Commencer

NetApp Console setup and administration

NetApp
January 27, 2026

Sommaire

Commencer

Apprendre les bases

En savoir plus sur la NetApp Console

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.

Elle est disponible sous forme de plateforme de service (SaaS) ou en option auto-hébergée que vous pouvez installer dans votre cloud souverain. Il assure la gestion du stockage, la mobilité des données, la protection des données, ainsi que l'analyse et le contrôle des données. Les fonctionnalités de gestion sont assurées par une console web et des API.

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

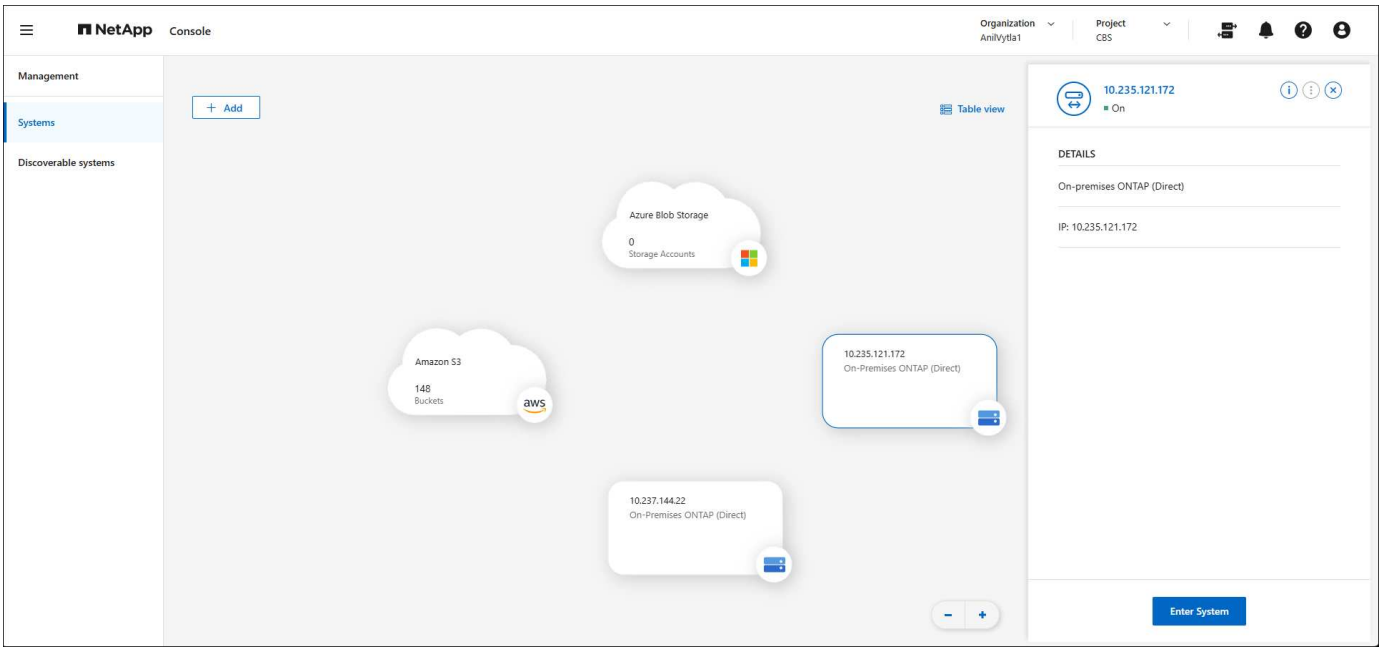
- Systèmes de la série E
- Clusters ONTAP
- Systèmes StorageGRID

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 .

NetApp Backup and Recovery

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

NetApp Data Classification

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

NetApp Copy and Sync

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.

Licenses and subscriptions

Gérez et surveillez vos licences et abonnements.

NetApp Disaster Recovery

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.

NetApp Ransomware Resilience

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

NetApp Replication

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.

NetApp Cloud Tiering

Étendez votre stockage ONTAP sur site au cloud.

NetApp Volume Caching

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 NetApp Console 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 NetApp Console 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 NetApp Console

La NetApp Console 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 NetApp Console"

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" .

Déploiement SaaS versus cloud souverain

Vous pouvez commencer à utiliser NetApp Console en vous inscrivant à l'offre SaaS ou en la déployant dans votre cloud souverain. Lorsque vous déployez NetApp Console dans un cloud souverain, NetApp limite la connectivité sortante afin de répondre aux exigences de sécurité et de conformité de votre organisation. Toutes les fonctionnalités et tous les services ne sont pas disponibles lorsque la console est déployée dans un cloud souverain.

NetApp continue de proposer BlueXP pour les sites qui ne souhaitent aucune connectivité sortante. BlueXP peut être installé sur votre réseau sans connectivité sortante. "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 modes de déploiement de la NetApp Console

La NetApp Console 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 NetApp Console 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 NetApp Console 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 NetApp Console 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 .

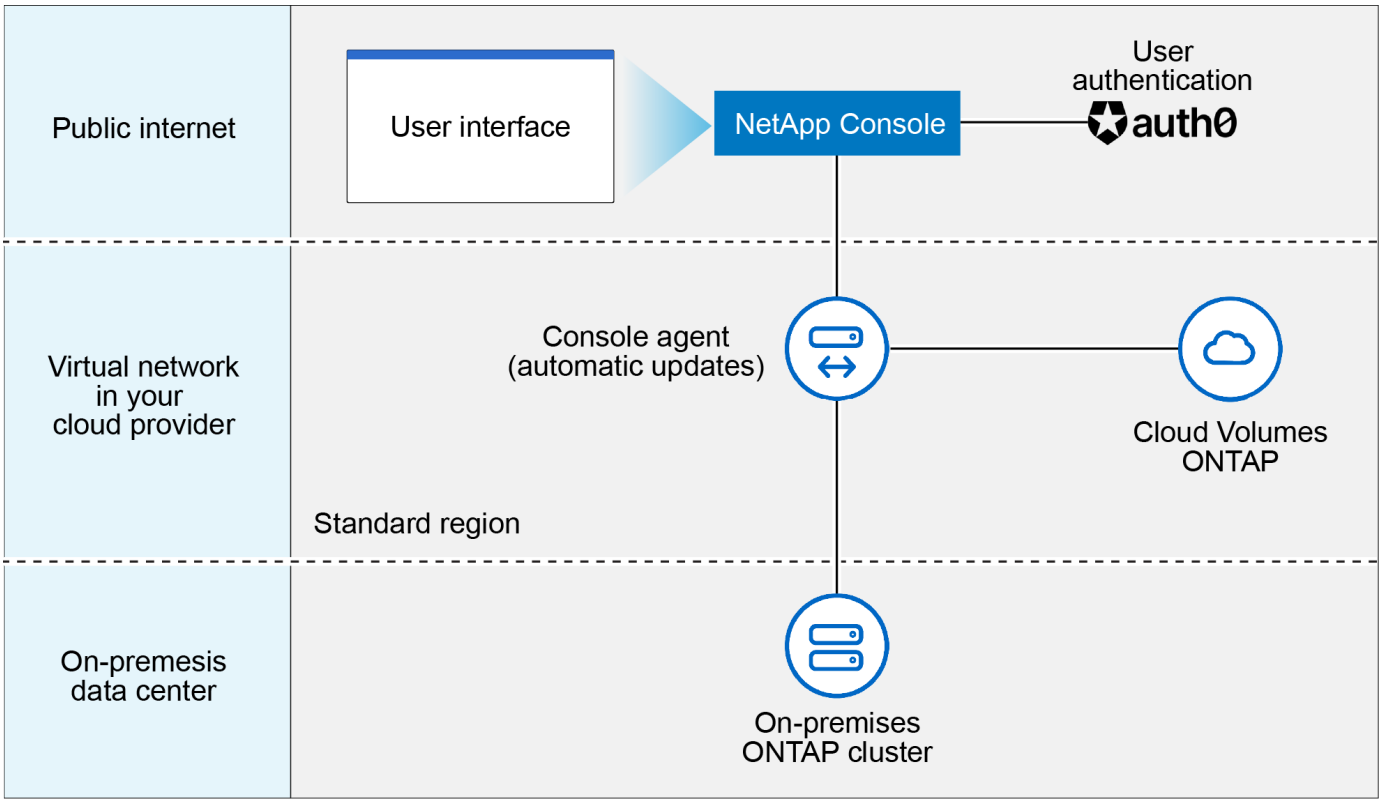
	Mode standard	Mode restreint
Connexion requise à la couche SaaS de la NetApp Console ?	Oui	Sortie uniquement
Connexion requise à votre fournisseur cloud ?	Oui	Oui, dans la région
Installation de l'agent de console	Depuis la console, la place de marché cloud ou l'installation manuelle	Place de marché 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

	Mode standard	Mode restreint
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 NetApp Console 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
- Utilisation manuelle d'un programme d'installation 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.

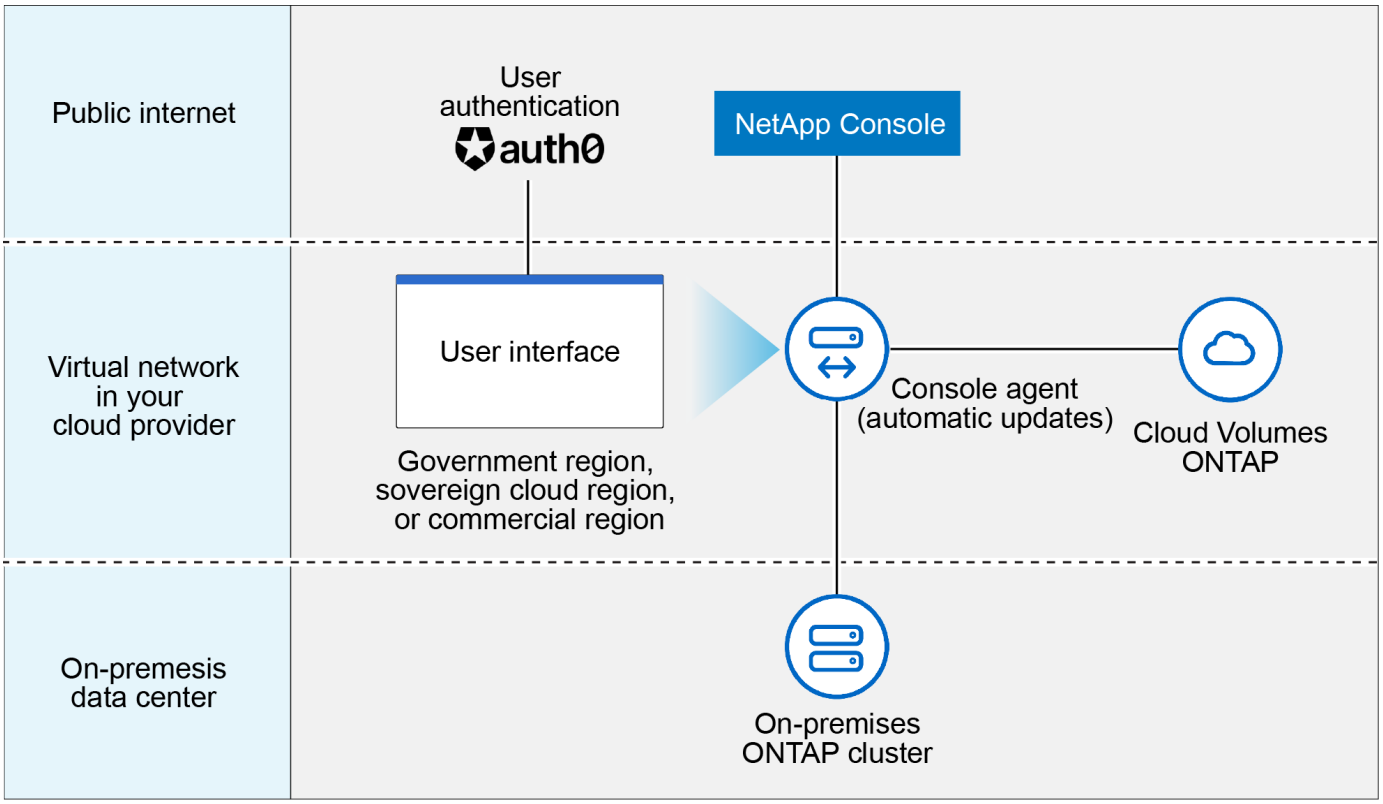
Comment démarrer avec le mode standard

Aller à la "NetApp Console" 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.
NetApp Data Classification	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
Licenses and subscriptions	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

Domaine de produits	Service ou fonctionnalité de données NetApp	Mode restreint
Services de données	Sauvegarde et récupération NetApp	Ouihttps://docs.netapp.com/us-en/data-services-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"^]
	NetApp Data Classification	Oui
	NetApp Copy and Sync	Non
	NetApp Disaster Recovery	Non
	NetApp Ransomware Resilience	Non
	NetApp Replication	Oui
	NetApp Cloud Tiering	Non
	Mise en cache des volumes NetApp	Non
	Usine de charges de travail NetApp	Non
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

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

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

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

Aperçu

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

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

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

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

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

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

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

Ajouter un compte NSS

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

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

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

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

Étapes

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

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

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

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

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

Quelle est la prochaine étape ?

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

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

Mettre à jour les informations d'identification NSS

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

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

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

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

Étapes

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

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

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

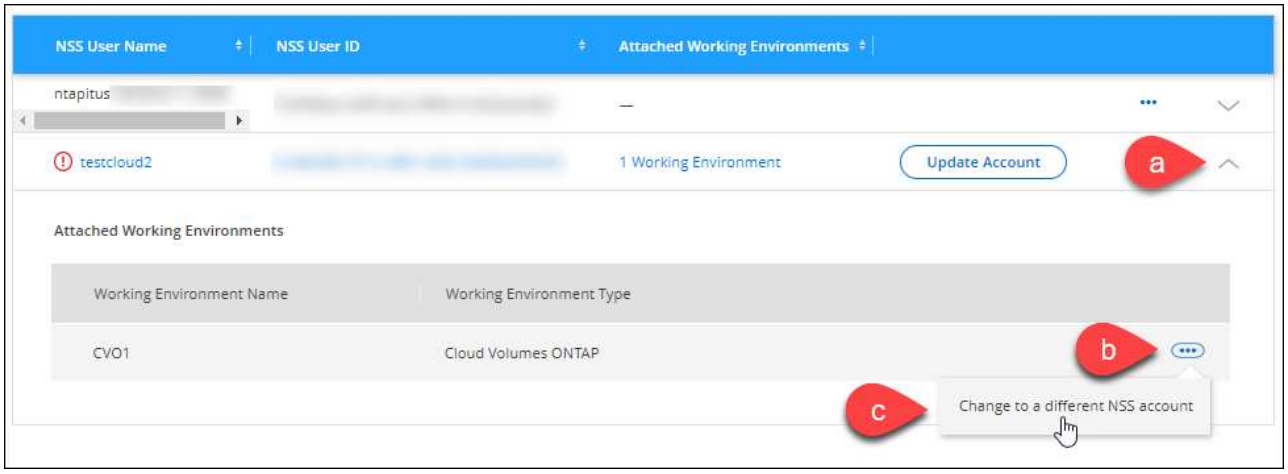
Attacher un système à un autre compte NSS

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

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

Étapes

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



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

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

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

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

Étapes

1. Dans **Administration > Support**.
2. Sélectionnez **Gestion NSS**.
3. Pour le compte NSS que vous souhaitez mettre à jour, sélectionnez ••• puis sélectionnez **Afficher l'adresse e-mail**. Vous pouvez utiliser le bouton Copier pour copier l'adresse e-mail.

Supprimer un compte NSS

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

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

Étapes

1. Dans **Administration > Support**.

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

En savoir plus sur les agents de la NetApp Console

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

Un agent Console vous permet de :

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

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

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

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

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

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

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

Les agents de console doivent être opérationnels à tout moment

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

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

Emplacements pris en charge

Vous pouvez installer des agents aux emplacements suivants :

- Amazon Web Services
- Microsoft Azure

  Déployez un agent de console dans Azure dans la même région que les systèmes Cloud Volumes ONTAP qu'il gère. Alternativement, déployez-le dans le "Paire de régions Azure" . Cela garantit qu'une connexion Azure Private Link est utilisée entre Cloud Volumes ONTAP et ses comptes de stockage associés. "Découvrez comment Cloud Volumes ONTAP utilise un lien privé Azure"

- Google Cloud

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

- Dans vos locaux

Communication avec les fournisseurs de cloud

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

Mode restreint

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

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

Comment installer un agent de console

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

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

Autorisations du fournisseur de cloud

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

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

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

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

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

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

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

Mises à niveau des agents

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

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

Maintenance du système d'exploitation et des machines virtuelles

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

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

Si vous (client) devez arrêter puis démarrer la machine virtuelle de l'agent de console, vous devez le faire à partir de la console de votre fournisseur de cloud ou en utilisant les procédures standard de gestion sur site.

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

Systèmes et agents multiples

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

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

Voici quelques exemples de déploiements d’agents :

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

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

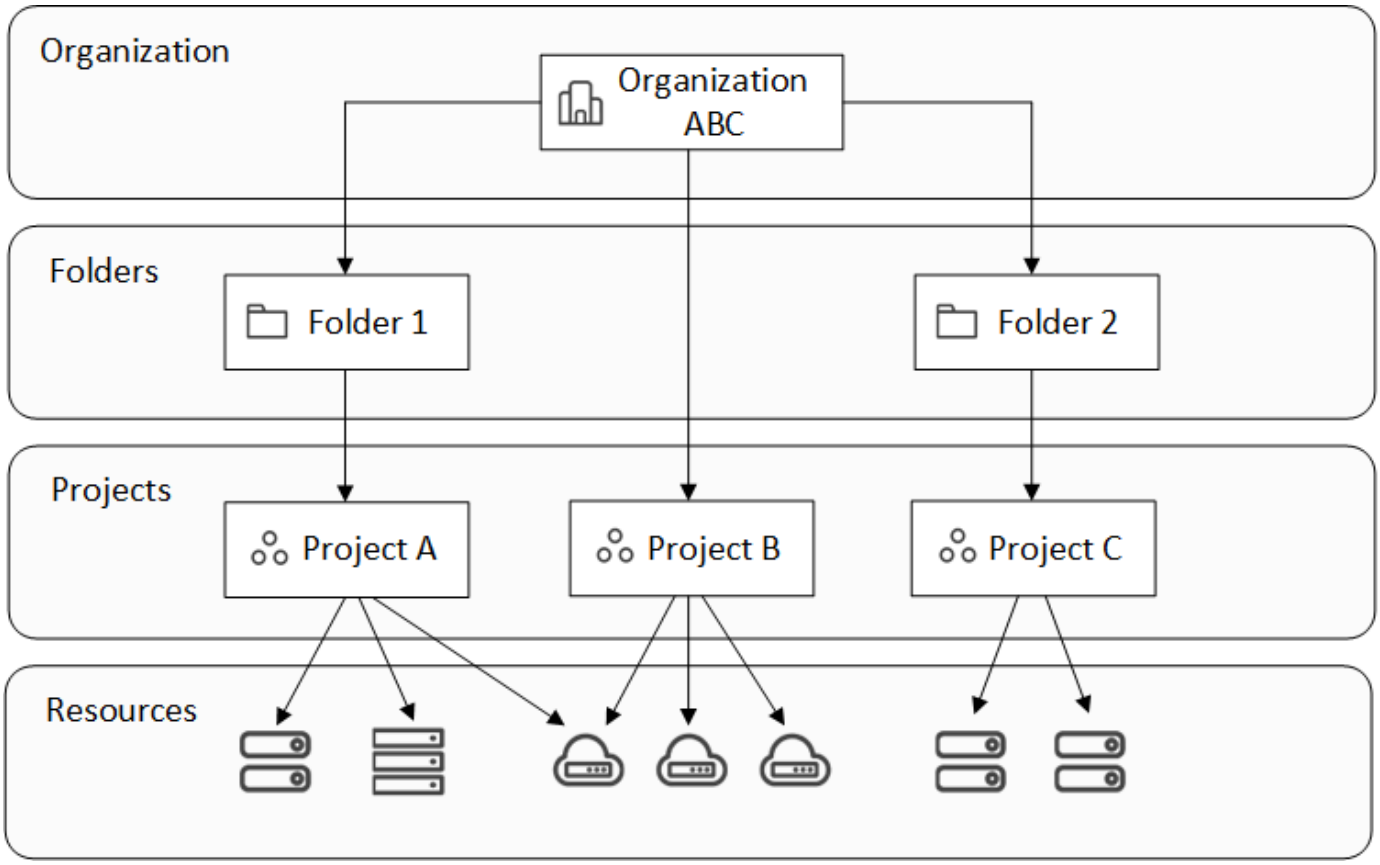
Utilisez la gestion des identités et des accès (IAM) de la console NetApp pour organiser vos ressources NetApp et contrôler l’accès en fonction de la structure de votre entreprise : par emplacement, département ou projet.

Les ressources sont organisées de manière hiérarchique : l’organisation se trouve au sommet, suivie des dossiers (qui peuvent contenir d’autres dossiers ou projets), puis des projets, qui contiennent des systèmes de stockage, des charges de travail et des agents.

Attribuez des autorisations de contrôle d’accès basé sur les rôles (RBAC) aux membres au niveau de l’organisation, du dossier ou du projet afin de garantir que les utilisateurs disposent de l’accès approprié aux ressources.

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

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



]

Composants de gestion des identités et des accès

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

Projets et dossiers au sein de votre organisation

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

Organisation

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

Projets

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

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

"Découvrez comment ajouter des projets à votre organisation."

Dossiers

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

"Apprenez comment ajouter des dossiers à votre organisation."

Ressources

Les *ressources* comprennent les systèmes de stockage, les abonnements Keystone , ainsi que les agents Console.

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

+

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

+

"Apprenez à associer des ressources à des projets."

Systèmes de stockage et abonnements Keystone

Les systèmes de stockage sont les principales ressources que vous gérez dans la NetApp Console. La NetApp Console prend en charge la gestion des systèmes de stockage sur site et dans le cloud. Vous devez ajouter un système de stockage à un projet avant que quiconque puisse y accéder.

Les systèmes de stockage sont automatiquement associés au projet dans lequel ils sont ajoutés, mais vous pouvez également les associer à d'autres projets ou dossiers depuis la page **Ressources**.

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

Agents de console

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

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

"Apprenez comment associer des agents à des projets."

Membres et rôles

Membres

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

Vous devez ajouter des membres à votre organisation après leur inscription à NetApp Console. Une fois ajoutés, vous pouvez leur attribuer des rôles pour leur donner accès aux ressources. Vous pouvez ajouter

manuellement des comptes de service depuis la console ou automatiser leur création et leur gestion via l'API IAM de la NetApp Console .

"Découvrez comment ajouter des membres à votre organisation."

Rôles d'accès

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

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

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

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

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

Exemples de stratégie IAM

stratégie des petites organisations

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

Exemple : Société ABC (équipe de 5 personnes)

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

Stratégie d'entreprise multirégionale

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

Exemple : Société XYZ (entreprise multinationale)

- **Structure :** Organisation > Dossiers régionaux (Amérique du Nord, Europe, Asie-Pacifique) > Dossiers de projet par région
- **Rôles de la plateforme :**
  - 1 **Administration de l'organisation** : Supervision globale et gestion des politiques
  - 3 **Administrateurs de dossiers ou de projets** : Contrôle régional (un par région)

    - 1 **Administrateur de la fédération** : Intégration du fournisseur d'identité d'entreprise
- **Rôles de stockage par région :**
    - 9 **Administration du stockage** : Découvrir et gérer les systèmes de stockage dans les régions attribuées
    - 2 **Visualiseur de stockage** : Surveillez les ressources de stockage dans différentes régions
    - 1 **Spécialiste de la santé du système** : Gérer la santé du stockage sans modifier le système
- **Rôles du service de données :**
    - Administration des sauvegardes et des restaurations : par projet, selon les responsabilités liées aux sauvegardes.
    - **Administrateur de la résilience aux ransomwares** : Supervision de l'équipe de sécurité sur l'ensemble des projets
- **Stratégie d'agents :** Agents régionaux associés à des projets géographiques appropriés
- **Avantages :** Sécurité renforcée grâce à la séparation des rôles, à l'autonomie régionale et au respect des réglementations locales

stratégie de spécialisation départementale

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

Exemple : TechCorp (entreprise technologique de taille moyenne)

- **Structure :** Organisation > Dossiers de département (Informatique, Sécurité, Développement) > Ressources spécifiques au projet
- **Rôles spécialisés :**
    - Équipe de sécurité : rôles d'administrateur de la résilience aux ransomwares et de consultant en classification.
    - Équipe de sauvegarde : **Super administrateur de sauvegarde et de restauration** pour des opérations de sauvegarde complètes
    - Équipe de développement : **Administrateur du stockage** pour la gestion de l'environnement de test
    - Équipe de conformité : **Analyste de soutien aux opérations** pour le suivi et la gestion des cas de soutien
- **Stratégie relative aux agents :** Les agents sont rattachés aux projets départementaux en fonction de la propriété des ressources.
- **Avantages :** Contrôle d'accès personnalisé, efficacité opérationnelle accrue et responsabilisation claire pour les tâches spécialisées

Prochaines étapes avec IAM dans la NetApp Console

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

Démarrez avec NetApp Console (SaaS)

Flux de travail de démarrage (SaaS)

Commencez à utiliser la NetApp Console (SaaS) en préparant le réseau pour la console, en vous inscrivant et en créant un compte, puis en utilisant l'assistant de la console pour configurer les fonctionnalités initiales.

Vous accédez à une console Web hébergée en tant que produit logiciel en tant que service (SaaS) de NetApp. Vous pouvez utiliser la console pour gérer votre environnement de stockage cloud hybride et utiliser les services de données NetApp .

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

Assurez-vous que les ordinateurs accédant à la console NetApp disposent d'un accès réseau aux points de terminaison requis.

"Apprenez à préparer le réseau pour la console NetApp ."

"Inscrivez-vous et créez une organisation"

Allez à "Console NetApp" et inscrivez-vous. Si le système vous invite à créer une organisation et que vous pensez qu'une organisation existe déjà pour votre entreprise, fermez la boîte de dialogue et informez-en l'administrateur de votre organisation. S'il n'y a pas actuellement d'administrateur d'organisation pour votre entreprise, vous pouvez revendiquer ce rôle. "Apprenez comment contacter un administrateur de l'organisation."

À ce stade, vous êtes connecté et pouvez utiliser l'assistant NetApp pour commencer à configurer la console. Pour commencer, associez votre compte de support NetApp et un agent Console pour activer toutes les fonctionnalités.

Si vous choisissez de ne pas utiliser l'assistant NetApp ou d'installer un agent Console, vous pouvez commencer à gérer le stockage et à utiliser des services tels que Digital Advisor, Amazon FSx for ONTAP, Azure NetApp Files, et bien plus encore. "Découvrez ce que vous pouvez faire sans agent de console".

Associez votre compte NetApp Support Site (NSS).

L'association de votre compte NetApp Support Site (NSS) à la console vous permet de gérer plus facilement vos licences et abonnements et d'accéder aux ressources d'assistance directement depuis la console.

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"

5 **Ajouter un système de stockage à la console**

Dans la NetApp Console, vous pouvez ajouter ou découvrir des systèmes de stockage pour gérer votre environnement de stockage cloud hybride. Utilisez l'assistant NetApp pour ajouter votre premier système de stockage.

Si vous installez un agent Console dans AWS, Microsoft Azure ou Google Cloud, la Console détecte automatiquement les informations relatives aux compartiments Amazon S3, au stockage Blob Azure ou aux compartiments Google Cloud Storage à l'emplacement où l'agent est installé. Ces systèmes sont automatiquement ajoutés à la page **Systèmes**.

- "Apprenez à découvrir un système ONTAP"
- "Découvrez comment utiliser un système StorageGRID"
- "Découvrez comment découvrir un système de la série E"

6 **"Abonnez-vous aux NetApp Intelligent Services (facultatif)"**

Inscrivez-vous aux NetApp Intelligent Services via votre fournisseur de cloud pour une facturation horaire (PAYGO) ou annuelle. Un abonnement comprend NetApp Backup and Recovery, Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience, NetApp Disaster Recovery et NetApp Data Classification.

Préparer l'accès réseau pour la NetApp Console

La NetApp Console, l'agent de la NetApp Console 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 NetApp Console en tant que logiciel en tant que service (SaaS)
- Agents de console que vous installez sur site ou dans le cloud. Agents de console.

Avec la version 4.0.0, 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 NetApp Console et les agents de la console

Chaque agent que vous déployez et chaque ordinateur qui accède à la NetApp Console doivent disposer de connexions aux points de terminaison répertoriés ci-dessous.

Les agents de console déployés chez votre fournisseur de cloud doivent avoir accès aux points de terminaison respectifs de ce fournisseur de cloud.

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

Les points de terminaison du fournisseur de cloud ont contacté l'agent de la console

Les agents de console doivent avoir accès à des points de terminaison supplémentaires s'ils sont déployés chez votre fournisseur de cloud.

Configurez l'accès au point de terminaison du réseau du fournisseur de cloud 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"

Points de terminaison des services de données contactés par l'agent de la console

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"

Points de terminaison pour les charges de travail

L'agent de la console doit pouvoir accéder au point de terminaison suivant pour les charges de travail NetApp .

Points de terminaison	But
https://api.workloads.netapp.com	La console Web contacte ce point de terminaison pour interagir avec les API Workload Factory afin de gérer et d'exploiter les charges de travail basées sur FSx pour ONTAP.

Inscrivez-vous ou connectez-vous à la NetApp Console

Pour utiliser la console, inscrivez-vous ou connectez-vous avec vos identifiants du site de support NetApp , ou créez un compte de connexion à la NetApp Console . Si vous êtes le premier de votre entreprise à vous inscrire, vous créez une nouvelle organisation en tant qu'administrateur. Si votre entreprise dispose déjà d'une organisation, inscrivez-vous ou connectez-vous avec vos identifiants existants du site de support NetApp ou l'authentification unique (SSO) de l'entreprise.

Inscrivez-vous à NetApp Console en tant qu'administrateur initial de l'organisation

Si votre entreprise ne dispose pas d'une organisation NetApp Console , inscrivez-vous pour en créer une. Le premier utilisateur devient l'administrateur de l'organisation et gère les comptes et les autorisations des utilisateurs. Vous pourrez modifier les rôles et ajouter d'autres administrateurs ultérieurement.

Étapes

1. Ouvrez un navigateur Web et accédez à la "NetApp Console"
2. Si vous possédez un compte sur le site d'assistance NetApp , saisissez directement l'adresse électronique associée à votre compte sur la page **Connexion**.

   La console vous inscrit automatiquement lors de cette première connexion avec vos identifiants du site d'assistance NetApp .

3. Si vous souhaitez vous inscrire en créant une connexion à la console, sélectionnez **S'inscrire**.
   a. Sur la page **Inscription**, saisissez les informations requises et sélectionnez **Suivant**.

      Seuls les caractères anglais sont autorisés dans le formulaire d'inscription.

   b. Consultez votre boîte de réception pour obtenir un e-mail de NetApp contenant des instructions pour vérifier votre adresse e-mail.

      Vérifiez votre adresse e-mail pour finaliser votre inscription.

4. Après vous être connecté, veuillez lire et accepter le contrat de licence utilisateur final.
5. Sur la page **Bienvenue**, créez une organisation.
6. Sélectionnez **Commençons**.

+ En tant que nouvel utilisateur et administrateur de l'organisation, vous suivez un processus guidé pour ajouter des ressources de stockage, créer un agent Console, et plus encore. "Découvrez comment utiliser l'assistant de console."

Prochaines étapes

En tant qu'administrateur, une fois que vous avez suivi les étapes indiquées dans l'Assistant de console, vous devez planifier votre stratégie d'identité et d'accès, ajouter des utilisateurs à votre organisation et leur attribuer des rôles. "Découvrez la gestion des identités et des accès pour la NetApp Console."

Inscrivez-vous ou connectez-vous à la NetApp Console lorsqu'une organisation existe déjà.

Si votre entreprise possède déjà une organisation NetApp Console , inscrivez-vous ou connectez-vous pour y accéder. Votre méthode d'inscription ou de connexion dépend de si votre entreprise utilise la fédération d'identités ou possède des identifiants pour le site de support NetApp . Sinon, créez un compte de connexion à la NetApp Console .

Étapes

1. Ouvrez un navigateur Web et accédez à la "NetApp Console"
2. Si vous possédez un compte sur le site d'assistance NetApp ou si votre entreprise a configuré l'authentification unique (SSO), saisissez votre adresse e-mail associée ou vos identifiants SSO sur la page **Connexion**. Suivez les instructions pour terminer la connexion.

   Dans les deux cas, vous êtes inscrit à la console dans le cadre de cette connexion initiale.

3. Si vous souhaitez vous inscrire en créant une connexion à la console, sélectionnez **S'inscrire**.
   a. Sur la page **Inscription**, saisissez les informations requises et sélectionnez **Suivant**.

      Seuls les caractères anglais sont autorisés dans le formulaire d'inscription.

   b. Consultez votre boîte de réception pour obtenir un e-mail de NetApp contenant des instructions pour vérifier votre adresse e-mail.

      Vérifiez votre adresse e-mail pour finaliser votre inscription.

4. Après vous être connecté, veuillez lire et accepter le contrat de licence utilisateur final.
5. Si le système vous invite à créer une organisation, fermez la boîte de dialogue et informez-en un administrateur de la console afin qu'il puisse vous ajouter à votre organisation et vous donner accès.

"Apprenez comment contacter un administrateur de l'organisation."

Prochaines étapes

Une fois que vous aurez accès à votre organisation, vous pourrez commencer à gérer le stockage et à utiliser les services de données qui vous sont attribués.

Commencer à utiliser l'assistant de la NetApp Console

Si vous êtes un nouvel utilisateur de la NetApp Console (SaaS) avec le rôle d'administrateur de l'organisation, vous pouvez utiliser l'assistant de la console pour vous guider tout au long du processus de configuration initiale. L'assistant vous aide à ajouter un compte NetApp Support Site (NSS), un agent Console, un cluster et 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 la console

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

Par défaut, la NetApp Console affiche l'assistant de console sur la page d'accueil pour les nouveaux utilisateurs qui possèdent le rôle d'administrateur de l'organisation. Elle reste disponible jusqu'à ce que vous ayez terminé les tâches obligatoires de création d'un agent Console et d'ajout d'un système.

Utilisez l'assistant pour effectuer ces tâches, qui constituent la configuration minimale de votre environnement NetApp Console :

- Ajoutez un compte de site de support NetApp (NSS).

  "Apprenez comment ajouter un compte NSS".

- Connectez-vous à votre infrastructure de stockage en déployant un agent Console.

  "Découvrez comment installer un agent Console sur site."

- Gérez un système de stockage en ajoutant ou en découvrant un cluster
- Ajoutez un abonnement au marketplace ou une licence PAYGO.

  "Apprenez comment ajouter des licences et des abonnements".

- Consultez les informations sur les services de données.

Premiers pas avec la NetApp Console (mode restreint)

Démarrage du flux de travail (mode restreint)

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

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

1 **"Préparez-vous au déploiement"**

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

2 **"Déployer l'agent de console"**

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

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

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

Préparez-vous au déploiement en mode restreint

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

Étape 1 : Comprendre le fonctionnement du mode restreint

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

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

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

"Découvrez comment fonctionne le mode restreint" .

Étape 2 : Examiner les options d'installation

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

- Depuis la place de marché AWS
- Depuis la place de marché Azure

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

Étape 3 : Examiner les exigences de l'hôte

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

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

Hôte dédié

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

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

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

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

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

Type d'instance AWS EC2

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

Taille de la machine virtuelle Azure

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

Type de machine Google Cloud

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

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

Hyperviseur

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

Exigences relatives au système d'exploitation et aux conteneurs

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

Système opérateur	Versions de systèmes d'exploitation prises en charge	Versions d'agent prises en charge	Outil de conteneur requis	SELinux
Red Hat Enterprise Linux		9,6 • Versions en langue anglaise uniquement. • L'hôte doit être enregistré auprès de Red Hat Subscription Management. S'il n'est pas enregistré, l'hôte ne peut pas accéder aux référentiels pour mettre à jour le logiciel tiers requis lors de l'installation de l'agent.	4.0.0 ou version ultérieure avec la console en mode standard ou en mode restreint	Podman version 5.4.0 avec podman-compose 1.5.0. Afficher les exigences de configuration de Podman .
Pris en charge en mode d'application ou en mode permissif		9,1 à 9,4 • Versions en langue anglaise uniquement. • L'hôte doit être enregistré auprès de Red Hat Subscription Management. S'il n'est pas enregistré, l'hôte ne peut pas accéder aux référentiels pour mettre à jour le logiciel tiers requis lors de l'installation de l'agent.	3.9.50 ou version ultérieure avec la console en mode standard ou en mode restreint	Podman version 4.9.4 avec podman-compose 1.5.0. Afficher les exigences de configuration de Podman .

Système opérateur	Versions de systèmes d'exploitation prises en charge	Versions d'agent prises en charge	Outil de conteneur requis	SELinux
Pris en charge en mode d'application ou en mode permissif		8,6 à 8,10 • Versions en langue anglaise uniquement. • L'hôte doit être enregistré auprès de Red Hat Subscription Management. S'il n'est pas enregistré, l'hôte ne peut pas accéder aux référentiels pour mettre à jour le logiciel tiers requis lors de l'installation de l'agent.	3.9.50 ou version ultérieure avec la console en mode standard ou en mode restreint	Podman version 4.6.1 ou 4.9.4 avec podman-compose 1.0.6. Afficher les exigences de configuration de Podman .
Pris en charge en mode d'application ou en mode permissif	Ubuntu		24,04 LTS	3.9.45 ou version ultérieure avec la NetApp Console en mode standard ou en mode restreint
Docker Engine 23.06 à 28.0.0.	Non pris en charge		22,04 LTS	3.9.50 ou version ultérieure

Étape 4 : installer Podman ou Docker Engine

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

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

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

  Afficher les versions de Podman prises en charge .

- Docker Engine est requis pour Ubuntu.

  Afficher les versions de Docker Engine prises en charge .

Exemple 1. Étapes

Podman

Suivez ces étapes pour installer et configurer Podman :

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

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

Étapes

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

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

2. Installez Podman.

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

   a. Pour Red Hat Enterprise Linux 9,6 :

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

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

   b. Pour Red Hat Enterprise Linux 9.1 à 9.4 :

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

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

   c. Pour Red Hat Enterprise Linux 8 :

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

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

3. Activez et démarrez le service podman.socket.

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

4. Installez python3.

```
sudo dnf install python3
```

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

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

6. Si vous utilisez Red Hat Enterprise 9 :

   a. Installez le paquetage du dépôt EPEL.

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

   +

   a. Installez le package podman-compose 1.5.0.

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

7. Si vous utilisez Red Hat Enterprise Linux 8 :

   a. Installez le paquetage du dépôt EPEL.

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

   b. Installez le package podman-compose 1.0.6.

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

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

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

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

```
podman info | grep networkBackend
```

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

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

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

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

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

v. Redémarrez podman.

```
systemctl restart podman
```

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

```
podman info | grep networkBackend
```

Moteur Docker

Suivez la documentation de Docker pour installer Docker Engine.

Étapes

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

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

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

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

Étape 5 : Préparer l'accès au réseau

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

Connexions aux réseaux cibles

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

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

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

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

+

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

Accès Internet sortant pour les opérations quotidiennes

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

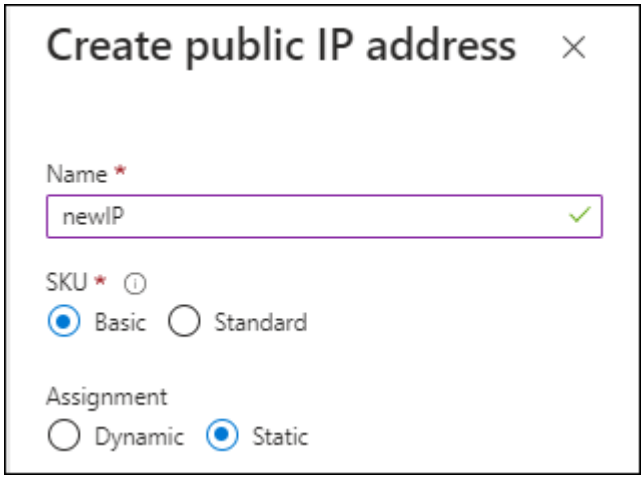
Points de terminaison	But
Environnements AWS	Services AWS (amazonaws.com) : • CloudFormation • Cloud de calcul élastique (EC2) • Gestion des identités et des accès (IAM) • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Service de stockage simple (S3)
Pour gérer les ressources AWS. Le point de terminaison dépend de votre région AWS. "Consultez la documentation AWS pour plus de détails"	Amazon FSX pour NetApp ONTAP: • api.workloads.netapp.com
La console Web contacte ce point de terminaison pour interagir avec les API Workload Factory afin de gérer et d'exploiter les charges de travail basées sur FSx pour ONTAP .	**Environnements Azure**
\ https://management.azure.com \ https://login.microsoftonline.com \ https://blob.core.windows.net \ https://core.windows.net	Pour gérer les ressources dans les régions publiques Azure.
\ https://management.usgovcloudapi.net \ https://login.microsoftonline.us \ https://blob.core.usgovcloudapi.net \ https://core.usgovcloudapi.net	Pour gérer les ressources dans les régions Azure Government.
\ https://management.chinacloudapi.cn \ https://login.chinacloudapi.cn \ https://blob.core.chinacloudapi.cn \ https://core.chinacloudapi.cn	Pour gérer les ressources dans les régions Azure Chine.

Points de terminaison	But
Environnements Google Cloud	\ https://www.googleapis.com/compute/v1/ \ https://compute.googleapis.com/compute/v1 \ https://cloudresourcemanager.googleapis.com/v1/projects \ https://www.googleapis.com/compute/beta \ https://storage.googleapis.com/storage/v1 \ https://www.googleapis.com/storage/v1 \ https://iam.googleapis.com/v1 \ https://cloudkms.googleapis.com/v1 \ https://config.googleapis.com/v1/projects
Pour gérer les ressources dans Google Cloud.	• Points de terminaison de la NetApp Console *
\ https://mysupport.netapp.com	Pour obtenir des informations de licence et envoyer des messages AutoSupport au support NetApp .
\ https://signin.b2c.netapp.com	Pour mettre à jour les informations d'identification du site de support NetApp (NSS) ou pour ajouter de nouvelles informations d'identification NSS à la NetApp Console.
\ https://support.netapp.com	Pour obtenir des informations de licence et envoyer des messages AutoSupport au support NetApp ainsi que pour recevoir des mises à jour logicielles pour Cloud Volumes ONTAP.
\ https://api.bluexp.netapp.com \ https://netapp-cloud-account.auth0.com \ https://netapp-cloud-account.us.auth0.com \ https://console.netapp.com \ https://components.console.bluexp.netapp.com \ https://cdn.auth0.com	Pour fournir des fonctionnalités et des services au sein de la NetApp Console.

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

Adresse IP publique dans Azure

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



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

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

"Documentation Azure : Référence IP publique"

Serveur proxy

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

- adresse IP
- Informations d'identification
- Certificat HTTPS

Ports

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

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

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

Activer NTP

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

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

Étape 6 : Préparer les autorisations cloud

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

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

Rôle AWS IAM

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

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

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

Étapes

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

Résultat

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

Clé d'accès AWS

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

Étapes

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

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

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

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

Rôle Azure

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

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

Étapes

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

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

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

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

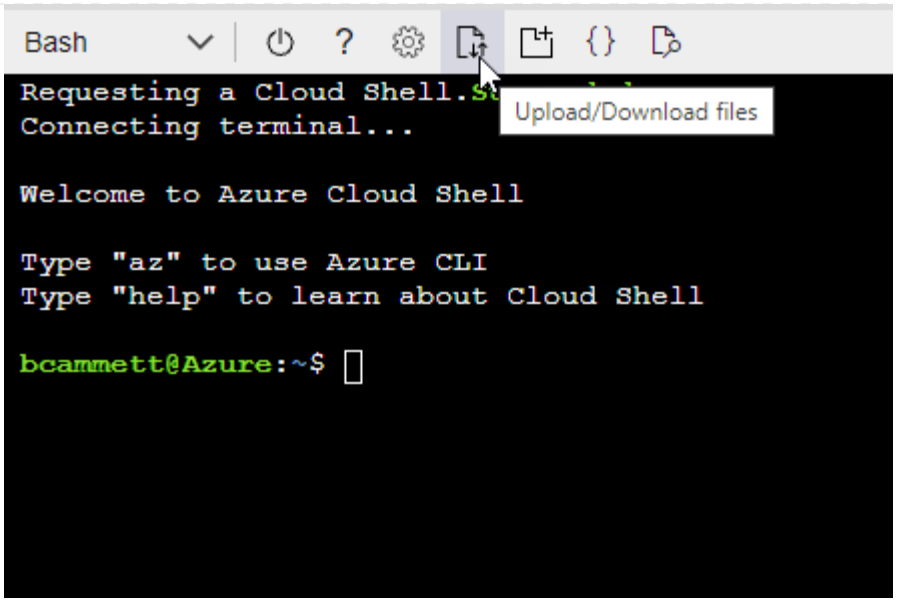
   Exemple

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

4. Utilisez le fichier JSON pour créer un rôle personnalisé dans Azure.

   Les étapes suivantes décrivent comment créer le rôle à l'aide de Bash dans Azure Cloud Shell.

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



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

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

Principal de service Azure

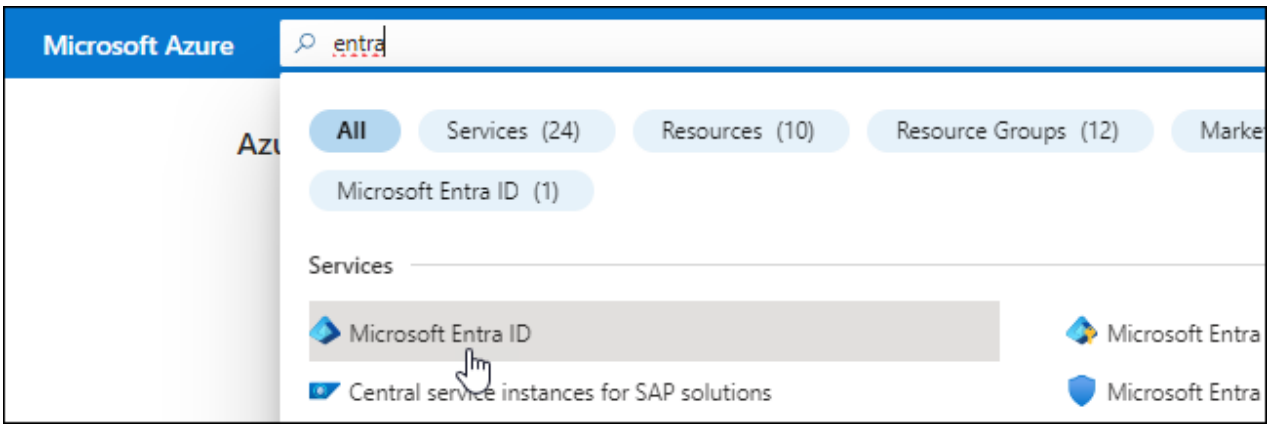
Créez et configurez un principal de service dans Microsoft Entra ID et obtenez les informations d'identification Azure dont la console a besoin. Vous devez fournir ces informations d'identification à la console après avoir installé l'agent de la console.

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

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

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

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



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

5. Précisez les détails de l'application :
   - **Nom**: Saisissez un nom pour l'application.
   - **Type de compte** : sélectionnez un type de compte (n'importe lequel fonctionnera avec la NetApp Console).
   - **URI de redirection**: Vous pouvez laisser ce champ vide.
6. Sélectionnez **S'inscrire**.

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

Affecter l'application à un rôle

1. Créer un rôle personnalisé :

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

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

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

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

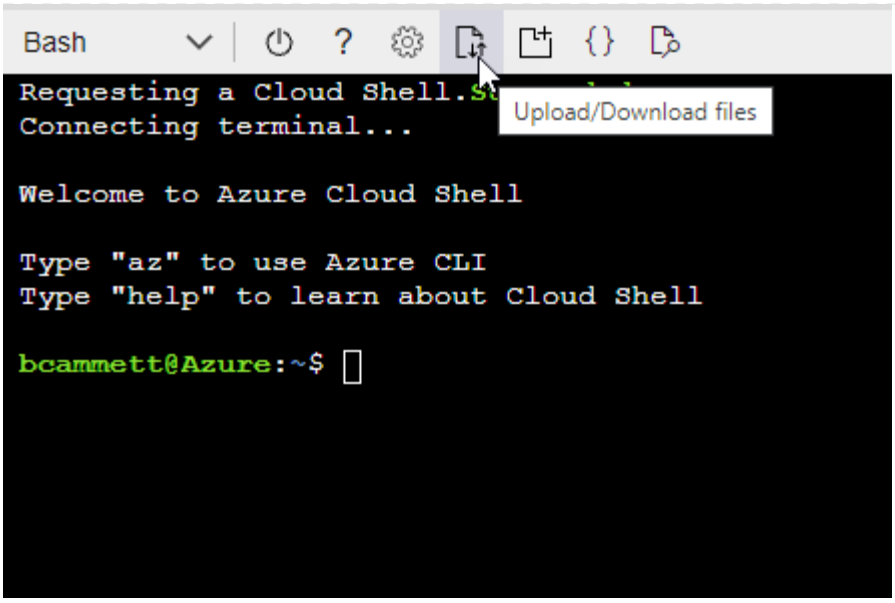
      Exemple

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

   c. Utilisez le fichier JSON pour créer un rôle personnalisé dans Azure.

      Les étapes suivantes décrivent comment créer le rôle à l'aide de Bash dans Azure Cloud Shell.

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



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

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

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

2. Affecter l'application au rôle :

   a. Depuis le portail Azure, ouvrez le service **Abonnements**.

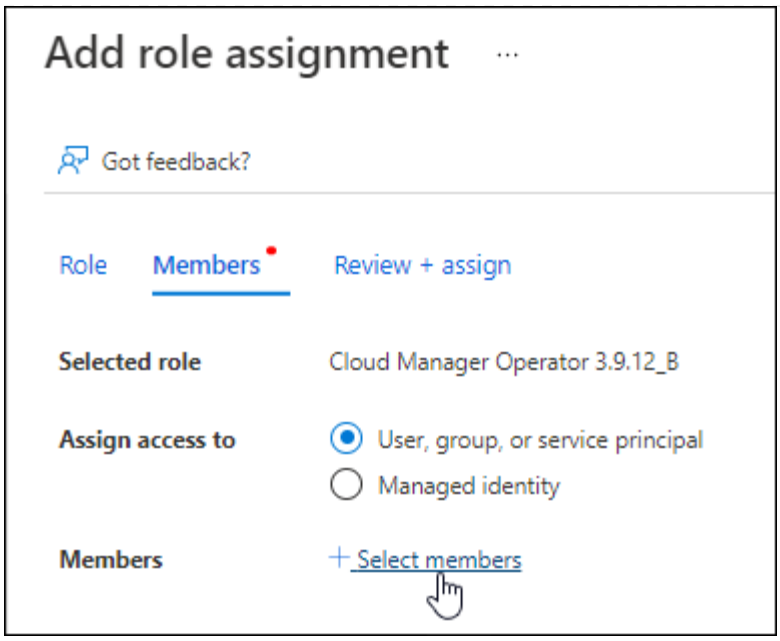
   b. Sélectionnez l'abonnement.

   c. Sélectionnez **Contrôle d'accès (IAM) > Ajouter > Ajouter une attribution de rôle**.

   d. Dans l'onglet **Rôle**, sélectionnez le rôle **Opérateur de console** et sélectionnez **Suivant**.

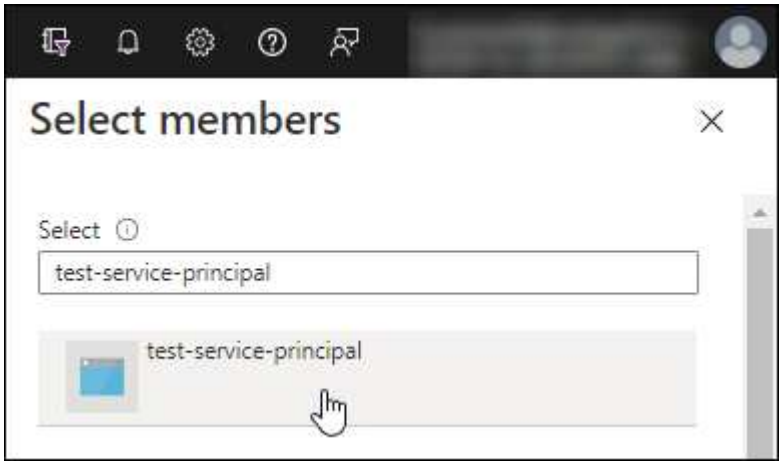
   e. Dans l'onglet **Membres**, procédez comme suit :

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



- Recherchez le nom de l'application.

  Voici un exemple :



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

f. Sélectionnez **Réviser + attribuer**.

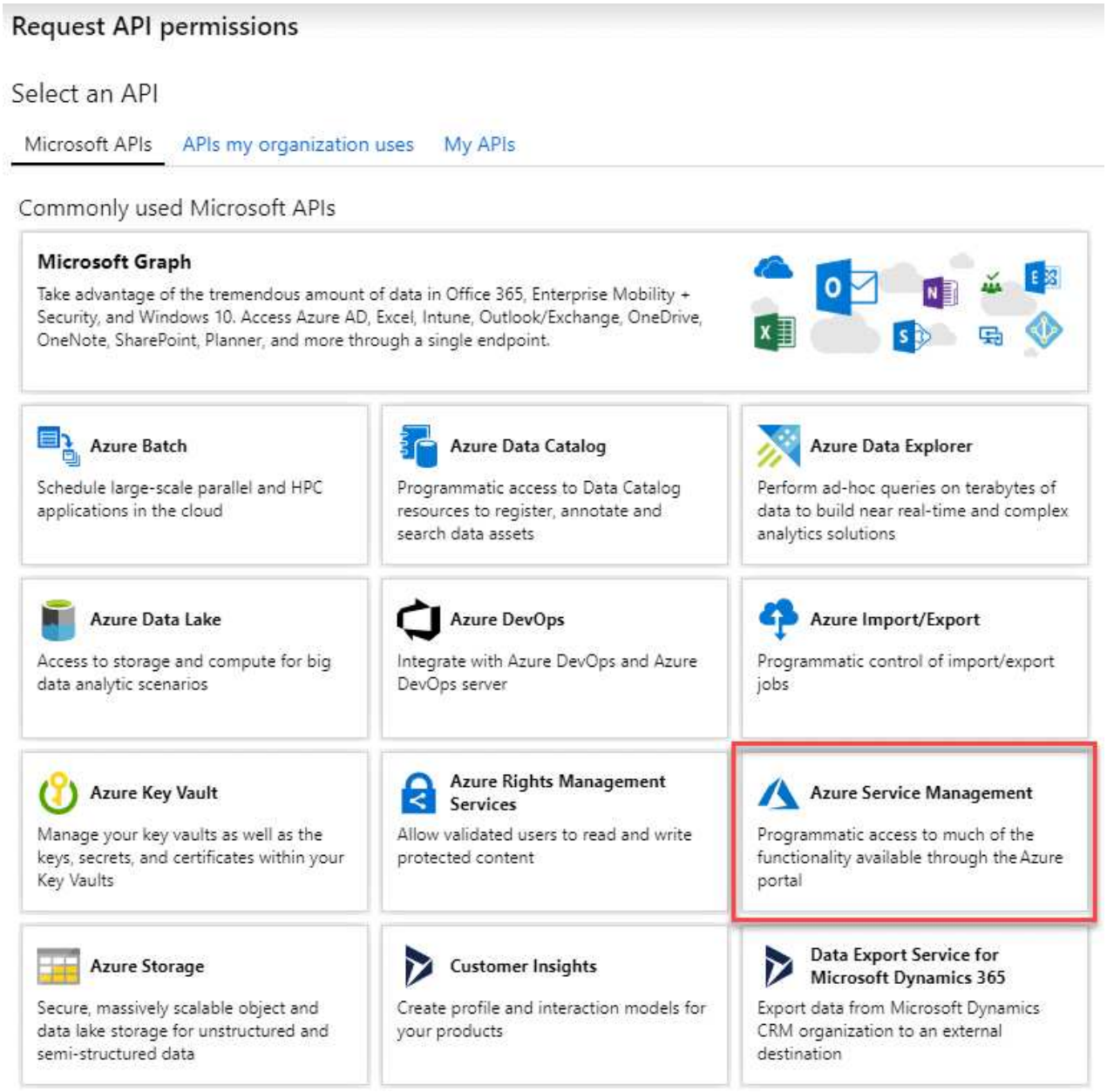
Le principal du service dispose désormais des autorisations Azure requises pour déployer l'agent de la console.

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

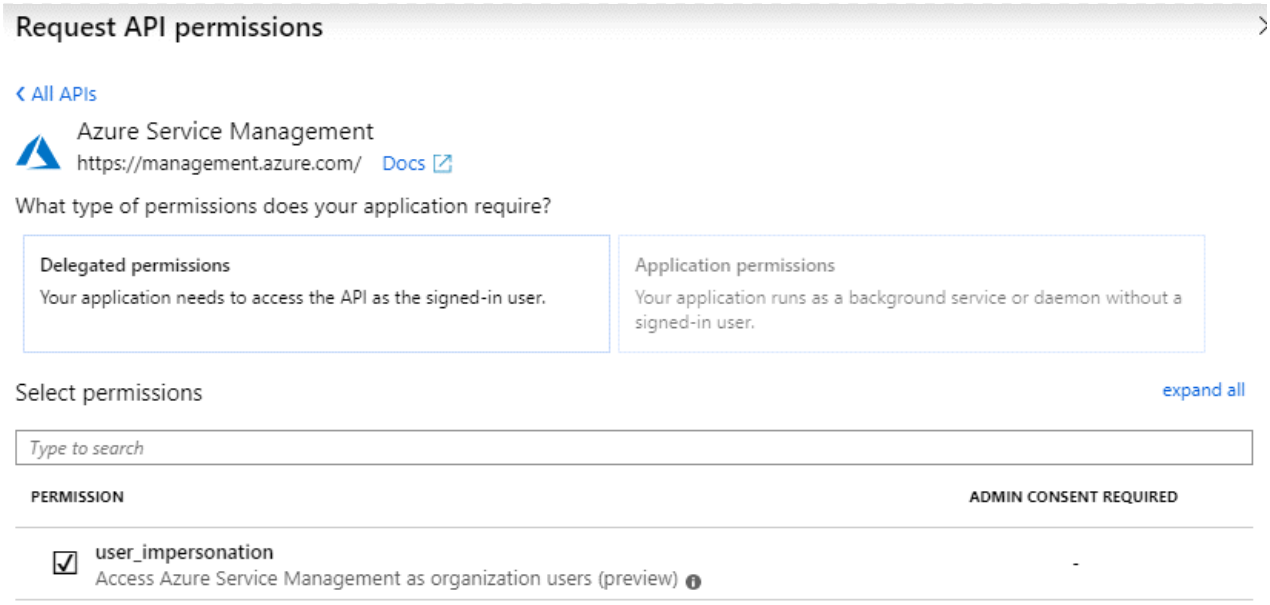
Ajouter des autorisations à l'API Windows Azure Service Management

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

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

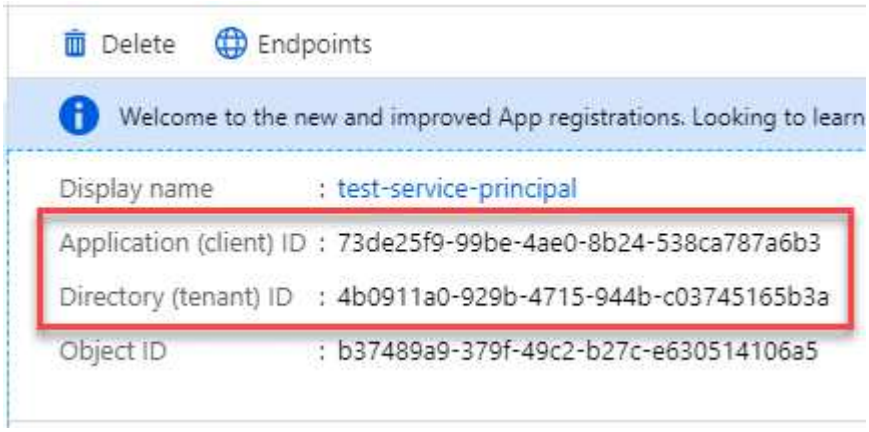


4. Sélectionnez **Accéder à Azure Service Management en tant qu'utilisateurs de l'organisation**, puis sélectionnez **Ajouter des autorisations**.



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

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



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

Créer un secret client

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

Résultat

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

Compte de service Google Cloud

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

Étapes

1. Créer un rôle personnalisé dans Google Cloud :

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

   b. Depuis Google Cloud, activez Cloud Shell.

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

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

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

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

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

2. Créer un compte de service dans Google Cloud :

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

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

   c. Sélectionnez le rôle que vous venez de créer.

   d. Terminez les étapes restantes pour créer le rôle.

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

Étape 7 : Activer les API Google Cloud

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

Étape

1. "Activez les API Google Cloud suivantes dans votre projet"
    - API Cloud Infrastructure Manager
    - 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 NetApp Console avec une connectivité sortante limitée. Pour commencer, installez l'agent de console, configurez la console en accédant à l'interface utilisateur qui s'exécute sur l'agent de console, puis fournissez les autorisations cloud que vous avez précédemment configurées.

Étape 1 : Installer l'agent de console

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

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

Place de marché commerciale AWS

Avant de commencer

Veuillez vous munir des éléments suivants :

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

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

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

  "Découvrez comment configurer les autorisations AWS"

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

  "Examen des exigences des agents".

- Une paire de clés pour l'instance EC2.

Étapes

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

   Le processus d'abonnement peut prendre quelques minutes.

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

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

7. Suivez les instructions pour configurer et déployer l'instance :
   - **Nom et balises** : saisissez un nom et des balises pour l'instance.
   - **Images d'application et de système d'exploitation** : ignorez cette section. L'AMI de l'agent de console est déjà sélectionné.
   - **Type d'instance** : Selon la disponibilité de la région, choisissez un type d'instance qui répond aux exigences de RAM et de CPU (t3.2xlarge est présélectionné et recommandé).
   - **Paire de clés (connexion)** : sélectionnez la paire de clés que vous souhaitez utiliser pour vous connecter en toute sécurité à l'instance.
   - **Paramètres réseau** : Modifiez les paramètres réseau selon vos besoins :
     - Choisissez le VPC et le sous-réseau souhaités.
     - Spécifiez si l'instance doit avoir une adresse IP publique.

        - Spécifiez les paramètres du groupe de sécurité qui activent les méthodes de connexion requises pour l'instance de l'agent de console : SSH, HTTP et HTTPS.

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

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

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

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

Résultat

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

Quelle est la prochaine étape ?

Configurer la NetApp Console.

AWS Gov Marketplace

Avant de commencer

Veuillez vous munir des éléments suivants :

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

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

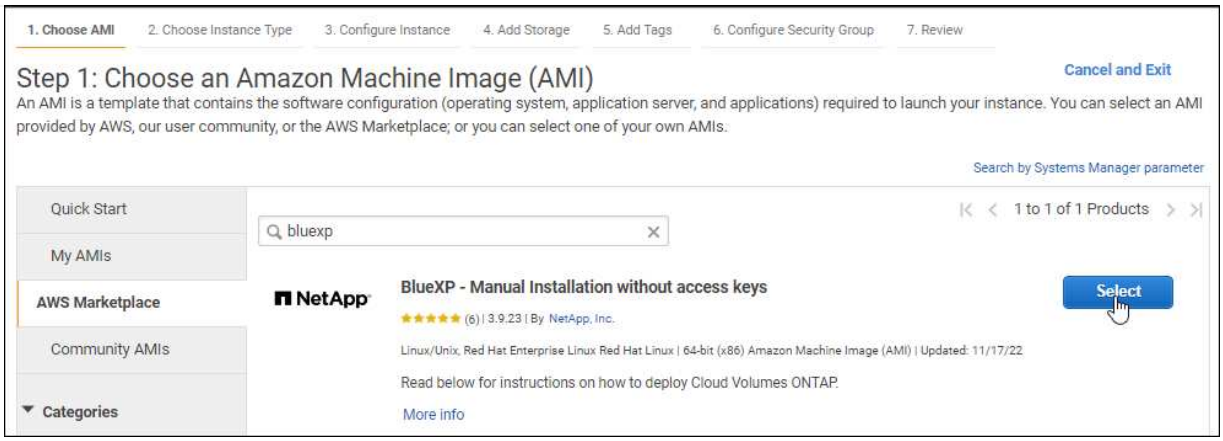
- Un rôle IAM avec une politique attachée qui inclut les autorisations requises pour l'agent de la console.

  "Découvrez comment configurer les autorisations AWS"

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

Étapes

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



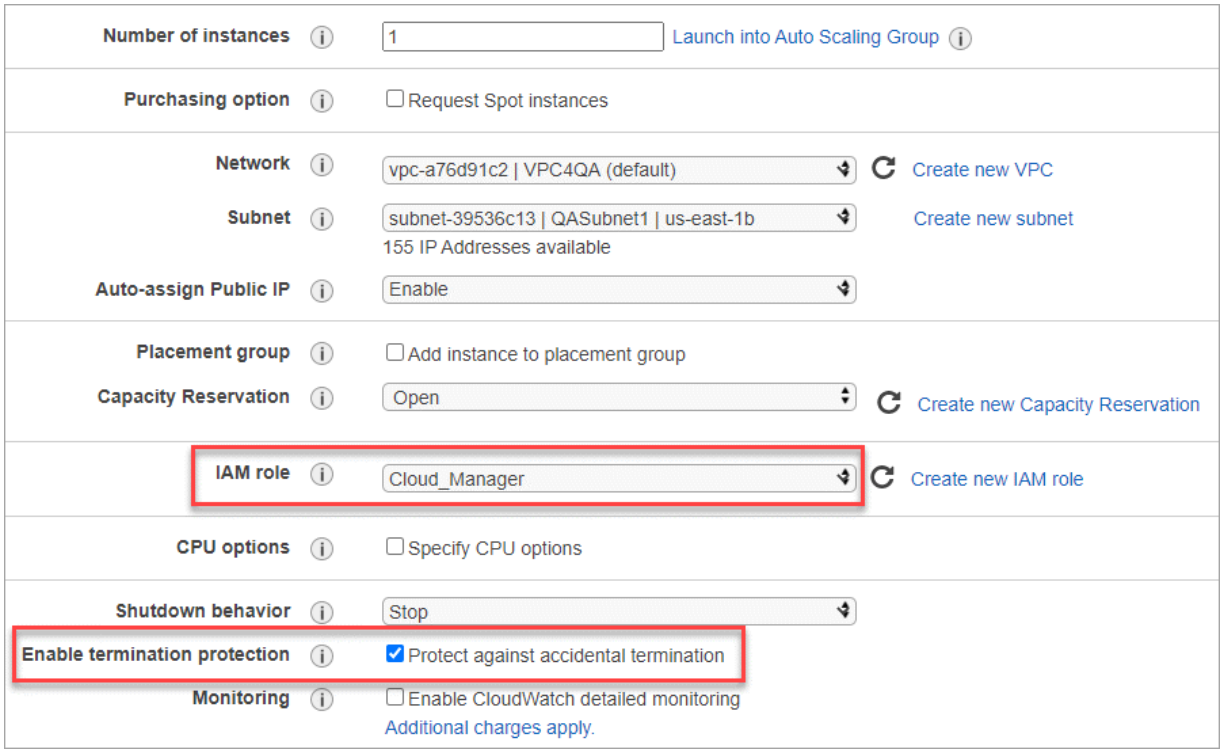
d. Sélectionnez **Continuer**.

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

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

  "Examiner les exigences de l'instance" .

- **Configurer les détails de l'instance** : sélectionnez un VPC et un sous-réseau, choisissez le rôle IAM que vous avez créé à l'étape 1, activez la protection de terminaison (recommandé) et choisissez toute autre option de configuration qui répond à vos besoins.



- **Ajouter du stockage** : Conservez les options de stockage par défaut.
- **Ajouter des balises** : saisissez des balises pour l'instance, si vous le souhaitez.
- **Configurer le groupe de sécurité** : spécifiez les méthodes de connexion requises pour l'instance de l'agent de console : SSH, HTTP et HTTPS.
- **Révision** : Vérifiez vos sélections et sélectionnez **Lancer**.

Résultat

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

Quelle est la prochaine étape ?

Configurer la console.

Place de marché Azure Gov

Avant de commencer

Vous devriez avoir les éléments suivants :

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

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

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

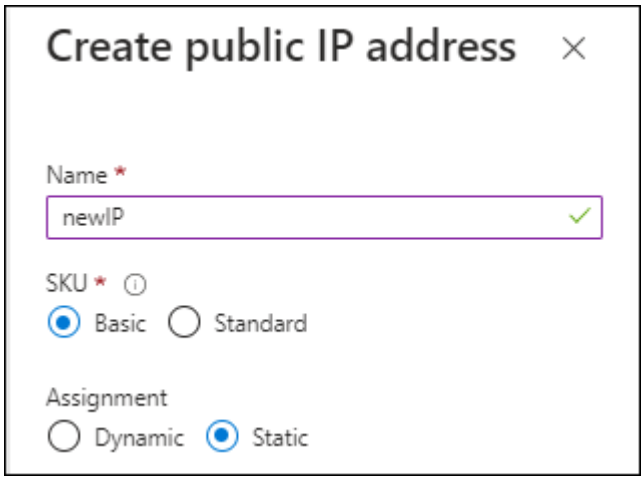
  "Découvrez comment configurer les autorisations Azure"

Étapes

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

   Notez les points suivants lorsque vous configurez la machine virtuelle :

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



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

"Documentation Azure : Référence IP publique"

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

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

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

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

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

Résultat

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

Quelle est la prochaine étape ?

Configurer la NetApp Console.

Installation manuelle (obligatoire pour Google Cloud)

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

Avant de commencer

Vous devriez avoir les éléments suivants :

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

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

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

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

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

console.

À propos de cette tâche

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

Étapes

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

   ```
   unset http_proxy
   unset https_proxy
   ```

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

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

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

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

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

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

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

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

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

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

+

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

+

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

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

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

+ Notez ce qui suit :

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

+ Par exemple :

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

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

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

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

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

      Par exemple:

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

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

Résultat

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

Quelle est la prochaine étape ?

Configurer la NetApp Console.

Étape 2 : Configurer la NetApp Console

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

Avant de commencer

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

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

Étapes

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

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

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

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

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

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

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

a. Sélectionnez **Commençons**.

Résultat

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

Quelle est la prochaine étape ?

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

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

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

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

"Apprenez à préparer les autorisations cloud" .

Rôle AWS IAM

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

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

Étapes

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

Clé d'accès AWS

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

Étapes

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

Rôle Azure

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

Étapes

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

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

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

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

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

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

Principal de service Azure

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

Étapes

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

Résultat

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

Compte de service Google Cloud

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

Étapes

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

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

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

S'abonner aux NetApp Intelligent Services (mode restreint)

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

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

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

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

Avant de commencer

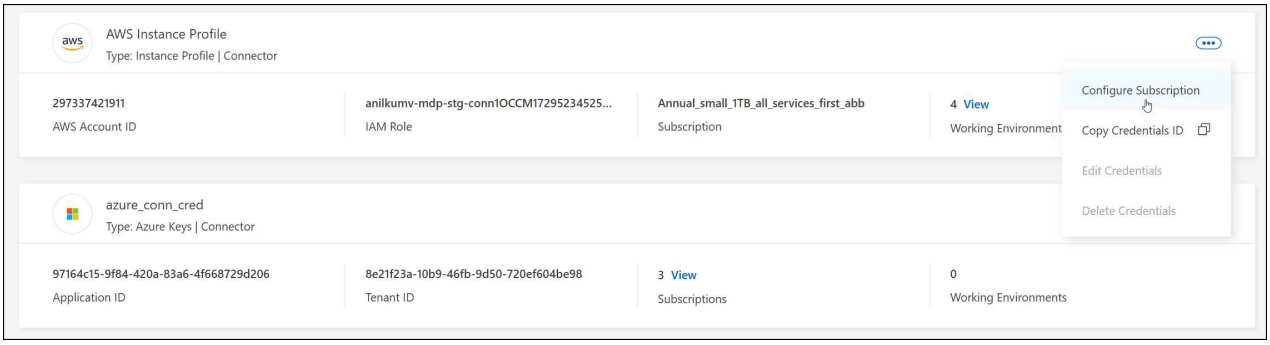
Vous devez déjà avoir déployé un agent de console pour vous abonner aux services de données. Vous devez associer un abonnement au marché aux informations d'identification cloud connectées à un agent de console.

AWS

Étapes

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

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



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

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

   b. Sélectionnez **S'abonner**.

   c. Sélectionnez **Configurer votre compte**.

      Vous serez redirigé vers la NetApp Console.

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

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

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

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

   ◦ Sélectionnez **Enregistrer**.

Azuré

Étapes

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

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

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

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

   b. Sélectionnez **S'abonner**.

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

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

      Vous serez redirigé vers la NetApp Console.

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

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

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

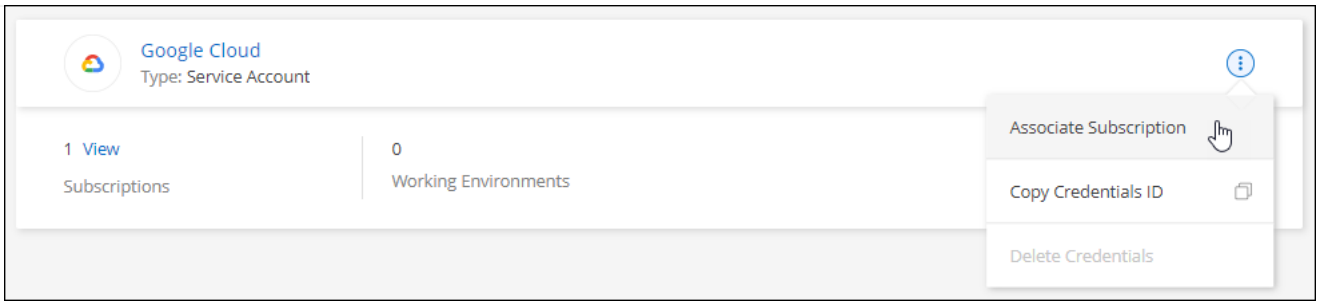
   Pour toutes les autres organisations ou comptes, vous devrez associer manuellement l'abonnement en répétant ces étapes.

   ◦ Sélectionnez **Enregistrer**.

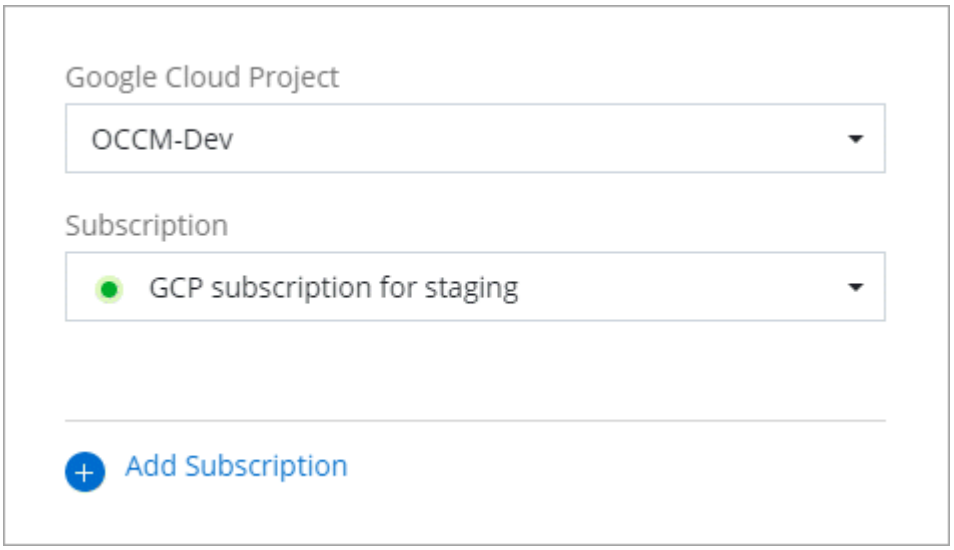
Google Cloud

Étapes

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



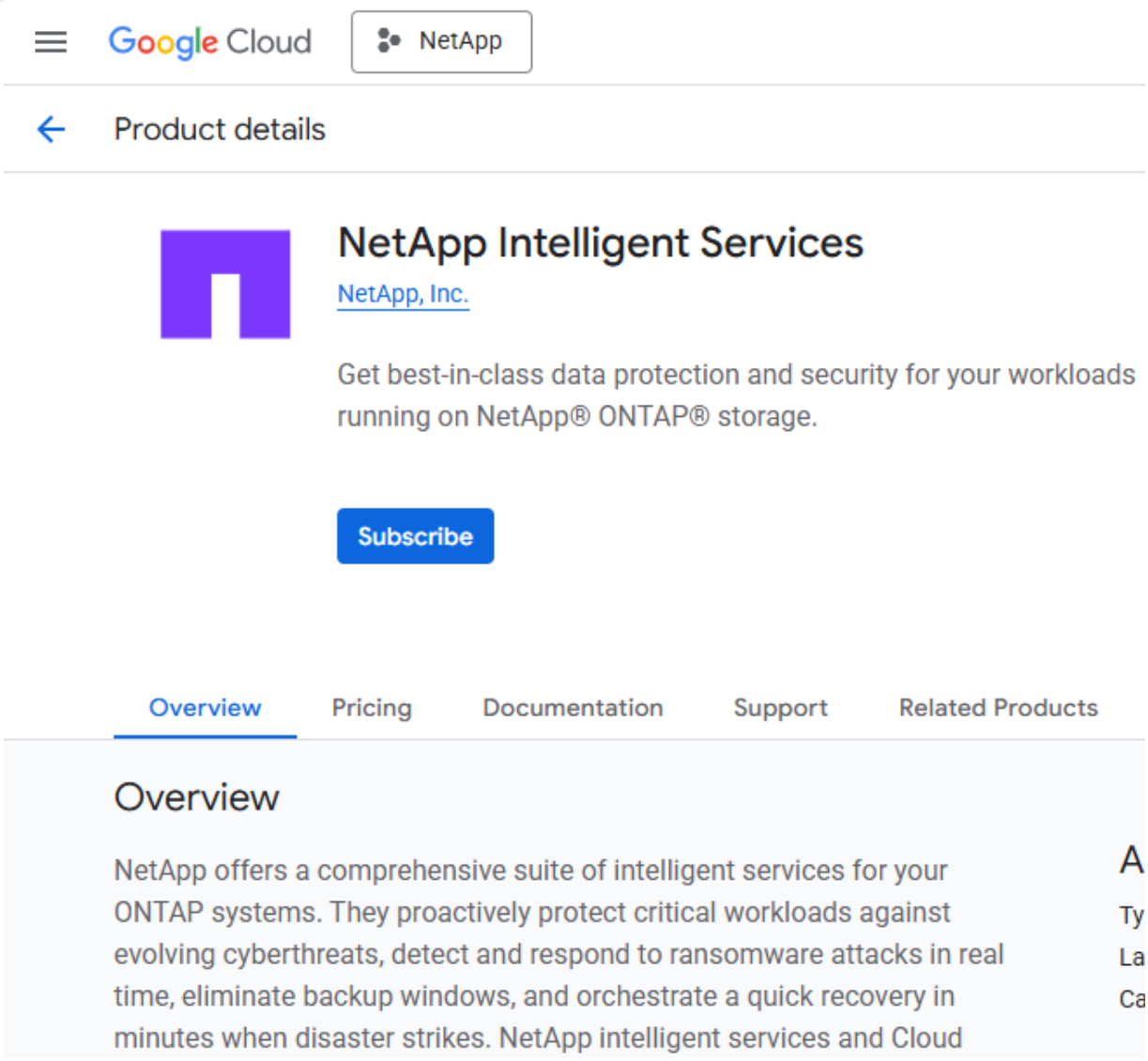
1. Pour configurer un abonnement existant avec les informations d'identification sélectionnées, sélectionnez un projet et un abonnement Google Cloud dans la liste déroulante, puis sélectionnez **Configurer**.



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

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

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

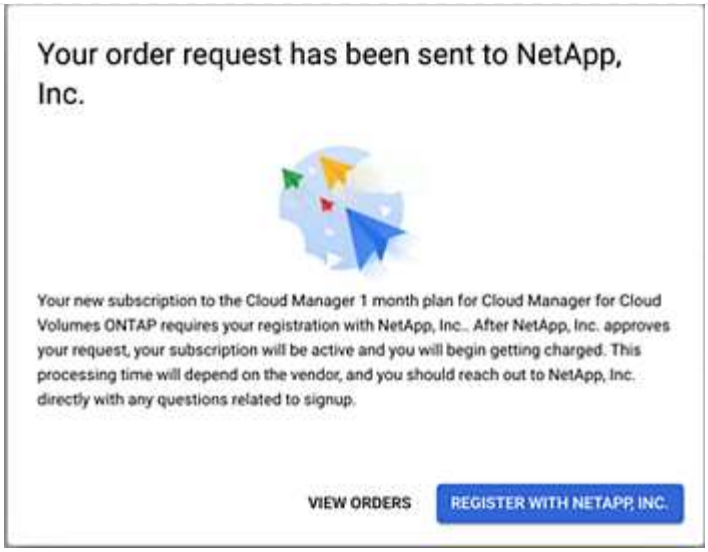


b. Sélectionnez **S'abonner**.
c. Sélectionnez le compte de facturation approprié et acceptez les conditions générales.
d. Sélectionnez **S'abonner**.

   Cette étape envoie votre demande de transfert à NetApp.

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

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



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

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

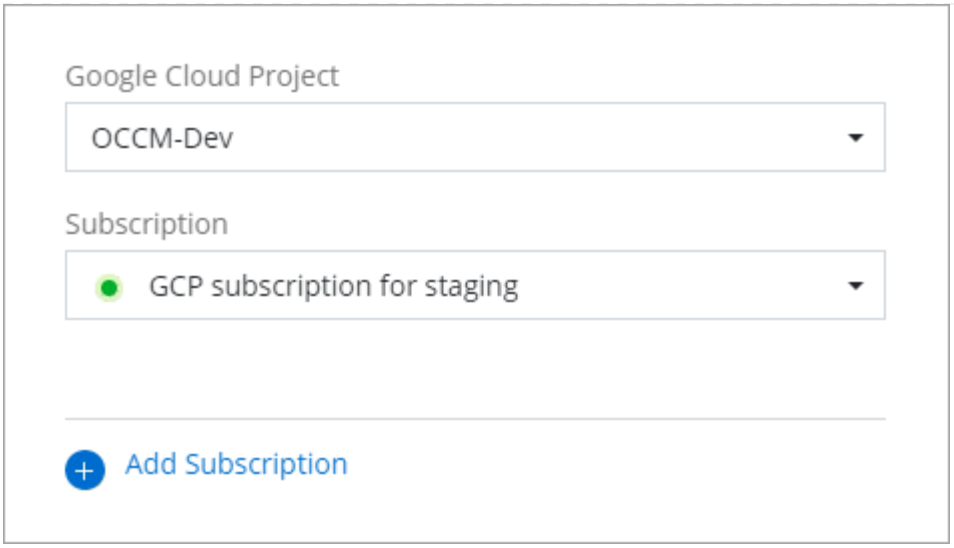
- Sélectionnez l'organisation de la console à laquelle vous souhaitez associer cet abonnement.
- Dans le champ **Remplacer l'abonnement existant**, choisissez si vous souhaitez remplacer automatiquement l'abonnement existant d'une organisation par ce nouvel abonnement.

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

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

◦ Sélectionnez **Enregistrer**.

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



Informations connexes

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

Ce que vous pouvez faire ensuite (mode restreint)

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

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

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

Informations connexes

"Modes de déploiement de la NetApp Console"

Commencez avec le 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/data-services-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
	Résilience aux 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

Informations sur le copyright

Informations sur les marques commerciales