeront des conteneurs dans le

`/var/lib/containers/storage` annuaire. Les montages externes ou les liens symboliques ne fonctionnent pas pour cet espace.

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 8, vérifiez que votre version Podman utilise 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 Red Hat Enterprise Linux.

   Pour Red Hat Enterprise Linux 9 :

```
sudo dnf install podman-2:<version>
```

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

   Pour Red Hat Enterprise Linux 8 :

```
sudo dnf install podman-3:<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.
6. Si vous utilisez Red Hat Enterprise :

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

   Pour Red Hat Enterprise Linux 9 :

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

   Pour Red Hat Enterprise Linux 8 :

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

7. 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.

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

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

      ```
      podman info | grep networkBackend
      ```

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

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

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

   d. 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` .

9. Redémarrez podman.

```
systemctl restart podman
```

10. 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 console Web NetApp

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://www.googleapis.com/deploymentmanager/v2/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://support.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 console NetApp .
\ 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 console NetApp .

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"

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 « connecteur » au niveau du projet :

      ```
      gcloud iam roles create connector --project=myproject --file=connector.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 de l'agent"	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 console NetApp 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 console NetApp 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 des systèmes Cloud Volumes ONTAP dans Google Cloud.

Étape

1. Activez les API Google Cloud suivantes dans votre projet :
    - API du gestionnaire de déploiement cloud V2
    - API 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)

      (Requis uniquement si vous prévoyez d'utiliser NetApp Backup and Recovery avec des clés de chiffrement gérées par le client (CMEK))

"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.

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

Le programme d'installation disponible sur le site de support NetApp peut être une version antérieure. 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 de l'agent de la console à partir du "Site de support NetApp" , puis copiez-le sur l'hôte Linux.

   Vous devez télécharger le programme d'installation de l'agent « en ligne » destiné à être utilisé sur votre réseau ou dans le cloud.

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 des informations de proxy si votre réseau nécessite un proxy pour l'accès à Internet. Vous pouvez ajouter un proxy transparent ou explicite. Les paramètres --proxy et --cacert sont facultatifs et vous ne serez pas invité à les ajouter. Si vous disposez d'un serveur proxy, vous devrez saisir les paramètres comme indiqué.

   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 console pour utiliser un serveur proxy HTTP ou HTTPS en utilisant l'un des formats suivants :

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

- https://nom-d'utilisateur:mot-de-passe@adresse:port
- https://nom-de-domaine%92nom-d'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 un \ comme indiqué ci-dessus.
  - L'agent de console ne prend pas en charge les noms d'utilisateur ou 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 préfixant d'une barre oblique inverse : & ou !

    Par exemple:

http://bxpproxyuser:netapp1\!@adresse:3128

`--cacert`spécifie un certificat signé par une autorité de certification à utiliser pour l'accès HTTPS entre l'agent de console et le serveur proxy. Ce paramètre est requis pour les serveurs proxy HTTPS, les serveurs proxy d'interception et les serveurs proxy transparents.

+ Voici un exemple de configuration d'un serveur proxy transparent. Lorsque vous configurez un proxy transparent, vous n'avez pas besoin de définir le serveur proxy. Vous ajoutez uniquement un certificat signé par une autorité de certification à votre hôte d'agent de console :

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

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
      ...
      # 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
      ...
      Esc:wq
      ```

c. 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 ne devez activer le mode restreint que si vous disposez d'un environnement sécurisé et que vous souhaitez déconnecter ce compte des services backend. Si c'est le cas,"suivez les étapes pour démarrer avec la console NetApp 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 console NetApp"

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 de console n'est pas pris en charge sur un hôte partagé avec d'autres applications. L'hôte doit être un hôte dédié. L'hôte peut être de n'importe quelle architecture répondant 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 de console nécessite cet espace dans `/var` car Docker ou Podman sont architecturés pour créer les conteneurs dans ce répertoire. Plus précisément, ils créeront des conteneurs dans le `/var/lib/containers/storage` annuaire. 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.

Configuration requise pour le système d'exploitation et les 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 a
Red Hat Enterprise Linux	9,1 à 9,4 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 Afficher les exigences de configuration de Podman .	Pris en charge en mode d'application ou en mode permissif • La gestion des systèmes Cloud Volumes ONTAP n'est PAS prise en charge par les agents sur lesquels SELinux est activé sur le système d'exploitation.
Ubuntu	24,04 LTS	3.9.45 ou version ultérieure avec la console NetApp en mode standard ou en mode restreint	Docker Engine 23.06 à 28.0.0.	Non pris en charge

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 console Web NetApp

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

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.

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.
\ 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 .

Points de terminaison	But
\ https://support.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 console NetApp .
\ 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 console NetApp .
\ 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 console NetApp 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

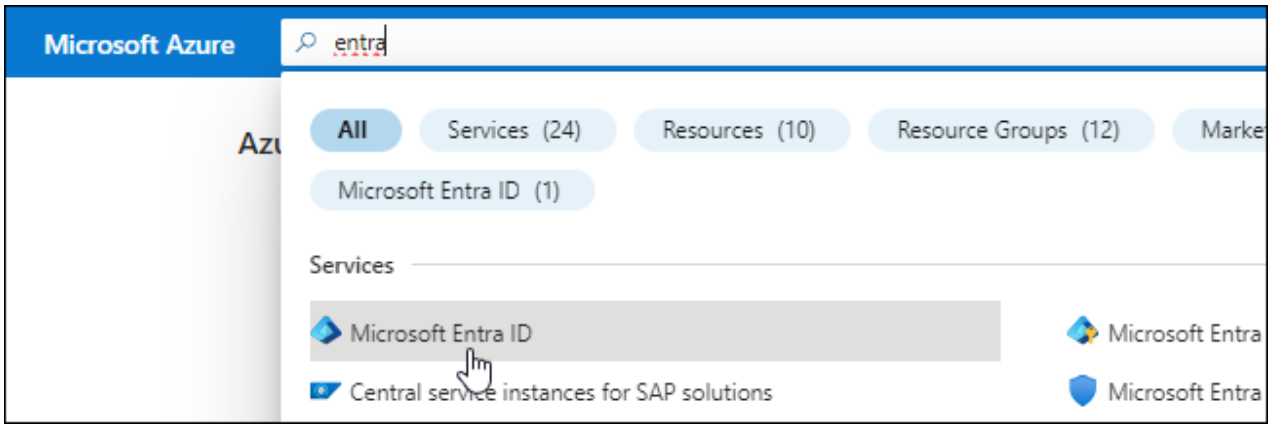
Lorsque l'agent de console est installé sur site, vous devez fournir à l'agent de console des autorisations Azure en configurant un principal de service dans Microsoft Entra ID et en obtenant les informations d'identification Azure dont l'agent de console a besoin.

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 console NetApp).
   - **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 .

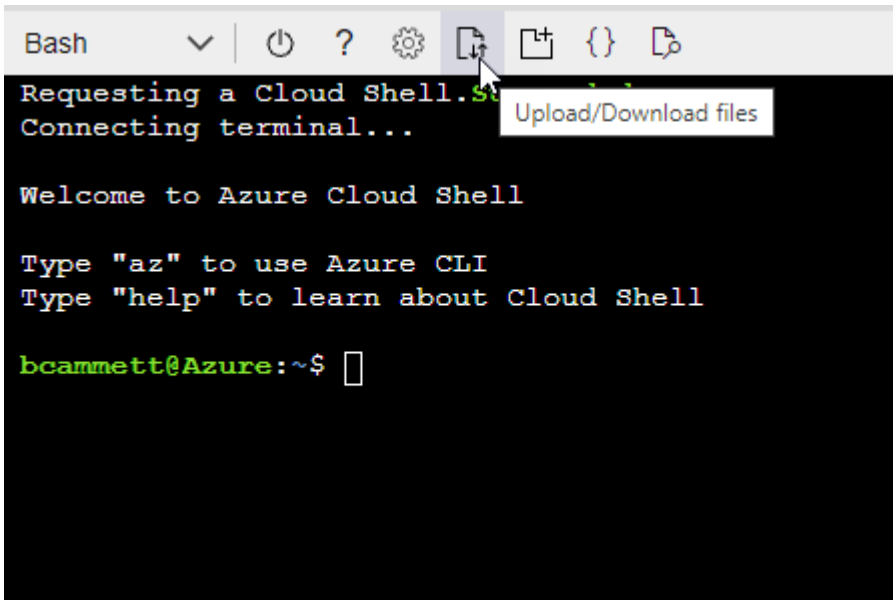
      Exemple

```
"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 :

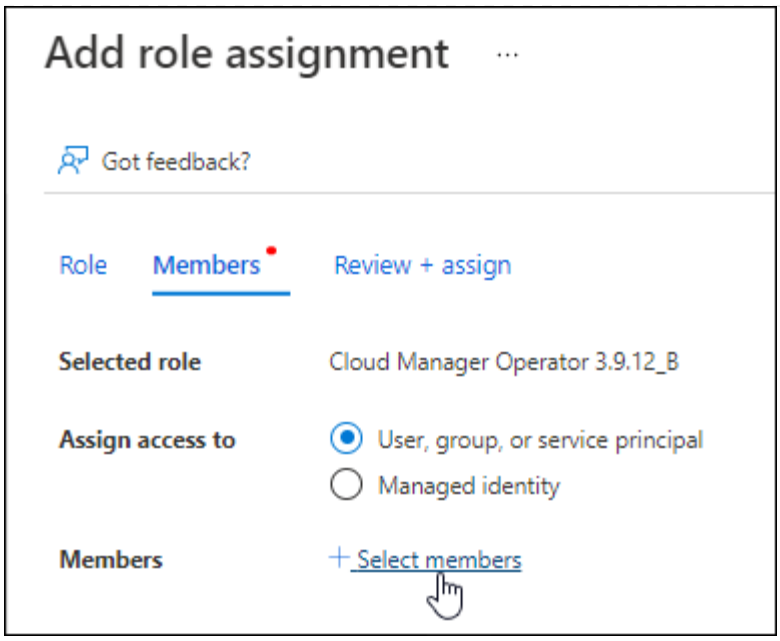
```
az role definition create --role-definition
Connector_Policy.json
```

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 :

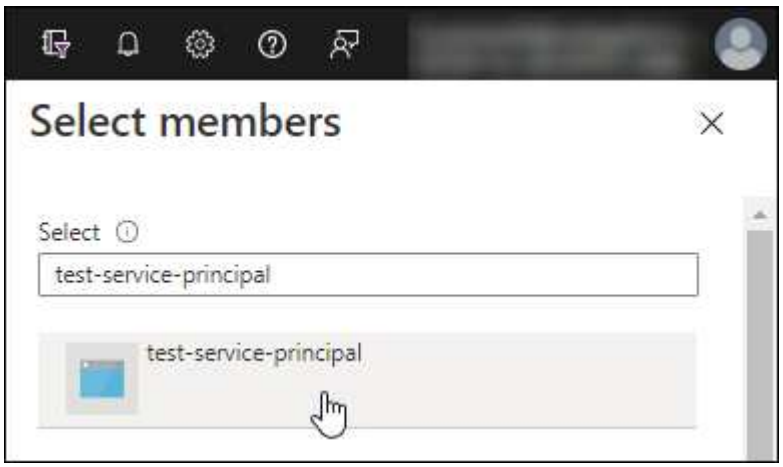
   a. Depuis le portail Azure, ouvrez le service **Abonnements**.
   b. Sélectionnez l'abonnement.
   c. Sélectionnez **Contrôle d'accès (IAM) > Ajouter > Ajouter une attribution de rôle**.
   d. Dans l'onglet **Rôle**, sélectionnez le rôle **Opérateur de console** et sélectionnez **Suivant**.
   e. Dans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

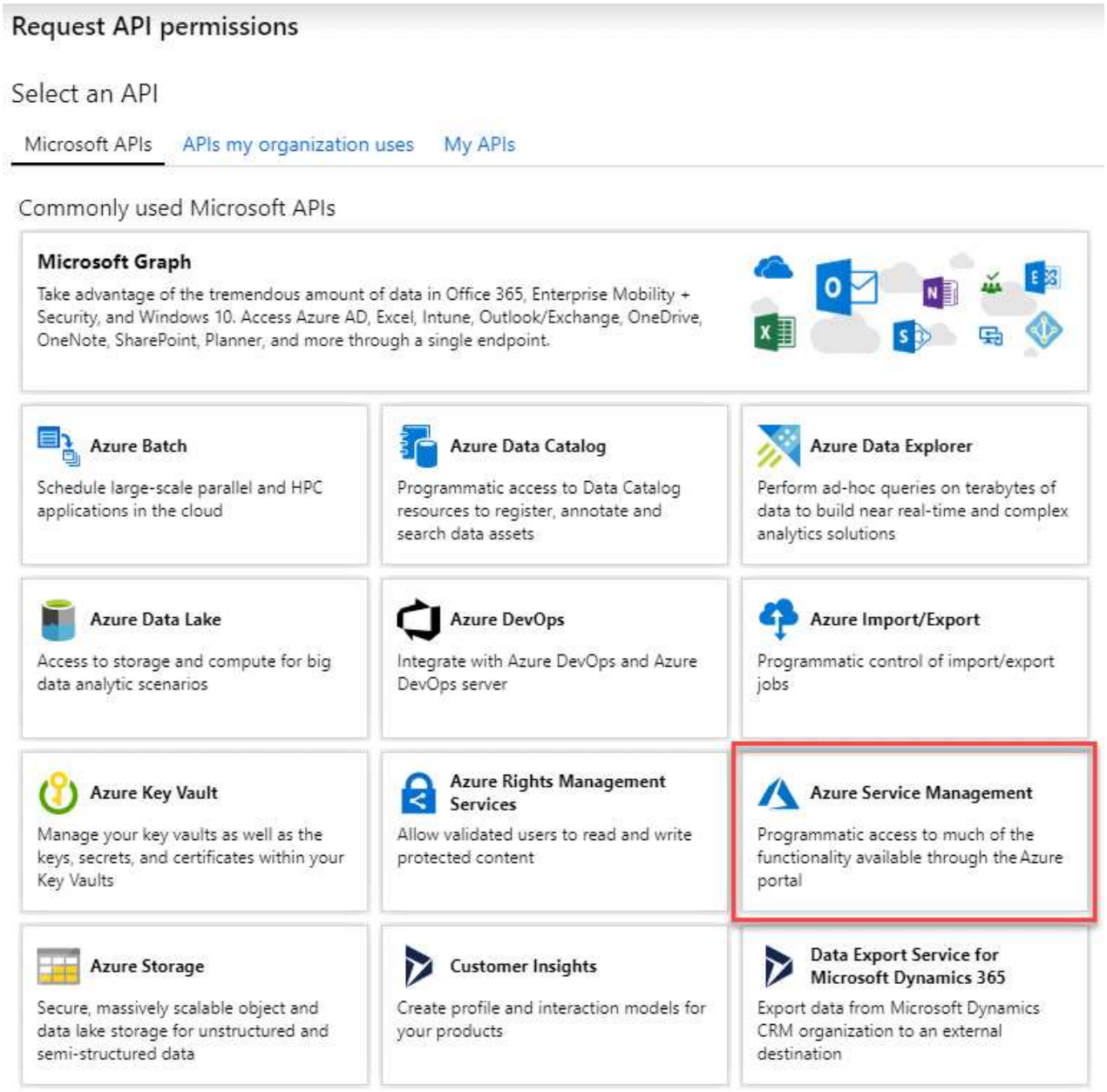
Le principal du service dispose désormais des autorisations Azure requises pour déployer l'agent de la console.

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 console NetApp , vous pouvez sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

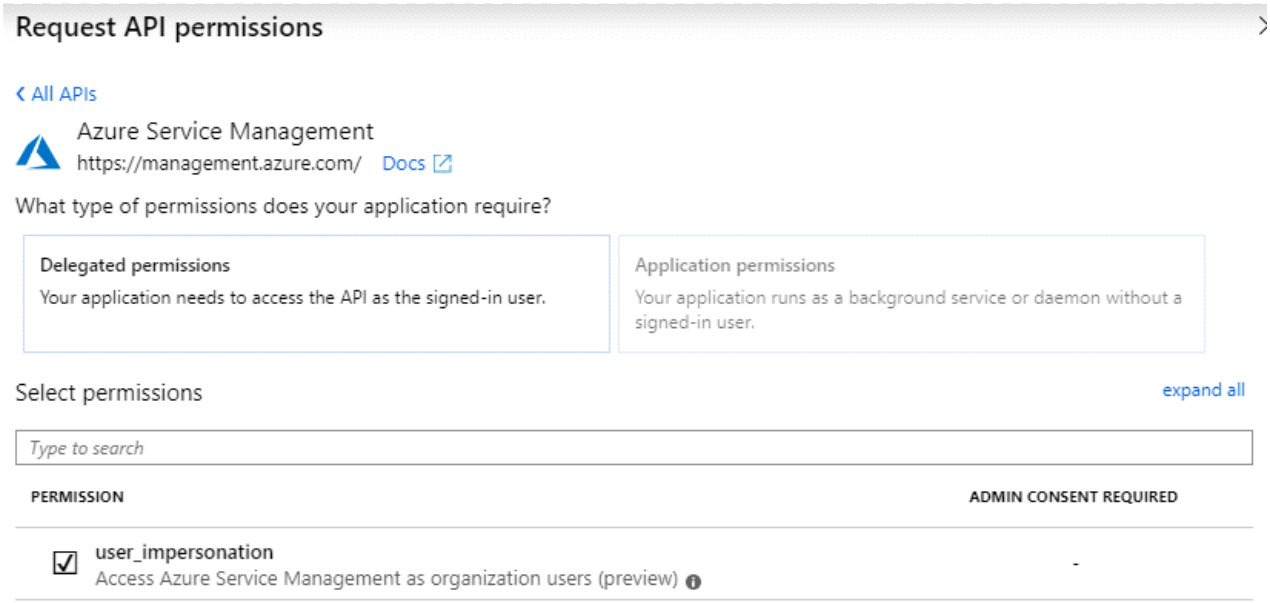
Ajouter des autorisations à l'API de gestion des services Windows Azure

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**.

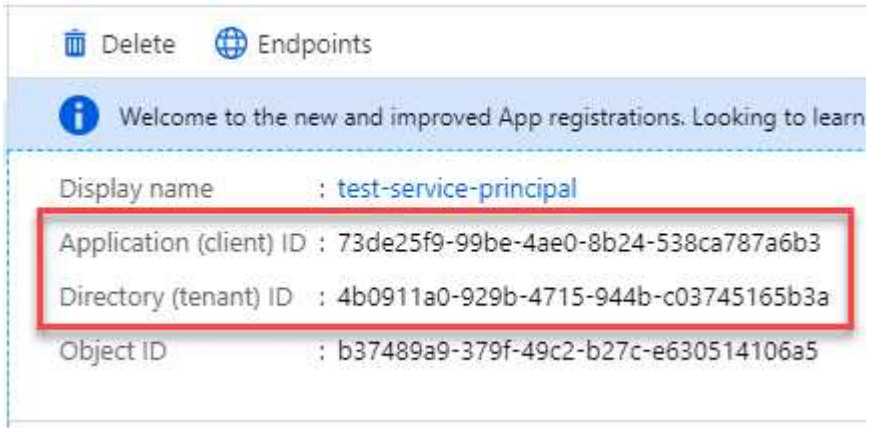


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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

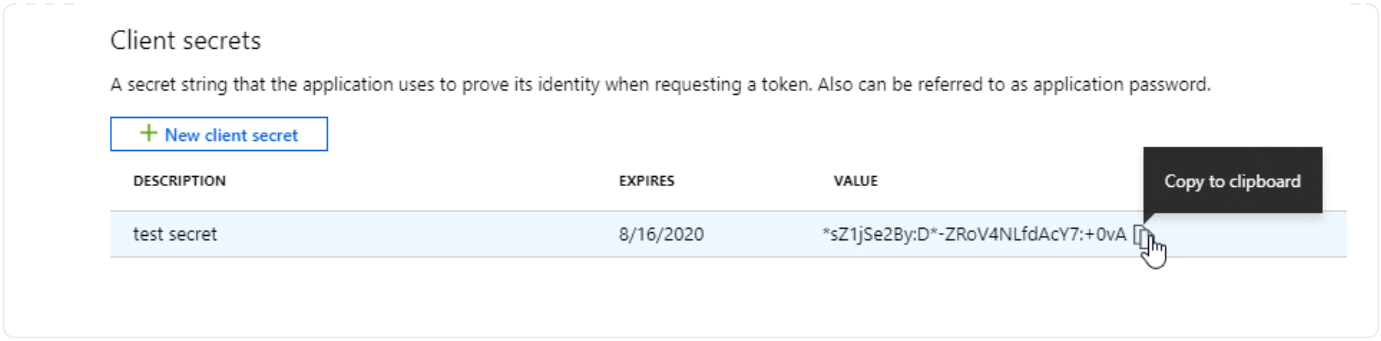
1. Dans le service **Microsoft Entra ID**, sélectionnez **Inscriptions d'applications** et sélectionnez l'application.
2. Copiez l'**ID d'application (client)** et l'**ID de répertoire (locataire)**.



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 8, vérifiez que votre version Podman utilise 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 Red Hat Enterprise Linux.

   Pour Red Hat Enterprise Linux 9 :

```
sudo dnf install podman-2:<version>
```

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

   Pour Red Hat Enterprise Linux 8 :

```
sudo dnf install podman-3:<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.
6. Si vous utilisez Red Hat Enterprise :

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

   Pour Red Hat Enterprise Linux 9 :

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

   Pour Red Hat Enterprise Linux 8 :

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

7. 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.

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

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

      ```
      podman info | grep networkBackend
      ```

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

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

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

   d. 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` .

9. Redémarrez podman.

```
systemctl restart podman
```

10. 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

Le programme d'installation disponible sur le site de support NetApp peut être une version antérieure. 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 de l'agent de la console à partir du "Site de support NetApp" , puis copiez-le sur l'hôte Linux.

   Vous devez télécharger le programme d'installation de l'agent « en ligne » destiné à être utilisé sur votre réseau ou dans le cloud.

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 des informations de proxy si votre réseau nécessite un proxy pour l'accès à Internet. Vous pouvez ajouter un proxy transparent ou explicite. Les paramètres --proxy et --cacert sont facultatifs et vous ne serez pas invité à les ajouter. Si vous disposez d'un serveur proxy, vous devrez saisir les paramètres comme indiqué.

   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 console pour utiliser un serveur proxy HTTP ou HTTPS en utilisant l'un des formats suivants :

- http://adresse:port
- http://nom-d'utilisateur:mot-de-passe@adresse:port
- http://nom-de-domaine%92nom-d'utilisateur:mot-de-passe@adresse:port
- https://adresse:port
- https://nom-d'utilisateur:mot-de-passe@adresse:port
- https://nom-de-domaine%92nom-d'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 un \ comme indiqué ci-dessus.
  - L'agent de console ne prend pas en charge les noms d'utilisateur ou 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 préfixant d'une barre oblique inverse : & ou !

    Par exemple:

http://bxpproxyuser:netapp1\!@adresse:3128

`--cacert`spécifie un certificat signé par une autorité de certification à utiliser pour l'accès HTTPS entre l'agent de console et le serveur proxy. Ce paramètre est requis pour les serveurs proxy HTTPS, les serveurs proxy d'interception et les serveurs proxy transparents.

+ Voici un exemple de configuration d'un serveur proxy transparent. Lorsque vous configurez un proxy transparent, vous n'avez pas besoin de définir le serveur proxy. Vous ajoutez uniquement un certificat signé par une autorité de certification à votre hôte d'agent de console :

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

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
...
# 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
...
Esc:wq
```

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

Quelle est la prochaine étape ?

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

Enregistrer l'agent de console auprès de la console NetApp

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 console NetApp

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 "Console NetApp" 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 "Console NetApp" 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 console NetApp .

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 console Web NetApp

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

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.

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.
\ 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 .

Points de terminaison	But
\ https://support.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 console NetApp .
\ 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 console NetApp .
\ 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 console NetApp 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

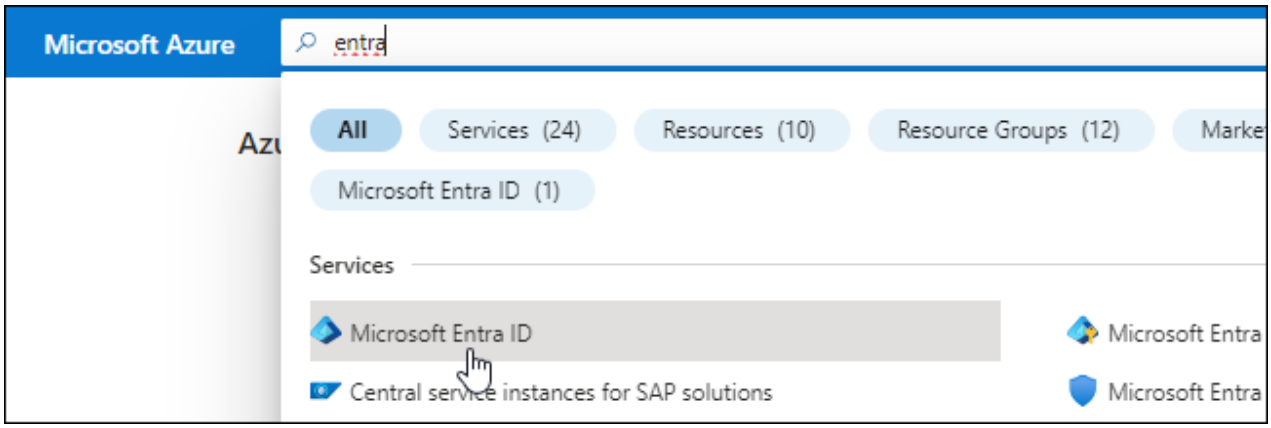
Lorsque l'agent de console est installé sur site, vous devez lui accorder des autorisations Azure en configurant un principal de service dans Microsoft Entra ID et en obtenant les informations d'identification Azure dont l'agent de console a besoin.

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 console NetApp).
   - **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 .

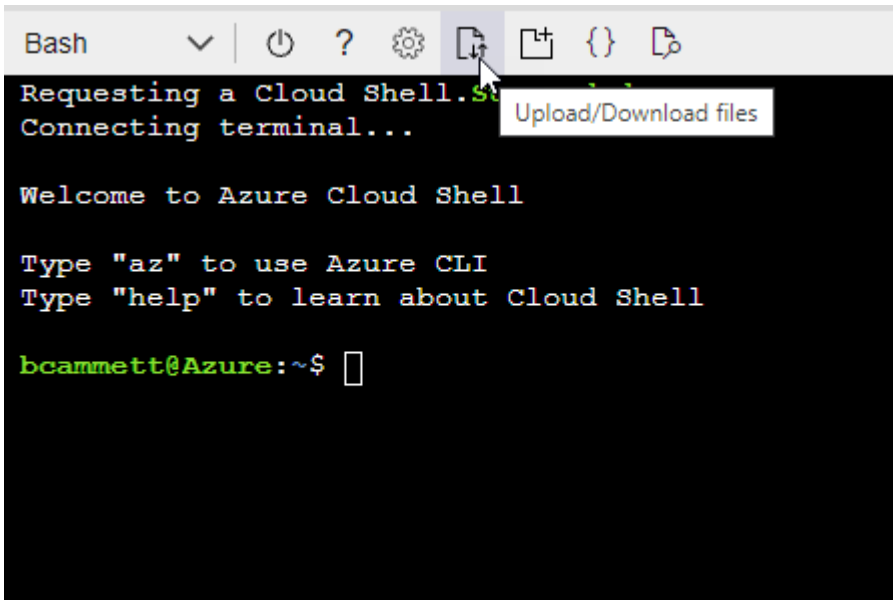
      Exemple

```
"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 :

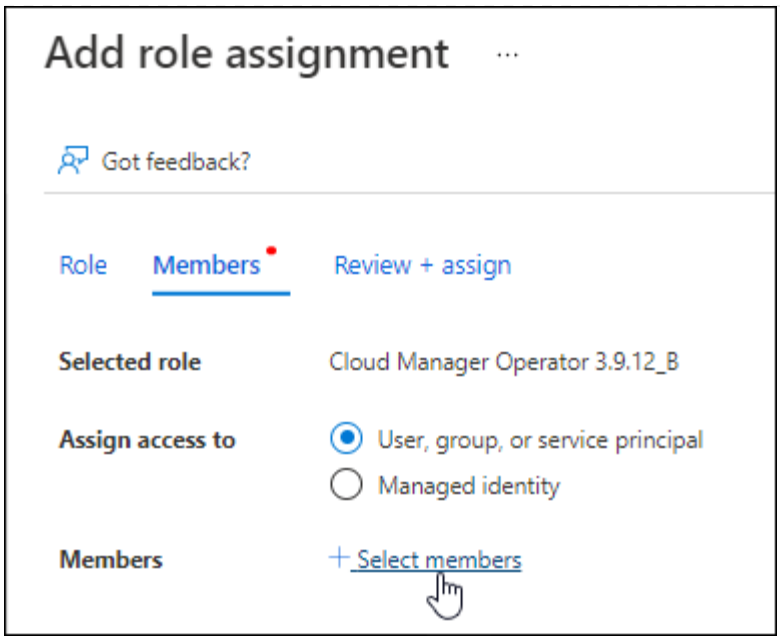
```
az role definition create --role-definition
Connector_Policy.json
```

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 :

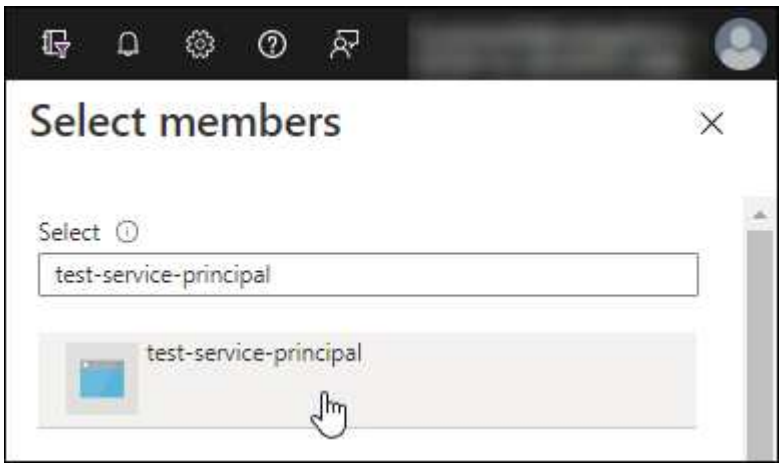
   a. Depuis le portail Azure, ouvrez le service **Abonnements**.
   b. Sélectionnez l'abonnement.
   c. Sélectionnez **Contrôle d'accès (IAM) > Ajouter > Ajouter une attribution de rôle**.
   d. Dans l'onglet **Rôle**, sélectionnez le rôle **Opérateur de console** et sélectionnez **Suivant**.
   e. Dans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

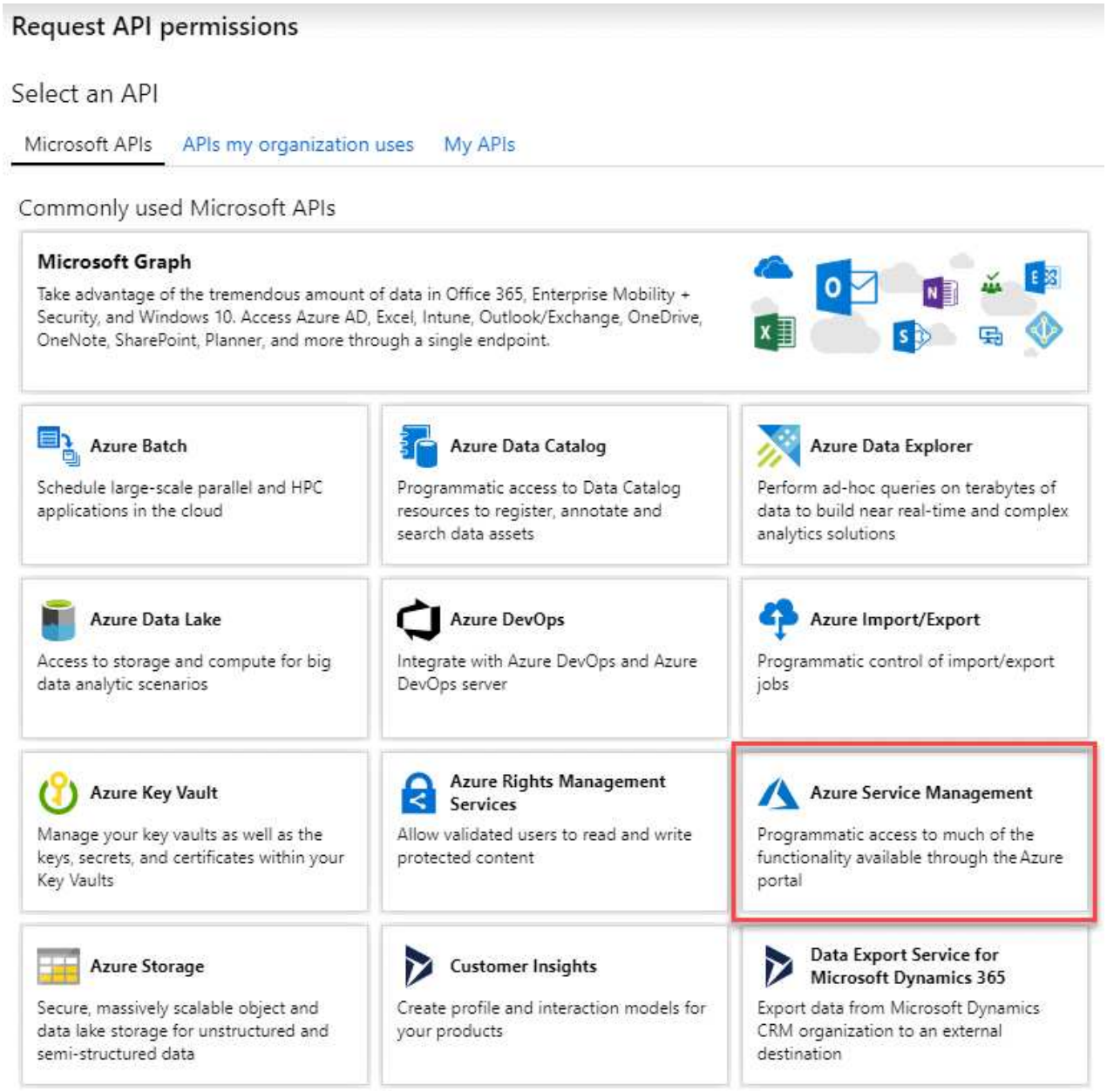
Le principal du service dispose désormais des autorisations Azure requises pour déployer l'agent de la console.

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 console NetApp , vous pouvez sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

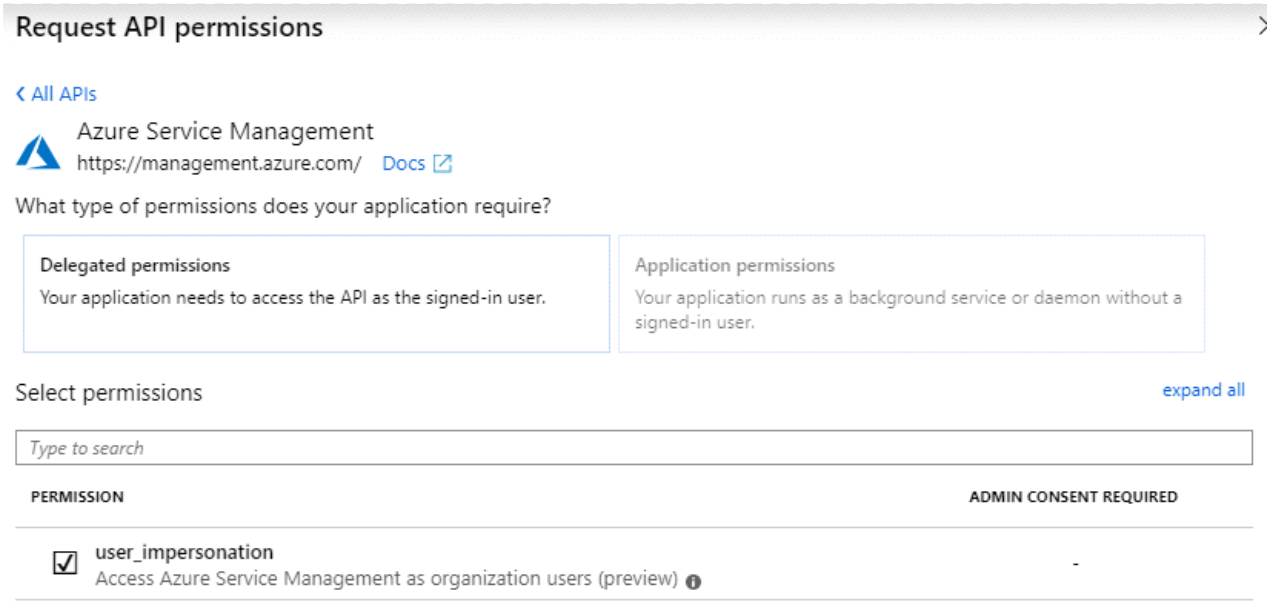
Ajouter des autorisations à l'API de gestion des services Windows Azure

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**.

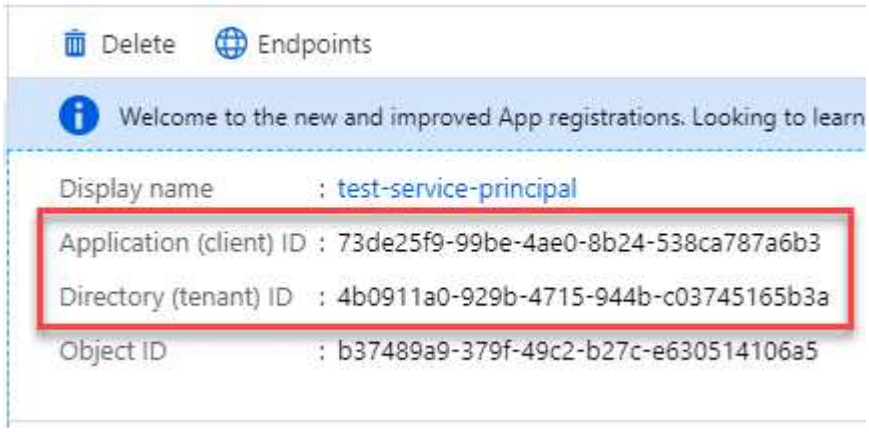


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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

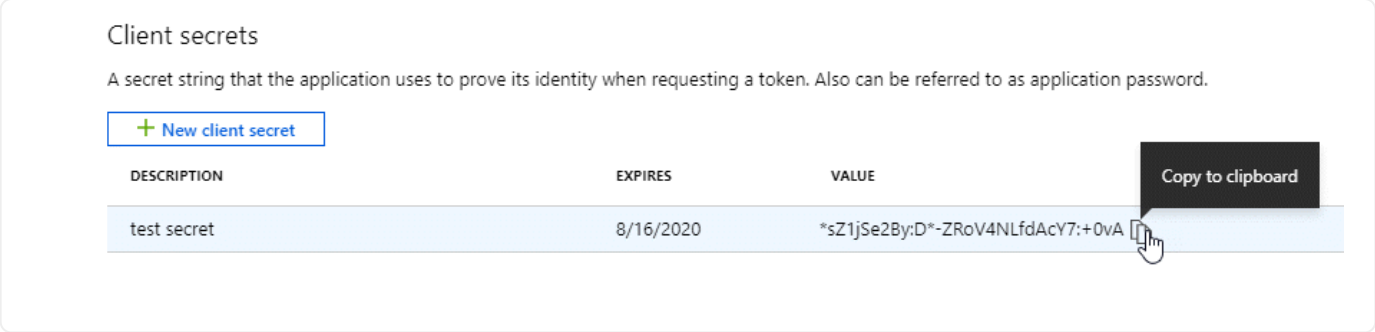
1. Dans le service **Microsoft Entra ID**, sélectionnez **Inscriptions d'applications** et sélectionnez l'application.
2. Copiez l'**ID d'application (client)** et l'**ID de répertoire (locataire)**.



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 console NetApp . 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 console NetApp .

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 sous la forme 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 console NetApp

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

Abonnez-vous aux services intelligents NetApp (mode standard)

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

Un abonnement au marketplace permet de facturer les services de données NetApp suivants :

- Sauvegarde et récupération NetApp
- Cloud Volumes ONTAP
- Hiérarchisation du cloud NetApp
- Résilience aux ransomwares NetApp
- Reprise après sinistre NetApp

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

Avant de commencer

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

AWS

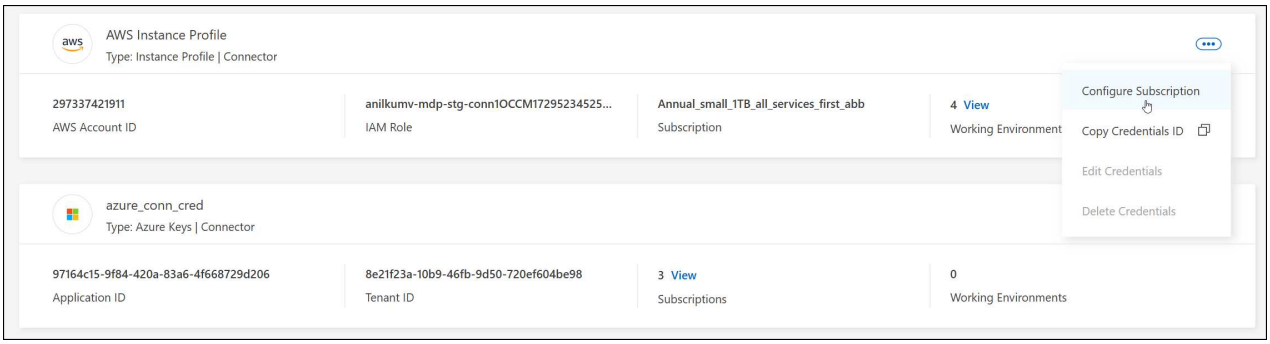
La vidéo suivante montre les étapes à suivre pour s'abonner à NetApp Intelligent Services depuis AWS Marketplace :

Abonnez-vous aux services intelligents NetApp depuis la place de marché AWS

Étapes

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

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



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 console NetApp .

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

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

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

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

- Sélectionnez **Enregistrer**.

Azuré

Étapes

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

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

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 console NetApp .

   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**.

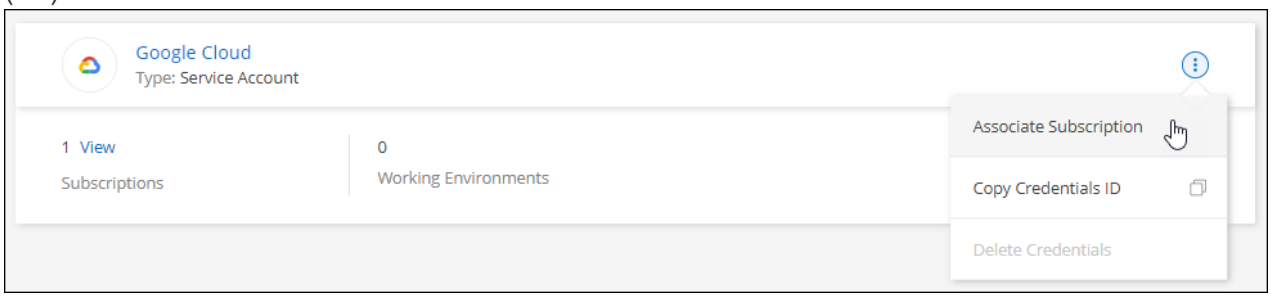
        La vidéo suivante montre les étapes à suivre pour s'abonner à partir de la Place de marché Azure :

   Abonnez-vous aux services intelligents NetApp depuis la place de marché Azure

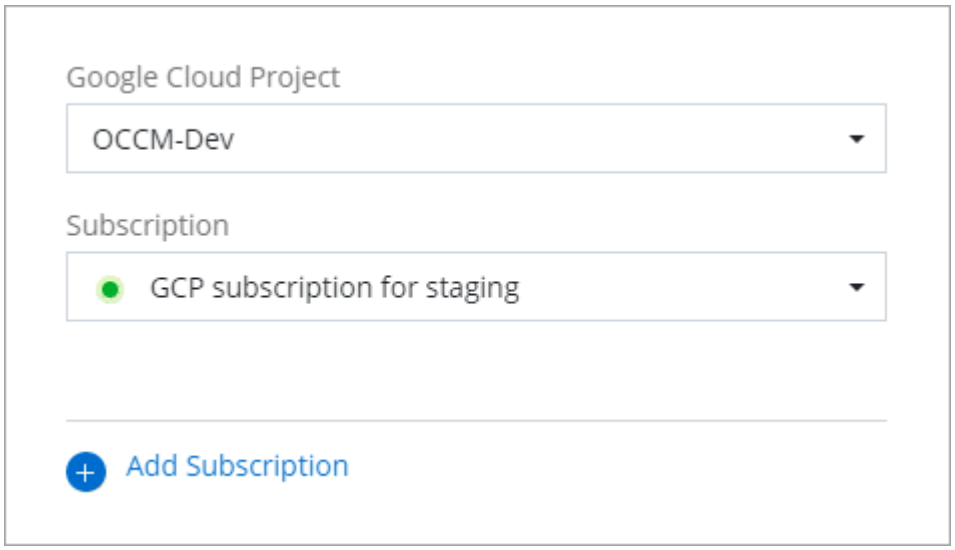
Google Cloud

Étapes

1. Sélectionnez **Administration > *Informations d'identification**.
2. Sélectionnez **Informations d'identification de l'organisation**.
3. Sélectionnez le menu d'action pour un ensemble d'informations d'identification associées à un agent de console, puis sélectionnez **Configurer l'abonnement**. + nouvelle capture d'écran nécessaire (TS)



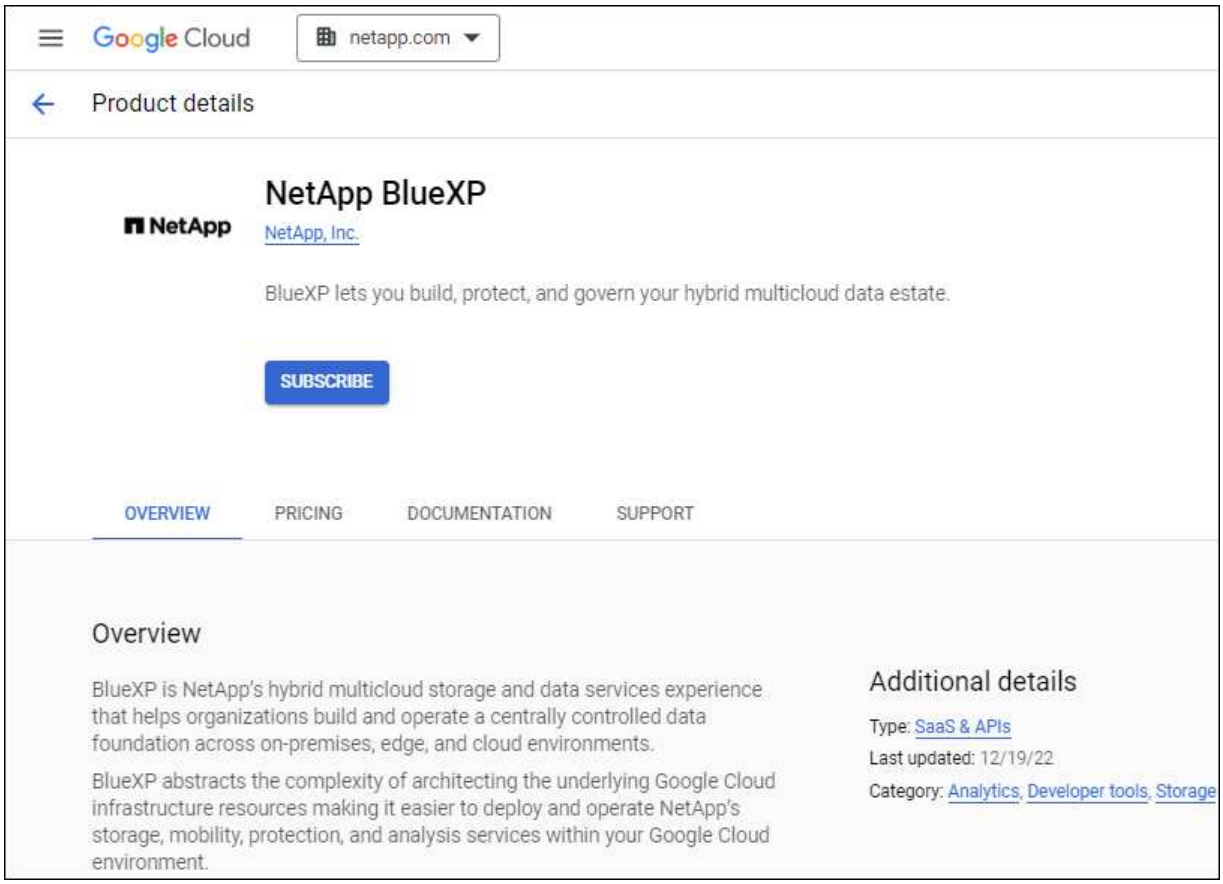
4. Pour configurer un abonnement existant avec les informations d'identification sélectionnées, sélectionnez un projet et un abonnement Google Cloud dans la liste déroulante, puis sélectionnez **Configurer**.



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

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

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

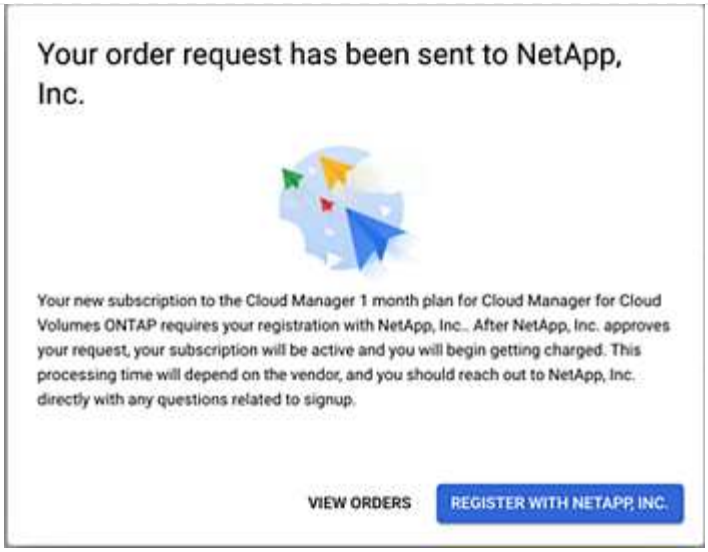


b. Sélectionnez **S'abonner**.
c. Sélectionnez le compte de facturation approprié et acceptez les conditions générales.
d. Sélectionnez **S'abonner**.

   Cette étape envoie votre demande de transfert à NetApp.

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

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



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

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

- 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.

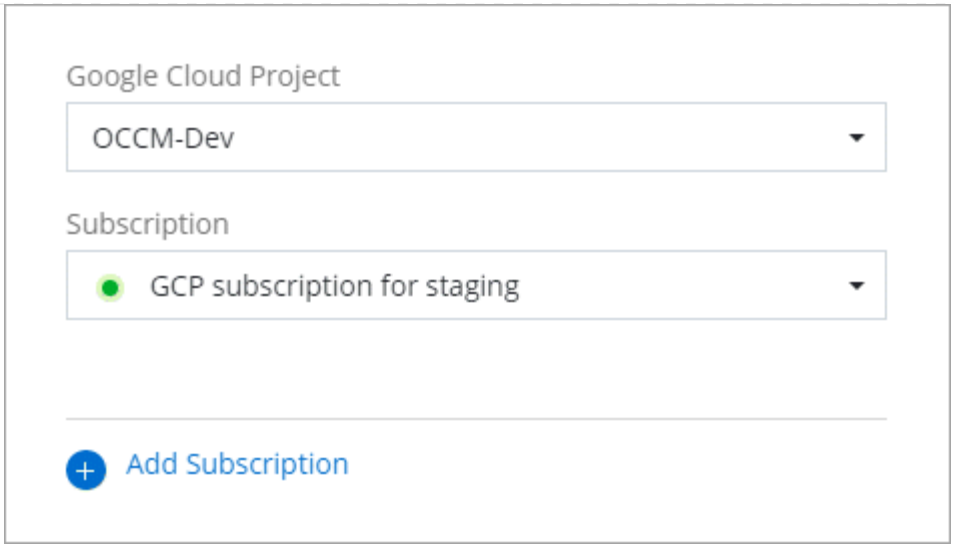
Pour toutes les autres organisations ou comptes, vous devrez associer manuellement l'abonnement en répétant ces étapes.

- Sélectionnez **Enregistrer**.

  La vidéo suivante montre les étapes à suivre pour s'abonner à partir de Google Cloud Marketplace :

Abonnez-vous à Google Cloud Marketplace

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



Informations connexes

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

Ce que vous pouvez faire ensuite (mode standard)

Maintenant que vous êtes connecté et que vous avez configuré la console NetApp en mode standard, les utilisateurs peuvent créer et découvrir des systèmes de stockage et utiliser les services de données NetApp .

Si vous avez installé un agent de console dans AWS, Microsoft Azure ou Google Cloud, la console découvre automatiquement des informations sur les compartiments Amazon S3, le stockage Azure Blob ou les compartiments Google Cloud Storage à l'emplacement où l'agent est installé. Ces systèmes sont automatiquement ajoutés à la page **Systèmes**.

Pour obtenir de l'aide, rendez-vous sur le "page d'accueil de la documentation de la console NetApp" pour afficher la documentation de la console NetApp .

Informations connexes

"Modes de déploiement de la console NetApp"

Démarrer avec le mode restreint

Démarrage du flux de travail (mode restreint)

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

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

1 **"Préparez-vous au déploiement"**

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

2 **"Déployer l'agent de console"**

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

3 **"Abonnez-vous aux services intelligents NetApp (facultatif)"**

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

Préparez-vous au déploiement en mode restreint

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

Étape 1 : Comprendre le fonctionnement du mode restreint

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

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

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

"Découvrez comment fonctionne le mode restreint" .

Étape 2 : Examiner les options d'installation

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

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

Étape 3 : Examiner les exigences de l'hôte

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

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

Hôte dédié

L'agent de console n'est pas pris en charge sur un hôte partagé avec d'autres applications. L'hôte doit être un hôte dédié. L'hôte peut être de n'importe quelle architecture répondant 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 de console nécessite cet espace dans `/var` car Docker ou Podman sont architecturés pour créer les conteneurs dans ce répertoire. Plus précisément, ils créeront des conteneurs dans le `/var/lib/containers/storage` annuaire. 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.

Configuration requise pour le système d'exploitation et les 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 a
Red Hat Enterprise Linux	9,1 à 9,4 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 Afficher les exigences de configuration de Podman .	Pris en charge en mode d'application ou en mode permissif • La gestion des systèmes Cloud Volumes ONTAP n'est PAS prise en charge par les agents sur lesquels SELinux est activé sur le système d'exploitation.
Ubuntu	24,04 LTS	3.9.45 ou version ultérieure avec la console NetApp en mode standard ou en mode restreint	Docker Engine 23.06 à 28.0.0.	Non pris en charge

Type d'instance AWS EC2

Un type d'instance qui répond aux exigences de CPU et de RAM ci-dessus. Nous recommandons t3.2xlarge.

Taille de la machine virtuelle Azure

Un type d'instance qui répond aux exigences de CPU et de RAM ci-dessus. Nous recommandons Standard_D8s_v3.

Type de machine Google Cloud

Un type d'instance qui répond aux exigences de CPU et de RAM ci-dessus. 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 "Fonctionnalités de la machine virtuelle blindée"

Espace disque dans /opt

100 Go d'espace doivent être disponibles

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

Espace disque dans /var

20 Go d'espace doivent être disponibles

L'agent de console nécessite cet espace dans `/var` car Docker ou Podman sont architecturés pour créer les conteneurs dans ce répertoire. Plus précisément, ils créeront des conteneurs dans le `/var/lib/containers/storage` annuaire. Les montages externes ou les liens symboliques ne fonctionnent pas pour cet espace.

Étape 4 : installer Podman ou Docker Engine

Pour installer manuellement l'agent de console, préparez l'hôte en installant Podman ou Docker Engine.

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

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

  Afficher les versions de Podman prises en charge .

- Docker Engine est requis pour Ubuntu.

  Afficher les versions de Docker Engine prises en charge .

Exemple 5. 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 8, vérifiez que votre version Podman utilise 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 Red Hat Enterprise Linux.

   Pour Red Hat Enterprise Linux 9 :

```
sudo dnf install podman-2:<version>
```

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

   Pour Red Hat Enterprise Linux 8 :

```
sudo dnf install podman-3:<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.
6. Si vous utilisez Red Hat Enterprise :

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

   Pour Red Hat Enterprise Linux 9 :

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

   Pour Red Hat Enterprise Linux 8 :

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

7. 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.

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

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

      ```
      podman info | grep networkBackend
      ```

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

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

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

   d. 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` .

9. Redémarrez podman.

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Moteur Docker

Suivez la documentation de Docker pour installer Docker Engine.

Étapes

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

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

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

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

Étape 5 : Préparer l'accès au réseau

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

Connexions aux réseaux cibles

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

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

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

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

+

Points de terminaison	But
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Pour fournir des fonctionnalités et des services au sein de la console NetApp .
\ https://cdn.auth0.com \ https://services.cloud.netapp.com	Votre navigateur Web se connecte à ces points de terminaison pour une authentification utilisateur centralisée via la console NetApp .

Accès Internet sortant pour les opérations quotidiennes

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

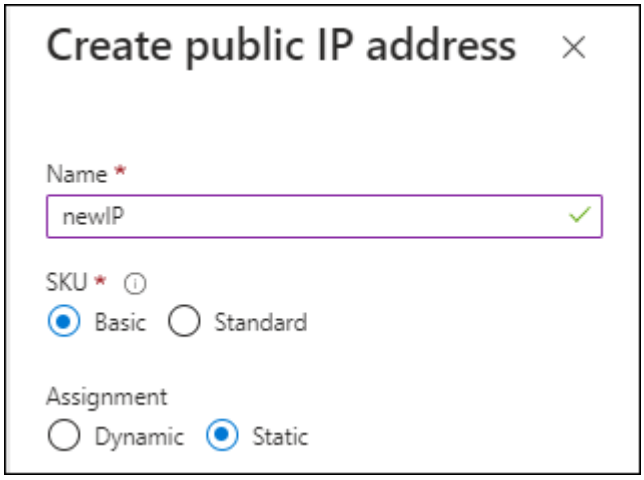
Points de terminaison	But
Environnements AWS	Services AWS (amazonaws.com) : • CloudFormation • Cloud de calcul élastique (EC2) • Gestion des identités et des accès (IAM) • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Service de stockage simple (S3)
Pour gérer les ressources AWS. Le point de terminaison dépend de votre région AWS. "Consultez la documentation AWS pour plus de détails"	**Environnements Azure**
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Pour gérer les ressources dans les régions publiques Azure.
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	Pour gérer les ressources dans les régions Azure Government.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Pour gérer les ressources dans les régions Azure Chine.

Points de terminaison	But
Environnements Google Cloud	\ https://www.googleapis.com/compute/v1/ \ https://compute.googleapis.com/compute/v1 \ https://cloudresourcemanager.googleapis.com/v1/projects \ https://www.googleapis.com/compute/beta \ https://storage.googleapis.com/storage/v1 \ https://www.googleapis.com/storage/v1 \ https://iam.googleapis.com/v1 \ https://cloudkms.googleapis.com/v1 \ https://www.googleapis.com/deploymentmanager/v2/projects
Pour gérer les ressources dans Google Cloud.	• Points de terminaison de la console NetApp *
\ https://mysupport.netapp.com	Pour obtenir des informations de licence et envoyer des messages AutoSupport au support NetApp .
\ https://support.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 console NetApp .
\ 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 console NetApp .

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

Adresse IP publique dans Azure

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



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

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

"Documentation Azure : Référence IP publique"

Serveur proxy

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

- adresse IP
- Informations d'identification
- Certificat HTTPS

Ports

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

- HTTP (80) et HTTPS (443) donnent accès à l'interface utilisateur locale, que vous utiliserez dans de rares circonstances.
- SSH (22) n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.
- Les connexions entrantes via le port 3128 sont requises si vous déployez des systèmes Cloud Volumes ONTAP dans un sous-réseau où une connexion Internet sortante n'est pas disponible.

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

Activer NTP

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

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

Étape 6 : Préparer les autorisations cloud

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

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

Rôle AWS IAM

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

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

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

Étapes

1. Connectez-vous à la console AWS et accédez au service IAM.
2. Créer une politique:
   a. Sélectionnez **Politiques > Créer une politique**.
   b. Sélectionnez **JSON** et copiez et collez le contenu du"Politique IAM pour l'agent de console" .
   c. Terminez les étapes restantes pour créer la politique.
3. Créer un rôle IAM :
   a. Sélectionnez **Rôles > Créer un rôle**.
   b. Sélectionnez **Service AWS > EC2**.
   c. Ajoutez des autorisations en joignant la politique que vous venez de créer.
   d. Terminez les étapes restantes pour créer le rôle.

Résultat

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

Clé d'accès AWS

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

Étapes

1. Connectez-vous à la console AWS et accédez au service IAM.
2. Créer une politique:
   a. Sélectionnez **Politiques > Créer une politique**.
   b. Sélectionnez **JSON** et copiez et collez le contenu du"Politique IAM pour l'agent de console" .
   c. Terminez les étapes restantes pour créer la politique.

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

   Pour les régions standard, les autorisations sont réparties sur deux politiques. Deux politiques sont requises en raison d'une limite de taille maximale de caractères pour les politiques gérées dans AWS. "En savoir plus sur les stratégies IAM pour l'agent de console" .
3. Attachez les politiques à un utilisateur IAM.
   - "Documentation AWS : Création de rôles IAM"
   - "Documentation AWS : Ajout et suppression de stratégies IAM"

4. Assurez-vous que l'utilisateur dispose d'une clé d'accès que vous pouvez ajouter à la console NetApp après avoir installé l'agent de console.

Rôle Azure

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

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

Étapes

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

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

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

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

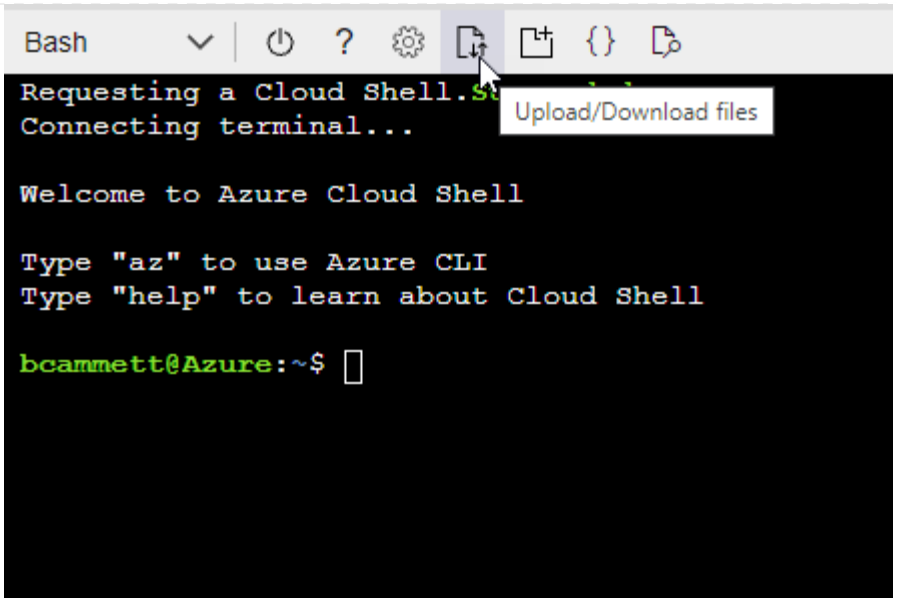
   Exemple

   ```
   "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 Connector_Policy.json
```

Principal de service Azure

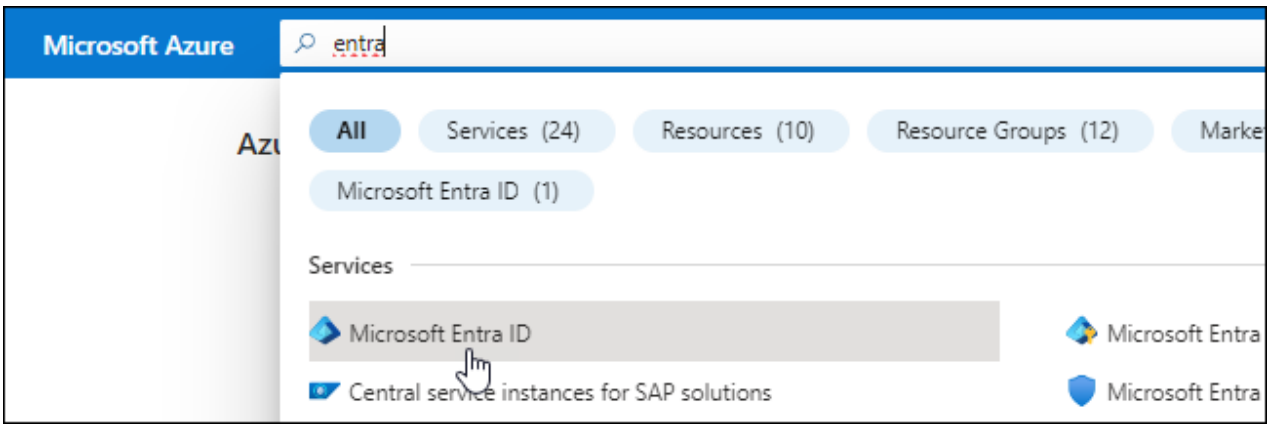
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont la console a besoin. Vous devez fournir ces informations d'identification à la console après avoir installé l'agent de la console.

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

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

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

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



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

5. Précisez les détails de l'application :
   - **Nom**: Saisissez un nom pour l'application.
   - **Type de compte** : sélectionnez un type de compte (n'importe lequel fonctionnera avec la console NetApp).
   - **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 .

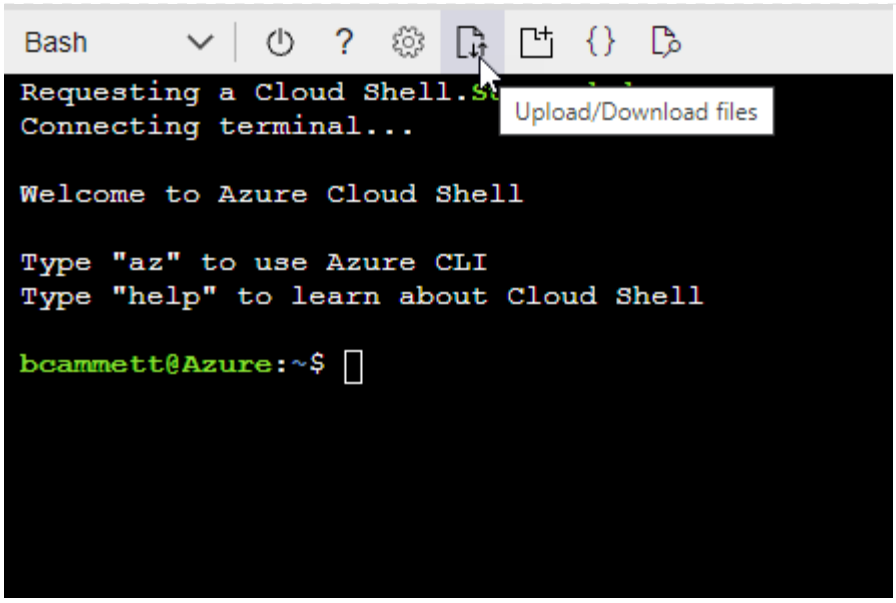
      Exemple

      ```
      "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
Connector_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**.

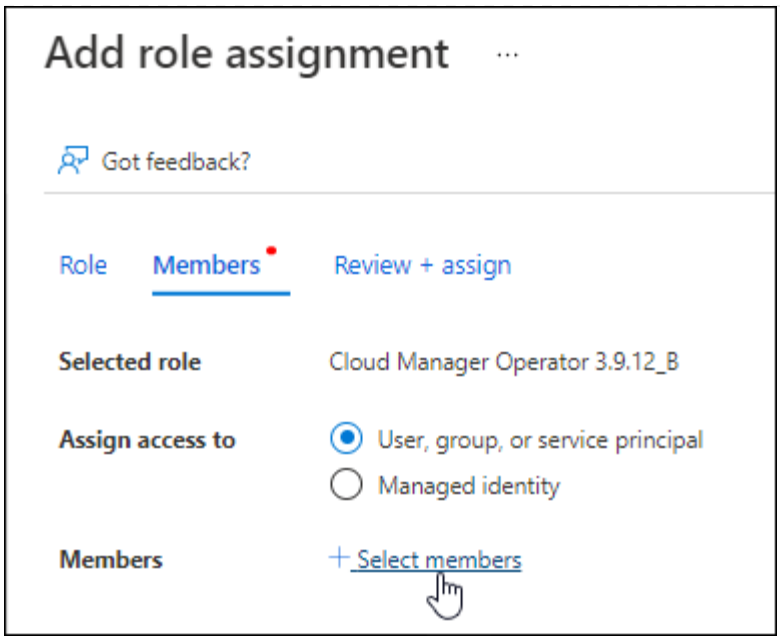
   b. Sélectionnez l'abonnement.

   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**.

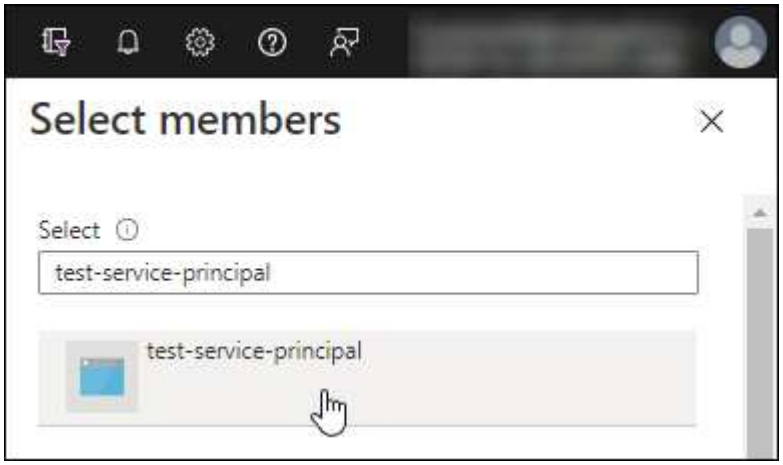
   e. Dans l'onglet **Membres**, procédez comme suit :

      - 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**.

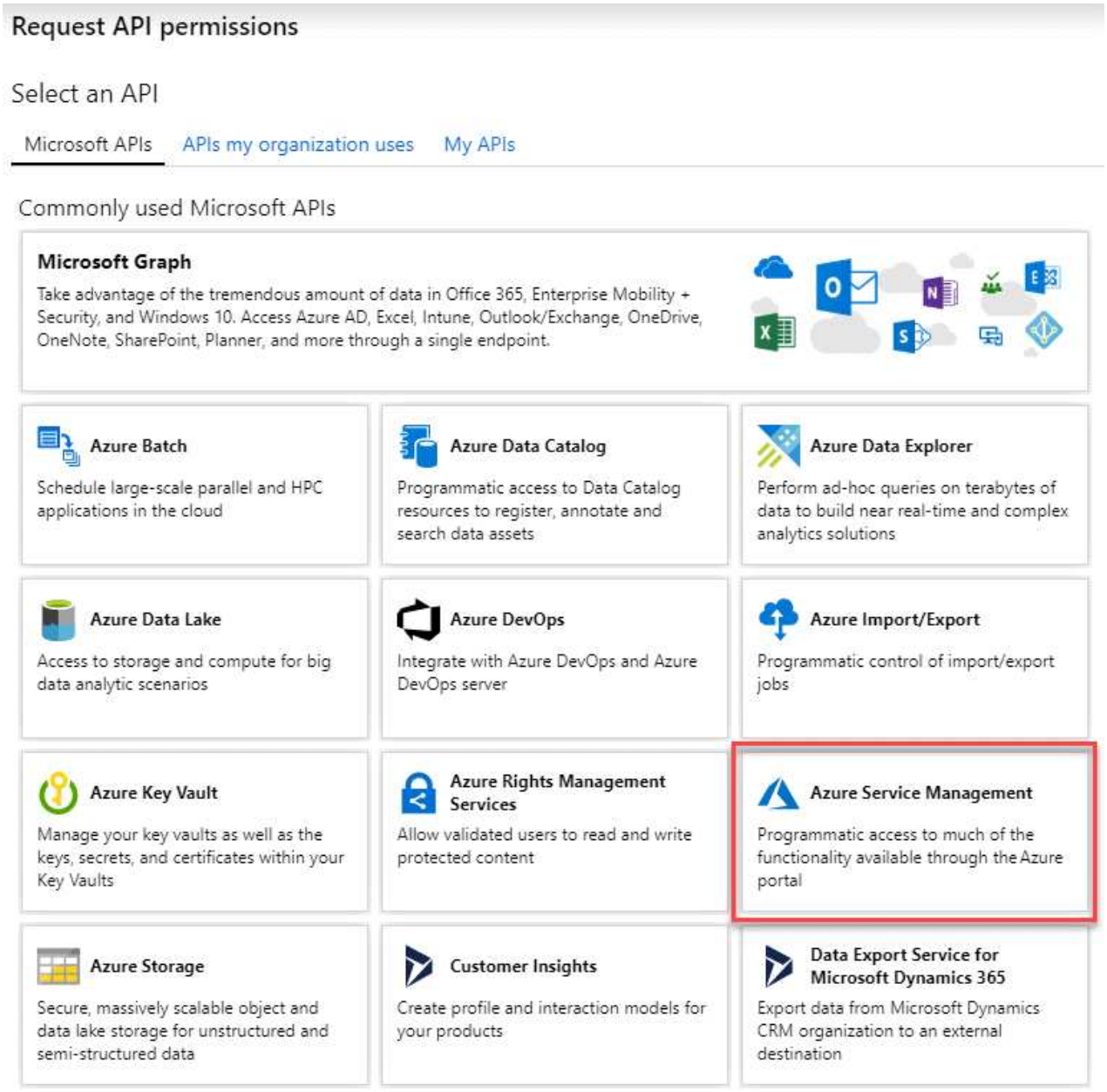
Le principal du service dispose désormais des autorisations Azure requises pour déployer l'agent de la console.

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 console NetApp , vous pouvez sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

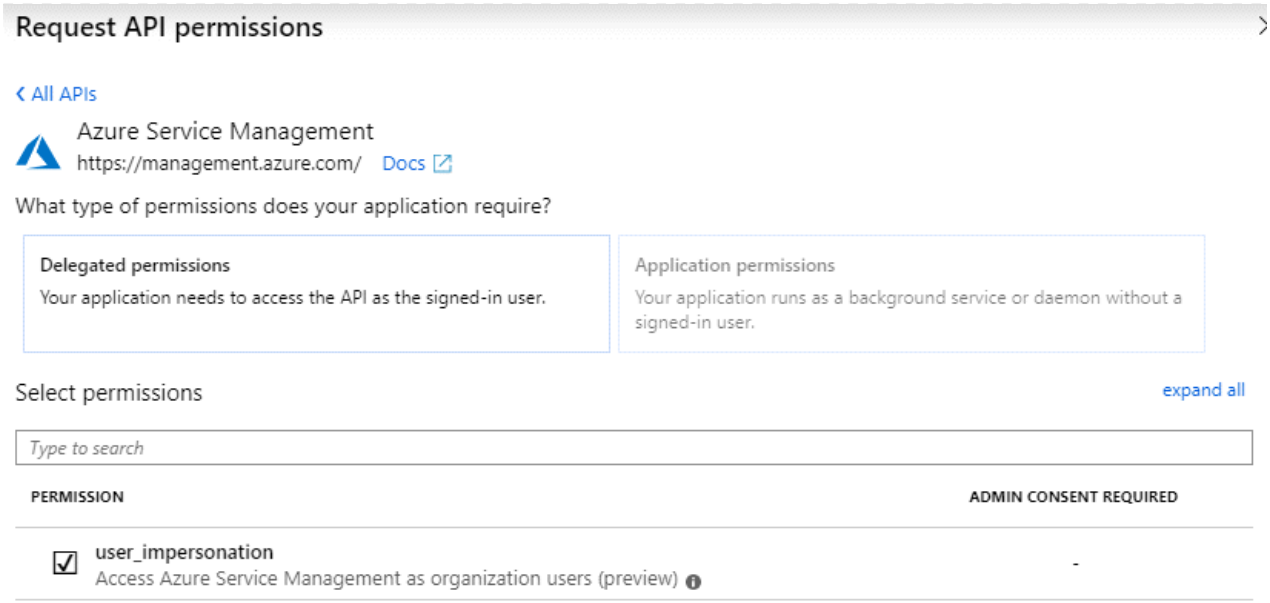
Ajouter des autorisations à l'API de gestion des services Windows Azure

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

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

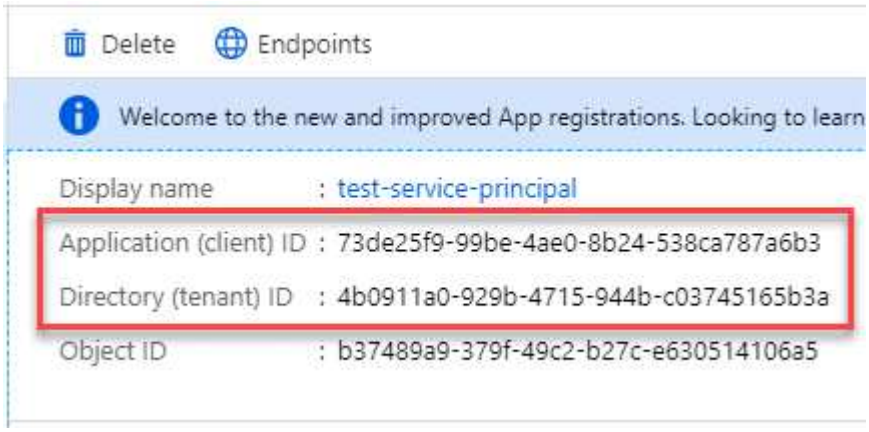


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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

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



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

Créer un secret client

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

Résultat

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

Compte de service Google Cloud

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

Étapes

1. Créer un rôle personnalisé dans Google Cloud :

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

   b. Depuis Google Cloud, activez Cloud Shell.

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

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

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

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

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

2. Créer un compte de service dans Google Cloud :

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

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

   c. Sélectionnez le rôle que vous venez de créer.

   d. Terminez les étapes restantes pour créer le rôle.

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

Résultat

Vous disposez désormais d'un compte de service que vous pouvez attribuer à l'instance de machine virtuelle de l'agent de console.

Étape 7 : Activer les API Google Cloud

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

Étape

1. "Activez les API Google Cloud suivantes dans votre projet"
    - API du gestionnaire de déploiement cloud V2
    - API 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)

      (Requis uniquement si vous prévoyez d'utiliser NetApp Backup and Recovery avec des clés de chiffrement gérées par le client (CMEK))

Déployer l'agent de console en mode restreint

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

Étape 1 : Installer l'agent de console

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

Place de marché commerciale AWS

Avant de commencer

Vous devriez avoir les éléments suivants :

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

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

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

  "Découvrez comment configurer les autorisations AWS"

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

  "Examen des exigences de l'instance" .

- Une paire de clés pour l'instance EC2.

Étapes

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

   Le processus d'abonnement peut prendre quelques minutes.

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

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

7. Suivez les instructions pour configurer et déployer l'instance :
   - **Nom et balises** : saisissez un nom et des balises pour l'instance.
   - **Images d'application et de système d'exploitation** : ignorez cette section. L'AMI de l'agent de console est déjà sélectionné.
   - **Type d'instance** : Selon la disponibilité de la région, choisissez un type d'instance qui répond aux exigences de RAM et de CPU (t3.2xlarge est présélectionné et recommandé).
   - **Paire de clés (connexion)** : sélectionnez la paire de clés que vous souhaitez utiliser pour vous connecter en toute sécurité à l'instance.
   - **Paramètres réseau** : Modifiez les paramètres réseau selon vos besoins :
     - Choisissez le VPC et le sous-réseau souhaités.
     - Spécifiez si l'instance doit avoir une adresse IP publique.

- Spécifiez les paramètres du groupe de sécurité qui activent les méthodes de connexion requises pour l'instance de l'agent de console : SSH, HTTP et HTTPS.

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

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

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

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

Résultat

AWS lance le logiciel avec les paramètres spécifiés. L'instance de l'agent de console et le logiciel s'exécutent en environ cinq minutes.

Quelle est la prochaine étape ?

Configurer la console NetApp .

Place de marché AWS Gov

Avant de commencer

Vous devriez avoir les éléments suivants :

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

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

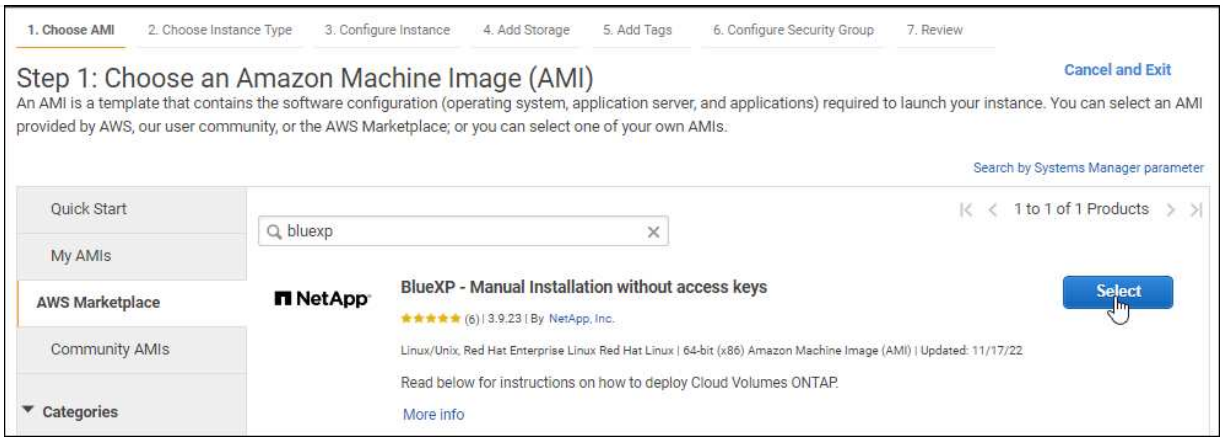
- Un rôle IAM avec une politique attachée qui inclut les autorisations requises pour l'agent de la console.

  "Découvrez comment configurer les autorisations AWS"

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

Étapes

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



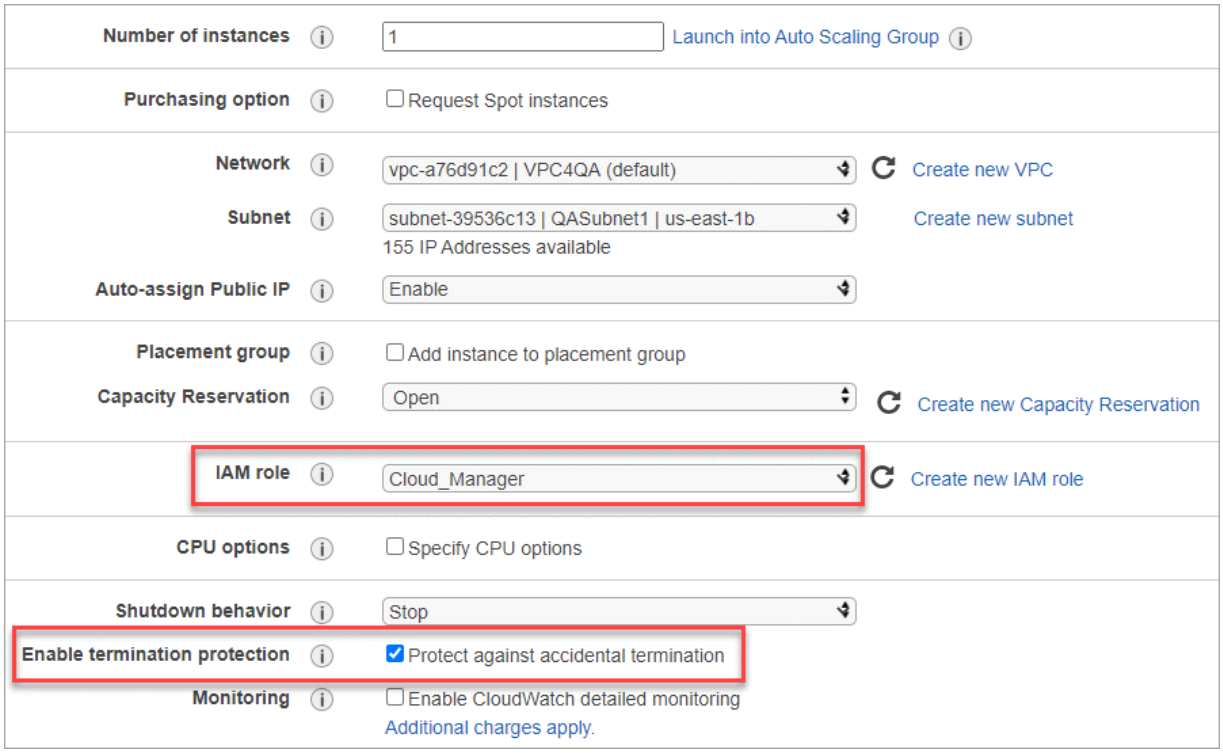
d. Sélectionnez **Continuer**.

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

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

     "Examiner les exigences de l'instance" .

   - **Configurer les détails de l'instance** : sélectionnez un VPC et un sous-réseau, choisissez le rôle IAM que vous avez créé à l'étape 1, activez la protection de terminaison (recommandée) et choisissez toute autre option de configuration qui répond à vos besoins.



   - **Ajouter du stockage** : Conservez les options de stockage par défaut.
   - **Ajouter des balises** : saisissez des balises pour l'instance, si vous le souhaitez.
   - **Configurer le groupe de sécurité** : spécifiez les méthodes de connexion requises pour l'instance de l'agent de console : SSH, HTTP et HTTPS.
   - **Révision** : Vérifiez vos sélections et sélectionnez **Lancer**.

Résultat

AWS lance le logiciel avec les paramètres spécifiés. L'instance de l'agent de console et le logiciel s'exécutent en environ cinq minutes.

Quelle est la prochaine étape ?

Configurer la console.

Place de marché Azure Gov

Avant de commencer

Vous devriez avoir les éléments suivants :

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

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

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

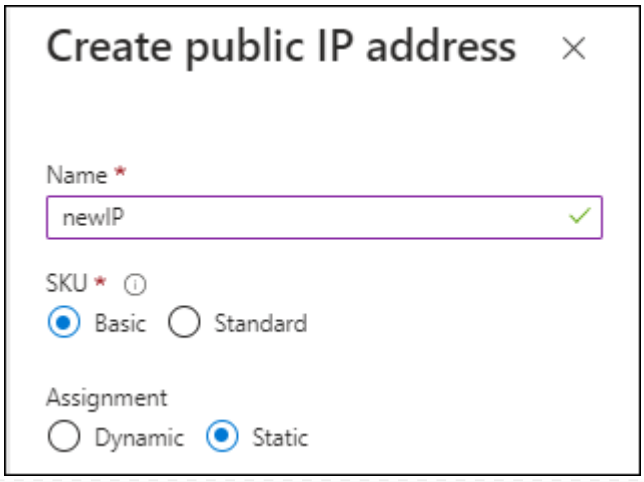
  "Découvrez comment configurer les autorisations Azure"

Étapes

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

   Notez les points suivants lorsque vous configurez la machine virtuelle :

   - **Taille de la VM** : Choisissez une taille de VM qui répond aux exigences de CPU et de RAM. Nous recommandons Standard_D8s_v3.
   - **Disques** : L'agent de console peut fonctionner de manière optimale avec des disques HDD ou SSD.
   - **IP publique** : si vous souhaitez utiliser une adresse IP publique avec la machine virtuelle de l'agent de console, l'adresse IP doit utiliser un SKU de base pour garantir que la console utilise cette adresse IP publique.



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

"Documentation Azure : Référence IP publique"

- **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.

Résultat

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

Quelle est la prochaine étape ?

Configurer la console NetApp .

Installation manuelle

Avant de commencer

Vous devriez avoir les éléments suivants :

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

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

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

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

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

À propos de cette tâche

Le programme d'installation disponible sur le site de support NetApp peut être une version antérieure. 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 de l'agent de la console à partir du "Site de support NetApp" , puis copiez-le sur l'hôte Linux.

   Vous devez télécharger le programme d'installation de l'agent « en ligne » destiné à être utilisé sur votre réseau ou dans le cloud.

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 des informations de proxy si votre réseau nécessite un proxy pour l'accès à Internet. Vous pouvez ajouter un proxy transparent ou explicite. Les paramètres --proxy et --cacert sont facultatifs et vous ne serez pas invité à les ajouter. Si vous disposez d'un serveur proxy, vous devrez saisir les paramètres comme indiqué.

   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 console pour utiliser un serveur proxy HTTP ou HTTPS en utilisant l'un

des formats suivants :

- http://adresse:port
- http://nom-d'utilisateur:mot-de-passe@adresse:port
- http://nom-de-domaine%92nom-d'utilisateur:mot-de-passe@adresse:port
- https://adresse:port
- https://nom-d'utilisateur:mot-de-passe@adresse:port
- https://nom-de-domaine%92nom-d'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 un \ comme indiqué ci-dessus.
  - L'agent de console ne prend pas en charge les noms d'utilisateur ou 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 préfixant d'une barre oblique inverse : & ou !

    Par exemple:

http://bxpproxyuser:netapp1\!@adresse:3128

`--cacert`spécifie un certificat signé par une autorité de certification à utiliser pour l'accès HTTPS entre l'agent de console et le serveur proxy. Ce paramètre est requis pour les serveurs proxy HTTPS, les serveurs proxy d'interception et les serveurs proxy transparents.

+ Voici un exemple de configuration d'un serveur proxy transparent. Lorsque vous configurez un proxy transparent, vous n'avez pas besoin de définir le serveur proxy. Vous ajoutez uniquement un certificat signé par une autorité de certification à votre hôte d'agent de console :

+

```
 ./NetApp_Console_Agent_Cloud_v4.0.0 --cacert
/tmp/cacert/certificate.cer
```

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
...
# 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
...
Esc:wq
```

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

Résultat

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

Quelle est la prochaine étape ?

Configurer la console NetApp .

Étape 2 : Configurer la console NetApp

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

Avant de commencer

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

Si votre identifiant est associé à une autre organisation, vous devrez vous inscrire avec un nouvel identifiant. Sinon, vous ne verrez pas l'option permettant d'activer le mode restreint sur l'écran de configuration.

Étapes

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

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

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

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

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

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

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

a. Sélectionnez **Commençons**.

Résultat

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

Quelle est la prochaine étape ?

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

Étape 3 : Accorder des autorisations à la console NetApp

Si vous avez déployé l'agent de console à partir de la Place de marché Azure ou si vous avez installé manuellement le logiciel de l'agent de console, vous devez fournir les autorisations que vous avez précédemment configurées.

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

"Apprenez à préparer les autorisations cloud" .

Rôle AWS IAM

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

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

Étapes

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

Clé d'accès AWS

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

Étapes

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

Rôle Azure

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

Étapes

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

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

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

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

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

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

Principal de service Azure

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

Étapes

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

Résultat

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

Compte de service Google Cloud

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

Étapes

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

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

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

S'abonner aux services intelligents NetApp (mode restreint)

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

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

- Sauvegarde et récupération NetApp
- Cloud Volumes ONTAP
- Hiérarchisation du cloud NetApp
- Résilience aux ransomwares NetApp
- Reprise après sinistre NetApp

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

Avant de commencer

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

AWS

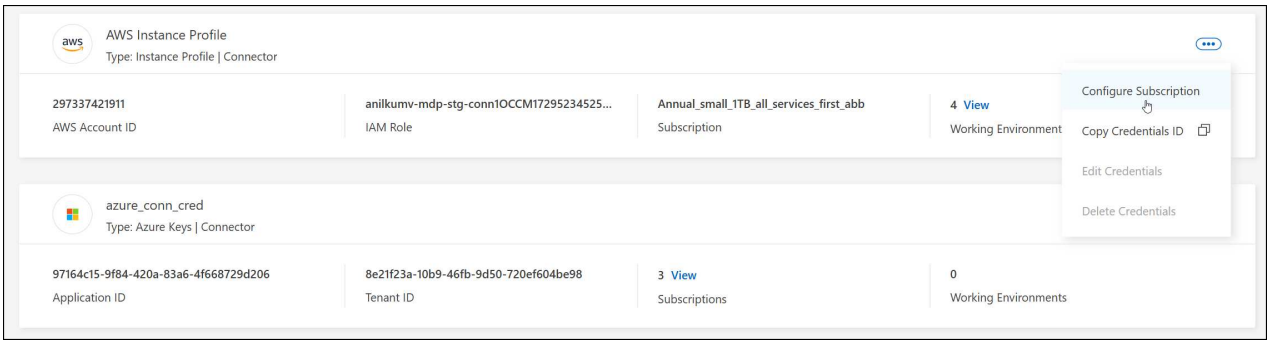
La vidéo suivante montre les étapes à suivre pour s'abonner à NetApp Intelligent Services depuis AWS Marketplace :

Abonnez-vous aux services intelligents NetApp depuis la place de marché AWS

Étapes

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

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



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 console NetApp .

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

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

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

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

- Sélectionnez **Enregistrer**.

Azuré

Étapes

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

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

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 console NetApp .

   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**.

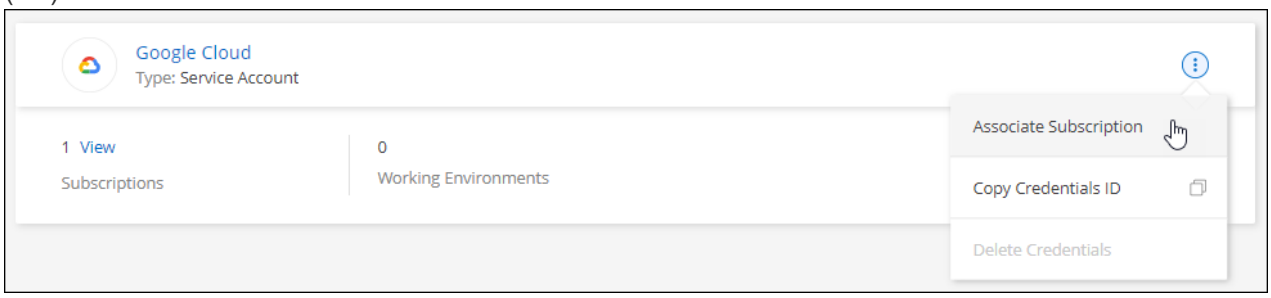
        La vidéo suivante montre les étapes à suivre pour s'abonner à partir de la Place de marché Azure :

   Abonnez-vous aux services intelligents NetApp depuis la place de marché Azure

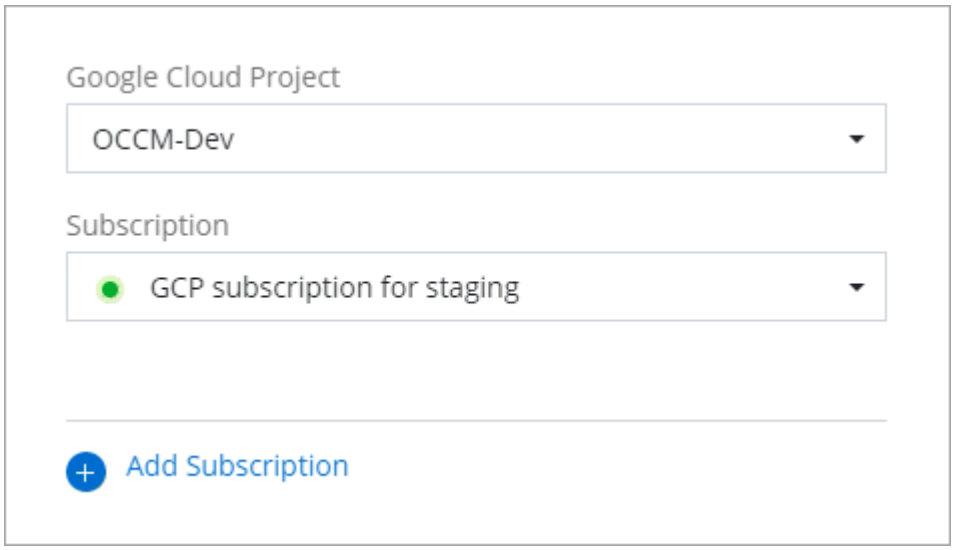
Google Cloud

Étapes

1. Sélectionnez **Administration > *Informations d'identification**.
2. Sélectionnez **Informations d'identification de l'organisation**.
3. Sélectionnez le menu d'action pour un ensemble d'informations d'identification associées à un agent de console, puis sélectionnez **Configurer l'abonnement**. + nouvelle capture d'écran nécessaire (TS)



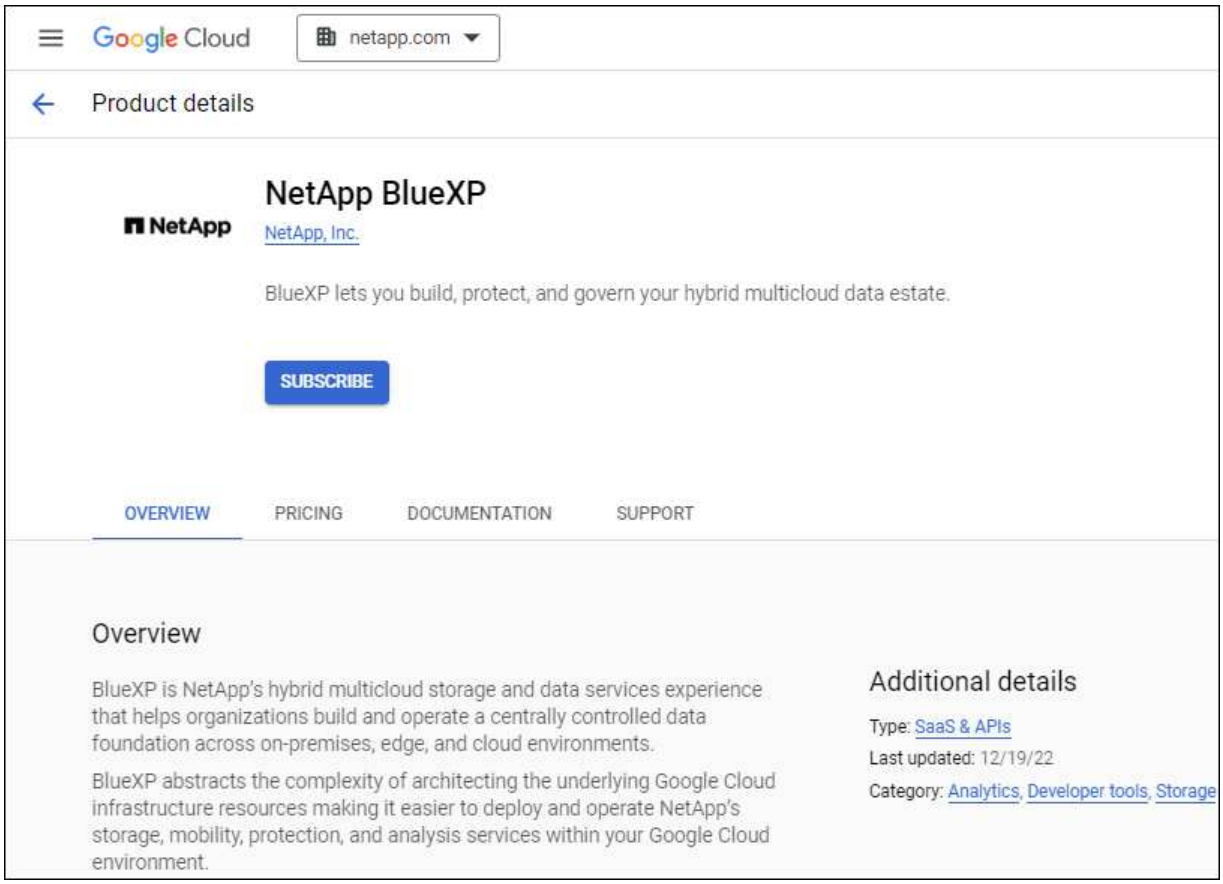
4. Pour configurer un abonnement existant avec les informations d'identification sélectionnées, sélectionnez un projet et un abonnement Google Cloud dans la liste déroulante, puis sélectionnez **Configurer**.



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

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

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

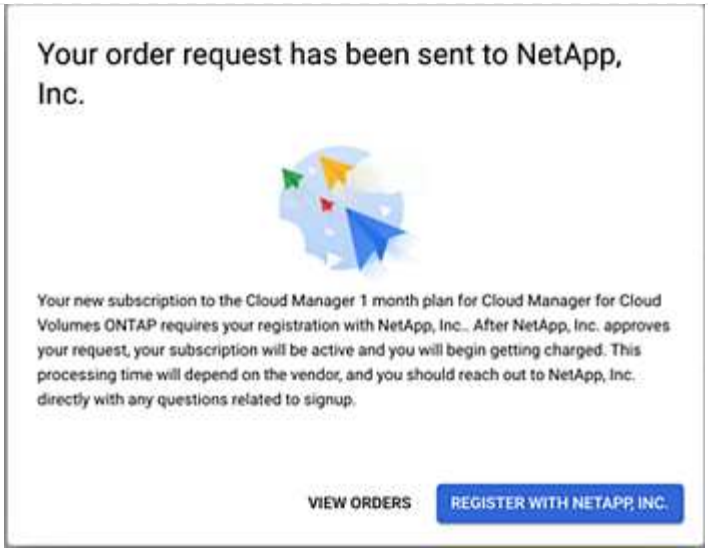


b. Sélectionnez **S'abonner**.
c. Sélectionnez le compte de facturation approprié et acceptez les conditions générales.
d. Sélectionnez **S'abonner**.

   Cette étape envoie votre demande de transfert à NetApp.

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

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



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

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

- 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.

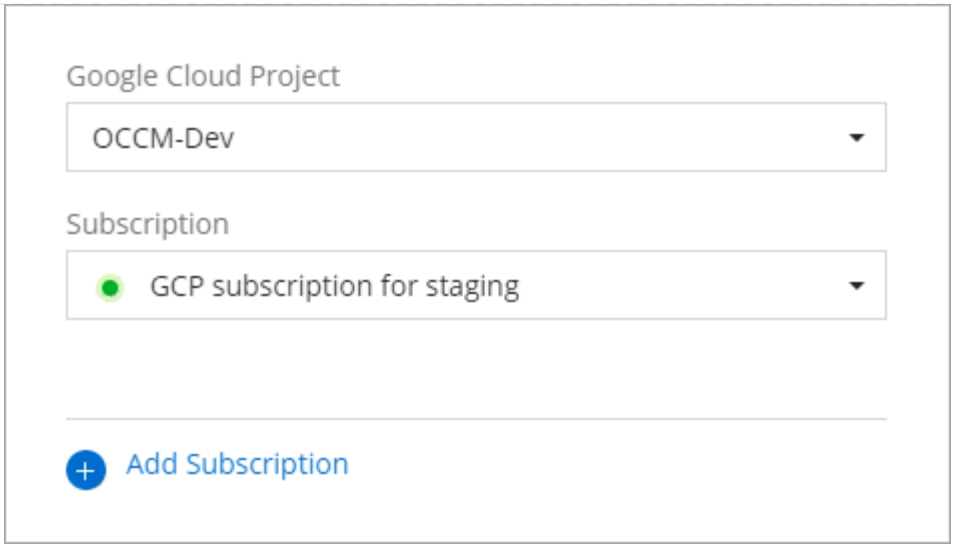
Pour toutes les autres organisations ou comptes, vous devrez associer manuellement l'abonnement en répétant ces étapes.

- Sélectionnez **Enregistrer**.

  La vidéo suivante montre les étapes à suivre pour s'abonner à partir de Google Cloud Marketplace :

Abonnez-vous à Google Cloud Marketplace

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



Informations connexes

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

Ce que vous pouvez faire ensuite (mode restreint)

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

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

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

Informations connexes

"Modes de déploiement de la console NetApp"

Démarrer avec l'interface héritée de BlueXP (mode privé)

Démarrage du flux de travail (mode privé BlueXP)

Le mode privé BlueXP (interface BlueXP héritée) est généralement utilisé avec des environnements locaux qui n'ont pas de connexion Internet et avec des régions cloud sécurisées, notamment AWS Secret Cloud, AWS Top Secret Cloud et Azure IL6. NetApp continue de prendre en charge ces environnements avec l'interface BlueXP héritée.

"Documentation PDF pour le mode privé BlueXP"

Fonctionnalités et services de données pris en charge avec le mode privé

Le tableau suivant peut vous aider à identifier rapidement quels services et fonctionnalités BlueXP sont pris en charge en mode privé.

Notez que certains services peuvent être pris en charge avec des limitations.

Domaine de produits	Service ou fonctionnalité BlueXP	Mode privé
Environnements de travail Cette partie du tableau répertorie la prise en charge de la gestion de l'environnement de travail à partir du canevas BlueXP . Il n'indique pas les destinations de sauvegarde prises en charge pour la BlueXP backup and recovery.	Amazon FSx pour ONTAP	Non
	Amazon S3	Non
	Azure Blob	Non
	Azure NetApp Files	Non
	Cloud Volumes ONTAP	Oui
	Google Cloud NetApp Volumes	Non
	Stockage Google Cloud	Non
	Clusters ONTAP sur site	Oui
	E-Series	Non
	StorageGRID	Non

Domaine de produits	Service ou fonctionnalité BlueXP	Mode privé
Services	Alertes	Non
	Sauvegarde et récupération	Ouihttps://docs.netapp.com/us-en/bluexp-backup-recovery/prev-ontap-protect-journey.html#support-for-sites-with-no-internet-connectivity["Afficher la liste des destinations de sauvegarde prises en charge pour les données de volume ONTAP"^]
	Classification	Oui
	Copier et synchroniser	Non
	Conseiller numérique	Non
	Portefeuille numérique	Oui
	Reprise après sinistre	Non
	Efficacité économique	Non
	Protection contre les ransomwares	Non
	Réplication	Oui
	Mises à jour logicielles	Non
	Durabilité	Non
	hiérarchisation	Non
	Mise en cache des volumes	Non
	Usine de charge de travail	Non
Caractéristiques	Gestion des identités et des accès	Oui
	Informations d'identification	Oui
	Fédération	Non
	Authentification multifacteur	Non
	Comptes NSS	Non
	Notifications	Non
	Recherche	Non
	Chronologie	Oui

Utiliser la console NetApp

Connectez-vous à la console NetApp

La manière dont vous vous connectez à la console NetApp dépend du mode de déploiement que vous utilisez.

Vous êtes automatiquement déconnecté après 24 heures ou si vous fermez votre navigateur.

"En savoir plus sur les modes de déploiement de la console" .

Mode standard

Après vous être inscrit à la console NetApp , vous pouvez vous connecter à partir de la console Web pour commencer à gérer vos données et votre infrastructure de stockage.

À propos de cette tâche

Vous pouvez vous connecter à la console NetApp en utilisant l'une des options suivantes :

- Vos informations d'identification du site de support NetApp (NSS) existantes
- Un compte NetApp Console utilisant votre adresse e-mail et un mot de passe
- Une connexion fédérée

  Vous pouvez utiliser l'authentification unique pour vous connecter à l'aide des informations d'identification de votre annuaire d'entreprise (identité fédérée). "Apprenez à configurer la fédération d'identité" .

Étapes

1. Ouvrez un navigateur Web et accédez à la "Console NetApp"
2. Sur la page **Connexion**, saisissez l'adresse e-mail associée à votre connexion.
3. Selon la méthode d'authentification associée à votre connexion, vous serez invité à saisir vos identifiants :
   - Identifiants cloud NetApp : saisissez votre mot de passe
   - Utilisateur fédéré : saisissez vos identifiants d'identité fédérée
   - Compte du site de support NetApp : saisissez vos identifiants de site de support NetApp

Résultat

Vous êtes maintenant connecté et pouvez commencer à l'utiliser pour gérer votre infrastructure multicloud hybride.

Mode restreint

Lorsque vous utilisez la console en mode restreint, vous devez vous connecter à la console à partir de l'interface utilisateur qui s'exécute localement sur l'agent.

À propos de cette tâche

La console prend en charge la connexion avec l'une des options suivantes en mode restreint :

- Une connexion à la console NetApp à l'aide de votre adresse e-mail et d'un mot de passe
- Une connexion fédérée

  Vous pouvez utiliser l'authentification unique pour vous connecter à l'aide des informations d'identification de votre annuaire d'entreprise (identité fédérée). "Apprenez à utiliser la fédération d'identité" .

Étapes

1. Ouvrez un navigateur Web et entrez l'adresse IP où l'agent est installé.
2. Entrez votre nom d'utilisateur et votre mot de passe pour vous connecter.

Afficher les métriques sur la page d'accueil de la console NetApp

La surveillance de l'état de votre parc de stockage garantit que vous êtes conscient des problèmes de protection du stockage et que vous pouvez prendre des mesures pour les résoudre. À l'aide de la page d'accueil de la console NetApp , affichez l'état de vos sauvegardes et restaurations à partir de NetApp Backup and Recovery et le nombre de charges de travail exposées à un risque d'attaque par ransomware ou protégées comme indiqué par NetApp Ransomware Resilience. Vous pouvez consulter la capacité de stockage des clusters individuels et Cloud Volumes ONTAP, les alertes ONTAP , la capacité de performances de stockage par cluster ou système Cloud Volumes ONTAP , les différents types de licences dont vous disposez, et bien plus encore.

Tous les volets de la page d'accueil affichent les données au niveau de l'organisation. Les volets Capacité de stockage et Performances de stockage affichent les systèmes associés aux projets auxquels l'utilisateur peut accéder en fonction des autorisations IAM.

Le système actualise les données de la page d'accueil toutes les cinq minutes. La mise en cache peut entraîner une différence entre les données de cette page et les valeurs réelles pendant 15 minutes maximum.

Des mesures précises sur la page d'accueil nécessitent des agents de console correctement dimensionnés et configurés.

Rôles de la console NetApp requis

Chaque volet de la page d'accueil nécessite des rôles d'utilisateur différents :

- **Volet Capacité de stockage** : Possibilité d'afficher la page Systèmes de la console NetApp
- * Volet d'alertes ONTAP * : administrateur de dossier ou de projet, analyste du support opérationnel, administrateur d'organisation, visualiseur d'organisation, super administrateur, super visualiseur
- **Volet Capacité de performances de stockage** : Possibilité d'afficher la page Systèmes de la console NetApp
- **Volet Licences et abonnements** : Administrateur de dossier ou de projet, Administrateur d'organisation, Visualiseur d'organisation, Super administrateur, Super visualiseur
- **Volet Résilience aux rançongiciels** : Administrateur de dossier ou de projet, Administrateur d'organisation, Administrateur de protection contre les rançongiciels, Visionneuse de protection contre les rançongiciels, Super administrateur, Super visionneuse
- **Volet Sauvegarde et récupération** : Administrateur de sauvegarde et de récupération, Super administrateur de sauvegarde et de récupération, Visionneuse de sauvegarde et de récupération, Administrateur de clone de sauvegarde et de récupération, Administrateur de dossier ou de projet, Administrateur d'organisation, Administrateur de restauration de sauvegarde et de récupération, Super administrateur, Super visionneuse

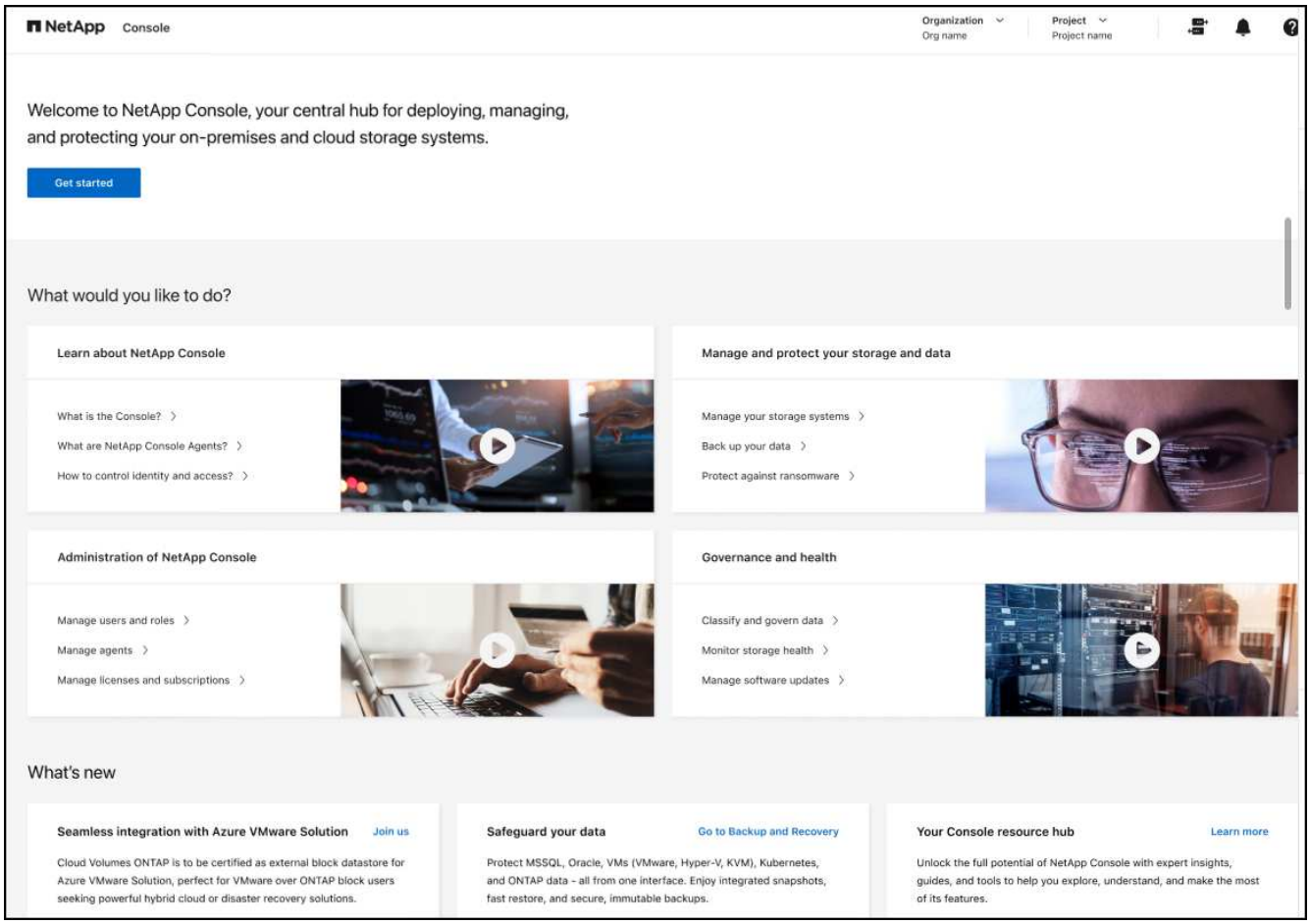
Si vous ne disposez pas des autorisations nécessaires pour accéder à un volet, celui-ci affiche un message indiquant que vous ne disposez pas des autorisations nécessaires pour l'utiliser.

"En savoir plus sur les rôles d'accès à la console NetApp ." .

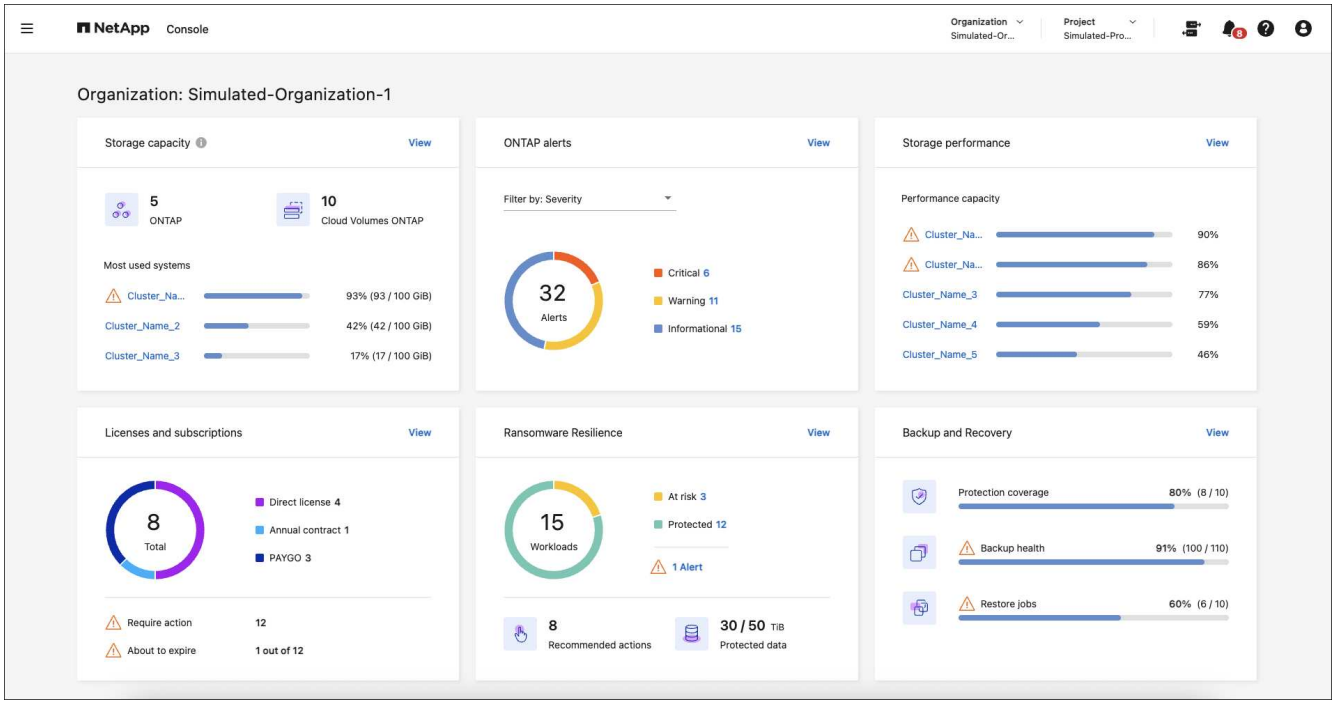
Étapes

1. Dans le menu de la console NetApp , sélectionnez **Accueil**.

   Si vous disposez du rôle d'administrateur d'organisation et qu'aucun agent ou système de stockage n'est configuré, la page d'accueil affiche les informations de démarrage.



   Si vous avez déjà configuré la console NetApp , qu'au moins un agent de console est activé et qu'au moins un cluster ou un système Cloud Volumes ONTAP a été ajouté sur cet agent, la page d'accueil affiche des mesures sur votre environnement de stockage.



Activer l’affichage des métriques sur la page d’accueil

Vous pouvez voir les métriques sur la page d’accueil lorsque les conditions suivantes sont remplies :

- Vous êtes connecté à une instance SaaS de la console NetApp .
- Vous appartenez à une organisation disposant de ressources de stockage existantes (agent et cluster ou système Cloud Volumes ONTAP).
- Au moins un agent de console est activé.
- Au moins un cluster ou un système Cloud Volumes ONTAP a été ajouté sur cet agent.

Pour permettre aux métriques d’apparaître sur la page d’accueil, effectuez les tâches suivantes :

- Activer au moins un agent de console.
- Ajoutez au moins un cluster ou un Cloud Volumes ONTAP à l’aide de cet agent.

Afficher la capacité de stockage globale

Le volet Capacité de stockage fournit les informations suivantes sur les clusters ONTAP et les systèmes Cloud Volumes ONTAP :

- Nombre de systèmes ONTAP découverts dans la console
- Nombre de systèmes Cloud Volumes ONTAP découverts dans la console
- Utilisation de la capacité par cluster

L’ordre des clusters ou des systèmes Cloud Volumes ONTAP est basé sur la quantité de capacité utilisée. Le cluster ou le système avec la capacité la plus élevée apparaît en premier pour une identification facile.

Les indicateurs d’avertissement s’affichent pour les clusters à 80 % de leur capacité, avec une mise à jour des données toutes les cinq minutes.

Si vous avez plusieurs projets, vous pouvez voir des données différentes dans le volet Capacité de stockage par rapport à la page Systèmes. Cela est dû au fait que la page Systèmes affiche des informations basées sur le niveau du projet, tandis que le volet Capacité de stockage affiche des informations au niveau de l'organisation. De plus, les données de ce volet peuvent différer des valeurs réelles pendant un maximum de 15 minutes, car les données sont mises en cache pendant cette durée afin d'optimiser les performances.

Étapes

1. Dans le menu de la console NetApp , examinez le volet Capacité de stockage.
2. Dans le volet Capacité de stockage, sélectionnez **Afficher** pour accéder à la page Systèmes de console.
3. Sur la page Systèmes, sélectionnez le projet contenant le cluster que vous souhaitez afficher.
4. Sur la page Systèmes, sélectionnez un cluster pour afficher plus de détails sur ce cluster.

Afficher les alertes ONTAP

Affichez les problèmes ou les risques potentiels dans vos environnements ONTAP sur site NetApp . Vous pouvez voir certaines alertes non EMS et certaines alertes EMS.

Les données sont mises à jour toutes les 5 minutes.

Vous pouvez voir les alertes ONTAP avec ces niveaux de gravité :

- Primordial
- Avertissement
- Informatif

Vous pouvez voir les alertes ONTAP pour ces zones d'impact :

- Capacité
- Performances
- Protection
- Disponibilité
- Sécurité

La mise en cache optimise les performances, mais peut entraîner une différence entre les données de ce volet et les valeurs réelles pendant 15 minutes maximum.

Systèmes pris en charge

- Un système NAS ou SAN ONTAP sur site est pris en charge.
- Les systèmes Cloud Volumes ONTAP ne sont pas pris en charge.

Sources de données prises en charge

Afficher les alertes concernant certains événements qui se produisent dans ONTAP. Il s'agit d'une combinaison d'alertes EMS et basées sur des métriques.

Pour plus de détails sur les alertes ONTAP , reportez-vous à "À propos des alertes ONTAP" .

Pour une liste des alertes que vous pourriez voir, reportez-vous à "Afficher les risques potentiels liés au stockage ONTAP" .

Étapes

1. Dans le menu de la console NetApp , examinez le volet Alertes ONTAP .
2. Vous pouvez également filtrer les alertes en sélectionnant le niveau de gravité ou modifier le filtre pour afficher les alertes en fonction de la zone d'impact.
3. Dans le volet Alertes ONTAP , sélectionnez **Afficher** pour accéder à la page Alertes de la console.

Afficher la capacité de performance de stockage

Examinez la capacité de performances de stockage utilisée par cluster ou système Cloud Volumes ONTAP pour déterminer l'impact de la capacité de performances, de la latence et des IOPS sur vos charges de travail. Par exemple, vous pourriez constater que vous devez déplacer les charges de travail pour minimiser la latence et maximiser les IOPS et le débit pour vos charges de travail critiques.

Le système organise les clusters et les systèmes par capacité de performance, en répertoriant d'abord la capacité la plus élevée pour une identification facile.

La mise en cache optimise les performances, mais peut entraîner une différence entre les données de ce volet et les valeurs réelles pendant 15 minutes maximum.

Étapes

1. Dans le menu de la console NetApp , examinez le volet Performances de stockage.
2. Dans le volet Performances de stockage, sélectionnez **Afficher** pour accéder à une page Performances qui répertorie tous les clusters et les données des systèmes Cloud Volumes ONTAP pour la capacité de performances, les IOPS et la latence.
3. Sélectionnez un cluster pour afficher ses détails dans le Gestionnaire système.

Afficher les licences et les abonnements dont vous disposez

Consultez les informations suivantes dans le volet Licences et abonnements :

- Le nombre total de licences et d'abonnements dont vous disposez.
- Le nombre de chaque type de licence et d'abonnement dont vous disposez (licence directe, contrat annuel ou PAYGO).
- Le nombre de licences et d'abonnements actifs, nécessitant une action ou approchant de l'expiration.
- Le système affiche des indicateurs à côté des types de licences qui nécessitent une action ou qui sont sur le point d'expirer.

Les données sont actualisées toutes les 5 minutes.

La mise en cache optimise les performances, mais peut entraîner une différence entre les données de ce volet et les valeurs réelles pendant 15 minutes maximum.

Étapes

1. Dans le menu de la console NetApp , examinez le volet Licences et abonnements.
2. Dans le volet Licences et abonnements, sélectionnez **Afficher** pour accéder à la page Licences et abonnements de la console.

Afficher l'état de résilience aux ransomwares

Découvrez si les charges de travail sont exposées à des attaques de ransomware ou protégées avec le service de données NetApp Ransomware Resilience. Vous pouvez consulter la quantité totale de données protégées, afficher le nombre d'actions recommandées et afficher le nombre d'alertes liées à la protection contre les ransomwares.

Les données sont actualisées toutes les 5 minutes et correspondent aux données affichées dans le tableau de bord de résilience NetApp Ransomware.

"En savoir plus sur la résilience aux ransomwares de NetApp" .

Étapes

1. Dans le menu de la console NetApp , examinez le volet Résilience aux ransomwares.
2. Effectuez l'une des opérations suivantes dans le volet Résilience aux ransomwares :
   - Sélectionnez **Afficher** pour accéder au tableau de bord de résilience NetApp Ransomware. Pour plus de détails, reportez-vous à "Surveiller l'état de la charge de travail à l'aide du tableau de bord de résilience NetApp Ransomware" .
   - Consultez les « Actions recommandées » dans le tableau de bord de résilience NetApp Ransomware. Pour plus de détails, reportez-vous à "Consultez les recommandations de protection sur le tableau de bord de résilience NetApp Ransomware" .
   - Sélectionnez le lien Alertes pour consulter les alertes sur la page Alertes de résilience NetApp Ransomware. Pour plus de détails, reportez-vous à "Gérez les alertes de ransomware détectées avec NetApp Ransomware Resilience" .

Afficher l'état de la sauvegarde et de la récupération

Consultez l'état général de vos sauvegardes et restaurations à partir de NetApp Backup and Recovery. Vous pouvez voir le nombre de ressources protégées et non protégées. Vous pouvez également voir le pourcentage de sauvegardes et d'opérations de restauration pour la protection de vos charges de travail. Un pourcentage plus élevé indique une meilleure protection des données.

Les données sont actualisées toutes les 5 minutes.

La mise en cache optimise les performances, mais peut entraîner une différence entre les données de ce volet et les valeurs réelles pendant 15 minutes maximum.

Étapes

1. Dans le menu de la console NetApp , examinez le volet Sauvegarde et récupération.
2. Sélectionnez **Afficher** pour accéder au tableau de bord de sauvegarde et de récupération NetApp . Pour plus de détails, reportez-vous à "Documentation sur la sauvegarde et la restauration NetApp" .

Gérez les paramètres utilisateur de votre console NetApp

Vous pouvez modifier votre profil de console, notamment changer votre mot de passe, activer l'authentification multifacteur (MFA) et voir qui est votre administrateur de console.

Dans la console, chaque utilisateur dispose d'un profil qui contient des informations sur l'utilisateur et ses paramètres. Vous pouvez afficher et modifier les paramètres de votre profil.

Changer votre nom d'affichage

Vous pouvez modifier le nom d'affichage de votre console qui est utilisé pour vous identifier et qui est visible par les autres utilisateurs. Votre nom d'affichage n'est pas le même que votre nom d'utilisateur ou votre adresse e-mail, qui ne peuvent pas être modifiés.

Étapes

1. Sélectionnez l'icône de profil dans le coin supérieur droit de la console pour afficher le panneau des paramètres utilisateur.
2. Sélectionnez l'icône **Modifier** à côté de votre nom.
3. Saisissez votre nouveau nom d'affichage dans le champ **Nom**.

Configurer l'authentification multifacteur

Configurez l'authentification multifacteur (MFA) pour améliorer la sécurité en exigeant une deuxième méthode de vérification.

Les utilisateurs qui utilisent l'authentification unique avec un fournisseur d'identité externe ou le site de support NetApp ne peuvent pas activer MFA. Si l'une de ces situations est vraie pour vous, vous ne verrez pas l'option permettant d'activer l'authentification multifacteur dans les paramètres de votre profil.

N'activez pas MFA si votre compte utilisateur est utilisé pour l'accès à l'API. L'authentification multifacteur arrête l'accès à l'API lorsqu'elle est activée pour un compte utilisateur. Utilisez des comptes de service pour tous les accès API.

Avant de commencer

- Vous devez déjà avoir téléchargé une application d'authentification, telle que Google Authenticator ou Microsoft Authenticator, sur votre appareil.
- Vous aurez besoin de votre mot de passe pour configurer MFA.

Si vous n'avez pas accès à votre application d'authentification ou si vous perdez votre code de récupération, contactez l'administrateur de votre console pour obtenir de l'aide.

Étapes

1. Sélectionnez l'icône de profil dans le coin supérieur droit de la console pour afficher le panneau des paramètres utilisateur.
2. Sélectionnez **Configurer** à côté de l'en-tête **Authentification multifacteur**.
3. Suivez les instructions pour configurer MFA pour votre compte.
4. Une fois l'opération terminée, vous serez invité à enregistrer votre code de récupération. Choisissez de copier le code ou de télécharger un fichier texte contenant le code. Conservez ce code dans un endroit sûr. Vous avez besoin du code de récupération si vous perdez l'accès à votre application d'authentification.

   Après avoir configuré l'authentification multifacteur, la console vous invite à saisir un code à usage unique depuis votre application d'authentification à chaque fois que vous vous connectez.

Régénérez votre code de récupération MFA

Vous ne pouvez utiliser les codes de récupération qu'une seule fois. Si vous utilisez ou perdez le vôtre, créez-en un nouveau.

Étapes

1. Sélectionnez l'icône de profil dans le coin supérieur droit de la console pour afficher le panneau des paramètres utilisateur.
2. Sélectionner ••• à côté de l'en-tête **Authentification multifacteur**.
3. Sélectionnez **Régénérer le code de récupération**.
4. Copiez le code de récupération généré et enregistrez-le dans un endroit sûr.

Supprimez votre configuration MFA

Pour arrêter d'utiliser l'authentification multifacteur (MFA) pour votre connexion, supprimez votre configuration MFA. Cela supprime la nécessité de saisir un code à usage unique depuis votre application d'authentification lorsque vous vous connectez.

Si vous ne parvenez pas à accéder à votre application d'authentification ou à votre code de récupération, vous devrez contacter l'administrateur de votre organisation pour réinitialiser votre configuration MFA.

Étapes

1. Sélectionnez l'icône de profil dans le coin supérieur droit de la console pour afficher le panneau des paramètres utilisateur.
2. Sélectionner ••• à côté de l'en-tête **Authentification multifacteur**.
3. Sélectionnez **Supprimer**.

Contactez l'administrateur de votre organisation

Si vous devez contacter l'administrateur de votre organisation, vous pouvez lui envoyer un e-mail directement depuis la console. L'administrateur gère les comptes utilisateurs et les autorisations au sein de votre organisation.

Vous devez disposer d'une application de messagerie par défaut configurée pour votre navigateur pour utiliser la fonctionnalité **Contacter les administrateurs**.

Étapes

1. Sélectionnez l'icône de profil dans le coin supérieur droit de la console pour afficher le panneau des paramètres utilisateur.
2. Sélectionnez **Contacter les administrateurs** pour envoyer un e-mail à l'administrateur de votre organisation.
3. Sélectionnez l'application de messagerie à utiliser.
4. Terminez l'e-mail et sélectionnez **Envoyer**.

Configurer le mode sombre (thème sombre)

Vous pouvez configurer la console pour qu'elle s'affiche en mode sombre.

Étapes

1. Sélectionnez l'icône de profil dans le coin supérieur droit de la console pour afficher le panneau des paramètres utilisateur.

2. Déplacez le curseur **Thème sombre** pour l’activer.

Administrer la console NetApp

Gestion des identités et des accès

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

La gestion des identités et des accès (IAM) dans la console NetApp vous permet d'organiser et de contrôler l'accès à vos ressources NetApp . Vous pouvez organiser vos ressources en fonction de la hiérarchie de votre organisation. Par exemple, vous pouvez organiser les ressources par emplacement géographique, site ou unité commerciale. Vous pouvez ensuite attribuer des rôles IAM aux membres de parties spécifiques de la hiérarchie, ce qui empêche l'accès aux ressources dans d'autres parties de la hiérarchie.

- "En savoir plus sur les modes de déploiement de la console"

Comment fonctionne IAM

IAM vous permet d'accorder l'accès aux ressources en attribuant aux utilisateurs des rôles d'accès à des parties spécifiques de la hiérarchie. Par exemple, un membre peut se voir attribuer le rôle d'administrateur de dossier ou de projet pour un projet comportant cinq ressources.

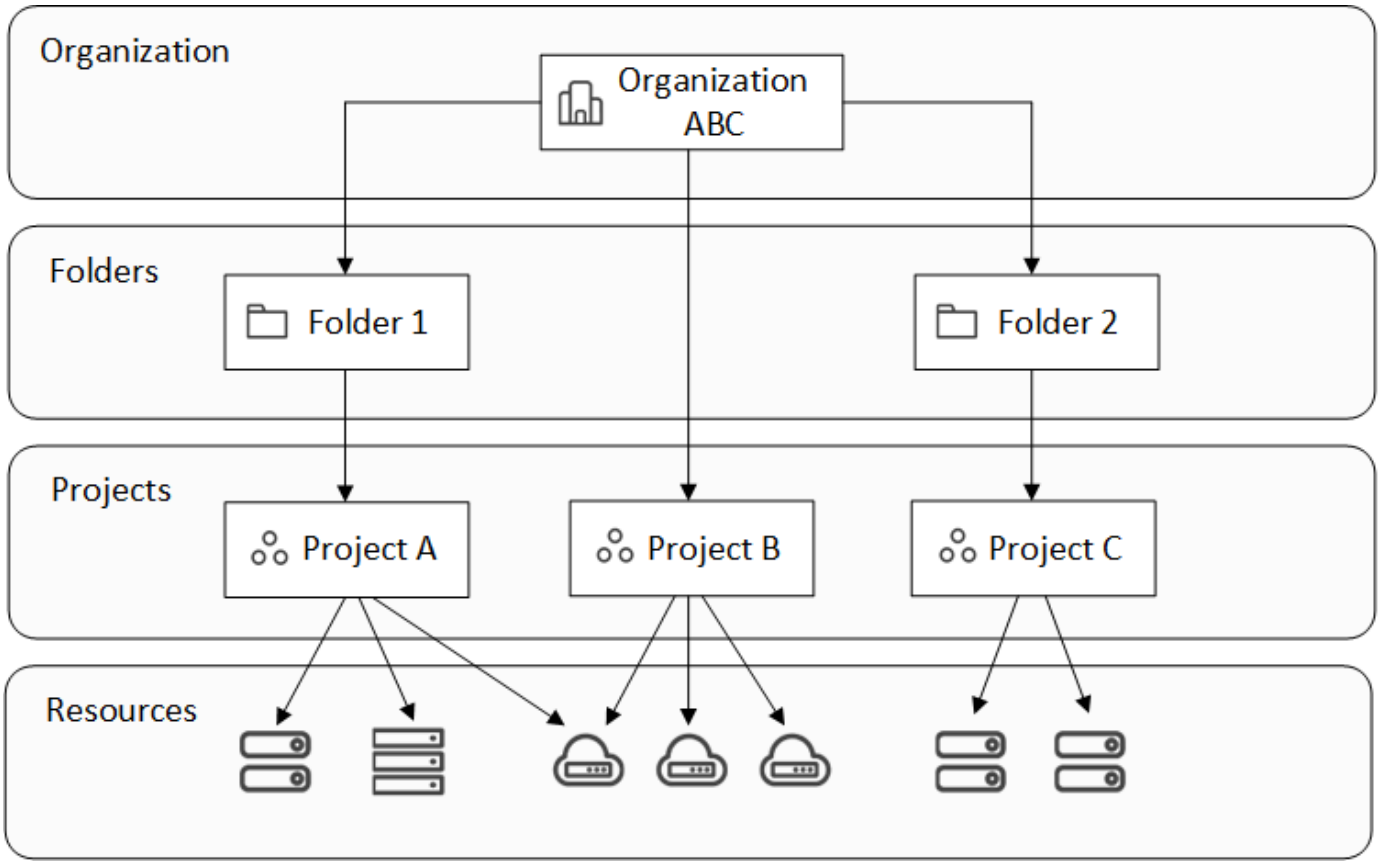
Lorsque vous utilisez IAM, vous gérez les composants suivants :

- L'organisation
- Dossiers
- Projets
- Ressources
- Membres
- Rôles et autorisations
- Agents de console

Les ressources sont organisées hiérarchiquement :

- L'organisation est le sommet de la hiérarchie.
- Les dossiers sont des enfants de l'organisation ou d'un autre dossier.
- Les projets sont des enfants de l'organisation ou d'un dossier.
- Les ressources sont associées à un ou plusieurs dossiers ou projets.

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



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.

Dossiers

Un *dossier* vous permet de regrouper des projets liés et de les séparer des autres projets de votre organisation. Par exemple, un dossier peut représenter un emplacement géographique (UE ou États-Unis Est), un site (Londres ou Toronto) ou une unité commerciale (ingénierie ou marketing).

Vous pouvez organiser des dossiers pour contenir des projets, d'autres dossiers ou les deux. Ils sont facultatifs.

Projets

Un *projet* représente un espace de travail dans la console auquel les membres de l'organisation accèdent à partir de la page **Systèmes** afin de gérer les ressources. Par exemple, un projet peut inclure un système Cloud Volumes ONTAP , un cluster ONTAP sur site ou un système de fichiers FSx pour ONTAP .

Une organisation peut avoir un ou plusieurs projets. Un projet peut résider directement sous l'organisation ou dans un dossier.

Ressources

Une *ressource* est un système que vous avez créé ou découvert dans la console.

Lorsque vous créez ou découvrez une ressource, la ressource est associée au projet actuellement

sélectionné. C'est peut-être le seul projet auquel vous souhaitez associer cette ressource. Mais vous pouvez choisir d'associer la ressource à des projets supplémentaires dans votre organisation.

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

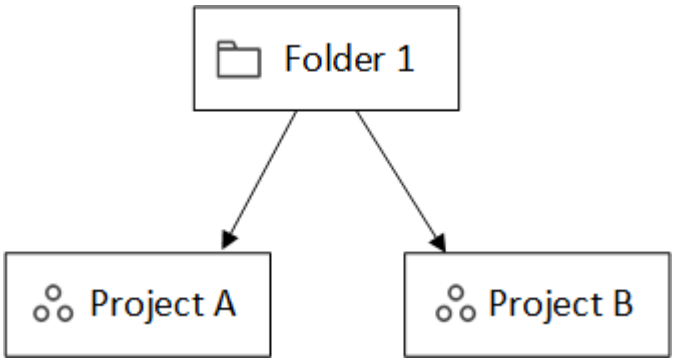
Les agents peuvent également être associés à plusieurs projets. En savoir plus sur l'utilisation des agents avec IAM .

Quand associer une ressource à un dossier

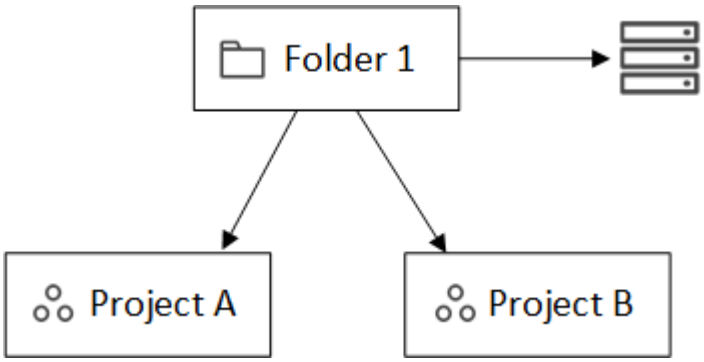
Vous avez également la possibilité d'associer une ressource à un dossier, mais cela est facultatif et répond aux besoins d'un cas d'utilisation spécifique.

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 :

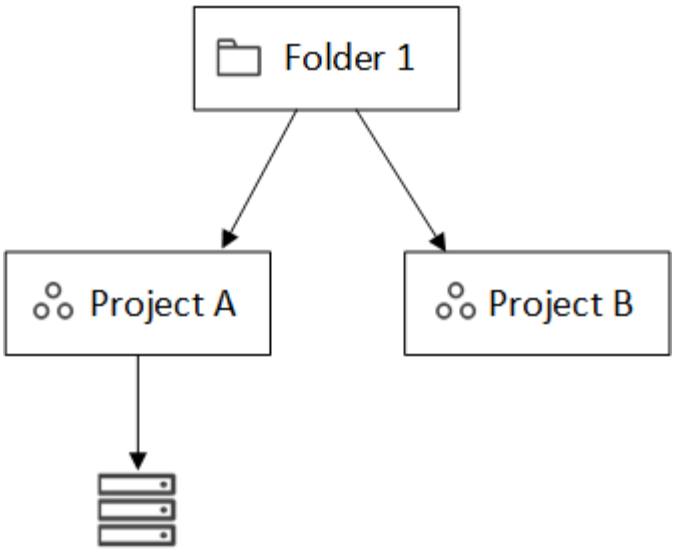


L'administrateur de l'organisation peut associer une ressource au dossier :



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.

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.

Chaque organisation comprend au moins un utilisateur avec le rôle *Administrateur de l'organisation* (la console attribue automatiquement ce rôle à l'utilisateur qui crée l'organisation). Vous pouvez ajouter d'autres membres à l'organisation et attribuer différentes autorisations à différents niveaux de la hiérarchie des ressources.

Rôles et autorisations

Vous n'accordez pas d'autorisations directement aux membres de l'organisation. Au lieu de cela, vous attribuez à chaque membre un rôle. Un rôle contient un ensemble d'autorisations qui permet à un membre d'effectuer des actions spécifiques à un niveau spécifique de la hiérarchie des ressources.

L'octroi de rôles au niveau hiérarchique restreint l'accès aux ressources et aux services dont un membre a besoin.

Où vous pouvez attribuer des rôles dans la hiérarchie

Lorsque vous associez un membre à un rôle, vous devez sélectionner l'organisation entière, un dossier spécifique ou un projet spécifique. Le rôle que vous sélectionnez donne à un membre des autorisations sur les ressources de la partie sélectionnée de la hiérarchie.

Héritage des rôles

Lorsque vous attribuez un rôle, celui-ci est hérité dans la hiérarchie de l'organisation :

Organisation
: Accorder à un membre un rôle d'accès au niveau de l'organisation lui donne des autorisations sur tous les dossiers, projets et ressources.

Dossiers
: Lorsque vous accordez un rôle d'accès au niveau du dossier, tous les dossiers, projets et ressources du

dossier héritent de ce rôle.

Par exemple, si vous attribuez un rôle au niveau du dossier et que ce dossier contient trois projets, le membre disposera d'autorisations sur ces trois projets et toutes les ressources associées.

Projets

Lorsque vous accordez un rôle d'accès au niveau du projet, toutes les ressources associées à ce projet héritent de ce rôle.

Rôles multiples

Vous pouvez attribuer à chaque membre de l'organisation un rôle à différents niveaux de la hiérarchie de l'organisation. Il peut s'agir du même rôle ou d'un rôle différent. Par exemple, vous pouvez attribuer un rôle de membre A au projet 1 et au projet 2. Ou vous pouvez attribuer un rôle de membre A pour le projet 1 et un rôle B pour le projet 2.

Rôles d'accès

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

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

Agents de console

Lorsqu'un *administrateur d'organisation* crée un agent de console, la console associe automatiquement cet agent à l'organisation et au projet actuellement sélectionné. L'administrateur de l'organisation a automatiquement accès à cet agent depuis n'importe quel endroit de l'organisation. Mais si vous avez d'autres membres dans votre organisation avec des rôles différents, ces membres ne peuvent accéder à cet agent qu'à partir du projet dans lequel il a été créé, sauf si vous associez cet agent à d'autres projets.

Vous rendez un agent de console disponible pour un autre projet dans ces cas :

- Vous souhaitez autoriser les membres de votre organisation à utiliser un agent existant pour créer ou découvrir des systèmes supplémentaires dans un autre projet
- Vous avez associé une ressource existante à un autre projet et cette ressource est gérée par un agent de console

  Si une ressource que vous associez à un projet supplémentaire est découverte à l'aide d'un agent de console, vous devez également associer l'agent au projet auquel la ressource est désormais associée. Sinon, l'agent et sa ressource associée ne sont pas accessibles depuis la page **Systèmes** par les membres qui n'ont pas le rôle *Administrateur de l'organisation*.

Vous pouvez créer une association à partir de la page **Agents** dans la console IAM :

- Associer un agent de console à un projet

  Lorsque vous associez un agent de console à un projet, cet agent est accessible depuis la page **Systèmes** lors de l'affichage du projet.

- Associer un agent de console à un dossier

  L'association d'un agent de console à un dossier ne rend pas automatiquement cet agent accessible à partir de tous les projets du dossier. Les membres de l'organisation ne peuvent pas accéder à un agent de console à partir d'un projet tant que vous n'avez pas associé l'agent à ce projet spécifique.

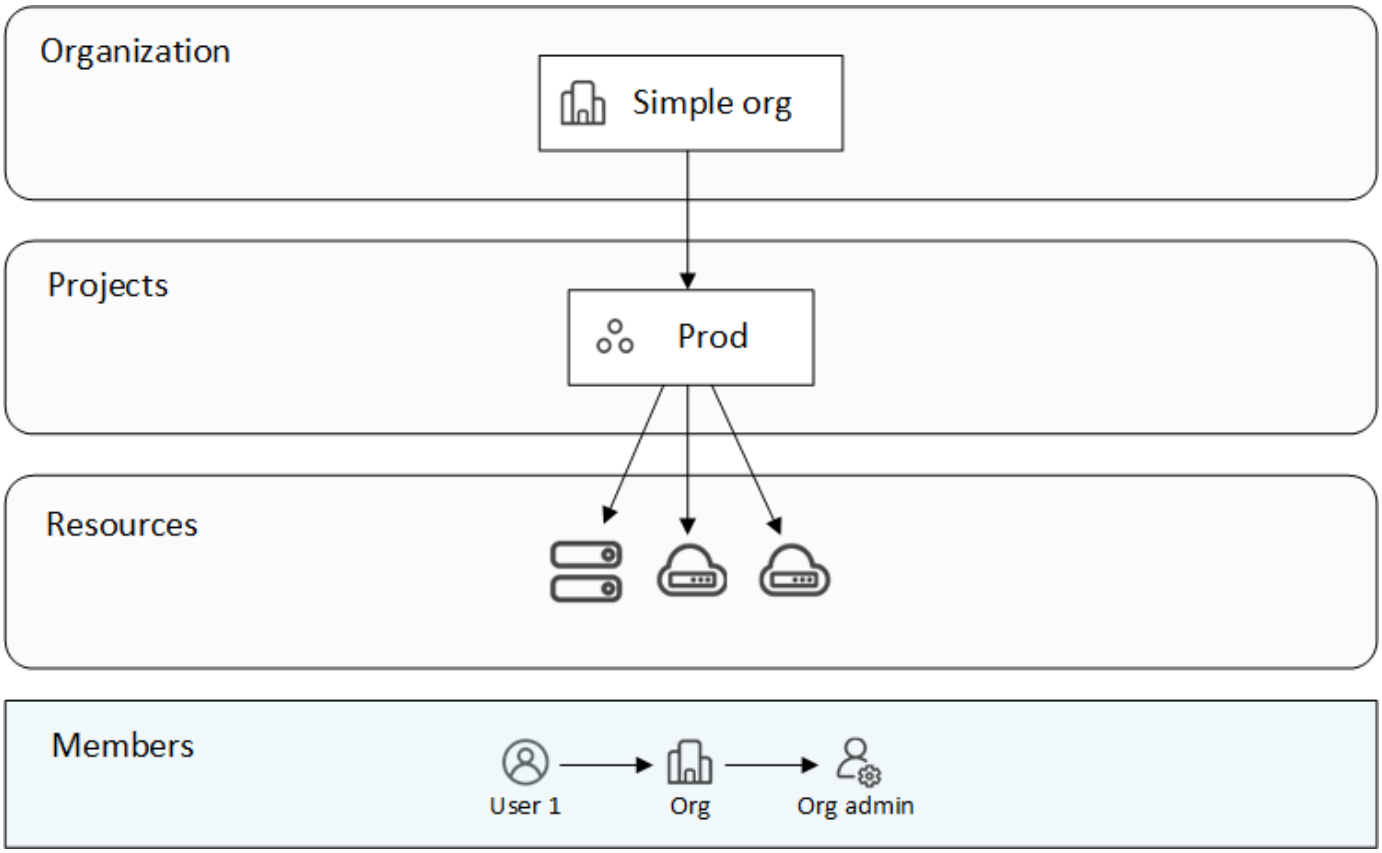
Un *administrateur d'organisation* peut associer un agent de console à un dossier afin que l'*administrateur de dossier ou de projet* puisse prendre la décision d'associer cet agent aux projets appropriés qui résident dans le dossier.

Exemples d'IAM

Ces exemples montrent comment vous pourriez mettre en place votre organisation.

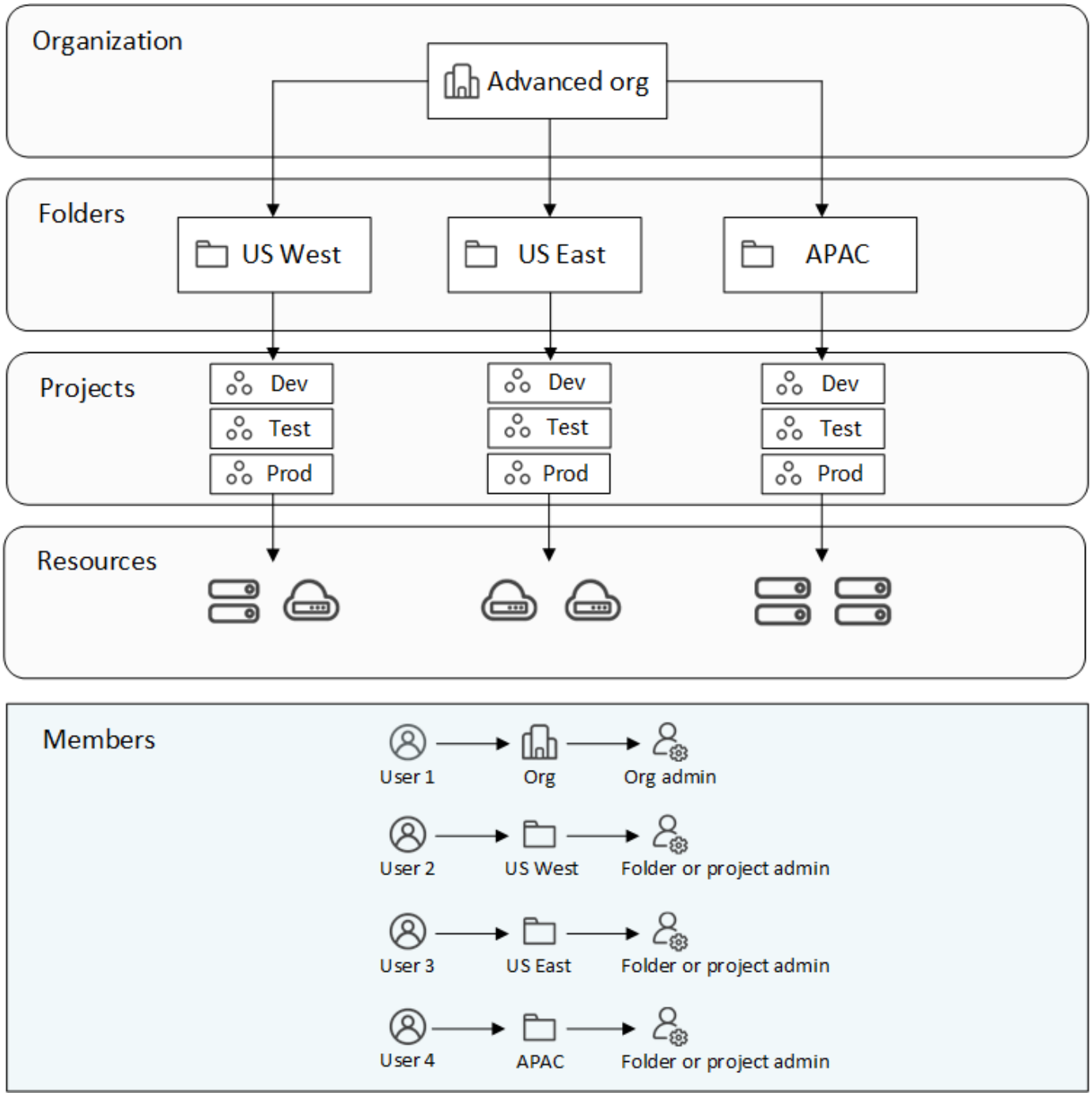
Organisation simple

Le diagramme suivant montre un exemple simple d'une organisation qui utilise le projet par défaut et aucun dossier. Un seul membre gère l'ensemble de l'organisation.



Organisation avancée

Le diagramme suivant montre une organisation qui utilise des dossiers pour organiser les projets pour chaque emplacement géographique de l'entreprise. Chaque projet dispose de son propre ensemble de ressources associées. Les membres comprennent un administrateur d'organisation et un administrateur pour chaque dossier de l'organisation.



Ce que vous pouvez faire avec IAM

Les exemples suivants décrivent comment vous pouvez utiliser IAM pour gérer votre organisation de console :

- Accordez des rôles spécifiques à des membres spécifiques afin qu'ils puissent uniquement effectuer les tâches requises.
- Modifier les autorisations des membres parce qu'ils ont changé de service ou parce qu'ils ont des responsabilités supplémentaires.
- Supprimer un utilisateur qui a quitté l'entreprise.
- Ajoutez des dossiers ou des projets à votre hiérarchie car une nouvelle unité commerciale a ajouté du stockage NetApp .

- Associez une ressource à un autre projet car cette ressource a une capacité qu'une autre équipe peut utiliser.
- Consultez les ressources auxquelles un membre peut accéder.
- Afficher les membres et les ressources associés à un projet spécifique.

Où aller ensuite

- "Démarrer avec IAM dans la console NetApp"
- "Organisez vos ressources dans la console NetApp avec des dossiers et des projets"
- "Gérer les membres de la console NetApp et leurs autorisations"
- "Gérer la hiérarchie des ressources dans votre organisation NetApp Console"
- "Associer des agents à des dossiers et des projets"
- "Basculer entre les projets et les organisations de la console NetApp"
- "Renommez votre organisation NetApp Console"
- "Surveiller ou auditer l'activité IAM"
- "Rôles d'accès à la console NetApp"
- "En savoir plus sur l'API pour NetApp Console IAM"

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

Lorsque vous vous inscrivez à la console NetApp , 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 devez disposer des autorisations **Administrateur d'organisation** pour administrer l'identité et l'accès de l'ensemble de votre organisation. Si vous disposez des autorisations **Administrateur de dossier ou de projet**, vous ne pouvez administrer que les dossiers et les projets pour lesquels vous disposez des autorisations.

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

Liez les comptes utilisateurs à votre organisation et attribuez des autorisations. 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 à partir 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 console NetApp"
- "En savoir plus sur l'API pour l'identité et l'accès"

Organisez vos ressources de la console NetApp avec des dossiers et des projets

Dans la console NetApp , vous organisez vos ressources NetApp à l'aide de projets et de dossiers. Un *projet* représente un espace de travail dans la console auquel les membres de l'organisation accèdent pour gérer les *ressources* (par exemple, un système Cloud Volumes ONTAP). Un *dossier* regroupe des projets liés. Après avoir organisé vos ressources en dossiers et projets, vous pouvez accorder un accès granulaire aux ressources en fournissant aux membres de l'organisation des autorisations sur des dossiers et des projets spécifiques.

Ajouter un dossier ou un projet

Lorsque vous créez votre organisation, elle comprend un seul projet. Ajoutez des projets pour gérer les ressources et des dossiers pour regrouper les projets associés.

La hiérarchie des ressources de votre organisation peut comporter jusqu'à sept niveaux, avec des dossiers imbriqués sur six niveaux de profondeur et des projets au septième.

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. Fournissez des détails sur le dossier ou le projet :

   - **Nom et emplacement** : saisissez un nom et choisissez un emplacement dans la hiérarchie pour le dossier ou le projet. Un dossier ou un projet peut être directement sous l'organisation ou à l'intérieur d'un dossier.
   - **Ressources** : Sélectionnez les ressources que vous souhaitez associer à ce dossier ou projet.

     Vous pouvez sélectionner des ressources associées au dossier parent ou au projet.

     "Apprenez quand associer une ressource à un dossier" .

   - **Accès** : Affichez les membres qui auront accès au dossier ou au projet en fonction des autorisations existantes déjà définies dans votre hiérarchie de ressources.

     Sélectionnez **Ajouter un membre** pour attribuer l'accès et un rôle à des membres supplémentaires. Un rôle définit les autorisations dont disposent les membres pour le dossier ou le projet.

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

6. Sélectionnez **Ajouter**.

Renommer un dossier ou un projet

Si nécessaire, vous pouvez modifier le nom de vos dossiers et projets.

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.

Avant de commencer

- Assurez-vous que le dossier ou le projet n'a aucune ressource associée. Apprenez à dissocier les ressources .
- Assurez-vous que le dossier ou le projet n'a aucune ressource associée.

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.

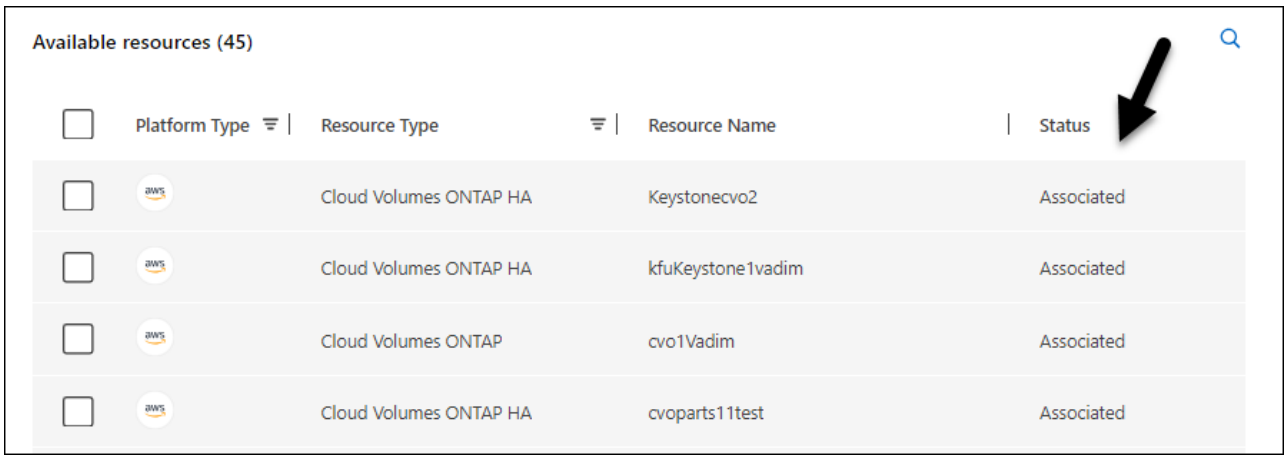
Afficher les ressources associées à un dossier ou à un projet

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

Les membres disposant d'autorisations pour un dossier ou un projet peuvent accéder à ses ressources associées.

Avant de commencer

"Apprenez quand associer une ressource à un dossier" .

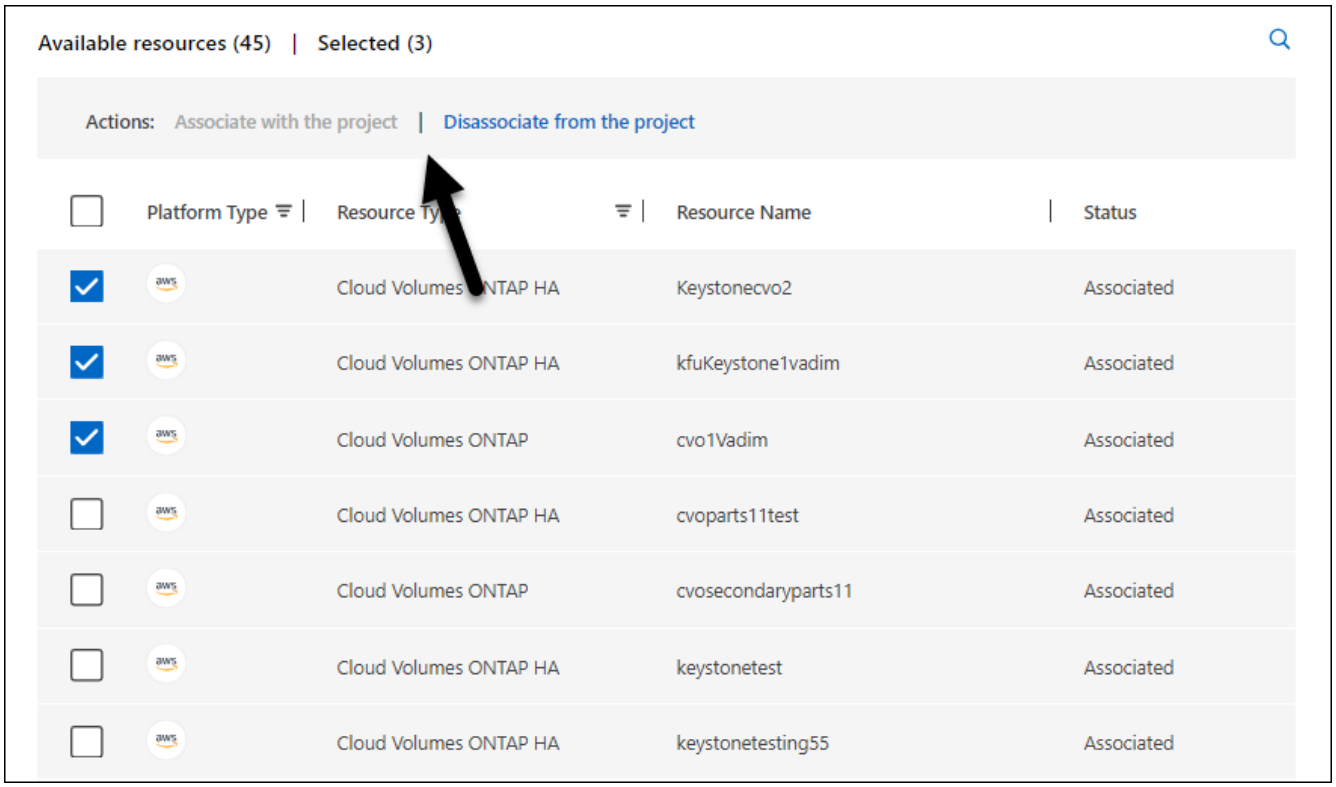
Étapes

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.

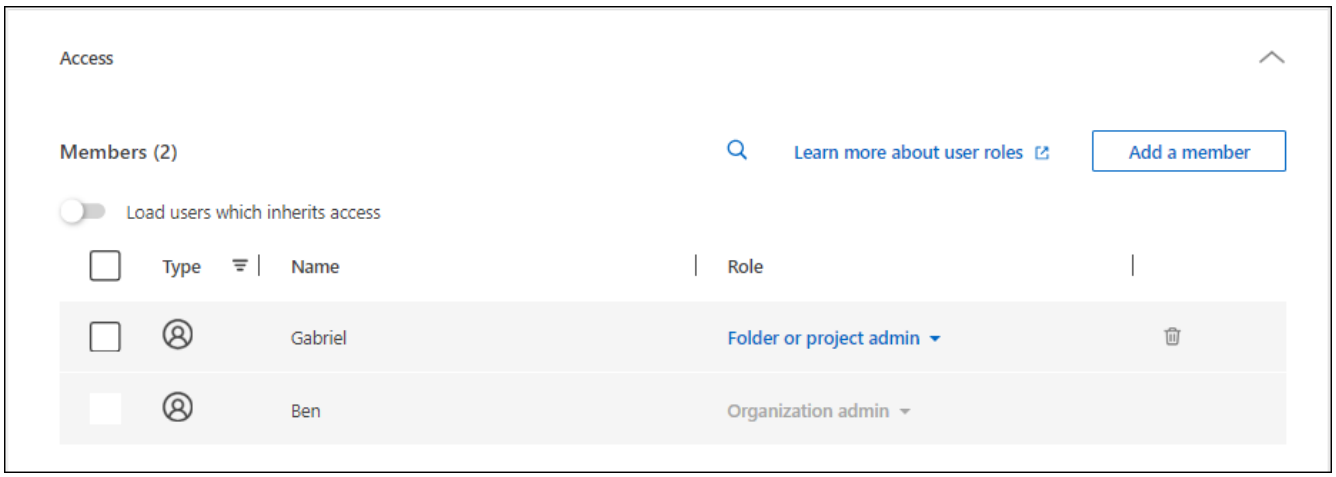
4. En fonction des ressources que vous avez sélectionnées, sélectionnez **Associer au projet** ou **Dissocier du projet**.



5. Sélectionnez **Appliquer**

Afficher les membres associés à un dossier ou à un projet

- 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

Modifiez l'accès des membres pour garantir que les bons membres peuvent accéder aux ressources associées.

L'accès des membres fourni à un niveau hiérarchique supérieur ne peut pas être modifié à des niveaux inférieurs. Mettez à jour les autorisations des membres au niveau hiérarchique supérieur pour modifier l'accès.

Alternativement, vous pouvez"gérer les autorisations depuis la page Membres" .

"En savoir plus sur l'héritage des rôles" .

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 console NetApp"
- "Démarrer avec l'identité et l'accès"
- "En savoir plus sur l'API d'identité et d'accès"

Ajouter des membres et des comptes de service à la console NetApp

Dans la console, vous pouvez ajouter des utilisateurs et des comptes de service à votre organisation et leur attribuer un ou plusieurs rôles dans votre hiérarchie de ressources. Un *rôle* contient un ensemble d'autorisations qui permet à un membre (utilisateur ou compte de service) d'effectuer des actions spécifiques à un niveau spécifique de la hiérarchie des ressources.

Vous avez besoin de l'un des rôles suivants pour gérer les utilisateurs et les autorisations :

- Administrateur de l'organisation

  Les utilisateurs avec ce rôle peuvent gérer tous les membres

- Administrateur de dossier ou de projet

  Les utilisateurs disposant de ce rôle peuvent gérer uniquement les membres d'un dossier ou d'un projet désigné

  L'administrateur du dossier ou du projet peut afficher tous les membres sur la page **Membres** mais gérer les autorisations uniquement pour les dossiers et les projets auxquels il a accès. "En savoir plus sur les actions qu'un *administrateur de dossier ou de projet* peut effectuer" .

Ajoutez des membres à votre organisation

Vous pouvez ajouter deux types de membres à votre organisation : un compte utilisateur et un compte de service. Les applications utilisent des comptes de service pour effectuer des tâches API sans intervention humaine. Une personne utilise généralement un compte utilisateur pour se connecter et gérer les ressources.

Les utilisateurs doivent s'inscrire à la console NetApp avant de pouvoir les ajouter à une organisation ou leur attribuer un rôle. Vous créez des comptes de service directement depuis la console.

Pour gérer les utilisateurs et leurs autorisations, vous devez disposer du rôle **Administrateur de l'organisation** ou du rôle **Administrateur de dossier ou de projet**. N'oubliez pas que les utilisateurs disposant du rôle **Administrateur de dossier ou de projet** ne peuvent gérer que les membres du dossier ou des projets pour lesquels ils disposent des autorisations d'administrateur.

Ajouter un compte utilisateur

Bien que les utilisateurs s'inscrivent eux-mêmes à la console NetApp , ils doivent être explicitement ajoutés à une organisation ou à des dossiers ou projets spécifiques pour accéder aux ressources de la console.

Étapes

1. Diriger l'utilisateur vers la visite "Console NetApp" pour s'inscrire.

   Une fois que les utilisateurs se sont inscrits, ils remplissent la page **Inscription**, vérifient leur courrier électronique et se connectent. Si la console invite les utilisateurs à créer une organisation, ils la ferment et vous informent de la création de leur compte. Vous pouvez ensuite ajouter l'utilisateur à votre organisation existante.

   "Découvrez comment vous inscrire à la console NetApp" .

2. Sélectionnez **Administration > Identité et accès**.
3. Sélectionnez **Membres**.
4. Sélectionnez **Ajouter un membre**.
5. Pour **Type de membre**, gardez **Utilisateur** sélectionné.
6. Pour **E-mail de l'utilisateur**, saisissez l'adresse e-mail de l'utilisateur associée à la connexion qu'il a créée.
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 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" .

9. Facultatif : sélectionnez un rôle ou un projet supplémentaire. Si vous souhaitez fournir l'accès à des

dossiers ou projets supplémentaires au sein de votre organisation ou accorder à l'utilisateur des rôles supplémentaires dans la zone sélectionnée, sélectionnez **Ajouter un rôle**, spécifiez un autre dossier ou projet ou une catégorie de rôle différente, puis choisissez un rôle.

10. Sélectionnez **Ajouter**.

    La console envoie à l'utilisateur un e-mail avec des instructions.

Ajouter un compte de service

Vous pouvez automatiser les tâches et intégrer les API de la console en toute sécurité avec les comptes de service. Lorsque vous créez un compte de service, choisissez entre deux méthodes d'authentification : à l'aide d'un ID client et d'un secret, ou à l'aide de l'authentification JWT (JSON Web Token). L'ID client et la méthode secrète conviennent aux configurations simples, tandis que l'authentification JWT offre une sécurité renforcée pour les environnements automatisés ou natifs du cloud. Choisissez l'option qui correspond le mieux à vos besoins de sécurité et à la manière dont vous prévoyez d'utiliser la console.

Si vous souhaitez utiliser 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. Si vous souhaitez utiliser l'authentification JWT, sélectionnez **Utiliser l'authentification JWT par clé privée** et téléchargez votre clé RSA publique ou votre certificat. Ignorez cette étape si vous souhaitez utiliser un identifiant client et un secret à la place.

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

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 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" .

9. Facultatif : sélectionnez un rôle ou un projet supplémentaire. Si vous souhaitez fournir l'accès à des dossiers ou projets supplémentaires au sein de votre organisation ou accorder à l'utilisateur des rôles supplémentaires dans la zone sélectionnée, sélectionnez **Ajouter un rôle**, spécifiez un autre dossier ou projet ou une catégorie de rôle différente, puis choisissez 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 affiche le secret du client une seule fois. Copiez-le en toute sécurité ; vous pourrez le recréer plus tard si nécessaire.

11. Si vous avez choisi l'authentification JWT, téléchargez ou copiez l'ID client et l'audience JWT. Ces informations ne sont affichées qu'une seule fois et ne peuvent pas être récupérées ultérieurement.
12. Sélectionnez **Fermer**.

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."

Vous pouvez afficher les comptes d'utilisateurs et les comptes de service à partir de la page **Membres**.

Vous pouvez également afficher tous les membres associés à un dossier ou à un projet spécifique. "Apprendre encore plus" .

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**.

Supprimer un membre de votre organisation

Vous devrez peut-être supprimer un membre de votre organisation, par exemple s'il quitte votre entreprise.

Le système supprime les autorisations du membre mais conserve ses comptes de console et de site de support NetApp .

Étapes

1. Depuis la page **Membres**, accédez à un membre dans le tableau, sélectionnez••• puis sélectionnez **Supprimer l'utilisateur**.
2. Confirmez que vous souhaitez supprimer le membre de votre organisation.

Recréer les informations d'identification pour un compte de service

Créez de nouvelles informations d'identification si vous les perdez ou si vous devez les mettre à jour.

Lorsque vous recréez les informations d'identification, vous supprimez les informations d'identification existantes pour le compte de service et en créez de nouvelles. Vous ne pouvez pas utiliser les informations d'identification précédentes.

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. + Le secret client ne s'affiche qu'une seule fois. Copiez-le ou téléchargez-le et stockez-le en toute sécurité.

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.

Les utilisateurs doivent reconfigurer MFA lors de la connexion après la suppression. Si l'utilisateur n'a perdu l'accès à son appareil MFA que temporairement, il peut utiliser le code de récupération qu'il a enregistré lors de la configuration de MFA 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.

Utiliser des rôles pour gérer l'accès des utilisateurs aux ressources de la console NetApp

Dans la console, vous pouvez attribuer des rôles aux utilisateurs en fonction de ce qu'ils doivent faire et où.

Les utilisateurs disposant du rôle **Administrateur d'organisation** ou **Administrateur de dossier ou de projet** ont la responsabilité d'attribuer des rôles à d'autres utilisateurs. Vous pouvez attribuer des rôles d'accès sur la base d'un projet ou d'un dossier. Par exemple, vous pouvez attribuer à un utilisateur le rôle d'administrateur de protection contre les ransomwares pour un projet et le rôle d'administrateur SnapCenter pour un autre projet. Alternativement, si un utilisateur a besoin du rôle d'administrateur de classification pour tous les projets d'un dossier spécifique, vous pouvez lui attribuer ce rôle au niveau du dossier.

Utilisez des rôles d'accès pour attribuer l'accès aux ressources de stockage en fonction des tâches spécifiques que les utilisateurs doivent effectuer. Par exemple, si un utilisateur doit interagir avec les services de protection contre les ransomwares, il doit disposer d'un rôle d'accès qui inclut des autorisations d'affichage ou d'administration pour le service de protection contre les ransomwares pour le projet pour lequel le rôle d'accès est accordé.

Attribuez des rôles aux utilisateurs en fonction de votre stratégie IAM pour une sécurité renforcée. Les rôles IAM garantissent que les utilisateurs disposent uniquement de l'accès dont ils ont besoin.

N'oubliez pas que vous ne pouvez pas accorder directement l'accès aux ressources. Affectez d'abord les ressources aux projets. Pensez à configurer votre hiérarchie de ressources avant d'attribuer l'accès aux utilisateurs."Apprenez à organiser vos ressources avec des dossiers et des projets."

Afficher les rôles attribués à un membre

Lorsque vous ajoutez un membre à votre organisation, vous êtes invité à lui attribuer un rôle. Vous pouvez permettre aux membres de 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**.

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 avoir plusieurs rôles au sein du 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 demander aux utilisateurs d'effectuer des tâches plus spécialisées. Vous pouvez également attribuer à un utilisateur le rôle d'administrateur de protection contre les ransomwares pour une organisation. Dans cet exemple, l'utilisateur serait en mesure d'effectuer des tâches de protection contre les ransomwares sur tous les projets au sein de votre organisation.

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

Un membre auquel est attribué le rôle d'administrateur d'organisation ne peut pas se voir attribuer de rôles supplémentaires. Ils disposent déjà d'autorisations sur l'ensemble de l'organisation. Un membre doté du rôle Dossier ou Projet ne peut se voir attribuer aucun autre rôle dans le dossier ou le projet où il possède déjà ce rôle. Ces deux rôles donnent accès à tous les services dans le cadre qui leur est attribué.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez le menu actions••• à côté du membre auquel vous souhaitez attribuer un rôle et sélectionnez **Ajouter un rôle**.
3. 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.

4. Sélectionnez **Ajouter de nouveaux rôles**.

Modifier le rôle attribué à un membre

Vous pouvez modifier les rôles attribués à un membre si vous devez ajuster l'accès d'un utilisateur.

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. Depuis la page **Membres**, accédez à un membre dans le tableau, sélectionnez ••• puis sélectionnez **Afficher les détails**.
3. 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.
4. 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 annuler l'attribution du rôle d'un membre, sélectionnez 🗑 à côté du rôle pour désattribuer le rôle respectif au membre. Il vous sera demandé de confirmer la suppression.

Gérer la hiérarchie des ressources dans votre organisation NetApp Console

Lorsque vous associez un membre à votre organisation, vous fournissez des autorisations au niveau de l'organisation, du dossier ou du projet. Pour garantir que ces membres disposent des autorisations nécessaires pour accéder aux bonnes ressources, vous devez gérer la hiérarchie des ressources de votre organisation en associant les ressources à des projets et des dossiers spécifiques. Une *ressource* est un système de stockage ou un agent de console que la console gère déjà ou dont elle a connaissance.

Consultez les ressources de votre organisation

Vous pouvez afficher les ressources découvertes et non découvertes associées à votre organisation. Les ressources non découvertes sont des ressources de stockage identifiées mais pas encore ajoutées à la console.

REMARQUE : la page Ressources exclut les ressources Amazon FSx for NetApp ONTAP, car les utilisateurs ne peuvent pas les associer à un rôle. Affichez-les sur la page Systèmes ou depuis Charges de travail.

Étapes

1. Sélectionnez **Administration > Identité et accès**.
2. Sélectionnez **Ressources**.
3. Sélectionnez **Recherche avancée et filtrage**.
4. Utilisez l'une des options disponibles pour trouver la ressource que vous recherchez :
   - **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 disponible.

Avant de commencer

Vous devez comprendre comment fonctionne l'association de ressources. "En savoir plus sur les ressources, notamment quand associer une ressource à un dossier" .

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

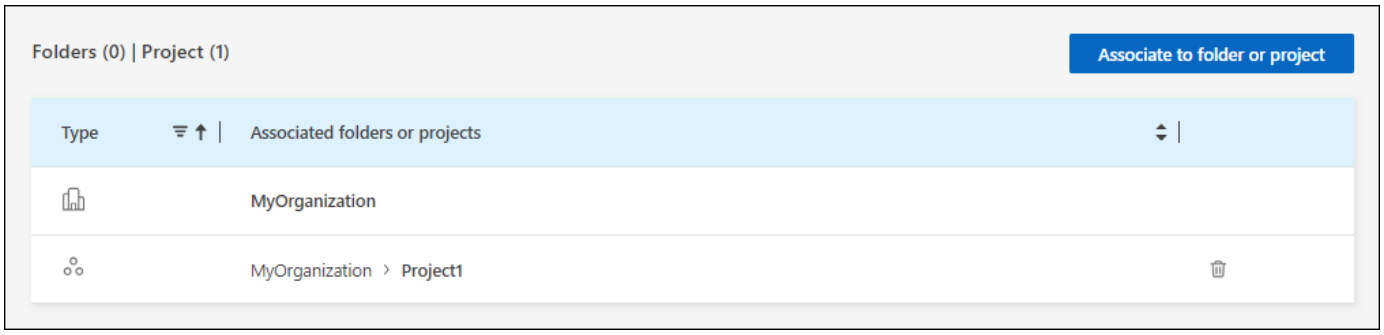
Vous pouvez afficher les dossiers et les projets associés à une ressource particulière.

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.



Si vous devez déterminer 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" .

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

Pour supprimer une ressource d'un dossier ou d'un projet, vous devez supprimer l'association entre le dossier ou le projet et la ressource. Lorsque vous supprimez l'association, cela empêche les membres de gérer la ressource dans le dossier ou le projet.

Pour supprimer une ressource découverte de l'ensemble de l'organisation, supprimez le système de la page **Systèmes**.

Étapes

1. Depuis la page **Ressources**, accédez à une ressource dans le tableau, sélectionnez••• puis sélectionnez **Afficher les détails**.
2. Pour le dossier ou le projet pour lequel vous souhaitez supprimer la ressource, sélectionnez
3. Confirmez que vous souhaitez supprimer l'association en sélectionnant **Supprimer**.

Informations connexes

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

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

Lorsqu'un *administrateur d'organisation* crée un agent de console, l'agent de console est automatiquement associé au projet actuellement sélectionné au sein de l'organisation. Bien qu'une personne disposant du rôle *Administrateur de l'organisation* puisse accéder à cet agent de console depuis n'importe où dans l'organisation. Les autres membres de

votre organisation ne peuvent accéder à cet agent de console qu'à partir du projet dans lequel il a été créé, sauf si vous associez cet agent de console à d'autres projets.

Avant de commencer

Découvrez comment fonctionne l'association d'agents de console. "En savoir plus sur l'utilisation de l'agent de console avec Identity and Access" .

À propos de cette tâche

Un *administrateur de dossier ou de projet* peut afficher tous les agents de la console sur la page **Agent** mais ne peut associer les agents de la console qu'aux dossiers et aux projets pour lesquels il dispose d'autorisations. "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 console NetApp"
- "En savoir plus sur la gestion des identités et des accès de la console NetApp"
- "Démarrer avec l'identité et l'accès"
- "En savoir plus sur l'API pour la gestion des identités et des accès"

Basculer entre les organisations, les projets et les agents de la console

Vous pouvez appartenir à plusieurs organisations de console ou disposer d'autorisations pour accéder à plusieurs projets ou agents au sein d'une organisation. En cas de besoin, vous pouvez facilement basculer entre les organisations, les projets et les agents de console pour accéder aux ressources associées à cette organisation, ce projet ou cet agent.

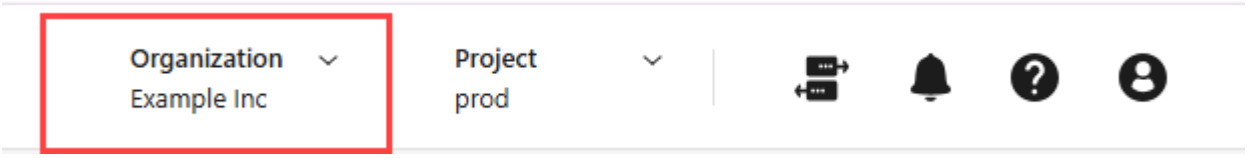
Vous pouvez appartenir à plusieurs organisations si une autre organisation vous invite à la rejoindre ou si vous en créez une vous-même. Vous pouvez créer une organisation supplémentaire en utilisant l'API. "Apprenez à créer une nouvelle organisation"

Basculer entre les organisations

Si vous êtes membre de plusieurs organisations, vous pouvez basculer entre elles à tout moment.

Étapes

1. Dans l'en-tête supérieur de la console, sélectionnez **Organisation**.



2. Si vous avez des organisations partenaires, sélectionnez l'onglet **Partenariat** pour afficher les organisations partenaires disponibles.

+ L'onglet **Partenariat** ne s'affiche pas si vous n'avez aucune organisation partenaire.

1. Sélectionnez une autre organisation, puis sélectionnez **Changer**.

+ Si vous avez des organisations partenaires, sélectionnez l'onglet **Partenariat** pour afficher les organisations partenaires disponibles.

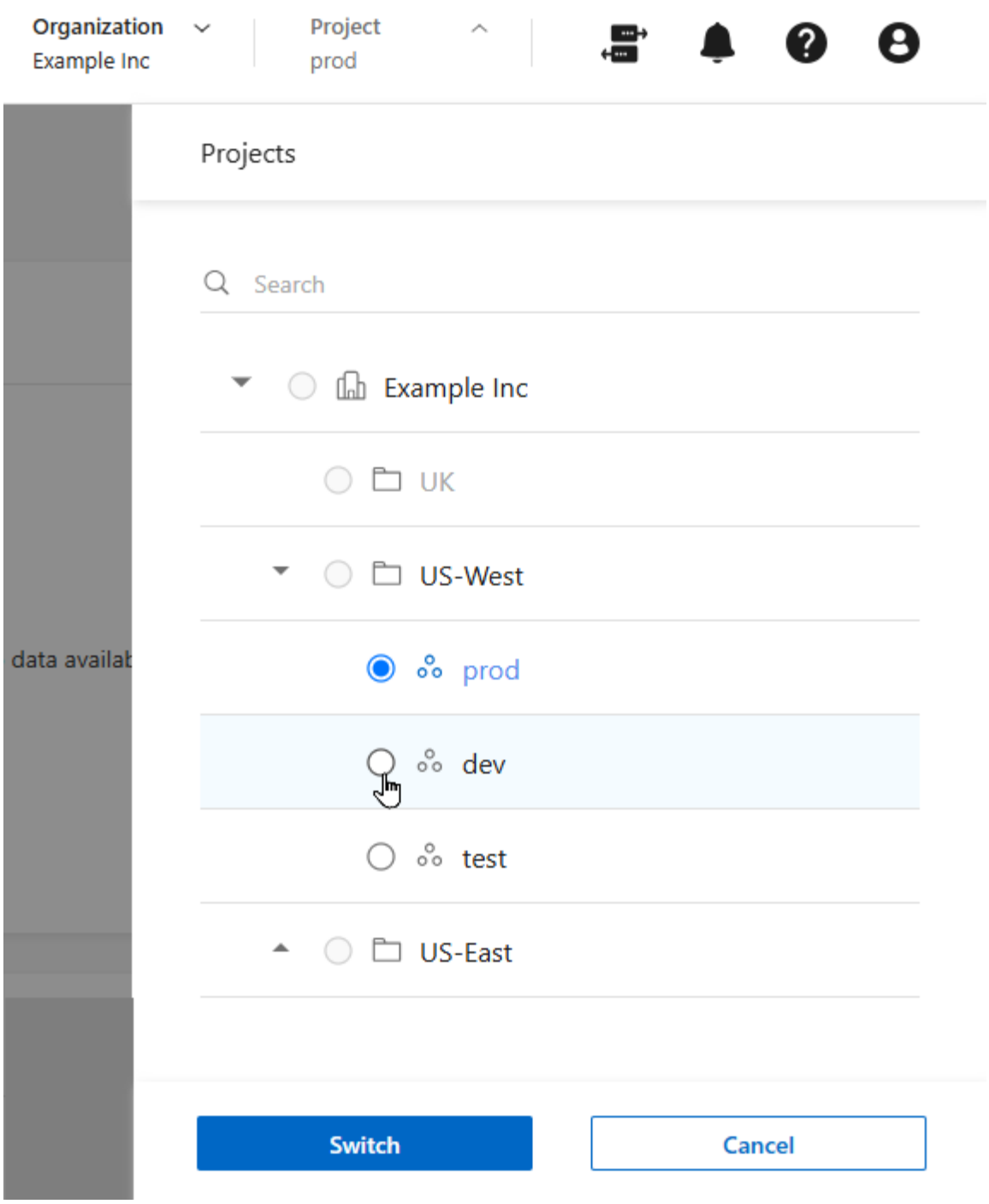
Basculer entre les projets

Si votre organisation comprend plusieurs projets et que vous avez accès à ces projets, vous pouvez basculer entre eux à tout moment.

Vous ne pouvez pas passer à un autre projet pendant que vous consultez l'une des pages **Identité et accès**.

Étapes

1. Dans l'en-tête supérieur de la console, sélectionnez **Projet**.
2. Parcourez les dossiers et les projets de votre organisation, sélectionnez le projet souhaité, puis sélectionnez **Basculer**.



Basculer entre les agents de la console

Si vous disposez de plusieurs agents de console, vous pouvez basculer entre eux pour voir les systèmes associés à un agent spécifique.

Étapes

1. Dans l'en-tête supérieur de la console, sélectionnez l'icône Agent.
2. Sélectionnez un autre agent, puis sélectionnez **Changer**.

Informations connexes

"Associer des agents à des dossiers et des projets" .

Informations connexes

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

ID d'organisation et de projet

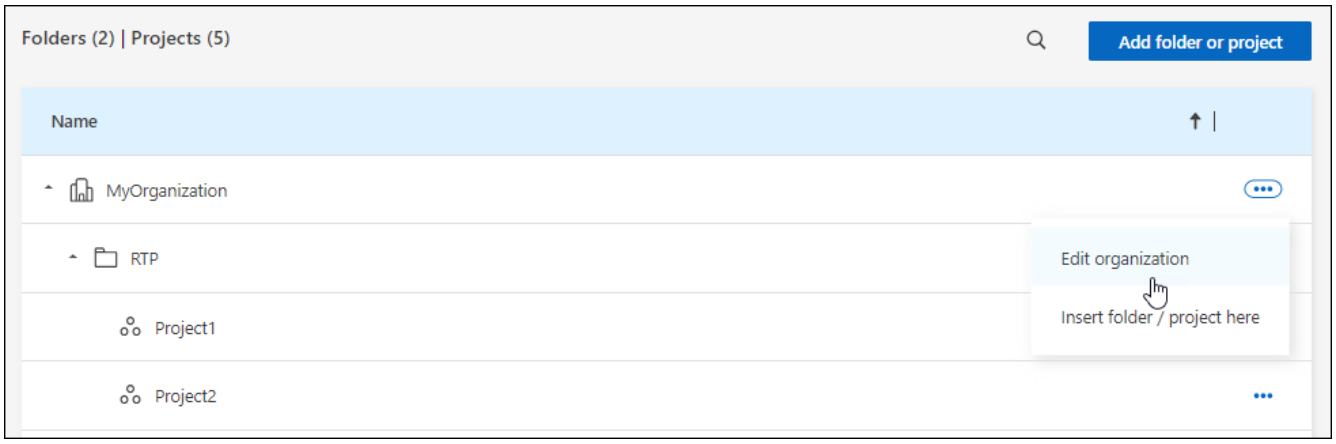
Votre organisation NetApp Console possède un nom et un ID. Vous pouvez choisir un nom pour votre organisation afin de l'identifier. Vous devrez peut-être également récupérer l'ID de l'organisation pour certaines intégrations.

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

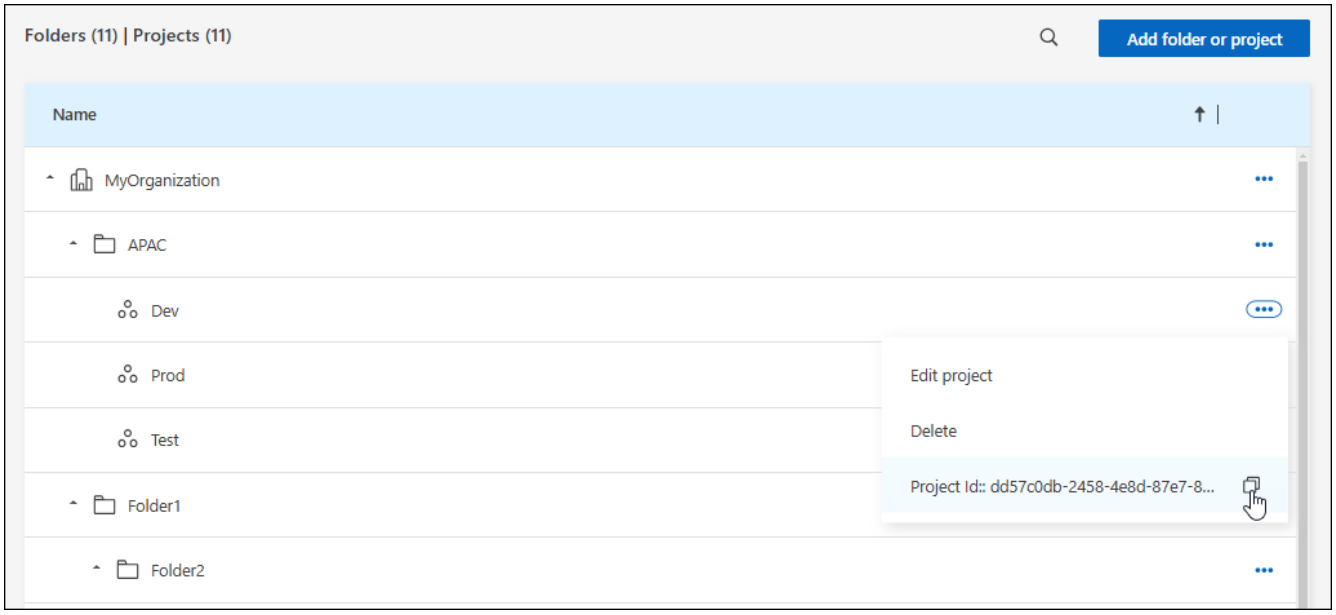
Vous devrez obtenir l’ID d’un projet si vous utilisez l’API. Par exemple, lors de la création d’un système Cloud Volumes ONTAP .

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"

Surveiller ou auditer l’activité IAM

Si vous devez surveiller ou auditer une action effectuée en lien avec l’identité et l’accès, vous pouvez afficher les détails à partir de la page Audit. Par exemple, vous souhaiterez peut-être vérifier qui a ajouté un membre à une organisation ou qu’un projet a été supprimé avec succès.

Étapes

1. Sélectionnez **Administration > Audit**.
2. Sur la page **Audit**, utilisez les filtres pour affiner les résultats. Sélectionnez **Service** puis **Location**.
3. Utilisez l’un des autres filtres pour modifier les actions affichées dans le tableau.

   Par exemple, vous pouvez utiliser le filtre **Utilisateur** pour afficher les actions liées à un compte utilisateur spécifique.

Rôles d’accès à la console NetApp

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

La gestion des identités et des accès (IAM) dans la console NetApp 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 console NetApp , 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.
"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.
"Administrateur de clone de sauvegarde et de récupération"	Cloner des applications et des données dans la sauvegarde et la récupération.

Rôle du service de données	Responsabilités
"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 classification des données NetApp . 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 n'a pas de rôle de spectateur.
"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 console NetApp SnapCenter n'a pas de rôle de visualiseur.

Liens connexes

- "En savoir plus sur la gestion des identités et des accès de la console NetApp"
- "Démarrer avec NetApp Console IAM"
- "Gérer les membres de la console NetApp 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 console NetApp , 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 visualiseur** 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 console NetApp 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 console NetApp

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

Google Cloud NetApp Volumes utilise le rôle suivant :

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

Rôles d'accès Keystone dans la console NetApp

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 console NetApp

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	Non
Gérer les alertes	Oui	Non
Créer des alertes pour soi-même	Oui	Oui
Licences et abonnements:		
Peut afficher les licences et les abonnements	Oui	Oui
* Page des rapports Keystone * :		

Fonctionnalité et action	Administrateur Keystone	Visionneuse 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 console NetApp

Vous pouvez attribuer le rôle suivant aux utilisateurs pour 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
Oui	Afficher la page d'audit et les notifications
Oui	Afficher, télécharger et configurer les alertes

Rôles d'accès au stockage pour la console NetApp

Vous pouvez attribuer les rôles suivants aux utilisateurs pour leur donner accès aux fonctionnalités de gestion du stockage dans la console NetApp . 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 console NetApp .

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 console NetApp

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
Supprimer les systèmes de la console	Oui	Non	Non
Modifier les systèmes	Oui	Non	Non
Créer des agents	Non	Non	Non
Conseiller numérique			

Fonctionnalité et action	Administrateur de stockage	Spécialiste de la santé du système	Visionneuse de stockage
Afficher toutes les pages et fonctions	Oui	Oui	Oui
Licences et abonnements			
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
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			

Fonctionnalité et action	Administrateur de stockage	Spécialiste de la santé du système	Visionneuse de stockage
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 sauvegarde et de récupération NetApp dans la console NetApp

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 console NetApp , 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 sauvegarde et de récupération NetApp 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 sauvegarde et de récupération NetApp 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 reprise après sinistre NetApp dans la console NetApp

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 console NetApp

Les rôles de résilience aux ransomwares permettent aux utilisateurs d'accéder à NetApp Ransomware Resilience. Les deux rôles sont administrateur de protection contre les ransomwares et visualiseur de protection contre les ransomwares. La principale différence entre les deux rôles réside dans les actions qu'ils peuvent entreprendre dans

Ransomware Resilience.

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

Fonctionnalité et action	Administrateur de la résilience aux ransomwares	Visionneuse de résilience aux ransomwares	Comportement utilisateur de Ransomware Resilience administrateur	Visualiseur de comportement utilisateur de Ransomware Resilience
Afficher le tableau de bord et tous les onglets	Oui	Oui	Non	Non
Sur le tableau de bord, mettre à jour le statut de la recommandation	Oui	Non	Non	Non
Démarrer un essai gratuit	Oui	Non	Non	Non
Lancer la découverte des charges de travail	Oui	Non	Non	Non
Initier la redécouverte des charges de travail	Oui	Non	Non	Non
Dans l'onglet Protéger :				
Ajouter, modifier ou supprimer des plans de protection	Oui	Non	Non	Non
Protéger les charges de travail	Oui	Non	Non	Non
Identifier l'exposition aux données sensibles	Oui	Non	Non	Non
Liste des plans de protection et des détails	Oui	Oui	Non	Non
Liste des groupes de protection	Oui	Oui	Non	Non
Afficher les détails du groupe de protection	Oui	Oui	Non	Non
Créer, modifier ou supprimer un groupe de protection	Oui	Non	Non	Non
Télécharger les données	Oui	Oui	Non	Non
Dans l'onglet Alertes :				
Afficher les alertes et les détails des alertes	Oui	Oui	Non	Non
Modifier le statut de l'incident	Oui	Non	Non	Non
Marquer l'alerte pour la récupération	Oui	Non	Non	Non

Fonctionnalité et action	Administrateur de la résilience aux ransomwares	Visionneuse de résilience aux ransomwares	Comportement utilisateur de Ransomware Resilience administrateur	Visualiseur de comportement utilisateur de Ransomware Resilience
Afficher les détails de l'incident	Oui	Oui	Non	Non
Rejeter ou résoudre les incidents	Oui	Non	Non	Non
Bloquer l'utilisateur	Oui	Non	Non	Non
Obtenez la liste complète des fichiers concernés	Oui	Non	Non	Non
Télécharger les données d'alertes	Oui	Oui	Non	Non
Afficher les activités suspectes des utilisateurs	Non	Non	Oui	Oui
Dans l'onglet Récupérer :				
Télécharger les fichiers concernés	Oui	Non	Non	Non
Restaurer la charge de travail	Oui	Non	Non	Non
Télécharger les données de récupération	Oui	Oui	Non	Non
Télécharger les rapports	Oui	Oui	Non	Non
Dans l'onglet Paramètres :				
Ajouter ou modifier des destinations de sauvegarde	Oui	Non	Non	Non
Lister les destinations de sauvegarde	Oui	Oui	Non	Non
Afficher les cibles SIEM connectées	Oui	Oui	Non	Non
Ajouter ou modifier des cibles SIEM	Oui	Non	Non	Non
Configurer l'exercice de préparation	Oui	Non	Non	Non
Commencer l'exercice de préparation	Oui	Non	Non	Non
Exercice de préparation à la réinitialisation	Oui	Non	Non	Non
Modifier l'exercice de préparation	Oui	Non	Non	Non

Fonctionnalité et action	Administrateur de la résilience aux ransomwares	Visionneuse de résilience aux ransomwares	Comportement utilisateur de Ransomware Resilience administrateur	Visualiseur de comportement utilisateur de Ransomware Resilience
Examen de l'état de préparation de l'exercice	Oui	Oui	Non	Non
Mettre à jour la configuration de la découverte	Oui	Non	Non	Non
Afficher la configuration de la découverte	Oui	Oui	Non	Non
Configurer les paramètres de comportement suspect des utilisateurs	Non	Non	Oui	Non
Dans l'onglet Rapports :				
Télécharger les rapports	Oui	Oui	Non	Non

Organisations partenaires

Partenariats dans la console NetApp

En créant des partenariats entre les organisations, la console NetApp permet aux partenaires de gérer en toute sécurité les ressources NetApp au-delà des frontières organisationnelles, simplifiant ainsi la collaboration et améliorant 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.

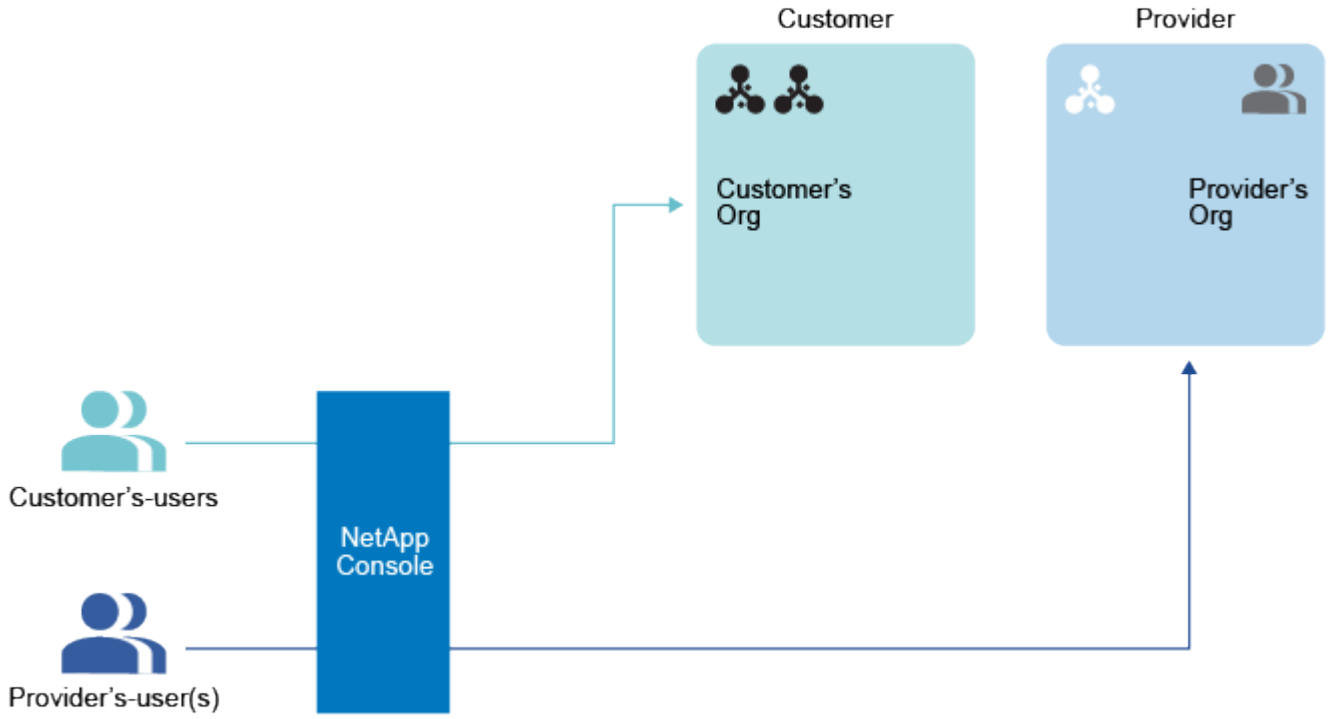
1. **Attribuer à un ou plusieurs utilisateurs le rôle d'administrateur de partenariat**

Affectez un ou plusieurs utilisateurs dans les organisations initiatrices et réceptrices au rôle d'administrateur de partenariat pour créer et gérer des partenariats. Vous pouvez affecter le rôle de visualiseur de partenariat aux utilisateurs qui ont uniquement besoin de visualiser les partenariats et non de les gérer.

2 Partagez l'identifiant de votre organisation avec l'organisation initiatrice

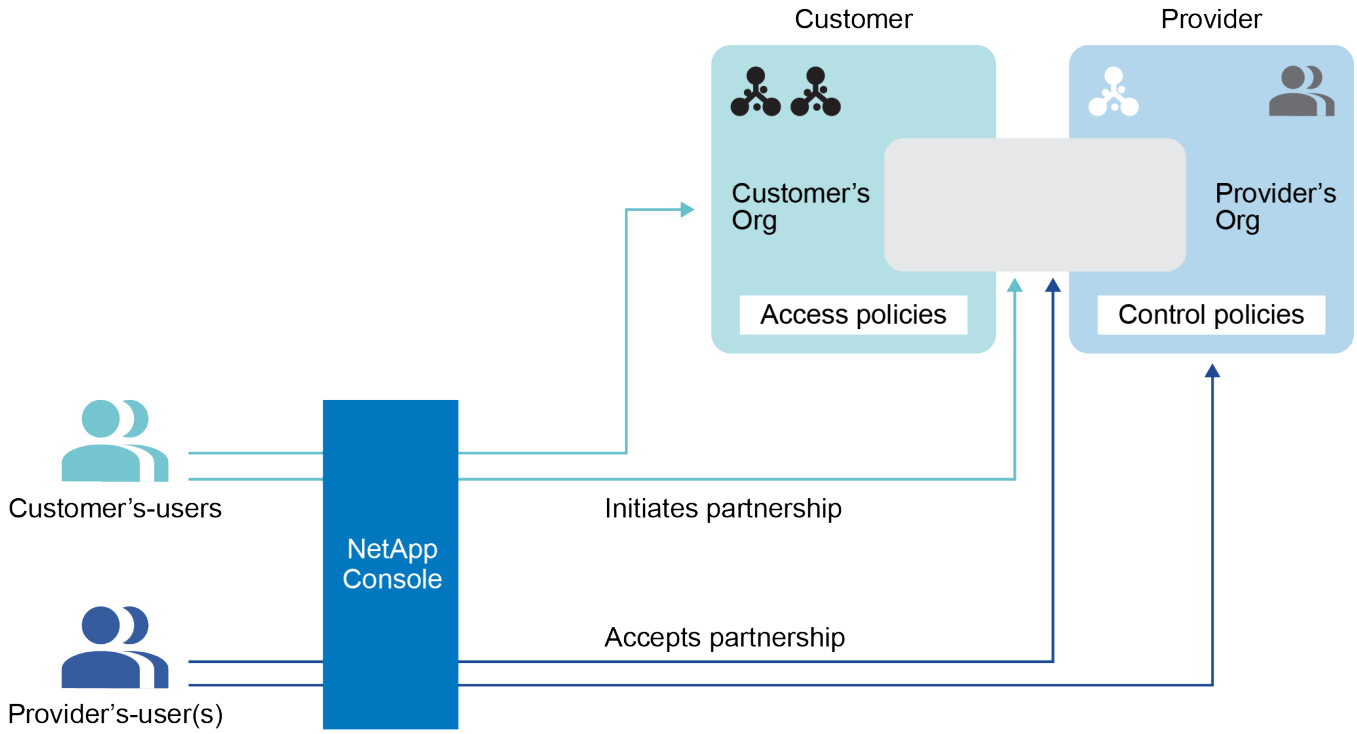
Pour initier un partenariat, l'initiateur doit connaître l'ID de l'organisation cible. Seule l'organisation concernée peut accéder à cet ID d'organisation. Partagez-le directement avec l'organisation initiatrice en dehors de la console NetApp par courrier électronique ou par une autre méthode.

L'organisation initiatrice est l'organisation qui accorde l'accès à ses ressources.



3 Initier le partenariat au sein de la console NetApp

L'organisation qui initie le partenariat le fait depuis la console NetApp en envoyant une demande de partenariat.



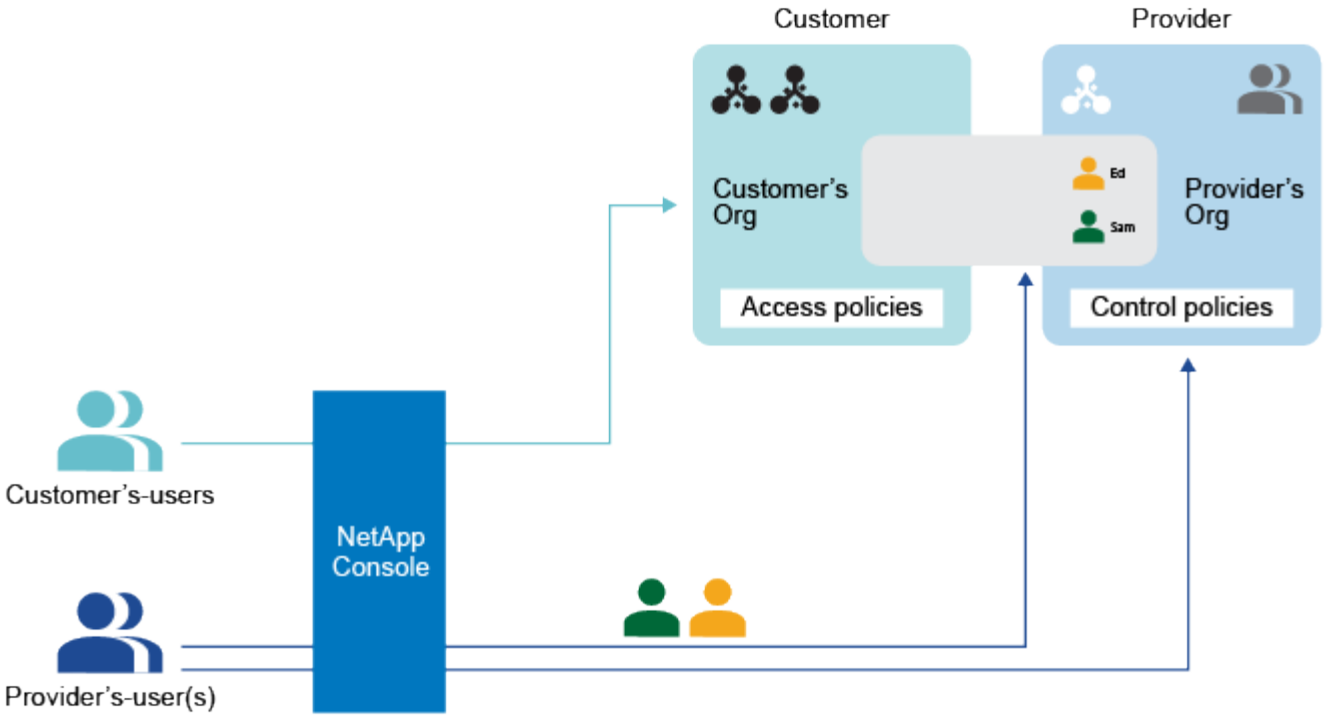
4 **Approuver le partenariat**

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**

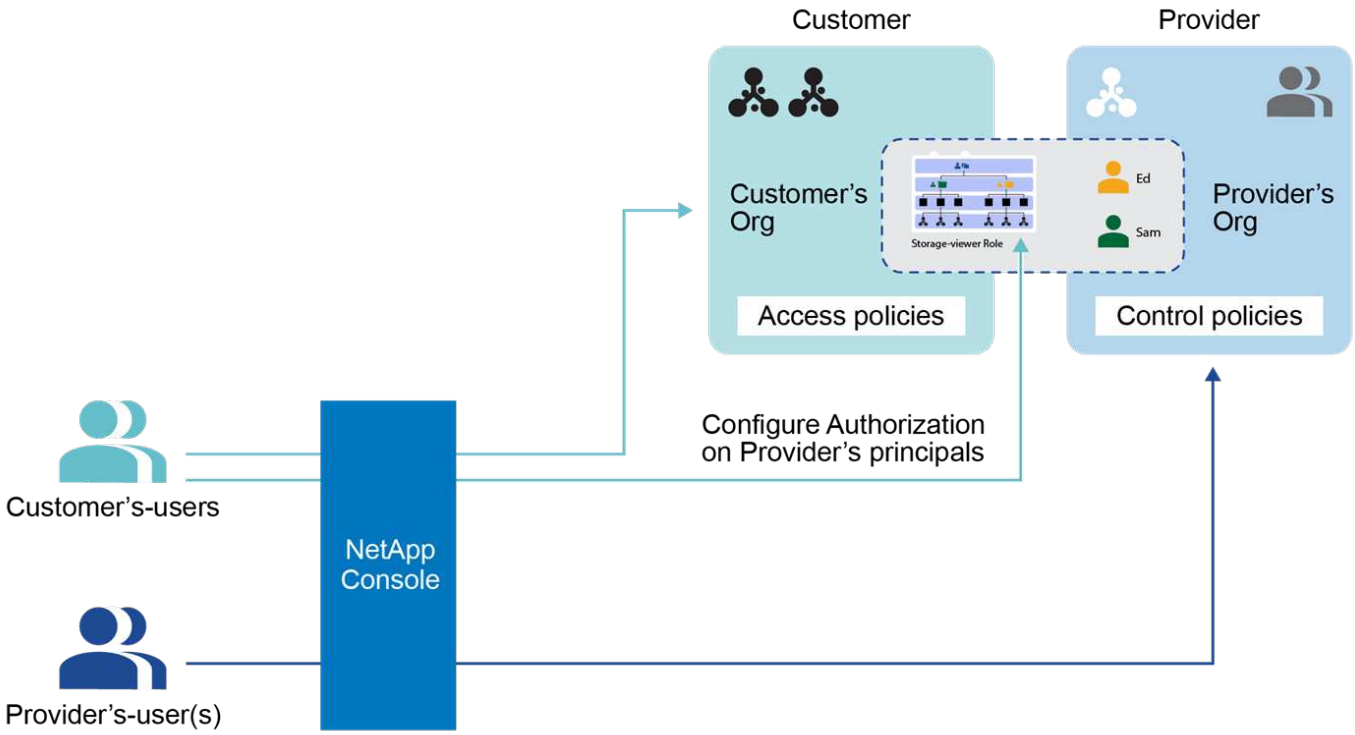
L'organisation réceptrice attribue des utilisateurs ou des comptes de service spécifiques de votre organisation au partenariat. L'organisation initiatrice attribue des rôles à ces utilisateurs.



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 console NetApp

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 respectif 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 respectif 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 annuler l'attribution du rôle d'un membre, sélectionnez 🗑 à côté du rôle pour désattribuer le rôle respectif au 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.

Fédération d’identité

Activer l’authentification unique en utilisant la fédération d’identité avec la console NetApp

L’authentification unique (fédération) simplifie le processus de connexion et améliore la sécurité en permettant aux utilisateurs de se connecter à la console NetApp 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."

Fédération d’identité avec le site de support 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.

Configurer une connexion fédérée 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 console NetApp

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.

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.

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.

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.

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.

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 console NetApp 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 console NetApp avec les services de fédération Active Directory (AD FS)

Fédérez vos services de fédération Active Directory (AD FS) avec la console NetApp pour activer l'authentification unique (SSO) pour la console NetApp . 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 console NetApp 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 console NetApp . 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 console NetApp .

Avant de commencer

- Un compte IdP avec des privilèges administratifs est requis. Coordonnez-vous avec votre administrateur IdP pour terminer les étapes.
- Identifiez le domaine que vous souhaitez utiliser pour la fédération. Vous pouvez utiliser votre domaine de messagerie ou un autre domaine que vous possédez. Si vous souhaitez utiliser un domaine autre que votre domaine de messagerie, vous devez d'abord vérifier le domaine dans la console. Vous pouvez le faire en suivant les étapes décrites dans le"Vérifiez votre domaine dans la console NetApp" sujet.

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 console NetApp 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 console NetApp 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 console NetApp 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 pour terminer le test et revenez à la console pour activer la connexion.
14. Sélectionnez **Suivant**.
15. Sur la page **Activer la fédération**, vérifiez les détails de la fédération, puis sélectionnez **Activer la fédération**.
16. Sélectionnez **Terminer** pour terminer le processus.

Une fois la fédération activée, les utilisateurs peuvent se connecter à la console NetApp à l'aide de leurs informations d'identification d'entreprise.

Fédérer la console NetApp avec Microsoft Entra ID

Fédérez-vous avec votre fournisseur IdP Microsoft Entra ID pour activer l'authentification unique (SSO) pour la console NetApp . 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.

Avant de commencer

- Un compte IdP avec des privilèges administratifs est requis. Coordonnez-vous avec votre administrateur IdP pour terminer les étapes.
- Identifiez le domaine que vous souhaitez utiliser pour la fédération. Vous pouvez utiliser votre domaine de messagerie ou un autre domaine que vous possédez. Si vous souhaitez utiliser un domaine autre que votre domaine de messagerie, vous devez d'abord vérifier le domaine dans la console. Vous pouvez le faire en suivant les étapes décrites dans le"Vérifiez votre domaine dans la console NetApp" sujet.

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 pour terminer le test et revenez à la console pour activer la connexion.
3. Sélectionnez **Suivant**.
4. Sur la page **Activer la fédération**, vérifiez les détails de la fédération, puis sélectionnez **Activer la fédération**.
5. Sélectionnez **Terminer** pour terminer le processus.

Une fois la fédération activée, les utilisateurs peuvent se connecter à la console NetApp à l'aide de leurs informations d'identification d'entreprise.

Fédérer la console NetApp avec PingFederate

Fédérez-vous avec votre fournisseur IdP PingFederate pour activer l'authentification unique (SSO) pour la console NetApp . 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.

Avant de commencer

- Un compte IdP avec des privilèges administratifs est requis. Coordonnez-vous avec votre administrateur IdP pour terminer les étapes.
- Identifiez le domaine que vous souhaitez utiliser pour la fédération. Vous pouvez utiliser votre domaine de messagerie ou un autre domaine que vous possédez. Si vous souhaitez utiliser un domaine autre que votre domaine de messagerie, vous devez d'abord vérifier le domaine dans la console. Vous pouvez le faire en suivant les étapes décrites dans le"Vérifiez votre domaine dans la console NetApp" sujet.

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 console NetApp :

      - 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 pour terminer le test et revenez à la console pour activer la connexion.
14. Sélectionnez **Suivant**.
15. Sur la page **Activer la fédération**, vérifiez les détails de la fédération, puis sélectionnez **Activer la fédération**.
16. Sélectionnez **Terminer** pour terminer le processus.

Une fois la fédération activée, les utilisateurs peuvent se connecter à la console NetApp à l'aide de leurs informations d'identification 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.

Avant de commencer

- Un compte IdP avec des privilèges administratifs est requis. Coordonnez-vous avec votre administrateur IdP pour terminer les étapes.
- Identifiez le domaine que vous souhaitez utiliser pour la fédération. Vous pouvez utiliser votre domaine de messagerie ou un autre domaine que vous possédez. Si vous souhaitez utiliser un domaine autre que votre domaine de messagerie, vous devez d'abord vérifier le domaine dans la console. Vous pouvez le faire en suivant les étapes décrites dans le"Vérifiez votre domaine dans la console NetApp" sujet.

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>
```

b. 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` .

c. Après avoir créé la confiance, copiez les valeurs suivantes à partir de votre serveur fournisseur SAML :
   - URL de connexion
   - URL de déconnexion (facultatif)

d. Téléchargez le certificat X.509 depuis le serveur de votre fournisseur SAML. Il doit être au format PEM, CER ou CRT.

9. Revenez à la console et sélectionnez **Suivant** pour créer la connexion.
10. Créez la connexion avec SAML.
    a. Saisissez l'**URL de connexion** de votre serveur SAML.
    b. Téléchargez le certificat X.509 que vous avez téléchargé depuis le serveur de votre fournisseur SAML.
    c. Si vous le souhaitez, saisissez l'**URL de déconnexion** de votre serveur SAML.
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 pour terminer le test et revenez à la console pour activer la connexion.
14. Sélectionnez **Suivant**.
15. Sur la page **Activer la fédération**, vérifiez les détails de la fédération, puis sélectionnez **Activer la fédération**.
16. Sélectionnez **Terminer** pour terminer le processus.

Une fois la fédération activée, les utilisateurs peuvent se connecter à la console NetApp à l'aide de leurs informations d'identification d'entreprise.

Gérer les fédérations dans la console NetApp

Vous pouvez gérer votre fédération dans la console NetApp . Vous pouvez le désactiver, mettre à jour les informations d'identification expirées, ainsi que le désactiver si vous n'en avez plus besoin.

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 également ajouter un domaine vérifié à une fédération existante, ce qui vous permet d'utiliser plusieurs domaines pour votre connexion fédérée.

Les événements de gestion de fédération tels que l'activation, la désactivation et la mise à jour des fédérations s'affichent dans la chronologie."En savoir plus sur les opérations de surveillance dans la console NetApp ."

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."

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 console NetApp . 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 console NetApp

Si vous avez déjà configuré la fédération via NetApp Cloud Central (une application externe à la console NetApp), 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**.

Agents de console

Maintenir la machine virtuelle de l'agent de console et le système d'exploitation

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

Si vous avez déjà un agent, vous devez en être conscient."modifications apportées aux systèmes d'exploitation Linux pris en charge" .

Correctifs du système d'exploitation et l'agent

Appliquez les correctifs de sécurité du système d'exploitation sans arrêter les services hôtes de l'agent.

Type de machine virtuelle ou d'instance

Si vous créez un agent de console à partir de la console, il déploie une instance de machine virtuelle dans votre fournisseur de cloud avec une configuration par défaut. Après avoir créé l'agent, ne passez pas à une instance de machine virtuelle plus petite avec moins de CPU ou de RAM.

Le tableau suivant répertorie les exigences en matière de CPU et de RAM :

processeur
: 8 cœurs ou 8 vCPU

BÉLIER
: 32 Go

"En savoir plus sur la configuration par défaut de l'agent" .

Surveiller l'agent

La console vous avertit lorsque la machine virtuelle de l'agent n'est pas saine, notamment en cas de problèmes d'espace disque, de RAM et de processeur. Surveillez ces notifications dans le centre de notifications de la console ou configurez des notifications par e-mail. Des augmentations occasionnelles de l'espace disque, de la mémoire ou de l'utilisation du processeur sont normales, mais si cela se produit fréquemment, vous devez prendre des mesures pour résoudre le problème.

Par exemple, la console vous avertit lorsqu'une ressource d'agent (CPU, RAM ou espace disque) dépasse 90 % de sa capacité totale pendant 30 minutes consécutives. Par la suite, si l'utilisation des ressources descend en dessous de ce seuil, la notification s'affiche comme résolue (verte) dans le Centre de notifications.

Travaillez avec le support NetApp si vous avez des questions sur la modification de votre machine virtuelle agent.

"Apprendre encore plus."

Notification	Action nécessaire
L'espace disque est trop élevé	"Consultez l'article de la base de connaissances NetApp" .

Notification	Action nécessaire
L'utilisation du processeur est trop élevée	Augmentez la taille du processeur de la machine virtuelle de l'agent dans votre fournisseur de cloud ou sur site, selon l'endroit où vous l'avez installé. Vous pouvez également créer des agents supplémentaires et répartir la charge de travail sur plusieurs agents. L'utilisation de la RAM peut varier en fonction de votre environnement, des charges de travail ONTAP , du nombre de systèmes Cloud Volumes ONTAP et des services de données que vous utilisez.
L'utilisation de la RAM est trop élevée	Augmentez la RAM de la machine virtuelle de l'agent dans votre fournisseur de cloud ou sur site, selon l'endroit où vous l'avez installé. Vous pouvez également créer des agents supplémentaires et répartir la charge de travail sur plusieurs agents. L'utilisation de la RAM peut varier en fonction de votre environnement, des charges de travail ONTAP , du nombre de systèmes Cloud Volumes ONTAP et des services de données que vous utilisez.

Arrêt et démarrage de la machine virtuelle de l'agent

Si nécessaire, arrêtez et démarrez la machine virtuelle de l'agent à l'aide de la console de votre fournisseur de cloud ou des procédures standard sur site.

"Sachez que l'agent de la console doit être opérationnel à tout moment" .

Se connecter à la machine virtuelle Linux

Si vous devez vous connecter à la machine virtuelle Linux sur laquelle l'agent s'exécute, utilisez les options de connectivité de votre fournisseur de cloud.

AWS

Lorsque vous créez l'instance d'agent dans AWS, fournissez une clé d'accès AWS et une clé secrète. Vous pouvez utiliser cette paire de clés pour vous connecter en SSH à l'instance. Utilisez le nom d'utilisateur « ubuntu » pour l'instance Linux EC2. Pour les agents créés avant mai 2023, utilisez le nom d'utilisateur « ec2-user ».

"Documentation AWS : connectez-vous à votre instance Linux"

Azuré

Lorsque vous créez la machine virtuelle de l'agent dans Azure, vous spécifiez un nom d'utilisateur et choisissez de vous authentifier avec un mot de passe ou une clé publique SSH. Utilisez la méthode d'authentification que vous avez choisie pour vous connecter à la machine virtuelle.

"Azure Docs : Connectez-vous à votre machine virtuelle via SSH"

Google Cloud

Vous ne pouvez pas spécifier de méthode d'authentification lorsque vous créez un agent dans Google Cloud. Cependant, vous pouvez vous connecter à l'instance de machine virtuelle Linux à l'aide de la console Google Cloud ou de Google Cloud CLI (gcloud).

"Google Cloud Docs : Se connecter aux machines virtuelles Linux"

Modifier l'adresse IP d'un agent

Vous pouvez modifier les adresses IP internes et publiques de l'instance d'agent attribuées par votre fournisseur de cloud si nécessaire.

Étapes

1. Suivez les instructions de votre fournisseur de cloud pour modifier l'adresse IP locale ou l'adresse IP publique (ou les deux) de l'instance de l'agent.
2. Redémarrez l'instance de l'agent pour enregistrer une nouvelle adresse IP publique auprès de la console.
3. Si vous avez modifié l'adresse IP privée, mettez à jour l'emplacement de sauvegarde des fichiers de configuration Cloud Volumes ONTAP afin que les sauvegardes soient envoyées à la nouvelle adresse IP privée sur l'agent.

   Mettez à jour l'emplacement de sauvegarde pour chaque système Cloud Volumes ONTAP .

   a. Depuis l'interface de ligne de commande Cloud Volumes ONTAP , définissez le niveau de privilège sur avancé :

   ```
   set -privilege advanced
   ```

   b. Exécutez la commande suivante pour afficher la cible de sauvegarde actuelle :

   ```
   system configuration backup settings show
   ```

   c. Exécutez la commande suivante pour mettre à jour l'adresse IP de la cible de sauvegarde :

   ```
   system configuration backup settings modify -destination <target-
   location>
   ```

Modifier les URI d'un agent

Vous pouvez ajouter et supprimer l'identifiant de ressource uniforme (URI) d'un agent.

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 la barre **URI de l'agent** pour afficher les URI de l'agent.
4. Ajoutez et supprimez des URI, puis sélectionnez **Appliquer**.

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 invites 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 console NetApp 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 que la console utilise 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**.

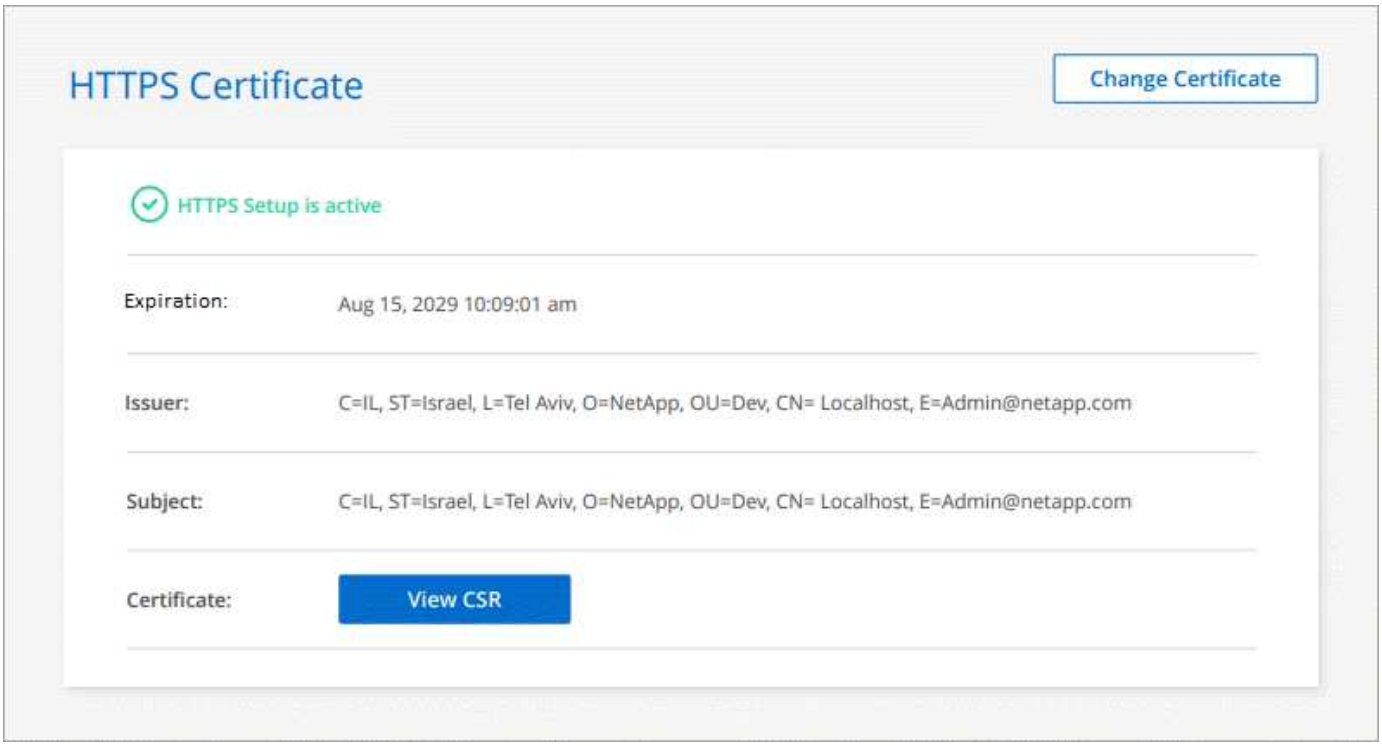
   L'agent de la console doit être actif pour pouvoir le modifier.

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**.
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 de console en utilisant le `proxy update` commande ou supprimez le serveur proxy transparent en utilisant le `proxy remove` commande. Pour plus d'informations, consultez la documentation de"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 de console pour utiliser un serveur proxy, vous pouvez activer le trafic API direct sur l'agent de console afin d'envoyer des appels API directement aux services du fournisseur cloud sans passer par le proxy. Les agents exécutés dans 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**.

Exiger l'utilisation d'IMDSv2 sur les instances Amazon EC2

La console NetApp prend en charge le service de métadonnées d'instance Amazon EC2 version 2 (IMDSv2) avec l'agent de console et avec Cloud Volumes ONTAP (y compris le médiateur pour les déploiements HA). Dans la plupart des cas, IMDSv2 est automatiquement configuré sur les nouvelles instances EC2. IMDSv1 a été activé avant mars 2024. Si vos politiques de sécurité l'exigent, vous devrez peut-être configurer manuellement IMDSv2 sur vos instances EC2.

Avant de commencer

- La version de l'agent de console doit être 3.9.38 ou ultérieure.
- Cloud Volumes ONTAP doit exécuter l'une des versions suivantes :
  - 9.12.1 P2 (ou tout patch ultérieur)
  - 9.13.0 P4 (ou tout correctif ultérieur)
  - 9.13.1 ou toute version ultérieure à cette version

- Cette modification nécessite le redémarrage des instances Cloud Volumes ONTAP .
- Ces étapes nécessitent l'utilisation de l'AWS CLI car vous devez modifier la limite de saut de réponse à 3.

À propos de cette tâche

IMDSv2 offre une protection renforcée contre les vulnérabilités. "En savoir plus sur IMDSv2 sur le blog de sécurité AWS"

Le service de métadonnées d'instance (IMDS) est activé comme suit sur les instances EC2 :

- Pour les nouveaux déploiements d'agents de console à partir de la console ou à l'aide "Scripts Terraform" IMDSv2 est activé par défaut sur l'instance EC2.
- Si vous lancez une nouvelle instance EC2 dans AWS, puis installez manuellement le logiciel de l'agent de la console, IMDSv2 est également activé par défaut.
- Si vous lancez l'agent de console depuis AWS Marketplace, IMDSv1 est activé par défaut. Vous pouvez configurer manuellement IMDSv2 sur l'instance EC2.
- Pour les agents de console existants, IMDSv1 est toujours pris en charge, mais vous pouvez configurer manuellement IMDSv2 sur l'instance EC2 si vous préférez.
- Pour Cloud Volumes ONTAP, IMDSv1 est activé par défaut sur les instances nouvelles et existantes. Vous pouvez configurer manuellement IMDSv2 sur les instances EC2 si vous préférez.

Étapes

1. Exiger l'utilisation d'IMDSv2 sur l'instance de l'agent de console :

   a. Connectez-vous à la machine virtuelle Linux pour l'agent de console.

      Lorsque vous avez créé l'instance de l'agent de console dans AWS, vous avez fourni une clé d'accès AWS et une clé secrète. Vous pouvez utiliser cette paire de clés pour vous connecter en SSH à l'instance. Le nom d'utilisateur de l'instance EC2 Linux est ubuntu (pour les agents de console créés avant mai 2023, le nom d'utilisateur était ec2-user).

      "Documentation AWS : connectez-vous à votre instance Linux"

   b. Installez l'AWS CLI.

      "Documentation AWS : Installer ou mettre à jour vers la dernière version de l'AWS CLI"

   c. Utilisez le `aws ec2 modify-instance-metadata-options` commande pour exiger l'utilisation d'IMDSv2 et pour modifier la limite de saut de réponse PUT à 3.

      Exemple

      ```
      aws ec2 modify-instance-metadata-options \
          --instance-id <instance-id> \
          --http-put-response-hop-limit 3 \
          --http-tokens required \
          --http-endpoint enabled
      ```

      Le `http-tokens` les paramètres définissent IMDSv2 comme requis. Quand `http-tokens` est requis, vous devez également définir `http-endpoint` à activé.

2. Exiger l'utilisation d'IMDSv2 sur les instances Cloud Volumes ONTAP :
   a. Aller à la "Console Amazon EC2"
   b. Dans le volet de navigation, sélectionnez **Instances**.
   c. Sélectionnez une instance Cloud Volumes ONTAP .
   d. Sélectionnez **Actions > Paramètres de l'instance > Modifier les options de métadonnées de l'instance**.
   e. Dans la boîte de dialogue **Modifier les options des métadonnées d'instance**, sélectionnez les éléments suivants :
      - Pour **Service de métadonnées d'instance**, sélectionnez **Activer**.
      - Pour **IMDSv2**, sélectionnez **Obligatoire**.
      - Sélectionnez **Enregistrer**.
   f. Répétez ces étapes pour les autres instances Cloud Volumes ONTAP , y compris le médiateur HA.
   g. "Arrêter et démarrer les instances Cloud Volumes ONTAP"

Résultat

L'instance de l'agent de console et les instances Cloud Volumes ONTAP sont désormais configurées pour utiliser IMDSv2.

Gérer les mises à niveau de l'agent de la console

Lorsque vous utilisez le mode standard ou le mode restreint, la console NetApp met automatiquement à niveau votre agent de console vers la dernière version, à condition que l'agent de console dispose d'un accès Internet sortant pour obtenir la mise à jour logicielle.

Si vous devez gérer manuellement le moment où l'agent de console est mis à niveau, vous pouvez désactiver les mises à niveau automatiques pour le mode standard ou le mode restreint.

Désactiver les mises à niveau automatiques

La désactivation de la mise à niveau automatique pour votre agent de console comprend deux étapes. Vous devez d'abord vous assurer que votre agent de console est sain et à jour. Ensuite, vous modifiez un fichier de configuration pour désactiver les mises à niveau automatiques.

Vous ne pouvez désactiver les mises à niveau automatiques que si vous disposez d'un agent de console version 3.9.48 ou supérieure.

Vérifiez la santé de votre agent

Vous devez vérifier que votre agent est stable et que tous les conteneurs exécutés sur votre machine virtuelle d'agent sont sains et en cours d'exécution. Une fois les mises à niveau automatiques désactivées, votre machine virtuelle agent cesse de rechercher de nouveaux services ou packages de mise à niveau.

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 avant de désactiver la mise à niveau automatique.

Docker (pour les déploiements Ubuntu et VCenter)

```
docker ps -a
```

Podman

```
podman ps -a
```

Désactiver la mise à niveau automatique de l'agent

Vous désactivez les mises à niveau automatiques en définissant l'indicateur *isUpgradeDisabled* dans le fichier *com/opt/application/netapp/service-manager-2/config.json*. Par défaut, cet indicateur est défini sur faux et votre agent est automatiquement mis à niveau. Vous pouvez définir cet indicateur sur vrai pour désactiver les mises à niveau automatiques. Vous devez être familiarisé avec la syntaxe JSON avant de terminer cette étape.

Pour réactiver la mise à niveau automatique, procédez comme suit et définissez l'indicateur *isUpgradeDisabled* sur false.

Étapes

1. Assurez-vous d'avoir vérifié que votre agent est à jour et sain.
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. Modifiez le fichier */opt/application/netapp/service-manager-2/config.json* et remplacez la valeur de l'indicateur *isUpgradeDisabled* par true.

```
  "isUpgradeDisabled": true,
```

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

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

6. Exécutez la commande suivante et vérifiez que l'état de l'agent indique *actif (en cours d'exécution)* : _

```
systemctl status netapp-service-manager.service
_
```

Mettre à niveau l'agent de la console

L'agent de la console doit redémarrer pendant le processus de mise à niveau afin que la console NetApp ne soit pas disponible pendant la mise à niveau.

Étapes

1. Téléchargez le logiciel de l'agent de la console à partir du "Site de support NetApp" .

2. Copiez le programme d'installation sur l'hôte Linux.
3. Attribuer des autorisations pour exécuter le script.

```
chmod +x /path/NetApp-Console-Agent-Offline-<version>
```

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

4. Exécutez le script d'installation :

```
sudo /path/NetApp-Console-Agent-Offline-<version>
```

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

5. Une fois la mise à niveau terminée, vous pouvez vérifier la version de l'agent en accédant à **Administration > Support > Agents**.

Travailler avec plusieurs agents de console

Si vous utilisez plusieurs agents de console, vous pouvez basculer entre ces agents de console directement depuis la console pour afficher les systèmes associés.

Basculer entre les agents de la console

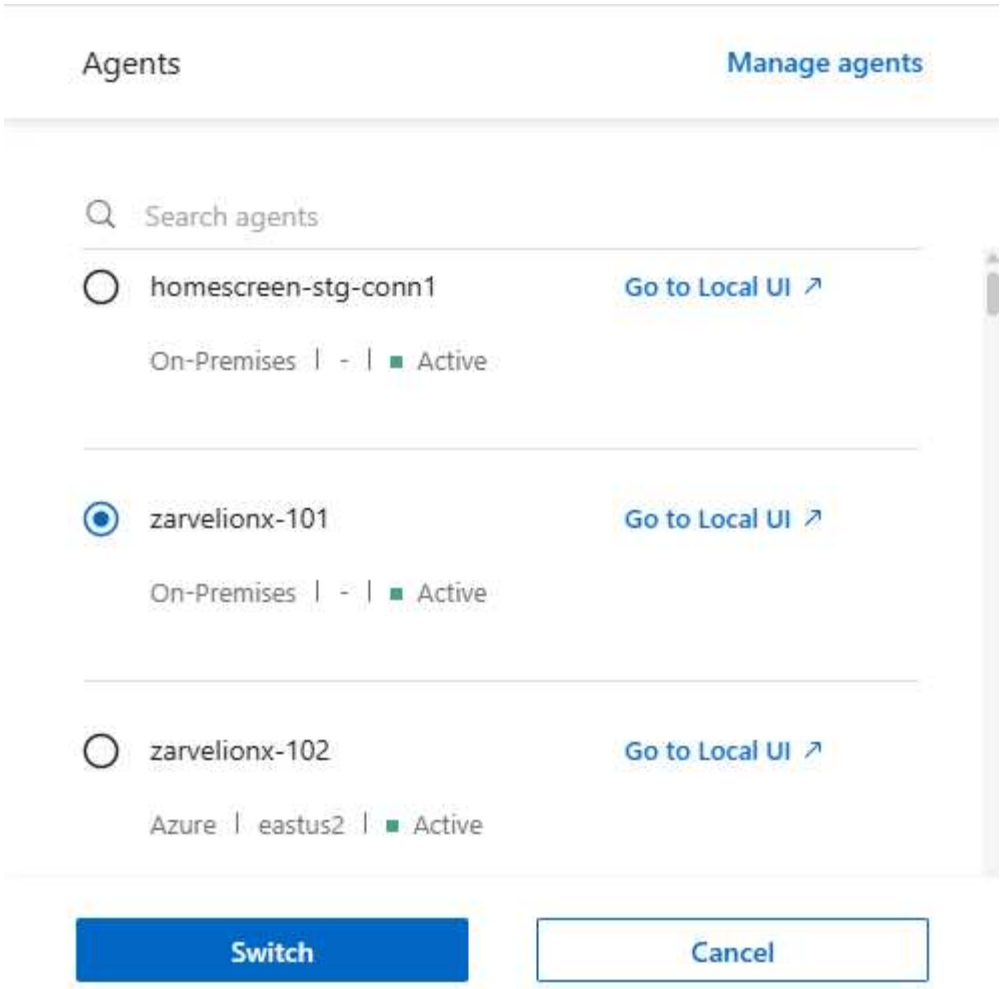
Si vous disposez de plusieurs agents de console, vous pouvez basculer entre eux pour voir les systèmes associés à un agent spécifique.

Par exemple, dans un environnement multicloud, vous pouvez avoir un agent dans AWS et un autre dans Google Cloud. Basculez entre ces agents pour gérer les systèmes Cloud Volumes ONTAP dans les environnements cloud respectifs.

Cette option n'est pas disponible lors de l'affichage de la console NetApp à partir de l'interface utilisateur locale de l'agent

Étape

1. Sélectionnez l'icône Agents de la console ( ) en haut à droite pour voir la liste des agents disponibles.



Résultat

La console s'actualise et affiche les systèmes associés à l'agent sélectionné.

Mettre en place une configuration de reprise après sinistre

Vous pouvez gérer un système avec plusieurs agents de console en même temps à des fins de reprise après sinistre. Si un agent de console tombe en panne, vous pouvez passer à l'autre agent pour gérer immédiatement le système.

Étapes

1. Basculez vers l'autre agent de console que vous souhaitez gérer avec l'agent de console.
2. Découvrez le système existant.
   - "Ajouter des systèmes Cloud Volumes ONTAP existants à la console"
   - "Découvrez les clusters ONTAP"
3. Si vous gérez un système Cloud Volumes ONTAP , réglez le mode de gestion de la capacité sur **Mode manuel**.

   Pour éviter les problèmes de conflit, seul l'agent de la console principale doit être défini sur **Mode automatique**.

   "En savoir plus sur le mode de gestion de la capacité"

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

Le tableau répertorie les messages d’erreur courants et leurs suggestions de résolution :

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 le problème persiste, contactez le support.
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 de support pour l’agent.	Ce message s’affiche si l’agent ne peut pas accéder à votre compte d’assistance.	• *.

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."

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.
- Vous souhaiterez peut-être également désactiver ces vérifications si vous continuez à utiliser la liste de points de terminaison précédente pour les mises à niveau de l'agent.

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. Vous devez être familiarisé avec la syntaxe JSON avant de terminer cette étape.

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
```

Échec de l'installation sur les points de terminaison utilisés pour les mises à niveau

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 **Configuration de l'agent de validation** ou ignorez la vérification de la configuration lors de l'installation dans un VCenter.

NetApp recommande de mettre à jour vos règles de pare-feu pour autoriser l'accès au"points finaux actuels" dans les meilleurs délais. "Apprenez à mettre à jour vos points de terminaison" .

Assurez-vous de vérifier que la seule erreur est liée aux points de terminaison précédents :

- \ https://bluexpinfraprod.eastus2.data.azurecr.io
- \ https://bluexpinfraprod.azurecr.io

S'il y a d'autres erreurs, vous devrez les résoudre avant de continuer.

Travailler avec le support NetApp

Si vous n'avez pas réussi à 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

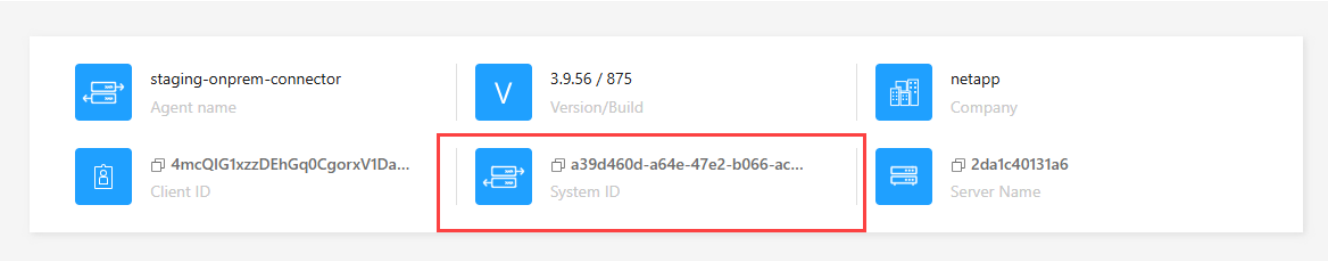
Pour vous aider à démarrer, vous aurez peut-être besoin de l'ID système de votre agent de console. L'ID est généralement utilisé à des fins de licence et de dépannage.

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 console NetApp 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 d'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 console NetApp" .

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 un agent de console est inactif, vous pouvez le supprimer de la liste des agents. Vous pouvez le faire si vous supprimez la machine virtuelle de l'agent ou si vous désinstallez le logiciel de l'agent.

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'action pour un agent inactif et sélectionnez **Supprimer l'agent**.
3. Saisissez le nom de l'agent pour confirmer, puis sélectionnez **Supprimer**.

Configuration par défaut de l'agent de console

Apprenez-en plus sur la configuration de l'agent de console avant de le déployer.

Configuration par défaut avec accès Internet

Les détails de configuration suivants s'appliquent si vous avez déployé un agent de console à partir de la console NetApp , à partir de la place de marché de votre fournisseur de cloud ou si vous avez installé manuellement un agent de console sur un hôte Linux local disposant d'un accès Internet.

Détails AWS

Si vous avez déployé un agent de console à partir de la console ou de la place de marché du fournisseur de cloud, notez les points suivants :

- Le type d'instance EC2 est t3.2xlarge.
- Le système d'exploitation de l'image est Ubuntu 22.04 LTS.

  Le système d'exploitation n'inclut pas d'interface graphique. Vous devez utiliser un terminal pour accéder au système.

- L'installation inclut Docker Engine, qui est l'outil d'orchestration de conteneurs requis.
- Le nom d'utilisateur de l'instance EC2 Linux est ubuntu (pour les agents créés avant mai 2023, le nom d'utilisateur était ec2-user).
- Le disque système par défaut est un disque gp2 de 100 Gio.

Détails Azure

Si vous avez déployé un agent de console à partir de la console ou de la place de marché du fournisseur de cloud, notez les points suivants :

- Le type de machine virtuelle est Standard_D8s_v3.
- Le système d'exploitation de l'image est Ubuntu 22.04 LTS.

  Le système d'exploitation n'inclut pas d'interface graphique. Vous devez utiliser un terminal pour accéder au système.

- L'installation inclut Docker Engine, qui est l'outil d'orchestration de conteneurs requis.
- Le disque système par défaut est un disque SSD premium de 100 Gio.

Détails de Google Cloud

Si vous avez déployé un agent de console à partir de la console, notez les points suivants :

- L'instance de VM est n2-standard-8.
- Le système d'exploitation de l'image est Ubuntu 22.04 LTS.

  Le système d'exploitation n'inclut pas d'interface graphique. Vous devez utiliser un terminal pour accéder au système.

- L'installation inclut Docker Engine, qui est l'outil d'orchestration de conteneurs requis.
- Le disque système par défaut est un disque persistant SSD de 100 Gio.

Dossier d'installation

Le dossier d'installation de l'agent se trouve à l'emplacement suivant :

/opt/application/netapp/cloudmanager

Fichiers journaux

Les fichiers journaux sont contenus dans les dossiers suivants :

- /opt/application/netapp/cloudmanager/log ou
- /opt/application/netapp/service-manager-2/logs (à partir des nouvelles installations 3.9.23)

  Les journaux de ces dossiers fournissent des détails sur l'agent de la console.

- /opt/application/netapp/cloudmanager/docker_occm/data/log

  Les journaux de ce dossier fournissent des détails sur les services cloud et le service de console qui s'exécute sur l'agent de console.

Service d'agent de console

- Le service d'agent de console est nommé occm.
- Le service occm dépend du service MySQL.

  Si le service MySQL est en panne, le service occm l'est également.

Ports

L'agent utilise les ports suivants sur l'hôte Linux :

- 80 pour l'accès HTTP
- 443 pour l'accès HTTPS

Configuration par défaut sans accès Internet

La configuration suivante s'applique si vous avez installé manuellement l'agent de console sur un hôte Linux local qui n'a pas accès à Internet. "En savoir plus sur cette option d'installation" .

- Le dossier d'installation de l'agent se trouve à l'emplacement suivant :

  /opt/application/netapp/ds

- Les fichiers journaux sont contenus dans les dossiers suivants :

  /var/lib/docker/volumes/ds_occmdata/_data/log

  Les journaux de ce dossier fournissent des détails sur l'agent de console et les images Docker.

- Tous les services s'exécutent dans des conteneurs Docker

  Les services dépendent du service d'exécution Docker en cours d'exécution

- L'agent utilise les ports suivants sur l'hôte Linux :
  - 80 pour l'accès HTTP
  - 443 pour l'accès HTTPS

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

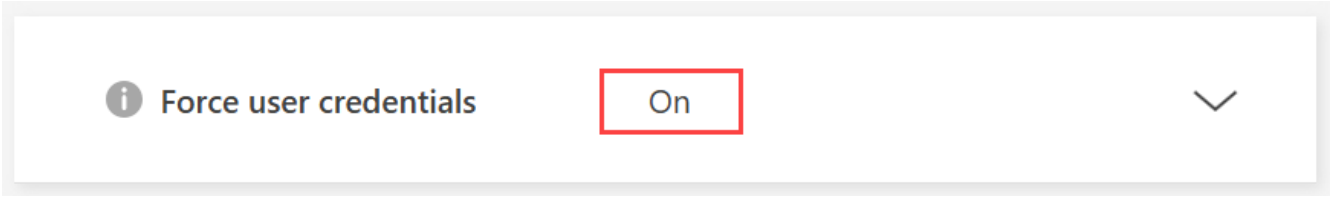
1. Sélectionnez **Administration > Agents**.
2. Sur la page **Aperçu**, sélectionnez le menu d'action pour un agent de console et sélectionnez **Modifier l'agent**.

   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.



Informations d'identification et abonnements

AWS

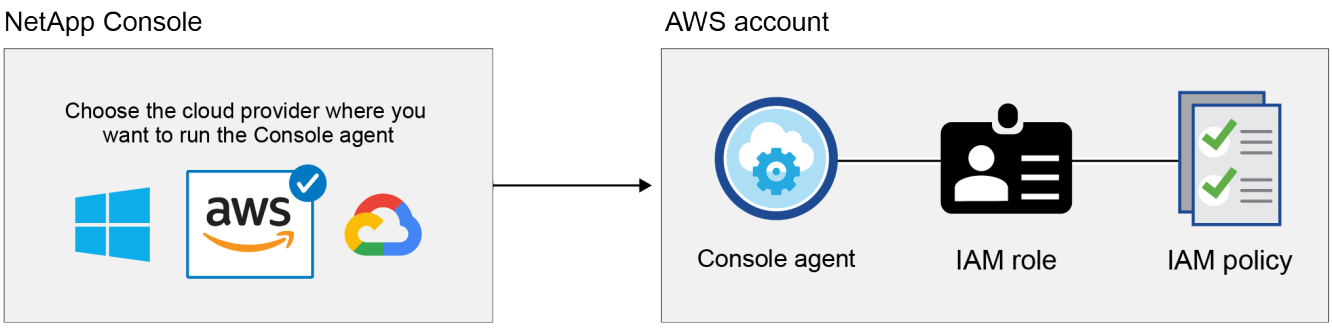
En savoir plus sur les informations d'identification et les autorisations AWS dans la console NetApp

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

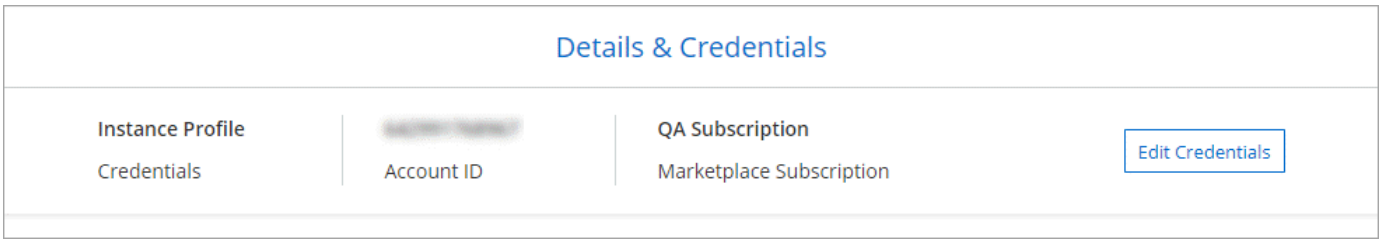
Informations d'identification AWS initiales

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 pour déployer la console dans AWS. Les autorisations requises sont répertoriées dans le lien : task-install-connector-aws-the Console.html#console-permissions-aws[Politique de déploiement de l'agent pour AWS].

Lorsque la console lance l'instance de l'agent de console dans AWS, elle crée un rôle IAM et un profil d'instance pour l'instance. 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. "Examiner comment la console 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

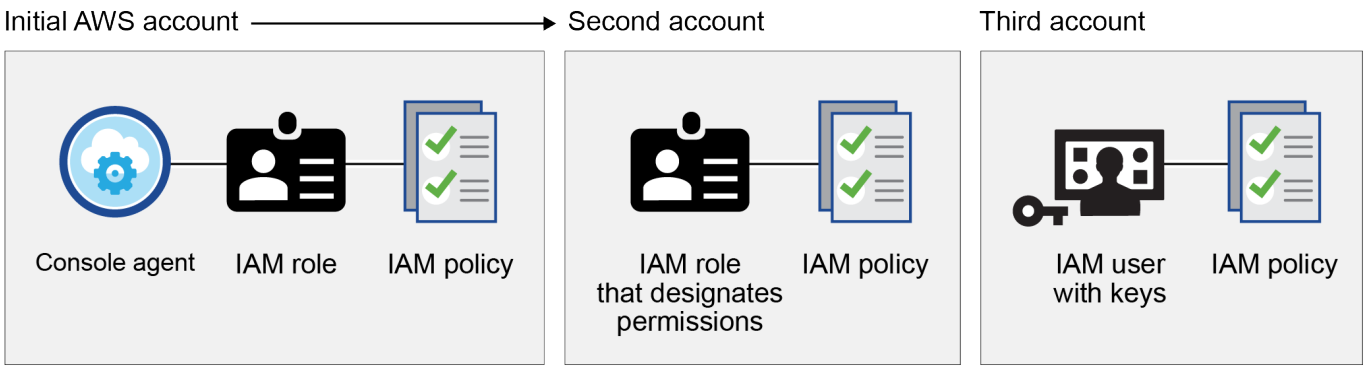
Vous pouvez ajouter des informations d'identification AWS supplémentaires à la console dans les cas suivants :

- Pour utiliser votre agent de 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.

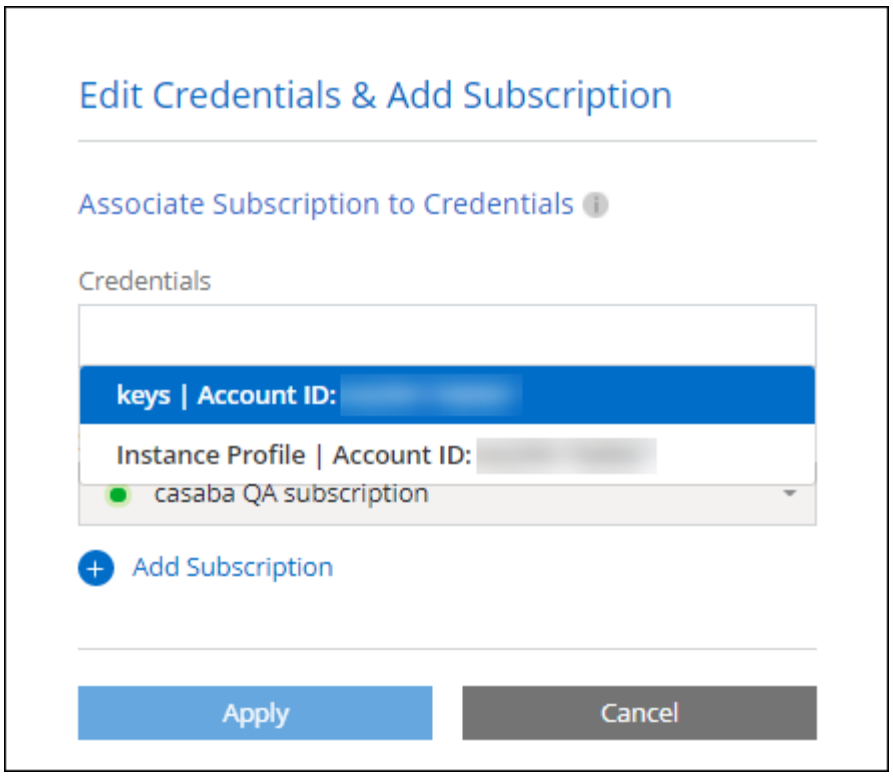
Ajoutez des informations d'identification AWS pour utiliser un agent de console avec un autre compte AWS

Si vous souhaitez utiliser la console avec des comptes AWS supplémentaires, vous pouvez fournir des clés AWS pour un utilisateur IAM ou l'ARN d'un rôle dans un compte approuvé. 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 devez ensuite ajouter 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 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 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

Les informations d'identification que vous ajoutez à un agent de console doivent être associées à un abonnement AWS Marketplace afin que vous puissiez payer Cloud Volumes ONTAP à un tarif horaire (PAYGO) et d'autres services de données NetApp ou via 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'instance de 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 est 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 dans AWS à partir d'AWS Marketplace et installer manuellement le logiciel de l'agent de la console sur votre propre hôte Linux.

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 console NetApp . 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 console NetApp .

- 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 console NetApp 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.

Si vous débutez avec la console,"Découvrez comment la console NetApp 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. "En savoir plus sur les informations d'identification et les autorisations AWS" .

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 une instance d'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 de confiance**, 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"

Résultat

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

Ajoutez les informations d'identification

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.

```
 New credentials in your cloud provider may take a few minutes to become
available. Then, add the credentials.
.Étapes
. Utilisez la barre de navigation supérieure pour sélectionner un agent de
console auquel vous souhaitez ajouter des informations d'identification.
. Dans la barre de navigation de gauche, sélectionnez *Administration >
Informations d'identification*.
. Sur la page *Informations d'identification de l'organisation*,
sélectionnez *Ajouter des informations d'identification* et suivez les
étapes de l'assistant.
```

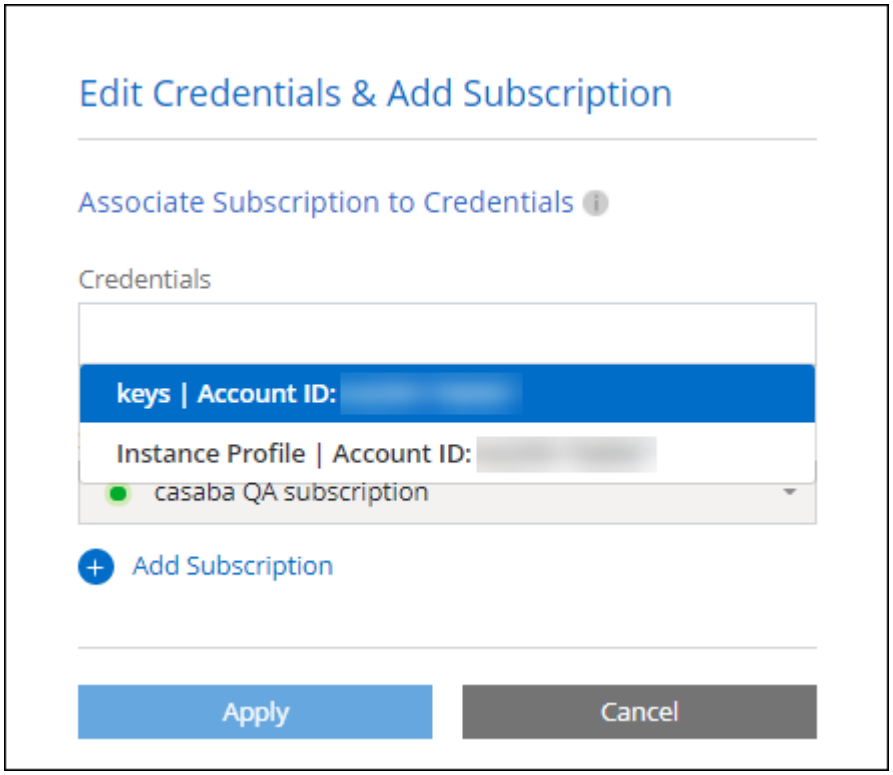
+
.. **Emplacement des informations d'identification** : Sélectionnez **Amazon Web Services > Agent**.
.. **Définir les informations d'identification** : fournissez l'ARN (Amazon Resource Name) d'un rôle IAM approuvé ou saisissez une clé d'accès AWS et une clé secrète.
.. **Abonnement Marketplace** : 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.

a. **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 système 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 console NetApp 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 de confiance**, sélectionnez **Compte AWS**.
   - Sélectionnez **Un autre compte AWS** et saisissez l'ID de la console NetApp 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

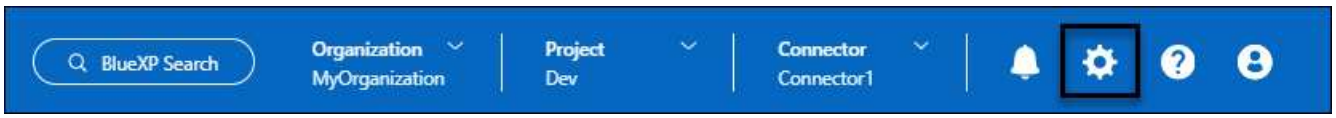
Après avoir fourni au rôle IAM les autorisations requises, ajoutez l'ARN du rôle à la console.

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** ou **Informations d'identification du compte**, sélectionnez **Ajouter des informations d'identification** et suivez les étapes de l'assistant.
   a. **Emplacement des informations d'identification** : sélectionnez *Amazon Web Services > Console NetApp *.
   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 Cloud Volumes ONTAP à un tarif horaire (PAYGO) ou via un contrat annuel, et de payer d'autres services de données.

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" .

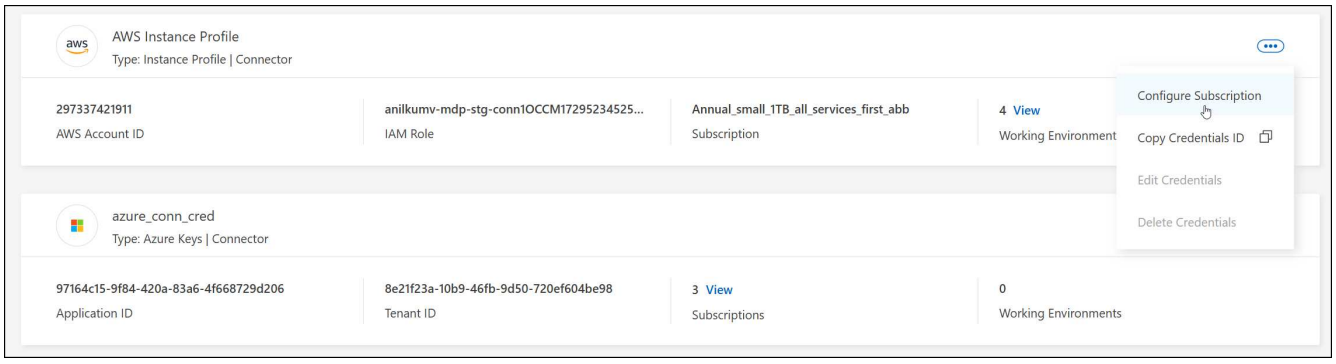
La vidéo suivante montre les étapes à suivre pour s'abonner à NetApp Intelligent Services depuis AWS Marketplace :

Abonnez-vous aux services intelligents NetApp depuis la place de marché AWS

Étapes

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

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



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 console NetApp .

   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 ou à votre compte

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 ou votre compte.

- "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 aux services de données intelligents NetApp 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 ou à votre compte Console.

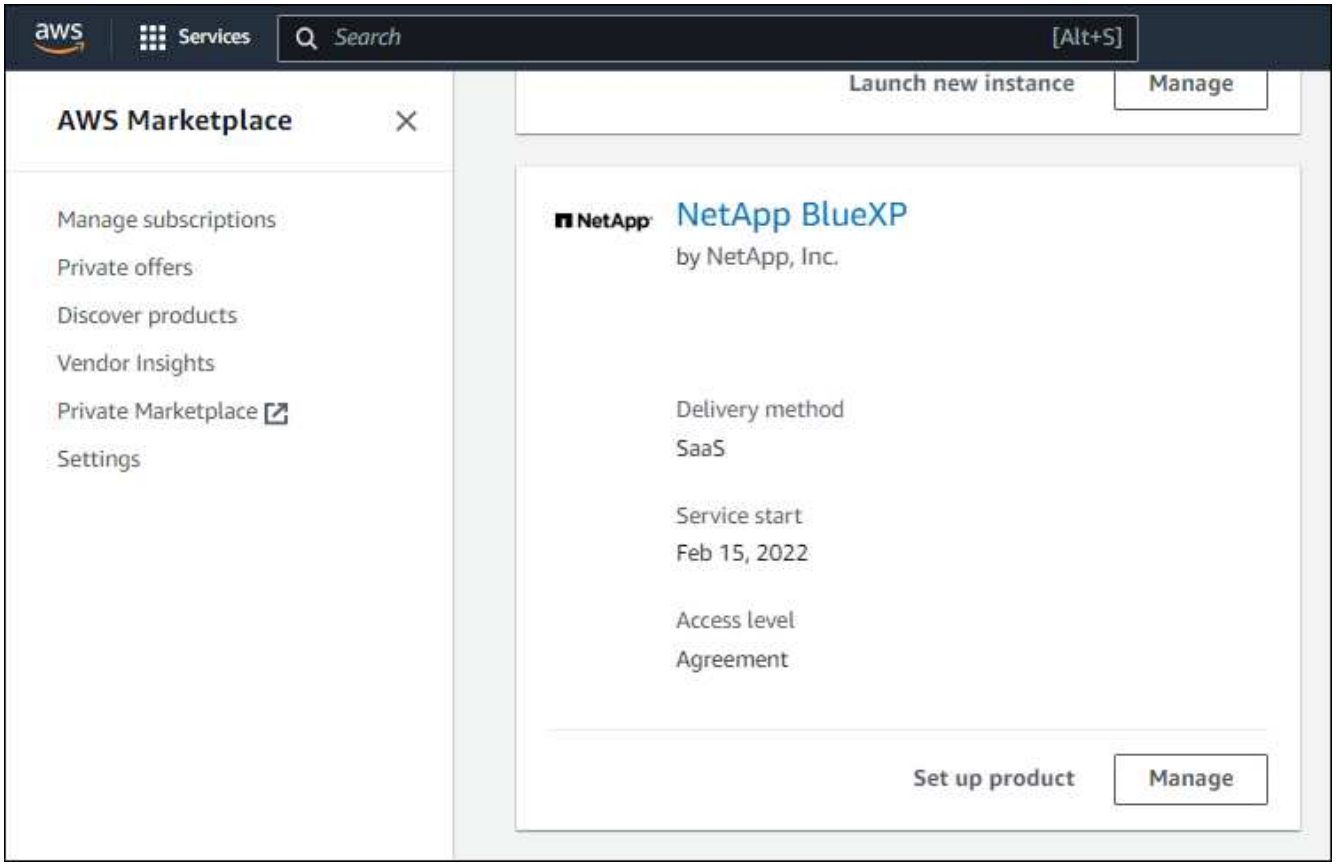
   a. Dans le menu de navigation, sélectionnez **Administration > Licences et abonnements**.

   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.

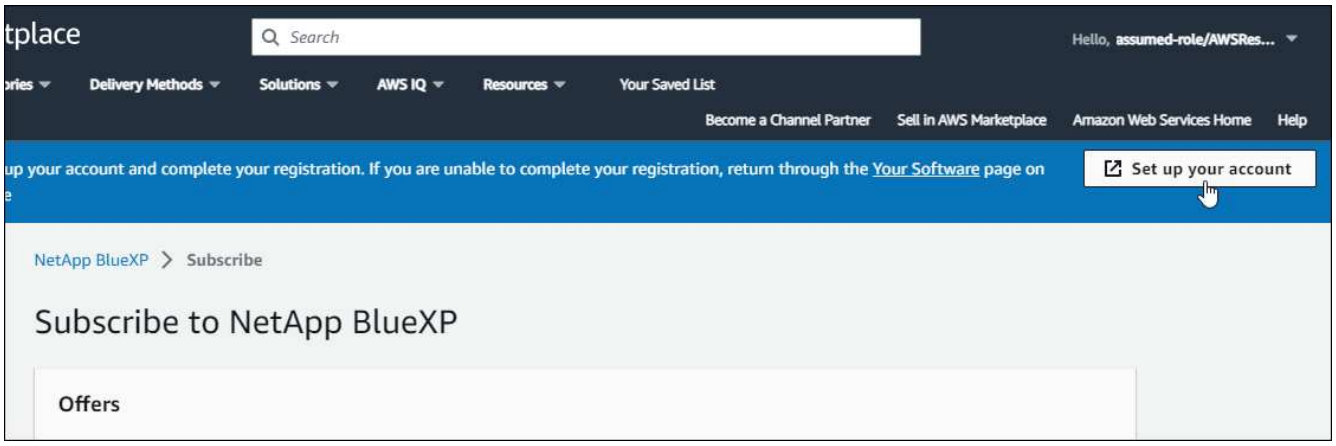
2. Connectez-vous à la console AWS et accédez à **Abonnements AWS Marketplace**.
3. Trouver l'abonnement.



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** :

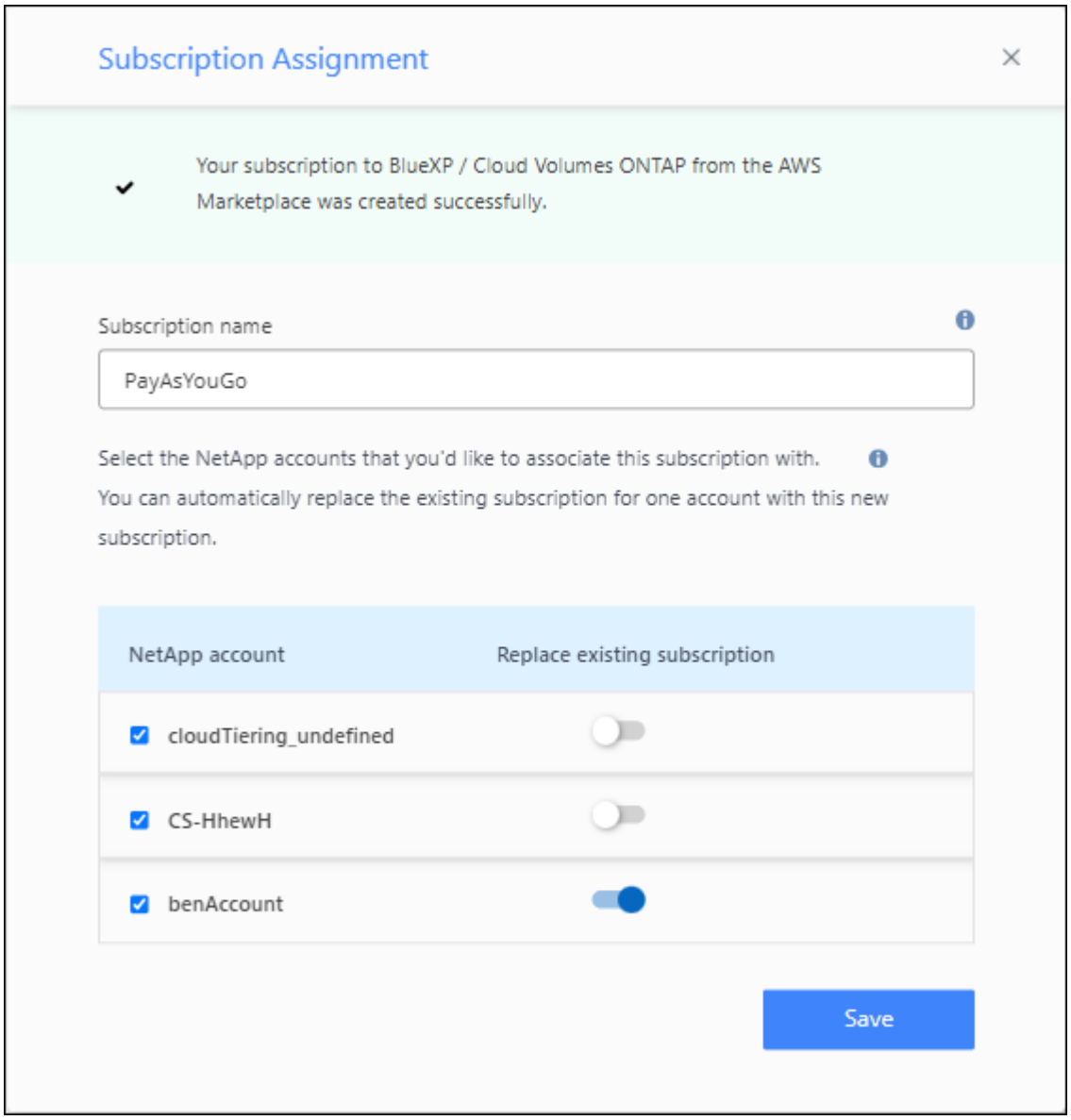
   - Sélectionnez les organisations ou les comptes de la console auxquels vous souhaitez associer cet

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.



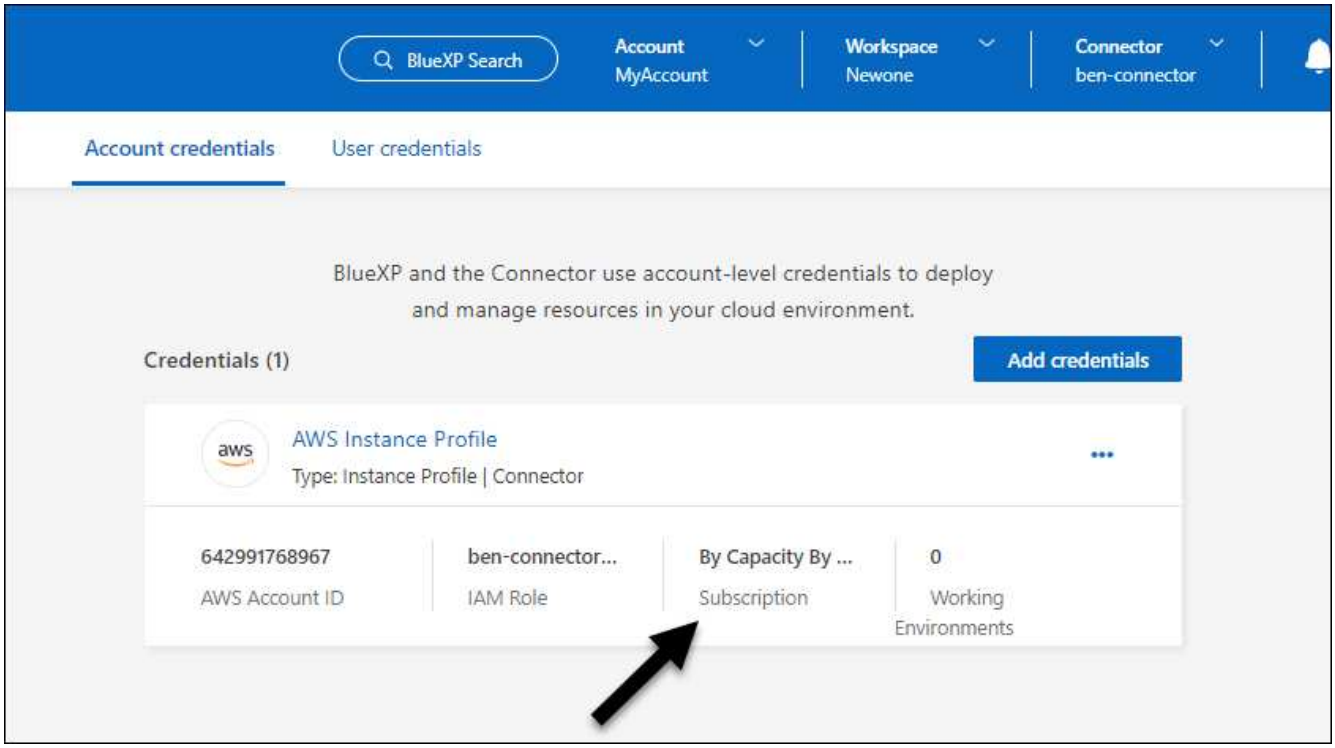
7. Confirmez que l'abonnement est associé à votre organisation ou à votre compte.
   a. Dans le menu de navigation, sélectionnez **Administration > Licences et abonnements**.
   b. Sélectionnez **Abonnements**.
   c. Vérifiez que votre abonnement apparaît.

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

   a. En haut à droite de la console, sélectionnez l'icône Paramètres, puis sélectionnez **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** ou **Informations d'identification du compte**, 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 une instance d'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

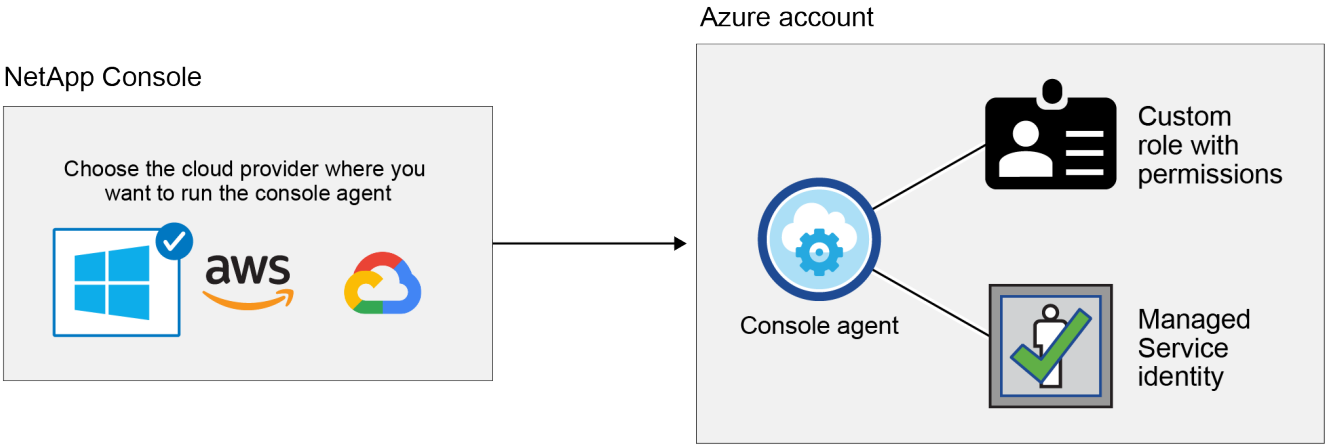
En savoir plus sur les informations d'identification et les autorisations Azure dans la console NetApp

Découvrez comment la console NetApp 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.

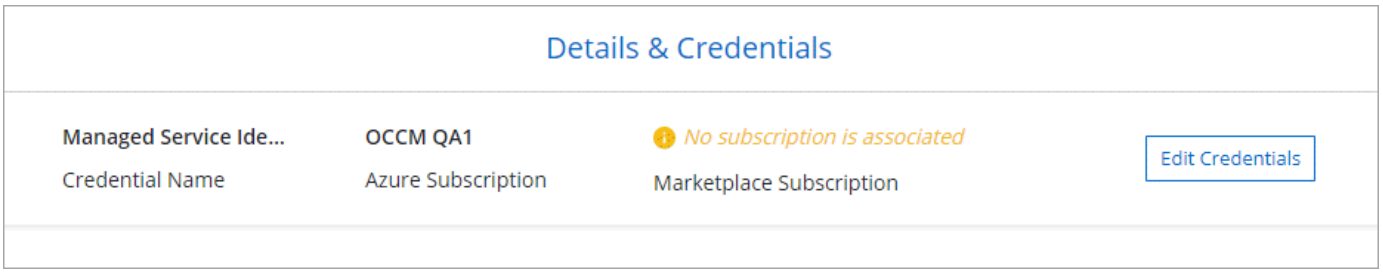
Informations d'identification Azure initiales

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 :



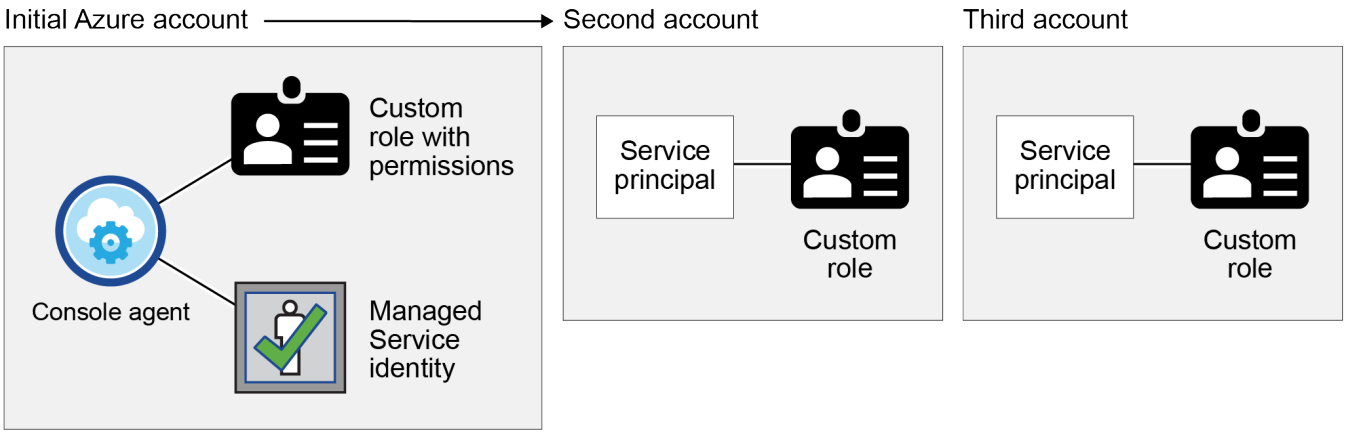
Vous pouvez déployer tous vos systèmes Cloud Volumes ONTAP à l'aide des informations d'identification Azure initiales ou ajouter des informations d'identification supplémentaires.

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" .

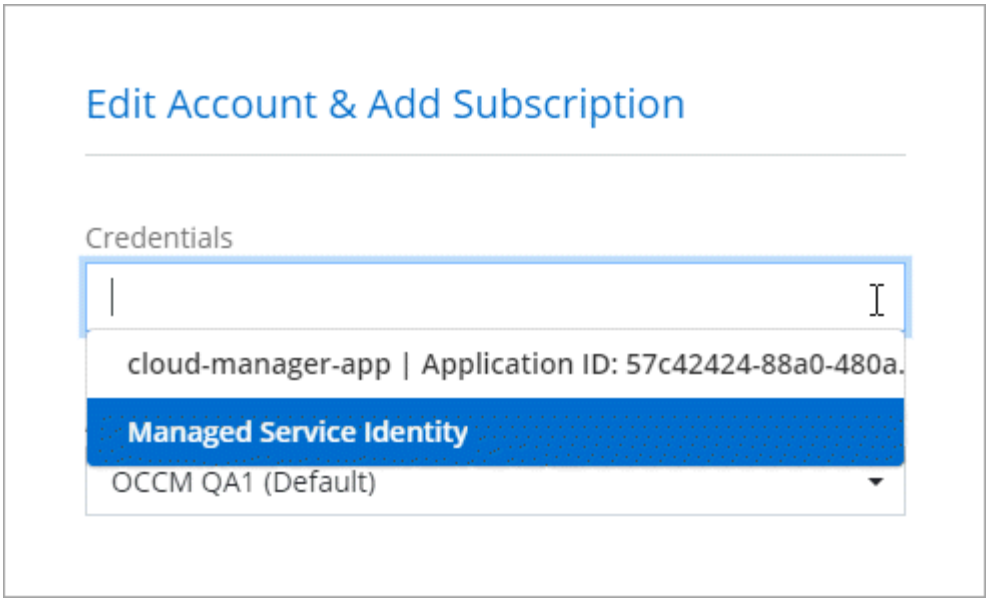
Informations d'identification Azure supplémentaires

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 console NetApp

Ajoutez et gérez les informations d'identification Azure afin que la console NetApp 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 managé, 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

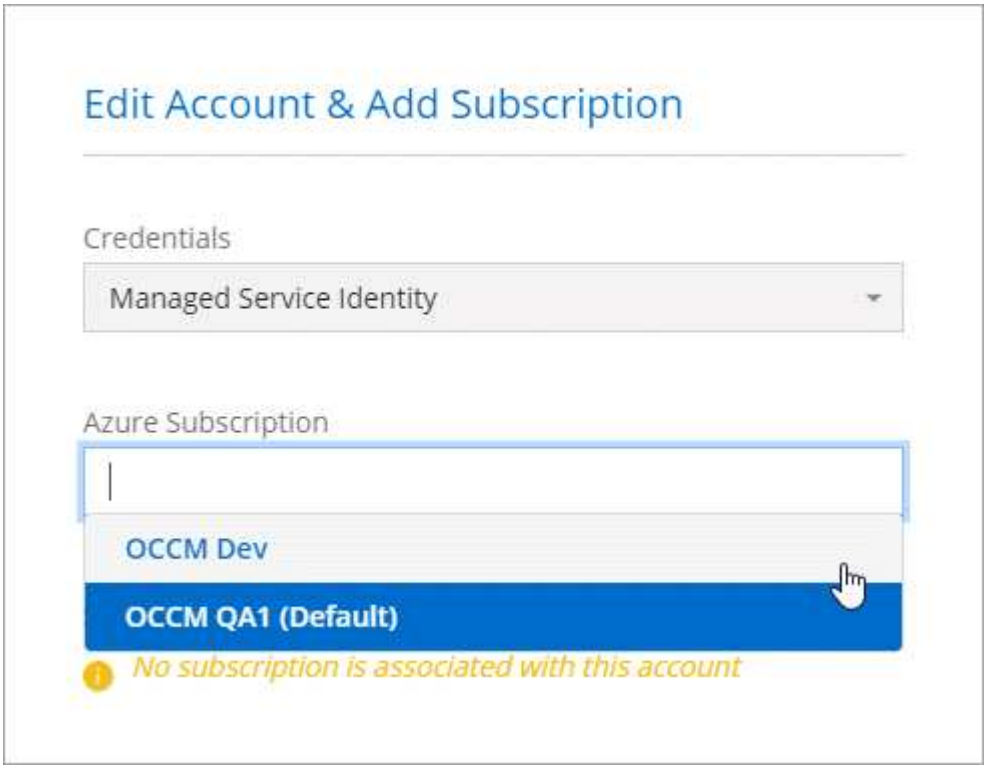
1. Connectez-vous au portail Azure.
2. Ouvrez le service **Abonnements**, puis sélectionnez l'abonnement dans lequel vous souhaitez déployer Cloud Volumes ONTAP.
3. Sélectionnez **Contrôle d'accès (IAM)**.
   a. Sélectionnez **Ajouter** > **Ajouter une attribution de rôle**, puis ajoutez les autorisations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

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" .

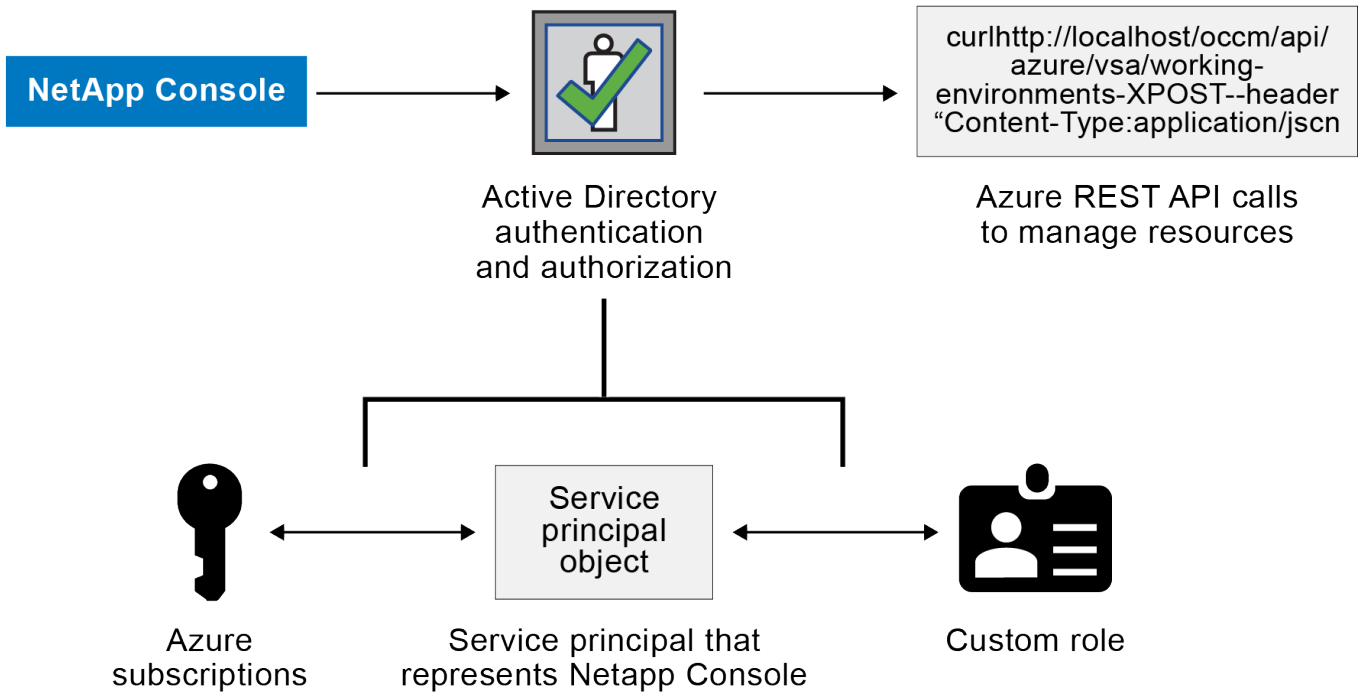
Si vous souhaitez déployer Cloud Volumes ONTAP à l'aide de *différentes* informations d'identification Azure, vous devez accorder les autorisations requises en créant et en configurant un principal de service dans Microsoft Entra ID pour chaque compte Azure. Vous pouvez ensuite ajouter les nouvelles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

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

Créer une application Microsoft Entra

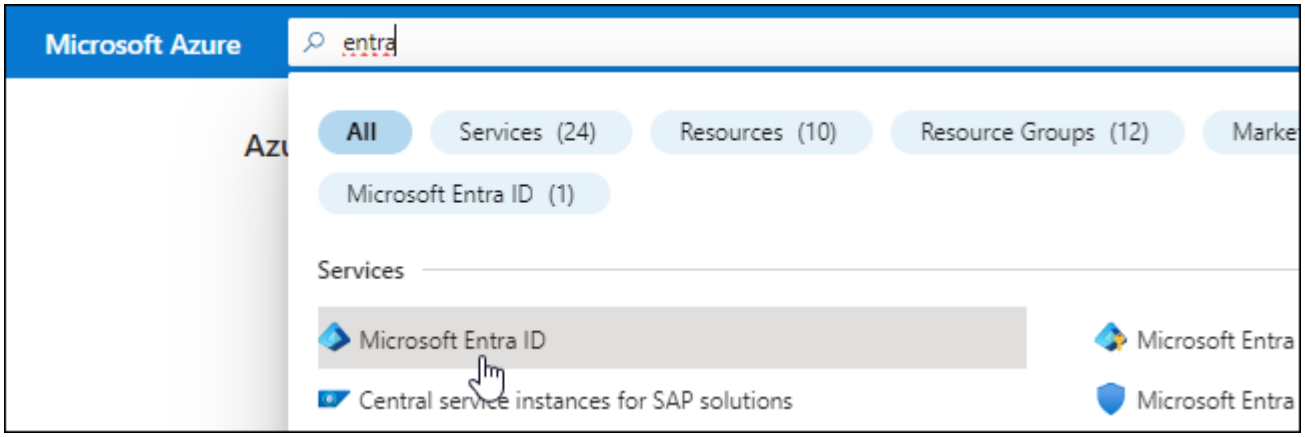
Créez une application Microsoft Entra et un principal de service que la console peut utiliser pour le contrôle d'accès basé sur les rôles.

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 console NetApp).
   - **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 .

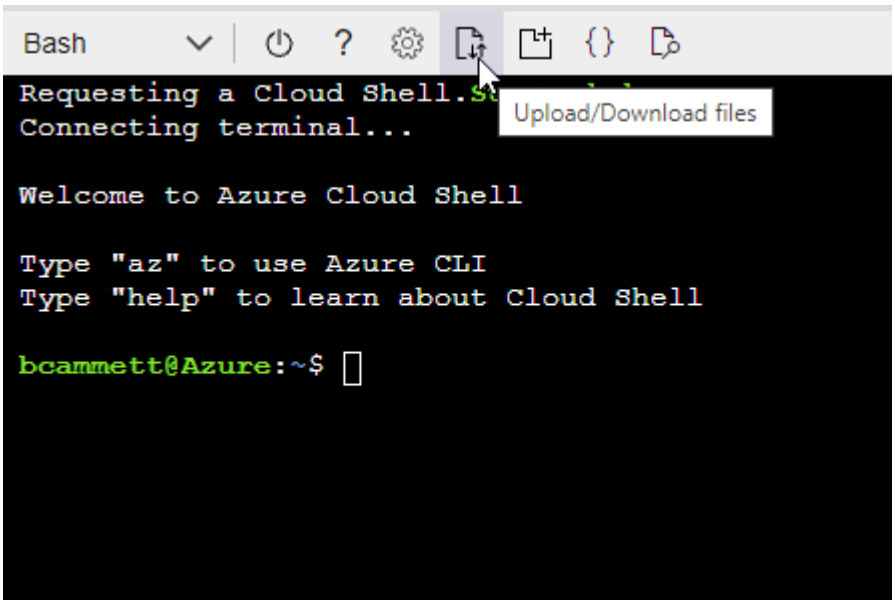
   Exemple

```
"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 Connector_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**.

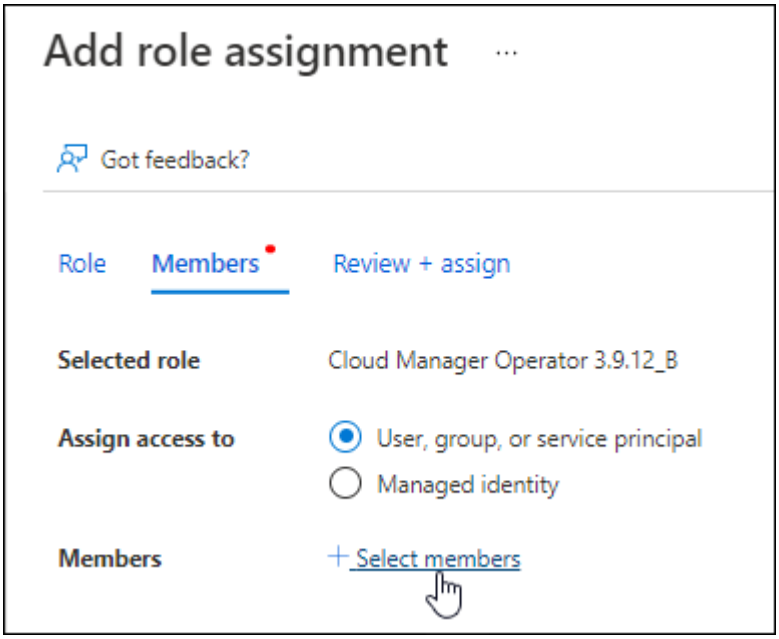
    b. Sélectionnez l'abonnement.

    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**.

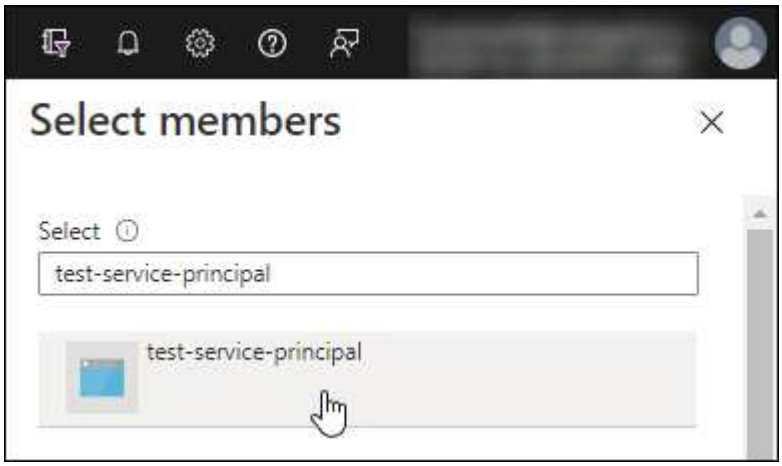
    e. Dans l'onglet **Membres**, procédez comme suit :

    - 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.

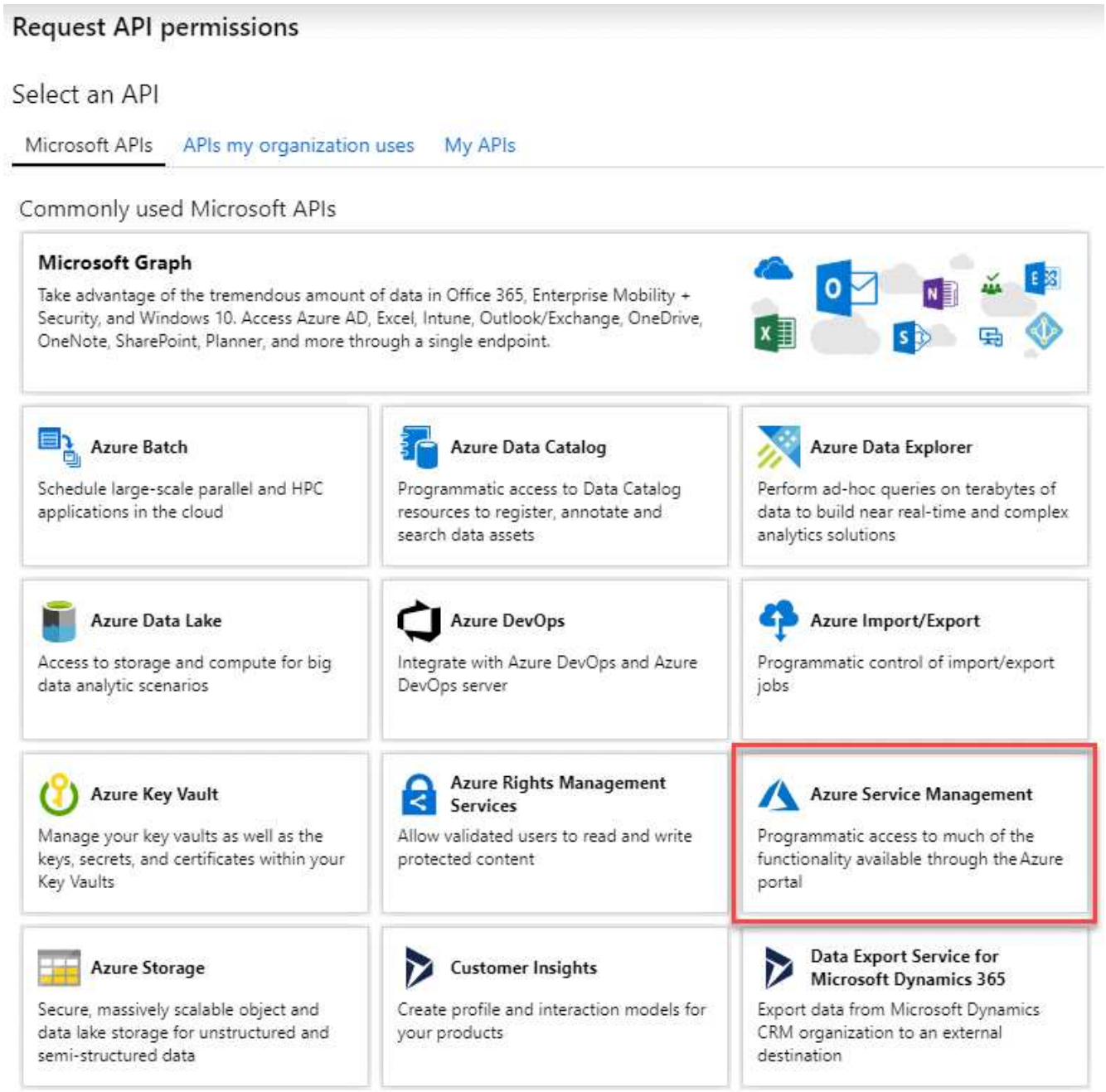
Si vous souhaitez déployer Cloud Volumes ONTAP à partir de plusieurs abonnements Azure, vous devez lier le principal de service à chacun de ces abonnements. Dans la console NetApp , vous pouvez sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

Ajouter des autorisations à l'API de gestion des services Windows Azure

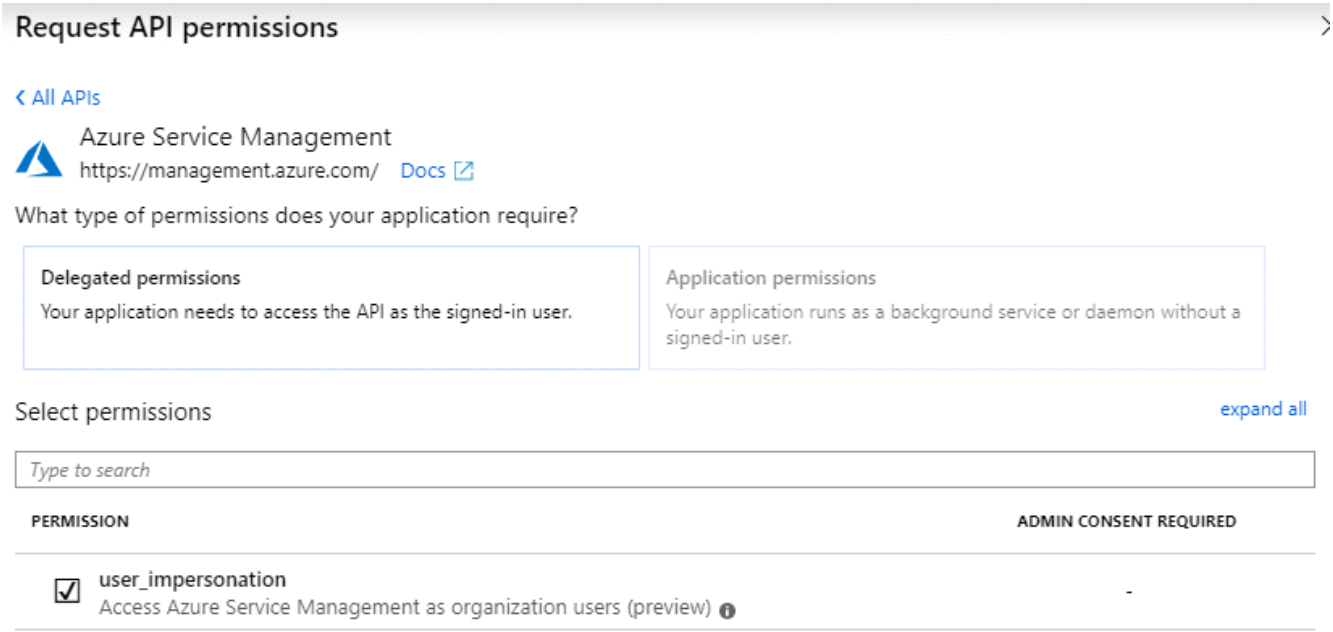
Vous devez attribuer les autorisations « API de gestion des services Windows Azure » au principal du service.

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**.

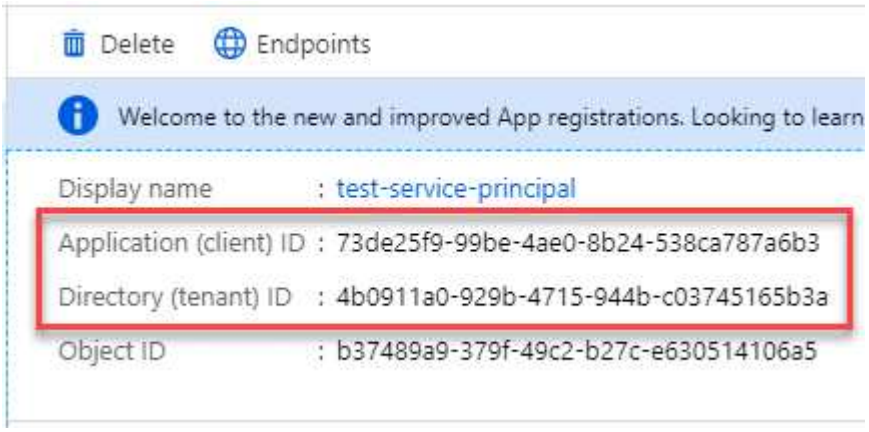


Obtenir l'ID de l'application et l'ID du répertoire

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" .

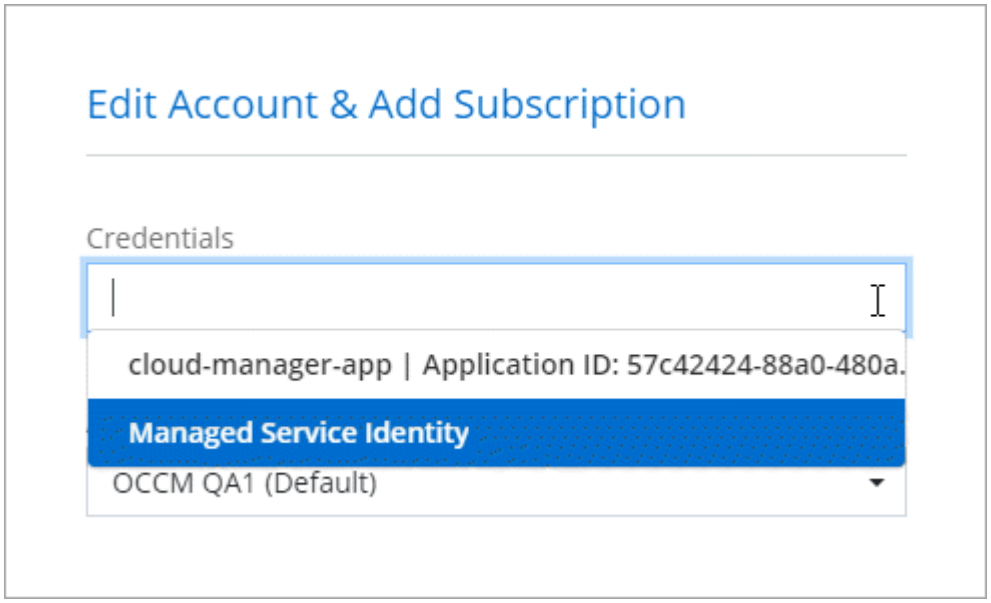
Étapes

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 déjà 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 à la place de marché à des informations d'identification associées à la console NetApp .

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 console NetApp .

   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**.

        La vidéo suivante montre les étapes à suivre pour s'abonner à partir de la Place de marché Azure :

   Abonnez-vous aux services intelligents NetApp depuis la place de marché Azure

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 console NetApp 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.

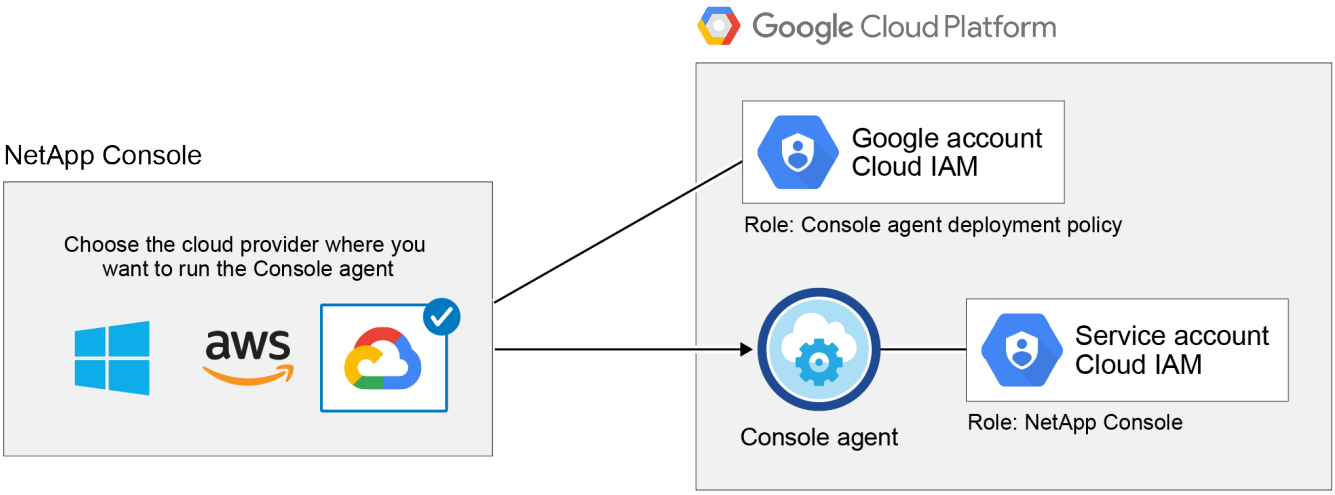
Projet et autorisations pour la console NetApp

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'instance de machine virtuelle de 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'instance VM. 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 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"

Gérer les informations d'identification et les abonnements Google Cloud pour la console NetApp

Vous pouvez gérer les informations d'identification Google Cloud associées à une instance de machine virtuelle d'agent de console en associant un abonnement à la place de marché et en résolvant les problèmes du processus d'abonnement. Ces deux tâches

garantissent que vous pouvez utiliser votre abonnement au marché pour payer les services de données.

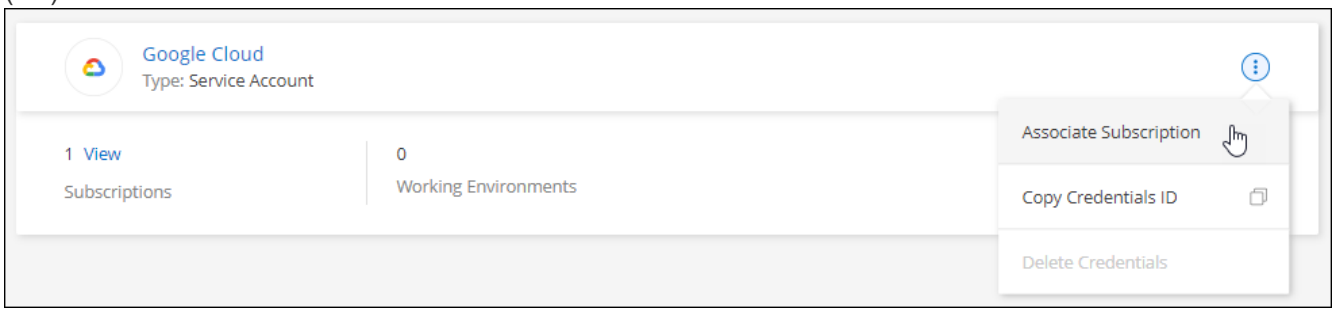
Associer un abonnement Marketplace aux identifiants Google Cloud

Lorsque vous déployez un agent de console dans Google Cloud, la console crée un ensemble d'informations d'identification par défaut associées à une instance de machine virtuelle d'agent de console. À tout moment, vous pouvez modifier l'abonnement Google Cloud Marketplace associé à ces informations d'identification. L'abonnement vous permet de créer un système Cloud Volumes ONTAP à la carte et d'utiliser d'autres services de données.

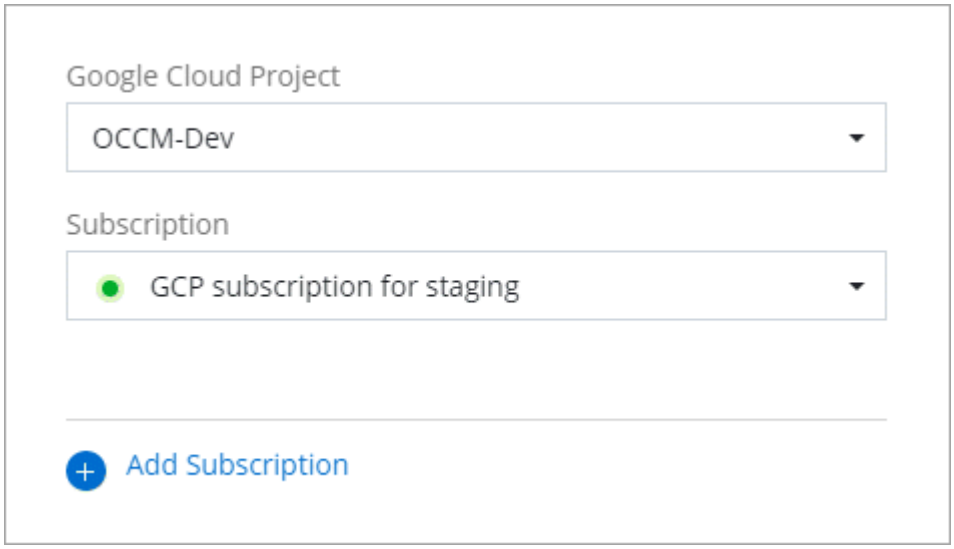
Le remplacement de l'abonnement actuel au marché par un nouvel abonnement modifie l'abonnement au marché pour tous les systèmes Cloud Volumes ONTAP existants et tous les nouveaux systèmes.

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**. + nouvelle capture d'écran nécessaire (TS)



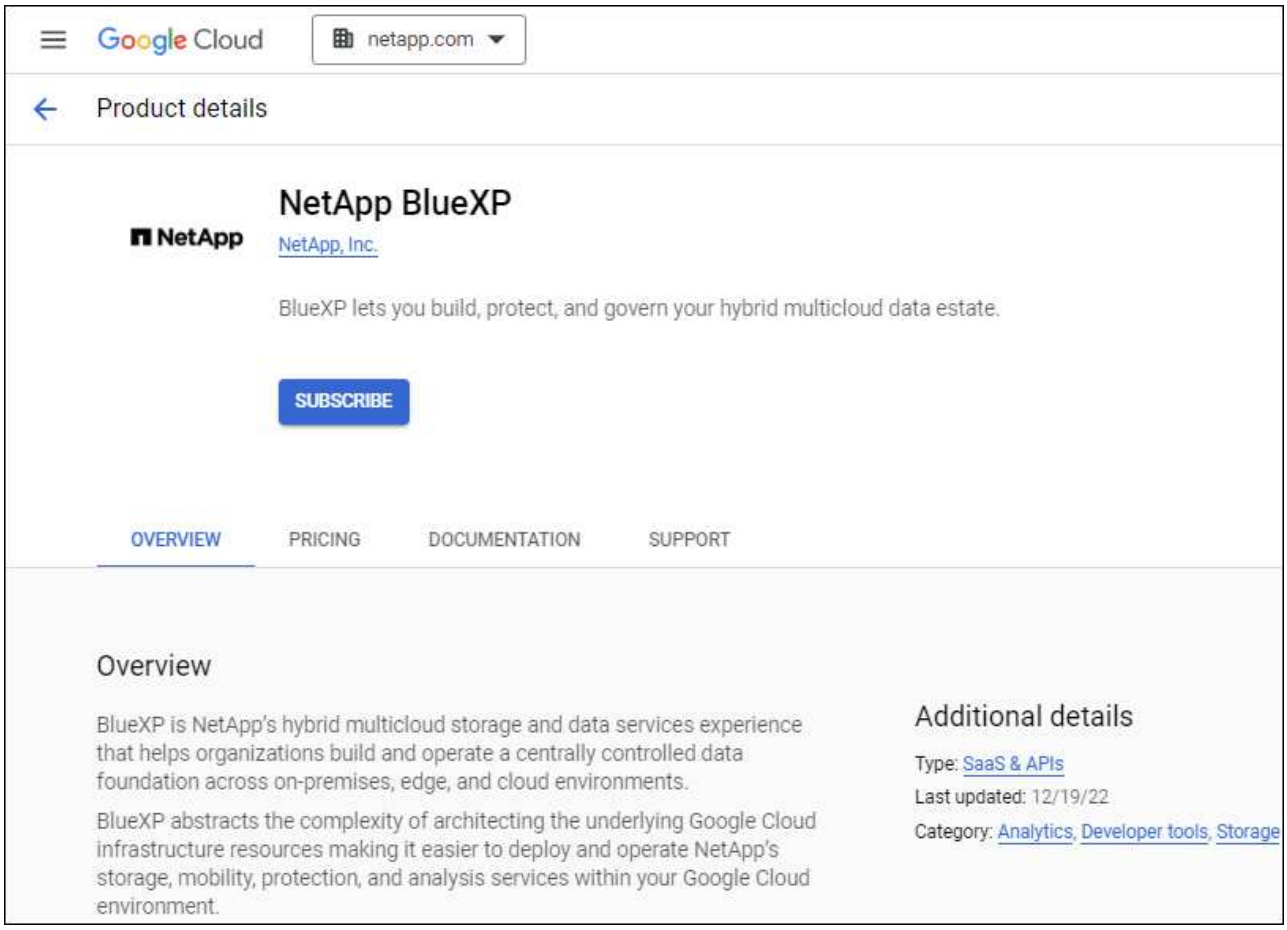
4. Pour configurer un abonnement existant avec les informations d'identification sélectionnées, sélectionnez un projet et un abonnement Google Cloud dans la liste déroulante, puis sélectionnez **Configurer**.



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

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

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



b. Sélectionnez **S'abonner**.

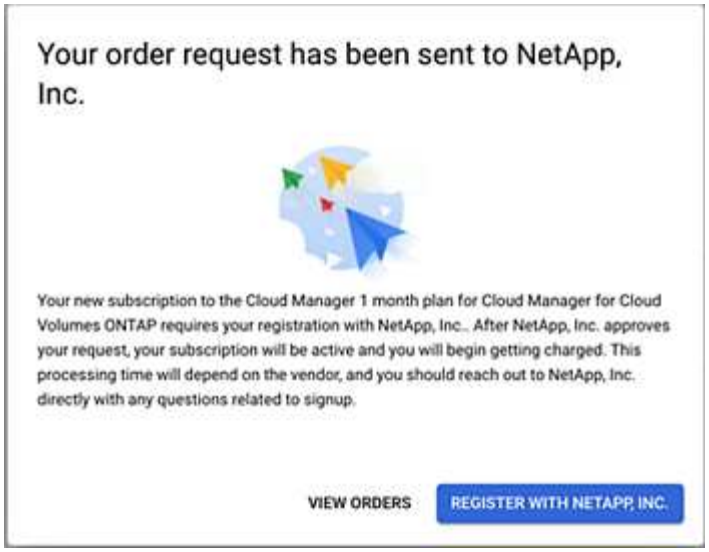
c. Sélectionnez le compte de facturation approprié et acceptez les conditions générales.

d. Sélectionnez **S'abonner**.

Cette étape envoie votre demande de transfert à NetApp.

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

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



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

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

- 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.

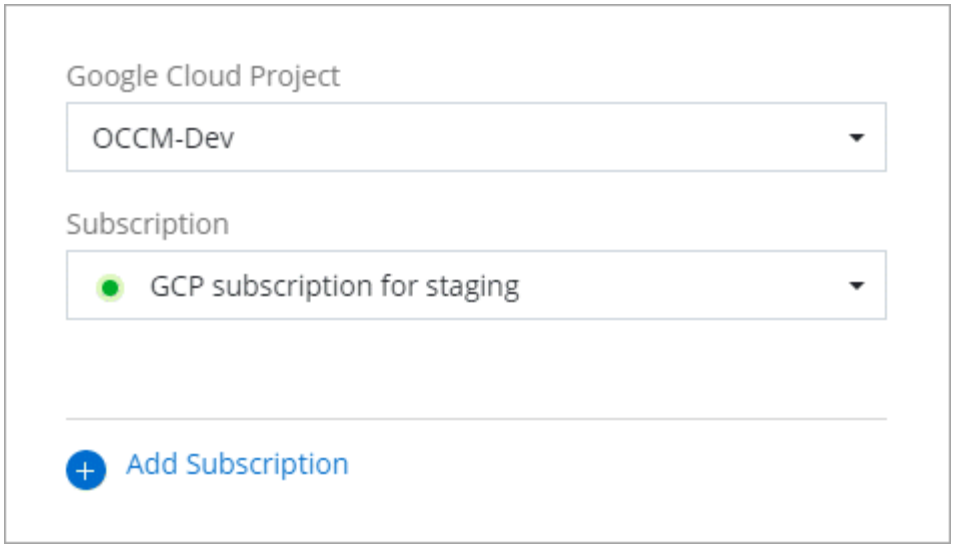
Pour toutes les autres organisations ou comptes, vous devrez associer manuellement l'abonnement en répétant ces étapes.

- Sélectionnez **Enregistrer**.

  La vidéo suivante montre les étapes à suivre pour s'abonner à partir de Google Cloud Marketplace :

Abonnez-vous à Google Cloud Marketplace

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

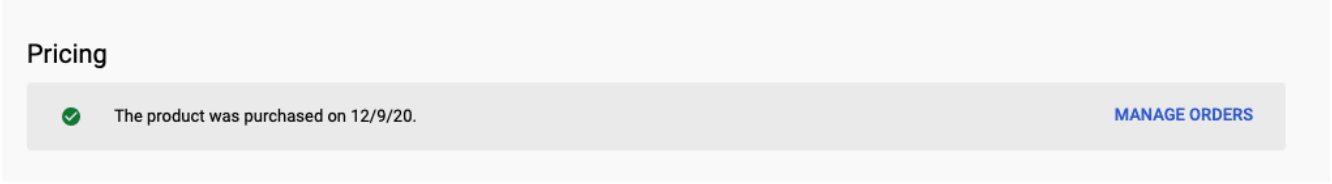


Résoudre les problèmes liés au processus d'abonnement à la Marketplace

Parfois, l'abonnement aux services de données NetApp via Google Cloud Marketplace peut devenir fragmenté en raison d'autorisations incorrectes ou du non-respect accidentel de la redirection vers la console. Si cela se produit, suivez les étapes suivantes pour terminer le processus d'abonnement.

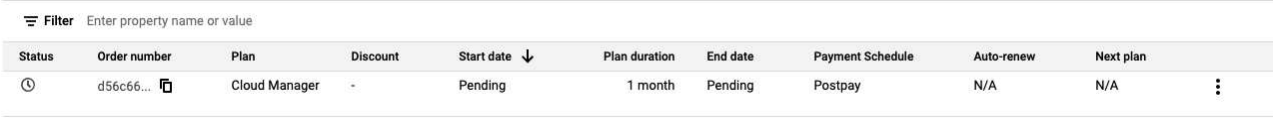
Étapes

1. Accédez au "Page NetApp sur Google Cloud Marketplace" pour vérifier l'état de la commande. Si la page indique **Gérer sur le fournisseur**, faites défiler vers le bas et sélectionnez **Gérer les commandes**.



   - Si la commande affiche une coche verte et que cela est inattendu, il est possible qu'une autre personne de l'organisation utilisant le même compte de facturation soit déjà abonnée. Si cela est inattendu ou si vous avez besoin des détails de cet abonnement, contactez votre équipe commerciale NetApp .

   - Si la commande affiche une horloge et le statut **En attente**, revenez à la page du marché et choisissez **Gérer sur le fournisseur** pour terminer le processus comme indiqué ci-dessus.



Gérer les informations d'identification NSS associées à la console NetApp

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 .

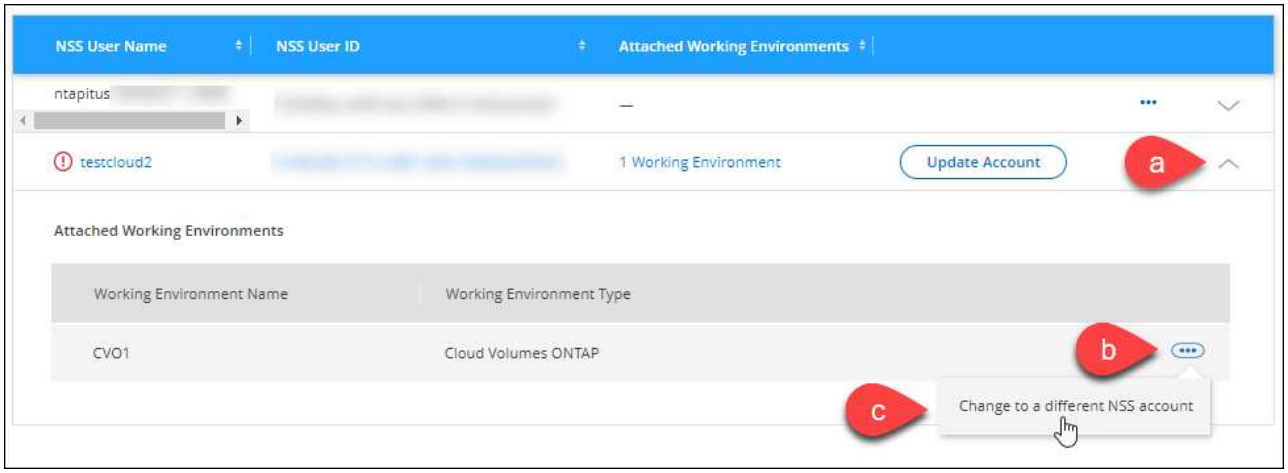
Attacher un système à un autre compte NSS

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 compte NSS différent .

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 console NetApp

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 console NetApp 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.

Surveiller les opérations de la console NetApp

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

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.

Utilisez la page Audit pour identifier qui a effectué une action ou son statut.

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 à partir de 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 console NetApp"

Types de notifications

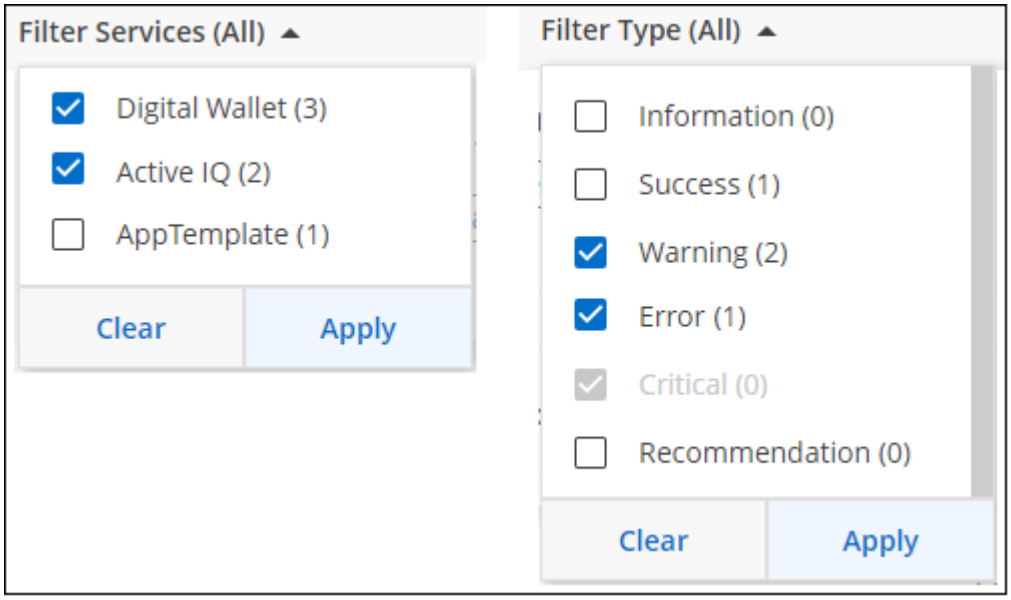
La console classe les notifications dans les catégories suivantes :

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.

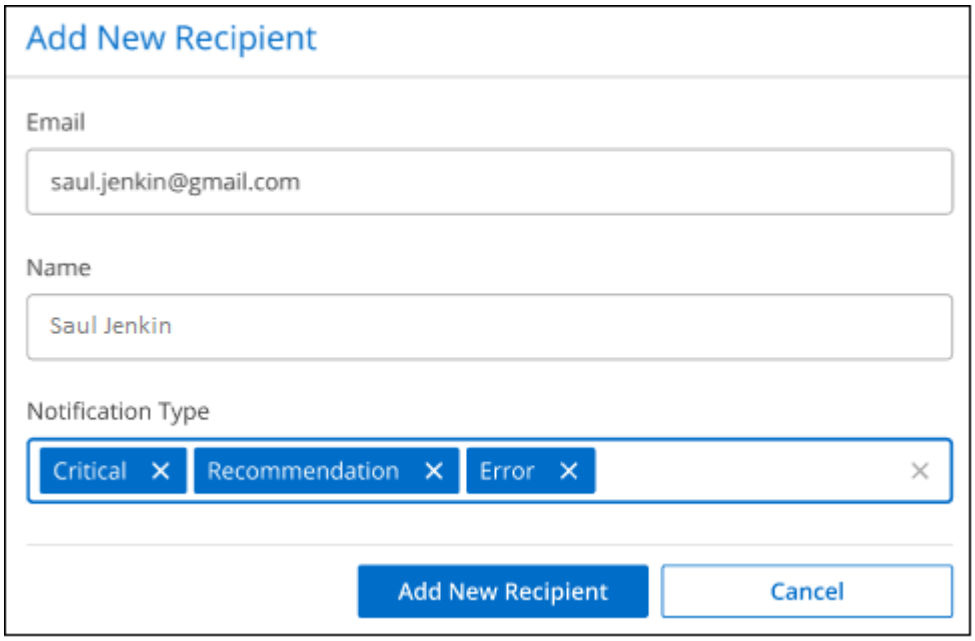
3. Sélectionnez un ou plusieurs utilisateurs à partir de la page *Utilisateurs de l'organisation* ou de la page *Destinataires supplémentaires* et choisissez le type de notifications à envoyer :
   - Pour apporter des modifications à un seul utilisateur, sélectionnez le menu dans la colonne Notifications 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**.

Référence

Console de maintenance des agents

Console de maintenance de l'agent de console

Vous pouvez utiliser la console de maintenance de l'agent de console pour configurer un agent de console afin d'utiliser un serveur proxy transparent.

Accéder à la console de maintenance de l'agent

Vous pouvez accéder à la console de maintenance à partir de l'hôte de l'agent de console. Accédez au répertoire suivant :

```
/opt/application/netapp/service-manager-2/agent-maint-console
```

Commandes proxy transparentes

La console de maintenance de l'agent fournit des commandes pour configurer l'agent afin d'utiliser un serveur proxy transparent.

Afficher la configuration actuelle du proxy transparent

Pour afficher la configuration actuelle du proxy transparent, utilisez la commande suivante :

```
./agent-maint-console proxy get
```

Ajouter un serveur proxy transparent

Pour ajouter un serveur proxy transparent, utilisez la commande suivante, où `/home/ubuntu/myCA1.pem` est le chemin d'accès au fichier de certificat pour le serveur proxy. Le fichier de certificat doit être au format PEM :

```
./agent-maint-console proxy add -c /home/ubuntu/myCA1.pem
```

Assurez-vous que le fichier de certificat se trouve dans le même répertoire que la commande ou spécifiez le chemin d'accès complet au fichier de certificat.

Mettre à jour le certificat pour un serveur proxy transparent

Pour mettre à jour le certificat d'un serveur proxy transparent, utilisez la commande suivante, où `/home/ubuntu/myCA1.pem` est le chemin vers le nouveau fichier de certificat pour le serveur proxy. Le fichier de certificat doit être au format PEM :

```
./agent-maint-console proxy update -c /home/ubuntu/myCA1.pem
```

Assurez-vous que le fichier de certificat se trouve dans le même répertoire que la commande ou spécifiez le chemin d'accès complet au fichier de certificat.

Supprimer un serveur proxy transparent

Pour supprimer le serveur proxy transparent, utilisez la commande suivante :

```
./agent-maint-console proxy remove
```

Afficher l'aide pour n'importe quelle commande

Pour afficher l'aide d'une commande, ajoutez `--help` à la commande. Par exemple, pour afficher l'aide relative à la `proxy add` commande, utilisez la commande suivante :

```
./agent-maint-console proxy add --help
```

Autorisations

Résumé des autorisations pour la console NetApp

Pour utiliser les fonctionnalités et services de la console NetApp , vous devez fournir des autorisations afin que la console puisse effectuer des opérations dans votre environnement cloud. Utilisez les liens sur cette page pour accéder rapidement aux autorisations dont vous avez besoin en fonction de votre objectif.

Autorisations AWS

La console NetApp nécessite des autorisations AWS pour un agent de console et pour des services individuels.

Agents de console

But	Description	Lien
Déployer un agent de console à partir de la console	L'utilisateur qui crée un agent de console à partir de la console a besoin d'autorisations spécifiques pour déployer l'instance dans AWS.	"Configurer les autorisations AWS"
Fournir des autorisations pour un agent de console	Lorsque la console déploie un agent de console, elle attache une stratégie à l'instance qui fournit les autorisations requises pour gérer les ressources et les processus de votre compte AWS. Vous devez configurer la politique vous-même si vous déployez un agent de console à partir d'AWS Marketplace, si vous installez manuellement un agent de console ou si vous"ajouter plus d'informations d'identification AWS à un agent de console" . Vous devez également vous assurer que la politique est à jour à mesure que de nouvelles autorisations sont ajoutées dans les versions ultérieures.	"Autorisations AWS pour un agent de console"

Sauvegarde et récupération NetApp

But	Description	Lien
Sauvegardez les clusters ONTAP sur site sur Amazon S3 avec NetApp Backup and Recovery	Lors de l'activation des sauvegardes sur vos volumes ONTAP , NetApp Backup and Recovery vous invite à saisir une clé d'accès et un secret pour un utilisateur IAM disposant d'autorisations spécifiques.	"Configurer les autorisations S3 pour les sauvegardes"

Cloud Volumes ONTAP

But	Description	Lien
Fournir des autorisations pour les nœuds Cloud Volumes ONTAP	Un rôle IAM doit être attaché à chaque nœud Cloud Volumes ONTAP dans AWS. Il en va de même pour le médiateur HA. L'option par défaut consiste à laisser la console créer les rôles IAM pour vous, mais vous pouvez utiliser les vôtres lors de la création du système dans la console.	"Apprenez à configurer vous-même les rôles IAM"

Copie et synchronisation NetApp

But	Description	Lien
Déployer le courtier de données dans AWS	Le compte utilisateur AWS que vous utilisez pour déployer le courtier de données doit disposer d'autorisations spécifiques.	"Autorisations requises pour déployer le courtier de données dans AWS"
Fournir des autorisations au courtier de données	Lorsque NetApp Copy and Sync déploie le courtier de données, il crée un rôle IAM pour l'instance du courtier de données. Vous pouvez déployer le courtier de données à l'aide de votre propre rôle IAM, si vous préférez.	"Conditions requises pour utiliser votre propre rôle IAM avec le courtier de données AWS"
Activer l'accès AWS pour un courtier de données installé manuellement	Si vous utilisez le courtier de données avec une relation de synchronisation qui inclut un bucket S3, vous devez préparer l'hôte Linux pour l'accès AWS. Lorsque vous installez le courtier de données, vous devez fournir des clés AWS pour un utilisateur IAM disposant d'un accès programmatique et d'autorisations spécifiques.	"Activation de l'accès à AWS"

FSx pour ONTAP

But	Description	Lien
Créer et gérer FSx pour ONTAP	Pour créer ou gérer un système Amazon FSx for NetApp ONTAP , vous devez ajouter des informations d'identification AWS à la console en fournissant l'ARN d'un rôle IAM qui donne à la console les autorisations nécessaires.	"Découvrez comment configurer les informations d'identification AWS pour FSx"

Hiérarchisation du cloud NetApp

But	Description	Lien
Hiérarchiser les clusters ONTAP sur site vers Amazon S3	Lorsque vous activez NetApp Cloud Tiering sur AWS, l'assistant vous invite à saisir une clé d'accès et une clé secrète. Ces informations d'identification sont transmises au cluster ONTAP afin ONTAP puisse hiérarchiser les données vers le compartiment S3.	"Configurer les autorisations S3 pour la hiérarchisation"

Autorisations Azure

La console nécessite des autorisations Azure pour un agent de console et pour des services individuels.

Agent de console

But	Description	Lien
Déployer un agent de console à partir de la console	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 une machine virtuelle d'agent de console dans Azure.	"Configurer les autorisations Azure"
Fournir des autorisations pour un agent de console	Lorsque la console déploie une machine virtuelle d'agent de console dans Azure, elle crée un rôle personnalisé qui fournit les autorisations requises pour gérer les ressources et les processus au sein de cet abonnement Azure. Vous devez configurer vous-même le rôle personnalisé si vous lancez un agent de console à partir de la place de marché, si vous installez manuellement un agent de console ou si vous"ajouter plus d'informations d'identification Azure à un agent de console" . Vous devez également vous assurer que la politique est à jour à mesure que de nouvelles autorisations sont ajoutées dans les versions ultérieures.	"Autorisations Azure pour un agent de console"

Sauvegarde et récupération NetApp

But	Description	Lien
Sauvegarder Cloud Volumes ONTAP sur le stockage blob Azure	Lorsque vous utilisez NetApp Backup and Recovery pour sauvegarder Cloud Volumes ONTAP, vous devez ajouter des autorisations à un agent de console dans les scénarios suivants : • Vous souhaitez utiliser la fonctionnalité « Rechercher et restaurer » • Vous souhaitez utiliser des clés de chiffrement gérées par le client (CMEK)	• "Sauvegardez les données Cloud Volumes ONTAP sur le stockage Azure Blob avec Backup and Recovery"

But	Description	Lien
Sauvegarder les clusters ONTAP locaux sur le stockage blob Azure	Lorsque vous utilisez NetApp Backup and Recovery pour sauvegarder des clusters ONTAP sur site, vous devez ajouter des autorisations à un agent de console afin d'utiliser la fonctionnalité « Rechercher et restaurer ».	"Sauvegardez les données ONTAP locales sur le stockage Azure Blob avec Backup and Recovery"

Copie et synchronisation NetApp

But	Description	Lien
Déployer le courtier de données dans Azure	Le compte d'utilisateur Azure que vous utilisez pour déployer le courtier de données doit disposer des autorisations requises.	"Autorisations requises pour déployer le courtier de données dans Azure"

Autorisations Google Cloud

La console nécessite des autorisations Google Cloud pour un agent de console et pour des services individuels.

Agents de console

But	Description	Lien
Déployer un agent de console à partir de la console	L'utilisateur Google Cloud qui déploie un agent de console à partir de la console a besoin d'autorisations spécifiques pour déployer un agent de console dans Google Cloud.	"Configurer les autorisations pour créer un agent de console"
Fournir des autorisations pour un agent de console	Le compte de service d'une instance de machine virtuelle d'agent de console doit disposer d'autorisations spécifiques pour les opérations quotidiennes. Vous devez associer le compte de service à un agent de console pendant le déploiement. Vous devez également vous assurer que la politique est à jour à mesure que de nouvelles autorisations sont ajoutées dans les versions ultérieures.	"Configurer les autorisations pour un agent de console"

Sauvegarde et récupération NetApp

But	Description	Lien
Sauvegarder Cloud Volumes ONTAP sur Google Cloud	Lorsque vous utilisez NetApp Backup and Recovery pour sauvegarder Cloud Volumes ONTAP, vous devez ajouter des autorisations à un agent de console dans les scénarios suivants : • Vous souhaitez utiliser la fonctionnalité « Rechercher et restaurer » • Vous souhaitez utiliser des clés de chiffrement gérées par le client (CMEK)	• "Sauvegardez les données Cloud Volumes ONTAP sur Google Cloud Storage avec Backup and Recovery" • "Autorisations pour les CMEK"
Sauvegarder les clusters ONTAP sur site sur Google Cloud	Lorsque vous utilisez NetApp Backup and Recovery pour sauvegarder des clusters ONTAP sur site, vous devez ajouter des autorisations à un agent de console afin d'utiliser la fonctionnalité « Rechercher et restaurer ».	"Sauvegardez les données ONTAP sur site sur Google Cloud Storage avec Backup and Recovery"

Copie et synchronisation NetApp

But	Description	Lien
Déployer le courtier de données dans Google Cloud	Assurez-vous que l'utilisateur Google Cloud qui déploie le courtier de données dispose des autorisations requises.	"Autorisations requises pour déployer le courtier de données dans Google Cloud"
Activer l'accès à Google Cloud pour un courtier de données installé manuellement	Si vous prévoyez d'utiliser le courtier de données avec une relation de synchronisation qui inclut un bucket Google Cloud Storage, vous devez préparer l'hôte Linux pour l'accès à Google Cloud. Lorsque vous installez le courtier de données, vous devez fournir une clé pour un compte de service disposant d'autorisations spécifiques.	"Activation de l'accès à Google Cloud"

Autorisations StorageGRID

La console nécessite des autorisations StorageGRID pour deux services.

Sauvegarde et récupération NetApp

But	Description	Lien
Sauvegarder les clusters ONTAP sur site sur StorageGRID	Lorsque vous préparez StorageGRID comme cible de sauvegarde pour les clusters ONTAP , NetApp Backup and Recovery vous invite à saisir une clé d'accès et un secret pour un utilisateur IAM disposant d'autorisations spécifiques.	"Préparez StorageGRID comme cible de sauvegarde"

Hiérarchisation du cloud NetApp

But	Description	Lien
Hiérarchiser les clusters ONTAP sur site vers StorageGRID	Lorsque vous configurez NetApp Cloud Tiering sur StorageGRID, vous devez fournir à Cloud Tiering une clé d'accès S3 et une clé secrète. La hiérarchisation du cloud utilise les clés pour accéder à vos buckets.	"Préparer la hiérarchisation vers StorageGRID"

Autorisations AWS pour l'agent de la console

Lorsque la console NetApp lance une instance d'agent de console dans AWS, elle attache une stratégie à l'instance qui fournit à l'agent des autorisations pour gérer les ressources et les processus au sein de ce compte AWS. L'agent utilise les autorisations pour effectuer des appels d'API vers plusieurs services AWS, notamment EC2, S3, CloudFormation, IAM, le service de gestion des clés (KMS), etc.

Politiques IAM

Les stratégies IAM disponibles ci-dessous fournissent les autorisations dont un agent de console a besoin pour gérer les ressources et les processus au sein de votre environnement de cloud public en fonction de votre région AWS.

Notez ce qui suit :

- Si vous créez un agent de console dans une région AWS standard directement à partir de la console, la console applique automatiquement des stratégies à l'agent.
- Vous devez configurer les stratégies vous-même si vous déployez l'agent à partir d'AWS Marketplace, si vous installez manuellement l'agent sur un hôte Linux ou si vous souhaitez ajouter des informations d'identification AWS supplémentaires à la console.
- Dans les deux cas, vous devez vous assurer que les politiques sont à jour 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.
- Si nécessaire, vous pouvez restreindre les politiques IAM en utilisant l'IAM `Condition` élément. "Documentation AWS : élément de condition"
- Pour consulter les instructions étape par étape pour utiliser ces politiques, reportez-vous aux pages suivantes :
  - "Configurer les autorisations pour un déploiement AWS Marketplace"
  - "Configurer les autorisations pour les déploiements sur site"
  - "Configurer les autorisations pour le mode restreint"

Sélectionnez votre région pour afficher les politiques requises :

Régions standard

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.

Politique n°1

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DescribeTags",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:CreatePlacementGroup",
                "ec2:DescribeReservedInstancesOfferings",
                "ec2:AssignPrivateIpAddresses",
                "ec2:CreateRoute",
                "ec2:DescribeVpcs",
                "ec2:ReplaceRoute",
```

```
                "ec2:UnassignPrivateIpAddresses",
                "ec2:DeleteSecurityGroup",
                "ec2:DeleteNetworkInterface",
                "ec2:DeleteSnapshot",
                "ec2:DeleteTags",
                "ec2:DeleteRoute",
                "ec2:DeletePlacementGroup",
                "ec2:DescribePlacementGroups",
                "ec2:DescribeVolumesModifications",
                "ec2:ModifyVolume",
                "cloudformation:CreateStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "cloudformation:DeleteStack",
                "iam:PassRole",
                "iam:CreateRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:ListInstanceProfiles",
                "iam:DeleteRole",
                "iam:DeleteRolePolicy",
                "iam:DeleteInstanceProfile",
                "iam:GetRolePolicy",
                "iam:GetRole",
                "sts:DecodeAuthorizationMessage",
                "sts:AssumeRole",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketPolicy",
                "s3:GetBucketAcl",
                "s3:PutObjectTagging",
                "s3:GetObjectTagging",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:PutObject",
                "s3:ListAllMyBuckets",
                "s3:GetObject",
```

```
                "s3:GetEncryptionConfiguration",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "fsx:Describe*",
                "fsx:List*",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "cvoServicePolicy"
        },
        {
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "kms:List*",
                "kms:Describe*",
                "ec2:DescribeVpcEndpoints",
                "kms:ListAliases",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
                "glue:BatchCreatePartition",
                "glue:BatchDeletePartition"
```

```
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "backupPolicy"
        },
        {
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketAcl",
                "s3:PutBucketPublicAccessBlock",
                "s3:GetObject",
                "s3:PutEncryptionConfiguration",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts",
                "s3:DeleteBucket",
                "s3:GetObjectVersionTagging",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:PutObjectVersionTagging",
                "s3:PutObjectRetention",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketVersioning",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning",
                "s3:BypassGovernanceRetention",
                "s3:PutBucketPolicy",
                "s3:PutBucketOwnershipControls"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
```

```
            ],
            "Effect": "Allow",
            "Sid": "backupS3Policy"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:DeleteBucket"
            ],
            "Resource": [
                "arn:aws:s3:::fabric-pool*"
            ],
            "Effect": "Allow",
            "Sid": "fabricPoolS3Policy"
        },
        {
            "Action": [
                "ec2:DescribeRegions"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "fabricPoolPolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/netapp-adc-manager": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
```

```
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume",
                "ec2:StopInstances",
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
        {
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Action": [
                "ec2:DeleteVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:volume/*"
            ],
            "Effect": "Allow"
        }
    ]
```

```
}
```

Politique n° 2

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Action": [
                "ec2:CreateTags",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "tag:getResources",
                "tag:getTagKeys",
                "tag:getTagValues",
                "tag:TagResources",
                "tag:UntagResources"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "tagServicePolicy"
        }
    ]
}
```

Régions GovCloud (États-Unis)

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "iam:ListInstanceProfiles",
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "ec2:ModifyVolumeAttribute",
                "sts:DecodeAuthorizationMessage",
                "ec2:DescribeImages",
                "ec2:DescribeRouteTables",
                "ec2:DescribeInstances",
                "iam:PassRole",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:DeleteVolume",
                "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:CreateSnapshot",
                "ec2:DeleteSnapshot",
```

```
                "ec2:DescribeSnapshots",
                "ec2:StopInstances",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:CreateBucket",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
```

```
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::fabric-pool*"
            ]
        },
        {
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws-us-gov:s3:::netapp-backup-*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
```

```
                "arn:aws-us-gov:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-us-gov:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Régions secrètes

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
```

```
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso-b:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Régions top secrètes

```
{
    "Version": "2012-10-17",
    "Statement": [{
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:ModifyInstanceAttribute",
                "ec2:DescribeRouteTables",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:DescribeVolumes",
                "ec2:ModifyVolumeAttribute",
                "ec2:DeleteVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DeleteSecurityGroup",
                "ec2:DescribeSecurityGroups",
                "ec2:RevokeSecurityGroupEgress",
                "ec2:RevokeSecurityGroupIngress",
                "ec2:AuthorizeSecurityGroupEgress",
                "ec2:AuthorizeSecurityGroupIngress",
                "ec2:CreateNetworkInterface",
                "ec2:DescribeNetworkInterfaces",
                "ec2:DeleteNetworkInterface",
                "ec2:ModifyNetworkInterfaceAttribute",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeDhcpOptions",
                "ec2:CreateSnapshot",
                "ec2:DeleteSnapshot",
                "ec2:DescribeSnapshots",
                "ec2:GetConsoleOutput",
                "ec2:DescribeKeyPairs",
                "ec2:DescribeRegions",
                "ec2:DeleteTags",
                "ec2:DescribeTags",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:ValidateTemplate",
                "iam:PassRole",
```

```
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:PutRolePolicy",
                "iam:CreateInstanceProfile",
                "iam:DeleteRolePolicy",
                "iam:AddRoleToInstanceProfile",
                "iam:RemoveRoleFromInstanceProfile",
                "iam:DeleteInstanceProfile",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "kms:List*",
                "kms:Describe*",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ec2:CreatePlacementGroup",
                "ec2:DeletePlacementGroup",
                "iam:ListinstanceProfiles"
            ],
            "Resource": "*"
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions"
            ],
            "Resource": [
                "arn:aws-iso:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

```
                "ec2:DetachVolume"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/WorkingEnvironment": "*"
                }
            },
            "Resource": [
                "arn:aws-iso:ec2:*:*:instance/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws-iso:ec2:*:*:volume/*"
            ]
        }
    ]
}
```

Comment les autorisations AWS sont utilisées

Les sections suivantes décrivent comment les autorisations sont utilisées pour chaque service de gestion ou de données de la console NetApp . Ces informations peuvent être utiles si les politiques de votre entreprise stipulent que les autorisations ne sont accordées qu'en cas de besoin.

Amazon FSx pour ONTAP

L'agent de console effectue les requêtes API suivantes pour gérer un système de fichiers Amazon FSx for ONTAP :

- ec2 : Décrire les instances
- ec2 : Décrire l'état de l'instance
- ec2 : Décrire l'attribut d'instance
- ec2 : Décrire les tables d'itinéraires
- ec2:Décrire les images
- ec2:Créer des balises
- ec2 : Décrire les volumes
- ec2 : Décrire les groupes de sécurité
- ec2 : Décrire les interfaces réseau

- ec2 : Décrire les sous-réseaux
- ec2 : Décrire les Vpcs
- ec2 : Décrire les options DHCP
- ec2 : Décrire les instantanés
- ec2 : Décrire les paires de clés
- ec2 : Décrire les régions
- ec2:Décrire les balises
- ec2 : Décrire les associations de profils d'instance Iam
- ec2 : Décrire les offres d'instances réservées
- ec2 : Décrire les points de terminaison Vpc
- ec2 : Décrire les Vpcs
- ec2 : Décrire les modifications des volumes
- ec2 : Décrire les groupes de placement
- kms:Liste*
- kms:Décrire*
- kms:Créer une subvention
- kms:ListeAliases
- fsx:Décrire*
- fsx:Liste*

Découverte de compartiment Amazon S3

L'agent de la console effectue la demande d'API suivante pour découvrir les compartiments Amazon S3 :

s3 : Obtenir la configuration du chiffrement

Sauvegarde et récupération NetApp

L'agent effectue les requêtes API suivantes pour gérer les sauvegardes dans Amazon S3 :

- s3 : Obtenir l'emplacement du bucket
- s3 : ListeTousMesSeaux
- s3:ListBucket
- s3:Créer un bucket
- s3 : Obtenir la configuration du cycle de vie
- s3 : PutLifecycleConfiguration
- s3 : Mettre en place le balisage du bucket
- s3 : ListBucketVersions
- s3 : Obtenir l'Acl du bucket
- s3 : PutBucketPublicAccessBlock
- kms:Liste*

- kms:Décrire*
- s3:Obtenir l'objet
- ec2 : Décrire les points de terminaison Vpc
- kms:ListeAliases
- s3 : PutEncryptionConfiguration

L'agent effectue les requêtes API suivantes lorsque vous utilisez la méthode Rechercher et restaurer pour restaurer des volumes et des fichiers :

- s3:Créer un bucket
- s3:Supprimer l'objet
- s3 : Supprimer la version de l'objet
- s3 : Obtenir l'Acl du bucket
- s3:ListBucket
- s3 : ListBucketVersions
- s3 : ListBucketMultipartUploads
- s3:PutObject
- s3:PutBucketAcl
- s3 : PutLifecycleConfiguration
- s3 : PutBucketPublicAccessBlock
- s3 : Abandonner le téléchargement en plusieurs parties
- s3 : ListeMultipartUploadParts
- athena:Démarrer l'exécution de la requête
- athéna:Obtenir les résultats de la requête
- athéna:GetQueryExecution
- athena:StopQueryExecution
- colle:Créer une base de données
- colle:Créer une table
- colle:Suppression par lots de partitions

L'agent effectue les requêtes API suivantes lorsque vous utilisez DataLock et NetApp Ransomware Resilience pour vos sauvegardes de volume :

- s3 : Obtenir le balisage de la version de l'objet
- s3 : GetBucketObjectLockConfiguration
- s3 : ObtenirObjectVersionAcl
- s3 : Mettre en place un balisage d'objet
- s3:Supprimer l'objet
- s3 : Supprimer le balisage d'objet
- s3 : Obtenir la rétention d'objet

- s3 : Supprimer le balisage de version d'objet
- s3:PutObject
- s3:Obtenir l'objet
- s3 : PutBucketObjectLockConfiguration
- s3 : Obtenir la configuration du cycle de vie
- s3 : ListBucketByTags
- s3 : Obtenir le balisage du bucket
- s3 : Supprimer la version de l'objet
- s3 : ListBucketVersions
- s3:ListBucket
- s3 : Mettre en place le balisage du bucket
- s3 : Obtenir le balisage des objets
- s3 : PutBucketVersioning
- s3 : Mettre en place la version de l'objet
- s3 : Obtenir la gestion des versions du bucket
- s3 : Obtenir l'Acl du bucket
- s3 : Contournement de la gouvernance et de la rétention
- s3 : PutObjectRetention
- s3 : Obtenir l'emplacement du bucket
- s3 : Obtenir la version de l'objet

L'agent effectue les requêtes API suivantes si vous utilisez un compte AWS différent pour vos sauvegardes Cloud Volumes ONTAP de celui que vous utilisez pour les volumes sources :

- s3 : PutBucketPolicy
- s3 : PutBucketOwnershipControls

Classification

L'agent effectue les requêtes API suivantes pour déployer la classification des données NetApp :

- ec2 : Décrire les instances
- ec2 : Décrire l'état de l'instance
- ec2 : Exécuter les instances
- ec2 : Terminer les instances
- ec2:Créer des balises
- ec2:Créer un volume
- ec2:AttachVolume
- ec2 : Créer un groupe de sécurité
- ec2 : Supprimer le groupe de sécurité
- ec2 : Décrire les groupes de sécurité

- ec2 : Créer une interface réseau
- ec2 : Décrire les interfaces réseau
- ec2 : Supprimer l'interface réseau
- ec2 : Décrire les sous-réseaux
- ec2 : Décrire les Vpcs
- ec2:Créer un instantané
- ec2 : Décrire les régions
- cloudformation:Créer une pile
- cloudformation:Supprimer la pile
- cloudformation:DescribeStacks
- cloudformation:Décrire les événements de pile
- iam:Ajouter un rôle au profil d'instance
- ec2 : AssociateIamInstanceProfile
- ec2 : Décrire les associations de profils d'instance Iam

L'agent effectue les requêtes API suivantes pour analyser les compartiments S3 lorsque vous utilisez la classification des données NetApp :

- iam:Ajouter un rôle au profil d'instance
- ec2 : AssociateIamInstanceProfile
- ec2 : Décrire les associations de profils d'instance Iam
- s3 : Obtenir le balisage du bucket
- s3 : Obtenir l'emplacement du bucket
- s3 : ListeTousMesSeaux
- s3:ListBucket
- s3 : Obtenir l'état de la politique du bucket
- s3 : Obtenir la politique du bucket
- s3 : Obtenir l'Acl du bucket
- s3:Obtenir l'objet
- je suis:GetRole
- s3:Supprimer l'objet
- s3 : Supprimer la version de l'objet
- s3:PutObject
- sts:Assumer le rôle

Cloud Volumes ONTAP

L'agent effectue les requêtes API suivantes pour déployer et gérer Cloud Volumes ONTAP dans AWS.

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créer et gérer des rôles IAM et des profils d'instance pour les instances Cloud Volumes ONTAP	iam:ListInstanceProfiles	Oui	Oui	Non
	je suis:Créer un rôle	Oui	Non	Non
	iam:Supprimer le rôle	Non	Oui	Oui
	je suis:PutRolePolicy	Oui	Non	Non
	iam:Créer un profil d'instance	Oui	Non	Non
	iam:Supprimer la politique de rôle	Non	Oui	Oui
	iam:Ajouter un rôle au profil d'instance	Oui	Non	Non
	iam:Supprimer le rôle du profil d'instance	Non	Oui	Oui
	iam:Supprimer le profil d'instance	Non	Oui	Oui
	je suis:PassRole	Oui	Non	Non
	ec2 : AssociateIamInstanceProfile	Oui	Oui	Non
	ec2 : Décrire les associations de profils d'instance Iam	Oui	Oui	Non
	ec2 : Dissocier le profil d'instance Iam	Non	Oui	Non
Décoder les messages d'état d'autorisation	sts:Décoder le message d'autorisation	Oui	Oui	Non
Décrivez les images spécifiées (AMI) disponibles pour le compte	ec2:Décrire les images	Oui	Oui	Non
Décrire les tables de routage dans un VPC (requis pour les paires HA uniquement)	ec2 : Décrire les tables d'itinéraires	Oui	Non	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Arrêter, démarrer et surveiller les instances	ec2 : StartInstances	Oui	Oui	Non
	ec2 : StopInstances	Oui	Oui	Non
	ec2 : Décrire les instances	Oui	Oui	Non
	ec2 : Décrire l'état de l'instance	Oui	Oui	Non
	ec2 : Exécuter les instances	Oui	Non	Non
	ec2 : Terminer les instances	Non	Non	Oui
	ec2 : Modifier l'attribut d'instance	Non	Oui	Non
Vérifiez que la mise en réseau améliorée est activée pour les types d'instances pris en charge	ec2 : Décrire l'attribut d'instance	Non	Oui	Non
Étiquetez les ressources avec les balises « WorkingEnvironment » et « WorkingEnvironment Id » qui sont utilisées pour la maintenance et l'allocation des coûts	ec2:Créer des balises	Oui	Oui	Non
Gérer les volumes EBS que Cloud Volumes ONTAP utilise comme stockage back-end	ec2:Créer un volume	Oui	Oui	Non
	ec2 : Décrire les volumes	Oui	Oui	Oui
	ec2 : Modifier l'attribut de volume	Non	Oui	Oui
	ec2:AttachVolume	Oui	Oui	Non
	ec2:SupprimerVolume	Non	Oui	Oui
	ec2 : DétacherVolume	Non	Oui	Oui

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créer et gérer des groupes de sécurité pour Cloud Volumes ONTAP	ec2 : Créer un groupe de sécurité	Oui	Non	Non
	ec2 : Supprimer le groupe de sécurité	Non	Oui	Oui
	ec2 : Décrire les groupes de sécurité	Oui	Oui	Oui
	ec2 : RévoquerSecurityGroupEgress	Oui	Non	Non
	ec2 : Autoriser la sortie du groupe de sécurité	Oui	Non	Non
	ec2 : Autoriser l'entrée du groupe de sécurité	Oui	Non	Non
	ec2 : Révoquer l'entrée du groupe de sécurité	Oui	Oui	Non
Créer et gérer des interfaces réseau pour Cloud Volumes ONTAP dans le sous-réseau cible	ec2 : Créer une interface réseau	Oui	Non	Non
	ec2 : Décrire les interfaces réseau	Oui	Oui	Non
	ec2 : Supprimer l'interface réseau	Non	Oui	Oui
	ec2 : Modifier l'attribut d'interface réseau	Non	Oui	Non
Obtenir la liste des sous-réseaux de destination et des groupes de sécurité	ec2 : Décrire les sous-réseaux	Oui	Oui	Non
	ec2 : Décrire les Vpcs	Oui	Oui	Non
Obtenir les serveurs DNS et le nom de domaine par défaut pour les instances Cloud Volumes ONTAP	ec2 : Décrire les options DHCP	Oui	Non	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Prendre des instantanés des volumes EBS pour Cloud Volumes ONTAP	ec2:Créer un instantané	Oui	Oui	Non
	ec2 : Supprimer l'instantané	Non	Oui	Oui
	ec2 : Décrire les instantanés	Non	Oui	Non
Capturez la console Cloud Volumes ONTAP , qui est attachée aux messages AutoSupport	ec2 : Obtenir la sortie de la console	Oui	Oui	Non
Obtenez la liste des paires de clés disponibles	ec2 : Décrire les paires de clés	Oui	Non	Non
Obtenez la liste des régions AWS disponibles	ec2 : Décrire les régions	Oui	Oui	Non
Gérer les balises des ressources associées aux instances Cloud Volumes ONTAP	ec2:Supprimer les balises	Non	Oui	Oui
	ec2:Décrire les balises	Non	Oui	Non
Créer et gérer des piles pour les modèles AWS CloudFormation	cloudformation:Créer une pile	Oui	Non	Non
	cloudformation:Supprimer la pile	Oui	Non	Non
	cloudformation:DescribeStacks	Oui	Oui	Non
	cloudformation:Décrire les événements de pile	Oui	Non	Non
	cloudformation:Valider le modèle	Oui	Non	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créer et gérer un compartiment S3 qu'un système Cloud Volumes ONTAP utilise comme niveau de capacité pour la hiérarchisation des données	s3:Créer un bucket	Oui	Oui	Non
	s3 : Supprimer le bucket	Non	Oui	Oui
	s3 : Obtenir la configuration du cycle de vie	Non	Oui	Non
	s3 : PutLifecycleConfiguration	Non	Oui	Non
	s3 : Mettre en place le balisage du bucket	Non	Oui	Non
	s3 : ListBucketVersions	Non	Oui	Non
	s3 : Obtenir l'état de la politique du bucket	Non	Oui	Non
	s3 : GetBucketPublicAccessBlock	Non	Oui	Non
	s3 : Obtenir l'Acl du bucket	Non	Oui	Non
	s3 : Obtenir la politique du bucket	Non	Oui	Non
	s3 : PutBucketPublicAccessBlock	Non	Oui	Non
	s3 : Obtenir le balisage du bucket	Non	Oui	Non
	s3 : Obtenir l'emplacement du bucket	Non	Oui	Non
	s3 : ListeTousMesSeaux	Non	Non	Non
	s3:ListBucket	Non	Oui	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Activer le chiffrement des données de Cloud Volumes ONTAP à l'aide d'AWS Key Management Service (KMS)	kms:Liste*	Oui	Oui	Non
	kms:ReEncrypt*	Oui	Non	Non
	kms:Décrire*	Oui	Oui	Non
	kms:Créer une subvention	Oui	Oui	Non
	kms : générer une clé de données sans texte brut	Oui	Oui	Non
Créer et gérer un groupe de placement réparti AWS pour deux nœuds HA et le médiateur dans une seule zone de disponibilité AWS	ec2 : Créer un groupe de placement	Oui	Non	Non
	ec2 : Supprimer le groupe de placement	Non	Oui	Oui
Créer des rapports	fsx:Décrire*	Non	Oui	Non
	fsx:Liste*	Non	Oui	Non
Créer et gérer des agrégats prenant en charge la fonctionnalité Amazon EBS Elastic Volumes	ec2 : Décrire les modifications des volumes	Non	Oui	Non
	ec2:ModifierVolume	Non	Oui	Non
Vérifiez si la zone de disponibilité est une zone locale AWS et validez que tous les paramètres de déploiement sont compatibles	ec2 : Décrire les zones de disponibilité	Oui	Non	Oui

Journal des modifications

Au fur et à mesure que des autorisations sont ajoutées et supprimées, nous les noterons dans les sections ci-dessous.

9 septembre 2024

Les autorisations ont été supprimées de la politique n° 2 pour les régions standard, car la console NetApp ne prend plus en charge la mise en cache de périphérie NetApp , la découverte et la gestion des clusters Kubernetes.

Afficher les autorisations qui ont été supprimées de la politique

```
        {
            "Action": [
                "ec2:DescribeRegions",
                "eks:ListClusters",
                "eks:DescribeCluster",
                "iam:GetInstanceProfile"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "K8sServicePolicy"
        },
        {
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudwatch:GetMetricStatistics",
                "cloudformation:ListStacks"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "GFCservicePolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/GFCInstance": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
                "ec2:DetachVolume"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
            "Effect": "Allow"
        },
```

9 mai 2024

Les autorisations suivantes sont désormais requises pour Cloud Volumes ONTAP:

ec2 : Décrire les zones de disponibilité

6 juin 2023

L'autorisation suivante est désormais requise pour Cloud Volumes ONTAP:

kms : générer une clé de données sans texte brut

14 février 2023

L'autorisation suivante est désormais requise pour NetApp Cloud Tiering :

ec2 : Décrire les points de terminaison Vpc

Autorisations Azure pour l'agent de console

Lorsque la console NetApp lance un agent de console dans Azure, elle attache un rôle personnalisé à la machine virtuelle qui fournit à l'agent des autorisations pour gérer les ressources et les processus au sein de cet abonnement Azure. L'agent utilise les autorisations pour effectuer des appels d'API vers plusieurs services Azure.

La nécessité ou non de créer ce rôle personnalisé pour l'agent dépend de la manière dont vous l'avez déployé.

Déploiement à partir de la console NetApp

Lorsque vous utilisez la console pour déployer la machine virtuelle de l'agent dans Azure, cela active une "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. Les autorisations du rôle sont maintenues à jour lorsque l'agent est mis à niveau. Vous n'avez pas besoin de créer ce rôle pour l'agent ni de gérer les mises à jour.

Déploiement manuel ou à partir de la place de marché Azure

Lorsque vous déployez l'agent à partir de la Place de marché Azure ou si vous installez manuellement l'agent sur un hôte Linux, vous devez configurer vous-même le rôle personnalisé et conserver ses autorisations avec toutes les modifications.

Vous devrez vous assurer que le rôle est à jour 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.

- Pour consulter les instructions étape par étape pour utiliser ces politiques, reportez-vous aux pages suivantes :
  - "Configurer les autorisations pour un déploiement Azure Marketplace"
  - "Configurer les autorisations pour les déploiements sur site"
  - "Configurer les autorisations pour le mode restreint"

```
{
    "Name": "Console Operator",
    "Actions": [
                    "Microsoft.Compute/disks/delete",
                    "Microsoft.Compute/disks/read",
```

```
                    "Microsoft.Compute/disks/write",
                    "Microsoft.Compute/locations/operations/read",
                    "Microsoft.Compute/locations/vmSizes/read",
                    "Microsoft.Resources/subscriptions/locations/read",
                    "Microsoft.Compute/operations/read",
                    "Microsoft.Compute/virtualMachines/instanceView/read",
                    "Microsoft.Compute/virtualMachines/powerOff/action",
                    "Microsoft.Compute/virtualMachines/read",
                    "Microsoft.Compute/virtualMachines/restart/action",
                    "Microsoft.Compute/virtualMachines/deallocate/action",
                    "Microsoft.Compute/virtualMachines/start/action",
                    "Microsoft.Compute/virtualMachines/vmSizes/read",
                    "Microsoft.Compute/virtualMachines/write",
                    "Microsoft.Compute/images/read",
                    "Microsoft.Network/locations/operationResults/read",
                    "Microsoft.Network/locations/operations/read",
                    "Microsoft.Network/networkInterfaces/read",
                    "Microsoft.Network/networkInterfaces/write",
                    "Microsoft.Network/networkInterfaces/join/action",
                    "Microsoft.Network/networkSecurityGroups/read",
                    "Microsoft.Network/networkSecurityGroups/write",
                    "Microsoft.Network/networkSecurityGroups/join/action",
                    "Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
                    "Microsoft.Network/virtualNetworks/subnets/read",
                    "Microsoft.Network/virtualNetworks/subnets/write",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",

"Microsoft.Network/virtualNetworks/virtualMachines/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
                    "Microsoft.Resources/deployments/operations/read",
                    "Microsoft.Resources/deployments/read",
                    "Microsoft.Resources/deployments/write",
                    "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.Storage/checknameavailability/read",
                    "Microsoft.Storage/operations/read",
                    "Microsoft.Storage/storageAccounts/listkeys/action",
                    "Microsoft.Storage/storageAccounts/read",
                    "Microsoft.Storage/storageAccounts/delete",
                    "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",

"Microsoft.Storage/storageAccounts/listAccountSas/action",
                    "Microsoft.Storage/usages/read",
                    "Microsoft.Compute/snapshots/write",
                    "Microsoft.Compute/snapshots/read",
                    "Microsoft.Compute/availabilitySets/write",
                    "Microsoft.Compute/availabilitySets/read",
                    "Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write",
                    "Microsoft.Network/loadBalancers/read",
                    "Microsoft.Network/loadBalancers/write",
                    "Microsoft.Network/loadBalancers/delete",

"Microsoft.Network/loadBalancers/backendAddressPools/read",

"Microsoft.Network/loadBalancers/backendAddressPools/join/action",

"Microsoft.Network/loadBalancers/loadBalancingRules/read",
                    "Microsoft.Network/loadBalancers/probes/read",
                    "Microsoft.Network/loadBalancers/probes/join/action",
                    "Microsoft.Authorization/locks/*",
                    "Microsoft.Network/routeTables/join/action",
                    "Microsoft.NetApp/netAppAccounts/read",
                    "Microsoft.NetApp/netAppAccounts/capacityPools/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
                    "Microsoft.Network/privateEndpoints/write",
```

```
"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/acti
on",

"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",

"Microsoft.Storage/storageAccounts/managementPolicies/read",

"Microsoft.Storage/storageAccounts/managementPolicies/write",
                    "Microsoft.Network/privateEndpoints/read",
                    "Microsoft.Network/privateDnsZones/write",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
                    "Microsoft.Network/virtualNetworks/join/action",
                    "Microsoft.Network/privateDnsZones/A/write",
                    "Microsoft.Network/privateDnsZones/read",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",

"Microsoft.Resources/deployments/operationStatuses/read",
                    "Microsoft.Insights/Metrics/Read",
                    "Microsoft.Compute/virtualMachines/extensions/write",
                    "Microsoft.Compute/virtualMachines/extensions/delete",
                    "Microsoft.Compute/virtualMachines/extensions/read",
                    "Microsoft.Compute/virtualMachines/delete",
                    "Microsoft.Network/networkInterfaces/delete",
                    "Microsoft.Network/networkSecurityGroups/delete",
                    "Microsoft.Resources/deployments/delete",
                    "Microsoft.Compute/diskEncryptionSets/read",
                    "Microsoft.Compute/snapshots/delete",
                    "Microsoft.Network/privateEndpoints/delete",
                    "Microsoft.Compute/availabilitySets/delete",
                    "Microsoft.KeyVault/vaults/read",
                    "Microsoft.KeyVault/vaults/accessPolicies/write",
                    "Microsoft.Compute/diskEncryptionSets/write",
                    "Microsoft.KeyVault/vaults/deploy/action",
                    "Microsoft.Compute/diskEncryptionSets/delete",
                    "Microsoft.Resources/tags/read",
                    "Microsoft.Resources/tags/write",
                    "Microsoft.Resources/tags/delete",
                    "Microsoft.Network/applicationSecurityGroups/write",
                    "Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",

"Microsoft.Network/networkSecurityGroups/securityRules/write",
                    "Microsoft.Network/applicationSecurityGroups/delete",
```

```
"Microsoft.Network/networkSecurityGroups/securityRules/delete",
                    "Microsoft.Synapse/workspaces/write",
                    "Microsoft.Synapse/workspaces/read",
                    "Microsoft.Synapse/workspaces/delete",
                    "Microsoft.Synapse/register/action",
                    "Microsoft.Synapse/checkNameAvailability/action",
                    "Microsoft.Synapse/workspaces/operationStatuses/read",
                    "Microsoft.Synapse/workspaces/firewallRules/read",

"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
                    "Microsoft.Synapse/workspaces/operationResults/read",

"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",

"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
                    "Microsoft.Compute/images/write",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
                    "Microsoft.Compute/virtualMachineScaleSets/write",
                    "Microsoft.Compute/virtualMachineScaleSets/read",
                    "Microsoft.Compute/virtualMachineScaleSets/delete"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Console Permissions",
    "IsCustom": "true"
}
```

Comment les autorisations Azure sont utilisées

Les sections suivantes décrivent comment les autorisations sont utilisées pour chaque système de stockage et service de données NetApp . Ces informations peuvent être utiles si les politiques de votre entreprise stipulent que les autorisations ne sont accordées qu'en cas de besoin.

Azure NetApp Files

L'agent effectue les requêtes API suivantes lorsque vous utilisez NetApp Data Classification pour analyser les données Azure NetApp Files :

- NetApp/netAppAccounts/read
- NetApp/netAppAccounts/capacityPools/read
- NetApp/netAppAccounts/capacityPools/volumes/write
- NetApp/netAppAccounts/capacityPools/volumes/read
- NetApp/netAppAccounts/capacityPools/volumes/delete

Sauvegarde et récupération NetApp

L'agent de console effectue les requêtes API suivantes pour NetApp Backup and Recovery :

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/lecture
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.KeyVault/vaults/lecture
- Microsoft.KeyVault/vaults/accessPolicies/write
- Microsoft.Network/networkInterfaces/lecture
- Microsoft.Ressources/abonnements/emplacements/lecture
- Microsoft.Network/virtualNetworks/lecture
- Microsoft.Network/virtualNetworks/sous-réseaux/lecture
- Microsoft.Resources/abonnements/resourceGroups/read
- Microsoft.Resources/abonnements/groupes de ressources/ressources/lecture
- Microsoft.Resources/abonnements/resourceGroups/write
- Microsoft.Autorisation/locks/*
- Microsoft.Network/privateEndpoints/écriture
- Microsoft.Network/privateEndpoints/lecture
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/écriture
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Network/privateDnsZones/A/écriture
- Microsoft.Network/privateDnsZones/lecture
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/lecture
- Microsoft.Network/networkInterfaces/supprimer
- Microsoft.Network/networkSecurityGroups/supprimer
- Microsoft.Resources/deployments/delete
- Microsoft.ManagedIdentity/userAssignedIdentities/assign/action

L'agent effectue les requêtes API suivantes lorsque vous utilisez la fonctionnalité Rechercher et restaurer :

- Microsoft.Synapse/espaces de travail/écriture
- Microsoft.Synapse/espaces de travail/lecture
- Microsoft.Synapse/espaces de travail/supprimer
- Microsoft.Synapse/register/action
- Microsoft.Synapse/checkNameAvailability/action
- Microsoft.Synapse/workspaces/operationStatuses/lecture
- Microsoft.Synapse/workspaces/firewallRules/lecture

- Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action
- Microsoft.Synapse/workspaces/operationResults/lecture
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action

Classification des données NetApp

L'agent effectue les requêtes API suivantes lorsque vous utilisez la classification des données.

Action	Utilisé pour l'installation ?	Utilisé pour les opérations quotidiennes ?
Microsoft.Compute/locations/operations/read	Oui	Oui
Microsoft.Compute/locations/vmSizes/lecture	Oui	Oui
Microsoft.Compute/opérations/lecture	Oui	Oui
Microsoft.Compute/virtualMachines/instanceView/read	Oui	Oui
Microsoft.Compute/virtualMachines/powerOff/action	Oui	Non
Microsoft.Compute/virtualMachines/read	Oui	Oui
Microsoft.Compute/virtualMachines/restart/action	Oui	Non
Microsoft.Compute/virtualMachines/start/action	Oui	Non
Microsoft.Compute/virtualMachines/vmSizes/lecture	Non	Oui
Microsoft.Compute/virtualMachines/write	Oui	Non
Microsoft.Compute/images/read	Oui	Oui
Microsoft.Compute/disks/delete	Oui	Non
Microsoft.Compute/disques/lecture	Oui	Oui
Microsoft.Compute/disques/écriture	Oui	Non
Microsoft.Storage/checknameavailability/lecture	Oui	Oui
Microsoft.Storage/opérations/lecture	Oui	Oui
Microsoft.Storage/storageAccounts/listkeys/action	Oui	Non
Microsoft.Storage/storageAccounts/lecture	Oui	Oui

Action	Utilisé pour l'installation ?	Utilisé pour les opérations quotidiennes ?
Microsoft.Storage/storageAccounts/write	Oui	Non
Microsoft.Storage/storageAccounts/blobServices/containers/read	Oui	Oui
Microsoft.Network/networkInterfaces/lecture	Oui	Oui
Microsoft.Network/networkInterfaces/write	Oui	Non
Microsoft.Network/networkInterfaces/join/action	Oui	Non
Microsoft.Network/networkSecurityGroups/lecture	Oui	Oui
Microsoft.Network/networkSecurityGroups/écriture	Oui	Non
Microsoft.Ressources/abonnements/emplacements/lecture	Oui	Oui
Microsoft.Network/locations/operationResults/lecture	Oui	Oui
Microsoft.Network/locations/operations/read	Oui	Oui
Microsoft.Network/virtualNetworks/lecture	Oui	Oui
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/lecture	Oui	Oui
Microsoft.Network/virtualNetworks/sous-réseaux/lecture	Oui	Oui
Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Oui	Oui
Microsoft.Network/virtualNetworks/virtualMachines/lecture	Oui	Oui
Microsoft.Network/virtualNetworks/sous-réseaux/join/action	Oui	Non
Microsoft.Network/virtualNetworks/sous-réseaux/écriture	Oui	Non
Microsoft.Network/routeTables/join/action	Oui	Non
Microsoft.Ressources/déploiements/opérations/lecture	Oui	Oui
Microsoft.Ressources/déploiements/lecture	Oui	Oui

Action	Utilisé pour l'installation ?	Utilisé pour les opérations quotidiennes ?
Microsoft.Ressources/déploiements /écriture	Oui	Non
Microsoft.Resources/ressources/lire	Oui	Oui
Microsoft.Resources/subscriptions/ operationresults/read	Oui	Oui
Microsoft.Resources/subscriptions/r esourceGroups/delete	Oui	Non
Microsoft.Resources/abonnements/ resourceGroups/read	Oui	Oui
Microsoft.Resources/abonnements/ groupes de ressources/ressources/lecture	Oui	Oui
Microsoft.Resources/abonnements/ resourceGroups/write	Oui	Non

Cloud Volumes ONTAP

L'agent effectue les requêtes API suivantes pour déployer et gérer Cloud Volumes ONTAP dans Azure.

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créer et gérer des machines virtuelles	Microsoft.Compute/locations/operations/read	Oui	Oui	Non
	Microsoft.Compute/locations/vmSizes/lecture	Oui	Oui	Non
	Microsoft.Ressources/abonnements/emplacements/lecture	Oui	Non	Non
	Microsoft.Compute/opérations/lecture	Oui	Oui	Non
	Microsoft.Compute/virtualMachines/instanceView/read	Oui	Oui	Non
	Microsoft.Compute/virtualMachines/powerOff/action	Oui	Oui	Non
	Microsoft.Compute/virtualMachines/read	Oui	Oui	Non
	Microsoft.Compute/virtualMachines/restart/action	Oui	Oui	Non
	Microsoft.Compute/virtualMachines/start/action	Oui	Oui	Non
	Microsoft.Compute/virtualMachines/deallocate/action	Non	Oui	Oui
	Microsoft.Compute/virtualMachines/vmSizes/lecture	Non	Oui	Non
	Microsoft.Compute/virtualMachines/write	Oui	Oui	Non
	Microsoft.Compute/virtualMachines/delete	Oui	Oui	Oui
	Microsoft.Resources/deployments/delete	Oui	Non	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Activer le déploiement à partir d'un disque dur virtuel	Microsoft.Compute/images/read	Oui	Non	Non
	Microsoft.Compute/images/write	Oui	Non	Non
Créer et gérer les interfaces réseau dans le sous-réseau cible	Microsoft.Network/networkInterfaces/lecture	Oui	Oui	Non
	Microsoft.Network/networkInterfaces/write	Oui	Oui	Non
	Microsoft.Network/networkInterfaces/join/action	Oui	Oui	Non
	Microsoft.Network/networkInterfaces/supprimer	Oui	Oui	Non
Créer et gérer des groupes de sécurité réseau	Microsoft.Network/networkSecurityGroups/lecture	Oui	Oui	Non
	Microsoft.Network/networkSecurityGroups/écriture	Oui	Oui	Non
	Microsoft.Network/networkSecurityGroups/join/action	Oui	Non	Non
	Microsoft.Network/networkSecurityGroups/supprimer	Non	Oui	Oui

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Obtenez des informations réseau sur les régions, le VNet cible et le sous-réseau, et ajoutez les machines virtuelles aux VNets	Microsoft.Network/locations/operationResults/lecture	Oui	Oui	Non
	Microsoft.Network/locations/operations/read	Oui	Oui	Non
	Microsoft.Network/virtualNetworks/lecture	Oui	Non	Non
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/lecture	Oui	Non	Non
	Microsoft.Network/virtualNetworks/sous-réseaux/lecture	Oui	Oui	Non
	Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Oui	Oui	Non
	Microsoft.Network/virtualNetworks/virtualMachines/lecture	Oui	Oui	Non
	Microsoft.Network/virtualNetworks/sous-réseaux/join/action	Oui	Oui	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créer et gérer des groupes de ressources	Microsoft.Ressources/déploiements/opérations/lecture	Oui	Oui	Non
	Microsoft.Ressources/déploiements/lecture	Oui	Oui	Non
	Microsoft.Ressources/déploiements/écriture	Oui	Oui	Non
	Microsoft.Resources/ressources/lire	Oui	Oui	Non
	Microsoft.Resources/subscriptions/operationresults/read	Oui	Oui	Non
	Microsoft.Resources/subscriptions/resourceGroups/delete	Oui	Oui	Oui
	Microsoft.Resources/abonnements/resourceGroups/read	Non	Oui	Non
	Microsoft.Resources/abonnements/groupes de ressources/ressources/lecture	Oui	Oui	Non
	Microsoft.Resources/abonnements/resourceGroups/write	Oui	Oui	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Gérer les comptes et les disques de stockage Azure	Microsoft.Compute/disques/lecture	Oui	Oui	Oui
	Microsoft.Compute/disques/écriture	Oui	Oui	Non
	Microsoft.Compute/disks/delete	Oui	Oui	Oui
	Microsoft.Storage/checknameavailability/lecture	Oui	Oui	Non
	Microsoft.Storage/opérations/lecture	Oui	Oui	Non
	Microsoft.Storage/storageAccounts/listkeys/action	Oui	Oui	Non
	Microsoft.Storage/storageAccounts/lecture	Oui	Oui	Non
	Microsoft.Storage/storageAccounts/supprimer	Non	Oui	Oui
	Microsoft.Storage/storageAccounts/write	Oui	Oui	Non
	Microsoft.Storage/usages/lecture	Non	Oui	Non
Activer les sauvegardes sur le stockage Blob et le chiffrement des comptes de stockage	Microsoft.Storage/storageAccounts/blobServices/containers/read	Oui	Oui	Non
	Microsoft.KeyVault/vaults/lecture	Oui	Oui	Non
	Microsoft.KeyVault/vaults/accessPolicies/write	Oui	Oui	Non
Activer les points de terminaison du service VNet pour la hiérarchisation des données	Microsoft.Network/virtualNetworks/sous-réseaux/écriture	Oui	Oui	Non
	Microsoft.Network/routeTables/join/action	Oui	Oui	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créer et gérer des instantanés gérés par Azure	Microsoft.Compute/snapshots/write	Oui	Oui	Non
	Microsoft.Compute/snapshots/read	Oui	Oui	Non
	Microsoft.Compute/snapshots/delete	Non	Oui	Oui
	Microsoft.Compute/disques/beginGetAccess/action	Non	Oui	Non
Créer et gérer des ensembles de disponibilité	Microsoft.Compute/availabilitySets/write	Oui	Non	Non
	Microsoft.Compute/availabilitySets/lecture	Oui	Non	Non
Activer les déploiements programmatiques à partir du marché	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read	Oui	Non	Non
	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write	Oui	Oui	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Gérer un équilibreur de charge pour les paires HA	Microsoft.Network/loadBalancers/lecture	Oui	Oui	Non
	Microsoft.Network/loadBalancers/write	Oui	Non	Non
	Microsoft.Network/loadBalancers/supprimer	Non	Oui	Oui
	Microsoft.Network/loadBalancers/backendAddressPools/lecture	Oui	Non	Non
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	Oui	Non	Non
	Microsoft.Network/loadBalancers/frontendIPConfigurations/lecture	Oui	Oui	Non
	Microsoft.Network/loadBalancers/loadBalancingRules/lecture	Oui	Non	Non
	Microsoft.Network/loadBalancers/sondes/lecture	Oui	Non	Non
	Microsoft.Network/loadBalancers/probes/join/action	Oui	Non	Non
Activer la gestion des verrous sur les disques Azure	Microsoft.Autorisation/locks/*	Oui	Oui	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Activer les points de terminaison privés pour les paires HA lorsqu'il n'y a pas de connectivité en dehors du sous-réseau	Microsoft.Network/privateEndpoints/écriture	Oui	Oui	Non
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action	Oui	Non	Non
	Microsoft.Storage/storageAccounts/privateEndpointConnections/lecture	Oui	Oui	Oui
	Microsoft.Network/privateEndpoints/lecture	Oui	Oui	Oui
	Microsoft.Network/privateDnsZones/écriture	Oui	Oui	Non
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/écriture	Oui	Oui	Non
	Microsoft.Network/virtualNetworks/join/action	Oui	Oui	Non
	Microsoft.Network/privateDnsZones/A/écriture	Oui	Oui	Non
	Microsoft.Network/privateDnsZones/lecture	Oui	Oui	Non
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/lecture	Oui	Oui	Non
Requis pour certains déploiements de machines virtuelles, en fonction du matériel physique sous-jacent	Microsoft.Resources/deployments/operationStatuses/lecture	Oui	Oui	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Supprimer des ressources d'un groupe de ressources en cas d'échec de déploiement ou de suppression	Microsoft.Network/privateEndpoints/supprimer	Oui	Oui	Non
	Microsoft.Compute/availabilitySets/delete	Oui	Oui	Non
Activer l'utilisation de clés de chiffrement gérées par le client lors de l'utilisation de l'API	Microsoft.Compute/diskEncryptionSets/lecture	Oui	Oui	Oui
	Microsoft.Compute/diskEncryptionSets/écriture	Oui	Oui	Non
	Microsoft.KeyVault/vaults/deploy/action	Oui	Non	Non
	Microsoft.Compute/diskEncryptionSets/delete	Oui	Oui	Oui
Configurer un groupe de sécurité d'application pour une paire HA afin d'isoler l'interconnexion HA et les cartes réseau du réseau de cluster	Microsoft.Network/applicationSecurityGroups/écriture	Non	Oui	Non
	Microsoft.Network/applicationSecurityGroups/lecture	Non	Oui	Non
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	Non	Oui	Non
	Microsoft.Network/networkSecurityGroups/securityRules/écriture	Oui	Oui	Non
	Microsoft.Network/applicationSecurityGroups/supprimer	Non	Oui	Oui
	Microsoft.Network/networkSecurityGroups/securityRules/supprimer	Non	Oui	Oui

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Lire, écrire et supprimer les balises associées aux ressources Cloud Volumes ONTAP	Microsoft.Ressources/tags/lecture	Non	Oui	Non
	Microsoft.Ressources/tags/write	Oui	Oui	Non
	Microsoft.Ressources/tags/supprimer	Oui	Non	Non
Crypter les comptes de stockage lors de la création	Microsoft.ManagedIdentity/userAssignedIdentities/assign/action	Oui	Oui	Non
Utilisez des ensembles de machines virtuelles évolutives en mode d'orchestration flexible afin de spécifier des zones spécifiques pour Cloud Volumes ONTAP	Microsoft.Compute/virtualMachineScaleSets/write	Oui	Non	Non
	Microsoft.Compute/virtualMachineScaleSets/lecture	Oui	Non	Non
	Microsoft.Compute/virtualMachineScaleSets/supprimer	Non	Non	Oui

hiérarchisation

L'agent effectue les requêtes API suivantes lorsque vous configurez NetApp Cloud Tiering.

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Resources/abonnements/resourceGroups/read
- Microsoft.Ressources/abonnements/emplacements/lecture

L'agent de la console effectue les demandes d'API suivantes pour les opérations quotidiennes.

- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/managementPolicies/lecture
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Storage/storageAccounts/lecture

Journal des modifications

Au fur et à mesure que des autorisations sont ajoutées et supprimées, nous les noterons dans les sections ci-dessous.

9 septembre 2024

Les autorisations suivantes ont été supprimées de la politique JSON car la console ne prend plus en charge la découverte et la gestion des clusters Kubernetes :

- Microsoft.ContainerService/managedClusters/listClusterUserCredential/action
- Microsoft.ContainerService/managedClusters/lecture

22 août 2024

Les autorisations suivantes ont été ajoutées à la stratégie JSON, car elles sont requises pour la prise en charge des ensembles de machines virtuelles identiques par Cloud Volumes ONTAP :

- Microsoft.Compute/virtualMachineScaleSets/write
- Microsoft.Compute/virtualMachineScaleSets/lecture
- Microsoft.Compute/virtualMachineScaleSets/supprimer

5 décembre 2023

Les autorisations suivantes ne sont plus nécessaires pour NetApp Backup and Recovery lors de la sauvegarde de données de volume sur le stockage Azure Blob :

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete

Ces autorisations sont requises pour d'autres services de stockage de la console. Elles resteront donc dans le rôle personnalisé de l'agent si vous utilisez ces autres services de stockage.

12 mai 2023

Les autorisations suivantes ont été ajoutées à la stratégie JSON car elles sont requises pour la gestion de Cloud Volumes ONTAP :

- Microsoft.Compute/images/write
- Microsoft.Network/loadBalancers/frontendIPConfigurations/lecture

Les autorisations suivantes ont été supprimées de la politique JSON car elles ne sont plus nécessaires :

- Microsoft.Storage/storageAccounts/blobServices/containers/write
- Microsoft.Network/publicIPAddresses/supprimer

23 mars 2023

L'autorisation « Microsoft.Storage/storageAccounts/delete » n'est plus nécessaire pour la classification des données.

Cette autorisation est toujours requise pour Cloud Volumes ONTAP.

5 janvier 2023

Les autorisations suivantes ont été ajoutées à la politique JSON :

- Microsoft.Storage/storageAccounts/listAccountSas/action

- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action

  Ces autorisations sont requises pour NetApp Backup and Recovery.

- Microsoft.Network/loadBalancers/backendAddressPools/join/action

  Cette autorisation est requise pour le déploiement de Cloud Volumes ONTAP .

Autorisations Google Cloud pour l'agent de la console

La console NetApp nécessite des autorisations pour effectuer des actions dans Google Cloud. Ces autorisations sont incluses dans un rôle personnalisé fourni par NetApp. Vous devez comprendre ce que l'agent fait avec ces autorisations.

Autorisations du compte de service

Le rôle personnalisé indiqué ci-dessous fournit les autorisations dont un agent de console a besoin pour gérer les ressources et les processus au sein de votre réseau Google Cloud.

Vous devrez appliquer ce rôle personnalisé à un compte de service qui est attaché à la machine virtuelle de l'agent de console.

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

Vous devez également vous assurer que le rôle est à jour 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.

```
title: NetApp Console agent
description: Permissions for the service account associated with the
Console agent instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- 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.addAccessConfig
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.updateDisplayDevice
- compute.instanceGroups.get
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
```

```
- 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
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
```

Comment les autorisations Google Cloud sont utilisées

Actions	But
- compute.disks.create - compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use	Pour créer et gérer des disques pour Cloud Volumes ONTAP.
- compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list	Pour créer des règles de pare-feu pour Cloud Volumes ONTAP.
- compute.globalOperations.get	Pour obtenir l'état des opérations.
- compute.images.get - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly	Pour obtenir des images pour les instances de VM.
- compute.instances.attachDisk - compute.instances.detachDisk	Pour attacher et détacher des disques à Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Pour créer et supprimer des instances de machine virtuelle Cloud Volumes ONTAP .
- compute.instances.get	Pour répertorier les instances de VM.
- compute.instances.getSerialPortOutput	Pour obtenir les journaux de la console.
- compute.instances.list	Pour récupérer la liste des instances dans une zone.
- compute.instances.setDeletionProtection	Pour définir la protection contre la suppression sur l'instance.
- compute.instances.setLabels	Pour ajouter des étiquettes.
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	Pour modifier le type de machine pour Cloud Volumes ONTAP.
- compute.instances.setMetadata	Pour ajouter des métadonnées.
- compute.instances.setTags	Pour ajouter des balises pour les règles de pare-feu.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Pour démarrer et arrêter Cloud Volumes ONTAP.
- compute.machineTypes.get	Pour obtenir le nombre de cœurs à vérifier, les quotas.
- compute.projects.get	Pour soutenir des projets multiples.
- compute.snapshots.create - compute.snapshots.delete - compute.snapshots.get - compute.snapshots.list - compute.snapshots.setLabels	Pour créer et gérer des instantanés de disque persistants.
- compute.networks.get - compute.networks.list - compute.regions.get - compute.regions.list - compute.subnetworks.get - compute.subnetworks.list - compute.zoneOperations.get - compute.zones.get - compute.zones.list	Pour obtenir les informations réseau nécessaires à la création d'une nouvelle instance de machine virtuelle Cloud Volumes ONTAP .

Actions	But
- 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	Pour déployer l'instance de machine virtuelle Cloud Volumes ONTAP à l'aide de Google Cloud Deployment Manager.
- logging.logEntries.list - logging.privateLogEntries.list	Pour obtenir les lecteurs de journaux de pile.
- resourcemanager.projects.get	Pour soutenir des projets multiples.
- storage.buckets.create - storage.buckets.delete - storage.buckets.get - storage.buckets.list - storage.buckets.update	Pour créer et gérer un bucket Google Cloud Storage pour la hiérarchisation des données.
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.list - cloudkms.keyRings.list	Pour utiliser les clés de chiffrement gérées par le client à partir du service Cloud Key Management avec Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - storage.objects.get - storage.objects.list	Pour définir un compte de service sur l'instance Cloud Volumes ONTAP . Ce compte de service fournit des autorisations pour la hiérarchisation des données vers un bucket Google Cloud Storage.
- compute.addresses.list	Pour récupérer les adresses dans une région lors du déploiement d'une paire HA.
- compute.backendServices.create - compute.regionBackendServices.create - compute.regionBackendServices.get - compute.regionBackendServices.list	Pour configurer un service backend pour distribuer le trafic dans une paire HA.
- compute.networks.updatePolicy	Pour appliquer des règles de pare-feu sur les VPC et les sous-réseaux pour une paire HA.
- compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	Pour activer la classification des données NetApp .
- compute.instanceGroups.get - compute.addresses.get - compute.instances.updateNetworkInterface	Pour créer et gérer des machines virtuelles de stockage sur des paires Cloud Volumes ONTAP HA.
- monitoring.timeSeries.list - storage.buckets.getIamPolicy	Pour découvrir des informations sur les buckets Google Cloud Storage.

Actions	But
- cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.getIamPolicy - cloudkms.cryptoKeys.list - cloudkms.cryptoKeys.setIamPolicy - cloudkms.keyRings.get - cloudkms.keyRings.getIamPolicy - cloudkms.keyRings.list - cloudkms.keyRings.setIamPolicy	Pour sélectionner vos propres clés gérées par le client dans l'assistant d'activation de NetApp Backup and Recovery au lieu d'utiliser les clés de chiffrement par défaut gérées par Google.

Journal des modifications

Au fur et à mesure que des autorisations sont ajoutées et supprimées, nous les noterons dans les sections ci-dessous.

06/02/2023

L'autorisation suivante a été ajoutée à cette politique :

- compute.instances.updateNetworkInterface

Cette autorisation est requise pour Cloud Volumes ONTAP.

27/01/2023

Les autorisations suivantes ont été ajoutées à la politique :

- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.porte-clés.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

Ces autorisations sont requises pour NetApp Backup and Recovery.

Ports

Règles du groupe de sécurité de l'agent de console dans AWS

Le groupe de sécurité AWS pour l'agent nécessite des règles entrantes et sortantes. La console NetApp crée automatiquement ce groupe de sécurité lorsque vous créez un agent de console à partir de la console. Vous devez configurer ce groupe de sécurité pour toutes les autres options d'installation.

Règles entrantes

Protocole	Port	But
SSH	22	Fournit un accès SSH à l'hôte de l'agent

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 à l'interface utilisateur locale et aux connexions à partir de l'instance de classification des données NetApp
TCP	3128	Fournit à Cloud Volumes ONTAP un accès Internet. Vous devez ouvrir manuellement ce port après le déploiement.

Règles de sortie

Le groupe de sécurité prédéfini pour l'agent ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de sortie de base. Si vous avez besoin de règles plus rigides, utilisez les règles sortantes avancées.

Règles de base pour les voyages sortants

Le groupe de sécurité prédéfini pour l'agent inclut les règles sortantes suivantes.

Protocole	Port	But
Tous les TCP	Tous	Tout le trafic sortant
Tout UDP	Tous	Tout le trafic sortant

Règles sortantes avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par l'agent

L'adresse IP source est l'hôte de l'agent.

Service	Protocole	Port	Destination	But
Appels API et AutoSupport	HTTPS	443	Gestion de cluster Internet sortant et ONTAP LIF	Appels d'API vers AWS, ONTAP, NetApp Data Classification et envoi de messages AutoSupport à NetApp
Appels d'API	TCP	3000	Médiateur ONTAP HA	Communication avec le médiateur ONTAP HA
	TCP	8080	Classification des données	Sonder l'instance de classification des données pendant le déploiement

Service	Protocole	Port	Destination	But
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par la console

Règles du groupe de sécurité de l'agent de console dans Azure

Le groupe de sécurité Azure pour l'agent nécessite des règles entrantes et sortantes. La console NetApp crée automatiquement ce groupe de sécurité lorsque vous créez un agent de console à partir de la console. Pour les autres options d'installation, vous devez configurer ce groupe de sécurité manuellement.

Règles entrantes

Protocole	Port	But
SSH	22	Fournit un accès SSH à l'hôte de l'agent
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 à l'interface utilisateur locale et des connexions depuis l'instance de classification des données NetApp
TCP	3128	Fournit à Cloud Volumes ONTAP un accès Internet pour envoyer des messages AutoSupport au support NetApp . Vous devez ouvrir manuellement ce port après le déploiement. "Découvrez comment l'agent est utilisé comme proxy pour les messages AutoSupport"

Règles de sortie

Le groupe de sécurité prédéfini pour l'agent ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de sortie de base. Si vous avez besoin de règles plus rigides, utilisez les règles sortantes avancées.

Règles de base pour les voyages sortants

Le groupe de sécurité prédéfini pour l'agent inclut les règles sortantes suivantes.

Protocole	Port	But
Tous les TCP	Tous	Tout le trafic sortant
Tout UDP	Tous	Tout le trafic sortant

Règles sortantes avancées

Si vous avez besoin de règles strictes pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par l'agent.

L'adresse IP source est l'hôte de l'agent.

Service	Protocole	Port	Destination	But
Appels API et AutoSupport	HTTPS	443	Gestion de cluster Internet sortant et ONTAP LIF	Appels d'API vers Azure, vers ONTAP, vers la classification des données NetApp et envoi de messages AutoSupport à NetApp
Appels d'API	TCP	8080	Classification des données	Sonder l'instance de classification des données pendant le déploiement
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par la console

Règles de pare-feu d'agent dans Google Cloud

Les règles de pare-feu Google Cloud pour l'agent nécessitent des règles entrantes et sortantes. La console NetApp crée automatiquement ce groupe de sécurité lorsque vous créez un agent de console à partir de la console. Pour les autres options d'installation, vous devez configurer ce groupe de sécurité manuellement.

Règles entrantes

Protocole	Port	But
SSH	22	Fournit un accès SSH à l'hôte de l'agent
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

Protocole	Port	But
TCP	3128	Fournit à Cloud Volumes ONTAP un accès Internet. Vous devez ouvrir manuellement ce port après le déploiement.

Règles de sortie

Les règles de pare-feu prédéfinies de l'agent ouvrent tout le trafic sortant. Suivez les règles sortantes de base si elles sont acceptables, ou utilisez des règles sortantes avancées pour des exigences plus strictes.

Règles de base pour les voyages sortants

Les règles de pare-feu prédéfinies pour l'agent incluent les règles sortantes suivantes.

Protocole	Port	But
Tous les TCP	Tous	Tout le trafic sortant
Tout UDP	Tous	Tout le trafic sortant

Règles sortantes avancées

Si vous avez besoin de règles strictes pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par l'agent.

L'adresse IP source est l'hôte de l'agent.

Service	Protocole	Port	Destination	But
Appels API et AutoSupport	HTTPS	443	Gestion de cluster Internet sortant et ONTAP LIF	Appels d'API vers Google Cloud, vers ONTAP, vers NetApp Data Classification et envoi de messages AutoSupport à NetApp
Appels d'API	TCP	8080	Classification des données	Sonder l'instance de classification des données pendant le déploiement
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par classification des données

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 console NetApp .

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

Points d'accès réseau requis pour la version 3.9.55 et les versions antérieures

Cette rubrique détaille l'accès réseau requis pour les versions du mode standard de la console NetApp antérieures à la version 4.0.0 de la console NetApp , l'agent de la console NetApp et l'accès Internet sortant des services de données NetApp et la possibilité de contacter les points de terminaison nécessaires. Vous devez vous assurer que la console et tous les agents que vous installez disposent du bon accès réseau pour fonctionner.

Vous devrez configurer l'accès réseau pour les ordinateurs qui accèdent à la console NetApp en tant que logiciel en tant que service (SaaS) et pour tous les agents de console que vous installez sur site ou dans le cloud. Vous pouvez également avoir besoin de points de terminaison supplémentaires pour certains services de données NetApp , notamment Cloud Volumes ONTAP.

Mettez à jour votre liste de points de terminaison vers la liste révisée pour la version 4.0.0 et supérieure

À partir de la version 4.0.0, les agents de console nécessitent moins de points de terminaison. Les déploiements existants avant la version 4.0.0 restent pris en charge. Après la mise à niveau vers la version 4.0.0 ou une version ultérieure, vous pouvez supprimer les anciens points de terminaison de votre liste d'autorisation lorsque cela vous convient.

NetApp vous recommande de mettre à jour vos règles de pare-feu pour utiliser la liste de points de terminaison révisée. La liste révisée est plus petite, donc plus sûre et plus facile à gérer.

Revoir"points de terminaison pris en charge pour la version 4.0.0 et supérieure"

Étapes

1. Mettre sur liste blanche les points de terminaison dans"Points de terminaison pris en charge pour la version 4.0.0 et supérieure" .
2. Redémarrez le service Service Manager 2 sur chaque agent en exécutant la commande suivante :

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

3. Exécutez la commande suivante et vérifiez que l'état de l'agent indique *actif (en cours d'exécution)* : _

```
systemctl status netapp-service-manager.service
```

4. Supprimez les anciens points de terminaison de votre liste autorisée.

Points de terminaison contactés par la console NetApp

Chaque ordinateur qui accède à la console NetApp doit disposer de connexions aux points de terminaison répertoriés ci-dessous.

Le système contacte ces points de terminaison dans deux scénarios :

- À partir d'un ordinateur accédant au "Console NetApp" en tant que logiciel en tant que service (SaaS).
- Depuis un ordinateur accédant directement à un hôte agent, soit pour se connecter et le configurer, soit pour accéder à la console depuis l'hôte agent.

Points de terminaison	But
\ https://support.netapp.com \ https://mysupport.netapp.com	Pour obtenir des informations de licence et envoyer des messages AutoSupport au support NetApp .
https://*.api.bluexp.netapp.com \ https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com \ https://cloudmanager.cloud.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com	Pour fournir des fonctionnalités et des services au sein de la console NetApp .

Points de terminaison	But
Choisissez entre deux ensembles de points de terminaison : • Option 1 (recommandée) \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net \ https://cloudmanagerinfraprod.azurecr.io	Pour obtenir des images pour les mises à niveau de l'agent de console. NetApp recommande d'autoriser les points de terminaison de l'option 1 dans votre pare-feu, car ils sont plus sécurisés, et d'interdire les points de terminaison de l'option 2, sauf si vous utilisez Ransomware Resilience ou Backup and Recovery. Notez les points suivants à propos de ces points de terminaison : • Les points de terminaison de l'option 1 sont pris en charge dans la version 3.9.47 et supérieure. Les versions antérieures à la version 3.9.47 ne prennent pas en charge la compatibilité descendante. • L'agent de console initie d'abord le contact avec les points de terminaison de l'option 2. Si ces points de terminaison ne sont pas accessibles, il contacte automatiquement les points de terminaison de l'option 1. • Si vous utilisez l'agent de console avec NetApp Backup and Recovery ou Ransomware Resilience, le système ne prend pas en charge les points de terminaison Option 1. Autoriser les points de terminaison de l'option 2 et interdire l'option 1.

Points de terminaison contactés par l'agent de la console

Vous installez l'agent de console sur site ou dans le cloud, et il contacte les points de terminaison pour effectuer les actions initiées par la console.

Les agents de console doivent accéder aux mêmes points de terminaison que la console NetApp , ainsi qu'à des points de terminaison supplémentaires si vous déployez l'agent chez votre fournisseur de cloud.

Points de terminaison d'agent pour AWS

Ces points de terminaison s'appliquent aux agents de console antérieurs à la version 4.0.0.

Points de terminaison	But
Services AWS (amazonaws.com) : CloudFormation Elastic Compute Cloud (EC2), gestion des identités et des accès (IAM), service de gestion des clés (KMS), service de jeton de sécurité (STS), service de stockage simple (S3).	Pour gérer les ressources dans AWS. Le point de terminaison exact dépend de la région AWS que vous utilisez. Consultez la documentation AWS pour plus de détails sur l'obtention d'informations sur les licences et l'envoi de messages AutoSupport au support NetApp .
\ https://support.netapp.com \ https://mysupport.netapp.com	Pour obtenir des informations de licence et envoyer des messages AutoSupport au support NetApp .

Points de terminaison	But
Choisissez entre deux ensembles de points de terminaison : • Option 1 (recommandée) \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net \ https://cloudmanagerinfraprod.azurecr.io	Pour obtenir des images pour les mises à niveau de l'agent de console. NetApp recommande d'autoriser les points de terminaison de l'option 1 dans votre pare-feu, car ils sont plus sécurisés, et d'interdire les points de terminaison de l'option 2, sauf si vous utilisez Ransomware Resilience ou Backup and Recovery. Notez les points suivants à propos de ces points de terminaison : • Les points de terminaison de l'option 1 sont pris en charge dans la version 3.9.47 et supérieure. Les versions antérieures à la version 3.9.47 ne prennent pas en charge la compatibilité descendante. • L'agent de console initie d'abord le contact avec les points de terminaison de l'option 2. Si ces points de terminaison ne sont pas accessibles, il contacte automatiquement les points de terminaison de l'option 1. • Si vous utilisez l'agent de console avec NetApp Backup and Recovery ou Ransomware Resilience, le système ne prend pas en charge les points de terminaison Option 1. Autoriser les points de terminaison de l'option 2 et interdire l'option 1.

Points de terminaison d'agent pour Azure

Ces points de terminaison s'appliquent aux agents de console antérieurs à la version 4.0.0.

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

Points de terminaison	But
Choisissez entre deux ensembles de points de terminaison : • Option 1 (recommandée) \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net \ https://cloudmanagerinfraprod.azurecr.io	Pour obtenir des images pour les mises à niveau de l'agent de console. NetApp recommande d'autoriser les points de terminaison de l'option 1 dans votre pare-feu, car ils sont plus sécurisés, et d'interdire les points de terminaison de l'option 2, sauf si vous utilisez Ransomware Resilience ou Backup and Recovery. Notez les points suivants à propos de ces points de terminaison : • Les points de terminaison de l'option 1 sont pris en charge dans la version 3.9.47 et supérieure. Les versions antérieures à la version 3.9.47 ne prennent pas en charge la compatibilité descendante. • L'agent de console initie d'abord le contact avec les points de terminaison de l'option 2. Si ces points de terminaison ne sont pas accessibles, il contacte automatiquement les points de terminaison de l'option 1. • Si vous utilisez l'agent de console avec NetApp Backup and Recovery ou Ransomware Resilience, le système ne prend pas en charge les points de terminaison Option 1. Autoriser les points de terminaison de l'option 2 et interdire l'option 1.

Points de terminaison d'agent pour Google Cloud

Ces points de terminaison s'appliquent aux agents de console antérieurs à la version 4.0.0.

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://www.googleapis.com/deploymentmanager/v2/project	Pour gérer les ressources dans Google Cloud.
\ https://support.netapp.com \ https://mysupport.netapp.com	Pour obtenir des informations de licence et envoyer des messages AutoSupport au support NetApp .

Points de terminaison	But
Choisissez entre deux ensembles de points de terminaison : • Option 1 (recommandée) \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net \ https://cloudmanagerinfraprod.azurecr.io	Pour obtenir des images pour les mises à niveau de l'agent de console. NetApp recommande d'autoriser les points de terminaison de l'option 1 dans votre pare-feu, car ils sont plus sécurisés, et d'interdire les points de terminaison de l'option 2. Notez les points suivants à propos de ces points de terminaison : • À partir de la version 3.9.47 de l'agent de console, le système prend en charge les points de terminaison répertoriés dans l'option 1. Les versions précédentes de l'agent de console ne prennent pas en charge la compatibilité descendante. • L'agent de la console contacte d'abord les points de terminaison dans l'option 2. Si ces points de terminaison ne sont pas accessibles, il contacte automatiquement les points de terminaison de l'option 1. • Si vous utilisez l'agent de console avec NetApp Backup and Recovery ou Ransomware Resilience, le système ne prend pas en charge les points de terminaison Option 1. Autoriser les points de terminaison de l'option 2 et interdire l'option 1.

Points de terminaison d'agent sur site

Connaissances et soutien

Inscrivez-vous pour obtenir de l'aide

L'enregistrement du support est requis pour recevoir un support technique spécifique à BlueXP et à ses solutions et services de stockage. L'enregistrement du support est également requis pour activer les flux de travail clés pour les systèmes Cloud Volumes ONTAP .

L'inscription au support n'active pas la prise en charge NetApp pour un service de fichiers de fournisseur cloud. Pour obtenir une assistance technique relative à un service de fichiers de fournisseur cloud, à son infrastructure ou à toute solution utilisant le service, reportez-vous à « Obtenir de l'aide » dans la documentation BlueXP de ce produit.

- "Amazon FSx pour ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Présentation de l'enregistrement de l'assistance

Il existe deux formes d'inscription pour activer le droit au support :

- Enregistrement du numéro de série de votre compte BlueXP (votre numéro de série à 20 chiffres 960xxxxxxxx situé sur la page Ressources d'assistance dans BlueXP).

  Il s'agit de votre identifiant d'abonnement d'assistance unique pour tout service au sein de BlueXP. Chaque abonnement de support au niveau du compte BlueXP doit être enregistré.

- Enregistrement des numéros de série Cloud Volumes ONTAP associés à un abonnement sur la place de marché de votre fournisseur de cloud (il s'agit de numéros de série 909201xxxxxxxx à 20 chiffres).

  Ces numéros de série sont communément appelés *numéros de série PAYGO* et sont générés par BlueXP au moment du déploiement de Cloud Volumes ONTAP .

L'enregistrement des deux types de numéros de série permet des fonctionnalités telles que l'ouverture de tickets d'assistance et la génération automatique de dossiers. L'enregistrement est terminé en ajoutant des comptes NetApp Support Site (NSS) à BlueXP comme décrit ci-dessous.

Enregistrez BlueXP pour le support NetApp

Pour vous inscrire au support et activer le droit de support, un utilisateur de votre organisation (ou compte) BlueXP doit associer un compte de site de support NetApp à sa connexion BlueXP . La manière dont vous vous inscrivez au support NetApp dépend du fait que vous possédez déjà ou non un compte NetApp Support Site (NSS).

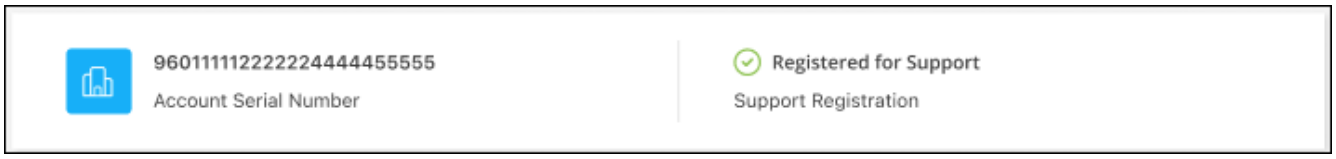
Client existant avec un compte NSS

Si vous êtes un client NetApp avec un compte NSS, il vous suffit de vous inscrire pour bénéficier du support via BlueXP.

Étapes

1. En haut à droite de la console BlueXP , sélectionnez l'icône Paramètres, puis sélectionnez **Informations d'identification**.
2. Sélectionnez **Informations d'identification de l'utilisateur**.
3. Sélectionnez **Ajouter des informations d'identification NSS** et suivez l'invite d'authentification du site de support NetApp (NSS).
4. Pour confirmer que le processus d'inscription a réussi, sélectionnez l'icône Aide, puis sélectionnez **Assistance**.

   La page **Ressources** devrait indiquer que votre organisation BlueXP est enregistrée pour bénéficier du support.

   Notez que les autres utilisateurs BlueXP ne verront pas ce même statut d'enregistrement de support s'ils n'ont pas associé un compte de site de support NetApp à leur connexion BlueXP . Cependant, cela ne signifie pas que votre organisation BlueXP n'est pas enregistrée pour bénéficier du support. Tant qu'un utilisateur de l'organisation a suivi ces étapes, votre organisation a été enregistrée.

Client existant mais pas de compte NSS

Si vous êtes un client NetApp existant avec des licences et des numéros de série existants mais pas de compte NSS, vous devez créer un compte NSS et l'associer à votre connexion BlueXP .

Étapes

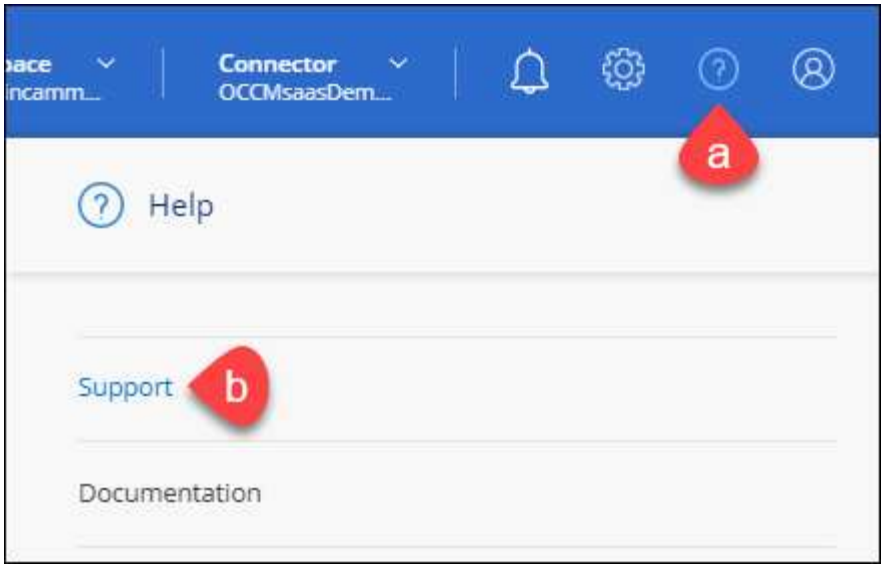
1. Créez un compte sur le site de support NetApp en remplissant le "Formulaire d'inscription des utilisateurs du site de support NetApp"
   a. Assurez-vous de sélectionner le niveau d'utilisateur approprié, qui est généralement * Client/Utilisateur final NetApp *.
   b. Assurez-vous de copier le numéro de série du compte BlueXP (960xxxx) utilisé ci-dessus pour le champ du numéro de série. Cela accélérera le traitement du compte.
2. Associez votre nouveau compte NSS à votre connexion BlueXP en suivant les étapes ci-dessousClient existant avec un compte NSS .

Tout nouveau chez NetApp

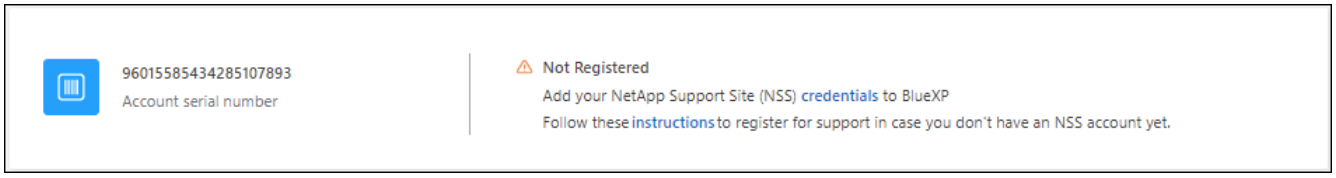
Si vous êtes nouveau sur NetApp et que vous n'avez pas de compte NSS, suivez chaque étape ci-dessous.

Étapes

1. Dans le coin supérieur droit de la console BlueXP , sélectionnez l'icône Aide, puis sélectionnez **Support**.



2. Recherchez le numéro de série de votre identifiant de compte sur la page d'inscription au support.



3. Accéder à "Site d'inscription au support de NetApp" et sélectionnez **Je ne suis pas un client NetApp enregistré**.
4. Remplissez les champs obligatoires (ceux avec des astérisques rouges).
5. Dans le champ **Gamme de produits**, sélectionnez **Cloud Manager**, puis sélectionnez votre fournisseur de facturation applicable.
6. Copiez le numéro de série de votre compte à l'étape 2 ci-dessus, effectuez la vérification de sécurité, puis confirmez que vous avez lu la politique de confidentialité des données mondiales de NetApp.

   Un email est immédiatement envoyé à la boîte mail prévue à cet effet pour finaliser cette transaction sécurisée. Assurez-vous de vérifier vos dossiers spam si l'e-mail de validation n'arrive pas dans quelques minutes.

7. Confirmez l'action depuis l'e-mail.

   La confirmation soumet votre demande à NetApp et vous recommande de créer un compte sur le site de support NetApp .

8. Créez un compte sur le site de support NetApp en remplissant le "Formulaire d'inscription des utilisateurs du site de support NetApp"
   a. Assurez-vous de sélectionner le niveau d'utilisateur approprié, qui est généralement * Client/Utilisateur final NetApp *.
   b. Assurez-vous de copier le numéro de série du compte (960xxxx) utilisé ci-dessus pour le champ du numéro de série. Cela accélérera le traitement.

Après avoir terminé

NetApp devrait vous contacter au cours de ce processus. Il s'agit d'un exercice d'intégration unique pour les nouveaux utilisateurs.

Une fois que vous avez votre compte de site de support NetApp , associez le compte à votre connexion BlueXP en suivant les étapes ci-dessousClient existant avec un compte NSS .

Associer les informations d'identification NSS pour la prise en charge de Cloud Volumes ONTAP

L'association des informations d'identification du site de support NetApp à votre organisation BlueXP est requise pour activer les workflows clés suivants pour Cloud Volumes ONTAP:

- Enregistrement des systèmes Cloud Volumes ONTAP prépayés pour le support

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

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

  Il est nécessaire de fournir votre compte NSS pour que BlueXP 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.

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

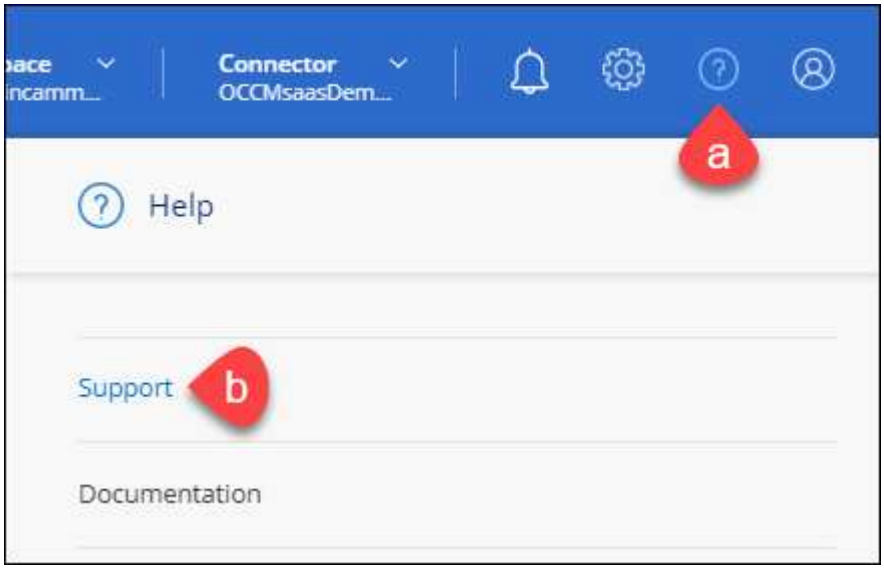
L'association des informations d'identification NSS à votre organisation BlueXP est différente du compte NSS associé à une connexion utilisateur BlueXP .

Ces informations d'identification NSS sont associées à votre ID d'organisation BlueXP spécifique. Les utilisateurs appartenant à l'organisation BlueXP peuvent accéder à ces informations d'identification depuis **Support > Gestion NSS**.

- Si vous disposez d'un compte client, vous pouvez ajouter un ou plusieurs comptes NSS.
- Si vous disposez d'un compte partenaire ou revendeur, vous pouvez ajouter un ou plusieurs comptes NSS, mais ils ne peuvent pas être ajoutés aux côtés des comptes de niveau client.

Étapes

1. Dans le coin supérieur droit de la console BlueXP , sélectionnez l'icône Aide, puis sélectionnez **Support**.



2. Sélectionnez **Gestion NSS > Ajouter un compte NSS**.
3. 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 spécifiques au support et aux licences.

4. Sur la page de connexion, indiquez votre adresse e-mail et votre mot de passe enregistrés sur le site de support NetApp pour effectuer le processus d'authentification.

   Ces actions permettent à BlueXP d'utiliser votre compte NSS pour des tâches telles que les téléchargements de licences, la vérification des mises à niveau de logiciels et les futures inscriptions au support.

   Notez ce qui suit :

   - Le compte NSS doit être un compte de niveau client (pas un compte invité ou temporaire). Vous pouvez avoir plusieurs comptes NSS au niveau client.
   - Il ne peut y avoir qu'un seul compte NSS si ce compte est un compte de niveau partenaire. Si vous essayez d'ajouter des comptes NSS au niveau client et qu'un compte au niveau partenaire existe, vous obtiendrez le message d'erreur suivant :

     « Le type de client NSS n'est pas autorisé pour ce compte car il existe déjà des utilisateurs NSS de types différents. »

   Il en va de même si vous disposez de comptes NSS préexistants au niveau client et que vous essayez d'ajouter un compte au niveau partenaire.

   - 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.

Obtenir de l'aide

NetApp fournit un support pour NetApp Console et ses services cloud de diverses manières. De nombreuses options d'auto-assistance gratuites sont disponibles 24h/24 et 7j/7, telles que des articles de la base de connaissances (KB) et un forum communautaire. Votre inscription au support inclut une assistance technique à distance via un ticket web.

Obtenir de l'aide pour un service de fichiers d'un fournisseur cloud

Pour obtenir une assistance technique relative à un service de fichiers de fournisseur cloud, à son infrastructure ou à toute solution utilisant le service, reportez-vous à la documentation de ce produit.

- "Amazon FSx pour ONTAP"
- "Azure NetApp Files"
- "Google Cloud NetApp Volumes"

Pour bénéficier d'un support technique spécifique à NetApp et à ses solutions de stockage et services de données, utilisez les options de support décrites ci-dessous.

Utiliser les options d'auto-assistance

Ces options sont disponibles gratuitement, 24 heures sur 24, 7 jours sur 7 :

- Documentation

  La documentation de la console NetApp que vous consultez actuellement.

- "Base de connaissances"

  Recherchez dans la base de connaissances NetApp pour trouver des articles utiles pour résoudre les problèmes.

- "Communautés"

  Rejoignez la communauté NetApp Console pour suivre les discussions en cours ou en créer de nouvelles.

Créer un dossier auprès du support NetApp

En plus des options d'auto-assistance ci-dessus, vous pouvez travailler avec un spécialiste du support NetApp pour résoudre tout problème après avoir activé le support.

Avant de commencer

- Pour utiliser la fonctionnalité **Créer un dossier**, vous devez d'abord associer vos informations d'identification du site de support NetApp à votre connexion à la console. "Découvrez comment gérer les informations d'identification associées à votre connexion à la console" .
- Si vous ouvrez un dossier pour un système ONTAP doté d'un numéro de série, votre compte NSS doit être associé au numéro de série de ce système.

Étapes

1. Dans la console NetApp , sélectionnez **Aide > Support**.
2. Sur la page **Ressources**, choisissez l'une des options disponibles sous Support technique :

   a. Sélectionnez **Appelez-nous** si vous souhaitez parler à quelqu'un au téléphone. Vous serez redirigé vers une page sur netapp.com qui répertorie les numéros de téléphone que vous pouvez appeler.

   b. Sélectionnez **Créer un dossier** pour ouvrir un ticket avec un spécialiste du support NetApp :

      - **Service** : sélectionnez le service auquel le problème est associé. Par exemple, * NetApp Console* lorsqu'il s'agit d'un problème de support technique lié aux flux de travail ou aux fonctionnalités de la console.
      - **Système** : Si applicable au stockage, sélectionnez * Cloud Volumes ONTAP* ou **On-Prem**, puis l'environnement de travail associé.

        La liste des systèmes est dans le périmètre de l'organisation de la console et de l'agent de console

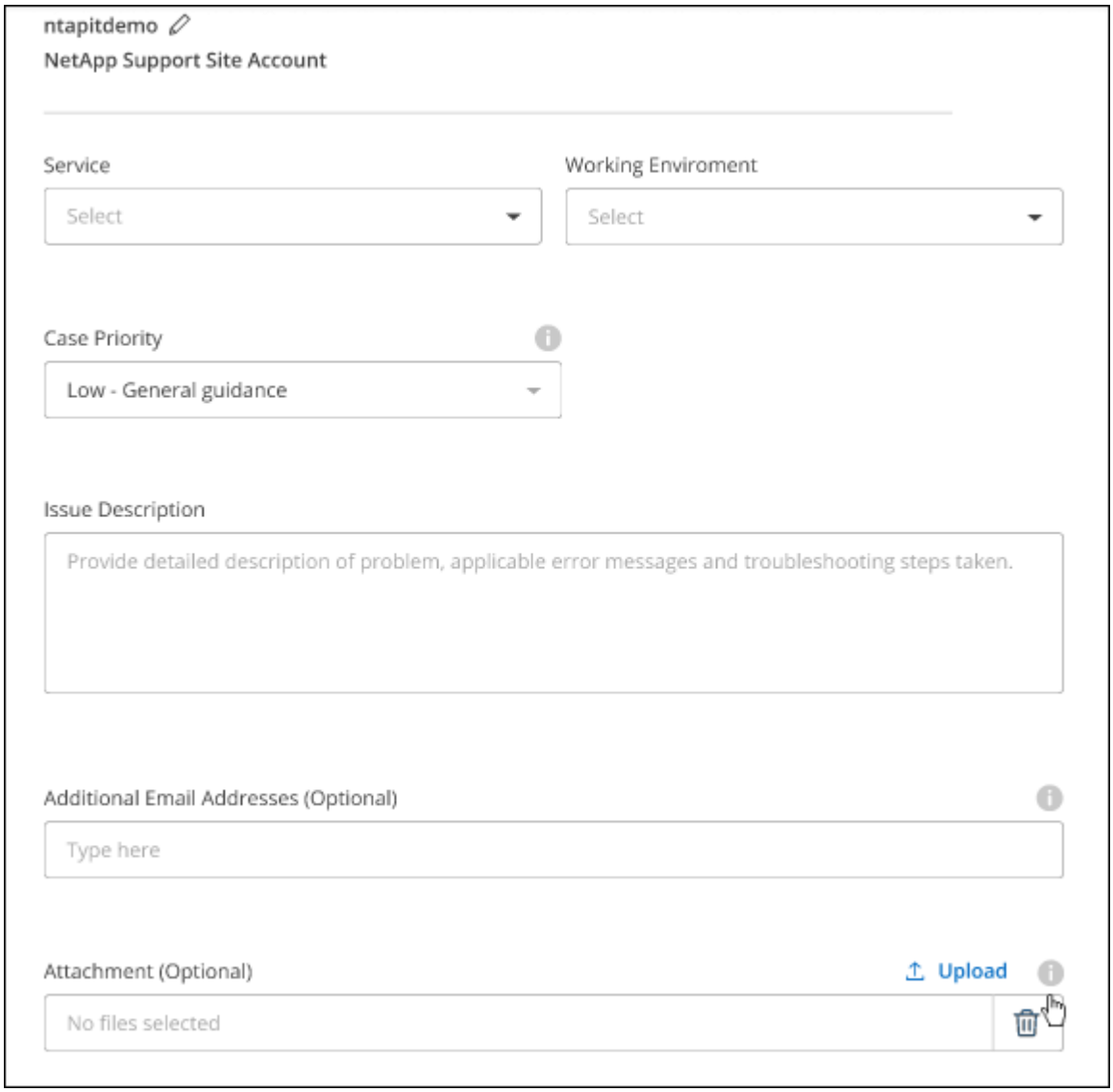
que vous avez sélectionné dans la bannière supérieure.

- **Priorité du cas** : Choisissez la priorité du cas, qui peut être Faible, Moyenne, Élevée ou Critique.

  Pour en savoir plus sur ces priorités, passez votre souris sur l'icône d'information à côté du nom du champ.

- **Description du problème** : Fournissez une description détaillée de votre problème, y compris tous les messages d'erreur applicables ou les étapes de dépannage que vous avez effectuées.
- **Adresses e-mail supplémentaires** : saisissez des adresses e-mail supplémentaires si vous souhaitez informer quelqu'un d'autre de ce problème.
- **Pièce jointe (facultatif)** : Téléchargez jusqu'à cinq pièces jointes, une à la fois.

  Les pièces jointes sont limitées à 25 Mo par fichier. Les extensions de fichiers suivantes sont prises en charge : txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx et csv.



Après avoir terminé

Une fenêtre contextuelle apparaîtra avec votre numéro de dossier d'assistance. Un spécialiste du support NetApp examinera votre cas et vous répondra dans les plus brefs délais.

Pour un historique de vos demandes d'assistance, vous pouvez sélectionner **Paramètres > Chronologie** et rechercher les actions nommées « créer une demande d'assistance ». Un bouton à l'extrême droite vous permet de développer l'action pour voir les détails.

Il est possible que vous rencontriez le message d'erreur suivant lorsque vous essayez de créer un dossier :

« Vous n'êtes pas autorisé à créer un dossier contre le service sélectionné »

Cette erreur peut signifier que le compte NSS et la société d'enregistrement à laquelle il est associé ne sont pas la même société d'enregistrement pour le numéro de série du compte NetApp Console (c'est-à-dire. 960xxxx) ou le numéro de série de l'environnement de travail. Vous pouvez demander de l'aide en utilisant l'une des options suivantes :

- Soumettez un cas non technique à https://mysupport.netapp.com/site/help

Gérez vos cas d'assistance

Vous pouvez afficher et gérer les cas d'assistance actifs et résolus directement depuis la console. Vous pouvez gérer les cas associés à votre compte NSS et à votre entreprise.

Notez ce qui suit :

- Le tableau de bord de gestion des cas en haut de la page offre deux vues :
  - La vue de gauche montre le nombre total de dossiers ouverts au cours des 3 derniers mois par le compte utilisateur NSS que vous avez fourni.
  - La vue de droite affiche le nombre total de dossiers ouverts au cours des 3 derniers mois au niveau de votre entreprise en fonction de votre compte utilisateur NSS.

  Les résultats du tableau reflètent les cas liés à la vue que vous avez sélectionnée.
- Vous pouvez ajouter ou supprimer des colonnes d'intérêt et filtrer le contenu des colonnes telles que Priorité et Statut. D'autres colonnes fournissent simplement des capacités de tri.

  Consultez les étapes ci-dessous pour plus de détails.
- Au niveau de chaque cas, nous offrons la possibilité de mettre à jour les notes du cas ou de fermer un cas qui n'est pas déjà au statut Fermé ou En attente de fermeture.

Étapes

1. Dans la console NetApp , sélectionnez **Aide > Support**.
2. Sélectionnez **Gestion des cas** et si vous y êtes invité, ajoutez votre compte NSS à la console.

   La page **Gestion des cas** affiche les cas ouverts liés au compte NSS associé à votre compte utilisateur de la console. Il s'agit du même compte NSS qui apparaît en haut de la page **Gestion NSS**.
3. Modifiez éventuellement les informations qui s'affichent dans le tableau :
   - Sous **Cas de l'organisation**, sélectionnez **Afficher** pour afficher tous les cas associés à votre entreprise.
   - Modifiez la plage de dates en choisissant une plage de dates exacte ou en choisissant une période différente.
   - Filtrer le contenu des colonnes.

- Modifiez les colonnes qui apparaissent dans le tableau en sélectionnant et ensuite choisir les colonnes que vous souhaitez afficher.

4. Gérer un dossier existant en sélectionnant et en sélectionnant l'une des options disponibles :
   - **Voir le cas** : Afficher tous les détails sur un cas spécifique.
   - **Mettre à jour les notes du cas** : fournissez des détails supplémentaires sur votre problème ou sélectionnez **Télécharger des fichiers** pour joindre jusqu'à un maximum de cinq fichiers.

     Les pièces jointes sont limitées à 25 Mo par fichier. Les extensions de fichiers suivantes sont prises en charge : txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx et csv.

   - **Fermer le dossier** : Fournissez des détails sur les raisons pour lesquelles vous fermez le dossier et sélectionnez **Fermer le dossier**.

Mentions légales

Les mentions légales donnent accès aux déclarations de droits d'auteur, aux marques déposées, aux brevets et bien plus encore.

Copyright

"https://www.netapp.com/company/legal/copyright/"

Marques de commerce

NETAPP, le logo NETAPP et les marques répertoriées sur la page Marques NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

"https://www.netapp.com/company/legal/trademarks/"

Brevets

Une liste actuelle des brevets détenus par NetApp est disponible à l'adresse suivante :

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

Politique de confidentialité

"https://www.netapp.com/company/legal/privacy-policy/"

Open source

Les fichiers d'avis fournissent des informations sur les droits d'auteur et les licences tiers utilisés dans les logiciels NetApp .

"Avis concernant la console NetApp"

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.