Documentation sur Cloud Manager et Cloud Volumes ONTAP

Cloud Manager 3.8

NetApp
March 25, 2024

Sommaire

Documentation sur Cloud Manager et Cloud Volumes ONTAP

Cloud Manager permet aux experts IT et aux architectes cloud de gérer de manière centralisée leur infrastructure multicloud hybride à l'aide des solutions cloud NetApp.

BlueXP

NetApp BlueXP étend et améliore les fonctionnalités fournies via Cloud Manager.

"Consultez la documentation BlueXP"

Découvrez les nouveautés

- "Modifications importantes apportées à Cloud Manager"
- "Nouveautés de Cloud Manager"
- "Nouveautés de Cloud Volumes ONTAP"

Commencez

- "Le gestionnaire Cloud"
- "Paramètres du compte"
- "Cloud Volumes ONTAP pour AWS"
- "Cloud Volumes ONTAP pour Azure"
- "Cloud Volumes ONTAP pour Google Cloud"
- "Azure NetApp Files"
- "Cloud Volumes Service pour AWS"
- "Cloud Volumes Service pour Google Cloud"
- "Conformité cloud"
- "Cache global de fichiers"
- "Sauvegarde dans le cloud"
- "Cloud Insights"

Automatisez avec les API

- "Guide du développeur API"
- "Échantillons d'automatisation"

Connectez-vous avec vos pairs, obtenez de l'aide et trouvez plus d'informations

- "Communauté NetApp : services de données cloud"

- "Prise en charge de NetApp Cloud Volumes ONTAP"
- "Où obtenir de l’aide et trouver plus d’informations"

Notes de mise à jour

Le gestionnaire Cloud

Nouveautés de Cloud Manager 3.8

Cloud Manager propose généralement une nouvelle version tous les mois afin de vous apporter de nouvelles fonctionnalités, améliorations et correctifs.

Vous recherchez une version précédente ?"Nouveautés de la version 3.7"
"Nouveautés de la version 3.6"
"Nouveautés de la version 3.5"

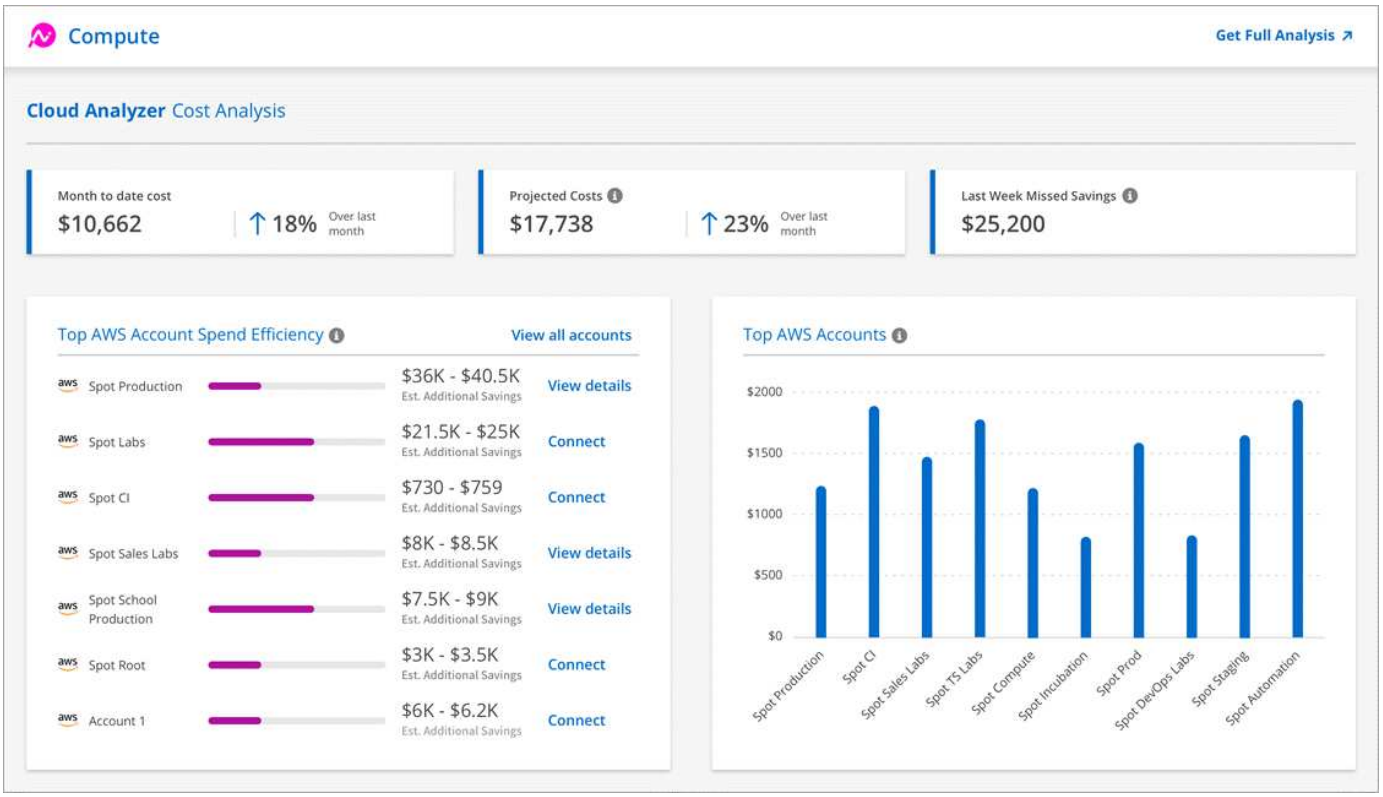
Nouveau fournisseur Terraform (19 octobre 2020)

Nous avons développé un nouveau fournisseur Terraform que les équipes DevOps peuvent utiliser avec Cloud Manager pour automatiser et intégrer Cloud Volumes ONTAP avec l'infrastructure-as-code.

"Découvrez le fournisseur netapp-cloudManager".

Mise à jour de Cloud Manager 3.8.9 (18 octobre 2020)

Valorisation "Spot's Cloud Analyzer", Cloud Manager peut désormais fournir une analyse des coûts généraux de vos dépenses de calcul dans le cloud et identifier les économies potentielles. Ces informations sont disponibles dans le service **Compute** de Cloud Manager. "En savoir plus >>".



Mise à jour de Cloud Manager 3.8.9 (13 octobre 2020)

Nous avons publié deux mises à jour de Cloud Tiering :

- Les licences pour Cloud Tiering sont désormais disponibles depuis Cloud Manager.

  Payez pour le Tiering des données d'un cluster ONTAP sur site vers le cloud, via un abonnement avec paiement à l'utilisation, une licence de hiérarchisation ONTAP appelée *FabricPool*, ou une combinaison des deux.

- Le service autonome Cloud Tiering a été supprimé. Vous devez désormais accéder à Cloud Tiering directement depuis Cloud Manager, où toutes les mêmes fonctionnalités sont disponibles.

Cloud Manager 3.8.9 (4 octobre 2020)

- Améliorations de Cloud Compliance
- Améliorations de Cloud Volumes Service pour AWS
- Intégration avec Cloud Sync
- Améliorations de la gestion de compte
- Changements pour les régions gouvernementales

Améliorations de Cloud Compliance

- Un nouveau rôle **Cloud Compliance Viewer** est disponible dans Cloud Manager.

  Les utilisateurs affectés à ce rôle peuvent uniquement afficher les informations de conformité et générer des rapports pour les espaces de travail auxquels ils sont autorisés à accéder. Elles ne peuvent pas gérer les paramètres de conformité cloud et n'ont pas accès aux autres fonctionnalités et services Cloud Manager. Cela peut jouer un rôle crucial pour votre équipe juridique afin qu'elle puisse surveiller les résultats de l'analyse de la conformité dans le cloud. Voir "rôles utilisateur" pour plus d'informations.

- Ajout de la prise en charge pour la numérisation des schémas de base de données MongoDB et PostgreSQL. Voir "analyse des schémas de base de données" pour en savoir plus.
- Les tarifs de conformité cloud changent depuis le 7 octobre.

  Les 1 premiers To de données analysés par Cloud Compliance dans un espace de travail Cloud Manager sont gratuits. Cela inclut les données des volumes Cloud Volumes ONTAP, des volumes Azure NetApp Files, des compartiments Amazon S3 et des schémas de base de données. Un abonnement est nécessaire pour numériser toutes les données supplémentaires après avoir atteint 1 To. Voir "tarifs" pour plus d'informations.

Améliorations de Cloud Volumes Service pour AWS

Lorsque vous créez un volume, vous pouvez choisir de le baser sur une copie Snapshot existante d'un autre volume.

Intégration avec Cloud Sync

Le service Cloud Sync de NetApp est à présent disponible dans Cloud Manager. Cloud Sync offre un moyen simple, sécurisé et automatisé de migrer vos données de n'importe quelle destination source vers n'importe quelle destination cible, dans le cloud ou sur votre site. "En savoir plus >>".

Améliorations de la gestion de compte

Nous avons ajouté d'autres moyens de gérer votre compte.

- Une présentation des ressources de votre compte est désormais disponible.

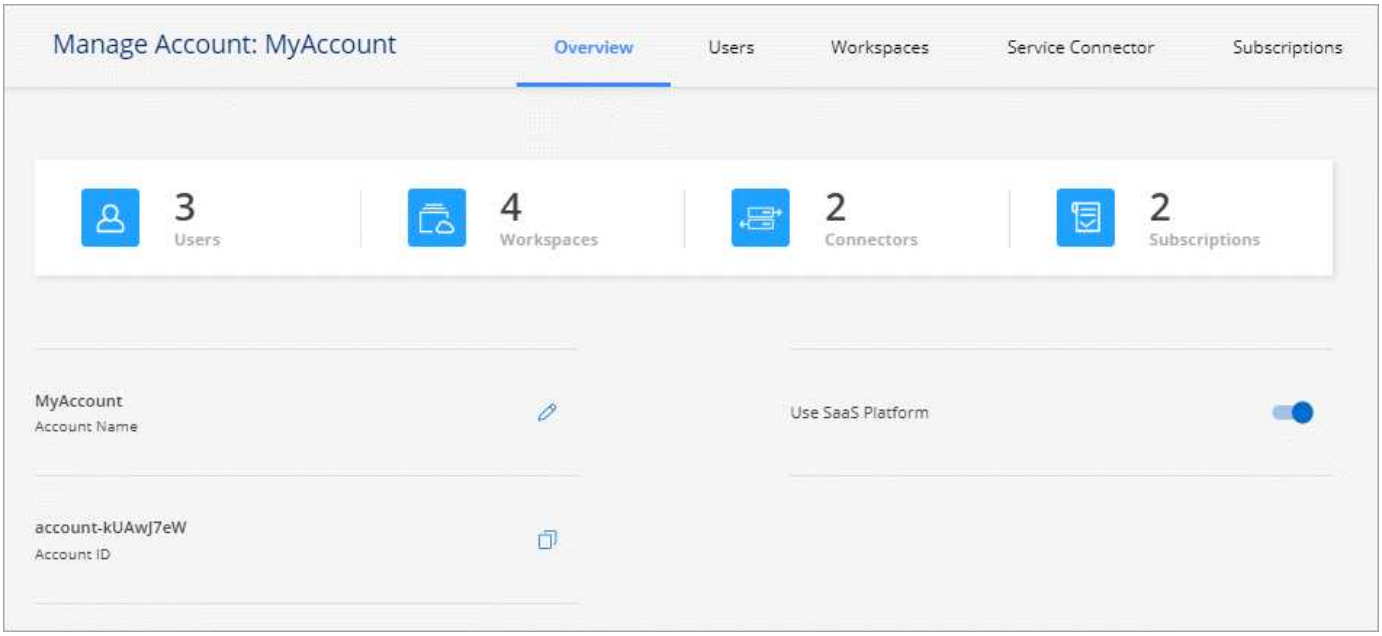
  Vous pouvez afficher rapidement le nombre d'utilisateurs, d'espaces de travail, de connecteurs et d'abonnements dans votre compte.

- Vous pouvez modifier le nom de votre compte.
- Vous pouvez copier votre ID de compte, votre ID d'espace de travail ou votre ID de connecteur.

  La copie de ces identifiants vous aidera à utiliser les fonctions d'automatisation que nous prévoyons.

- Vous pouvez désactiver l'utilisation de la plateforme SaaS.

  Nous ne recommandons pas de désactiver la plate-forme SaaS, sauf si vous devez vous conformer aux politiques de sécurité de votre entreprise. En désactivant la plateforme SaaS, vous vous limitent votre capacité à utiliser les services cloud intégrés de NetApp. "En savoir plus >>".



Changements pour les régions gouvernementales

Si vous déployez un connecteur dans une région AWS GovCloud, une région Azure Government ou une région Azure DoD, l'accès à Cloud Manager est désormais disponible uniquement via l'adresse IP d'hôte d'un connecteur. L'accès à la plateforme SaaS est désactivé pour l'ensemble du compte.

Cela signifie que seuls les utilisateurs privilégiés qui peuvent accéder au VPC/vNet interne de l'utilisateur final peuvent utiliser l'interface ou l'API de Cloud Manager.

"En savoir plus sur cette limitation".

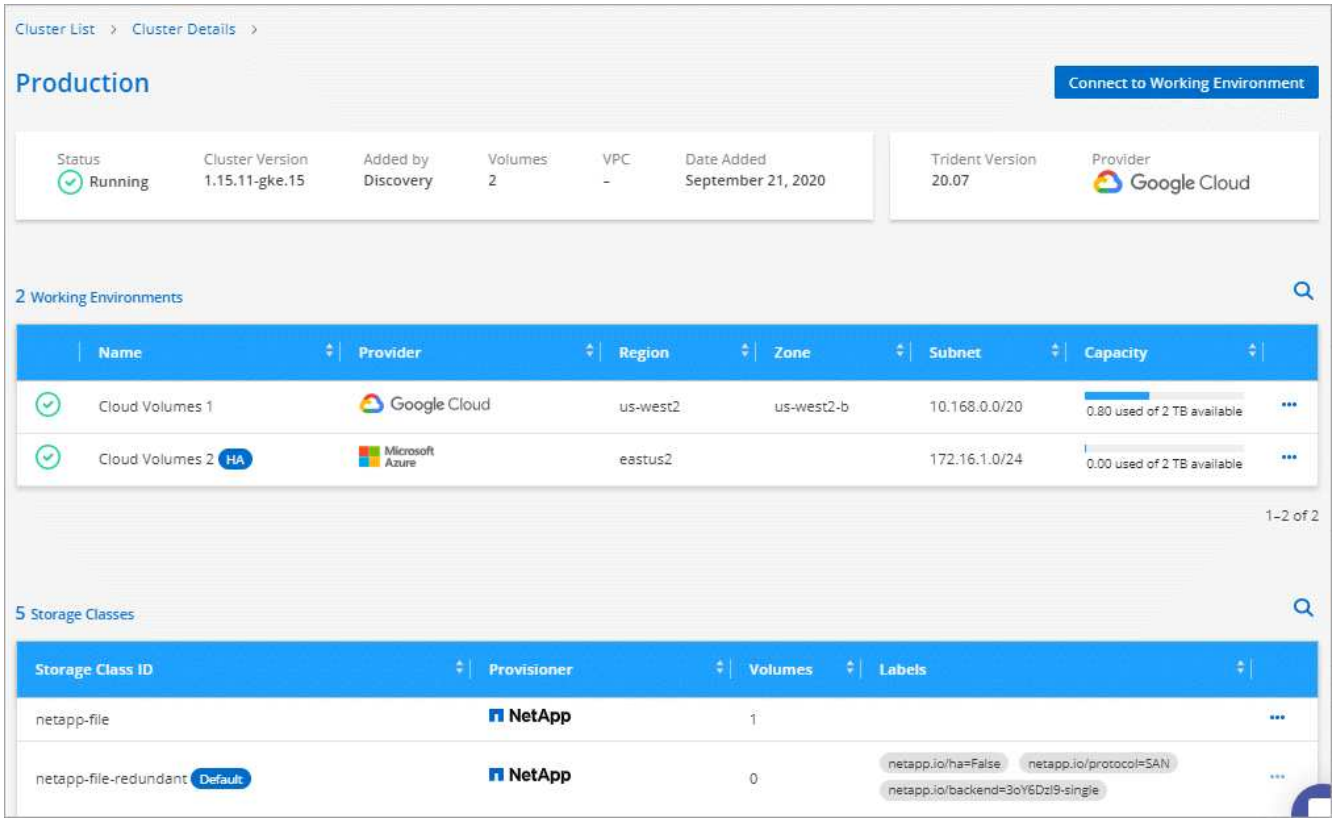
Mise à jour de Cloud Manager 3.8.8 (22 septembre 2020)

Nous avons amélioré le service Kubernetes pour faciliter l'utilisation et fournir des fonctionnalités supplémentaires :

- Nous avons facilité la découverte des clusters Kubernetes exécutés dans le service Kubernetes géré de votre fournisseur cloud.

  Il vous suffit de cliquer sur **découvrir les clusters** et Cloud Manager détecte vos clusters gérés en utilisant les autorisations du fournisseur de cloud que vous avez déjà fournies.

- Vous pouvez désormais afficher plus d'informations sur un cluster Kubernetes découvert, notamment son état, le nombre de volumes, les classes de stockage, etc.



- Nous avons ajouté une vérification des ressources et des erreurs pour vérifier que la communication est disponible entre le cluster et Cloud Volumes ONTAP. Si ce n'est pas le cas, nous vous le ferons savoir.

"Découvrez comment démarrer".

Notez que le compte de service pour un connecteur nécessite les autorisations suivantes pour découvrir et gérer les clusters Kubernetes exécutés dans Google Kubernetes Engine (GKE) :

```
- container.*
```

Mise à jour de Cloud Manager 3.8.8 (10 septembre 2020)

Les améliorations suivantes sont disponibles lors du déploiement de Global File cache via Cloud Manager :

- Une paire haute disponibilité Cloud Volumes ONTAP dans AWS est désormais prise en charge en tant que plateforme de stockage back-end pour votre système de stockage central.
- Plusieurs instances centrales de cache de fichiers globaux peuvent être déployées dans une conception Load Distributed.

"En savoir plus sur Global File cache".

Cloud Manager 3.8.8 (9 septembre 2020)

- Prise en charge de Cloud Volumes Service pour Google Cloud
- La sauvegarde dans le cloud prend désormais en charge les clusters ONTAP sur site
- Améliorations de la sauvegarde dans le cloud
- Améliorations de Cloud Compliance
- Navigation mise à jour
- Améliorations de l'administration

Prise en charge de Cloud Volumes Service pour Google Cloud

- Ajoutez un environnement de travail pour gérer les Cloud Volumes Service existants pour les volumes GCP et créer de nouveaux volumes. "Découvrez comment".
- Créez et gérez des volumes NFS v3 et NFS v4.1 pour les clients Linux et UNIX, et les volumes SMB 3.x pour les clients Windows.
- Créez, supprimez et restaurez des snapshots de volume.

La sauvegarde dans le cloud prend désormais en charge les clusters ONTAP sur site

Commencez à sauvegarder les données stockées dans vos systèmes ONTAP sur site vers le cloud. Intégrez une sauvegarde dans le cloud à vos environnements de travail sur site pour sauvegarder des volumes dans le stockage Azure Blob. "En savoir plus >>".

Améliorations de la sauvegarde dans le cloud

Nous avons révisé l'interface utilisateur pour une meilleure utilisation :

- Page de liste des volumes pour voir facilement les volumes sauvegardés avec les sauvegardes disponibles
- Page des paramètres de sauvegarde pour afficher les paramètres de sauvegarde de chaque environnement de travail

Améliorations de Cloud Compliance

- Capacité à analyser les données à partir des bases de données

  Scannez vos bases de données pour identifier les données personnelles et sensibles qui résident dans chaque schéma. Les bases de données prises en charge incluent Oracle, SAP HANA et SQL Server (MSSQL). "En savoir plus sur la numérisation de bases de données".

- Capacité à analyser des volumes de protection des données (DP)

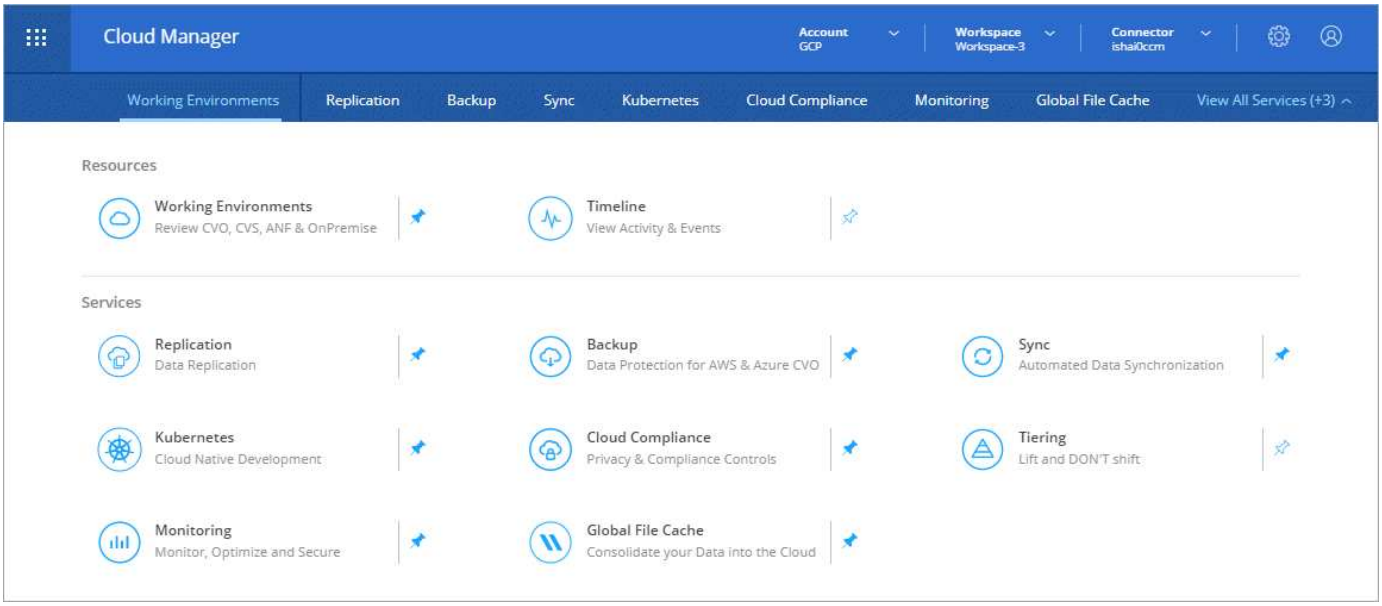
  Les volumes DP sont des volumes de destination à partir des opérations SnapMirror en général depuis des clusters ONTAP sur site. Vous pouvez désormais identifier facilement les données personnelles et sensibles qui résident dans les fichiers sur site. "Découvrez comment".

Navigation mise à jour

Nous avons actualisé l'en-tête dans Cloud Manager pour faciliter la navigation entre les services clouds

NetApp.

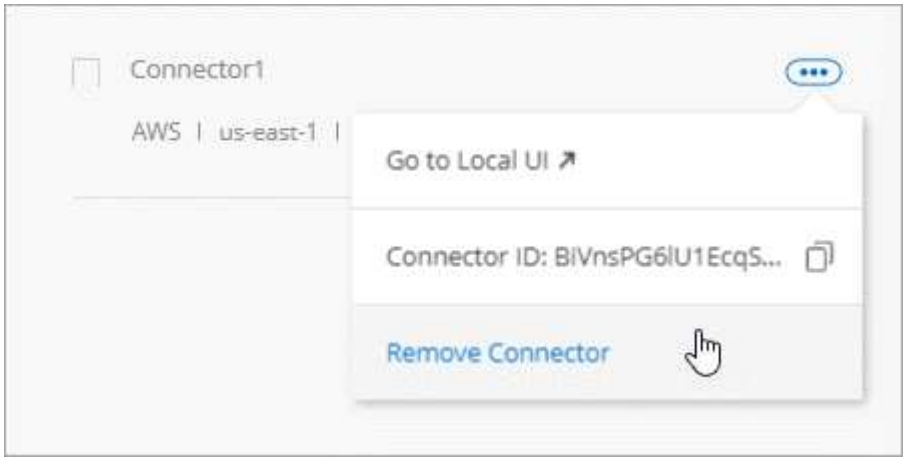
Cliquez sur **Afficher tous les services** et vous pouvez épingler et désépingler les services que vous souhaitez voir dans la navigation.



Comme vous pouvez le voir, nous avons également actualisé les menus déroulants compte, espace de travail et connecteur, ce qui facilite l'affichage de vos sélections actuelles.

Améliorations de l'administration

- Vous pouvez maintenant supprimer les connecteurs inactifs de Cloud Manager. "Découvrez comment".



- Vous pouvez désormais remplacer l'abonnement Marketplace actuellement associé aux identifiants de votre fournisseur cloud. Si vous avez besoin de modifier votre facturation, cette modification peut vous aider à vous assurer que vous êtes facturé via l'abonnement Marketplace approprié.

  Découvrez comment "Dans AWS", "Dans Azure", et "Dans GCP".

Mise à jour sur les autorisations Azure requises (6 août 2020)

Pour éviter les échecs de déploiement d'Azure, vérifiez que votre stratégie Cloud Manager dans Azure inclut l'autorisation suivante :

```
"Microsoft.Resources/deployments/operationStatuses/read"
```

Azure requiert désormais cette autorisation pour certains déploiements de machines virtuelles (elle dépend du matériel physique sous-jacent utilisé lors du déploiement).

"Consultez la dernière politique Cloud Manager pour Azure".

Cloud Manager 3.8.7 (3 août 2020)

- Nouvelle expérience en tant que service
- Améliorations de Cloud Volumes ONTAP
- Améliorations de Azure NetApp Files
- Améliorations de Cloud Volumes Service pour AWS
- Améliorations de Cloud Compliance
- Améliorations de la sauvegarde dans le cloud
- Prise en charge de Global File cache

Nouvelle expérience en tant que service

Nous avons totalement introduit une expérience SaaS pour Cloud Manager. Cette nouvelle expérience facilite l'utilisation de Cloud Manager et nous permet de proposer des fonctionnalités supplémentaires pour gérer votre infrastructure de cloud hybride.

Cloud Manager inclut un "Interface SaaS" Cet outil est intégré à NetApp Cloud Central et aux connecteurs qui permettent à Cloud Manager de gérer les ressources et les processus au sein de votre environnement de cloud public. (Le connecteur est en fait le même que le logiciel Cloud Manager que vous avez installé.)

> Un connecteur est nécessaire dans la plupart des cas, mais il n'est pas nécessaire d'utiliser Azure NetApp Files, Cloud Volumes Service ou Cloud Sync depuis Cloud Manager.

Comme nous l'avons déjà mentionné dans ces notes de version, vous devrez mettre à niveau le type de machine de vos connecteurs pour accéder aux nouvelles fonctionnalités que nous proposons. Cloud Manager vous invite à modifier le type de machine. "En savoir plus >>".

Améliorations de Cloud Volumes ONTAP

Deux améliorations sont disponibles pour Cloud Volumes ONTAP.

- **Plusieurs licences BYOL pour allouer de la capacité supplémentaire**

  Vous pouvez désormais acheter plusieurs licences pour un système Cloud Volumes ONTAP BYOL afin d'allouer plus de 368 To de capacité. Par exemple, vous pouvez acheter deux licences pour allouer une capacité allant jusqu'à 736 To à Cloud Volumes ONTAP. Vous pouvez également acheter quatre licences pour obtenir jusqu'à 1.4 po.

  Le nombre de licences que vous pouvez acheter pour un système à un seul nœud ou une paire HA est illimité.

  Notez que les limites de disques peuvent vous empêcher d'atteindre la limite de capacité en utilisant des disques seuls. Vous pouvez aller au-delà de la limite des disques de "tiering des données inactives vers le

stockage objet". Pour plus d'informations sur les limites de disques, reportez-vous à la section "Limites de stockage dans les notes de mise à jour de Cloud Volumes ONTAP".

"Apprenez à ajouter une nouvelle licence système".

- **Crypter les disques gérés Azure à l'aide de clés externes**

  Vous pouvez désormais chiffrer les disques gérés Azure sur des systèmes Cloud Volumes ONTAP à un seul nœud à l'aide de clés externes provenant d'un autre compte. Cette fonctionnalité est prise en charge à l'aide d'API.

  Lors de la création du système à un nœud, il vous suffit d'ajouter ce qui suit à la demande d'API :

```
"azureEncryptionParameters": {
      "key": <azure id of encryptionset>
  }
```

  Cette fonctionnalité requiert de nouvelles autorisations, comme indiqué dans la dernière "Cloud Manager policy pour Azure".

```
"Microsoft.Compute/diskEncryptionSets/read"
```

Améliorations de Azure NetApp Files

Cette version inclut un certain nombre d'améliorations en matière de prise en charge d'Azure NetApp Files.

- **Configuration Azure NetApp Files**

  Vous pouvez désormais configurer et gérer Azure NetApp Files directement à partir de Cloud Manager. "Découvrez comment".

- **Prise en charge du nouveau protocole**

  Il est désormais possible de créer des volumes NFSv4.1 et SMB.

- **Gestion des instantanés de pool de capacité et de volume**

  Cloud Manager vous permet de créer, de supprimer et de restaurer des snapshots de volumes. Vous avez également la possibilité de créer de nouveaux pools de capacité et de spécifier leurs niveaux de service.

- **Possibilité de modifier des volumes**

  Vous pouvez modifier un volume en modifiant sa taille et en gérant les balises.

Améliorations de Cloud Volumes Service pour AWS

La prise en charge d'Cloud Volumes Service pour AWS intègre de nombreuses améliorations dans Cloud Manager.

- **Prise en charge du nouveau protocole**

Il est désormais possible de créer des volumes NFSv4.1, des volumes SMB et des volumes à double protocole. Auparavant, vous pouviez uniquement créer et détecter les volumes NFSv3 dans Cloud Manager.

- **Prise en charge de l'instantané**

  Vous pouvez créer des règles Snapshot pour automatiser la création de snapshots de volumes, créer un snapshot à la demande, restaurer un volume à partir d'un snapshot, créer un volume basé sur un snapshot existant, et bien plus encore. Voir "Gestion des copies Snapshot de Cloud volumes" pour en savoir plus.

- **Créez le volume initial dans une région à partir de Cloud Manager**

  Avant cette version, le premier volume de chaque région a dû être créé dans l'interface Cloud Volumes Service pour AWS. Vous pouvez maintenant vous abonner à "L'un des services NetApp Cloud Volumes Service sur AWS Marketplace" Puis créez le premier volume depuis Cloud Manager.

Améliorations de Cloud Compliance

Cloud Compliance est désormais disponible avec les améliorations suivantes.

- **Processus de déploiement révisé pour votre instance Cloud Compliance**

  L'instance Cloud Compliance est configurée et déployée à l'aide d'un nouvel assistant dans Cloud Manager. Une fois le déploiement terminé, activez le service pour chaque environnement de travail que vous souhaitez analyser.

- **Possibilité de sélectionner les volumes à analyser dans un environnement de travail**

  Vous pouvez désormais activer et désactiver la numérisation de volumes individuels dans un environnement de travail Cloud Volumes ONTAP ou Azure NetApp Files. Si vous n'avez pas besoin de scanner certains volumes pour des raisons de conformité, désactivez-les.

  "En savoir plus sur la désactivation de l'analyse des volumes."

- **Onglets de navigation pour atteindre rapidement votre zone d'intérêt**

  Les nouveaux onglets Tableau de bord, Investigation et Configuration vous permettent d'accéder plus facilement à ces sections.

- **Rapport HIPAA**

  Un nouveau rapport sur la loi HIPAA (Health Insurance Portability and Accountability Act) est désormais disponible. Ce rapport est conçu pour aider votre organisation à respecter les lois HIPAA sur la protection des données personnelles.

  "En savoir plus sur le rapport HIPAA."

- **Nouveau type de données personnelles sensibles**

  Cloud Compliance peut désormais trouver des codes médicaux CIM-9-cm dans des fichiers.

- **Nouveau type de données personnelles**

  Cloud Compliance peut désormais trouver deux nouveaux identifiants nationaux dans les fichiers : l'ID croate (OIB) et l'ID grec.

Améliorations de la sauvegarde dans le cloud

Les améliorations suivantes sont désormais disponibles pour Backup vers le cloud :

- **Apportez votre propre licence (BYOL) est maintenant disponible**

  La sauvegarde dans le cloud n'est disponible qu'avec une licence PAYGO (Pay As You Go). Une licence BYOL permet d'acheter une licence auprès de NetApp pour utiliser Backup to Cloud pendant une certaine période et pour un espace de sauvegarde maximal. Lorsque l'une ou l'autre limite est atteinte, vous devez renouveler la licence.

  "En savoir plus sur la nouvelle licence Backup to Cloud BYOL."

- **Prise en charge des volumes de protection des données (DP)**

  Les volumes de protection des données peuvent être sauvegardés et restaurés dès maintenant.

Prise en charge de Global File cache

NetApp Global File cache vous permet de consolider les silos de serveurs de fichiers distribués en un seul environnement de stockage global cohérent dans le cloud public. Un système de fichiers accessible partout dans le cloud est ainsi créé, que tous les emplacements distribués peuvent utiliser comme s'ils étaient locaux.

À partir de cette version, l'instance Global File cache Management et l'instance Core peuvent être déployées et gérées via Cloud Manager. Le processus de déploiement initial permet de gagner plusieurs heures et de bénéficier d'une fenêtre unique via Cloud Manager pour tous les systèmes déployés. Les instances globales de cache de fichiers Edge sont toujours déployées localement dans les bureaux distants.

Voir "Présentation du cache de fichiers global" pour en savoir plus.

La configuration initiale pouvant être déployée à l'aide de Cloud Manager doit répondre aux exigences suivantes. D'autres configurations, comme Cloud Volumes Service, Azure NetApp Files, Cloud Volumes Service pour AWS et GCP, continuent d'être déployées en suivant les procédures existantes. "En savoir plus >>".

- La plateforme de stockage interne utilisée comme stockage central doit être un environnement de travail dans lequel vous avez déployé une paire Cloud Volumes ONTAP HA dans Azure.

  Les autres plateformes de stockage et autres fournisseurs cloud ne sont pas pris en charge à l'heure actuelle via Cloud Manager, mais peuvent être déployés via des procédures de déploiement héritées.

- Le réseau Fibre Channel Core peut être déployé uniquement en tant qu'instance autonome.

  Si vous devez utiliser une conception Load Distributed qui inclut plusieurs instances Core, vous devez utiliser les procédures héritées.

Cette fonctionnalité requiert de nouvelles autorisations, comme indiqué dans la dernière "Cloud Manager policy pour Azure".

```
"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
```

L'expérience améliorée exige un type de machine plus robuste (15 juillet 2020)

Pour améliorer l'expérience de Cloud Manager, vous devez mettre à niveau votre type de machine afin d'accéder aux nouvelles fonctionnalités que nous vous proposons. Les améliorations comprendront un "Expérience en tant que service dans Cloud Manager" enfin, des intégrations améliorées et nouvelles des services cloud.

Cloud Manager vous invite à modifier le type de machine.

Voici quelques détails :

1. Afin de garantir que les ressources appropriées sont disponibles pour fonctionner correctement les nouvelles fonctionnalités de Cloud Manager, nous avons modifié l'instance par défaut, la machine virtuelle et le type de machine comme suit :
   - AWS : instance de t3.XLarge
   - Azure: DS3 v2
   - GCP : N1-standard-4

   Ces tailles par défaut sont le minimum pris en charge "En fonction des besoins en processeur et en RAM".
2. Dans le cadre de cette transition, Cloud Manager nécessite l'accès au terminal suivant pour obtenir des images logicielles des composants de conteneur pour une infrastructure Docker :

   https://cloudmanagerinfraprod.azurecr.io

   Assurez-vous que votre pare-feu autorise l'accès à ce terminal à partir de Cloud Manager.

Cloud Manager 3.8.6 (6 juillet 2020)

- Prise en charge des volumes iSCSI
- Prise en charge de l'ensemble des règles de Tiering

Prise en charge des volumes iSCSI

Cloud Manager vous permet désormais de créer des volumes iSCSI pour les clusters Cloud Volumes ONTAP et ONTAP sur site directement à partir de l'interface utilisateur.

Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons

simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".

> Vous pouvez créer des LUN supplémentaires depuis System Manager ou l'interface de ligne de commandes.

Prise en charge de l'ensemble des règles de Tiering

Vous pouvez désormais choisir la règle toutes les règles de Tiering lors de la création ou de la modification d'un volume pour Cloud Volumes ONTAP. Lorsque vous utilisez la règle de Tiering, les données sont immédiatement marquées comme inactives et hiérarchisées vers le stockage objet dès que possible. "En savoir plus sur le Tiering des données".

Cloud Manager transition vers SaaS (22 juin 2020)

Découvrez Cloud Manager comme une expérience en tant que service. Cette nouvelle expérience facilite l'utilisation de Cloud Manager et nous permet de proposer des fonctionnalités supplémentaires pour gérer votre infrastructure de cloud hybride. "En savoir plus >>".

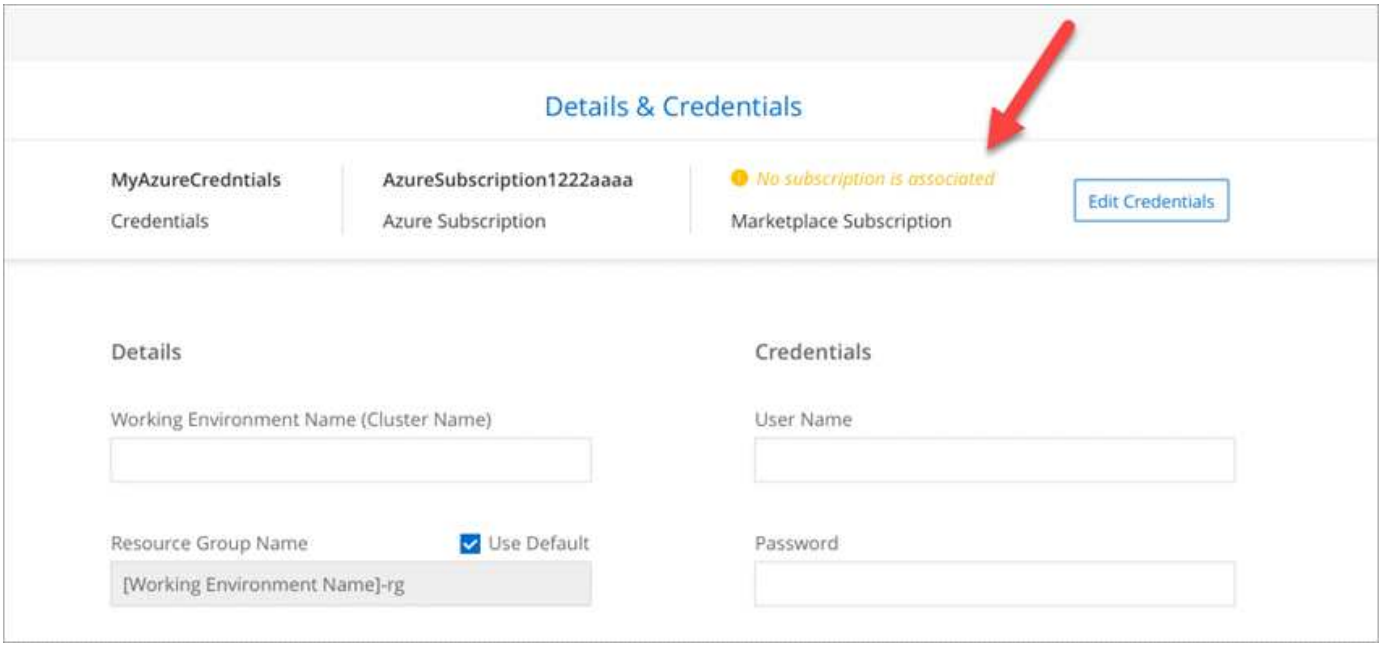
Cloud Manager 3.8.5 (31 mai 2020)

- Nouvel abonnement requis dans Azure Marketplace
- Améliorations de la sauvegarde dans le cloud
- Améliorations de Cloud Compliance

Nouvel abonnement requis dans Azure Marketplace

Un nouvel abonnement est disponible sur Azure Marketplace. Cet abonnement unique est nécessaire pour déployer Cloud Volumes ONTAP 9.7 PAYGO (sauf pour votre système d'essai gratuit de 30 jours). Par ailleurs, cet abonnement nous permet de proposer des fonctionnalités d'extension pour Cloud Volumes ONTAP PAYGO et BYOL. Vous serez facturé à partir de cet abonnement pour chaque système Cloud Volumes ONTAP PAYGO que vous créez et chaque fonction complémentaire que vous activez.

Lorsque vous déployez un nouveau système Cloud Volumes ONTAP (9.7 P1 ou ultérieure), Cloud Manager vous invite à vous abonner à cette offre.



Améliorations de la sauvegarde dans le cloud

Les améliorations suivantes sont désormais disponibles pour Backup vers le cloud :

- Dans Azure, vous pouvez désormais créer un nouveau groupe de ressources ou sélectionner un groupe de ressources existant au lieu d'en créer un pour vous. Impossible de modifier le groupe de ressources après l'activation de la sauvegarde dans le cloud.
- Dans AWS, vous pouvez maintenant sauvegarder des instances Cloud Volumes ONTAP résidant sur un compte AWS différent de celui de votre compte Cloud Manager AWS.
- D'autres options sont désormais disponibles lors de la sélection de la planification de sauvegarde pour les volumes. Outre les options de sauvegarde quotidiennes, hebdomadaires et mensuelles, vous pouvez désormais sélectionner l'une des règles définies par le système et qui prévoient des règles combinées, telles 30 que les sauvegardes quotidiennes, hebdomadaires 13 et 12 mensuelles.
- Après avoir supprimé toutes les sauvegardes d'un volume, vous pouvez à nouveau commencer à créer des sauvegardes pour ce volume. Il s'agissait d'une limitation connue dans la version précédente.

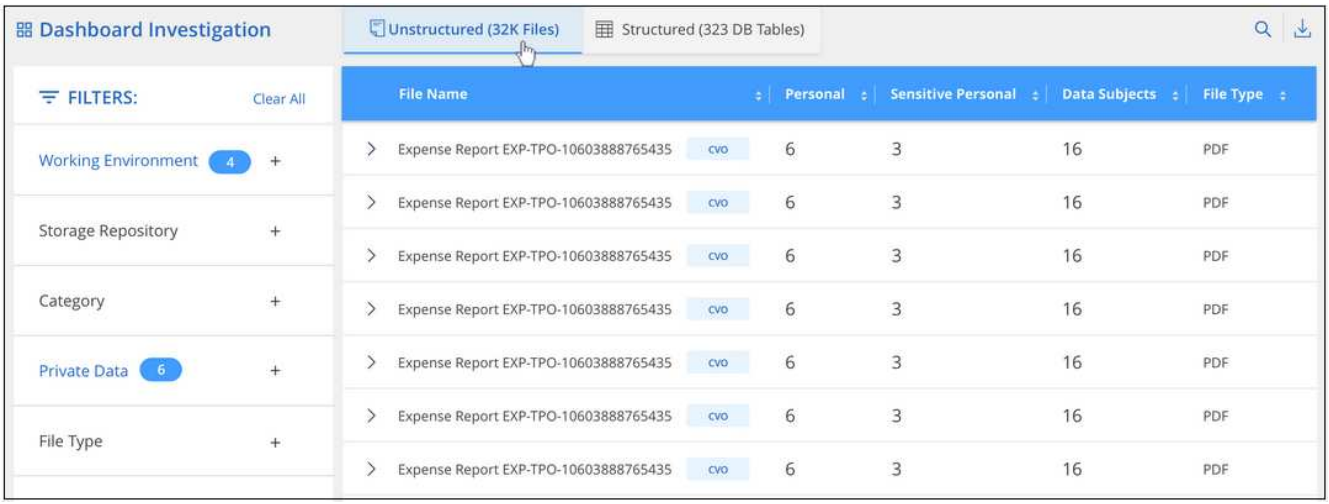
Améliorations de Cloud Compliance

Vous pouvez bénéficier des améliorations suivantes pour Cloud Compliance.

- Vous pouvez désormais analyser des compartiments S3 qui se trouvent dans différents comptes AWS que l'instance Cloud Compliance. Il vous suffit de créer un rôle sur ce nouveau compte pour que l'instance Cloud Compliance existante puisse se connecter à ces compartiments. "En savoir plus >>".

  Si vous avez configuré Cloud Compliance avant la version 3.8.5, vous devez modifier l'existant "Rôle IAM pour l'instance Cloud Compliance" pour utiliser cette fonctionnalité.

- Vous pouvez désormais filtrer le contenu de la page d'enquête pour n'afficher que les résultats que vous souhaitez voir. Les filtres comprennent l'environnement de travail, la catégorie, les données privées, le type de fichier, la date de la dernière modification, Et si les autorisations de l'objet S3 sont ouvertes à un accès public.



- Vous pouvez désormais activer et désactiver Cloud Compliance dans un environnement de travail directement à partir de l'onglet Cloud Compliance.

Mise à jour de Cloud Manager 3.8.4 (10 mai 2020)

Nous avons publié une amélioration pour Cloud Manager 3.8.4.

Intégration avec Cloud Insights

Grâce au service NetApp Cloud Insights, Cloud Manager vous donne des informations sur l'état et les performances de vos instances Cloud Volumes ONTAP et vous aide à résoudre et à optimiser les problèmes liés aux performances de votre environnement de stockage cloud. "En savoir plus >>".

Cloud Manager 3.8.4 (3 mai 2020)

Cloud Manager 3.8.4 comprend notamment :

Améliorations de la sauvegarde dans le cloud

Les améliorations suivantes sont désormais disponibles pour la sauvegarde dans le cloud (anciennement *Backup to S3* pour AWS) :

- **Sauvegarde vers stockage Azure Blob**

  Cloud Volumes ONTAP est désormais disponible dans Azure pour la sauvegarde dans le cloud. La solution de sauvegarde dans le cloud offre des fonctionnalités de sauvegarde et de restauration pour la protection et l'archivage à long terme de vos données cloud. "En savoir plus >>".

- **Suppression de sauvegardes**

  Vous pouvez désormais supprimer toutes les sauvegardes d'un volume spécifique directement depuis l'interface Cloud Manager. "En savoir plus >>".

Cloud Manager 3.8.3 (5 avril 2020)

- Intégration avec NetApp Cloud Tiering
- Migration des données vers Azure NetApp Files
- Améliorations de Cloud Compliance

- Sauvegardez vers les améliorations S3
- Volumes iSCSI avec API

Intégration avec NetApp Cloud Tiering

Le service NetApp Cloud Tiering est désormais disponible dans Cloud Manager. NetApp Cloud Tiering permet de transférer les données depuis un cluster ONTAP sur site vers un stockage objet à moindre coût dans le cloud. Cela libère de l'espace de stockage hautes performances sur le cluster pour davantage de charges de travail.

"En savoir plus >>".

Migration des données vers Azure NetApp Files

Vous pouvez désormais migrer des données NFS ou SMB vers Azure NetApp Files directement depuis Cloud Manager. La synchronisation des données est optimisée par le service Cloud Sync de NetApp.

"Découvrez comment migrer des données vers Azure NetApp Files".

Améliorations de Cloud Compliance

Cloud Compliance est désormais disponible avec les améliorations suivantes.

- **Essai gratuit de 30 jours pour Amazon S3**

  Une version d'essai gratuite de 30 jours est désormais disponible pour analyser les données Amazon S3 avec Cloud Compliance. Si vous avez précédemment activé Cloud Compliance sur Amazon S3, votre version d'évaluation gratuite de 30 jours est active à partir d'aujourd'hui (5 avril 2020).

  Un abonnement à AWS Marketplace est nécessaire pour continuer à analyser Amazon S3 à la fin de la période d'essai gratuite. "Découvrez comment vous inscrire".

  "En savoir plus sur la tarification pour scanner Amazon S3".

- **Nouveau type de données personnelles**

  Cloud Compliance trouve désormais un nouvel identifiant national dans les fichiers : l'identifiant brésilien (CPF).

  "En savoir plus sur les types de données personnelles".

- **Prise en charge des catégories de métadonnées supplémentaires**

  Cloud Compliance peut désormais catégoriser vos données en neuf catégories de métadonnées supplémentaires. "Consultez la liste complète des catégories de métadonnées prises en charge".

Sauvegardez vers les améliorations S3

Les améliorations suivantes sont désormais disponibles pour le service Backup vers S3.

- **Politique de cycle de vie S3 pour les sauvegardes**

  Les sauvegardes commencent dans la classe de stockage *Standard* et passent à la classe de stockage *Standard-Infrequent Access* après 30 jours.

- **Suppression de sauvegardes**

  Vous pouvez désormais supprimer des sauvegardes à l'aide d'une API Cloud Manager. "En savoir plus >>".

- **Bloquer l'accès public**

  Cloud Manager permet à présent de "Fonctionnalité d'accès public aux blocs Amazon S3" Dans le compartiment S3, les sauvegardes sont stockées.

Volumes iSCSI avec API

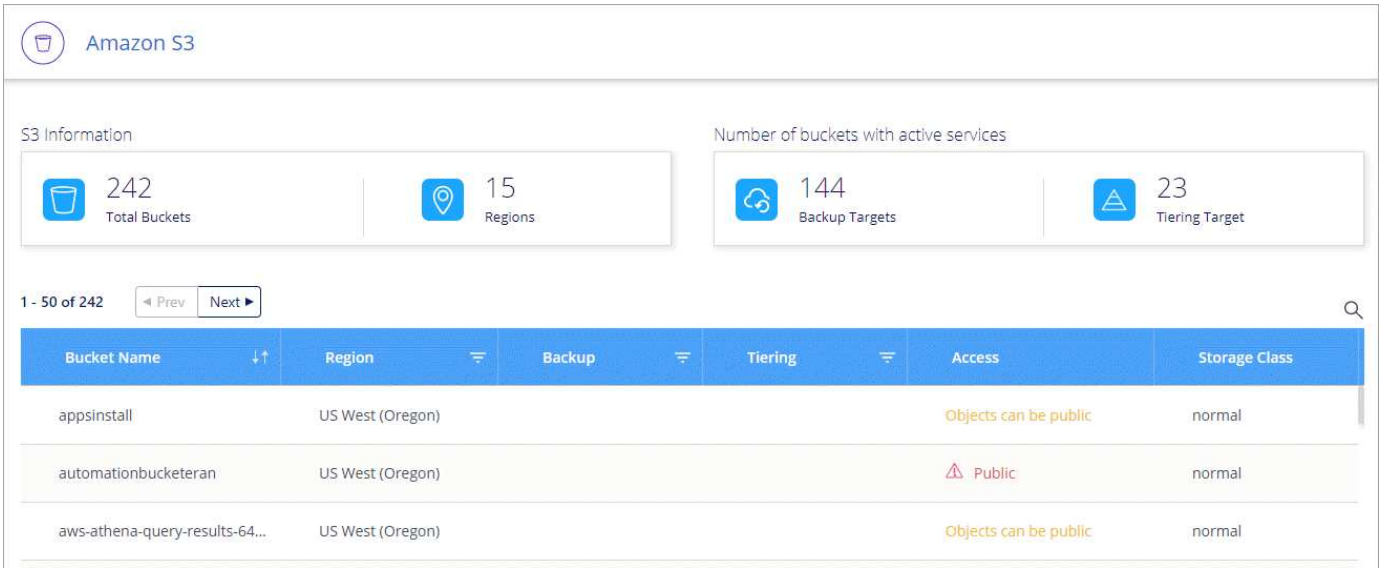
Les API Cloud Manager vous permettent désormais de créer des volumes iSCSI. "Voir un exemple ici".

Cloud Manager 3.8.2 (1er mars 2020)

- Les environnements de travail Amazon S3
- Améliorations de Cloud Compliance
- Version NFS pour les volumes
- Prise en charge des régions Azure Government

Les environnements de travail Amazon S3

Cloud Manager détecte désormais automatiquement les informations relatives aux compartiments Amazon S3 qui résident dans le compte AWS sur lequel il est installé. Vous pouvez ainsi consulter facilement des informations détaillées sur vos compartiments S3, notamment la région, le niveau d'accès, la classe de stockage et voir si le compartiment est utilisé avec Cloud Volumes ONTAP pour les sauvegardes ou le Tiering des données. Vous pouvez également analyser les compartiments S3 avec Cloud Compliance, comme décrit ci-dessous.



Améliorations de Cloud Compliance

Cloud Compliance est désormais disponible avec les améliorations suivantes.

- **Prise en charge d'Amazon S3**

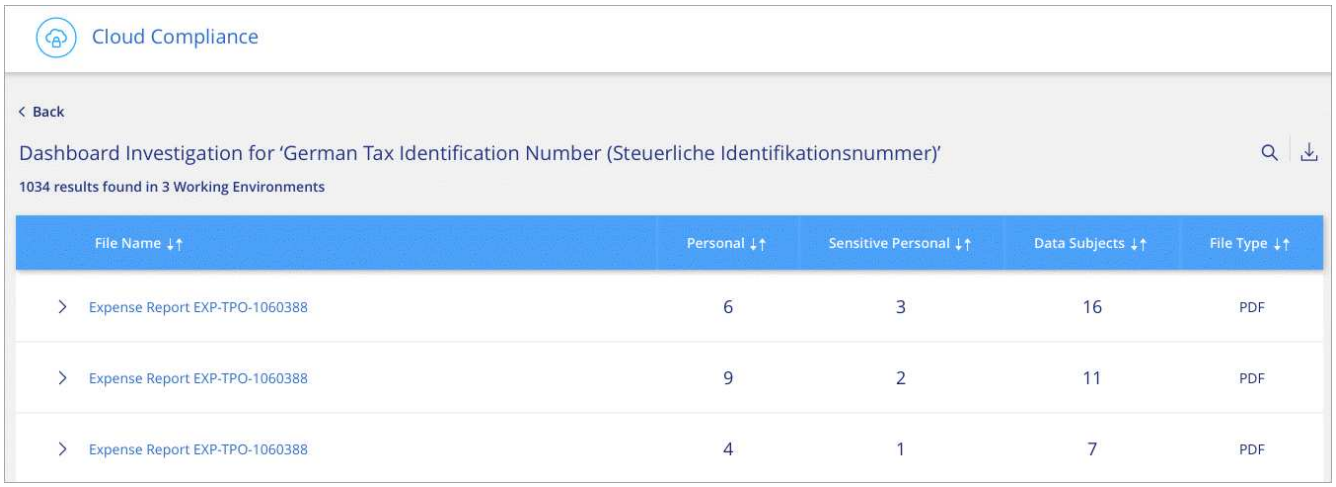
Cloud Compliance peut à présent analyser vos compartiments Amazon S3 pour identifier les données personnelles et sensibles qui résident dans le stockage objet S3. Cloud Compliance peut analyser n'importe quel compartiment du compte, quel que soit son origine pour une solution NetApp.

"Découvrez comment démarrer".

- **Page d'enquête**

  Une nouvelle page Investigation est maintenant disponible pour chaque type de fichier personnel, fichier personnel sensible, catégorie et type de fichier. La page affiche des détails sur les fichiers affectés et vous permet de trier par les fichiers qui incluent les données les plus personnelles, les données personnelles sensibles et les noms des sujets de données. Cette page remplace le rapport CSV précédemment disponible.

  Voici un exemple :



  "En savoir plus sur la page Investigation".

- **Rapport DSS PCI**

  Un nouveau rapport PCI DSS (Payment Card Industry Data Security Standard) est maintenant disponible. Ce rapport peut vous aider à identifier la distribution des informations de carte de crédit dans vos dossiers. Vous pouvez visualiser le nombre de fichiers contenant des informations de carte de crédit, que les environnements de travail soient protégés par le chiffrement, la protection contre les ransomwares, les informations de conservation, et bien plus encore.

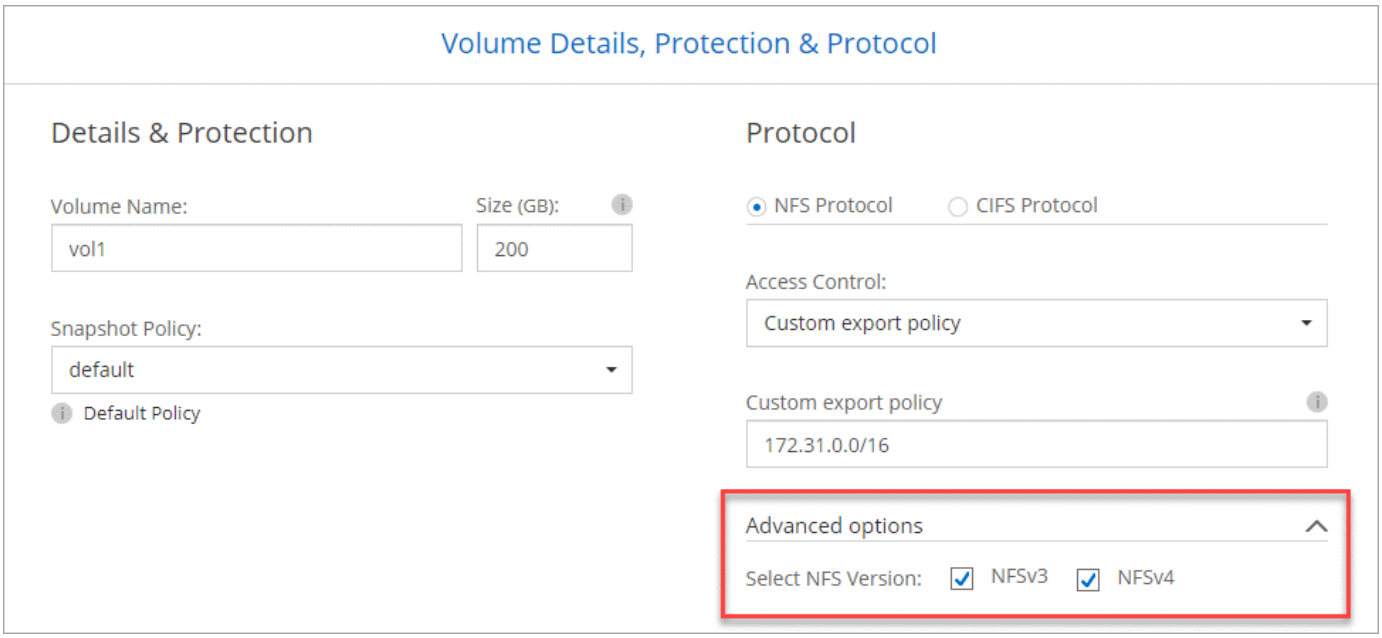
  "En savoir plus sur le rapport PCI DSS".

- **Nouveau type de données personnelles sensibles**

  Cloud Compliance peut désormais trouver des codes médicaux ICD-10-cm, utilisés dans le secteur médical et de la santé.

Version NFS pour les volumes

Vous pouvez maintenant sélectionner la version NFS à activer sur un volume lorsque vous créez ou modifiez un volume pour Cloud Volumes ONTAP.



Prise en charge des régions Azure Government

Les paires HA Cloud Volumes ONTAP sont désormais prises en charge dans les régions Azure Government.

"Consultez la liste des régions Azure prises en charge".

Mise à jour de Cloud Manager 3.8.1 (16 février 2020)

Nous avons publié quelques améliorations dans Cloud Manager 3.8.1.

Sauvegardez vers les améliorations S3

- Les copies de sauvegarde sont désormais stockées dans un compartiment S3 créé par Cloud Manager dans votre compte AWS, avec un compartiment par environnement de travail Cloud Volumes ONTAP.
- La sauvegarde vers S3 est désormais prise en charge dans toutes les régions AWS "Dans ce cas, Cloud Volumes ONTAP est pris en charge".
- Vous pouvez définir le planning de sauvegarde sur quotidien, hebdomadaire ou mensuel.
- Cloud Manager n'a plus besoin de configurer des *liens privés* vers le service Backup vers S3.

Ces améliorations nécessitent des autorisations S3 supplémentaires. Le rôle IAM qui fournit des autorisations à Cloud Manager doit inclure des autorisations provenant des dernières "Politique de Cloud Manager".

"En savoir plus sur Backup vers S3".

Mises à jour AWS

Nous avons introduit la prise en charge de nouvelles instances EC2 et une modification du nombre de disques de données pris en charge pour Cloud Volumes ONTAP 9.6 et 9.7. Consultez les modifications dans les notes de mise à jour de Cloud Volumes ONTAP.

- "Notes de version de Cloud Volumes ONTAP 9.7"
- "Notes de version de Cloud Volumes ONTAP 9.6"

Cloud Manager 3.8.1 (2 février 2020)

- Améliorations de Cloud Compliance
- Améliorations apportées aux comptes et aux abonnements
- Améliorations apportées au calendrier

Améliorations de Cloud Compliance

Cloud Compliance est désormais disponible avec les améliorations suivantes.

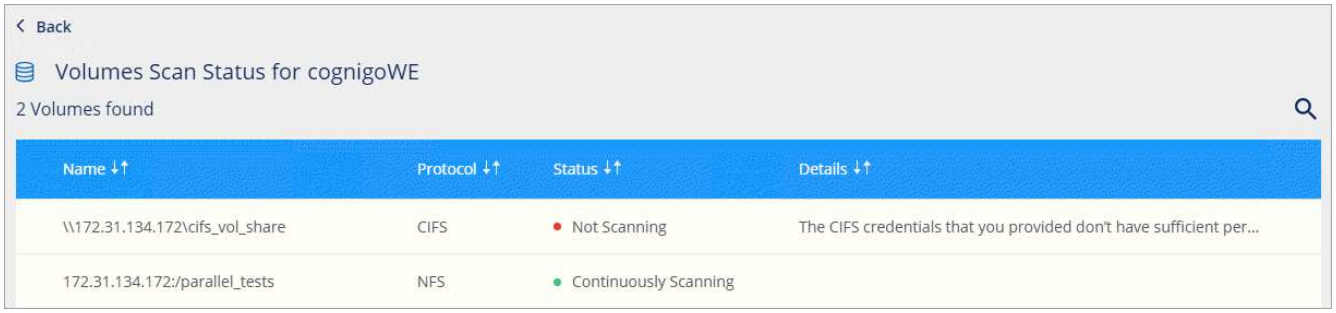
- * Prise en charge de Azure NetApp Files*

  Nous avons le plaisir de vous annoncer que Cloud Compliance peut désormais analyser Azure NetApp Files pour identifier les données personnelles et sensibles qui résident sur les volumes.

  "Découvrez comment démarrer".

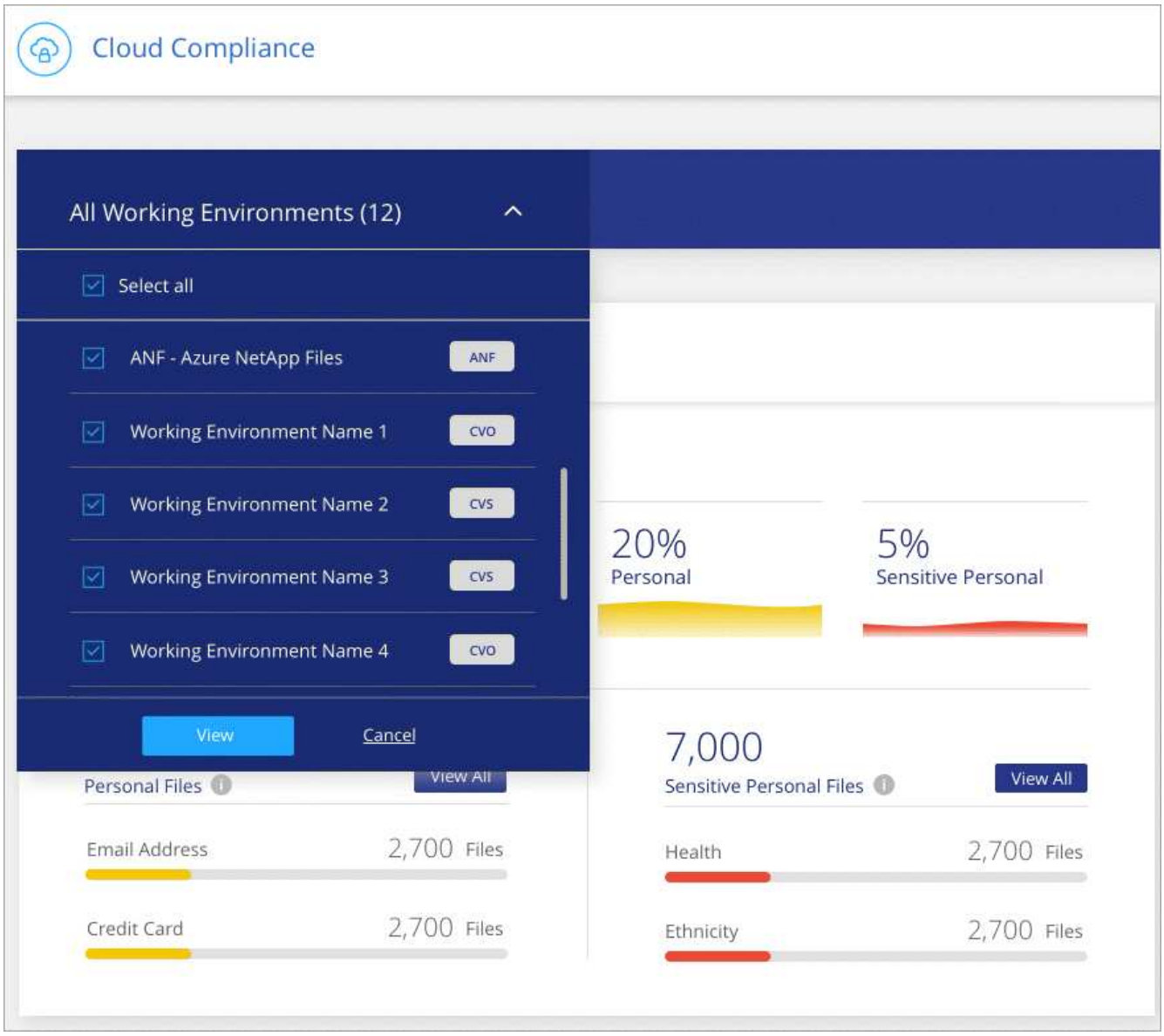
- **Etat de numérisation**

  Cloud Compliance affiche désormais l'état de scan pour chaque volume CIFS et NFS, y compris les messages d'erreur que vous pouvez utiliser pour corriger les problèmes.



- **Filtrer le tableau de bord par environnement de travail**

  Vous pouvez désormais filtrer le contenu du tableau de bord Cloud Compliance afin de voir les données de conformité pour des environnements de travail spécifiques.



- **Nouveau type de données personnelles**

  Cloud Compliance peut désormais identifier un permis de conduire en Californie lors de l'analyse de données.

- **Prise en charge des catégories supplémentaires**

  Trois catégories supplémentaires sont prises en charge : les données d'application, les journaux et les fichiers de base de données et d'index.

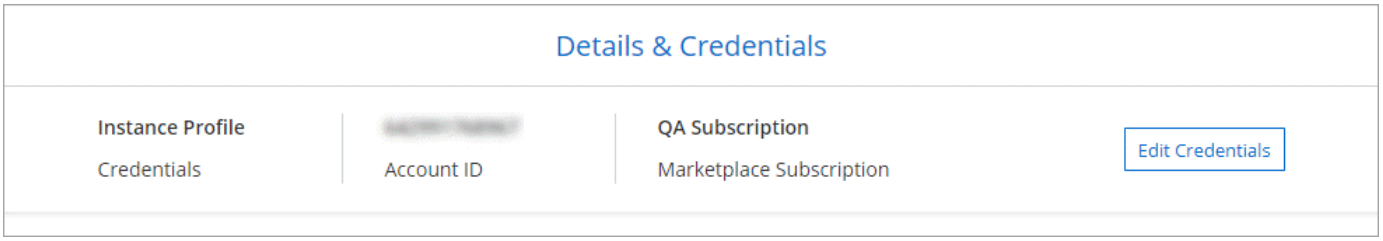
  "En savoir plus sur les catégories".

Améliorations apportées aux comptes et aux abonnements

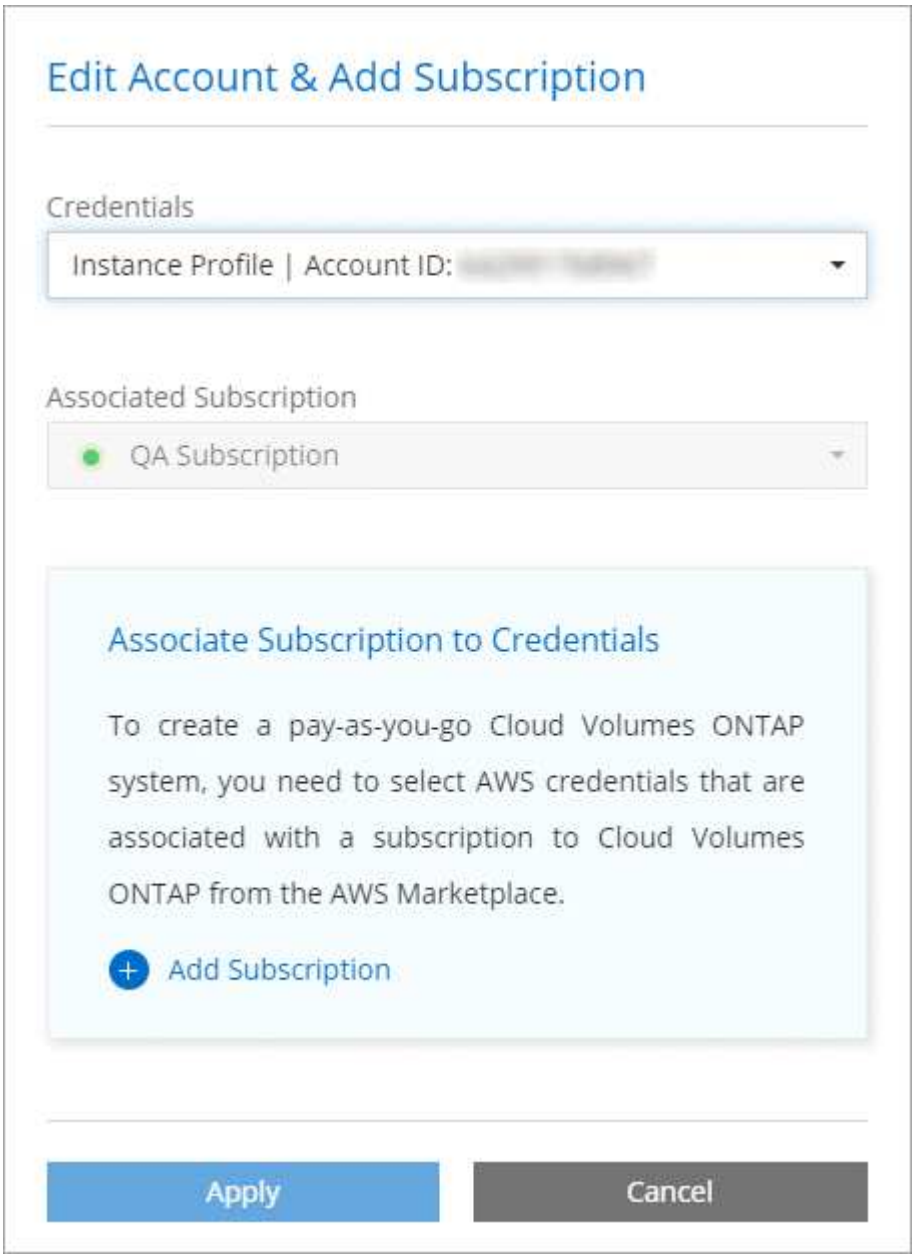
Nous avons simplifié la sélection d'un compte AWS ou d'un projet GCP, ainsi que l'abonnement Marketplace pour un système Cloud Volumes ONTAP avec paiement basé sur l'utilisation. Ces améliorations vous permettent de vous assurer que vous payez à partir du compte ou du projet approprié.

Par exemple, lorsque vous créez un système dans AWS, cliquez sur **Modifier les informations**

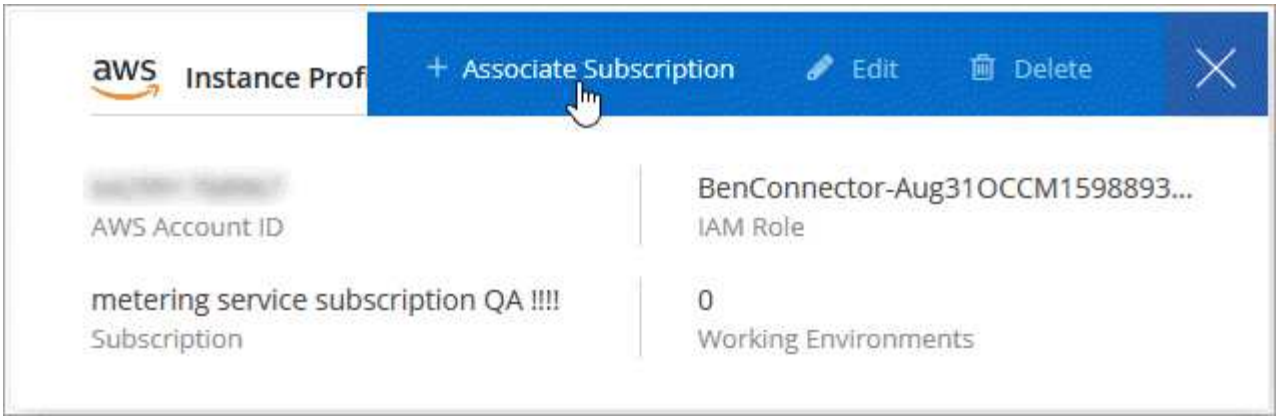
d'identification si vous ne souhaitez pas utiliser le compte et l'abonnement par défaut :



Ensuite, vous pouvez choisir les identifiants du compte à utiliser et l'abonnement AWS Marketplace associé. Vous pouvez même ajouter un abonnement Marketplace, si vous le souhaitez.



Si vous gérez plusieurs abonnements AWS, vous pouvez les attribuer à différentes informations d'identification AWS à partir de la page informations d'identification des paramètres :

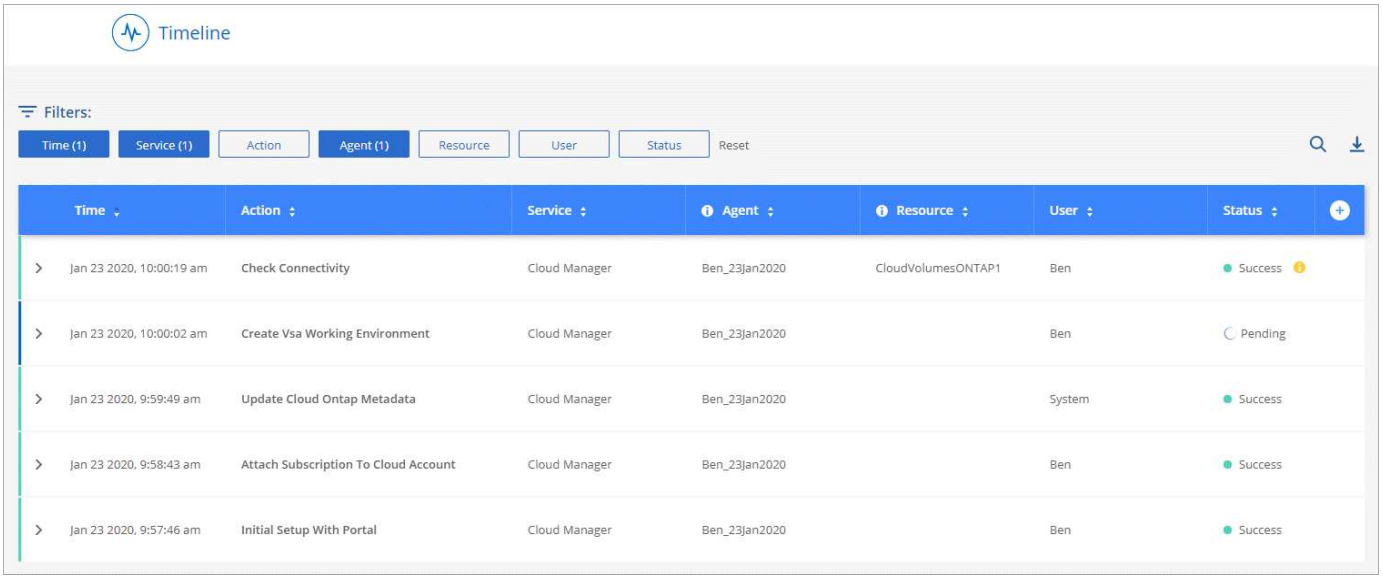


"Découvrez comment gérer les identifiants AWS dans Cloud Manager".

Améliorations apportées au calendrier

La chronologie a été améliorée afin de vous fournir des informations complémentaires sur les services cloud NetApp que vous utilisez.

- La chronologie montre maintenant les actions de tous les systèmes Cloud Manager au sein du même compte Cloud Central
- Vous pouvez désormais trouver plus facilement des informations en filtrant, en recherchant et en ajoutant et en supprimant des colonnes
- Vous pouvez à présent télécharger les données de la chronologie au format CSV
- À l'avenir, le calendrier montrera des actions pour chaque service cloud NetApp que vous utilisez (mais vous pouvez filtrer les informations en un seul service)



Cloud Manager 3.8 (8 janvier 2020)

- Amélioration DE LA HAUTE DISPONIBILITÉ dans Azure
- Améliorations du Tiering des données dans GCP

Amélioration DE LA HAUTE DISPONIBILITÉ dans Azure

Les améliorations suivantes sont désormais disponibles pour les paires HA Cloud Volumes ONTAP dans Azure.

- **Remplacer les verrous CIFS pour Cloud Volumes ONTAP HA dans Azure**

  Vous pouvez désormais activer un paramètre dans Cloud Manager qui empêche les problèmes liés au basculement du stockage Cloud Volumes ONTAP lors des événements de maintenance Azure. Lorsque vous activez ce paramètre, Cloud Volumes ONTAP vetoes les verrous CIFS et réinitialise les sessions CIFS actives. "En savoir plus >>".

- **Connexion HTTPS de Cloud Volumes ONTAP aux comptes de stockage**

  Vous pouvez désormais activer une connexion HTTPS à partir d'une paire HA Cloud Volumes ONTAP 9.7 vers des comptes de stockage Azure lors de la création d'un environnement de travail. Notez que l'activation de cette option peut avoir un impact sur les performances d'écriture. Vous ne pouvez pas modifier le paramètre après avoir créé l'environnement de travail.

- **Prise en charge des comptes de stockage v2 à usage général Azure**

  Les comptes de stockage créés par Cloud Manager pour les paires haute disponibilité Cloud Volumes ONTAP 9.7 sont désormais des comptes de stockage v2 à usage général.

Améliorations du Tiering des données dans GCP

Les améliorations suivantes sont disponibles pour le Tiering des données Cloud Volumes ONTAP dans GCP.

- **Classes de stockage Google Cloud pour le Tiering des données**

  Vous pouvez désormais choisir une classe de stockage pour les données Tiering Cloud Volumes ONTAP vers Google Cloud Storage :

  - Stockage standard (par défaut)
  - Stockage « nearline »
  - Stockage de la ligne de refroidissement

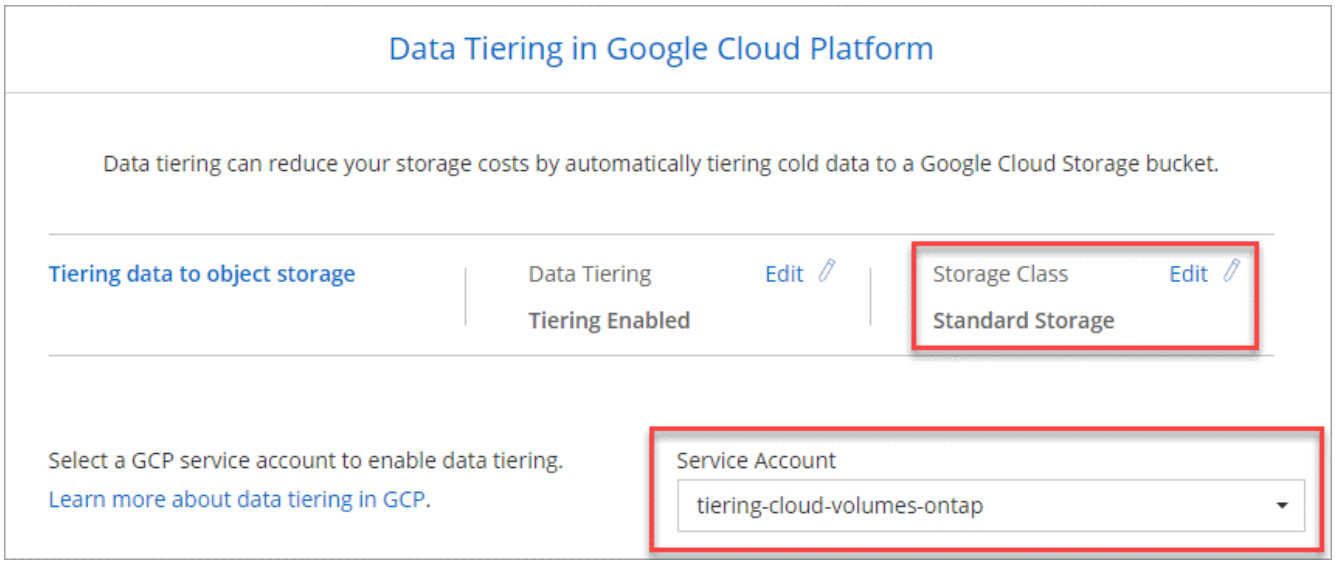
    "En savoir plus sur les classes de stockage Google Cloud".

  "Découvrez comment changer la classe de stockage pour Cloud Volumes ONTAP".

- **Hiérarchisation des données à l'aide d'un compte de service**

  Depuis la version 9.7, Cloud Manager attribue désormais un compte de service sur l'instance Cloud Volumes ONTAP. Ce compte de service fournit des autorisations de Tiering des données vers un compartiment Google Cloud Storage. Ce changement assure plus de sécurité et nécessite moins d'installation. Pour obtenir des instructions détaillées lors du déploiement d'un nouveau système, "reportez-vous à l'étape 4 de cette page".

  L'image suivante montre l'assistant Environnement de travail où vous pouvez sélectionner une classe de stockage et un compte de service :



Cloud Manager requiert les autorisations GCP suivantes pour ces améliorations, comme illustré en dernier "Règle Cloud Manager pour GCP".

```
- storage.buckets.update
- compute.instances.setServiceAccount
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
```

Transition de Cloud Manager vers SaaS

Nous avons proposé une expérience SaaS pour Cloud Manager. Cette nouvelle expérience facilite l'utilisation de Cloud Manager et nous permet de proposer des fonctionnalités supplémentaires pour gérer votre infrastructure de cloud hybride.

Expérience précédente de Cloud Manager

Le logiciel Cloud Manager comprenait auparavant une interface utilisateur et une couche de gestion qui envoyait des demandes aux fournisseurs de cloud. Pour commencer, déployez Cloud Manager dans votre réseau cloud ou sur site, puis accédez à l'interface utilisateur qui s'exécute sur cette instance.

Cette expérience a changé.

La nouvelle expérience SaaS

L'interface Cloud Manager est désormais accessible via une interface utilisateur SaaS que vous vous connectez à partir de NetApp Cloud Central. Vous n'avez plus besoin d'accéder à une interface utilisateur à partir d'un logiciel qui s'exécute sur votre réseau.

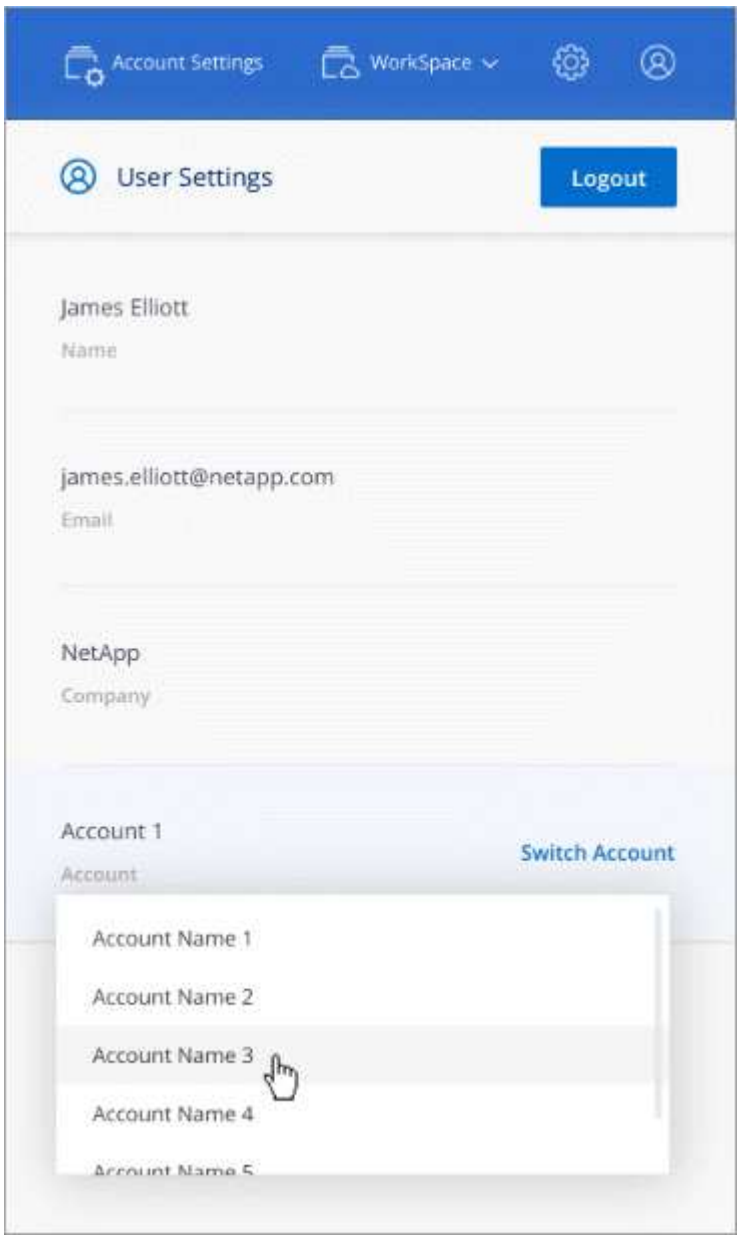
Dans la plupart des cas, vous devez déployer un *Connector* dans votre réseau cloud ou sur site. Il est le logiciel nécessaire pour gérer Cloud Volumes ONTAP et d'autres services de données cloud. (Le connecteur est en fait le même que le logiciel Cloud Manager que vous avez installé.)

Avantages

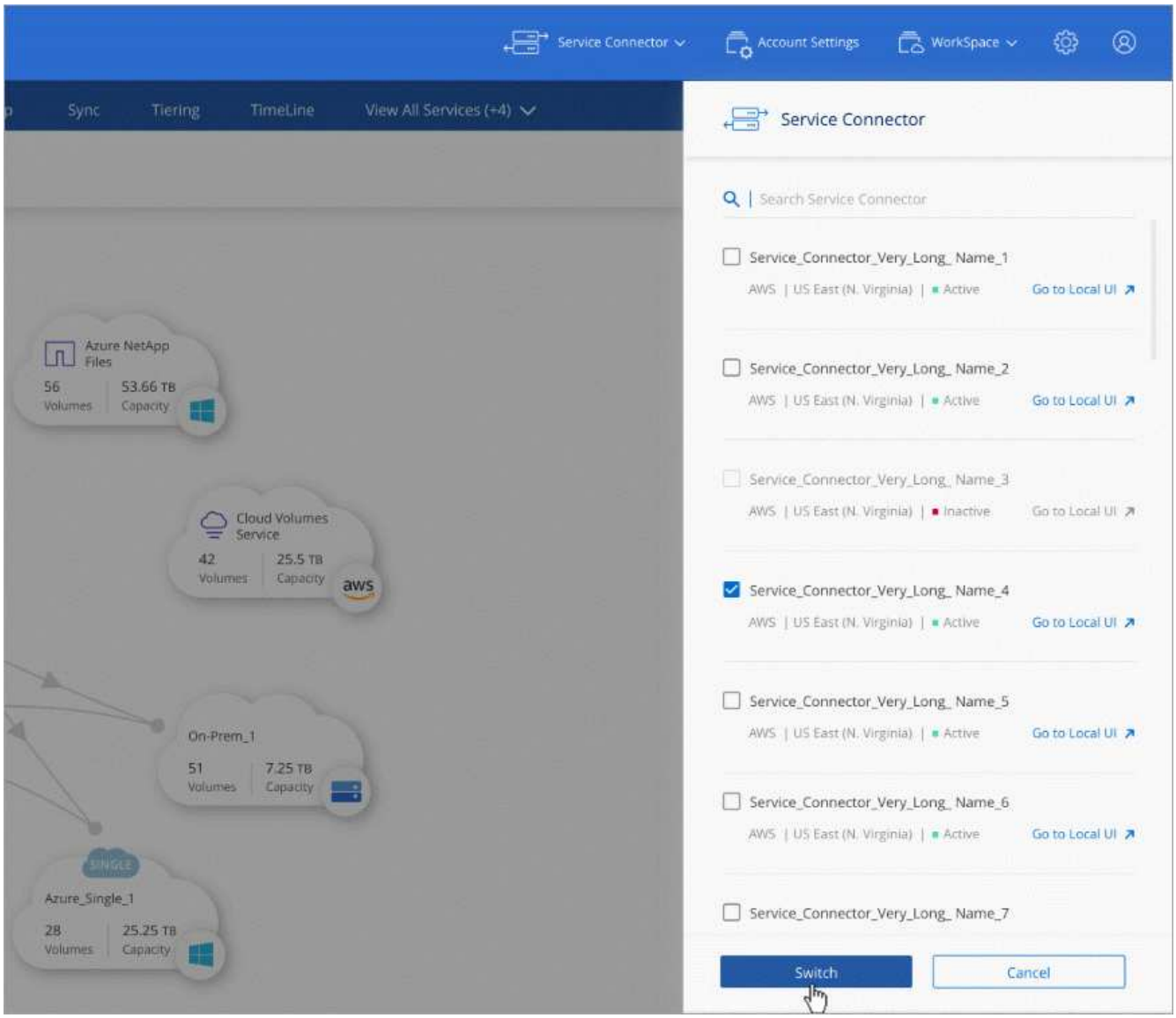
Cette approche SaaS présente plusieurs avantages :

- Il nous est ainsi possible de proposer des fonctionnalités de gestion supplémentaires pour Azure NetApp Files et Cloud Volumes Service sans avoir à déployer le logiciel dans votre environnement.
- Vous pouvez facilement basculer d'un compte Cloud Central à l'autre.

  Si un utilisateur est associé à plusieurs comptes Cloud Central, il peut à tout moment passer à un autre compte à partir du menu User Settings. Ils peuvent alors voir les connecteurs et les environnements de travail associés à ce compte.



- Vous pouvez facilement passer d'un connecteur à l'autre (ce que vous connaissez aujourd'hui comme le logiciel Cloud Manager) installé sur différents réseaux ou fournisseurs de Cloud.

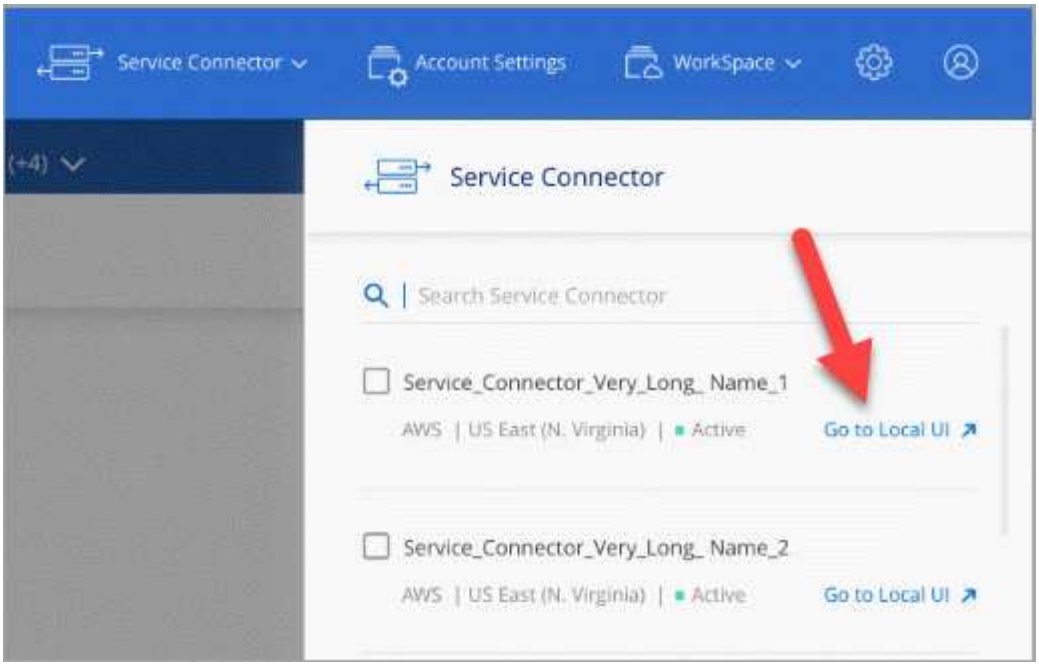


Interface utilisateur locale

Bien que vous devriez effectuer presque toutes les tâches à partir de l'interface utilisateur SaaS, une interface utilisateur locale est toujours disponible sur le connecteur. Cette interface est nécessaire pour quelques tâches qui doivent être effectuées à partir du connecteur lui-même :

- Configuration d'un serveur proxy
- Installation d'un correctif
- Téléchargement des messages AutoSupport

Vous pouvez accéder à l'interface utilisateur locale directement à partir de l'interface utilisateur SaaS :



Modifications en fonction de l'instance, du serveur virtuel et du type d'ordinateur

Dans Cloud Manager, nous avons modifié l'instance minimale requise, la machine virtuelle et le type de machine en fonction des ressources appropriées pour les nouvelles fonctionnalités et les prochaines fonctionnalités :

- AWS : instance de t3.XLarge
- Azure: DS3 v2
- GCP : N1-standard-4

Lorsque vous mettez à niveau le type de machine, vous aurez accès à des fonctionnalités telles que Kubernetes, Global File cache, Monitoring, etc.

Ces tailles par défaut sont le minimum pris en charge "En fonction des besoins en processeur et en RAM".

Cloud Manager vous invite à modifier le type de machine du connecteur.

Problèmes connus

Les problèmes connus identifient les problèmes susceptibles de vous empêcher d'utiliser cette version du produit avec succès.

Cette version de Cloud Manager ne présente aucun problème connu.

Vous trouverez les problèmes connus relatifs à Cloud Volumes ONTAP dans le "Notes de version de Cloud Volumes ONTAP" Et pour les logiciels ONTAP en général dans le "Notes de version de ONTAP".

Limites connues

Les limitations connues identifient les plateformes, les périphériques ou les fonctions qui ne sont pas pris en charge par cette version du produit, ou qui ne fonctionnent pas correctement avec elle. Examinez attentivement ces limites.

Les connecteurs doivent rester en fonctionnement

Un connecteur doit rester en fonctionnement en permanence. Il est important pour la santé et le fonctionnement continus des services que vous proposez.

Par exemple, un connecteur est un composant clé de la santé et du fonctionnement des systèmes Cloud Volumes ONTAP PAYGO. Si un connecteur est hors tension, les systèmes Cloud Volumes ONTAP PAYGO s'arrêtent après une perte de communication avec un connecteur pendant plus de 14 jours.

La plateforme SaaS est désactivée pour les régions du secteur public

Si vous déployez un connecteur dans une région AWS GovCloud, une région Azure Government ou une région Azure DoD, l'accès à Cloud Manager n'est disponible qu'via l'adresse IP d'hôte d'un connecteur. L'accès à la plateforme SaaS est désactivé pour l'ensemble du compte.

Cela signifie que seuls les utilisateurs privilégiés qui peuvent accéder au VPC/vNet interne de l'utilisateur final peuvent utiliser l'interface ou l'API de Cloud Manager.

Cloud Manager ne propose pas non plus les services suivants :

- Conformité cloud
- Kubernetes
- Tiering dans le cloud
- Cache global de fichiers
- Surveillance (Cloud Insights)

Vous devez utiliser la plateforme SaaS pour pouvoir utiliser ces services.

Les hôtes Linux partagés ne sont pas pris en charge

Le connecteur n'est pas pris en charge sur un hôte partagé avec d'autres applications. L'hôte doit être un hôte dédié.

Cloud Manager ne prend pas en charge les volumes FlexGroup

Cloud Volumes ONTAP prend en charge les volumes FlexGroup, mais pas Cloud Manager. Si vous créez un volume FlexGroup depuis System Manager ou depuis l'interface de ligne de commandes, définissez le mode de gestion de la capacité de Cloud Manager sur Manuel. Le mode automatique peut ne pas fonctionner correctement avec les volumes FlexGroup.

Modifications importantes apportées à Cloud Manager

Cette page présente les changements importants apportés à Cloud Manager, qui peuvent vous aider à utiliser le service dès que nous y apportons de nouvelles améliorations. Vous devez continuer à lire le "Quoi de neuf" pour en savoir plus sur toutes les nouvelles fonctionnalités et améliorations.

Modifications du SaaS

Nous avons introduit une expérience SaaS pour Cloud Manager. Cette nouvelle expérience facilite l'utilisation de Cloud Manager et nous permet de proposer des fonctionnalités supplémentaires pour gérer votre infrastructure de cloud hybride.

- "Transition de Cloud Manager vers SaaS"
- "Découvrez le fonctionnement de Cloud Manager"

Changement de type de machine

Dans Cloud Manager, nous avons modifié l'instance minimale requise, la machine virtuelle et le type de machine en fonction des ressources appropriées pour les nouvelles fonctionnalités et les prochaines fonctionnalités :

- AWS : instance de t3.XLarge
- Azure: DS3 v2
- GCP : N1-standard-4

Lorsque vous mettez à niveau le type de machine, vous aurez accès à des fonctionnalités telles que Kubernetes, Global File cache, Monitoring, etc.

Ces tailles par défaut sont le minimum pris en charge "En fonction des besoins en processeur et en RAM".

Cloud Manager vous invite à modifier le type de machine du connecteur.

Paramètres du compte

Nous avons introduit les comptes Cloud Central pour fournir la colocation, vous aider à organiser les utilisateurs et les ressources dans des espaces de travail isolés, et pour gérer l'accès aux connecteurs et aux abonnements.

- "En savoir plus sur les comptes Cloud Central : utilisateurs, espaces de travail, connecteurs et abonnements"
- "Découvrez comment utiliser votre compte"
- "Découvrez comment gérer votre compte après sa configuration"

Nouvelles autorisations

Cloud Manager nécessite parfois des autorisations supplémentaires sur les fournisseurs de cloud à mesure que nous introduirons de nouvelles fonctionnalités et améliorations. Cette section identifie les nouvelles autorisations qui sont maintenant requises.

Vous trouverez la liste des autorisations les plus récentes sur le "Page des règles de Cloud Manager".

AWS

Depuis la version 3.8.1, vous devez disposer des autorisations suivantes pour utiliser Backup to Cloud avec Cloud Volumes ONTAP. "En savoir plus >>".

```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

Azure

- Pour éviter les échecs de déploiement d'Azure, vérifiez que votre stratégie Cloud Manager dans Azure inclut l'autorisation suivante :

```
"Microsoft.Resources/deployments/operationStatuses/read"
```

- À partir de la version 3.8.7, l'autorisation suivante est requise pour chiffrer les disques gérés Azure sur des

systèmes Cloud Volumes ONTAP à un seul nœud à l'aide de clés externes provenant d'un autre compte. "En savoir plus >>".

```
"Microsoft.Compute/diskEncryptionSets/read"
```

- Les autorisations suivantes sont requises pour activer le cache global de fichiers sur Cloud Volumes ONTAP. "En savoir plus >>".

```
"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
```

GCP

Nouvelles autorisations de gestion Kubernetes

Depuis la version 3.8.8, le compte de service d'un connecteur nécessite les autorisations suivantes pour découvrir et gérer les clusters Kubernetes qui s'exécutent dans Google Kubernetes Engine (GKE) :

```
- container.*
```

Nouvelles autorisations de Tiering des données

Depuis la version 3.8, vous devez disposer des autorisations suivantes pour utiliser un compte de service pour le Tiering des données. "En savoir plus >>".

```
- storage.buckets.update
- compute.instances.setServiceAccount
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
```

Nouveaux terminaux

Le connecteur nécessite un accès Internet sortant pour gérer les ressources et les processus au sein de votre environnement de cloud public. Cette section identifie les nouveaux terminaux qui sont maintenant requis.

Vous pouvez trouver le "liste complète des points de terminaison accessibles à partir de votre navigateur web ici" et le "Liste complète des noeuds finaux accessibles par le connecteur ici".

- Les utilisateurs doivent accéder à Cloud Manager à partir d'un navigateur Web en contactant le terminal suivant :

  https://cloudmanager.netapp.com

- Pour obtenir des images logicielles de composants de conteneur pour une infrastructure Docker, les connecteurs doivent accéder au terminal suivant :

  https://cloudmanagerinfraprod.azurecr.io

  Assurez-vous que votre pare-feu autorise l'accès à ce noeud final à partir du connecteur.

Commencez avec Cloud Manager

Découvrez Cloud Manager

Cloud Manager permet aux experts IT et aux architectes cloud de gérer de manière centralisée leur infrastructure multicloud hybride à l'aide des solutions cloud NetApp.

Caractéristiques

Cloud Manager est une plateforme de gestion SaaS de grande qualité qui vous permet de garder le contrôle sur vos données, où qu'elles se trouvent.

- Configuration et utilisation "Cloud Volumes ONTAP" pour une gestion efficace des données multiprotocole sur l'ensemble des clouds.
- Configuration et utilisation des services de stockage de fichiers : "Azure NetApp Files", "Cloud Volumes Service pour AWS", et "Cloud Volumes Service pour Google Cloud".
- Découvrez et gérez les clusters ONTAP sur site en créant des volumes, en sauvegardant dans le cloud, en répliquant les données dans l'ensemble de votre cloud hybride et en effectuant le Tiering des données inactives dans le cloud.
- Services clouds intégrés et logiciels similaires à ceux proposés "Conformité cloud", "Cloud Insights", "Cloud Backup Service", "Trident", et plus encore.

"En savoir plus sur Cloud Manager".

Fournisseurs de stockage objet pris en charge

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

Le coût

Cloud Manager est gratuit pour NetApp.

Pour la plupart des tâches, Cloud Manager vous invite à déployer un connecteur dans votre réseau cloud, ce qui entraîne des frais supplémentaires pour l'instance de calcul et le stockage associé. Vous avez la possibilité d'exécuter le logiciel de connecteur sur votre site.

Fonctionnement de Cloud Manager

Cloud Manager inclut une interface SaaS intégrée à NetApp Cloud Central et des connecteurs qui gèrent Cloud Volumes ONTAP et d'autres services cloud.

Services à la demande

Cloud Manager est accessible via un "Interface utilisateur SaaS" Et les API. Cette expérience SaaS vous permet d'accéder automatiquement aux toutes dernières fonctionnalités dès leur sortie et de basculer facilement entre vos comptes et connecteurs Cloud Central.

NetApp Cloud Central

"NetApp Cloud Central" cette solution est centralisée pour l'accès et la gestion "Services clouds NetApp". Avec l'authentification utilisateur centralisée, vous pouvez utiliser le même ensemble d'identifiants pour accéder à Cloud Manager et à d'autres services cloud tels qu'Cloud Insights.

Lorsque vous vous connectez à Cloud Manager pour la première fois, vous êtes invité à créer un *compte Cloud Central*. Ce compte fournit la colocation et vous permet d'organiser les utilisateurs et les ressources dans des *espaces de travail* isolés.

Connecteurs

Dans la plupart des cas, un administrateur de compte devra déployer un *Connector* dans votre réseau cloud ou sur site. Ce connecteur permet à Cloud Manager de gérer les ressources et les processus au sein de votre environnement de cloud public.

Un connecteur doit rester en fonctionnement en permanence. Il est important pour la santé et le fonctionnement continus des services que vous proposez.

Par exemple, un connecteur est un composant clé de la santé et du fonctionnement des systèmes Cloud Volumes ONTAP PAYGO. Si un connecteur est hors tension, les systèmes Cloud Volumes ONTAP PAYGO s'arrêtent après une perte de communication avec un connecteur pendant plus de 14 jours.

"En savoir plus sur le moment où les connecteurs sont nécessaires et leur fonctionnement".

Présentation du réseau

Avant de se connecter à Cloud Manager, vous devez vous assurer que leur navigateur Web peut accéder à des terminaux spécifiques. Ensuite, vous devez vérifier les besoins en réseau pour le type spécifique d'environnement de travail et de services qui seront utilisés.

Terminaux accessibles à partir de votre navigateur Web

Les utilisateurs doivent accéder à Cloud Manager à partir d'un navigateur Web. La machine exécutant le navigateur Web doit disposer de connexions aux terminaux suivants :

Terminaux	Objectif
https://cloudmanager.cloud.netapp.com	Pour vous connecter à l'interface SaaS Cloud Manager.
https://api.services.cloud.netapp.com	Pour contacter les API Cloud Central.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Votre navigateur Web se connecte à ces terminaux pour une authentification centralisée des utilisateurs via NetApp Cloud Central.
https://widget.intercom.io	Vous bénéficiez d'un chat en ligne pour discuter avec des experts du cloud NetApp.

Index des besoins réseau

- "Connecteurs"

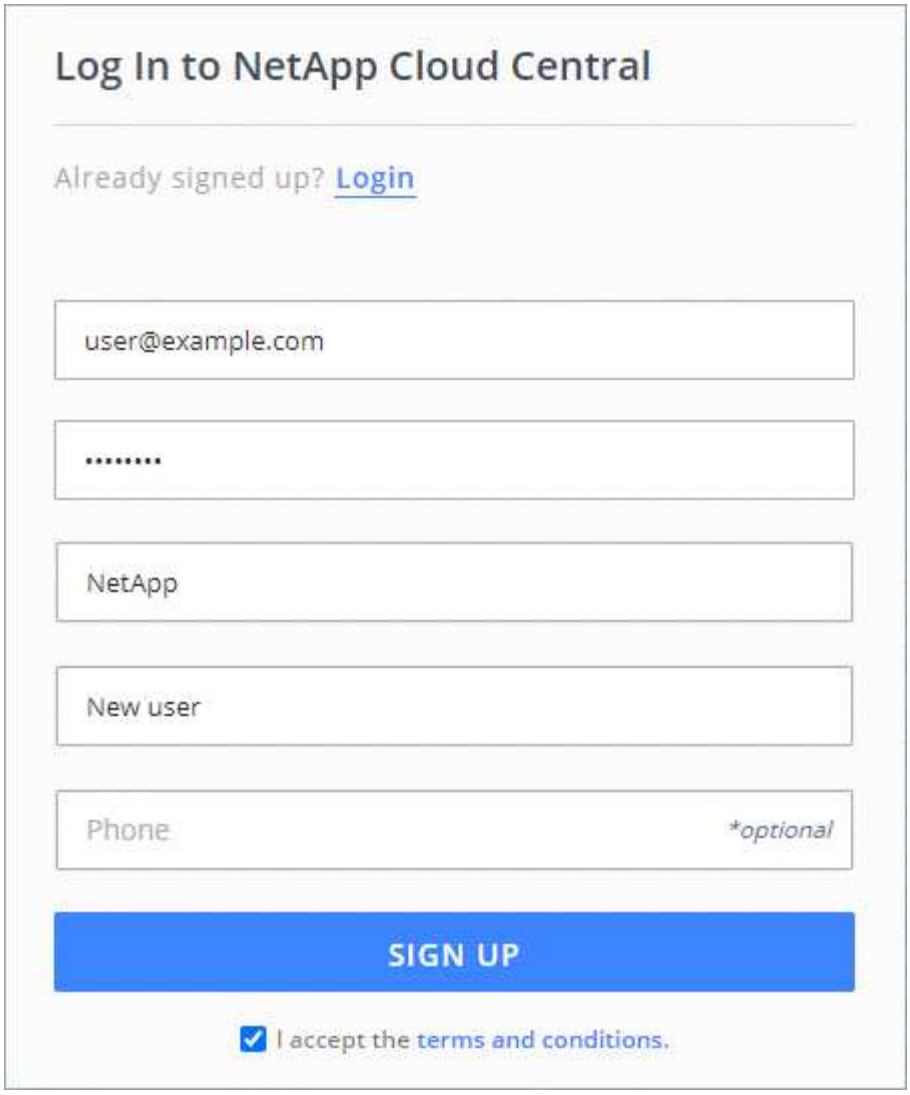
- "Cloud Volumes ONTAP pour AWS"
- "Cloud Volumes ONTAP pour Azure"
- "Cloud Volumes ONTAP pour GCP"
- "Réplication des données entre les systèmes ONTAP"
- "Cloud Compliance pour Cloud Volumes ONTAP ou Azure NetApp Files"
- "Cloud Compliance pour Amazon S3"
- "Clusters ONTAP sur site"
  - "Tiering des données depuis les clusters ONTAP vers Amazon S3"
  - "Tiering des données depuis les clusters ONTAP vers le stockage Azure Blob"
  - "Tiering des données depuis les clusters ONTAP vers Google Cloud Storage"
  - "Tiering des données depuis les clusters ONTAP vers StorageGRID"

S’inscrire à NetApp Cloud Central

Inscrivez-vous à NetApp Cloud Central pour accéder aux services cloud de NetApp.

Étapes

1. Ouvrez un navigateur Web et accédez à "NetApp Cloud Central".
2. Cliquez sur **s’inscrire**.
3. Remplissez le formulaire et cliquez sur **s’inscrire**.



4. Attendez qu'un e-mail soit envoyé par NetApp Cloud Central.
5. Cliquez sur le lien dans l'e-mail pour vérifier votre adresse e-mail.

Résultat

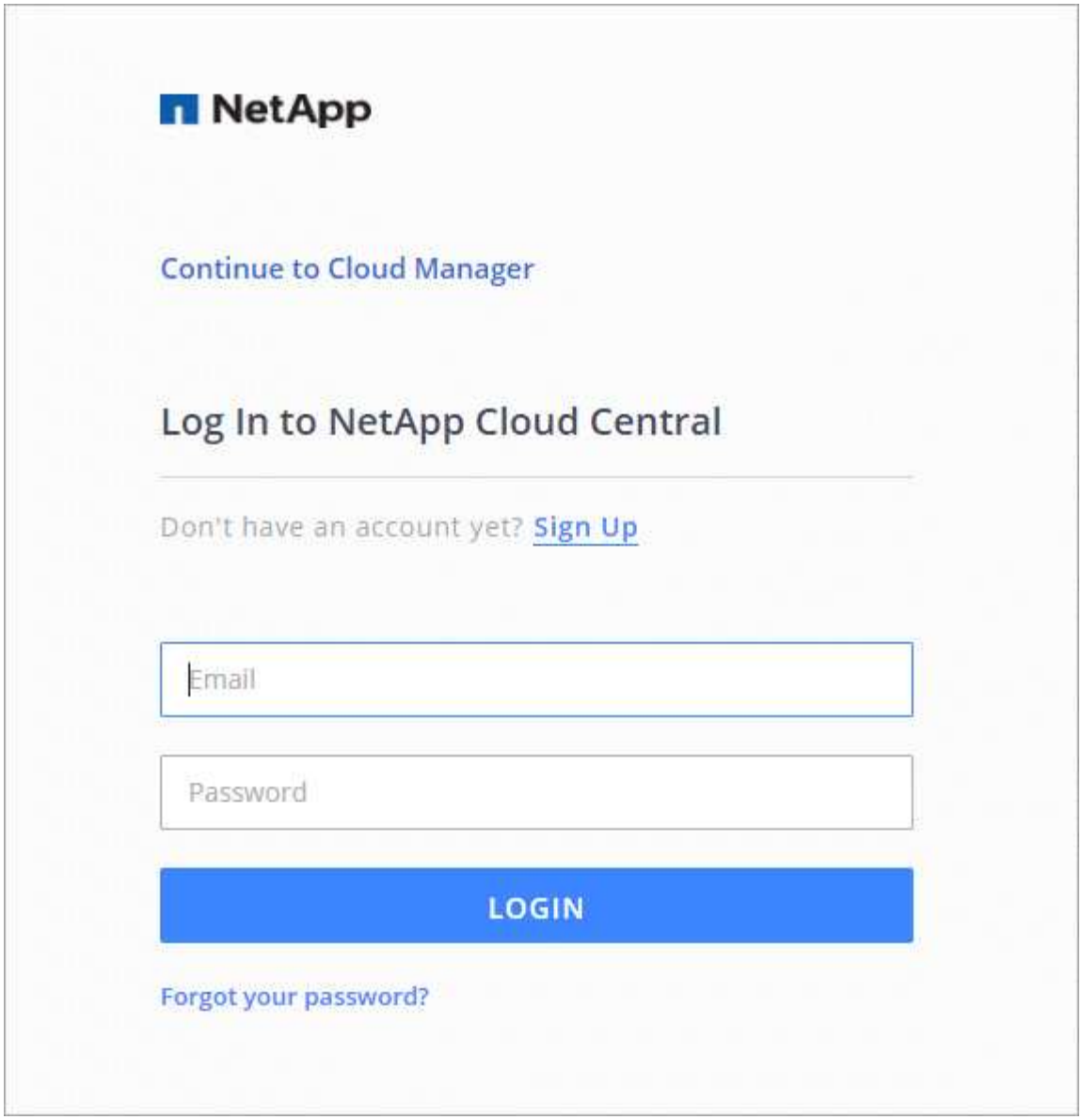
Vous disposez désormais d'un utilisateur Cloud Central actif.

Connectez-vous à Cloud Manager

L'interface Cloud Manager est accessible via une interface utilisateur SaaS, en accédant à https://cloudmanager.netapp.com.

Étapes

1. Ouvrez un navigateur Web et accédez à https://cloudmanager.netapp.com.
2. Connectez-vous à l'aide de vos identifiants NetApp Cloud Central.



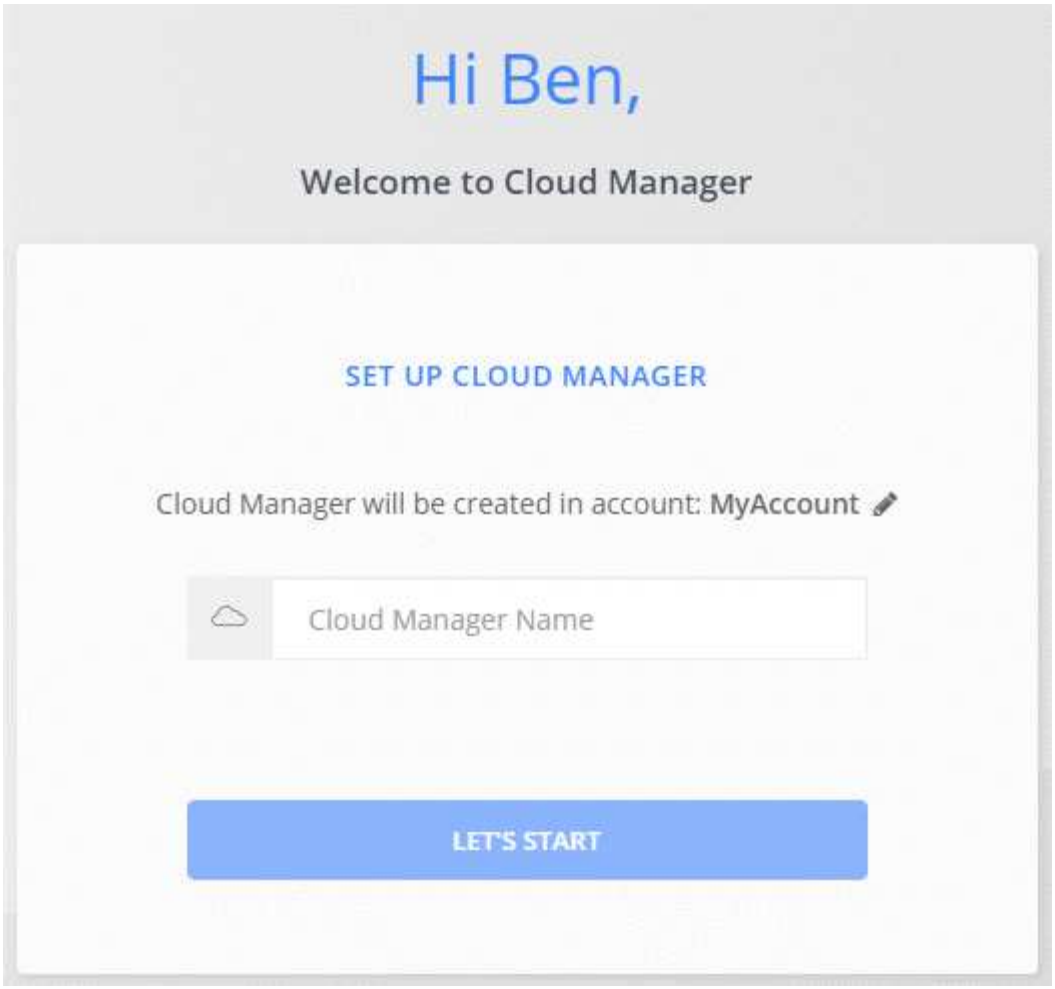
Configurez un compte Cloud Central

Paramètres du compte : utilisateurs, espaces de travail, connecteurs et abonnements

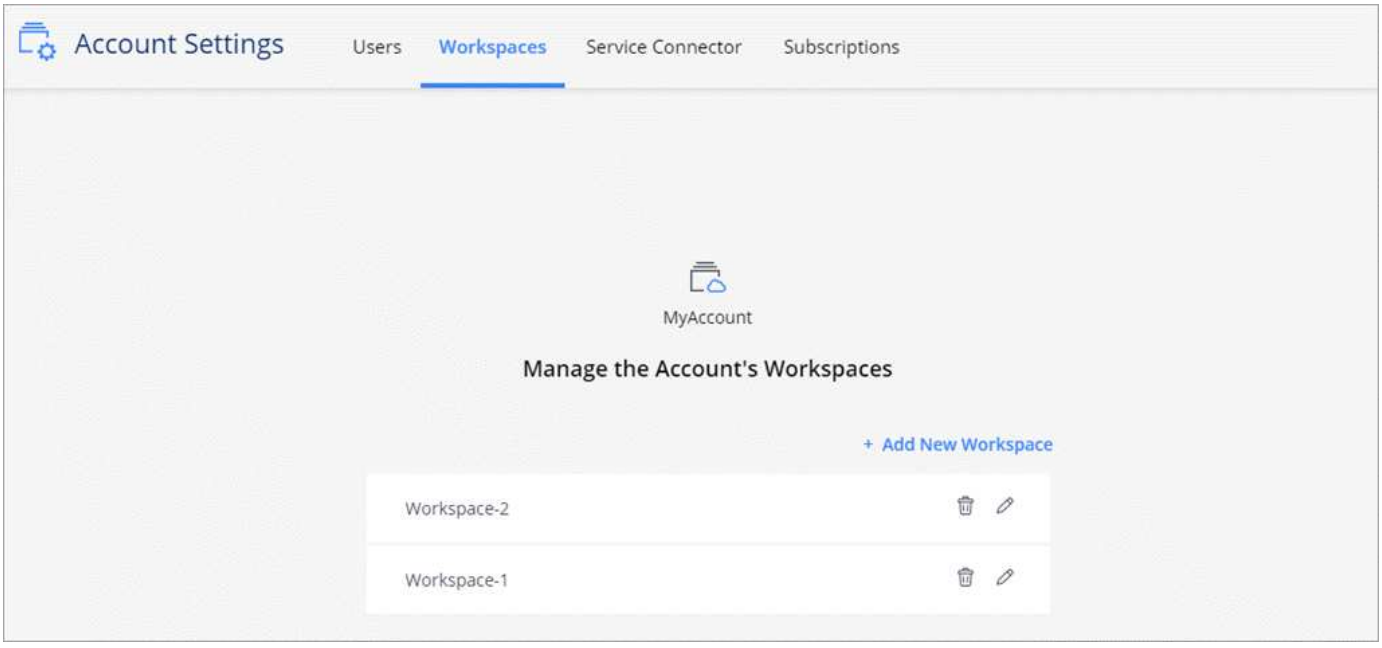
Un *Cloud Central account* propose la colocation et vous permet d'organiser des utilisateurs et des ressources dans des espaces de travail isolés à partir de Cloud Manager.

Par exemple, plusieurs utilisateurs peuvent déployer et gérer des systèmes Cloud Volumes ONTAP dans des environnements isolés appelés *espaces de travail*. Ces espaces de travail sont invisibles pour les autres utilisateurs, à moins qu'ils ne soient partagés.

Lorsque vous accédez pour la première fois à Cloud Manager, vous êtes invité à sélectionner ou à créer un compte Cloud Central :



Les administrateurs de comptes peuvent ensuite modifier les paramètres de ce compte en gérant les utilisateurs, les espaces de travail, les connecteurs et les abonnements :



Pour obtenir des instructions détaillées, reportez-vous à la section "Configuration du compte Cloud Central".

Paramètres du compte

Le widget Paramètres de compte dans Cloud Manager permet aux administrateurs de compte de gérer un compte Cloud Central. Si vous venez de créer votre compte, vous commencerez de zéro. Mais si vous avez déjà configuré un compte, vous verrez *All* les utilisateurs, les espaces de travail, les connecteurs et les abonnements associés au compte.

Utilisateurs

Les utilisateurs qui s'affichent dans les paramètres de compte sont les utilisateurs NetApp Cloud Central que vous associez à votre compte Cloud Central. L'association d'un utilisateur à un compte et d'un ou plusieurs espaces de travail dans ce compte permet à ces utilisateurs de créer et de gérer des environnements de travail dans Cloud Manager.

Lorsque vous associez un utilisateur, vous lui attribuez un rôle :

- *Account Admin* : peut effectuer n'importe quelle action dans Cloud Manager.
- *Workspace Admin* : permet de créer et de gérer des ressources dans l'espace de travail affecté.
- *Cloud Compliance Viewer*: Peut uniquement afficher les informations de conformité et générer des rapports pour les systèmes auxquels ils sont autorisés à accéder.

Espaces de travail

Dans Cloud Manager, un espace de travail isole tout nombre de *environnements de travail* des autres environnements de travail. Les administrateurs de l'espace de travail ne peuvent pas accéder aux environnements de travail dans un espace de travail à moins que l'administrateur du compte n'associe l'administrateur à cet espace de travail.

Un environnement de travail représente un système de stockage :

- Un système Cloud Volumes ONTAP à un seul nœud ou une paire HA
- Un cluster ONTAP sur site dans votre réseau
- Un cluster ONTAP dans une configuration de stockage privé NetApp

Connecteurs

Un connecteur permet à Cloud Manager de gérer les ressources et les processus au sein de votre environnement de cloud public. Il s'exécute sur une instance de machine virtuelle que vous déployez dans votre fournisseur cloud ou sur un hôte sur site que vous avez configuré.

Vous pouvez utiliser un connecteur avec plusieurs services de données cloud NetApp. Par exemple, si vous avez déjà un connecteur pour Cloud Manager, vous pouvez le sélectionner lors de la configuration du service Cloud Tiering.

Abonnements

Le widget Paramètres du compte affiche les abonnements NetApp associés au compte sélectionné.

Lorsque vous vous abonnez à Cloud Manager sur le marché d'un fournisseur cloud, vous êtes redirigé vers Cloud Central où vous devez enregistrer votre abonnement et l'associer à des comptes spécifiques.

Après votre inscription, chaque abonnement est disponible dans le widget Paramètres du compte. Vous ne verrez que les abonnements associés au compte que vous consultez actuellement.

Vous avez la possibilité de renommer un abonnement et de dissocier l'abonnement d'un ou plusieurs comptes.

Par exemple, disons que vous avez deux comptes et que chacun est facturé par le biais d'abonnements distincts. Vous pouvez dissocier un abonnement de l'un des comptes afin que les utilisateurs de ce compte ne choisissent pas accidentellement l'abonnement incorrect lors de la création d'un environnement de travail Cloud Volume ONTAP.

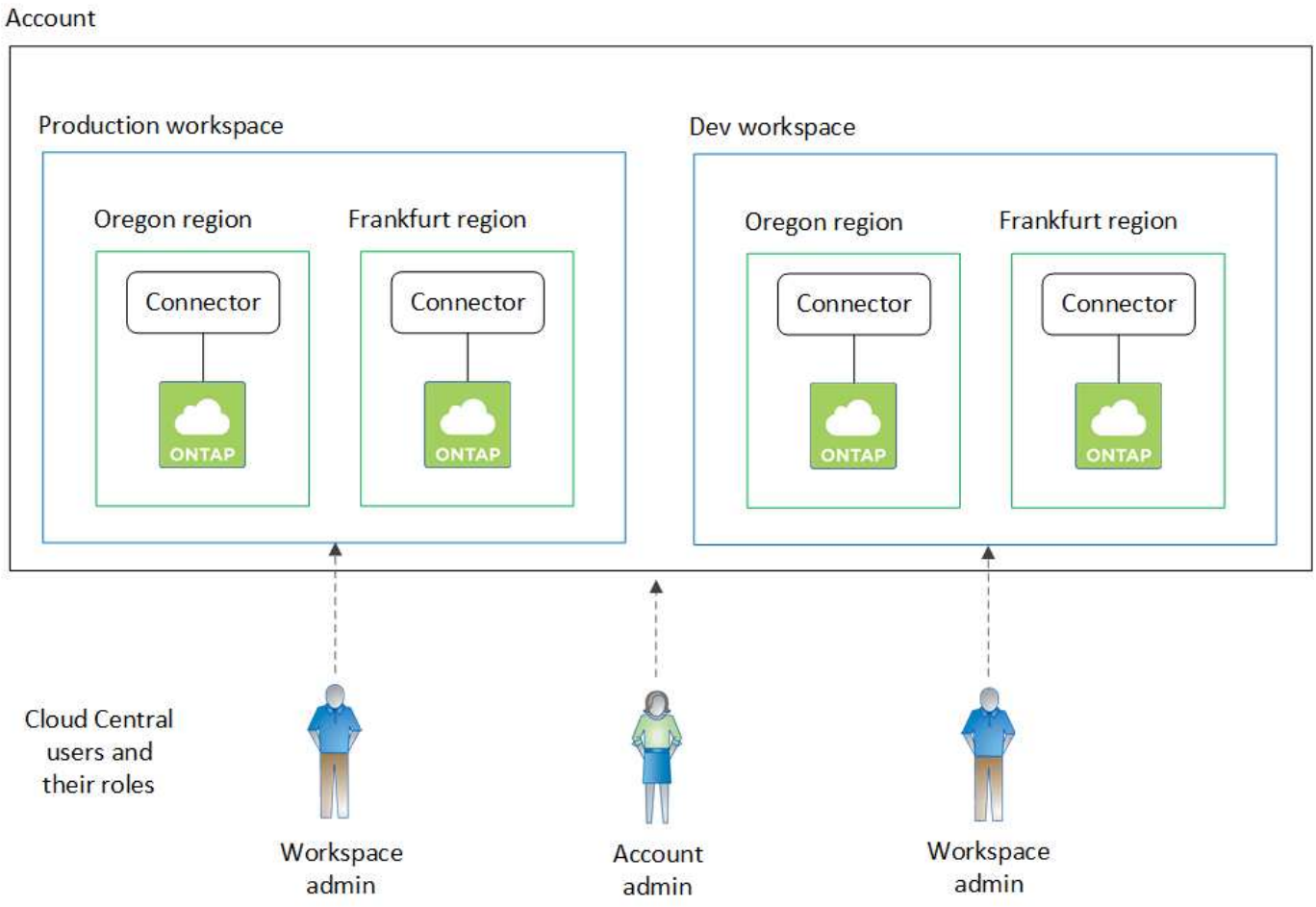
Exemples

Les exemples suivants décrivent comment configurer vos comptes.

> Dans les deux exemples d'images ci-dessous, le connecteur et les systèmes Cloud Volumes ONTAP ne résident pas *dans* le compte NetApp Cloud Central—ils s'exécutent dans un fournisseur cloud. Il s'agit d'une représentation conceptuelle de la relation entre chaque composant.

Exemple 1

L'exemple suivant montre un compte qui utilise deux espaces de travail pour créer des environnements isolés. Le premier espace de travail est pour un environnement de production et le second pour un environnement de développement.

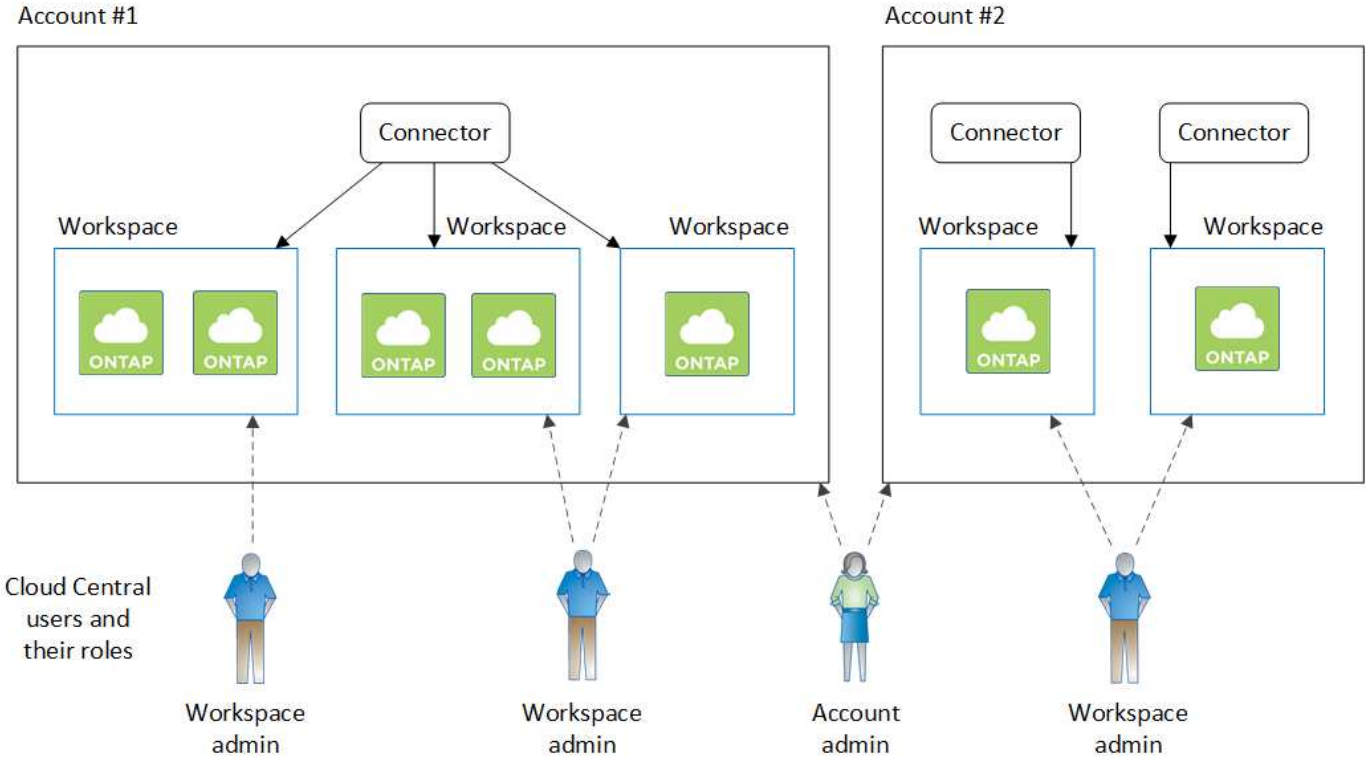


Exemple 2

Voici un autre exemple illustrant le niveau de colocation le plus élevé en utilisant deux comptes Cloud Central

distincts. Par exemple, un fournisseur de services peut utiliser Cloud Manager dans un compte pour fournir des services à ses clients, tout en utilisant un autre compte pour la reprise après incident de l'une de ses business units.

Notez que le compte 2 comprend deux connecteurs distincts. Cela peut arriver si vous disposez de systèmes dans des régions distinctes ou dans des fournisseurs cloud distincts.



Configuration d'espaces de travail et d'utilisateurs sur le compte Cloud Central

Lorsque vous vous connectez à Cloud Manager pour la première fois, vous êtes invité à créer un *compte NetApp Cloud Central*. Ce compte fournit la colocation et vous permet d'organiser les utilisateurs et les ressources dans des *espaces de travail* isolés.

"Découvrez comment fonctionnent les comptes Cloud Central".

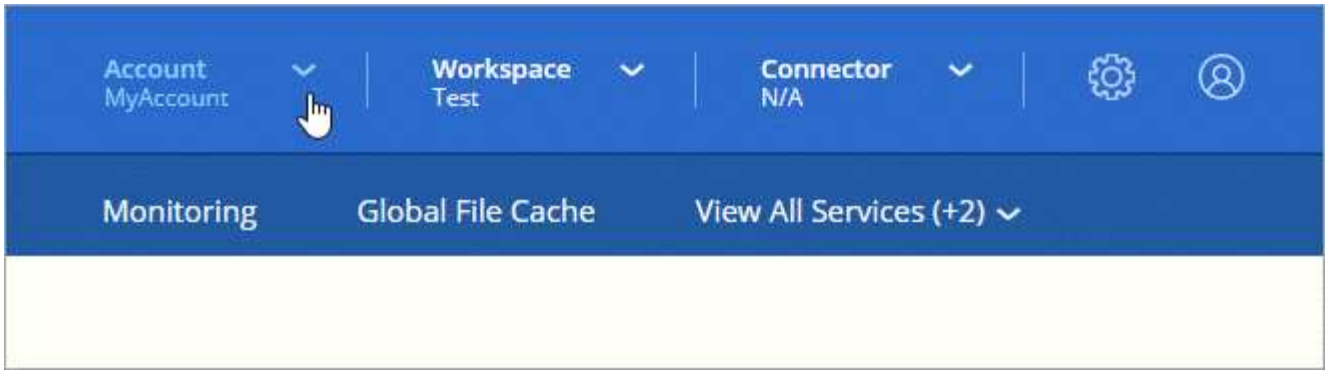
Configurez votre compte Cloud Central pour que les utilisateurs puissent accéder à Cloud Manager et aux environnements de travail dans un espace de travail. Il vous suffit d'ajouter un seul utilisateur ou plusieurs utilisateurs et espaces de travail.

Ajout d'espaces de travail

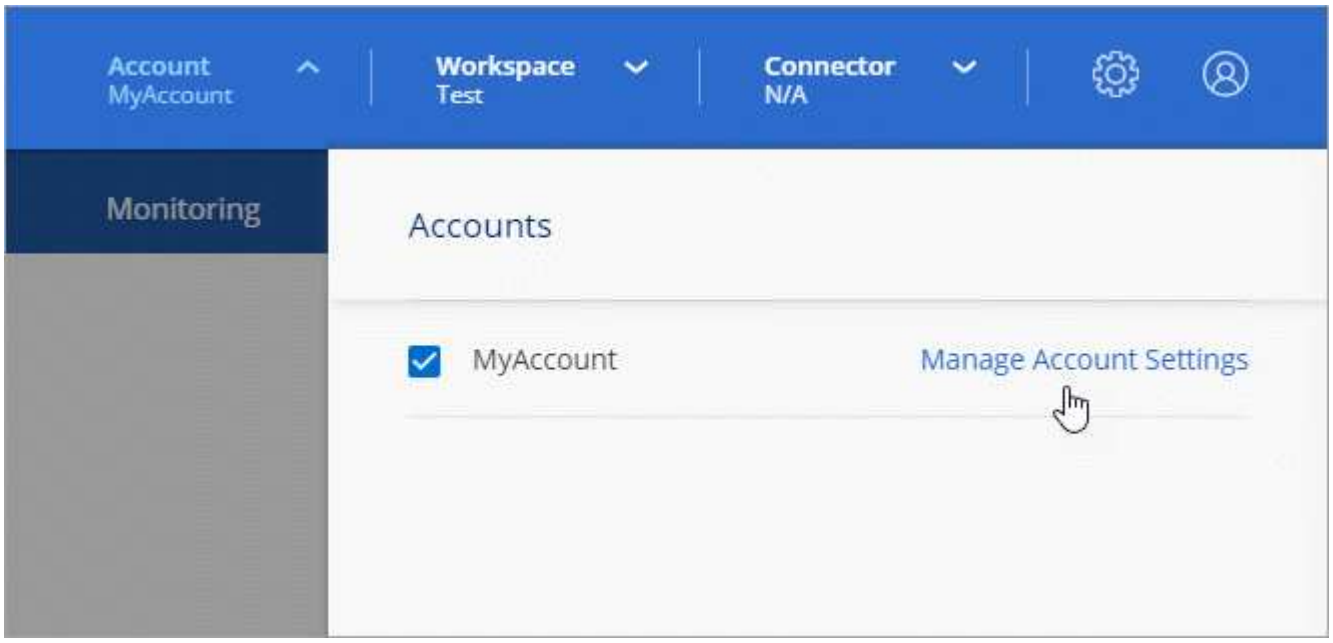
Dans Cloud Manager, les espaces de travail vous permettent d'isoler un ensemble d'environnements de travail d'autres environnements de travail et d'autres utilisateurs. Par exemple, vous pouvez créer deux espaces de travail et associer des utilisateurs distincts à chaque espace de travail.

Étapes

1. Dans la partie supérieure de Cloud Manager, cliquez sur la liste déroulante **Account**.



2. Cliquez sur **gérer le compte** en regard du compte actuellement sélectionné.



3. Cliquez sur **espaces de travail**.
4. Cliquez sur **Ajouter un nouvel espace de travail**.
5. Entrez un nom pour l'espace de travail et cliquez sur **Ajouter**.

Une fois que vous avez terminé

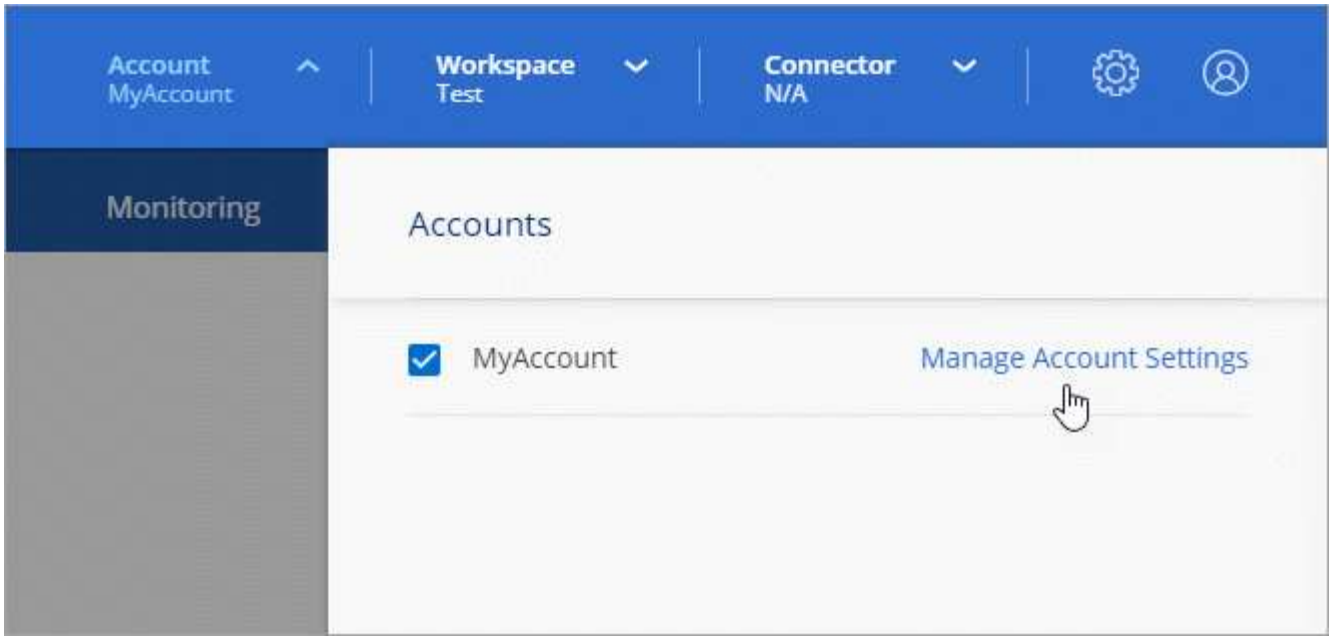
Si un administrateur d'espace de travail doit accéder à cet espace de travail, vous devez associer l'utilisateur. Vous devez également associer des connecteurs à l'espace de travail pour que les administrateurs de l'espace de travail puissent utiliser ces connecteurs.

Ajout d'utilisateurs

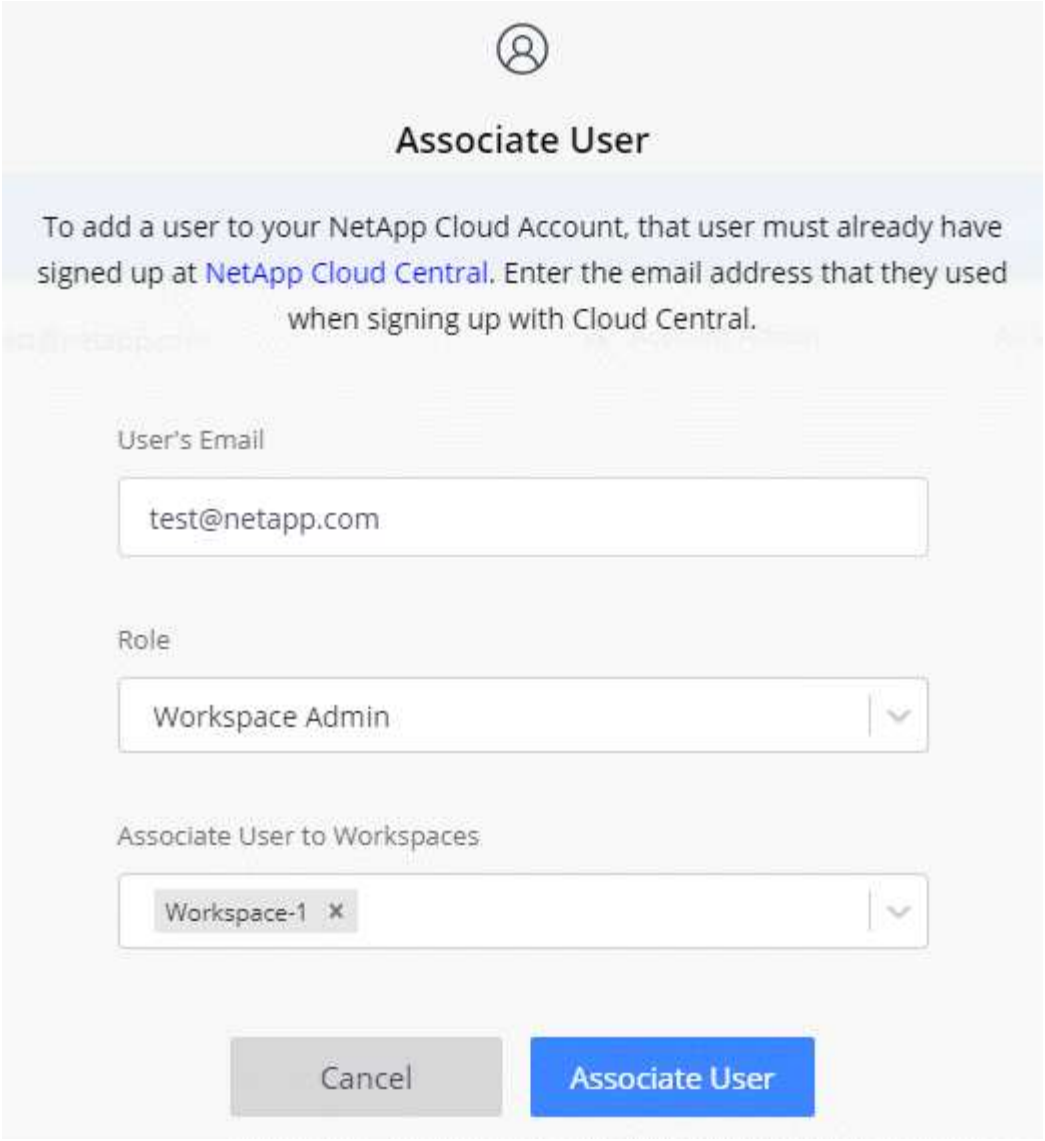
Associez les utilisateurs de Cloud Central au compte Cloud Central pour qu'ils puissent créer et gérer des environnements de travail dans Cloud Manager.

Étapes

1. Si l'utilisateur ne l'a pas déjà fait, demandez-lui d'aller à "NetApp Cloud Central" et s'inscrire.
2. En haut de Cloud Manager, cliquez sur la liste déroulante **compte** et cliquez sur **gérer compte**.



3. Dans l'onglet utilisateurs, cliquez sur **associer utilisateur**.
4. Entrez l'adresse e-mail de l'utilisateur et sélectionnez un rôle pour l'utilisateur :
   - **Administrateur de compte** : peut effectuer n'importe quelle action dans Cloud Manager.
   - **Workspace Admin** : permet de créer et de gérer des ressources dans des espaces de travail attribués.
   - **Compliance Viewer** : peut uniquement afficher les informations de conformité et générer des rapports pour les espaces de travail auxquels ils ont la permission d'accéder.
5. Si vous avez sélectionné Workspace Admin ou Compliance Viewer, sélectionnez un ou plusieurs espaces de travail à associer à cet utilisateur.



6. Cliquez sur **associer utilisateur**.

Résultat

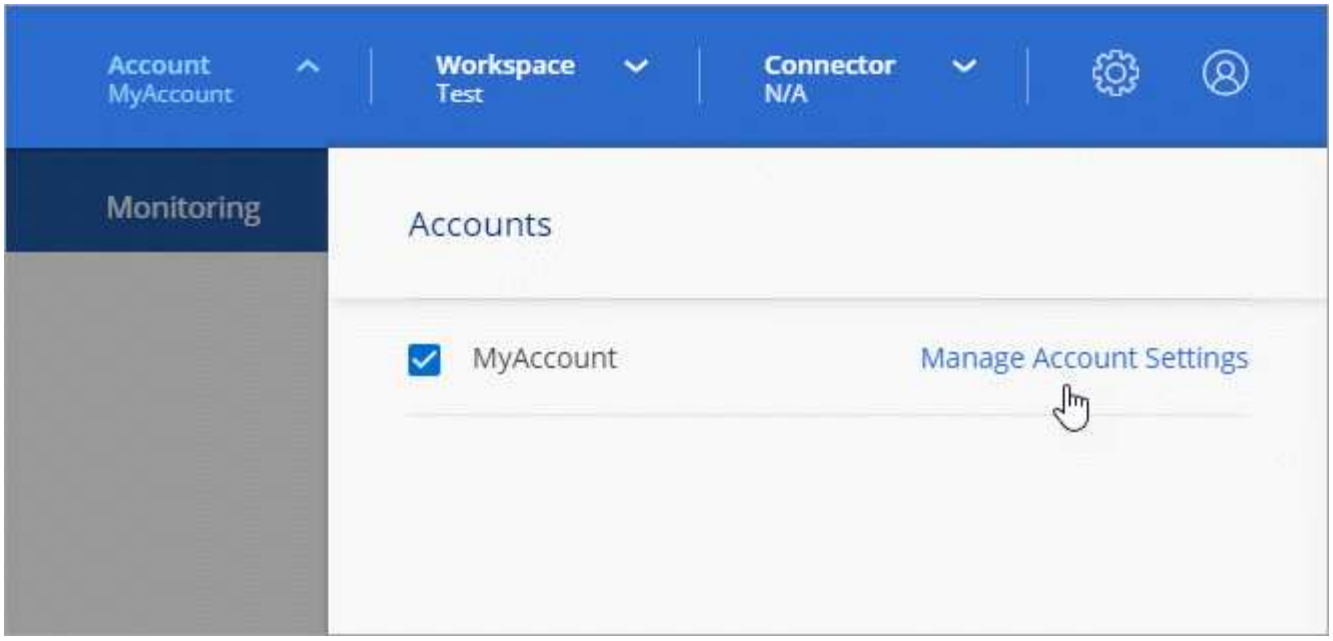
L'utilisateur doit recevoir un e-mail de la part de NetApp Cloud Central intitulé « Account Association ». Il contient les informations nécessaires pour accéder à Cloud Manager.

Association des administrateurs d'espace de travail aux espaces de travail

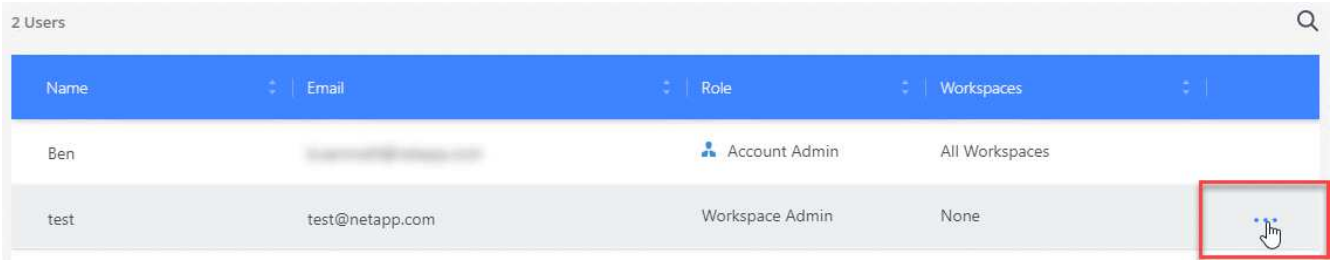
Vous pouvez associer des administrateurs d'espace de travail à des espaces de travail supplémentaires à tout moment. L'association de l'utilisateur lui permet de créer et d'afficher les environnements de travail dans cet espace de travail.

Étapes

1. En haut de Cloud Manager, cliquez sur la liste déroulante **compte** et cliquez sur **gérer compte**.



2. Dans l'onglet utilisateurs, cliquez sur le menu d'action de la ligne correspondant à l'utilisateur.



3. Cliquez sur **gérer les espaces de travail**.
4. Sélectionnez un ou plusieurs espaces de travail et cliquez sur **appliquer**.

Résultat

L'utilisateur peut désormais accéder à ces espaces de travail à partir de Cloud Manager, tant que le connecteur était également associé aux espaces de travail.

Association de connecteurs aux espaces de travail

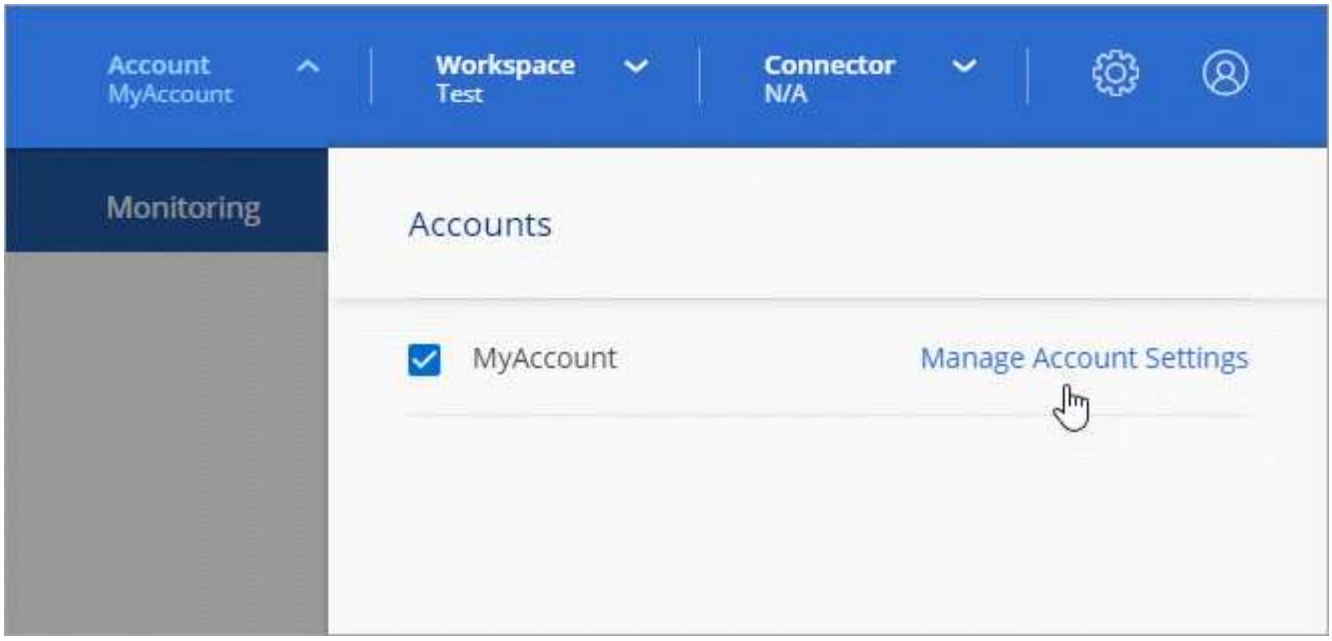
Vous devez associer un connecteur aux espaces de travail pour que les administrateurs d'espace de travail puissent utiliser ces connecteurs pour créer des systèmes Cloud Volumes ONTAP.

Si vous ne disposez que d'administrateurs de compte, il n'est pas nécessaire d'associer le connecteur aux espaces de travail. Ils peuvent accéder par défaut à tous les espaces de travail dans Cloud Manager.

"En savoir plus sur les utilisateurs, les espaces de travail et les connecteurs".

Étapes

1. En haut de Cloud Manager, cliquez sur la liste déroulante **compte** et cliquez sur **gérer compte**.



2. Cliquez sur **connecteur**.
3. Cliquez sur **gérer les espaces de travail** pour le connecteur que vous souhaitez associer.
4. Sélectionnez un ou plusieurs espaces de travail et cliquez sur **appliquer**.

Résultat

Les administrateurs d'espace de travail peuvent désormais utiliser ces connecteurs pour créer des systèmes Cloud Volumes ONTAP.

Et la suite ?

Maintenant que vous avez configuré votre compte, vous pouvez le gérer à tout moment en supprimant des utilisateurs, en gérant des espaces de travail, des connecteurs et des abonnements. "En savoir plus >>".

Configurer un connecteur

En savoir plus sur les connecteurs

Dans la plupart des cas, un administrateur de compte devra déployer un *Connector* dans votre réseau cloud ou sur site. Ce connecteur permet à Cloud Manager de gérer les ressources et les processus au sein de votre environnement de cloud public.

Lorsqu'un connecteur est nécessaire

Un connecteur est nécessaire pour utiliser l'une des fonctionnalités suivantes dans Cloud Manager :

- Cloud Volumes ONTAP
- Clusters ONTAP sur site
- Conformité cloud
- Kubernetes
- Sauvegarde dans le cloud

- Contrôle
- Tiering sur site
- Cache global de fichiers
- Découverte des compartiments Amazon S3

Un connecteur est ***NOT*** requis pour Azure NetApp Files, Cloud Volumes Service ou Cloud Sync.

Même si aucun connecteur n'est nécessaire pour configurer et gérer Azure NetApp Files, un connecteur est nécessaire si vous souhaitez utiliser Cloud Compliance pour analyser les données Azure NetApp Files.

Emplacements pris en charge

Un connecteur est pris en charge aux emplacements suivants :

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- Sur site

Pour créer un système Cloud Volumes ONTAP dans Google Cloud, vous devez également disposer d'un connecteur exécuté dans Google Cloud. Vous ne pouvez pas utiliser un connecteur qui fonctionne à un autre emplacement.

Les connecteurs doivent rester en fonctionnement

Un connecteur doit rester en fonctionnement en permanence. Il est important pour la santé et le fonctionnement continus des services que vous proposez.

Par exemple, un connecteur est un composant clé de la santé et du fonctionnement des systèmes Cloud Volumes ONTAP PAYGO. Si un connecteur est hors tension, les systèmes Cloud Volumes ONTAP PAYGO s'arrêtent après une perte de communication avec un connecteur pendant plus de 14 jours.

Comment créer un connecteur

Un administrateur de compte doit créer un connecteur avant qu'un administrateur d'espace de travail puisse créer un environnement de travail Cloud Volumes ONTAP et utiliser les autres fonctionnalités répertoriées ci-dessus.

Un administrateur de compte peut créer un connecteur de différentes façons :

- Directement dans Cloud Manager (recommandé)
  - "Création dans AWS"
  - "Création dans Azure"
  - "Création dans GCP"
- "Depuis AWS Marketplace"
- "À partir d'Azure Marketplace"
- "En téléchargeant et installant le logiciel sur un hôte Linux existant"

Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l'avez pas encore créé.

Autorisations

Des autorisations spécifiques sont nécessaires pour créer le connecteur et un autre ensemble d'autorisations est nécessaire pour l'instance de connecteur elle-même.

Autorisations pour créer un connecteur

L'utilisateur qui crée un connecteur depuis Cloud Manager a besoin de permissions spécifiques pour déployer l'instance dans votre fournisseur de cloud de votre choix. Cloud Manager vous rappelle les exigences d'autorisation lorsque vous créez un connecteur.

"Affichez les règles de chaque fournisseur cloud".

Autorisations pour l'instance de connecteur

Le connecteur nécessite des autorisations spécifiques de fournisseurs cloud pour effectuer des opérations en votre nom. Par exemple, pour déployer et gérer Cloud Volumes ONTAP.

Lorsque vous créez un connecteur directement depuis Cloud Manager, Cloud Manager crée le connecteur avec les autorisations dont il a besoin. Vous n'avez rien à faire.

Si vous créez vous-même le connecteur à partir d'AWS Marketplace, d'Azure Marketplace ou d'une installation manuelle du logiciel, vous devez vous assurer que les autorisations appropriées sont en place.

"Affichez les règles de chaque fournisseur cloud".

Quand utiliser plusieurs connecteurs

Dans certains cas, vous n'avez peut-être besoin que d'un seul connecteur, mais vous pourriez avoir besoin de deux connecteurs ou plus.

Voici quelques exemples :

- Vous utilisez un environnement multicloud (AWS et Azure), c'est pourquoi vous avez un connecteur dans AWS et un autre dans Azure. Chacun gère les systèmes Cloud Volumes ONTAP exécutés dans ces environnements.
- Un fournisseur de services peut utiliser un seul compte Cloud Central pour fournir des services à ses clients, tout en utilisant un autre compte pour assurer la reprise après incident de l'une de ses business units. Chaque compte aurait des connecteurs distincts.

Quand passer d'un connecteur à un autre

Lorsque vous créez votre premier connecteur, Cloud Manager utilise automatiquement ce connecteur pour chaque environnement de travail supplémentaire que vous créez. Une fois que vous avez créé un connecteur supplémentaire, vous devrez passer de l'un à l'autre pour voir les environnements de travail spécifiques à chaque connecteur.

"Apprenez à passer d'un connecteur à un autre".

Interface utilisateur locale

Pendant que vous devriez effectuer presque toutes les tâches à partir du "Interface utilisateur SaaS", Une interface utilisateur locale est toujours disponible sur le connecteur. Cette interface est nécessaire pour quelques tâches qui doivent être effectuées à partir du connecteur lui-même :

- "Configuration d'un serveur proxy"
- Installation d'un correctif (en général, vous travaillerez avec le personnel NetApp pour installer un correctif)
- Téléchargement de messages AutoSupport (généralement dirigés par le personnel NetApp en cas de problème)

"Découvrez comment accéder à l'interface utilisateur locale".

Mises à niveau des connecteurs

Le connecteur met automatiquement à jour son logiciel à la dernière version, tant qu'il l'a fait "accès internet sortant" pour obtenir la mise à jour logicielle.

Exigences de mise en réseau pour le connecteur

Configurez votre réseau de sorte que le connecteur puisse gérer les ressources et les processus au sein de votre environnement de cloud public. L'étape la plus importante consiste à garantir l'accès Internet sortant à différents terminaux.

Si votre réseau utilise un serveur proxy pour toutes les communications vers Internet, vous pouvez spécifier le serveur proxy à partir de la page Paramètres. Reportez-vous à la section "Configuration du connecteur pour utiliser un serveur proxy".

Connexion aux réseaux cibles

Un connecteur nécessite une connexion réseau au type d'environnement de travail que vous créez et aux services que vous prévoyez d'activer.

Par exemple, si vous installez un connecteur sur le réseau de votre entreprise, vous devez configurer une connexion VPN sur le VPC ou le vnet dans lequel vous lancez Cloud Volumes ONTAP.

Accès Internet sortant

Le connecteur nécessite un accès Internet sortant pour gérer les ressources et les processus au sein de votre environnement de cloud public. L'accès Internet sortant est également requis si vous souhaitez installer manuellement le connecteur sur un hôte Linux ou accéder à l'interface utilisateur locale exécutée sur le connecteur.

Les sections suivantes identifient les terminaux spécifiques.

Terminaux pour gérer les ressources dans AWS

Lors de la gestion des ressources dans AWS, un connecteur contacte les terminaux suivants :

Terminaux	Objectif
Services AWS (amazonaws.com): • CloudFormation • Cloud de calcul élastique (EC2) • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Service de stockage simple (S3) Le noeud final exact dépend de la région dans laquelle vous déployez Cloud Volumes ONTAP. "Reportez-vous à la documentation AWS pour plus de détails."	Permet à Connector de déployer et de gérer Cloud Volumes ONTAP dans AWS.
https://api.services.cloud.netapp.com:443	Demandes d'API à NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Permet d'accéder aux images logicielles, aux manifestes et aux modèles.
https://repo.cloud.support.netapp.com	Permet de télécharger les dépendances de Cloud Manager.
http://repo.mysql.com/	Utilisé pour télécharger MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Permet au connecteur d'accéder aux manifestes, aux modèles et aux images de mise à niveau Cloud Volumes ONTAP et de les télécharger.
https://cloudmanagerinfraprod.azurecr.io	Accédez aux images logicielles des composants de conteneur pour une infrastructure exécutant Docker et fournie une solution pour les intégrations des services avec Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.
https://cloudmanager.cloud.netapp.com	Communication avec le service Cloud Manager, notamment les comptes Cloud Central.
https://netapp-cloud-account.auth0.com	Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs.
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Permet d'ajouter votre ID de compte AWS à la liste des utilisateurs autorisés pour Backup vers S3.
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Communication avec NetApp AutoSupport.

Terminaux	Objectif
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Communication avec NetApp pour les licences système et l'inscription au support.
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Il permet à NetApp de collecter les informations nécessaires à la résolution des problèmes.
https://ipa-signer.cloudmanager.netapp.com	Génération des licences par Cloud Manager (par exemple, une licence FlexCache pour Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Nécessaire pour connecter des systèmes Cloud Volumes ONTAP avec un cluster Kubernetes. Les terminaux permettent l'installation de NetApp Trident.
Divers sites tiers, par exemple : • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Les emplacements tiers sont sujets à modification.	Lors des mises à niveau, Cloud Manager télécharge les derniers packages pour les dépendances tierces.

Terminaux pour gérer les ressources dans Azure

Lors de la gestion des ressources dans Azure, un connecteur contacte les terminaux suivants :

Terminaux	Objectif
https://management.azure.com https://login.microsoftonline.com	Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans la plupart des régions d'Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans les régions d'Azure Allemagne.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans les régions d'Azure US Gov.
https://api.services.cloud.netapp.com:443	Demandes d'API à NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Permet d'accéder aux images logicielles, aux manifestes et aux modèles.
https://repo.cloud.support.netapp.com	Permet de télécharger les dépendances de Cloud Manager.
http://repo.mysql.com/	Utilisé pour télécharger MySQL.

Terminaux	Objectif
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Permet au connecteur d'accéder aux manifestes, aux modèles et aux images de mise à niveau Cloud Volumes ONTAP et de les télécharger.
https://cloudmanagerinfraprod.azurecr.io	Accédez aux images logicielles des composants de conteneur pour une infrastructure exécutant Docker et fournie une solution pour les intégrations des services avec Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.
https://cloudmanager.cloud.netapp.com	Communication avec le service Cloud Manager, notamment les comptes Cloud Central.
https://netapp-cloud-account.auth0.com	Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs.
https://mysupport.netapp.com	Communication avec NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Communication avec NetApp pour les licences système et l'inscription au support.
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Il permet à NetApp de collecter les informations nécessaires à la résolution des problèmes.
https://ipa-signer.cloudmanager.netapp.com	Génération des licences par Cloud Manager (par exemple, une licence FlexCache pour Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Nécessaire pour connecter des systèmes Cloud Volumes ONTAP avec un cluster Kubernetes. Les terminaux permettent l'installation de NetApp Trident.
*.blob.core.windows.net	Requis pour les paires haute disponibilité lors de l'utilisation d'un proxy.

Terminaux	Objectif
Divers sites tiers, par exemple : • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Les emplacements tiers sont sujets à modification.	Lors des mises à niveau, Cloud Manager télécharge les derniers packages pour les dépendances tierces.

Des terminaux pour gérer les ressources dans GCP

Lors de la gestion des ressources dans GCP, un connecteur contacte les terminaux suivants :

Terminaux	Objectif
https://www.googleapis.com	Permet au connecteur de contacter les API Google pour le déploiement et la gestion de Cloud Volumes ONTAP dans GCP.
https://api.services.cloud.netapp.com:443	Demandes d'API à NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Permet d'accéder aux images logicielles, aux manifestes et aux modèles.
https://repo.cloud.support.netapp.com	Permet de télécharger les dépendances de Cloud Manager.
http://repo.mysql.com/	Utilisé pour télécharger MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Permet au connecteur d'accéder aux manifestes, aux modèles et aux images de mise à niveau Cloud Volumes ONTAP et de les télécharger.
https://cloudmanagerinfraprod.azurecr.io	Accédez aux images logicielles des composants de conteneur pour une infrastructure exécutant Docker et fournie une solution pour les intégrations des services avec Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.
https://cloudmanager.cloud.netapp.com	Communication avec le service Cloud Manager, notamment les comptes Cloud Central.
https://netapp-cloud-account.auth0.com	Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs.
https://mysupport.netapp.com	Communication avec NetApp AutoSupport.

Terminaux	Objectif
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Communication avec NetApp pour les licences système et l'inscription au support.
https://client.infra.support.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.us-west-1.amazonaws.com https://trigger.asup.netapp.com.s3.us-west-1.amazonaws.com	Il permet à NetApp de collecter les informations nécessaires à la résolution des problèmes.
https://ipa-signer.cloudmanager.netapp.com	Génération des licences par Cloud Manager (par exemple, une licence FlexCache pour Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Nécessaire pour connecter des systèmes Cloud Volumes ONTAP avec un cluster Kubernetes. Les terminaux permettent l'installation de NetApp Trident.
Divers sites tiers, par exemple : • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.com Les emplacements tiers sont sujets à modification.	Lors des mises à niveau, Cloud Manager télécharge les derniers packages pour les dépendances tierces.

Noeuds finaux pour installer le connecteur sur un hôte Linux

Vous avez la possibilité d'installer manuellement le logiciel Connector sur votre propre hôte Linux. Dans ce cas, le programme d'installation du connecteur doit accéder aux URL suivantes pendant le processus d'installation :

- http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
- https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
- https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

L'hôte peut essayer de mettre à jour les packages du système d'exploitation lors de l'installation. L'hôte peut contacter différents sites de mise en miroir pour ces packages OS.

Les terminaux accessibles à partir de votre navigateur Web lors de l'utilisation de l'interface utilisateur locale

Bien que vous devriez effectuer presque toutes les tâches à partir de l'interface utilisateur SaaS, une interface utilisateur locale est toujours disponible sur le connecteur. La machine exécutant le navigateur Web doit disposer de connexions aux terminaux suivants :

Terminaux	Objectif
L'hôte du connecteur	Vous devez entrer l'adresse IP de l'hôte depuis un navigateur Web pour charger la console Cloud Manager. En fonction de votre connectivité avec votre fournisseur de cloud, vous pouvez utiliser l'IP privée ou une adresse IP publique attribuée à l'hôte : • Une adresse IP privée fonctionne si vous disposez d'un VPN et d'un accès direct à votre réseau virtuel • Un IP public fonctionne dans tous les scénarios de mise en réseau Dans tous les cas, vous devez sécuriser l'accès au réseau en vous assurant que les règles du groupe de sécurité autorisent l'accès à partir des adresses IP ou des sous-réseaux autorisés uniquement.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Votre navigateur Web se connecte à ces terminaux pour une authentification centralisée des utilisateurs via NetApp Cloud Central.
https://widget.intercom.io	Vous bénéficiez d'un chat en ligne pour discuter avec des experts du cloud NetApp.

Ports et groupes de sécurité

Il n'y a pas de trafic entrant vers le connecteur, sauf si vous le lancez. HTTP et HTTPS permettent l'accès au "Interface utilisateur locale", que vous utiliserez dans de rares circonstances. SSH n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

Règles pour le connecteur dans AWS

Le groupe de sécurité du connecteur nécessite à la fois des règles entrantes et sortantes.

Règles entrantes

La source des règles entrantes dans le groupe de sécurité prédéfini est 0.0.0.0/0.

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP depuis les navigateurs Web du client vers l'interface utilisateur locale et les connexions à partir de Cloud Compliance
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale
TCP	3128	Fournit l'instance Cloud Compliance avec un accès Internet si votre réseau AWS n'utilise pas de NAT ou de proxy

Règles de sortie

Le groupe de sécurité prédéfini pour le connecteur ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour le connecteur inclut les règles de trafic sortant suivantes.

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles UDP	Tout	Tout le trafic sortant

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par le connecteur.

L'adresse IP source est l'hôte du connecteur.

Service	Protocole	Port	Destination	Objectif
Active Directory	TCP	88	Forêt Active Directory	Authentification Kerberos V.
	TCP	139	Forêt Active Directory	Session de service NetBIOS
	TCP	389	Forêt Active Directory	LDAP
	TCP	445	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	TCP	749	Forêt Active Directory	Modification et définition du mot de passe de Kerberos V Active Directory (RPCSEC_GSS)
	UDP	137	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	Forêt Active Directory	Service de datagrammes NetBIOS
	UDP	464	Forêt Active Directory	Administration des clés Kerberos
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	API appelle AWS et ONTAP et envoie des messages AutoSupport à NetApp
Appels API	TCP	3000	LIF de gestion de cluster ONTAP	Appels API vers ONTAP
	TCP	8088	Sauvegarde vers S3	Appels d'API vers Backup vers S3
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par Cloud Manager
Conformité cloud	HTTP	80	Instance Cloud Compliance	Cloud Compliance pour Cloud Volumes ONTAP

Règles pour le connecteur dans Azure

Le groupe de sécurité du connecteur nécessite à la fois des règles entrantes et sortantes.

Règles entrantes

La source des règles entrantes dans le groupe de sécurité prédéfini est 0.0.0.0/0.

Port	Protocole	Objectif
22	SSH	Fournit un accès SSH à l'hôte du connecteur
80	HTTP	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale
443	HTTPS	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale

Règles de sortie

Le groupe de sécurité prédéfini pour le connecteur ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour le connecteur inclut les règles de trafic sortant suivantes.

Port	Protocole	Objectif
Tout	Tous les protocoles TCP	Tout le trafic sortant
Tout	Tous les protocoles UDP	Tout le trafic sortant

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par le connecteur.

L'adresse IP source est l'hôte du connecteur.

Service	Port	Protocole	Destination	Objectif
Active Directory	88	TCP	Forêt Active Directory	Authentification Kerberos V.
	139	TCP	Forêt Active Directory	Session de service NetBIOS
	389	TCP	Forêt Active Directory	LDAP
	445	TCP	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	464	TCP	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	749	TCP	Forêt Active Directory	Modification et définition du mot de passe de Kerberos V Active Directory (RPCSEC_GSS)
	137	UDP	Forêt Active Directory	Service de noms NetBIOS
	138	UDP	Forêt Active Directory	Service de datagrammes NetBIOS
	464	UDP	Forêt Active Directory	Administration des clés Kerberos
Appels API et AutoSupport	443	HTTPS	LIF de gestion de cluster ONTAP et Internet sortant	API appelle AWS et ONTAP et envoie des messages AutoSupport à NetApp
Appels API	3000	TCP	LIF de gestion de cluster ONTAP	Appels API vers ONTAP
DNS	53	UDP	DNS	Utilisé pour la résolution DNS par Cloud Manager

Règles pour le connecteur dans GCP

Les règles de pare-feu du connecteur exigent à la fois des règles entrantes et sortantes.

Règles entrantes

La source des règles entrantes dans les règles de pare-feu prédéfinies est 0.0.0.0/0.

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale

Règles de sortie

Les règles de pare-feu prédéfinies pour le connecteur ouvrent tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

Les règles de pare-feu prédéfinies pour le connecteur comprennent les règles de trafic sortant suivantes.

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles UDP	Tout	Tout le trafic sortant

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par le connecteur.

L'adresse IP source est l'hôte du connecteur.

Service	Protocole	Port	Destination	Objectif
Active Directory	TCP	88	Forêt Active Directory	Authentification Kerberos V.
	TCP	139	Forêt Active Directory	Session de service NetBIOS
	TCP	389	Forêt Active Directory	LDAP
	TCP	445	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	TCP	749	Forêt Active Directory	Modification et définition du mot de passe de Kerberos V Active Directory (RPCSEC_GSS)
	UDP	137	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	Forêt Active Directory	Service de datagrammes NetBIOS
	UDP	464	Forêt Active Directory	Administration des clés Kerberos
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	Par des appels d'API à GCP et à ONTAP, et par l'envoi de messages AutoSupport à NetApp
Appels API	TCP	3000	LIF de gestion de cluster ONTAP	Appels API vers ONTAP
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par Cloud Manager

Création d'un connecteur dans AWS à partir de Cloud Manager

Un administrateur de compte doit déployer un *Connector* avant de pouvoir utiliser la plupart des fonctionnalités de Cloud Manager. "Apprenez quand un connecteur est nécessaire". Ce connecteur permet à Cloud Manager de gérer les ressources et les processus au sein de votre environnement de cloud public.

Cette page explique comment créer un connecteur dans AWS directement depuis Cloud Manager. Vous avez également la possibilité de "Créez le connecteur à partir d'AWS Marketplace", ou à "téléchargez le logiciel et installez-le sur votre propre hôte".

Ces étapes doivent être réalisées par un utilisateur qui a le rôle d'administrateur de compte. Un administrateur d'espace de travail ne peut pas créer de connecteur.

Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l'avez pas encore créé.

Configuration des autorisations AWS pour créer un connecteur

Avant de déployer un connecteur depuis Cloud Manager, vous devez vous assurer que votre compte AWS dispose des autorisations appropriées.

Étapes

1. Téléchargez la politique IAM des connecteurs à l'emplacement suivant :

   "NetApp Cloud Manager : règles AWS, Azure et GCP"

2. Dans la console IAM AWS, créez votre propre règle en copiant et collant le texte de la politique IAM du connecteur.
3. Associez la règle que vous avez créée à l'étape précédente à l'utilisateur IAM qui crée le connecteur à partir de Cloud Manager.

Résultat

L'utilisateur AWS dispose désormais des autorisations nécessaires pour créer le connecteur à partir de Cloud Manager. Vous devez spécifier les clés d'accès AWS pour cet utilisateur lorsque vous y êtes invité par Cloud Manager.

Création d'un connecteur dans AWS

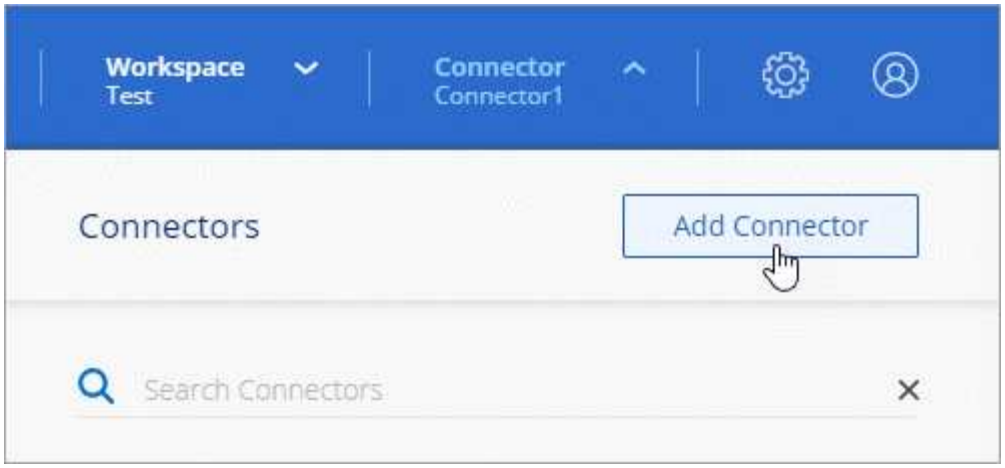
Avec Cloud Manager, vous pouvez créer un connecteur dans AWS directement depuis son interface utilisateur.

Ce dont vous avez besoin

- Une clé d'accès AWS et une clé secrète pour un utilisateur IAM qui dispose de la "autorisations requises".
- Un VPC, un sous-réseau et un keyair dans votre région AWS de votre choix.

Étapes

1. Si vous créez votre premier environnement de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites. Sinon, cliquez sur la liste déroulante **Connector** et sélectionnez **Add Connector**.



2. Cliquez sur **commençons**.
3. Choisissez **Amazon Web Services** comme fournisseur de cloud.

   Rappelez-vous que le connecteur doit disposer d'une connexion réseau au type d'environnement de travail que vous créez et aux services que vous prévoyez d'activer.

   "En savoir plus sur les exigences de mise en réseau pour le connecteur".

4. Passez en revue ce dont vous aurez besoin et cliquez sur **Continuer**.
5. Fournissez les informations requises :
   - **Informations d'identification AWS** : saisissez un nom pour l'instance et spécifiez la clé d'accès AWS et la clé secrète qui répondent aux exigences d'autorisation.
   - **Location** : spécifiez une région AWS, un VPC et un sous-réseau pour l'instance.
   - **Réseau** : sélectionnez la paire de clés à utiliser avec l'instance, si vous souhaitez activer une adresse IP publique et spécifiez éventuellement une configuration proxy.
   - **Groupe de sécurité** : choisissez de créer ou non un nouveau groupe de sécurité ou de sélectionner un groupe de sécurité existant qui autorise l'accès HTTP, HTTPS et SSH entrant.

     Il n'y a pas de trafic entrant vers le connecteur, sauf si vous le lancez. HTTP et HTTPS permettent l'accès au "Interface utilisateur locale", que vous utiliserez dans de rares circonstances. SSH n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

6. Cliquez sur **Créer**.

   L'instance doit être prête dans environ 7 minutes. Vous devez rester sur la page jusqu'à ce que le processus soit terminé.

Une fois que vous avez terminé

Vous devez associer un connecteur aux espaces de travail pour que les administrateurs d'espace de travail puissent utiliser ces connecteurs pour créer des systèmes Cloud Volumes ONTAP. Si vous ne disposez que d'administrateurs de compte, il n'est pas nécessaire d'associer le connecteur aux espaces de travail. Ils peuvent accéder par défaut à tous les espaces de travail dans Cloud Manager. "En savoir plus >>".

Création d'un connecteur dans Azure à partir de Cloud Manager

Un administrateur de compte doit déployer un *Connector* avant de pouvoir utiliser la plupart des fonctionnalités de Cloud Manager. "Apprenez quand un connecteur est nécessaire". Ce connecteur permet à Cloud Manager de gérer les ressources et les processus au sein de votre environnement de cloud public.

Cette page explique comment créer un connecteur dans Azure directement depuis Cloud Manager. Vous avez également la possibilité de "Créez le connecteur à partir d'Azure Marketplace", ou à "téléchargez le logiciel et installez-le sur votre propre hôte".

Ces étapes doivent être réalisées par un utilisateur qui a le rôle d'administrateur de compte. Un administrateur d'espace de travail ne peut pas créer de connecteur.

Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l'avez pas encore créé.

Configuration des autorisations Azure pour créer un connecteur

Avant de déployer un connecteur depuis Cloud Manager, vous devez vous assurer que votre compte Azure dispose des autorisations appropriées.

Étapes

1. Créer un rôle personnalisé à l'aide de la politique Azure pour le connecteur :

   a. Téléchargez le "Règle Azure pour le connecteur".

      Cliquez avec le bouton droit de la souris sur le lien et cliquez sur **Enregistrer le lien sous…** pour télécharger le fichier.

   b. Modifiez le fichier JSON en ajoutant votre ID d'abonnement Azure à la portée attribuable.

      Exemple

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

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

      L'exemple suivant montre comment créer un rôle personnalisé à l'aide de l'interface de ligne de commande Azure CLI 2.0 :

      ```
      az role definition create --role-definition
      C:\Policy_for_Setup_As_Service_Azure.json
      ```

   Vous devez maintenant avoir un rôle personnalisé appelé *Azure SetupAsService*.

2. Attribuez le rôle à l'utilisateur qui déploiera le connecteur à partir de Cloud Manager :

   a. Ouvrez le service **abonnements** et sélectionnez l'abonnement de l'utilisateur.

b. Cliquez sur **contrôle d'accès (IAM)**.

c. Cliquez sur **Ajouter** > **Ajouter une affectation de rôle**, puis ajoutez les autorisations suivantes :

- Sélectionnez le rôle **Azure SetupAsService**.

> Azure SetupAsService est le nom par défaut fourni dans "Stratégie de déploiement de Connector pour Azure". Si vous avez choisi un autre nom pour le rôle, sélectionnez-le à la place.

- Attribuez l'accès à un utilisateur, groupe ou application AD **Azure**.
- Sélectionnez le compte utilisateur.
- Cliquez sur **Enregistrer**.

Résultat

L'utilisateur Azure dispose désormais des autorisations nécessaires pour déployer le connecteur à partir de Cloud Manager.

Création d'un connecteur dans Azure

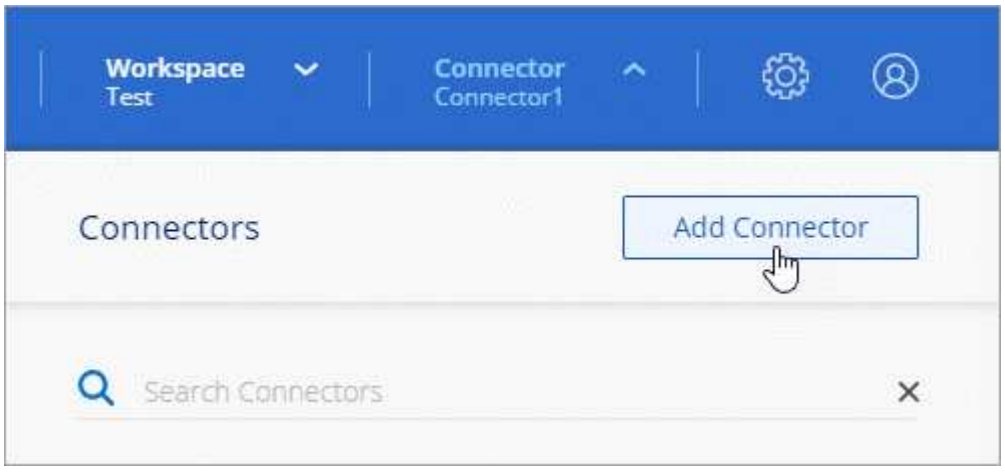
Cloud Manager vous permet de créer un connecteur dans Azure directement à partir de son interface utilisateur.

Ce dont vous avez besoin

- Le "autorisations requises" Pour votre compte Azure.
- Un abonnement Azure.
- Un vnet et un sous-réseau dans votre région Azure de votre choix.

Étapes

1. Si vous créez votre premier environnement de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites. Sinon, cliquez sur la liste déroulante **Connector** et sélectionnez **Add Connector**.



2. Cliquez sur **commençons**.
3. Choisissez **Microsoft Azure** comme fournisseur cloud.

   Rappelez-vous que le connecteur doit disposer d'une connexion réseau au type d'environnement de travail que vous créez et aux services que vous prévoyez d'activer.

"En savoir plus sur les exigences de mise en réseau pour le connecteur".

4. Passez en revue ce dont vous aurez besoin et cliquez sur **Continuer**.
5. Si vous y êtes invité, connectez-vous à votre compte Microsoft, qui devrait disposer des autorisations requises pour créer la machine virtuelle.

   Ce formulaire est détenu et hébergé par Microsoft. Vos identifiants ne sont pas fournis à NetApp.

   Si vous êtes déjà connecté à un compte Azure, Cloud Manager l'utilise automatiquement. Si vous avez plusieurs comptes, vous devrez peut-être vous déconnecter d'abord pour vous assurer que vous utilisez le bon compte.

6. Fournissez les informations requises :
   - **Authentification VM** : saisissez un nom pour la machine virtuelle ainsi qu'un nom d'utilisateur et un mot de passe ou une clé publique.
   - **Paramètres de base** : choisissez un abonnement Azure, une région Azure, et si vous souhaitez créer un nouveau groupe de ressources ou utiliser un groupe de ressources existant.
   - **Réseau** : choisissez un réseau VNet et un sous-réseau, si vous souhaitez activer une adresse IP publique, et spécifiez éventuellement une configuration proxy.
   - **Groupe de sécurité** : choisissez de créer ou non un nouveau groupe de sécurité ou de sélectionner un groupe de sécurité existant qui autorise l'accès HTTP, HTTPS et SSH entrant.

   Il n'y a pas de trafic entrant vers le connecteur, sauf si vous le lancez. HTTP et HTTPS permettent l'accès au "Interface utilisateur locale", que vous utiliserez dans de rares circonstances. SSH n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

7. Cliquez sur **Créer**.

   La machine virtuelle doit être prête en 7 minutes environ. Vous devez rester sur la page jusqu'à ce que le processus soit terminé.

Une fois que vous avez terminé

Vous devez associer un connecteur aux espaces de travail pour que les administrateurs d'espace de travail puissent utiliser ces connecteurs pour créer des systèmes Cloud Volumes ONTAP. Si vous ne disposez que d'administrateurs de compte, il n'est pas nécessaire d'associer le connecteur aux espaces de travail. Ils peuvent accéder par défaut à tous les espaces de travail dans Cloud Manager. "En savoir plus >>".

Création d'un connecteur dans GCP à partir de Cloud Manager

Un administrateur de compte doit déployer un *Connector* avant de pouvoir utiliser la plupart des fonctionnalités de Cloud Manager. "Apprenez quand un connecteur est nécessaire". Ce connecteur permet à Cloud Manager de gérer les ressources et les processus au sein de votre environnement de cloud public.

Cette page explique comment créer un connecteur dans GCP directement depuis Cloud Manager. Vous avez également la possibilité de "téléchargez le logiciel et installez-le sur votre propre hôte".

Ces étapes doivent être réalisées par un utilisateur qui a le rôle d'administrateur de compte. Un administrateur d'espace de travail ne peut pas créer de connecteur.

Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l'avez pas encore créé.

Configuration des autorisations GCP pour créer un connecteur

Avant de déployer un connecteur depuis Cloud Manager, vous devez vous assurer que votre compte GCP dispose des autorisations appropriées et qu'un compte de service est configuré pour la machine virtuelle Connector.

Étapes

1. Assurez-vous que l'utilisateur GCP qui déploie Cloud Manager à partir de NetApp Cloud Central dispose des autorisations dans le "Règle de déploiement du connecteur pour GCP".

   "Vous pouvez créer un rôle personnalisé à l'aide du fichier YAML" puis joignez-le à l'utilisateur. Vous devrez utiliser la ligne de commande gcloud pour créer le rôle.

2. Configurez un compte de service disposant des autorisations nécessaires à Cloud Manager pour créer et gérer des systèmes Cloud Volumes ONTAP dans des projets.

   Vous allez associer ce compte de service à la machine virtuelle Connector lorsque vous la créez à partir de Cloud Manager.

   a. "Créer un rôle dans GCP" qui inclut les autorisations définies dans le "Règle Cloud Manager pour GCP". Là encore, vous devrez utiliser la ligne de commande gcloud.

      Les autorisations contenues dans ce fichier YAML sont différentes des autorisations de l'étape 2a.

   b. "Créez un compte de service GCP et appliquez le rôle personnalisé que vous venez de créer".

   c. Si vous souhaitez déployer Cloud Volumes ONTAP dans d'autres projets, "Accordez l'accès en ajoutant le compte de service avec le rôle Cloud Manager à ce projet". Vous devrez répéter cette étape pour chaque projet.

Résultat

L'utilisateur GCP dispose désormais des autorisations nécessaires pour créer le connecteur depuis Cloud Manager et le compte de service de la machine virtuelle Connector est configuré.

Activation des API Google Cloud

Plusieurs API sont nécessaires pour déployer le connecteur et Cloud Volumes ONTAP.

Étape

1. "Activez les API Google Cloud suivantes dans votre projet".
   - API Cloud Deployment Manager V2
   - API de journalisation cloud
   - API Cloud Resource Manager
   - API du moteur de calcul
   - API de gestion des identités et des accès

Création d'un connecteur dans GCP

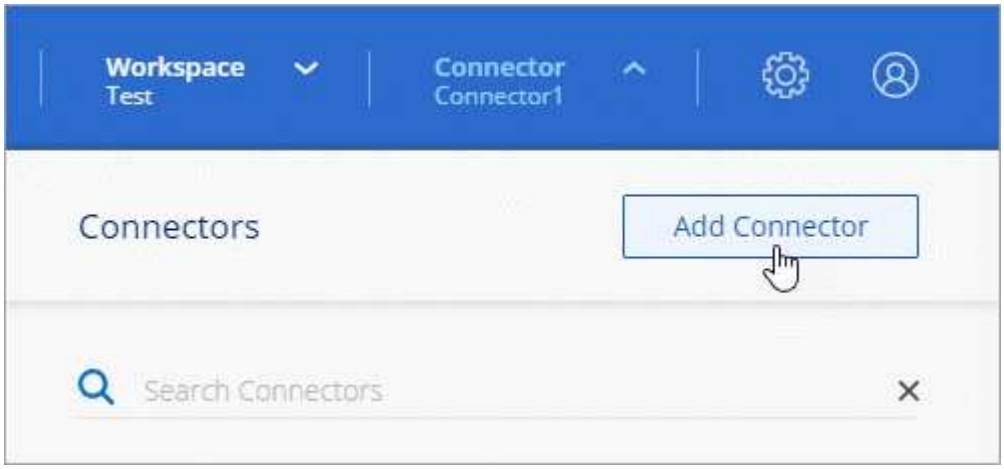
Avec Cloud Manager, vous pouvez créer un connecteur dans GCP directement à partir de son interface utilisateur.

Ce dont vous avez besoin

- Le "autorisations requises" Pour votre compte Google Cloud.
- Un projet Google Cloud.
- Compte de service disposant des autorisations requises pour créer et gérer Cloud Volumes ONTAP.
- VPC et sous-réseau dans votre région Google Cloud.

Étapes

1. Si vous créez votre premier environnement de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites. Sinon, cliquez sur la liste déroulante **Connector** et sélectionnez **Add Connector**.



2. Cliquez sur **commençons**.
3. Choisissez **Google Cloud Platform** comme fournisseur de cloud.

   Rappelez-vous que le connecteur doit disposer d'une connexion réseau au type d'environnement de travail que vous créez et aux services que vous prévoyez d'activer.

   "En savoir plus sur les exigences de mise en réseau pour le connecteur".

4. Passez en revue ce dont vous aurez besoin et cliquez sur **Continuer**.
5. Si vous y êtes invité, connectez-vous à votre compte Google, qui devrait disposer des autorisations requises pour créer l'instance de machine virtuelle.

   Le formulaire est détenu et hébergé par Google. Vos identifiants ne sont pas fournis à NetApp.

6. Fournissez les informations requises :
   - **Paramètres de base** : saisissez un nom pour l'instance de machine virtuelle et spécifiez un compte de projet et de service disposant des autorisations requises.
   - **Location** : spécifiez une région, une zone, un VPC et un sous-réseau pour l'instance.
   - **Réseau** : permet d'activer ou non une adresse IP publique et de spécifier éventuellement une configuration proxy.
   - **Politique de pare-feu** : Choisissez si vous souhaitez créer une nouvelle politique de pare-feu ou si

vous souhaitez sélectionner une politique de pare-feu existante qui autorise l'accès HTTP, HTTPS et SSH entrant.

> Il n'y a pas de trafic entrant vers le connecteur, sauf si vous le lancez. HTTP et HTTPS permettent l'accès au "Interface utilisateur locale", que vous utiliserez dans de rares circonstances. SSH n'est nécessaire que si vous devez vous connecter à l'hôte pour le dépannage.

7. Cliquez sur **Créer**.

   L'instance doit être prête dans environ 7 minutes. Vous devez rester sur la page jusqu'à ce que le processus soit terminé.

Une fois que vous avez terminé

Vous devez associer un connecteur aux espaces de travail pour que les administrateurs d'espace de travail puissent utiliser ces connecteurs pour créer des systèmes Cloud Volumes ONTAP. Si vous ne disposez que d'administrateurs de compte, il n'est pas nécessaire d'associer le connecteur aux espaces de travail. Ils peuvent accéder par défaut à tous les espaces de travail dans Cloud Manager. "En savoir plus >>".

Par où aller plus loin

Maintenant que vous êtes connecté et que vous configurez Cloud Manager, les utilisateurs peuvent commencer à créer et découvrir des environnements de travail.

- "Commencez avec Cloud Volumes ONTAP pour AWS"
- "Commencez avec Cloud Volumes ONTAP pour Azure"
- "Lancez-vous avec Cloud Volumes ONTAP pour Google Cloud"
- "Configurer Azure NetApp Files"
- "Configuration d'Cloud Volumes Service pour AWS"
- "Découvrez un cluster ONTAP sur site"
- "Découvrez vos compartiments Amazon S3"

Si vous êtes administrateur, vous pouvez gérer les paramètres de Cloud Manager après avoir créé votre premier connecteur.

- "En savoir plus sur les connecteurs"
- "Gérez un certificat HTTPS pour l'accès sécurisé"
- "Configurer les paramètres proxy"

Gérer Cloud Volumes ONTAP

Apprendre

Découvrez Cloud Volumes ONTAP

Avec Cloud Volumes ONTAP, vous optimisez les performances et les coûts de stockage cloud tout en améliorant la protection, la sécurité et la conformité des données.

Cloud Volumes ONTAP est une appliance de stockage exclusivement logicielle qui exécute le logiciel de gestion des données ONTAP dans le cloud. Il offre un système de stockage haute performance doté de plusieurs fonctionnalités clés :

- Fonctionnalités d'efficacité du stockage

  Exploitez les fonctionnalités intégrées de déduplication et de compression des données, de provisionnement fin et de clonage pour réduire les coûts de stockage.

- Haute disponibilité

  Fiabilité exceptionnelle et continuité de l'activité en cas de défaillances dans votre environnement cloud.

- Protection des données

  Cloud Volumes ONTAP exploite SnapMirror, la technologie de réplication leader du secteur, pour répliquer les données sur site vers le cloud. Ainsi, il est possible de disposer de copies secondaires dans différents cas d'utilisation.

  Cloud Volumes ONTAP s'intègre également avec Cloud Backup Service pour fournir des fonctionnalités de sauvegarde et de restauration pour la protection et l'archivage à long terme de vos données cloud.

- Tiering des données

  Basculez entre pools de stockage hautes performances et faibles performances à la demande sans interrompre les applications.

- La cohérence des applications

  Cohérence des copies NetApp Snapshot avec NetApp SnapCenter

- Sécurité des données

  Cloud Volumes ONTAP prend en charge le cryptage des données et protège contre les virus et les attaques par ransomware.

- Contrôles de conformité à la confidentialité

  L'intégration avec Cloud Compliance vous aide à comprendre le contexte des données et à identifier les données sensibles.

Les licences des fonctionnalités ONTAP sont incluses dans Cloud Volumes ONTAP.

"Afficher les configurations Cloud Volumes ONTAP prises en charge"

"En savoir plus sur Cloud Volumes ONTAP"

Stockage

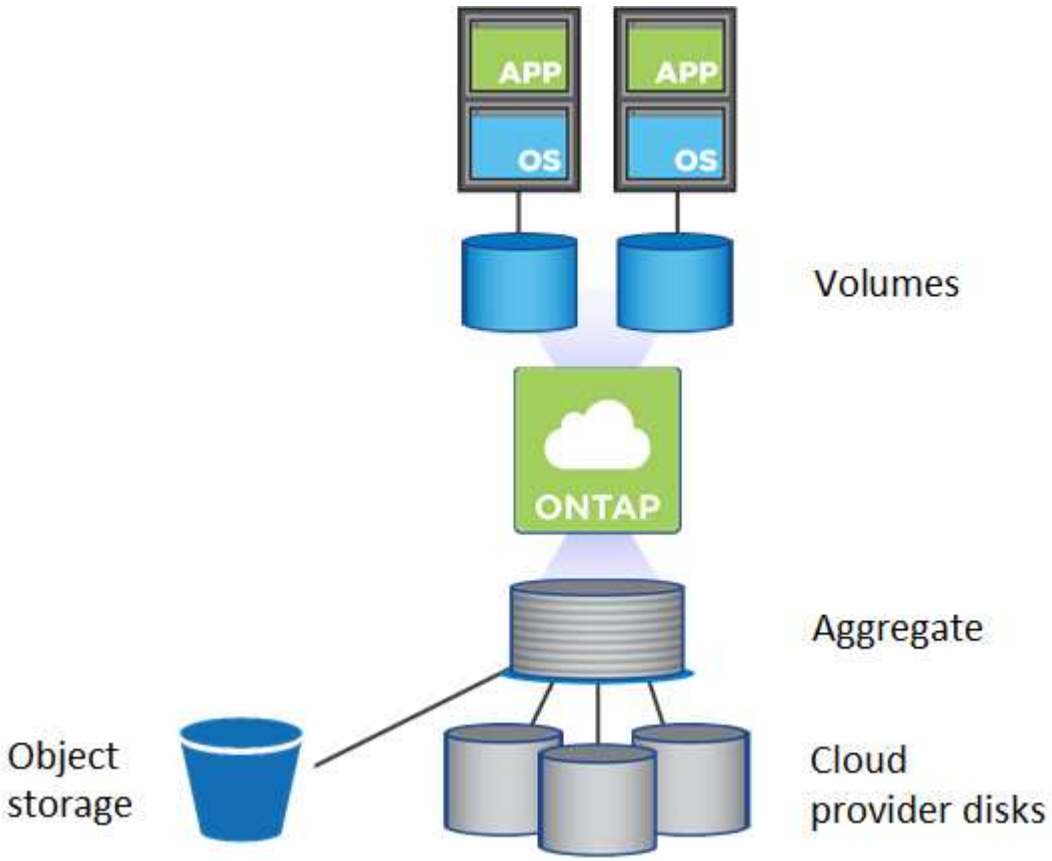
Disques et agrégats

Comprendre comment Cloud Volumes ONTAP utilise le stockage cloud pour vous aider à comprendre vos coûts de stockage.

Tous les disques et agrégats doivent être créés et supprimés directement de Cloud Manager. Vous ne devez pas effectuer ces actions à partir d'un autre outil de gestion. Cela peut avoir un impact sur la stabilité du système, entraver la possibilité d'ajouter des disques à l'avenir et générer potentiellement des frais de fournisseur de cloud redondant.

Présentation

Cloud Volumes ONTAP utilise le stockage du fournisseur cloud comme disques et les regroupe dans un ou plusieurs agrégats. Les agrégats fournissent du stockage à un ou plusieurs volumes.



Plusieurs types de disques clouds sont pris en charge. Lorsque vous déployez Cloud Volumes ONTAP, vous choisissez le type de disque lorsque vous créez un volume et la taille de disque par défaut.

Le volume total de stockage acheté auprès d'un fournisseur cloud est la *capacité brute*. La *capacité utilisable* est inférieure car environ 12 à 14 % représente la surcharge réservée à l'utilisation de Cloud Volumes ONTAP. Par exemple, si Cloud Manager crée un agrégat de 500 Go, la capacité utilisable est de 442,94 Go.

Le stockage AWS

Dans AWS, Cloud Volumes ONTAP utilise le stockage EBS pour les données utilisateur et le stockage NVMe local en tant que Flash cache sur certains types d'instances EC2.

Stockage EBS

Dans AWS, un agrégat peut contenir jusqu'à 6 disques de même taille. La taille maximale du disque est de 16 To.

Le type de disque EBS sous-jacent peut être SSD à usage général, SSD IOPS provisionné, disque dur optimisé pour le débit ou disque dur froid. Vous pouvez associer un disque EBS à Amazon S3 pour "déplacez les données inactives vers un stockage objet à faible coût".

À un niveau élevé, les différences entre les types de disques EBS sont les suivantes :

- *Des disques SSD* à usage générique permettent d'équilibrer les coûts et les performances pour une grande variété de charges de travail. La performance est définie en termes d'IOPS.
- *Les disques SSD* d'IOPS provisionnés sont pour les applications stratégiques qui requièrent des performances optimales à un coût plus élevé.
- *Les disques HDD* optimisés en termes de débit sont destinés aux charges de travail fréquemment utilisées qui exigent un débit rapide et cohérent à un prix inférieur.
- *Les disques durs* froide sont utilisés pour les sauvegardes ou les données rarement utilisées, car les performances sont très faibles. Tout comme les disques HDD optimisés en termes de débit, les performances sont définies en termes de débit.

Les disques durs inactifs ne sont pas pris en charge avec les configurations haute disponibilité et le Tiering des données.

Stockage NVMe local

Certains types d'instances EC2 incluent le stockage NVMe local, qui est utilisé par Cloud Volumes ONTAP "Flash cache".

- Liens connexes*
- "Documentation AWS : types de volume EBS"
- "Découvrez comment choisir les types et les tailles de disques pour vos systèmes dans AWS"
- "Consultez les limites de stockage pour Cloud Volumes ONTAP dans AWS"
- "Étude des configurations pour Cloud Volumes ONTAP prises en charge dans AWS"

Le stockage Azure

Dans Azure, un agrégat peut contenir jusqu'à 12 disques de même taille. Le type de disque et la taille de disque maximale dépendent de l'utilisation d'un système à un seul nœud ou d'une paire haute disponibilité :

Systèmes à un seul nœud

Les systèmes à un seul nœud peuvent utiliser trois types de disques gérés Azure :

- *Des disques gérés SSD de premier choix* fournir des performances élevées aux charges de travail exigeantes en E/S à un coût plus élevé.
- *Des disques gérés SSD standard* assurent des performances prévisibles pour les charges de travail nécessitant un faible niveau d'IOPS.
- *Les disques gérés HDD standard* sont un bon choix si vous n'avez pas besoin d'IOPS élevées et souhaitez réduire vos coûts.

  Chaque type de disque géré a une taille de disque maximale de 32 To.

  Vous pouvez coupler un disque géré avec le stockage Azure Blob à "déplacez les données inactives vers un stockage objet à faible coût".

Paires HA

Les paires HAUTE DISPONIBILITÉ utilisent des objets blob de pages Premium qui ont une taille de disque maximale de 8 To.

- Liens connexes*
- "Documentation Microsoft Azure : présentation du stockage Microsoft Azure"
- "Découvrez comment choisir les types et les tailles de disques pour vos systèmes dans Azure"
- "Consultez les limites de stockage pour Cloud Volumes ONTAP dans Azure"

Stockage GCP

Dans GCP, un agrégat peut contenir jusqu'à 6 disques de même taille. La taille maximale du disque est de 16 To.

Le type de disque peut être soit *Zonal SSD persistent disks* soit *Zonal standard persistent disks*. Vous pouvez coupler des disques persistants avec un compartiment Google Storage vers "déplacez les données inactives vers un stockage objet à faible coût".

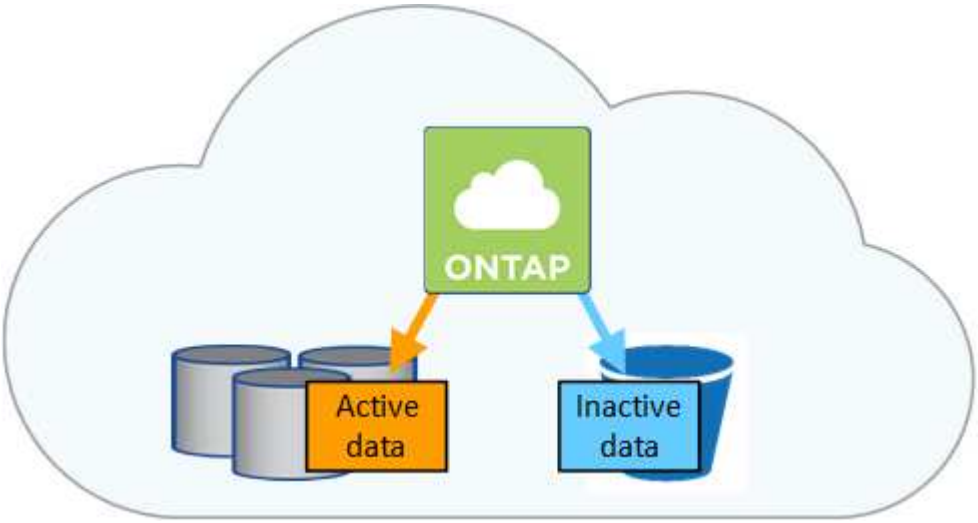
- Liens connexes*
- "Documentation sur Google Cloud Platform : options de stockage"
- "Consultez les limites de stockage des Cloud Volumes ONTAP dans GCP"

Type de RAID

Pour chaque agrégat Cloud Volumes ONTAP, le type RAID est RAID0 (répartition). Aucun autre type de RAID n'est pris en charge. Cloud Volumes ONTAP fait appel au fournisseur cloud pour assurer la disponibilité et la durabilité des disques.

Vue d'ensemble du hiérarchisation des données

Réduisez vos coûts de stockage en permettant le Tiering automatisé des données inactives vers un stockage objet à faible coût. Les données actives conservent les disques SSD ou HDD haute performance, tandis que les données inactives sont envoyées vers un stockage objet à faible coût. Vous pouvez ainsi récupérer de l'espace sur votre stockage principal et réduire le stockage secondaire.



Cloud Volumes ONTAP prend en charge le Tiering des données dans AWS, Azure et Google Cloud Platform. La hiérarchisation des données est optimisée par la technologie FabricPool.

Inutile d'installer une licence pour activer le Tiering des données (FabricPool).

Tiering des données dans AWS

Lorsque vous activez le Tiering des données dans AWS, Cloud Volumes ONTAP utilise EBS comme Tier de performance pour les données actives et AWS S3 comme Tier de capacité pour les données inactives.

Tier de performance

Le niveau de performance peut être des disques SSD à usage général, des disques SSD IOPS provisionnés ou des disques durs optimisés pour le débit.

Des disques SSD/HDD FAS

Un système Cloud Volumes ONTAP transfère les données inactives vers un seul compartiment S3 à l'aide de la classe de stockage *Standard*. La norme est idéale pour les données fréquemment consultées stockées dans plusieurs zones de disponibilité.

Cloud Manager crée un compartiment S3 unique pour chaque environnement de travail et le nomme ce compartiment unique « fabric-pool-*cluster* ». Un compartiment S3 différent n'est pas créé pour chaque volume.

Classes de stockage

La classe de stockage par défaut pour les données hiérarchisées dans AWS est *Standard*. Si vous ne prévoyez pas d'accéder aux données inactives, vous pouvez réduire vos coûts de stockage en changeant la classe de stockage à l'une des catégories suivantes : *Intelligent Tiering*, *One-zone Infrequent Access* ou *Standard-Infrequent Access*. Lorsque vous modifiez la classe de stockage, les données inactives commencent dans la classe de stockage Standard et sont transitions vers la classe de stockage que vous avez sélectionnée, si les données ne sont pas accessibles après 30 jours.

Les coûts d'accès sont plus élevés si vous accédez aux données. Prenez donc ces considérations avant de changer la classe de stockage. "En savoir plus sur les classes de stockage Amazon S3".

Vous pouvez sélectionner une classe de stockage lors de la création de l'environnement de travail et la modifier à tout moment après. Pour plus de détails sur la modification de la classe de stockage, voir "Tiering des données inactives vers un stockage objet à faible coût".

La classe de stockage du Tiering des données est étendue au système - elle n'est pas par volume.

Tiering des données dans Azure

Lorsque vous activez le Tiering des données dans Azure, Cloud Volumes ONTAP utilise des disques gérés Azure comme un Tier de performance pour les données actives et le stockage Azure Blob comme un Tier de capacité pour les données inactives.

Tier de performance

Le Tier de performance peut être soit des disques SSD, soit des disques durs.

Des disques SSD/HDD FAS

Un système Cloud Volumes ONTAP transfère les données inactives vers un seul conteneur Blob à l'aide du Tier de stockage Azure *hot*. Le Tier actif est idéal pour les données fréquemment utilisées.

> Cloud Manager crée un nouveau compte de stockage avec un container unique pour chaque environnement de travail Cloud Volumes ONTAP. Le nom du compte de stockage est aléatoire. Un container différent n'est pas créé pour chaque volume.

Les niveaux d'accès au stockage

Le niveau d'accès au stockage par défaut pour les données hiérarchisées dans Azure est le *hot* Tier. Si vous ne prévoyez pas d'accéder aux données inactives, vous pouvez réduire vos coûts de stockage en utilisant le niveau de stockage *cool*. Lorsque vous modifiez le niveau de stockage, les données inactives commencent dans le Tier de stockage à chaud et se transfère sur le Tier de stockage à froid, si les données ne sont pas accessibles au bout de 30 jours.

Les coûts d'accès sont plus élevés si vous accédez aux données, prenez donc ces considérations avant de changer le Tier de stockage. "En savoir plus sur les tiers d'accès au stockage Azure Blob".

Vous pouvez sélectionner un niveau de stockage lors de la création de l'environnement de travail et le modifier à tout moment après. Pour plus d'informations sur la modification du niveau de stockage, reportez-vous à la section "Tiering des données inactives vers un stockage objet à faible coût".

Le niveau d'accès au stockage pour le Tiering des données concerne l'ensemble du système - il ne s'agit pas de par volume.

Tiering des données dans GCP

Lorsque vous activez le Tiering des données dans GCP, Cloud Volumes ONTAP utilise des disques persistants comme Tier de performance pour les données actives et un compartiment Google Cloud Storage comme Tier de capacité pour les données inactives.

Tier de performance

Le Tier de performance peut être soit des disques SSD, soit des disques HDD (disques standard).

Des disques SSD/HDD FAS

Un système Cloud Volumes ONTAP transfère les données inactives vers un seul compartiment de stockage cloud Google à l'aide de la classe de stockage *régional*.

> Cloud Manager crée un compartiment unique pour chaque environnement de travail et lui attribue un identifiant unique « fabric-pool »-*cluster*. Un compartiment différent n'est pas créé pour chaque volume.

Classes de stockage

La classe de stockage par défaut pour les données hiérarchisées est la classe *Standard Storage*. Si les données sont rarement utilisées, vous pouvez réduire vos coûts de stockage en utilisant *Nearline Storage* ou *Coldline Storage*. Lorsque vous modifiez la classe de stockage, les données inactives commencent dans la classe de stockage standard et sont transitions vers la classe de stockage que vous avez sélectionnée, si les données ne sont pas accessibles après 30 jours.

Les coûts d'accès sont plus élevés si vous accédez aux données. Prenez donc ces considérations avant de changer la classe de stockage. "En savoir plus sur les classes de stockage pour Google Cloud Storage".

Vous pouvez sélectionner un niveau de stockage lors de la création de l'environnement de travail et le modifier à tout moment après. Pour plus de détails sur la modification de la classe de stockage, voir "Tiering des données inactives vers un stockage objet à faible coût".

La classe de stockage du Tiering des données est étendue au système - elle n'est pas par volume.

Tiering des données et limites de capacité

Si vous activez le Tiering des données, la limite de capacité d'un système reste la même. La limite est répartie entre le niveau de performance et le niveau de capacité.

Stratégies de hiérarchisation des volumes

Pour activer la hiérarchisation des données, vous devez sélectionner une stratégie de hiérarchisation des volumes lorsque vous créez, modifiez ou répliquez un volume. Vous pouvez sélectionner une stratégie différente pour chaque volume.

Certaines stratégies de hiérarchisation ont une période de refroidissement minimale associée, qui définit le temps pendant lequel les données utilisateur d'un volume doivent rester inactives pour que les données soient considérées comme "froides" et déplacées vers le niveau de capacité.

Cloud Manager vous permet de choisir parmi les règles de Tiering des volumes suivantes lorsque vous créez ou modifiez un volume :

Snapshot uniquement

Après avoir atteint une capacité de 50 %, Cloud Volumes ONTAP met à niveau les données utilisateur à froid des copies Snapshot qui ne sont pas associées au système de fichiers actif au niveau de la capacité. La période de refroidissement est d'environ 2 jours.

En cas de lecture, les blocs de données à froid sur le niveau de capacité deviennent chauds et sont déplacés vers le niveau de performance.

Tout

Toutes les données (sans les métadonnées) sont immédiatement marquées comme inactives et hiérarchisées vers le stockage objet dès que possible. Il n'est pas nécessaire d'attendre 48 heures que les nouveaux blocs d'un volume soient inactifs. Notez que les blocs situés dans le volume avant la définition de toutes les règles exigent 48 heures pour être froids.

Si les blocs de données inactives du Tier cloud sont lus, ceux-ci restent inactives et ne sont pas réécrits sur le Tier de performance. Cette règle est disponible à partir de ONTAP 9.6.

Auto

Après avoir atteint une capacité de 50 %, Cloud Volumes ONTAP met à niveau des blocs de données à froid dans un volume vers un niveau de capacité. Les données à froid comprennent non seulement des

copies Snapshot, mais aussi des données utilisateur à froid provenant du système de fichiers actif. La période de refroidissement est d'environ 31 jours.

Cette stratégie est prise en charge à partir de Cloud Volumes ONTAP 9.4.

En cas de lecture aléatoire, les blocs de données à froid du niveau de capacité deviennent chauds et passent au niveau de performance. Si elles sont lues par des lectures séquentielles, telles que celles associées aux analyses d'index et d'antivirus, les blocs de données à froid restent froids et ne passent pas au niveau de performance.

Aucune

Conserve les données d'un volume dans le niveau de performance, ce qui empêche leur déplacement vers le niveau de capacité.

Lorsque vous répliquez un volume, vous pouvez choisir le Tiering des données dans le stockage objet. Si c'est le cas, Cloud Manager applique la règle **Backup** au volume de protection des données. Depuis Cloud Volumes ONTAP 9.6, la règle de hiérarchisation **All** remplace la règle de sauvegarde.

La désactivation de Cloud Volumes ONTAP a des répercussions sur la période de refroidissement

Les blocs de données sont refroidis par des analyses de refroidissement. Durant ce processus, la température des blocs pendant lesquels leur température de bloc n'a pas été utilisée est déplacée (refroidie) vers la valeur inférieure suivante. La durée de refroidissement par défaut dépend de la règle de Tiering du volume :

- Auto : 31 jours
- Snapshot uniquement : 2 jours

Cloud Volumes ONTAP doit être en cours d'exécution pour que l'acquisition de refroidissement fonctionne. Si le Cloud Volumes ONTAP est désactivé, le refroidissement s'arrête également. Les temps de refroidissement peuvent ainsi être plus longs.

Configuration du tiering des données

Pour obtenir des instructions et une liste des configurations prises en charge, reportez-vous à la section "Tiering des données inactives vers un stockage objet à faible coût".

Gestion du stockage

Cloud Manager permet une gestion simplifiée et avancée du stockage Cloud Volumes ONTAP.

> Tous les disques et agrégats doivent être créés et supprimés directement de Cloud Manager. Vous ne devez pas effectuer ces actions à partir d'un autre outil de gestion. Cela peut avoir un impact sur la stabilité du système, entraver la possibilité d'ajouter des disques à l'avenir et générer potentiellement des frais de fournisseur de cloud redondant.

Provisionnement du stockage

Cloud Manager facilite le provisionnement du stockage pour Cloud Volumes ONTAP en achetant des disques et en gérant des agrégats pour vous. Il vous suffit de créer des volumes. Si vous le souhaitez, vous pouvez utiliser une option d'allocation avancée pour provisionner vous-même des agrégats.

Provisionnement simplifié

Les agrégats fournissent un stockage cloud aux volumes. Cloud Manager crée des agrégats pour vous lorsque vous lancez une instance et que vous provisionnez des volumes supplémentaires.

Lorsque vous créez un volume, Cloud Manager fait l'une des trois opérations suivantes :

- Il place le volume sur un agrégat existant qui dispose d'un espace libre suffisant.
- Il place le volume sur un agrégat existant en achetant plus de disques pour cet agrégat.
- Il achète des disques pour un nouvel agrégat et place le volume sur cet agrégat.

Cloud Manager détermine où placer un nouveau volume en se base sur plusieurs facteurs : la taille maximale d'un agrégat, l'activation ou non du provisionnement fin et les seuils d'espace disponible pour les agrégats.

L'administrateur du compte peut modifier les seuils d'espace libre à partir de la page **Paramètres**.

Sélection de la taille du disque pour les agrégats dans AWS

Lorsque Cloud Manager crée de nouveaux agrégats pour Cloud Volumes ONTAP dans AWS, il augmente progressivement la taille du disque dans un agrégat, à mesure que le nombre d'agrégats dans le système augmente. Cloud Manager vous permet ainsi d'utiliser la capacité maximale du système avant d'atteindre le nombre maximal de disques de données autorisés par AWS.

Par exemple, Cloud Manager peut choisir les tailles de disque suivantes pour les agrégats dans un système Cloud Volumes ONTAP Premium ou BYOL :

Numéro d'agrégat	Taille du disque	Capacité d'agrégat max.
1	500 Mo.	3 To
4	1 To	6 To
6	2 To	12 To

Vous pouvez choisir vous-même la taille du disque en utilisant l'option d'allocation avancée.

Allocation avancée

Plutôt que de laisser Cloud Manager gérer les agrégats pour vous, vous pouvez le faire vous-même. "À partir de la page **allocation avancée**", vous pouvez créer de nouveaux agrégats qui incluent un nombre spécifique de disques, ajouter des disques à un agrégat existant et créer des volumes dans des agrégats spécifiques.

Gestion de la capacité

L'administrateur du compte peut décider si Cloud Manager vous informe des décisions en matière de capacité de stockage ou si Cloud Manager gère automatiquement les besoins en capacité pour vous. Il peut vous aider à comprendre le fonctionnement de ces modes.

Gestion automatique de la capacité

Le mode de gestion de la capacité est défini sur automatique par défaut. Dans ce mode, Cloud Manager achète automatiquement de nouveaux disques pour les instances Cloud Volumes ONTAP lorsque plus de capacité est nécessaire, supprime les ensembles de disques (agrégats) inutilisés, déplace des volumes entre

les agrégats si nécessaire et tente de rétablir la panne des disques.

Les exemples suivants illustrent le fonctionnement de ce mode :

- Si un agrégat de 5 disques EBS ou moins atteint le seuil de capacité, Cloud Manager achète automatiquement de nouveaux disques pour cet agrégat afin que les volumes puissent continuer à croître.
- Si un agrégat de 12 disques Azure atteint le seuil de capacité, Cloud Manager déplace automatiquement un volume de cet agrégat vers un agrégat de capacité disponible ou vers un nouvel agrégat.

  Si Cloud Manager crée un nouvel agrégat pour le volume, il sélectionne une taille de disque qui convient à sa taille.

  Notez que l'espace libre est désormais disponible sur l'agrégat d'origine. Les volumes existants ou les nouveaux volumes peuvent utiliser cet espace. L'espace ne peut pas être renvoyé vers AWS, Azure ou GCP dans ce scénario.

- Si un agrégat ne contient pas de volumes pendant plus de 12 heures, Cloud Manager le supprime.

Gestion des LUN avec gestion automatique de la capacité

La gestion automatique de la capacité de Cloud Manager ne s'applique pas aux LUN. Lorsque Cloud Manager crée un LUN, il désactive la fonctionnalité de croissance automatique.

Gestion des inodes avec gestion automatique de la capacité

Cloud Manager surveille l'utilisation d'inode sur un volume. Lorsque 85 % des inodes sont utilisés, Cloud Manager augmente la taille du volume pour augmenter le nombre d'inodes disponibles. Le nombre de fichiers qu'un volume peut contenir est déterminé par le nombre d'inodes qu'il possède.

Gestion manuelle de la capacité

Si l'administrateur du compte définit le mode de gestion de la capacité sur manuel, Cloud Manager affiche les messages action requise lorsque les décisions relatives à la capacité doivent être prises. Les mêmes exemples décrits en mode automatique s'appliquent au mode manuel, mais il vous appartient d'accepter les actions.

Flash cache

Certaines configurations Cloud Volumes ONTAP dans AWS et Azure incluent le stockage NVMe local, qui utilise Cloud Volumes ONTAP comme *Flash cache* pour de meilleures performances.

Qu'est-ce que Flash cache ?

Flash cache accélère l'accès aux données grâce à la mise en cache intelligente en temps réel des données utilisateur et des métadonnées NetApp lues récemment. Elle est efficace pour les charges de travail exigeant une capacité de lecture aléatoire maximale, dont les bases de données, la messagerie et les services de fichiers.

Instances prises en charge dans AWS

Sélectionnez l'un des types d'instances EC2 suivants avec un système Cloud Volumes ONTAP Premium ou BYOL existant :

- c5d.4xlarge
- c5d.9xlarge
- c5d.18xlarge
- m5d.cum
- m5d.12xlarge
- r5d.2xlarge

Type de VM pris en charge dans Azure

Sélectionnez le type de machine virtuelle Standard_L8S_v2 avec un système Cloud Volumes ONTAP BYOL à un seul nœud dans Azure.

Limites

- La compression doit être désactivée sur tous les volumes pour tirer parti des améliorations des performances de Flash cache.

  Sélectionnez l'efficacité du stockage lors de la création d'un volume depuis Cloud Manager, ou créez un volume, puis "Désactiver la compression des données à l'aide de l'interface de ligne de commande".

- La réactivation du cache après un redémarrage n'est pas prise en charge avec Cloud Volumes ONTAP.

Stockage WORM

Vous pouvez activer le stockage WORM (écriture unique) en lecture seule sur un système Cloud Volumes ONTAP pour conserver les fichiers sous forme non modifiée pendant une période de conservation spécifiée. Le stockage WORM est optimisé par la technologie SnapLock en mode Entreprise, ce qui signifie que les fichiers WORM sont protégés au niveau des fichiers.

Une fois qu'un fichier a été validé sur le stockage WORM, il ne peut pas être modifié, même après l'expiration de la période de conservation. Une horloge inviolable détermine le moment où la période de conservation d'un fichier WORM s'est écoulée.

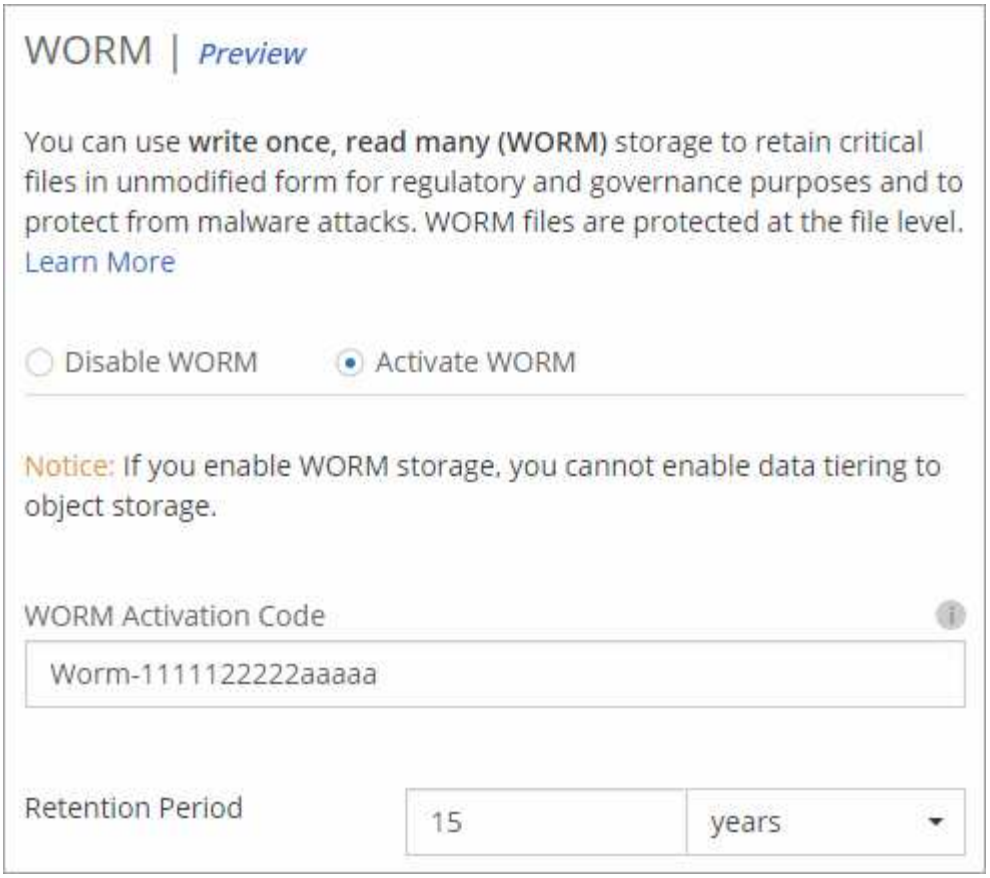
Une fois la période de conservation écoulée, vous êtes responsable de la suppression des fichiers dont vous n'avez plus besoin.

Activation du stockage WORM

Vous pouvez activer le stockage WORM sur un système Cloud Volumes ONTAP lorsque vous créez un nouvel environnement de travail. Cela inclut la spécification d'un code d'activation et la définition de la période de conservation par défaut des fichiers. Vous pouvez obtenir un code d'activation à l'aide de l'icône de chat située dans l'angle inférieur droit de l'interface de Cloud Manager.

Vous ne pouvez pas activer le stockage WORM sur des volumes individuels --WORM doit être activé au niveau du système.

L'image suivante montre comment activer le stockage WORM lors de la création d'un environnement de travail :



Validation de fichiers sur WORM

Vous pouvez utiliser une application pour valider des fichiers sur WORM via NFS ou CIFS, ou utiliser l'interface de ligne de commande ONTAP pour auto-valider des fichiers sur WORM automatiquement. Vous pouvez également utiliser un fichier WORM inscriptible pour conserver les données écrites de façon incrémentielle, comme les informations de journal.

Après avoir activé le stockage WORM sur un système Cloud Volumes ONTAP, vous devez utiliser l'interface de ligne de commande ONTAP pour toute la gestion du stockage WORM. Pour obtenir des instructions, reportez-vous à la section "Documentation ONTAP".

La prise en charge de Cloud Volumes ONTAP pour le stockage WORM équivaut au mode SnapLock Enterprise.

Limites

- Si vous supprimez ou déplacez un disque directement depuis AWS ou Azure, un volume peut être supprimé avant sa date d'expiration.
- Lorsque le stockage WORM est activé, le Tiering des données vers le stockage objet ne peut pas être activé.
- La sauvegarde dans le cloud doit être désactivée pour activer le stockage WORM.

Paires haute disponibilité

Paires haute disponibilité dans AWS

Une configuration haute disponibilité (HA) Cloud Volumes ONTAP assure des opérations sans interruption et une tolérance aux pannes. Dans AWS, les données sont mises en miroir de manière synchrone entre les deux nœuds.

Présentation

Dans AWS, les configurations haute disponibilité de Cloud Volumes ONTAP incluent les composants suivants :

- Deux nœuds Cloud Volumes ONTAP dont les données sont mises en miroir de manière synchrone.
- Instance médiateur qui fournit un canal de communication entre les nœuds pour faciliter les processus de reprise et de remise du stockage.

L'instance du médiateur exécute le système d'exploitation Linux sur une instance t2.micro et utilise un disque magnétique EBS d'environ 8 Go.

Reprise et remise du stockage

Si un nœud tombe en panne, l'autre nœud peut servir les données à son partenaire pour fournir un service de données continu. Les clients peuvent accéder aux mêmes données à partir du nœud partenaire, car les données ont été mises en miroir de manière synchrone auprès du partenaire.

Après le redémarrage du nœud, le partenaire doit resynchroniser les données avant de pouvoir retourner le stockage. Le temps nécessaire à la resynchronisation des données dépend de la quantité de données modifiées pendant la panne du nœud.

RPO et RTO

Une configuration haute disponibilité maintient la haute disponibilité de vos données comme suit :

- L'objectif du point de récupération (RPO) est de 0 seconde. Vos données sont transactionnaires, sans perte de données.
- L'objectif de temps de récupération (RTO) est de 60 secondes. En cas de panne, les données doivent être disponibles en 60 secondes ou moins.

Modèles de déploiement HA

Vous pouvez garantir la haute disponibilité de vos données en déployant une configuration haute disponibilité sur plusieurs zones de disponibilité (AZS) ou dans un seul AZ. Vous devriez consulter plus de détails sur chaque configuration afin de choisir celle qui répond le mieux à vos besoins.

Cloud Volumes ONTAP HA dans plusieurs zones de disponibilité

Le déploiement d'une configuration haute disponibilité dans plusieurs zones de disponibilité (AZS) garantit une haute disponibilité de vos données en cas de défaillance avec un système AZ ou une instance exécutant un nœud Cloud Volumes ONTAP. Vous devez comprendre l'impact des adresses IP NAS sur l'accès aux données et le basculement du stockage.

Accès aux données NFS et CIFS

Lorsqu'une configuration haute disponibilité est répartie entre plusieurs zones de disponibilité, *adresses IP flottantes* activez l'accès client NAS. Les adresses IP flottantes, qui doivent se trouver en dehors des blocs

CIDR pour tous les VPC de la région, peuvent migrer entre les nœuds en cas de défaillance. Les clients ne sont pas accessibles de manière native en dehors du VPC, sauf si vous "Configuration d'une passerelle de transit AWS".

Si vous ne pouvez pas configurer de passerelle de transit, des adresses IP privées sont disponibles pour les clients NAS qui ne sont pas du VPC. Cependant, ces adresses IP sont statiques ; elles ne peuvent pas basculer d'un nœud à l'autre.

Avant de déployer une configuration haute disponibilité sur plusieurs zones de disponibilité, vous devez consulter les exigences relatives aux adresses IP flottantes et aux tables de routage. Vous devez spécifier les adresses IP flottantes lors du déploiement de la configuration. Les adresses IP privées sont automatiquement créées par Cloud Manager.

Pour plus de détails, voir "Configuration réseau AWS requise pour Cloud Volumes ONTAP HA dans plusieurs AZS".

Accès aux données iSCSI

La communication de données entre VPC n'est pas un problème car iSCSI n'utilise pas d'adresses IP flottantes.

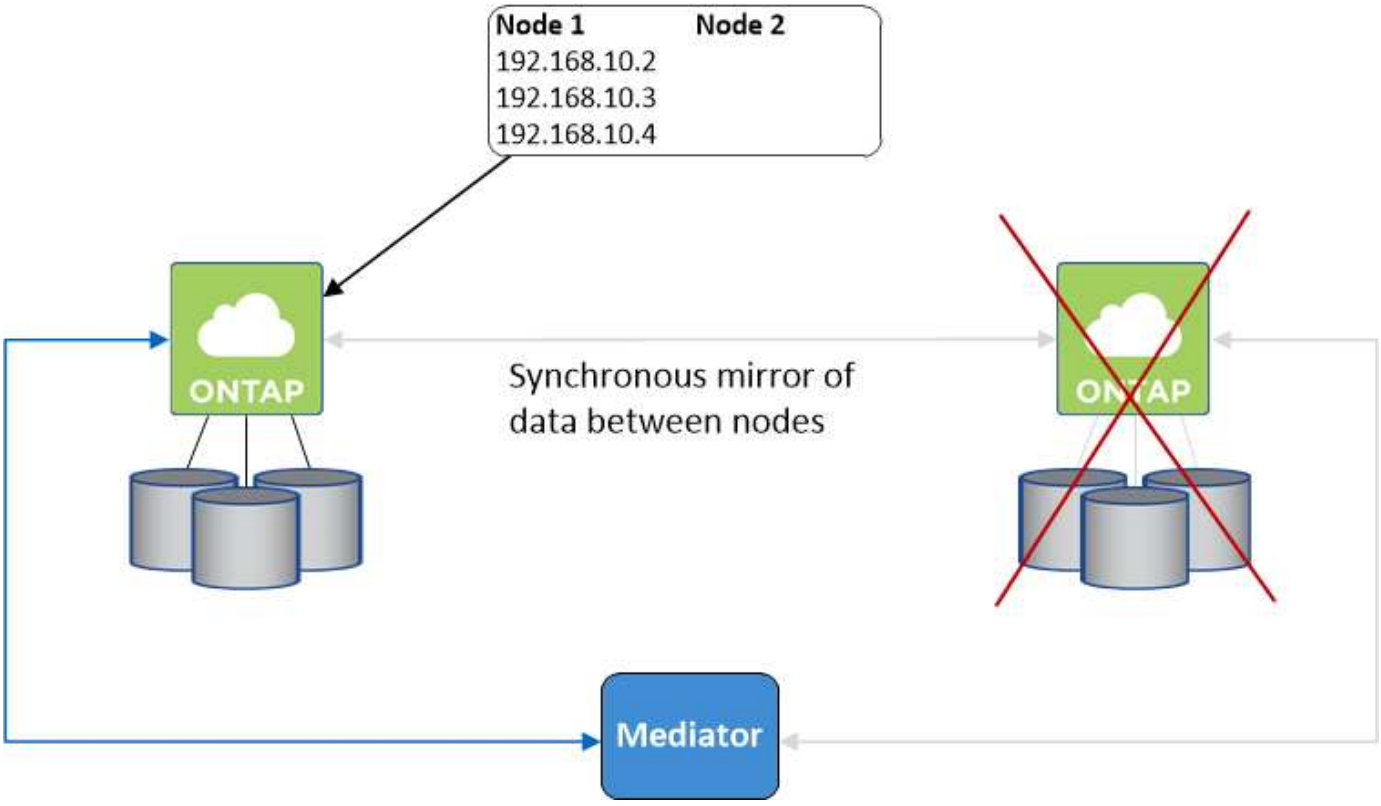
Reprise et remise du stockage pour iSCSI

Pour iSCSI, Cloud Volumes ONTAP utilise les E/S multichemins (MPIO) et l'accès aux unités logiques asymétriques (ALUA) pour gérer le basculement de chemin entre les chemins optimisés et non optimisés.

Pour plus d'informations sur les configurations hôtes spécifiques qui prennent en charge ALUA, consultez le "Matrice d'interopérabilité NetApp" Et le Guide d'installation et de configuration des utilitaires hôtes pour votre système d'exploitation hôte.

Reprise et remise du stockage pour NAS

Lorsque le basculement se produit dans une configuration NAS utilisant des adresses IP flottantes, l'adresse IP flottante du nœud que les clients utilisent pour accéder aux données transférées sur l'autre nœud. L'image suivante illustre la reprise du stockage dans une configuration NAS à l'aide d'adresses IP flottantes. Si le nœud 2 s'arrête, l'adresse IP flottante du nœud 2 passe au nœud 1.



Les adresses IP de données NAS utilisées pour l'accès VPC externe ne peuvent pas migrer entre les nœuds en cas de défaillance. Si un nœud est hors ligne, vous devez remonter manuellement les volumes vers des clients en dehors du VPC à l'aide de l'adresse IP de l'autre nœud.

Une fois le nœud défaillant remis en ligne, remontez les clients vers les volumes à l'aide de l'adresse IP d'origine. Cette étape est nécessaire pour éviter le transfert de données inutiles entre deux nœuds HA, ce qui peut entraîner un impact significatif sur les performances et la stabilité.

Vous pouvez facilement identifier l'adresse IP correcte dans Cloud Manager en sélectionnant le volume et en cliquant sur **Mount Command**.

Cloud Volumes ONTAP HA dans une seule zone de disponibilité

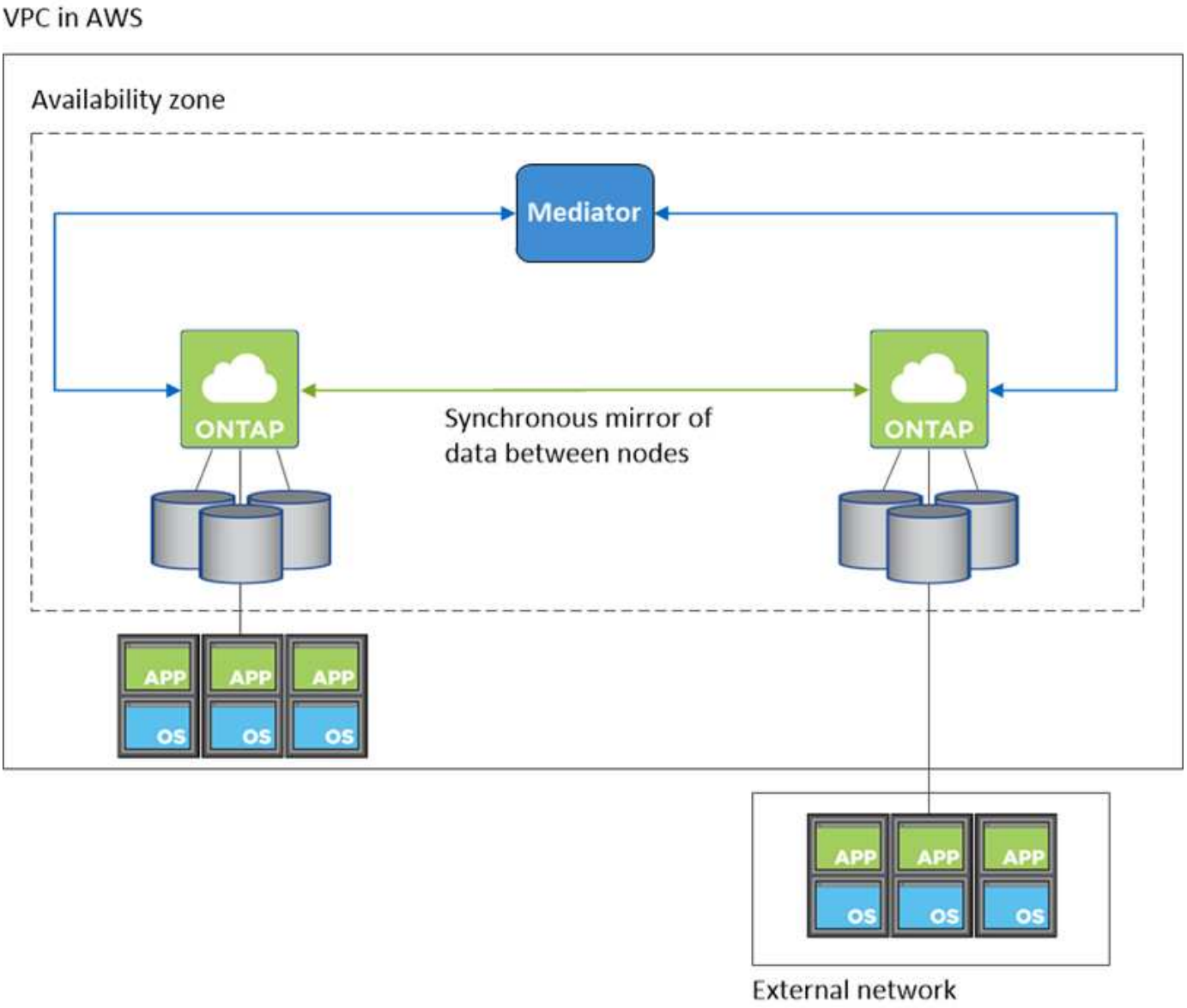
Le déploiement d'une configuration HA dans une seule zone de disponibilité (AZ) peut garantir une haute disponibilité de vos données en cas de défaillance d'une instance exécutant un nœud Cloud Volumes ONTAP. Toutes les données sont accessibles en mode natif depuis l'extérieur du VPC.

> Cloud Manager crée un "Groupe de placement AWS réparti" Et lance les deux nœuds haute disponibilité de ce groupe de placement. Le groupe de placement réduit le risque de défaillances simultanées en répartissant les instances sur un matériel sous-jacent distinct. Cette fonctionnalité améliore la redondance en termes de calcul, et non en termes de défaillance des disques.

Accès aux données

Cette configuration étant dans un seul AZ, elle ne nécessite pas d'adresses IP flottantes. Vous pouvez utiliser la même adresse IP pour accéder aux données depuis le VPC et depuis l'extérieur du VPC.

L'image suivante montre une configuration HA dans un seul AZ. Les données sont accessibles depuis le VPC et depuis l'extérieur du VPC.



Reprise et remise du stockage

Pour iSCSI, Cloud Volumes ONTAP utilise les E/S multichemins (MPIO) et l'accès aux unités logiques asymétriques (ALUA) pour gérer le basculement de chemin entre les chemins optimisés et non optimisés.

Pour plus d'informations sur les configurations hôtes spécifiques qui prennent en charge ALUA, consultez le "Matrice d'interopérabilité NetApp" Et le Guide d'installation et de configuration des utilitaires hôtes pour votre système d'exploitation hôte.

Pour les configurations NAS, les adresses IP des données peuvent migrer entre les nœuds HA en cas de défaillance. Cela garantit l'accès du client au stockage.

Fonctionnement du stockage dans une paire haute disponibilité

Contrairement à un cluster ONTAP, le stockage dans une paire Cloud Volumes ONTAP HA n'est pas partagé entre les nœuds. En revanche, les données sont mises en miroir de manière synchrone entre les nœuds afin que les données soient disponibles en cas de panne.

Allocation du stockage

Lorsque vous créez un nouveau volume et des disques supplémentaires sont requis, Cloud Manager alloue le même nombre de disques aux deux nœuds, crée un agrégat en miroir, puis crée le nouveau volume. Par exemple, si deux disques sont requis pour le volume, Cloud Manager alloue deux disques par nœud pour un total de quatre disques.

Configurations de stockage

Vous pouvez utiliser une paire HA comme configuration active-active, dans laquelle les deux nœuds servent les données aux clients ou comme configuration active-passive, dans laquelle le nœud passif répond aux demandes de données uniquement s'il a pris en charge le stockage pour le nœud actif.

Vous ne pouvez configurer une configuration active-active que si vous utilisez Cloud Manager dans la vue du système de stockage.

Attentes en matière de performances pour une configuration haute disponibilité

Une configuration Cloud Volumes ONTAP HA réplique de manière synchrone les données entre les nœuds, ce qui consomme de la bande passante réseau. Par conséquent, vous pouvez vous attendre aux performances suivantes par rapport à une configuration Cloud Volumes ONTAP à nœud unique :

- Pour les configurations haute disponibilité qui ne servent que des données provenant d'un seul nœud, les performances de lecture sont comparables aux performances de lecture d'une configuration à un nœud, alors que les performances d'écriture sont plus faibles.
- Pour les configurations haute disponibilité qui servent les données des deux nœuds, les performances de lecture sont supérieures aux performances de lecture d'une configuration à nœud unique et les performances d'écriture sont identiques ou supérieures.

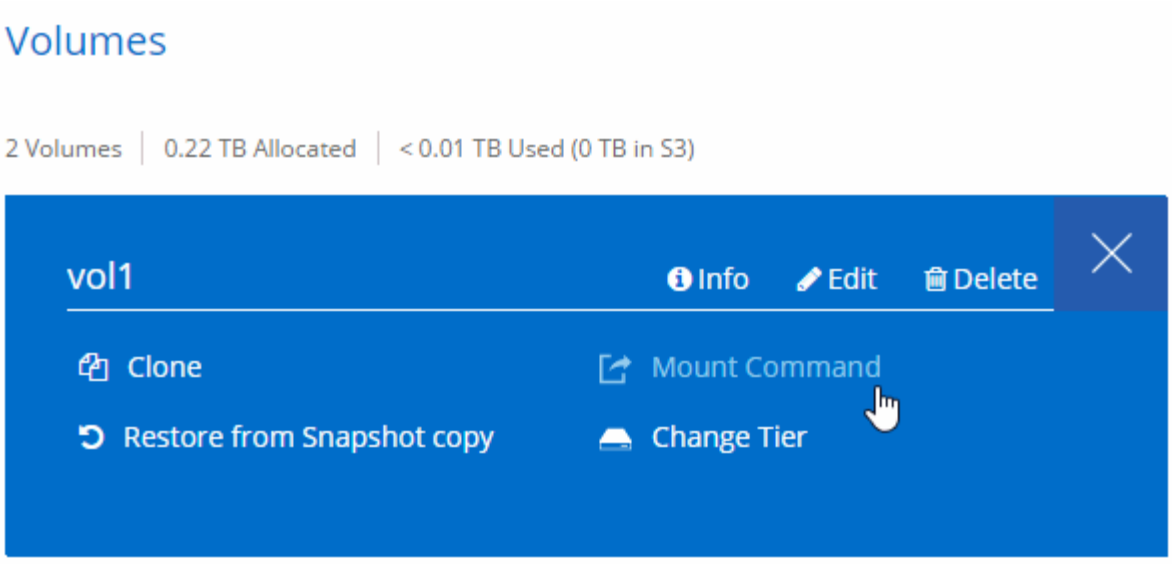
Pour plus d'informations sur les performances de Cloud Volumes ONTAP, reportez-vous à "Performance".

Accès client au stockage

Les clients doivent accéder aux volumes NFS et CIFS en utilisant l'adresse IP de données du nœud sur lequel réside le volume. Si les clients NAS accèdent à un volume en utilisant l'adresse IP du nœud partenaire, le trafic passe entre les deux nœuds, ce qui réduit les performances.

Si vous déplacez un volume entre les nœuds d'une paire HA, vous devez remonter le volume en utilisant l'adresse IP de l'autre nœud. Sinon, vous pouvez bénéficier d'une performance réduite. Si les clients prennent en charge les renvois NFSv4 ou la redirection de dossiers pour CIFS, vous pouvez activer ces fonctionnalités sur les systèmes Cloud Volumes ONTAP pour éviter de remanier le volume. Pour plus d'informations, consultez la documentation ONTAP.

Vous pouvez facilement identifier l'adresse IP correcte dans Cloud Manager :

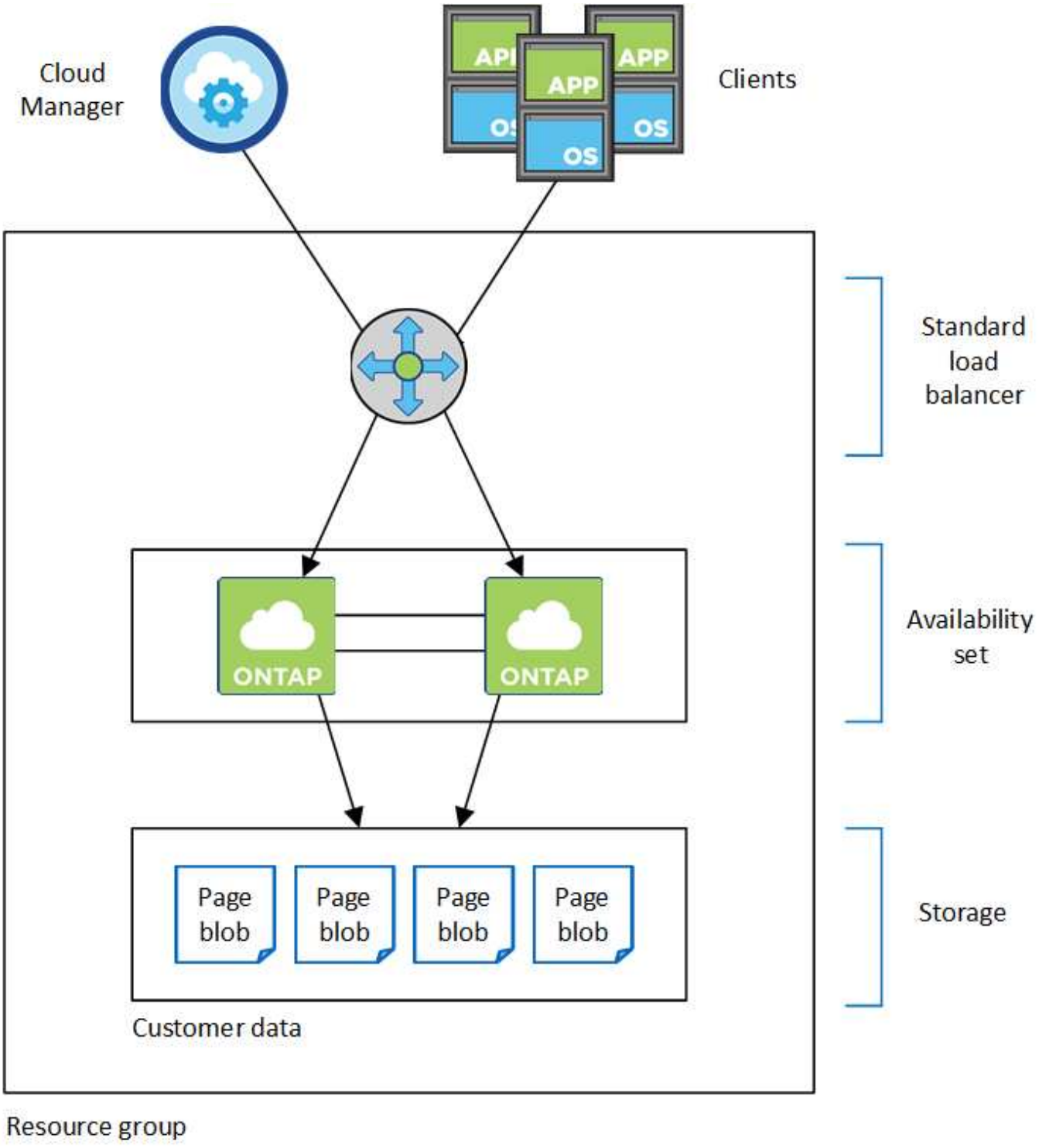


Paires haute disponibilité dans Azure

Une paire haute disponibilité Cloud Volumes ONTAP offre une fiabilité exceptionnelle et la continuité de l'activité en cas de défaillances dans votre environnement cloud. Dans Azure, le stockage est partagé entre les deux nœuds.

Composants DE HAUTE DISPONIBILITÉ

Une configuration Cloud Volumes ONTAP HA dans Azure inclut les composants suivants :



Les composants Azure que Cloud Manager déploie sont les suivants :

Équilibreur de la charge Azure Standard

Le répartiteur de charge gère le trafic entrant vers la paire haute disponibilité Cloud Volumes ONTAP.

Ensemble de disponibilité

L'ensemble de disponibilité garantit que les nœuds se trouvent dans des domaines de panne et de mise à jour différents.

Disques

Les données client résident sur les blobs de la page Premium Storage. Chaque nœud a accès au stockage de l'autre nœud. Du stockage supplémentaire est également requis pour "des données « boot », « root » et « core »".

Comptes de stockage

- Un seul compte de stockage est nécessaire pour les disques gérés.
- Un ou plusieurs comptes de stockage sont requis pour les blobs de la page stockage Premium, car la limite de capacité de disque par compte de stockage est atteinte.

  "Documentation Azure : objectifs d'évolutivité et de performances du stockage Azure pour les comptes de stockage".

- Un seul compte de stockage est nécessaire pour le Tiering des données vers le stockage Azure Blob.
- Depuis Cloud Volumes ONTAP 9.7, les comptes de stockage créés par Cloud Manager pour les paires HA sont des comptes de stockage v2 à usage général.
- Vous pouvez activer une connexion HTTPS à partir d'une paire haute disponibilité Cloud Volumes ONTAP 9.7 vers des comptes de stockage Azure lors de la création d'un environnement de travail. Notez que l'activation de cette option peut avoir un impact sur les performances d'écriture. Vous ne pouvez pas modifier le paramètre après avoir créé l'environnement de travail.

RPO et RTO

Une configuration haute disponibilité maintient la haute disponibilité de vos données comme suit :

- L'objectif du point de récupération (RPO) est de 0 seconde. Vos données sont transactionnaires, sans perte de données.
- L'objectif de temps de récupération (RTO) est de 60 secondes. En cas de panne, les données doivent être disponibles en 60 secondes ou moins.

Reprise et remise du stockage

À l'instar d'un cluster ONTAP physique, le stockage d'une paire HA Azure est partagé entre les nœuds. Des connexions au stockage du partenaire permettent à chaque nœud d'accéder au stockage de l'autre nœud dans le cas d'un *basculement*. Les mécanismes de basculement de chemin réseau garantissent que les clients et les hôtes continuent de communiquer avec le nœud survivant. Le partenaire *fournit* du stockage supplémentaire lorsque le nœud est revenu en ligne.

Pour les configurations NAS, les adresses IP des données migrent automatiquement entre les nœuds haute disponibilité en cas de défaillance.

Pour iSCSI, Cloud Volumes ONTAP utilise les E/S multichemins (MPIO) et l'accès aux unités logiques asymétriques (ALUA) pour gérer le basculement de chemin entre les chemins optimisés et non optimisés.

Pour plus d'informations sur les configurations hôtes spécifiques qui prennent en charge ALUA, consultez le "Matrice d'interopérabilité NetApp" Et le Guide d'installation et de configuration des utilitaires hôtes pour votre système d'exploitation hôte.

Configurations de stockage

Vous pouvez utiliser une paire HA comme configuration active-active, dans laquelle les deux nœuds servent les données aux clients ou comme configuration active-passive, dans laquelle le nœud passif répond aux

demandes de données uniquement s'il a pris en charge le stockage pour le nœud actif.

Limitations de LA HAUTE DISPONIBILITÉ

Les limites suivantes affectent les paires HA Cloud Volumes ONTAP dans Azure :

- Les paires HAUTE DISPONIBILITÉ sont prises en charge avec Cloud Volumes ONTAP Standard, Premium et BYOL. Explorer n'est pas pris en charge.
- NFSv4 n'est pas pris en charge. NFSv3 est pris en charge.
- Les paires HA ne sont pas prises en charge dans certaines régions.

  "Consultez la liste des régions Azure prises en charge".

"Découvrez comment déployer un système HA dans Azure".

L'évaluation

Vous pouvez évaluer Cloud Volumes ONTAP avant d'investir dans le logiciel. La manière la plus courante est de lancer la version PAYGO de votre premier système Cloud Volumes ONTAP pour bénéficier d'un essai gratuit de 30 jours. Une licence d'évaluation BYOL est également proposée en option.

Si vous avez besoin d'aide concernant votre démonstration de faisabilité, contactez "Les équipes commerciales" ou accédez à l'option de chat disponible sur "NetApp Cloud Central" Et depuis Cloud Manager.

Essais gratuits de 30 jours pour PAYGO

Un essai gratuit de 30 jours est disponible si vous prévoyez de payer pour Cloud Volumes ONTAP au fur et à mesure. Pour commencer une version d'évaluation gratuite de 30 jours de Cloud Volumes ONTAP depuis Cloud Manager, vous pouvez créer votre premier système Cloud Volumes ONTAP sur le compte d'un payeur.

Il n'y a pas de frais de licence logicielle à l'heure, mais des frais d'infrastructure facturés par votre fournisseur cloud s'appliquent toujours.

Un essai gratuit est automatiquement converti en abonnement horaire payé à la date d'expiration. Si vous arrêtez l'instance dans le délai imparti, l'instance suivante que vous déployez ne fait pas partie de l'essai gratuit (même si elle est déployée dans les 30 jours).

Les essais avec paiement à l'utilisation sont effectués par un fournisseur cloud et ne peuvent être extensibles par aucun moyen.

Licences d'évaluation pour BYOL

Une licence d'évaluation BYOL est adaptée aux clients qui prévoient de payer pour Cloud Volumes ONTAP en achetant une licence appelée NetApp. Votre équipe de gestion de compte, votre ingénieur commercial ou votre partenaire vous permet d'obtenir une licence d'évaluation.

La clé d'évaluation est bonne pendant 30 jours et peut être utilisée plusieurs fois, chacune pendant 30 jours (indépendamment du jour de création).

À la fin de 30 jours, des arrêts quotidiens se produisent, il est donc préférable de prévoir à l'avance. Vous pouvez appliquer une nouvelle licence BYOL à la licence d'évaluation pour une mise à niveau sans déplacement des données (redémarrage obligatoire des systèmes à un seul nœud). Vos données hébergées

sont **non** supprimées à la fin de la période d'essai.

Vous ne pouvez pas mettre à niveau le logiciel Cloud Volumes ONTAP lors de l'utilisation d'une licence d'évaluation.

Licences

Chaque système Cloud Volumes ONTAP BYOL doit être équipé d'une licence système installée avec un abonnement actif. Cloud Manager simplifie le processus en gérant les licences pour vous et en vous informant avant leur expiration. Les licences BYOL sont également disponibles pour la sauvegarde dans le cloud.

Licences de système BYOL

Vous pouvez acheter plusieurs licences pour un système Cloud Volumes ONTAP BYOL pour allouer plus de 368 To de capacité. Par exemple, vous pouvez acheter deux licences pour allouer une capacité allant jusqu'à 736 To à Cloud Volumes ONTAP. Vous pouvez également acheter quatre licences pour obtenir jusqu'à 1.4 po.

Le nombre de licences que vous pouvez acheter pour un système à un seul nœud ou une paire HA est illimité.

Notez que les limites de disques peuvent vous empêcher d'atteindre la limite de capacité en utilisant des disques seuls. Vous pouvez aller au-delà de la limite des disques de "tiering des données inactives vers le stockage objet". Pour plus d'informations sur les limites de disques, reportez-vous à la section "Limites de stockage dans les notes de mise à jour de Cloud Volumes ONTAP".

Gestion des licences pour un nouveau système

Lorsque vous créez un système BYOL, Cloud Manager vous demande le numéro de série de votre licence et votre compte sur le site de support NetApp. Cloud Manager utilise ce compte pour télécharger le fichier de licence de NetApp et l'installer sur le système Cloud Volumes ONTAP.

"Découvrez comment ajouter des comptes au site de support NetApp à Cloud Manager".

Si Cloud Manager ne peut pas accéder au fichier de licence via la connexion Internet sécurisée, vous pouvez obtenir le fichier vous-même, puis le charger manuellement dans Cloud Manager. Pour obtenir des instructions, reportez-vous à la section "Gestion des licences BYOL pour Cloud Volumes ONTAP".

Avertissement d'expiration de licence

Cloud Manager vous avertit 30 jours avant l'expiration d'une licence, puis à nouveau à l'expiration de la licence. L'image suivante montre un avertissement d'expiration de 30 jours :

Vous pouvez sélectionner l'environnement de travail pour consulter le message.

Si vous ne renouvelez pas la licence à temps, le système Cloud Volumes ONTAP s'arrête. Si vous le

redémarrez, il s'arrête de nouveau.

> Cloud Volumes ONTAP peut également vous avertir par e-mail, par un poste SNMP ou par un serveur syslog à l'aide de notifications d'événements EMS (Event Management System). Pour obtenir des instructions, reportez-vous au "Guide de configuration rapide de ONTAP 9 EMS".

Renouvellement de la licence

Lorsque vous renouvelez un abonnement BYOL en contactant un représentant NetApp, Cloud Manager obtient automatiquement la nouvelle licence auprès de NetApp et l'installe sur le système Cloud Volumes ONTAP.

Si Cloud Manager ne peut pas accéder au fichier de licence via la connexion Internet sécurisée, vous pouvez obtenir le fichier vous-même, puis le charger manuellement dans Cloud Manager. Pour obtenir des instructions, reportez-vous à la section "Gestion des licences BYOL pour Cloud Volumes ONTAP".

Licences de sauvegarde BYOL

Une licence de sauvegarde BYOL permet d'acheter une licence auprès de NetApp, afin d'utiliser Backup to Cloud pendant une certaine période et pour un espace de sauvegarde maximal. Lorsque l'une ou l'autre limite est atteinte, vous devez renouveler la licence.

"En savoir plus sur la licence BYOL Backup to Cloud".

Sécurité

Cloud Volumes ONTAP prend en charge le cryptage des données et protège contre les virus et les attaques par ransomware.

Cryptage des données au repos

Cloud Volumes ONTAP prend en charge les technologies de cryptage suivantes :

- Solutions de chiffrement NetApp (NVE et NAE)
- Service de gestion des clés AWS
- Chiffrement de service de stockage Azure
- Chiffrement par défaut Google Cloud Platform

Vous pouvez utiliser les solutions de chiffrement NetApp avec le chiffrement natif d'AWS, Azure ou GCP, qui chiffrer les données au niveau de l'hyperviseur. Cela permettrait de fournir un double chiffrement, ce qui peut être souhaité pour des données très sensibles. Lors de l'accès aux données chiffrées, elles sont non chiffrées à deux reprises au niveau de l'hyperviseur (à l'aide de clés fournies par le fournisseur cloud), puis à l'aide des solutions de chiffrement NetApp (à l'aide de clés fournies par un gestionnaire de clés externe).

Solutions de chiffrement NetApp (NVE et NAE)

Cloud Volumes ONTAP prend en charge NVE (NetApp Volume Encryption) et NAE (NetApp Aggregate Encryption) avec un gestionnaire de clés externe. NVE et NAE sont des solutions logicielles qui permettent le chiffrement des données au repos (conformes à la norme FIPS) de volumes 140-2.

- NVE chiffre les données au repos un volume à la fois. Chaque volume de données dispose de sa propre clé de chiffrement unique.

- NAE est une extension de NVE qui chiffre les données pour chaque volume, tandis que les volumes partagent une clé dans l'ensemble de l'agrégat. NAE permet également la déduplication de blocs communs à tous les volumes de l'agrégat.

NVE et NAE utilisent tous deux le chiffrement AES 256 bits.

"En savoir plus sur NetApp Volume Encryption et NetApp Aggregate Encryption".

Depuis Cloud Volumes ONTAP 9.7, le chiffrement d'agrégat NetApp (NAE) est activé par défaut après la configuration d'un gestionnaire de clés externe. Pour les nouveaux volumes qui ne font pas partie d'un agrégat NAE, NetApp Volume Encryption (NVE) est activé par défaut (par exemple, si des agrégats existants ont été créés avant de configurer un gestionnaire de clés externe).

La configuration d'un gestionnaire de clés pris en charge est la seule étape requise. Pour obtenir des instructions de configuration, reportez-vous à la section "Cryptage de volumes grâce aux solutions de cryptage NetApp".

Service de gestion des clés AWS

Lorsque vous lancez un système Cloud Volumes ONTAP dans AWS, vous pouvez activer le chiffrement des données à l'aide du "AWS Key Management Service (KMS)". Cloud Manager demande des clés de données à l'aide d'une clé principale client (CMK).

Une fois que vous avez créé un système Cloud Volumes ONTAP, vous ne pouvez pas modifier la méthode de chiffrement des données AWS.

Si vous souhaitez utiliser cette option de cryptage, vous devez vous assurer que le système AWS KMS est correctement configuré. Pour plus de détails, voir "Configuration du système AWS KMS".

Chiffrement de service de stockage Azure

"Chiffrement de service de stockage Azure" Les données au repos sont activées par défaut pour les données Cloud Volumes ONTAP dans Azure. Aucune configuration n'est requise.

Vous pouvez chiffrer les disques gérés Azure sur des systèmes Cloud Volumes ONTAP à un seul nœud à l'aide de clés externes provenant d'un autre compte. Cette fonctionnalité est prise en charge à l'aide des API Cloud Manager.

Lors de la création du système à un nœud, il vous suffit d'ajouter ce qui suit à la demande d'API :

```
"azureEncryptionParameters": {
      "key": <azure id of encryptionset>
  }
```

Les clés gérées par le client ne sont pas prises en charge avec les paires haute disponibilité Cloud Volumes ONTAP.

Chiffrement par défaut Google Cloud Platform

"Chiffrement des données au repos Google Cloud Platform" Est activé par défaut pour Cloud Volumes ONTAP. Aucune configuration n'est requise.

Google Cloud Storage chiffre toujours vos données avant leur écriture sur le disque, mais vous pouvez utiliser les API Cloud Manager pour créer un système Cloud Volumes ONTAP qui utilise des clés de chiffrement *gérées par le client*. Il s'agit des clés que vous créez et gérez dans GCP à l'aide du service Cloud Key Management. "En savoir plus >>".

Analyse antivirus ONTAP

Vous pouvez utiliser la fonctionnalité antivirus intégrée sur les systèmes ONTAP pour protéger les données contre les virus ou tout autre code malveillant.

L'analyse antivirus ONTAP, appelée *Vscan*, associe le meilleur logiciel antivirus tiers à des fonctionnalités ONTAP, vous offrant ainsi la flexibilité nécessaire pour contrôler quels fichiers sont analysés et à quel moment.

Pour plus d'informations sur les fournisseurs, les logiciels et les versions pris en charge par Vscan, voir le "Matrice d'interopérabilité NetApp".

Pour plus d'informations sur la configuration et la gestion de la fonctionnalité antivirus sur les systèmes ONTAP, consultez la "Guide de configuration antivirus ONTAP 9".

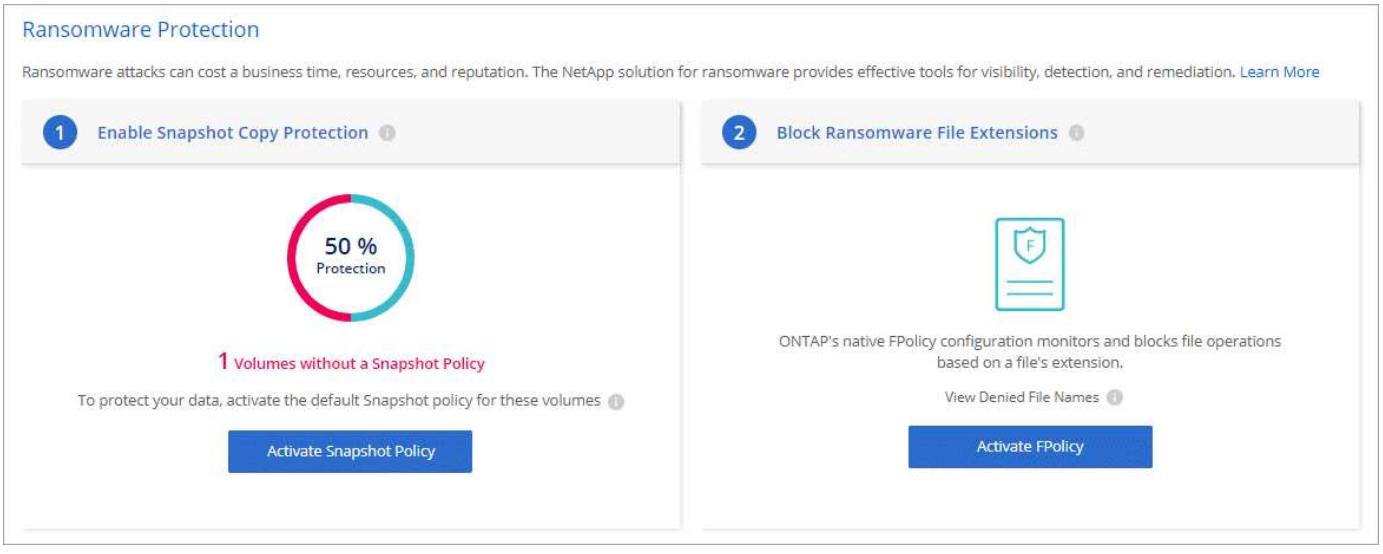
Protection par ransomware

Les attaques par ransomware peuvent coûter du temps, des ressources et de la réputation à l'entreprise. Cloud Manager vous permet d'implémenter la solution NetApp contre les attaques par ransomware qui fournit des outils efficaces pour la visibilité, la détection et la résolution de problèmes.

- Cloud Manager identifie les volumes qui ne sont pas protégés par une règle Snapshot et vous permet d'activer la règle Snapshot par défaut sur ces volumes.

  Les copies Snapshot sont en lecture seule, ce qui empêche la corruption par ransomware. Ils peuvent également assurer la granularité pour créer des images d'une copie de fichiers unique ou d'une solution complète de reprise après incident.

- Cloud Manager vous permet également de bloquer les extensions de fichiers ransomware courantes en activant la solution FPolicy d'ONTAP.



"Découvrez comment implémenter la solution NetApp contre les attaques par ransomware".

Performance

Vous pouvez consulter les résultats des performances pour déterminer les charges de travail appropriées à Cloud Volumes ONTAP.

- Cloud Volumes ONTAP pour AWS

  "Rapport technique NetApp 4383 : caractérisation des performances de Cloud Volumes ONTAP dans Amazon Web Services avec des charges de travail applicatives".

- Cloud Volumes ONTAP pour Microsoft Azure

  "Rapport technique NetApp 4671 : caractérisation des performances de Cloud Volumes ONTAP dans Azure avec les charges de travail applicatives".

- Cloud Volumes ONTAP pour Google Cloud

  "Rapport technique NetApp 4816 : caractérisation des performances d'Cloud Volumes ONTAP pour Google Cloud".

Configuration par défaut pour Cloud Volumes ONTAP

La configuration par défaut de Cloud Volumes ONTAP peut vous aider à configurer et administrer vos systèmes, surtout si vous connaissez ONTAP, car la configuration par défaut de Cloud Volumes ONTAP est différente de ONTAP.

Valeurs par défaut

- Cloud Volumes ONTAP est disponible en tant que système à un seul nœud dans AWS, Azure et GCP, ainsi qu'en tant que paire HA dans AWS et Azure.
- Cloud Manager crée une VM de stockage accessible aux données lorsqu'elle déploie Cloud Volumes ONTAP. Certaines configurations prennent en charge des machines virtuelles de stockage supplémentaires. "En savoir plus sur la gestion des machines virtuelles de stockage".
- Cloud Manager installe automatiquement les licences de fonctionnalités ONTAP suivantes sur Cloud Volumes ONTAP :
  - CIFS
  - FlexCache
  - FlexClone
  - ISCSI
  - Chiffrement de volume NetApp (uniquement pour les systèmes BYOL ou enregistrés de PAYGO)
  - NFS
  - SnapMirror
  - SnapRestore
  - SnapVault
- Plusieurs interfaces réseau sont créées par défaut :
  - Un LIF de gestion de cluster

- Un FRV intercluster
- Une LIF de gestion SVM sur des systèmes HA dans Azure, des systèmes à un seul nœud dans AWS, et en option sur des systèmes HA dans plusieurs zones de disponibilité AWS
- Un LIF de gestion des nœuds
- Un LIF de données iSCSI
- Un LIF de données CIFS et NFS

> Le basculement LIF est désactivé par défaut pour Cloud Volumes ONTAP en raison des exigences d'EC2. La migration d'un LIF vers un port différent rompt le mappage externe entre les adresses IP et les interfaces réseau de l'instance, ce qui rend le LIF inaccessible.

- Cloud Volumes ONTAP envoie des sauvegardes de configuration au connecteur via HTTPS.

  Les sauvegardes sont accessibles à partir de https://ipaddress/occm/offboxconfig/ Où *ipaddress* est l'adresse IP de l'hôte du connecteur.

- Cloud Manager définit quelques attributs de volume différemment des autres outils de gestion (System Manager ou CLI, par exemple).

  Le tableau suivant répertorie les attributs de volume définis par Cloud Manager différemment des valeurs par défaut :

Attribut	Valeur définie par Cloud Manager
Mode Autosize	Grandir
Positionnement automatique maximum	1 000 pour cent L'administrateur du compte peut modifier cette valeur à partir de la page Paramètres.
Style de sécurité	NTFS pour les volumes CIFS UNIX pour les volumes NFS
Style de garantie de l'espace	Aucune
Autorisations UNIX (NFS uniquement)	776

  Pour plus d'informations sur ces attributs, reportez-vous à la page *volume create* man.

Données de démarrage et de racine pour Cloud Volumes ONTAP

Outre le stockage des données utilisateur, Cloud Manager achète également du stockage cloud pour le démarrage et les données root sur chaque système Cloud Volumes ONTAP.

AWS

- Deux disques par nœud pour les données de démarrage et racines :
  - 9.7 : disque io1 de 160 Go pour les données de démarrage et disque gp2 de 220 Go pour les données racine
  - 9.6 : disque io1 de 93 Go pour les données de démarrage et disque gp2 de 140 Go pour les données racine
  - 9.5 : disque io1 de 45 Go pour les données de démarrage et disque gp2 de 140 Go pour les données racine
- Un instantané EBS pour chaque disque d'initialisation et disque racine
- Pour les paires HA, un volume EBS pour l'instance Mediator, qui est d'environ 8 Go

Azure (un seul nœud)

- Trois disques SSD Premium :
  - Un disque de 10 Go pour les données de démarrage
  - Un disque de 140 Go pour les données racines
  - Un disque de 128 Go pour NVRAM

    Si la machine virtuelle que vous avez choisie pour Cloud Volumes ONTAP prend en charge les disques SSD Ultra, le système utilise un disque SSD Ultra pour la NVRAM, plutôt qu'un disque SSD premium.
- Un disque dur standard de 1024 Go pour économiser les cœurs
- Un snapshot Azure pour chaque disque d'initialisation et disque racine

Azure (paires HA)

- Deux disques SSD premium de 10 Go pour le volume de démarrage (un par nœud)
- Deux blobs de page de stockage Premium de 140 Go pour le volume racine (un par nœud)
- Deux disques durs standard de 1024 Go pour économiser les cœurs (un par nœud)
- Deux disques SSD premium de 128 Go pour la NVRAM (un par nœud)
- Un snapshot Azure pour chaque disque d'initialisation et disque racine

GCP

- Un disque persistant standard de 10 Go pour les données de démarrage
- Un disque persistant standard de 64 Go pour les données racines
- Un disque persistant standard de 500 Go pour la NVRAM
- Un disque persistant standard de 216 Go pour la sauvegarde des cœurs
- Un snapshot GCP chacun pour le disque de démarrage et le disque racine

Où résident les disques

Cloud Manager dispose du stockage comme suit :

- Les données de démarrage résident sur un disque relié à l'instance ou à la machine virtuelle.

  Ce disque, qui contient l'image d'amorçage, n'est pas disponible pour Cloud Volumes ONTAP.

- Les données root, qui contiennent la configuration du système et les journaux, résident dans aggr0.
- Le volume racine de la machine virtuelle de stockage (SVM) réside dans aggr1.
- Les volumes de données résident également dans aggr1.

Le cryptage

Les disques de démarrage et racine sont toujours cryptés dans Azure et Google Cloud Platform car le chiffrement est activé par défaut dans ces fournisseurs de Cloud.

Lorsque vous activez le chiffrement des données dans AWS à l'aide du service de gestion des clés (KMS), les disques racine et de démarrage pour Cloud Volumes ONTAP sont également chiffrés. Cela comprend le disque de démarrage de l'instance médiateur dans une paire HA. Les disques sont chiffrés à l'aide du CMK que vous sélectionnez lors de la création de l'environnement de travail.

Commencez dans AWS

Mise en route avec Cloud Volumes ONTAP pour AWS

Découvrez Cloud Volumes ONTAP pour AWS en quelques étapes.

Créer un connecteur

Si vous n'avez pas de "Connecteur" Cependant, un administrateur de compte doit en créer un. "Découvrez comment créer un connecteur dans AWS".

Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à déployer un connecteur si vous n'en possédez pas encore.

Planification de la configuration

Cloud Manager propose des packages préconfigurés qui répondent aux exigences de vos workloads, ou vous pouvez créer votre propre configuration. Dans ce dernier cas, il est important de connaître les options dont vous disposez. "En savoir plus >>".

Configurez votre réseau

1. Vérifiez que votre VPC et vos sous-réseaux prennent en charge la connectivité entre le connecteur et Cloud Volumes ONTAP.
2. Activez l'accès Internet sortant à partir du VPC cible de sorte que le connecteur et le Cloud Volumes ONTAP puissent contacter plusieurs terminaux.

   Cette étape est importante car le connecteur ne peut pas gérer Cloud Volumes ONTAP sans accès Internet sortant. Si vous devez limiter la connectivité sortante, reportez-vous à la liste des noeuds finaux pour "Le connecteur et le Cloud Volumes ONTAP".

3. Configurez un terminal VPC sur le service S3.

Un point de terminaison VPC est requis si vous souhaitez transférer des données à froid de Cloud Volumes ONTAP vers un stockage objet économique.

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

Configuration du KMS AWS

Si vous souhaitez utiliser le chiffrement Amazon avec Cloud Volumes ONTAP, vous devez vous assurer qu'une clé principale client (CMK) active existe. Vous devez également modifier la stratégie de clé pour chaque CMK en ajoutant le rôle IAM qui fournit des autorisations au connecteur en tant qu'utilisateur *key*. "En savoir plus >>".

Lancez Cloud Volumes ONTAP à l'aide de Cloud Manager

Cliquez sur **Ajouter un environnement de travail**, sélectionnez le type de système que vous souhaitez déployer et suivez les étapes de l'assistant. "Lisez les instructions détaillées".

Liens connexes

- "L'évaluation"
- "Création d'un connecteur depuis Cloud Manager"
- "Lancement d'un connecteur depuis AWS Marketplace"
- "Installation du logiciel du connecteur sur un hôte Linux"
- "Ce que fait Cloud Manager avec les autorisations AWS"

Planification de votre configuration Cloud Volumes ONTAP dans AWS

Lorsque vous déployez Cloud Volumes ONTAP dans AWS, vous pouvez soit choisir un système préconfiguré qui correspond aux exigences de vos workloads, soit créer votre propre configuration. Dans ce dernier cas, il est important de connaître les options dont vous disposez.

Choix d'un type de licence

Deux options de tarification sont disponibles pour Cloud Volumes ONTAP : le paiement à l'utilisation ou le modèle BYOL (où vous apportez votre propre licence). Le paiement basé sur l'utilisation vous permet de choisir entre trois licences : explore, Standard ou Premium. Chacune d'elles fournit une capacité distincte et des options de calcul différentes.

"Configurations prises en charge pour Cloud Volumes ONTAP 9.7 dans AWS"

Compréhension des limites de stockage

La limite de capacité brute d'un système Cloud Volumes ONTAP dépend de la licence. Des limites supplémentaires ont un impact sur la taille des agrégats et des volumes. Il est important de connaître ces dernières lors de la planification de la configuration.

"Limites de stockage pour Cloud Volumes ONTAP 9.7 dans AWS"

Dimensionnement de votre système dans AWS

Le dimensionnement du système Cloud Volumes ONTAP permet de répondre à vos besoins de performance et de capacité. Quelques points clés sont à noter lors de la sélection d'un type d'instance, d'un type de disque et d'une taille de disque :

Type d'instance

- Assurez-vous que les exigences de vos workloads correspondent aux valeurs maximales de débit et d'IOPS pour chaque type d'instance EC2.
- Si plusieurs utilisateurs écrivent dans le système en même temps, choisissez un type d'instance disposant de suffisamment de processeurs pour gérer les requêtes.
- Si votre champ d'application implique essentiellement la lecture, optez pour un système disposant de suffisamment de mémoire RAM.
  - "Documentation AWS : types d'instances Amazon EC2"
  - "Documentation AWS : instances optimisées pour Amazon EBS"

Type de disque EBS

Les SSD à usage générique sont les types de disques les plus courants pour les systèmes Cloud Volumes ONTAP. Pour en savoir plus sur les utilisations des disques EBS, reportez-vous à la section "Documentation AWS : types de volume EBS".

Taille des disques EBS

Lorsque vous lancez un système Cloud Volumes ONTAP, vous devez choisir une taille de disque initiale. Après cela, vous pouvez "Laissez Cloud Manager gérer la capacité d'un système à votre place", mais si vous voulez "créez des agrégats vous-même", soyez conscient des éléments suivants :

- Tous les disques qui composent un agrégat doivent être de la même taille.
- Les performances des disques EBS sont liées à leur taille. La taille détermine les IOPS de base et la durée maximale en rafale pour les disques SSD, ainsi que le débit de base et en rafale pour les disques HDD.
- Finalement, vous devez choisir la taille de disque qui vous donne le *performances soutenues* dont vous avez besoin.
- Même si vous choisissez des disques de plus grande capacité (par exemple, six disques de 4 To), vous risquez de ne pas obtenir tous les IOPS, car l'instance EC2 peut atteindre sa limite de bande passante.

  Pour en savoir plus sur les performances des disques EBS, consultez la "Documentation AWS : types de volume EBS".

Pour plus d'informations sur le dimensionnement de votre système Cloud Volumes ONTAP dans AWS, visionnez la vidéo suivante :

[] | *https://img.youtube.com/vi/GELcXmOuYPw/maxresdefault.jpg*

Choix d'une configuration qui prend en charge Flash cache

Certaines configurations Cloud Volumes ONTAP dans AWS incluent le stockage NVMe local, utilisé par Cloud Volumes ONTAP *Flash cache* pour de meilleures performances. "En savoir plus sur Flash cache".

Fiche technique d’informations sur le réseau AWS

Lorsque vous lancez Cloud Volumes ONTAP dans AWS, vous devez spécifier des informations concernant votre réseau VPC. Vous pouvez utiliser un modèle pour recueillir ces informations auprès de votre administrateur.

Informations réseau pour Cloud Volumes ONTAP

Informations sur AWS	Votre valeur
Région	
VPC	
Sous-réseau	
Groupe de sécurité (s’il s’agit du vôtre)	

Informations réseau pour une paire HA dans plusieurs AZS

Informations sur AWS	Votre valeur
Région	
VPC	
Groupe de sécurité (s’il s’agit du vôtre)	
Zone de disponibilité du nœud 1	
Sous-réseau de nœud 1	
Zone de disponibilité du nœud 2	
Sous-réseau de nœud 2	
Zone de disponibilité d’un médiateur	
Sous-réseau médiateur	
Paire de touches pour le médiateur	
Adresse IP flottante pour le port de gestion du cluster	
Adresse IP flottante pour les données du nœud 1	
Adresse IP flottante pour les données du nœud 2	
Tables de routage pour les adresses IP flottantes	

Sélection d'une vitesse d'écriture

Cloud Manager permet de choisir un paramètre de vitesse d'écriture pour les systèmes Cloud Volumes ONTAP à un seul nœud. Avant de choisir une vitesse d'écriture, vous devez comprendre les différences entre les paramètres normaux et élevés et les risques et les recommandations lors de l'utilisation de la vitesse d'écriture élevée.

Différence entre une vitesse d'écriture standard et une vitesse d'écriture élevée

Lorsque vous choisissez la vitesse d'écriture standard, les données sont écrites directement sur le disque, réduisant ainsi le risque de perte de données en cas d'interruption imprévue du système.

Lorsque vous choisissez la vitesse d'écriture élevée, les données sont mises en tampon dans la mémoire avant d'être écrites sur le disque, ce qui accélère les performances d'écriture. Toutefois, la mise en cache peut entraîner une perte de données en cas de panne système.

Le volume de données pouvant être perdues en cas de panne système correspond à l'étendue des deux derniers points de cohérence. Le point de cohérence consiste à écrire des données mises en tampon sur le disque. Un point de cohérence se produit lorsque le journal d'écriture est plein ou après 10 secondes (selon la première éventualité). Cependant, la performance des volumes AWS EBS peut affecter le temps de traitement des points de cohérence.

Quand utiliser une vitesse d'écriture élevée

Optez pour la vitesse d'écriture élevée si vos workloads nécessitent des performances d'écriture rapides et que vous ne craignez pas de perdre des données.

Recommandations lors de l'utilisation d'une vitesse d'écriture élevée

Si vous activez la vitesse d'écriture élevée, vous devez assurer la protection de l'écriture au niveau de la couche applicative.

Choix d'un profil d'utilisation du volume

ONTAP comprend plusieurs fonctionnalités d'efficacité du stockage qui permettent de réduire la quantité totale de stockage nécessaire. Lorsque vous créez un volume dans Cloud Manager, vous pouvez choisir un profil qui active ou désactive ces fonctionnalités. Vous devez en savoir plus sur ces fonctionnalités pour vous aider à choisir le profil à utiliser.

Les fonctionnalités d'efficacité du stockage NetApp offrent les avantages suivants :

Provisionnement fin
: Met à la disposition des hôtes ou des utilisateurs une quantité de stockage logique supérieure au stockage effectivement présent dans votre pool physique. L'espace de stockage est alloué de manière dynamique, et non au préalable, à chaque volume lors de l'écriture des données.

Déduplication
: Améliore l'efficacité en identifiant les blocs de données identiques et en les remplaçant par des références à un seul bloc partagé. Cette technique réduit les besoins de stockage en éliminant les blocs de données redondants qui résident dans le même volume.

Compression
: Réduit la capacité physique requise pour stocker les données en les compressant dans un volume sur un stockage primaire, secondaire ou d'archivage.

Configurez votre réseau

Configuration réseau requise pour Cloud Volumes ONTAP dans AWS

Configurez votre réseau AWS pour que les systèmes Cloud Volumes ONTAP puissent fonctionner correctement.

Conditions générales requises pour Cloud Volumes ONTAP

Les exigences suivantes doivent être respectées dans AWS.

Accès Internet sortant pour les nœuds Cloud Volumes ONTAP

Les nœuds Cloud Volumes ONTAP nécessitent un accès Internet sortant pour envoyer des messages à NetApp AutoSupport, qui surveille de façon proactive l'état de votre stockage.

Les règles de routage et de pare-feu doivent autoriser le trafic AWS HTTP/HTTPS vers les terminaux suivants pour que Cloud Volumes ONTAP puisse envoyer les messages AutoSupport :

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

  Si vous disposez d'une instance NAT, vous devez définir une règle de groupe de sécurité entrante qui autorise le trafic HTTPS du sous-réseau privé vers Internet.

  "Découvrez comment configurer AutoSupport".

Accès Internet sortant pour le médiateur haute disponibilité

L'instance de médiateur haute disponibilité doit disposer d'une connexion sortante au service AWS EC2 pour qu'il puisse faciliter le basculement du stockage. Pour fournir la connexion, vous pouvez ajouter une adresse IP publique, spécifier un serveur proxy ou utiliser une option manuelle.

L'option manuelle peut être une passerelle NAT ou un terminal VPC d'interface, du sous-réseau cible au service AWS EC2. Pour plus de détails sur les terminaux VPC, reportez-vous à "Documentation AWS : terminaux VPC d'interface (AWS PrivateLink)".

Nombre d'adresses IP

Cloud Manager attribue le nombre suivant d'adresses IP à Cloud Volumes ONTAP dans AWS :

- Un seul nœud : 6 adresses IP
- Paires HA en simple AZS : 15 adresses
- Paires HAUTE DISPONIBILITÉ dans plusieurs adresses AZS : 15 ou 16 adresses IP

  Notez que Cloud Manager crée une LIF de gestion des SVM sur des systèmes à un seul nœud, mais pas sur des paires haute disponibilité dans une même zone de disponibilité. Vous pouvez choisir de créer ou non une LIF de gestion SVM sur des paires HA dans plusieurs AZS.

  Une LIF est une adresse IP associée à un port physique. Une LIF de gestion SVM est nécessaire pour les outils de gestion tels que SnapCenter.

Groupes de sécurité

Vous n'avez pas besoin de créer de groupes de sécurité car Cloud Manager le fait pour vous. Si vous devez utiliser votre propre, reportez-vous à la section "Règles de groupe de sécurité".

Connexion de Cloud Volumes ONTAP à AWS S3 pour le hiérarchisation des données

Si vous souhaitez utiliser EBS comme niveau de performance et AWS S3 comme niveau de capacité, vous devez vous assurer que Cloud Volumes ONTAP est connecté à S3. La meilleure façon de fournir cette connexion est de créer un terminal VPC vers le service S3. Pour obtenir des instructions, reportez-vous à la section "Documentation AWS : création d'un terminal de passerelle".

Lorsque vous créez le terminal VPC, veillez à sélectionner la région, le VPC et la table de routage correspondant à l'instance Cloud Volumes ONTAP. Vous devez également modifier le groupe de sécurité pour ajouter une règle HTTPS sortante qui active le trafic vers le terminal S3. Dans le cas contraire, Cloud Volumes ONTAP ne peut pas se connecter au service S3.

Si vous rencontrez des problèmes, reportez-vous à la section "Centre de connaissances du support AWS : pourquoi ne puis-je pas me connecter à un compartiment S3 à l'aide d'un terminal VPC de passerelle ?"

Connexions aux systèmes ONTAP dans d'autres réseaux

Pour répliquer des données entre un système Cloud Volumes ONTAP dans AWS et ONTAP sur d'autres réseaux, vous devez disposer d'une connexion VPN entre AWS VPC et l'autre réseau, par exemple Azure VNet ou votre réseau d'entreprise. Pour obtenir des instructions, reportez-vous à la section "Documentation AWS : configuration d'une connexion VPN AWS".

DNS et Active Directory pour CIFS

Si vous souhaitez provisionner le stockage CIFS, vous devez configurer DNS et Active Directory dans AWS ou étendre votre configuration sur site à AWS.

Le serveur DNS doit fournir des services de résolution de noms pour l'environnement Active Directory. Vous pouvez configurer les jeux d'options DHCP pour qu'ils utilisent le serveur DNS EC2 par défaut, qui ne doit pas être le serveur DNS utilisé par l'environnement Active Directory.

Pour obtenir des instructions, reportez-vous à la section "Documentation AWS : active Directory Domain Services sur le cloud AWS : déploiement de référence rapide".

Besoins en paires haute disponibilité dans plusieurs AZS

D'autres exigences de mise en réseau AWS s'appliquent aux configurations Cloud Volumes ONTAP HA qui utilisent plusieurs zones de disponibilité (AZS). Avant de lancer une paire haute disponibilité, vous devez consulter ces exigences car vous devez saisir les informations de mise en réseau dans Cloud Manager.

Pour comprendre le fonctionnement des paires haute disponibilité, voir "Paires haute disponibilité".

Zones de disponibilité

Ce modèle de déploiement haute disponibilité utilise plusieurs AZS pour assurer la haute disponibilité de vos données. Vous devez utiliser un système AZ dédié pour chaque instance Cloud Volumes ONTAP et l'instance médiateur, qui fournit un canal de communication entre la paire HA.

Adresses IP flottantes pour les données NAS et la gestion de cluster/SVM

Les configurations HAUTE DISPONIBILITÉ de plusieurs AZS utilisent des adresses IP flottantes qui migrent entre les nœuds en cas de défaillance. Sauf vous, ils ne sont pas accessibles de manière native depuis l'extérieur du VPC "Configuration d'une passerelle de transit AWS".

Une adresse IP flottante concerne la gestion du cluster, l'une concerne les données NFS/CIFS sur le nœud

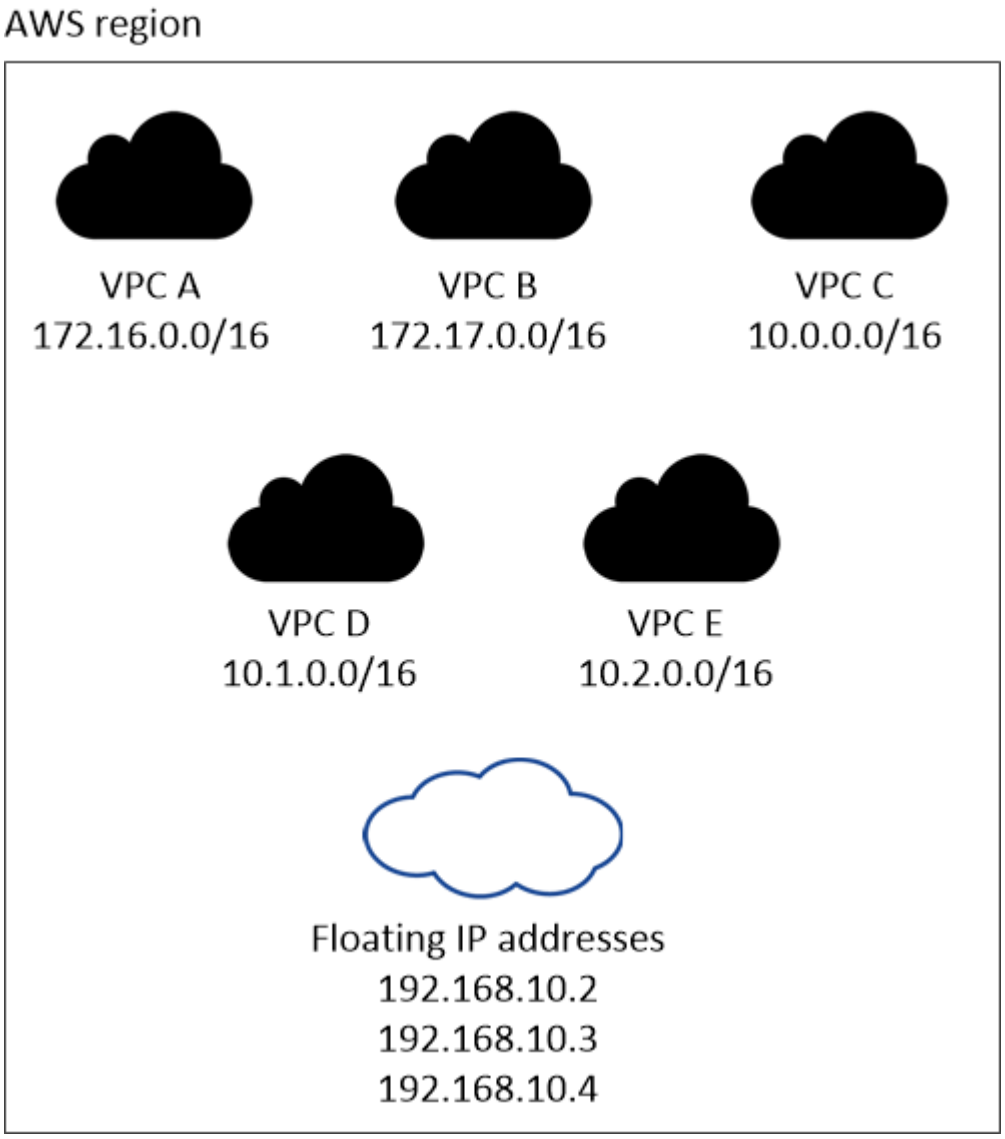
1 et l'autre les données NFS/CIFS sur le nœud 2. Une quatrième adresse IP flottante est facultative pour la gestion des SVM.

> Une adresse IP flottante est requise pour la LIF de management du SVM si vous utilisez SnapDrive pour Windows ou SnapCenter avec la paire haute disponibilité. Si vous ne spécifiez pas l'adresse IP lors du déploiement du système, vous pouvez créer la LIF plus tard. Pour plus de détails, voir "Configuration de Cloud Volumes ONTAP".

Vous devez saisir les adresses IP flottantes dans Cloud Manager lors de la création d'un environnement de travail Cloud Volumes ONTAP HA. Cloud Manager alloue les adresses IP à la paire HA lors du lancement du système.

Les adresses IP flottantes doivent être en dehors des blocs CIDR sur tous les VPC de la région AWS dans laquelle vous déployez la configuration HA. Considérez les adresses IP flottantes comme un sous-réseau logique en dehors des VPC de votre région.

L'exemple suivant illustre la relation entre les adresses IP flottantes et les VPC d'une région AWS. Alors que les adresses IP flottantes sont en dehors des blocs CIDR pour tous les VPC, elles sont routables vers les sous-réseaux via des tables de routage.



Cloud Manager crée automatiquement des adresses IP statiques pour l'accès iSCSI et pour l'accès NAS des clients en dehors du VPC. Vous n'avez pas besoin de répondre à des exigences relatives à ces types d'adresses IP.

Passerelle de transport pour activer l'accès IP flottant depuis l'extérieur du VPC

"Configuration d'une passerelle de transit AWS" Pour permettre l'accès aux adresses IP flottantes d'une paire haute disponibilité de l'extérieur du VPC où réside la paire haute disponibilité.

Tables de routage

Une fois que vous avez spécifié les adresses IP flottantes dans Cloud Manager, vous devez sélectionner les tables de route qui doivent inclure des routes vers les adresses IP flottantes. Cela permet au client d'accéder à la paire haute disponibilité.

Si vous n'avez qu'une seule table de routage pour les sous-réseaux dans votre VPC (la table de routage principale), Cloud Manager ajoute automatiquement les adresses IP flottantes à cette table de routage. Si vous avez plusieurs tables de routage, il est très important de sélectionner les tables de routage appropriées au lancement de la paire haute disponibilité. Dans le cas contraire, certains clients n'ont peut-être pas accès à Cloud Volumes ONTAP.

Par exemple, vous pouvez avoir deux sous-réseaux associés à différentes tables de routage. Si vous sélectionnez la table de routage A, mais pas la table de routage B, les clients du sous-réseau associé à la table de routage A peuvent accéder à la paire HA, mais les clients du sous-réseau associé à la table de routage B ne peuvent pas.

Pour plus d'informations sur les tables de routage, voir "Documentation AWS : tables de routage".

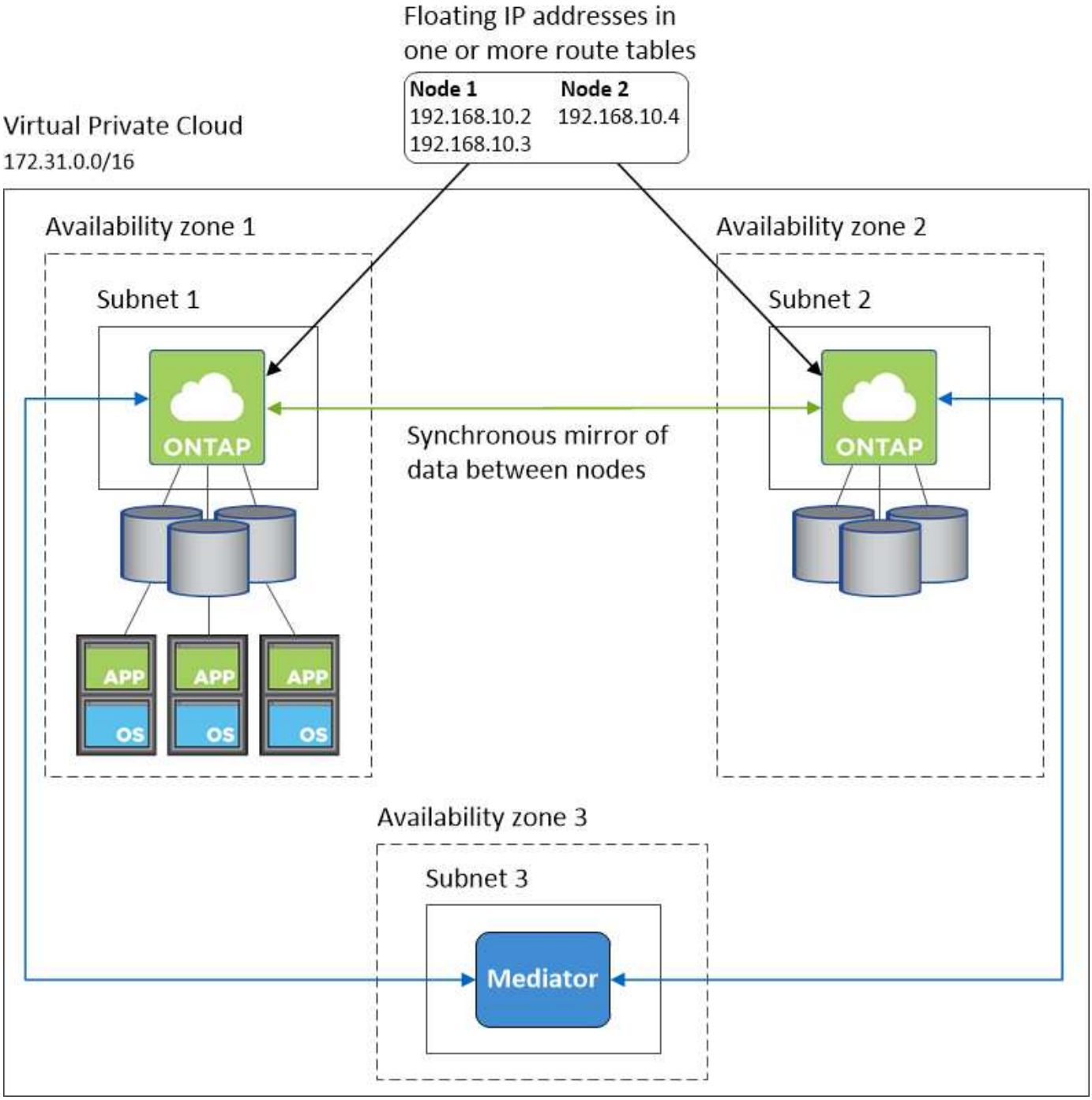
Connexion aux outils de gestion NetApp

Pour utiliser les outils de gestion NetApp avec des configurations haute disponibilité figurant dans plusieurs modèles AZS, vous disposez de deux options de connexion :

1. Déployez les outils de gestion NetApp sur un autre VPC et "Configuration d'une passerelle de transit AWS". La passerelle permet d'accéder à l'adresse IP flottante de l'interface de gestion du cluster à partir de l'extérieur du VPC.
2. Déployez les outils de gestion NetApp sur le même VPC avec une configuration de routage similaire à celle des clients NAS.

Exemple de configuration haute disponibilité

L'image suivante montre une configuration HA optimale dans AWS fonctionnant comme une configuration active-passive :



Configuration requise pour le connecteur

Configurez votre réseau afin que le connecteur puisse gérer les ressources et les processus au sein de votre environnement de cloud public. L'étape la plus importante consiste à garantir l'accès Internet sortant à différents terminaux.

Si votre réseau utilise un serveur proxy pour toutes les communications vers Internet, vous pouvez spécifier le serveur proxy à partir de la page Paramètres. Reportez-vous à la section "Configuration du connecteur pour utiliser un serveur proxy".

Connexion aux réseaux cibles

Un connecteur nécessite une connexion réseau aux VPC et VNets dans lesquels vous souhaitez déployer Cloud Volumes ONTAP.

Par exemple, si vous installez un connecteur sur le réseau de votre entreprise, vous devez configurer une connexion VPN sur le VPC ou le vnet dans lequel vous lancez Cloud Volumes ONTAP.

Accès Internet sortant

Le connecteur nécessite un accès Internet sortant pour gérer les ressources et les processus au sein de votre environnement de cloud public. Lors de la gestion des ressources dans AWS, un connecteur contacte les terminaux suivants :

Terminaux	Objectif
Services AWS (amazonaws.com): • CloudFormation • Cloud de calcul élastique (EC2) • Service de gestion des clés (KMS) • Service de jetons de sécurité (STS) • Service de stockage simple (S3) Le noeud final exact dépend de la région dans laquelle vous déployez Cloud Volumes ONTAP. "Reportez-vous à la documentation AWS pour plus de détails."	Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans AWS.
https://api.services.cloud.netapp.com:443	Demandes d'API à NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Permet d'accéder aux images logicielles, aux manifestes et aux modèles.
https://repo.cloud.support.netapp.com	Permet de télécharger les dépendances de Cloud Manager.
http://repo.mysql.com/	Utilisé pour télécharger MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Permet à Cloud Manager d'accéder aux manifestes, aux modèles et aux images de mise à niveau Cloud Volumes ONTAP et de les télécharger.
https://cloudmanagerinfraprod.azurecr.io	Accédez aux images logicielles des composants de conteneur pour une infrastructure exécutant Docker et fournie une solution pour les intégrations des services avec Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.
https://cloudmanager.cloud.netapp.com	Communication avec le service Cloud Manager, notamment les comptes Cloud Central.

Terminaux	Objectif
https://netapp-cloud-account.auth0.com	Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs.
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Permet d'ajouter votre ID de compte AWS à la liste des utilisateurs autorisés pour Backup vers S3.
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Communication avec NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Communication avec NetApp pour les licences système et l'inscription au support.
https://ipa-signer.cloudmanager.netapp.com	Génération des licences par Cloud Manager (par exemple, une licence FlexCache pour Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Nécessaire pour connecter des systèmes Cloud Volumes ONTAP avec un cluster Kubernetes. Les terminaux permettent l'installation de NetApp Trident.
Divers sites tiers, par exemple : • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Les emplacements tiers sont sujets à modification.	Lors des mises à niveau, Cloud Manager télécharge les derniers packages pour les dépendances tierces.

Bien que vous devriez effectuer presque toutes les tâches à partir de l'interface utilisateur SaaS, une interface utilisateur locale est toujours disponible sur le connecteur. La machine exécutant le navigateur Web doit disposer de connexions aux terminaux suivants :

Terminaux	Objectif
L'hôte du connecteur	Vous devez entrer l'adresse IP de l'hôte depuis un navigateur Web pour charger la console Cloud Manager. En fonction de votre connectivité avec votre fournisseur de cloud, vous pouvez utiliser l'IP privée ou une adresse IP publique attribuée à l'hôte : • Une adresse IP privée fonctionne si vous disposez d'un VPN et d'un accès direct à votre réseau virtuel • Un IP public fonctionne dans tous les scénarios de mise en réseau Dans tous les cas, vous devez sécuriser l'accès au réseau en vous assurant que les règles du groupe de sécurité autorisent l'accès à partir des adresses IP ou des sous-réseaux autorisés uniquement.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Votre navigateur Web se connecte à ces terminaux pour une authentification centralisée des utilisateurs via NetApp Cloud Central.
https://widget.intercom.io	Vous bénéficiez d'un chat en ligne pour discuter avec des experts du cloud NetApp.

Configuration d'une passerelle de transit AWS pour les paires HA dans plusieurs AZS

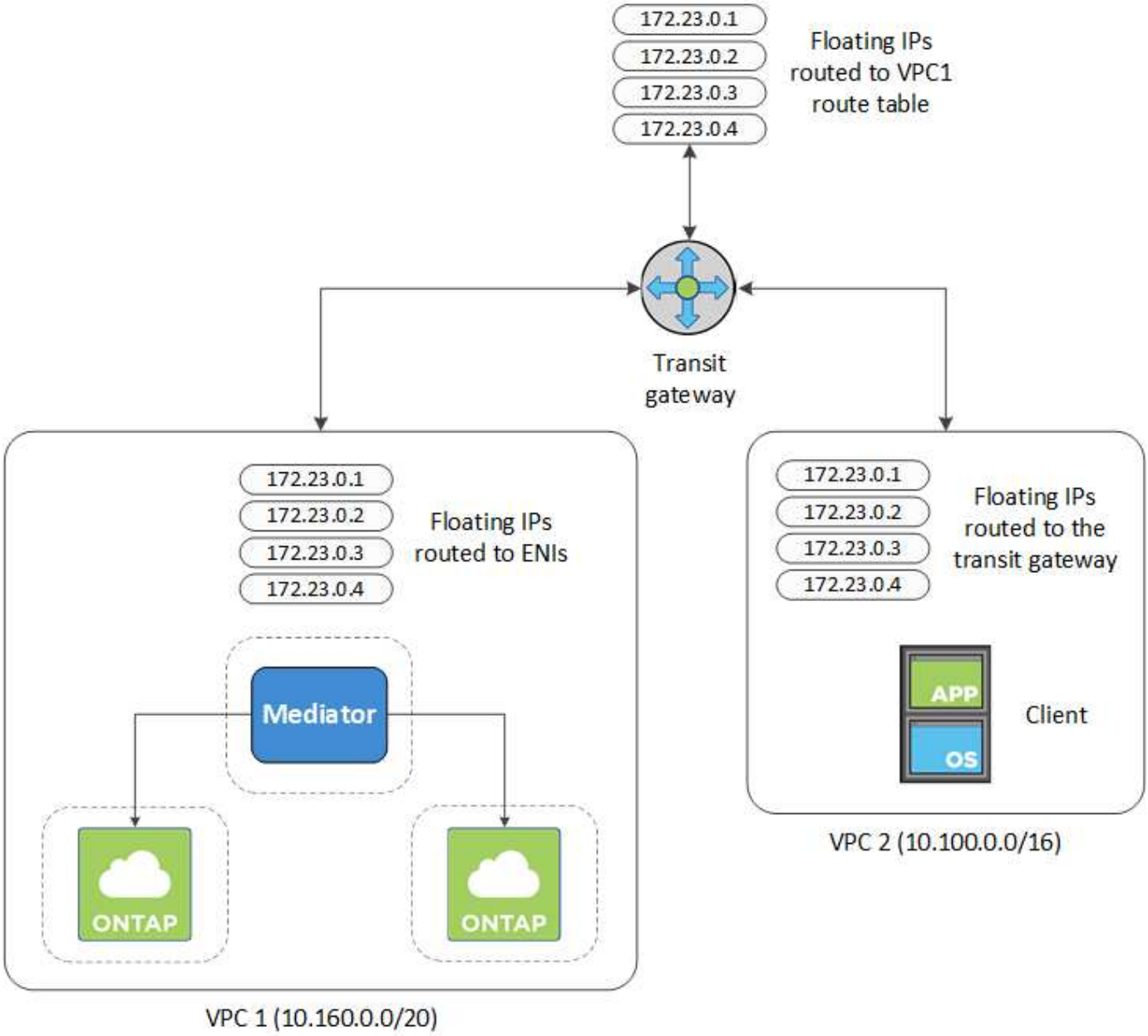
Configurez une passerelle de transit AWS pour autoriser l'accès à une paire HA "Adresses IP flottantes" Depuis l'extérieur du VPC, où réside la paire HA.

Lorsqu'une configuration Cloud Volumes ONTAP HA est répartie sur plusieurs zones de disponibilité AWS, des adresses IP flottantes sont nécessaires pour l'accès aux données NAS depuis le VPC. Ces adresses IP flottantes peuvent migrer entre les nœuds en cas de défaillance, mais elles ne sont pas accessibles de manière native en dehors du VPC. Des adresses IP privées séparées permettent un accès aux données depuis l'extérieur du VPC, mais elles ne permettent pas de procéder à un basculement automatique.

Des adresses IP flottantes sont également nécessaires pour l'interface de gestion du cluster et la LIF de gestion du SVM facultative.

Si vous configurez une passerelle de transit AWS, vous activez l'accès aux adresses IP flottantes depuis l'extérieur sur le VPC où réside la paire haute disponibilité. Les clients NAS et les outils de gestion NetApp en dehors du VPC peuvent accéder aux adresses IP flottantes.

Voici un exemple illustrant deux VPC connectés par une passerelle de transit. Un système haute disponibilité réside dans un VPC, tandis qu'un client réside dans l'autre. Vous pouvez ensuite monter un volume NAS sur le client à l'aide de l'adresse IP flottante.

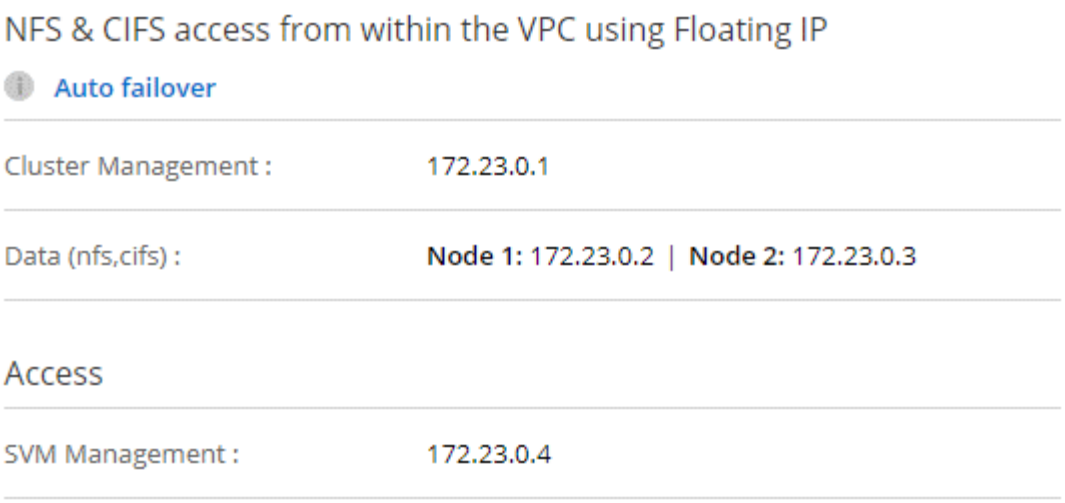


Les étapes suivantes montrent comment configurer une configuration similaire.

Étapes

1. "Créez une passerelle de transit et connectez les VPC à la passerelle".
2. Créer des routes dans la table de routage de la passerelle de transit en spécifiant les adresses IP flottantes de la paire HA.

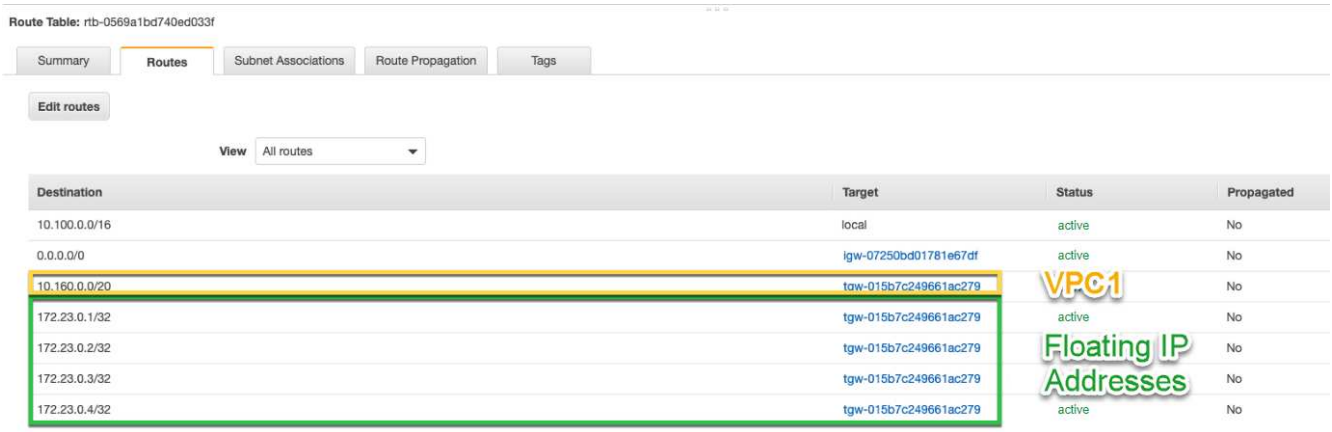
   Les adresses IP flottantes se trouvent sur la page des informations sur l'environnement de travail dans Cloud Manager. Voici un exemple :



L'exemple d'image suivant montre la table de routage pour la passerelle de transit. Il comprend les routes vers les blocs CIDR des deux VPC et quatre adresses IP flottantes utilisées par Cloud Volumes ONTAP.

3. Modifiez la table de routage des VPC qui doivent accéder aux adresses IP flottantes.
   a. Ajoutez des entrées de route aux adresses IP flottantes.
   b. Ajoutez une entrée de route au bloc CIDR du VPC où réside la paire HA.

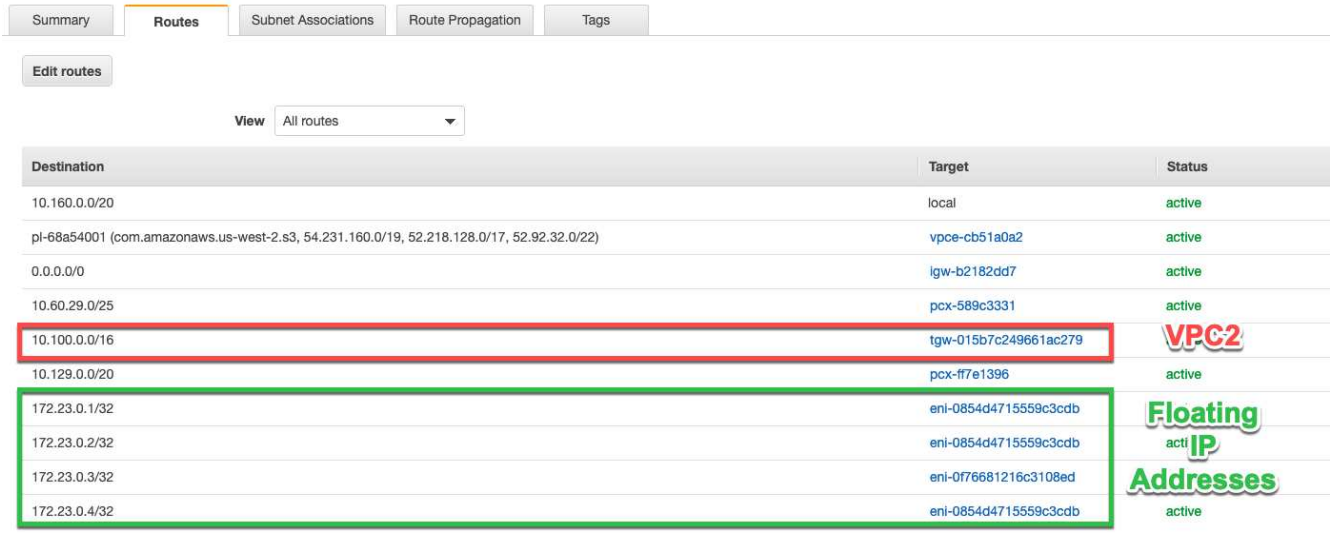
      L'exemple d'image suivant montre la table de route pour VPC 2, qui comprend les routes vers VPC 1 et les adresses IP flottantes.



4. Modifiez la table de routage du VPC de la paire HA en ajoutant une route vers le VPC qui doit accéder aux adresses IP flottantes.

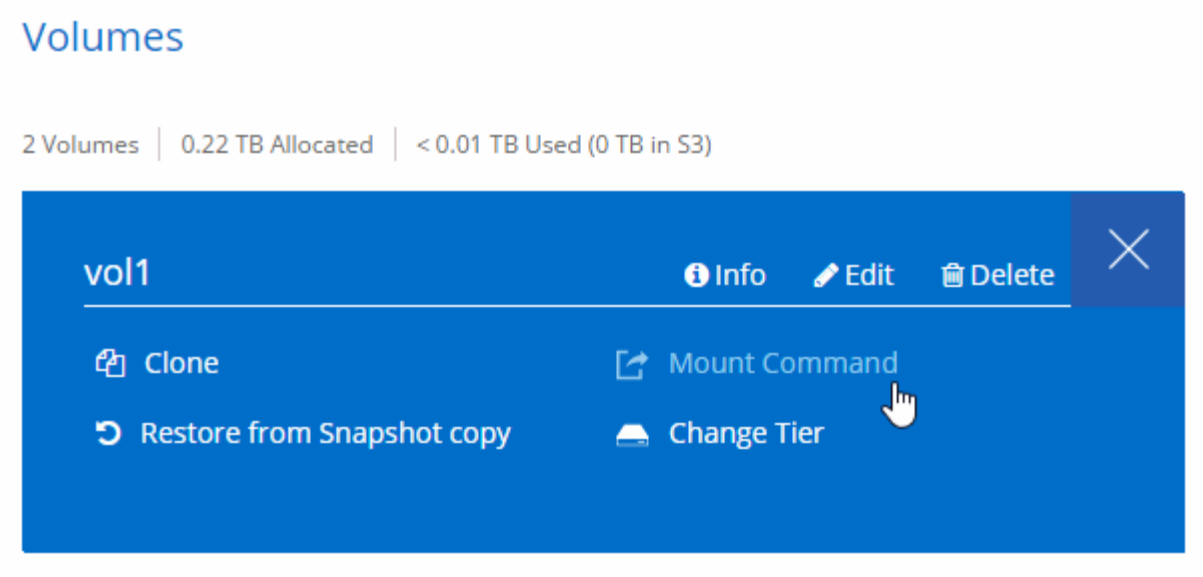
   Cette étape est importante car elle termine le routage entre les VPC.

   L'exemple d'image suivant montre la table de routage pour VPC 1. Elle inclut une route vers les adresses IP flottantes et vers VPC 2, c'est-à-dire où réside un client. Cloud Manager a automatiquement ajouté les adresses IP flottantes à la table de routage lors du déploiement de la paire haute disponibilité.



5. Montez les volumes sur des clients à l'aide de l'adresse IP flottante.

   Vous trouverez l'adresse IP correcte dans Cloud Manager en sélectionnant un volume et en cliquant sur **Mount Command**.



- Liens connexes*
- "Paires haute disponibilité dans AWS"
- "Configuration réseau requise pour Cloud Volumes ONTAP dans AWS"

Règles de groupe de sécurité pour AWS

Cloud Manager crée des groupes de sécurité AWS qui incluent les règles entrantes et sortantes que le connecteur et Cloud Volumes ONTAP doivent fonctionner correctement. Vous pouvez vous référer aux ports à des fins de test ou si vous préférez que votre utilise ses propres groupes de sécurité.

Règles pour Cloud Volumes ONTAP

Le groupe de sécurité pour Cloud Volumes ONTAP requiert des règles entrantes et sortantes.

Règles entrantes

La source des règles entrantes dans le groupe de sécurité prédéfini est 0.0.0.0/0.

Protocole	Port	Objectif
Tous les protocoles ICMP	Tout	Envoi d'une requête ping à l'instance
HTTP	80	Accès HTTP à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
HTTPS	443	Accès HTTPS à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
SSH	22	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
TCP	111	Appel de procédure à distance pour NFS
TCP	139	Session de service NetBIOS pour CIFS

Protocole	Port	Objectif
TCP	161-162	Protocole de gestion de réseau simple
TCP	445	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
TCP	658	Montage NFS
TCP	749	Kerberos
TCP	2049	Démon du serveur NFS
TCP	3260	Accès iSCSI via le LIF de données iSCSI
TCP	4045	Démon de verrouillage NFS
TCP	4046	Surveillance de l'état du réseau pour NFS
TCP	10000	Sauvegarde avec NDMP
TCP	11104	Gestion des sessions de communication intercluster pour SnapMirror
TCP	11105	Transfert de données SnapMirror à l'aide de LIF intercluster
UDP	111	Appel de procédure à distance pour NFS
UDP	161-162	Protocole de gestion de réseau simple
UDP	658	Montage NFS
UDP	2049	Démon du serveur NFS
UDP	4045	Démon de verrouillage NFS
UDP	4046	Surveillance de l'état du réseau pour NFS
UDP	4049	Protocole NFS rquotad

Règles de sortie

Le groupe de sécurité prédéfini pour Cloud Volumes ONTAP ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour Cloud Volumes ONTAP inclut les règles de sortie suivantes.

Protocole	Port	Objectif
Tous les protocoles ICMP	Tout	Tout le trafic sortant
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles UDP	Tout	Tout le trafic sortant

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par Cloud Volumes ONTAP.

La source est l'interface (adresse IP) du système Cloud Volumes ONTAP.

Service	Protocole	Port	Source	Destination	Objectif
Active Directory	TCP	88	FRV de gestion des nœuds	Forêt Active Directory	Authentification Kerberos V.
	UDP	137	FRV de gestion des nœuds	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	FRV de gestion des nœuds	Forêt Active Directory	Service de datagrammes NetBIOS
	TCP	139	FRV de gestion des nœuds	Forêt Active Directory	Session de service NetBIOS
	TCP ET UDP	389	FRV de gestion des nœuds	Forêt Active Directory	LDAP
	TCP	445	FRV de gestion des nœuds	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	UDP	464	FRV de gestion des nœuds	Forêt Active Directory	Administration des clés Kerberos
	TCP	749	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)
	TCP	88	LIF de données (NFS, CIFS, iSCSI)	Forêt Active Directory	Authentification Kerberos V.
	UDP	137	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de datagrammes NetBIOS
	TCP	139	FRV de données (NFS, CIFS)	Forêt Active Directory	Session de service NetBIOS
	TCP ET UDP	389	FRV de données (NFS, CIFS)	Forêt Active Directory	LDAP
	TCP	445	FRV de données (NFS, CIFS)	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	UDP	464	FRV de données (NFS, CIFS)	Forêt Active Directory	Administration des clés Kerberos
	TCP	749	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)
Sauvegarde vers S3	TCP	5010	FRV InterCluster	Sauvegarder le terminal ou restaurer le terminal	Des opérations de sauvegarde et de restauration pour la fonctionnalité Backup vers S3

Service	Protocole	Port	Source	Destination	Objectif
Cluster	Tout le trafic	Tout le trafic	Tous les LIF sur un nœud	Tous les LIF de l'autre nœud	Communications InterCluster (Cloud Volumes ONTAP HA uniquement)
	TCP	3000	FRV de gestion des nœuds	Ha médiateur	Appels ZAPI (Cloud Volumes ONTAP HA uniquement)
	ICMP	1	FRV de gestion des nœuds	Ha médiateur	Rester en vie (Cloud Volumes ONTAP HA uniquement)
DHCP	UDP	68	FRV de gestion des nœuds	DHCP	Client DHCP pour la première configuration
DHCPS	UDP	67	FRV de gestion des nœuds	DHCP	Serveur DHCP
DNS	UDP	53	FRV de gestion des nœuds et FRV de données (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600-18699	FRV de gestion des nœuds	Serveurs de destination	Copie NDMP
SMTP	TCP	25	FRV de gestion des nœuds	Serveur de messagerie	Les alertes SMTP peuvent être utilisées pour AutoSupport
SNMP	TCP	161	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	UDP	161	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	TCP	162	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	UDP	162	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
SnapMirror	TCP	11104	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Gestion des sessions de communication intercluster pour SnapMirror
	TCP	11105	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Transfert de données SnapMirror
Syslog	UDP	514	FRV de gestion des nœuds	Serveur Syslog	Messages de transfert syslog

Règles pour le groupe de sécurité externe du médiateur de haute disponibilité

Le groupe de sécurité externe prédéfini pour le médiateur Cloud Volumes ONTAP HA inclut les règles entrantes et sortantes suivantes.

Règles entrantes

La source des règles entrantes est 0.0.0.0/0.

Protocole	Port	Objectif
SSH	22	Connexions SSH au médiateur haute disponibilité
TCP	3000	Accès à l'API RESTful depuis le connecteur

Règles de sortie

Le groupe de sécurité prédéfini du médiateur HA ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini du médiateur HA inclut les règles de sortie suivantes.

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles UDP	Tout	Tout le trafic sortant

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par le médiateur haute disponibilité.

Protocole	Port	Destination	Objectif
HTTP	80	Adresse IP du connecteur	Télécharger les mises à niveau pour le médiateur
HTTPS	443	Services API AWS	Assistance pour le basculement du stockage
UDP	53	Services API AWS	Assistance pour le basculement du stockage

Plutôt que d'ouvrir les ports 443 et 53, vous pouvez créer un terminal VPC d'interface à partir du sous-réseau cible vers le service AWS EC2.

Règles pour le groupe de sécurité interne du médiateur de haute disponibilité

Le groupe de sécurité interne prédéfini pour le médiateur Cloud Volumes ONTAP HA inclut les règles suivantes. Cloud Manager crée toujours ce groupe de sécurité. Vous n'avez pas la possibilité d'utiliser vos propres ressources.

Règles entrantes

Le groupe de sécurité prédéfini inclut les règles entrantes suivantes.

Protocole	Port	Objectif
Tout le trafic	Tout	Communication entre le médiateur HA et les nœuds HA

Règles de sortie

Le groupe de sécurité prédéfini inclut les règles de sortie suivantes.

Protocole	Port	Objectif
Tout le trafic	Tout	Communication entre le médiateur HA et les nœuds HA

Règles pour le connecteur

Le groupe de sécurité du connecteur nécessite à la fois des règles entrantes et sortantes.

Règles entrantes

La source des règles entrantes dans le groupe de sécurité prédéfini est 0.0.0.0/0.

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP depuis les navigateurs Web du client vers l'interface utilisateur locale et les connexions à partir de Cloud Compliance
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale
TCP	3128	Fournit l'instance Cloud Compliance avec un accès Internet si votre réseau AWS n'utilise pas de NAT ou de proxy

Règles de sortie

Le groupe de sécurité prédéfini pour le connecteur ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour le connecteur inclut les règles de trafic sortant suivantes.

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles UDP	Tout	Tout le trafic sortant

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par le connecteur.

L'adresse IP source est l'hôte du connecteur.

Service	Protocole	Port	Destination	Objectif
Active Directory	TCP	88	Forêt Active Directory	Authentification Kerberos V.
	TCP	139	Forêt Active Directory	Session de service NetBIOS
	TCP	389	Forêt Active Directory	LDAP
	TCP	445	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	TCP	749	Forêt Active Directory	Modification et définition du mot de passe de Kerberos V Active Directory (RPCSEC_GSS)
	UDP	137	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	Forêt Active Directory	Service de datagrammes NetBIOS
	UDP	464	Forêt Active Directory	Administration des clés Kerberos
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	API appelle AWS et ONTAP et envoie des messages AutoSupport à NetApp
Appels API	TCP	3000	LIF de gestion de cluster ONTAP	Appels API vers ONTAP
	TCP	8088	Sauvegarde vers S3	Appels d'API vers Backup vers S3
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par Cloud Manager
Conformité cloud	HTTP	80	Instance Cloud Compliance	Cloud Compliance pour Cloud Volumes ONTAP

Configuration du système AWS KMS

Si vous souhaitez utiliser le chiffrement Amazon avec Cloud Volumes ONTAP, vous devez configurer le service AWS Key Management Service (KMS).

Étapes

1. S'assurer qu'une clé principale client (CMK) active existe.

   La CMK peut être une CMK gérée par AWS ou une CMK gérée par le client. Il peut être hébergé sur le même compte AWS que Cloud Manager et Cloud Volumes ONTAP ou dans un autre compte AWS.

   "Documentation AWS : clés principales client (CMK)"

2. Modifiez la stratégie clé pour chaque CMK en ajoutant le rôle IAM qui fournit des autorisations à Cloud Manager en tant que *utilisateur clé*.

   L'ajout du rôle IAM en tant qu'utilisateur clé donne aux utilisateurs Cloud Manager les autorisations d'utiliser le CMK avec Cloud Volumes ONTAP.

   "Documentation AWS : modification des clés"

3. Si le CMK se trouve dans un autre compte AWS, procédez comme suit :

   a. Accédez à la console KMS à partir du compte où réside la CMK.

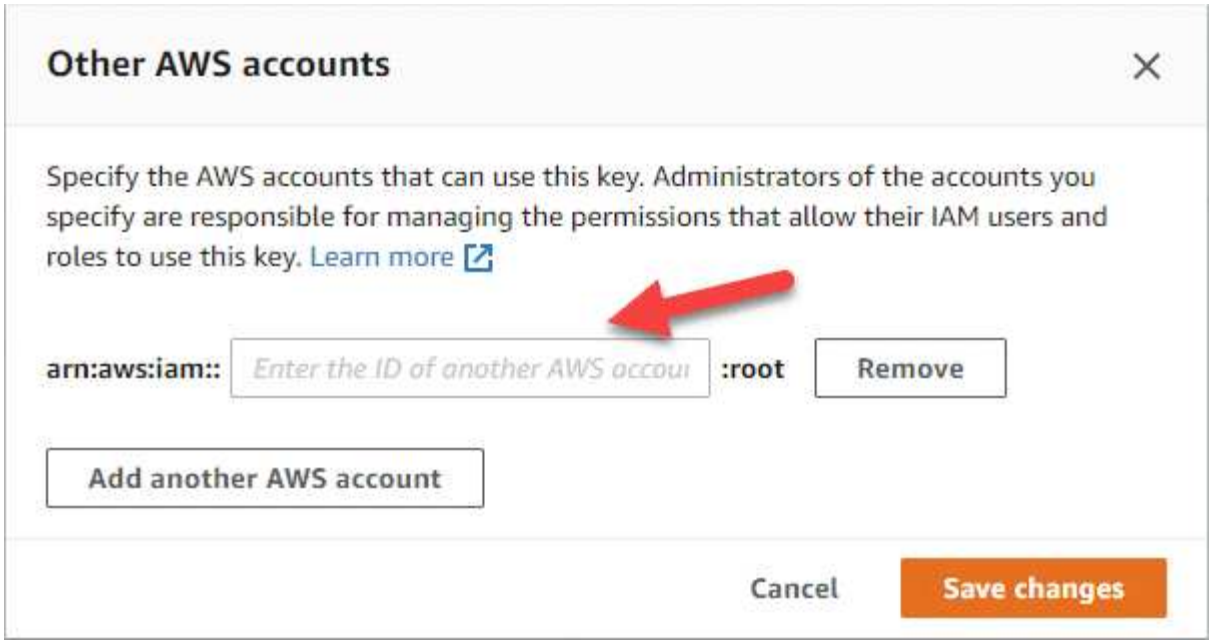
   b. Sélectionnez la touche.

   c. Dans le volet **Configuration générale**, copiez l'ARN de la clé.

      Vous devrez fournir l'ARN dans Cloud Manager lors de la création du système Cloud Volumes ONTAP.

   d. Dans le volet **autres comptes AWS**, ajoutez le compte AWS qui fournit les autorisations à Cloud Manager.

      Dans la plupart des cas, il s'agit du compte sur lequel réside Cloud Manager. Si Cloud Manager n'a pas été installé dans AWS, il s'agit du compte sur lequel vous avez fourni les clés d'accès AWS à Cloud Manager.



e. Passez maintenant au compte AWS qui fournit les autorisations nécessaires à Cloud Manager et ouvrez la console IAM.

f. Créez une stratégie IAM qui inclut les autorisations répertoriées ci-dessous.

g. Associez la règle au rôle IAM ou à l'utilisateur IAM qui donne des autorisations à Cloud Manager.

   La règle suivante fournit les autorisations requises par Cloud Manager pour utiliser le CMK à partir du compte AWS externe. Veillez à modifier la région et l'ID de compte dans les sections « ressource ».

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

+
Pour plus d'informations sur ce processus, reportez-vous à la section "Documentation AWS : autoriser les comptes AWS externes à accéder à un CMK".

Lancement d'Cloud Volumes ONTAP dans AWS

Vous pouvez lancer Cloud Volumes ONTAP dans une configuration à système unique ou en tant que paire haute disponibilité dans AWS.

Lancement d'un système Cloud Volumes ONTAP à un seul nœud dans AWS

Si vous souhaitez lancer Cloud Volumes ONTAP dans AWS, vous devez créer un nouvel environnement de travail dans Cloud Manager.

Avant de commencer

- Vous devez avoir un "Connecteur associé à votre espace de travail".

> Vous devez être un administrateur de compte pour créer un connecteur. Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l'avez pas encore fait.

- "Vous devez être prêt à laisser le connecteur fonctionner en permanence".
- Vous devriez avoir préparé en choisissant une configuration et en obtenant les informations de mise en réseau AWS auprès de votre administrateur. Pour plus de détails, voir "Planification de votre configuration Cloud Volumes ONTAP".
- Si vous souhaitez lancer un système BYOL, vous devez disposer du numéro de série à 20 chiffres (clé de licence).
- Si vous souhaitez utiliser CIFS, vous devez avoir configuré DNS et Active Directory. Pour plus de détails, voir "Configuration réseau requise pour Cloud Volumes ONTAP dans AWS".

Description de la tâche

Immédiatement après la création de l'environnement de travail, Cloud Manager lance une instance de test dans le VPC spécifié pour vérifier la connectivité. En cas de réussite, Cloud Manager met immédiatement fin à l'instance, puis lance le déploiement du système Cloud Volumes ONTAP. Si Cloud Manager ne parvient pas à vérifier la connectivité, la création de l'environnement de travail échoue. L'instance de test est soit t2.nano (pour la location VPC par défaut), soit m3.medium (pour la location VPC dédiée).

Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
2. **Choisissez un emplacement** : sélectionnez **Amazon Web Services** et **Cloud Volumes ONTAP Single Node**.
3. **Détails et informations d'identification** : modifiez éventuellement les informations d'identification et l'abonnement AWS, entrez un nom d'environnement de travail, ajoutez des balises si nécessaire, puis entrez un mot de passe.

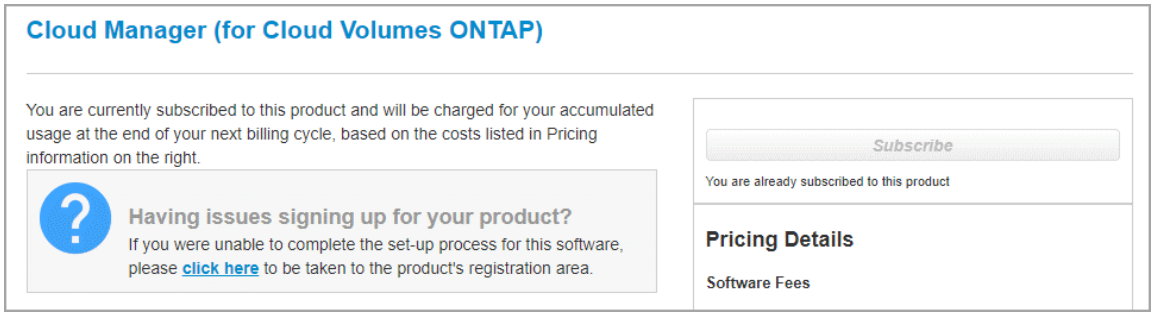
   Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Nom de l'environnement de travail	Cloud Manager utilise le nom de l'environnement de travail pour nommer à la fois le système Cloud Volumes ONTAP et l'instance Amazon EC2. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.
Ajouter des étiquettes	Les étiquettes AWS sont des métadonnées pour vos ressources AWS. Cloud Manager ajoute les balises à l'instance Cloud Volumes ONTAP et à chaque ressource AWS associée à l'instance. Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section "Documentation AWS : balisage des ressources Amazon EC2".
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte d'administration du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via OnCommand System Manager ou sa CLI.
Modifier les informations d'identification	Sélectionnez les identifiants AWS et l'abonnement Marketplace pour les utiliser avec ce système Cloud Volumes ONTAP. Cliquez sur **Ajouter un abonnement** pour associer les informations d'identification sélectionnées à un abonnement. Pour créer un système Cloud Volumes ONTAP à l'utilisation, vous devez sélectionner les identifiants AWS associés à un abonnement à Cloud Volumes ONTAP depuis AWS Marketplace. Vous serez facturé à partir de cet abonnement pour chaque système Cloud Volumes ONTAP 9.6 ou ultérieur de PAYGO que vous créez et chaque fonctionnalité d'extension activée."Découvrez comment ajouter des identifiants AWS à Cloud Manager".

Découvrez dans cette vidéo comment associer un abonnement payant basé sur l'utilisation Marketplace à vos identifiants AWS :

► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_aws.mp4 *(video)*

Si plusieurs utilisateurs IAM travaillent sur le même compte AWS, chaque utilisateur doit s'abonner. Après l'abonnement du premier utilisateur, AWS Marketplace informe les autres utilisateurs qu'ils sont déjà abonnés, comme illustré dans l'image ci-dessous. Lorsqu'un abonnement est en place pour AWS *account*, chaque utilisateur IAM doit s'associer à cet abonnement. Si le message ci-dessous s'affiche, cliquez sur le lien **cliquez ici** pour accéder à Cloud Central et terminer le processus.

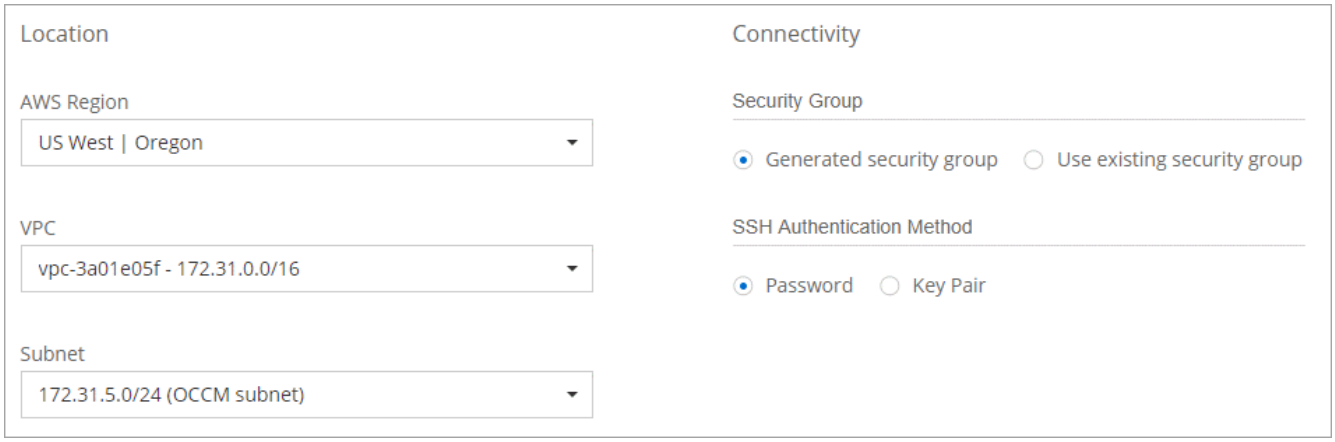


4. **Services** : conservez les services activés ou désactivez les services individuels que vous ne souhaitez pas utiliser avec Cloud Volumes ONTAP.

- "En savoir plus sur Cloud Compliance".
- "En savoir plus sur la sauvegarde dans le cloud".
- "En savoir plus sur la surveillance".

5. **Location & Connectivity** : saisissez les informations de réseau que vous avez enregistrées dans la fiche de travail AWS.

   L'image suivante montre la page remplie :



6. **Data Encryption** : choisissez pas de cryptage de données ou de cryptage géré par AWS.

   Pour le chiffrement géré par AWS, vous pouvez choisir une autre clé maître client (CMK) dans votre compte ou un autre compte AWS.

   Une fois que vous avez créé un système Cloud Volumes ONTAP, vous ne pouvez pas modifier la méthode de chiffrement des données AWS.

   "Découvrez comment configurer le KMS AWS pour Cloud Volumes ONTAP".

   "En savoir plus sur les technologies de cryptage prises en charge".

7. **Compte sur le site de licence et de support** : indiquez si vous souhaitez utiliser le paiement à l'utilisation ou BYOL, puis indiquez un compte sur le site de support NetApp.

   Pour comprendre le fonctionnement des licences, reportez-vous à la section "Licences".

   Un compte sur le site de support NetApp est facultatif afin de bénéficier d'un paiement à l'utilisation, mais requis pour les systèmes BYOL. "Découvrez comment ajouter des comptes au site de support NetApp".

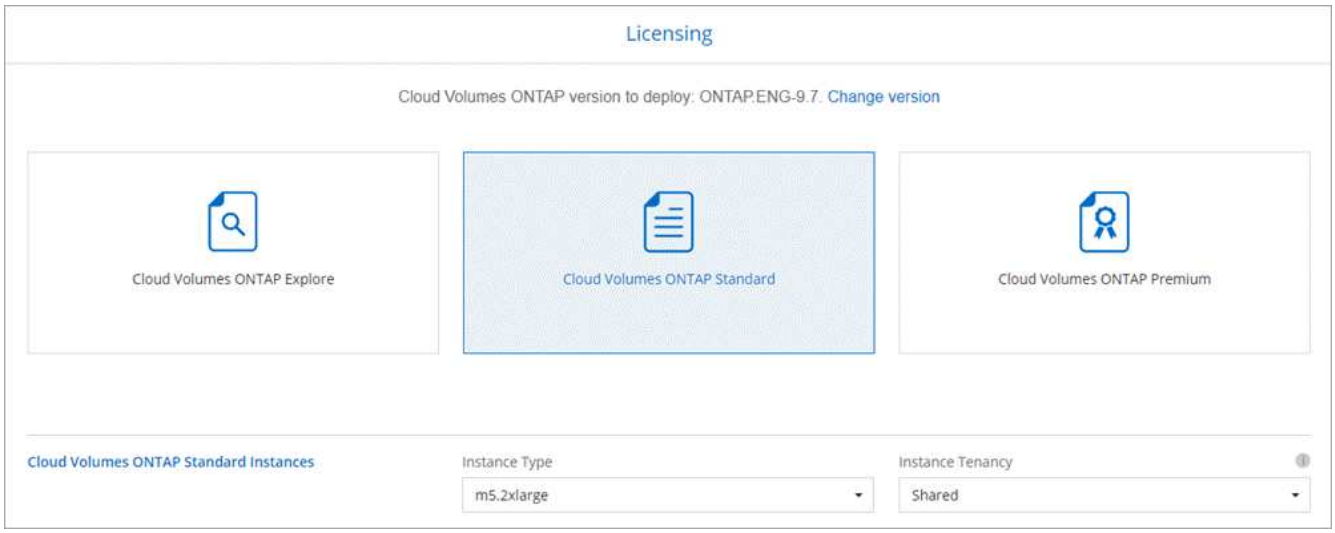
8. **Packages préconfigurés** : sélectionnez un des packages pour lancer rapidement Cloud Volumes ONTAP, ou cliquez sur **Créer ma propre configuration**.

   Si vous choisissez l'un des packages, vous n'avez qu'à spécifier un volume, puis à revoir et approuver la configuration.

9. **Rôle IAM** : vous devez conserver l'option par défaut pour permettre à Cloud Manager de créer le rôle pour vous.

   Si vous préférez utiliser votre propre police, elle doit satisfaire "Configuration requise pour les nœuds Cloud Volumes ONTAP".

10. **Licence** : modifiez la version de Cloud Volumes ONTAP selon vos besoins, sélectionnez une licence, un type d'instance et la location d'instance.



Si vos besoins changent après le lancement de l'instance, vous pouvez modifier la licence ou le type d'instance ultérieurement.

> Si une version plus récente de Release Candidate, General Availability ou patch est disponible pour la version sélectionnée, Cloud Manager met à jour le système à cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.6 RC1 et 9.6 GA est disponible. La mise à jour ne se produit pas d'une version à l'autre, par exemple de 9.6 à 9.7.

11. **Ressources de stockage sous-jacentes** : Choisissez les paramètres de l'agrégat initial : un type de disque, une taille pour chaque disque et si la hiérarchisation des données doit être activée.

    Notez ce qui suit :

    - Le type de disque correspond au volume initial. Vous pouvez choisir un autre type de disque pour les volumes suivants.
    - La taille du disque correspond à tous les disques de l'agrégat initial et à tous les agrégats supplémentaires créés par Cloud Manager lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente à l'aide de l'option d'allocation avancée.

      Pour obtenir de l'aide sur le choix du type et de la taille d'un disque, reportez-vous à la section "Dimensionnement de votre système dans AWS".

    - Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
    - Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants.

      "Découvrez le fonctionnement du Tiering des données".

12. **Vitesse d'écriture et WORM** : choisissez **Normal** ou **vitesse d'écriture élevée**, et activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

    La sélection d'une vitesse d'écriture est prise en charge avec les systèmes à un seul nœud uniquement.

"En savoir plus sur la vitesse d'écriture".

IMPOSSIBLE D'activer WORM si le Tiering des données était activé.

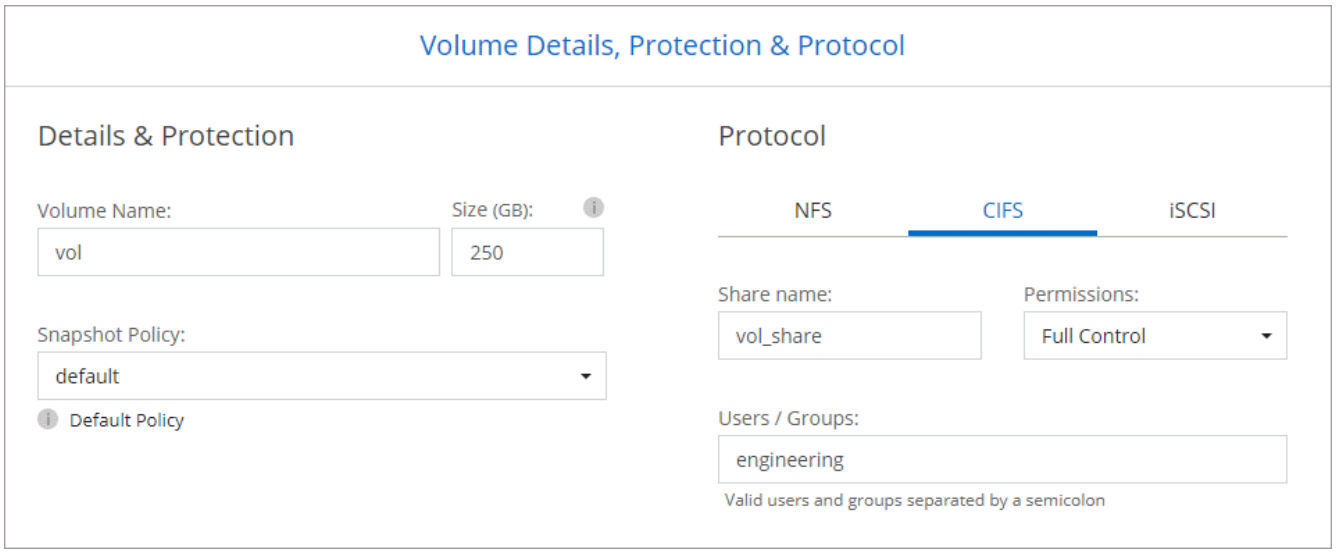
"En savoir plus sur le stockage WORM".

13. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, Cloud Manager entre une valeur qui donne accès à toutes les instances du sous-réseau.
Autorisations et utilisateurs/groupes (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur à l'aide du format domaine\nom d'utilisateur.
Stratégie Snapshot	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de buste hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".

L'image suivante montre la page Volume remplie pour le protocole CIFS :



14. **Configuration CIFS** : si vous choisissez le protocole CIFS, configurez un serveur CIFS.

Champ	Description
Adresse IP principale et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS.
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Nom de serveur CIFS unique dans le domaine AD.
Unité organisationnelle	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Si vous configurez AWS Managed Microsoft AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer **ou=ordinateurs,ou=corp** dans ce champ.
Domaine DNS	Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD.
Serveur NTP	Sélectionnez **utiliser le domaine Active Directory** pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la "Guide du développeur de l'API Cloud Manager" pour plus d'informations.

15. **Profil d'utilisation, type de disque et règle de hiérarchisation** : choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifiez la règle de hiérarchisation du volume, si nécessaire.

    Pour plus d'informations, voir "Présentation des profils d'utilisation des volumes" et "Vue d'ensemble du hiérarchisation des données".

16. **Revue et approbation** : consultez et confirmez vos choix.

a. Consultez les détails de la configuration.

b. Cliquez sur **plus d'informations** pour en savoir plus sur le support et les ressources AWS que Cloud Manager achètera.

c. Cochez les cases **Je comprends…**.

d. Cliquez sur **Go**.

Résultat

Cloud Manager lance l'instance Cloud Volumes ONTAP. Vous pouvez suivre la progression dans la chronologie.

Si vous rencontrez des problèmes lors du lancement de l'instance Cloud Volumes ONTAP, consultez le message d'échec. Vous pouvez également sélectionner l'environnement de travail et cliquer sur Re-create environment.

Pour obtenir de l'aide supplémentaire, consultez la page "Prise en charge de NetApp Cloud Volumes ONTAP".

Une fois que vous avez terminé

- Si vous avez provisionné un partage CIFS, donnez aux utilisateurs ou aux groupes des autorisations sur les fichiers et les dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier.
- Si vous souhaitez appliquer des quotas aux volumes, utilisez System Manager ou l'interface de ligne de commande.

  Les quotas vous permettent de restreindre ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree.

Lancement d'une paire Cloud Volumes ONTAP HA dans AWS

Si vous souhaitez lancer une paire Cloud Volumes ONTAP HA dans AWS, vous devez créer un environnement de travail HA dans Cloud Manager.

Avant de commencer

- Vous devez avoir un "Connecteur associé à votre espace de travail".

  Vous devez être un administrateur de compte pour créer un connecteur. Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l'avez pas encore fait.

- "Vous devez être prêt à laisser le connecteur fonctionner en permanence".
- Vous devriez avoir préparé en choisissant une configuration et en obtenant les informations de mise en réseau AWS auprès de votre administrateur. Pour plus de détails, voir "Planification de votre configuration Cloud Volumes ONTAP".
- Si vous avez acheté des licences BYOL, vous devez disposer d'un numéro de série à 20 chiffres (clé de licence) pour chaque nœud.
- Si vous souhaitez utiliser CIFS, vous devez avoir configuré DNS et Active Directory. Pour plus de détails, voir "Configuration réseau requise pour Cloud Volumes ONTAP dans AWS".

Restriction

À l'heure actuelle, les paires haute disponibilité ne sont pas prises en charge avec les posts d'AWS.

Description de la tâche

Immédiatement après la création de l'environnement de travail, Cloud Manager lance une instance de test dans le VPC spécifié pour vérifier la connectivité. En cas de réussite, Cloud Manager met immédiatement fin à l'instance, puis lance le déploiement du système Cloud Volumes ONTAP. Si Cloud Manager ne parvient pas à vérifier la connectivité, la création de l'environnement de travail échoue. L'instance de test est soit t2.nano (pour la location VPC par défaut), soit m3.medium (pour la location VPC dédiée).

Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
2. **Choisissez un emplacement** : sélectionnez **Amazon Web Services** et **Cloud Volumes ONTAP Single Node**.
3. **Détails et informations d'identification** : modifiez éventuellement les informations d'identification et l'abonnement AWS, entrez un nom d'environnement de travail, ajoutez des balises si nécessaire, puis entrez un mot de passe.

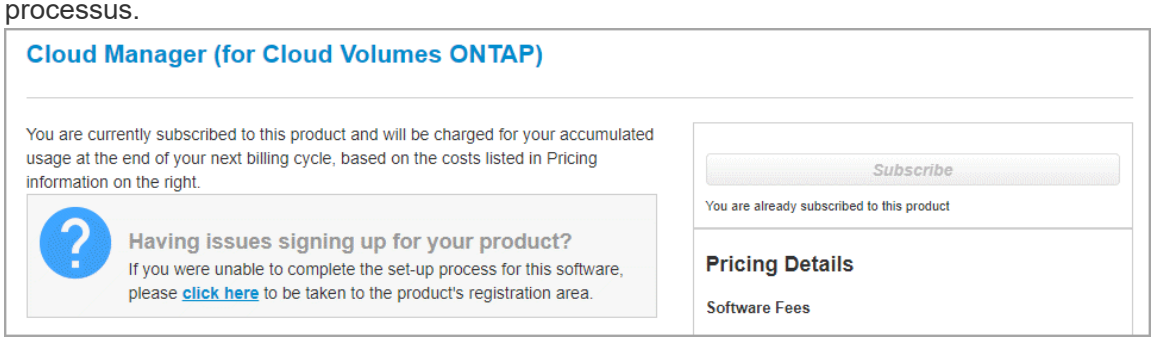
   Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Nom de l'environnement de travail	Cloud Manager utilise le nom de l'environnement de travail pour nommer à la fois le système Cloud Volumes ONTAP et l'instance Amazon EC2. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.
Ajouter des étiquettes	Les étiquettes AWS sont des métadonnées pour vos ressources AWS. Cloud Manager ajoute les balises à l'instance Cloud Volumes ONTAP et à chaque ressource AWS associée à l'instance. Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section "Documentation AWS : balisage des ressources Amazon EC2".
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte d'administration du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via OnCommand System Manager ou sa CLI.
Modifier les informations d'identification	Sélectionnez les identifiants AWS et l'abonnement Marketplace pour les utiliser avec ce système Cloud Volumes ONTAP. Cliquez sur **Ajouter un abonnement** pour associer les informations d'identification sélectionnées à un abonnement. Pour créer un système Cloud Volumes ONTAP à l'utilisation, vous devez sélectionner les identifiants AWS associés à un abonnement à Cloud Volumes ONTAP depuis AWS Marketplace. Vous serez facturé à partir de cet abonnement pour chaque système Cloud Volumes ONTAP 9.6 ou ultérieur de PAYGO que vous créez et chaque fonctionnalité d'extension activée."Découvrez comment ajouter des identifiants AWS à Cloud Manager".

   Découvrez dans cette vidéo comment associer un abonnement payant basé sur l'utilisation Marketplace à vos identifiants AWS :

   ► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_aws.mp4 *(video)*

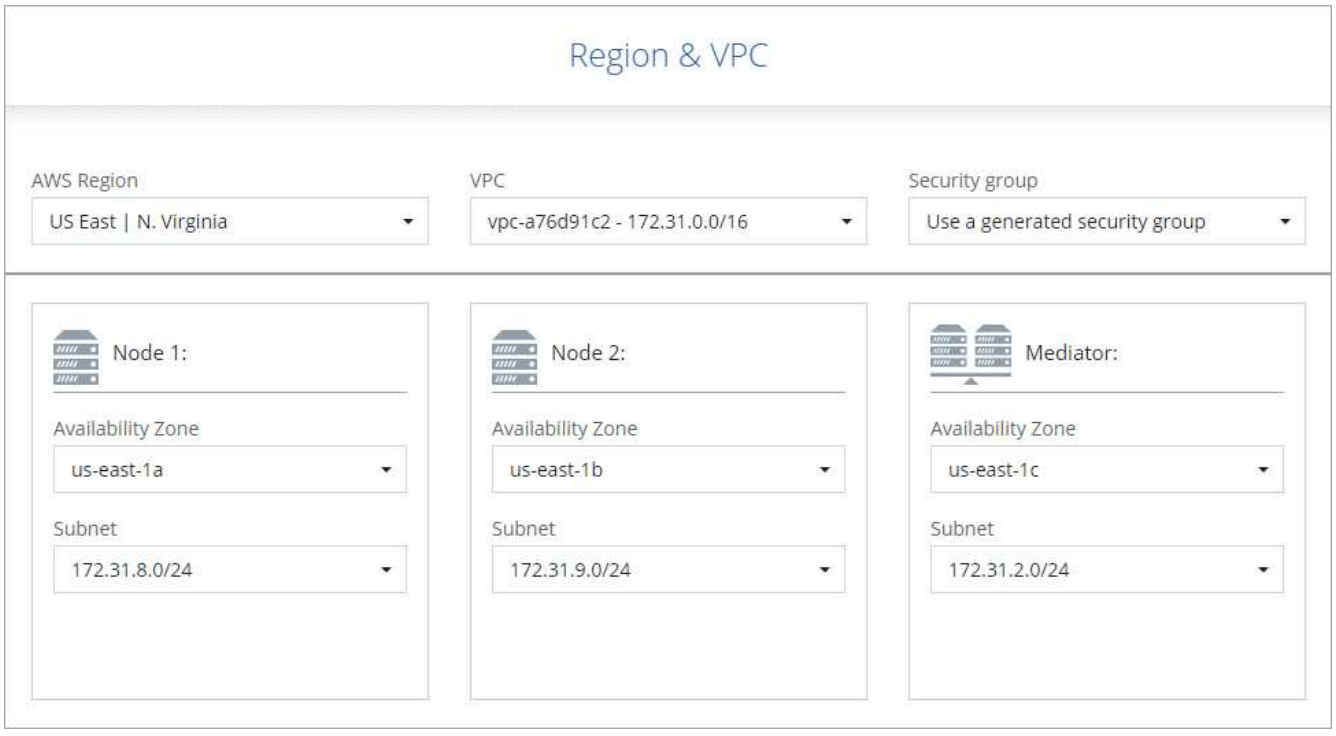
Si plusieurs utilisateurs IAM travaillent sur le même compte AWS, chaque utilisateur doit s'abonner. Après l'abonnement du premier utilisateur, AWS Marketplace informe les autres utilisateurs qu'ils sont déjà abonnés, comme illustré dans l'image ci-dessous. Lorsqu'un abonnement est en place pour AWS *account*, chaque utilisateur IAM doit s'associer à cet abonnement. Si le message ci-dessous s'affiche, cliquez sur le lien **cliquez ici** pour accéder à Cloud Central et terminer le
processus.



4. **Services** : conservez les services activés ou désactivez les services individuels que vous ne souhaitez pas utiliser avec ce système Cloud Volumes ONTAP.
   - "En savoir plus sur Cloud Compliance".
   - "En savoir plus sur la sauvegarde dans le cloud".
   - "En savoir plus sur la surveillance".
5. **Modèles de déploiement haute disponibilité** : choisir une configuration haute disponibilité.

   Pour obtenir un aperçu des modèles de déploiement, voir "Cloud Volumes ONTAP HA pour AWS".
6. **Région et VPC** : saisissez les informations de réseau que vous avez enregistrées dans la fiche AWS.

   L'image suivante montre la page remplie pour une configuration plusieurs AZ :



7. **Connectivité et authentification SSH** : choisissez des méthodes de connexion pour la paire HA et le médiateur.
8. **IP flottantes** : si vous choisissez plusieurs adresses AZS, spécifiez les adresses IP flottantes.

   Les adresses IP doivent se trouver en dehors du bloc CIDR pour tous les VPC de la région. Pour plus de détails, voir "Configuration réseau AWS requise pour Cloud Volumes ONTAP HA dans plusieurs AZS".

9. **Tables de routage** : si vous choisissez plusieurs AZS, sélectionnez les tables de routage qui doivent inclure les routes vers les adresses IP flottantes.

   Si vous disposez de plusieurs tables de routage, il est très important de sélectionner les tables de routage correctes. Dans le cas contraire, certains clients n'ont peut-être pas accès à la paire Cloud Volumes ONTAP HA. Pour plus d'informations sur les tables de routage, voir "Documentation AWS : tables de routage".

10. **Data Encryption** : choisissez pas de cryptage de données ou de cryptage géré par AWS.

    Pour le chiffrement géré par AWS, vous pouvez choisir une autre clé maître client (CMK) dans votre compte ou un autre compte AWS.

    Une fois que vous avez créé un système Cloud Volumes ONTAP, vous ne pouvez pas modifier la méthode de chiffrement des données AWS.

    "Découvrez comment configurer le KMS AWS pour Cloud Volumes ONTAP".

    "En savoir plus sur les technologies de cryptage prises en charge".

11. **Compte sur le site de licence et de support** : indiquez si vous souhaitez utiliser le paiement à l'utilisation ou BYOL, puis indiquez un compte sur le site de support NetApp.

    Pour comprendre le fonctionnement des licences, reportez-vous à la section "Licences".

    Un compte sur le site de support NetApp est facultatif afin de bénéficier d'un paiement à l'utilisation, mais requis pour les systèmes BYOL. "Découvrez comment ajouter des comptes au site de support NetApp".

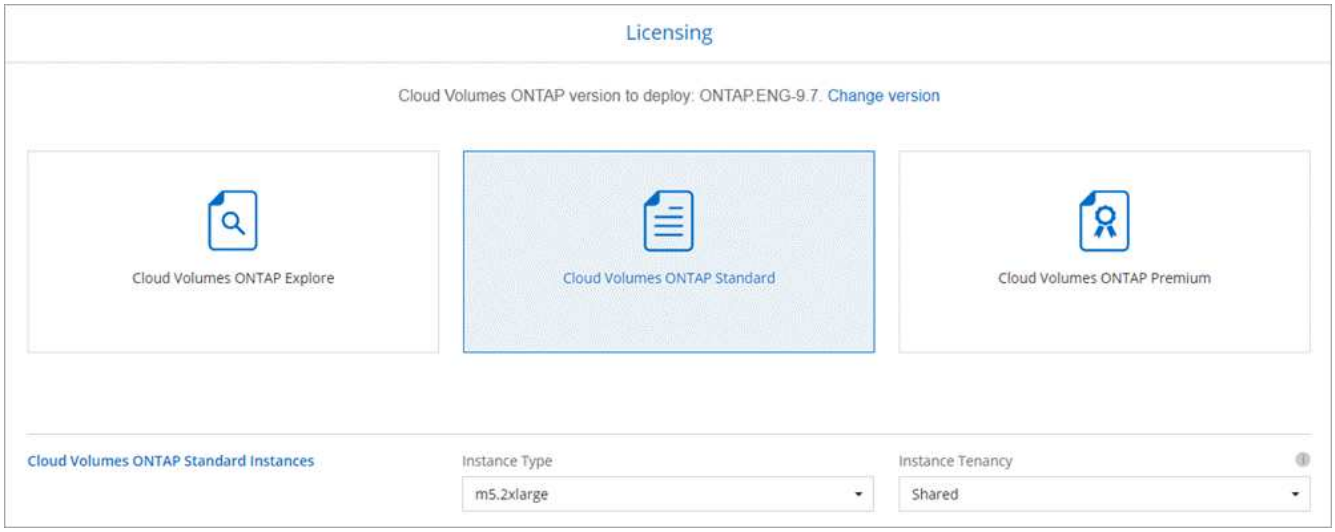
12. **Packages préconfigurés** : sélectionnez un des packages pour lancer rapidement un système Cloud Volumes ONTAP ou cliquez sur **Créer ma propre configuration**.

    Si vous choisissez l'un des packages, vous n'avez qu'à spécifier un volume, puis à revoir et approuver la configuration.

13. **Rôle IAM** : vous devez conserver l'option par défaut pour permettre à Cloud Manager de créer les rôles pour vous.

    Si vous préférez utiliser votre propre police, elle doit satisfaire "Configuration requise pour les nœuds Cloud Volumes ONTAP et le médiateur HA".

14. **Licence** : modifiez la version de Cloud Volumes ONTAP selon vos besoins, sélectionnez une licence, un type d'instance et la location d'instance.



Si vos besoins changent après le lancement des instances, vous pouvez modifier la licence ou le type d'instance ultérieurement.

> Si une version plus récente de Release Candidate, General Availability ou patch est disponible pour la version sélectionnée, Cloud Manager met à jour le système à cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.6 RC1 et 9.6 GA est disponible. La mise à jour ne se produit pas d'une version à l'autre, par exemple de 9.6 à 9.7.

15. **Ressources de stockage sous-jacentes** : Choisissez les paramètres de l'agrégat initial : un type de disque, une taille pour chaque disque et si la hiérarchisation des données doit être activée.

    Notez ce qui suit :

    - Le type de disque correspond au volume initial. Vous pouvez choisir un autre type de disque pour les volumes suivants.
    - La taille du disque correspond à tous les disques de l'agrégat initial et à tous les agrégats supplémentaires créés par Cloud Manager lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente à l'aide de l'option d'allocation avancée.

      Pour obtenir de l'aide sur le choix du type et de la taille d'un disque, reportez-vous à la section "Dimensionnement de votre système dans AWS".

    - Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
    - Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants.

      "Découvrez le fonctionnement du Tiering des données".

16. **WORM** : activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

    IMPOSSIBLE D'activer WORM si le Tiering des données était activé.

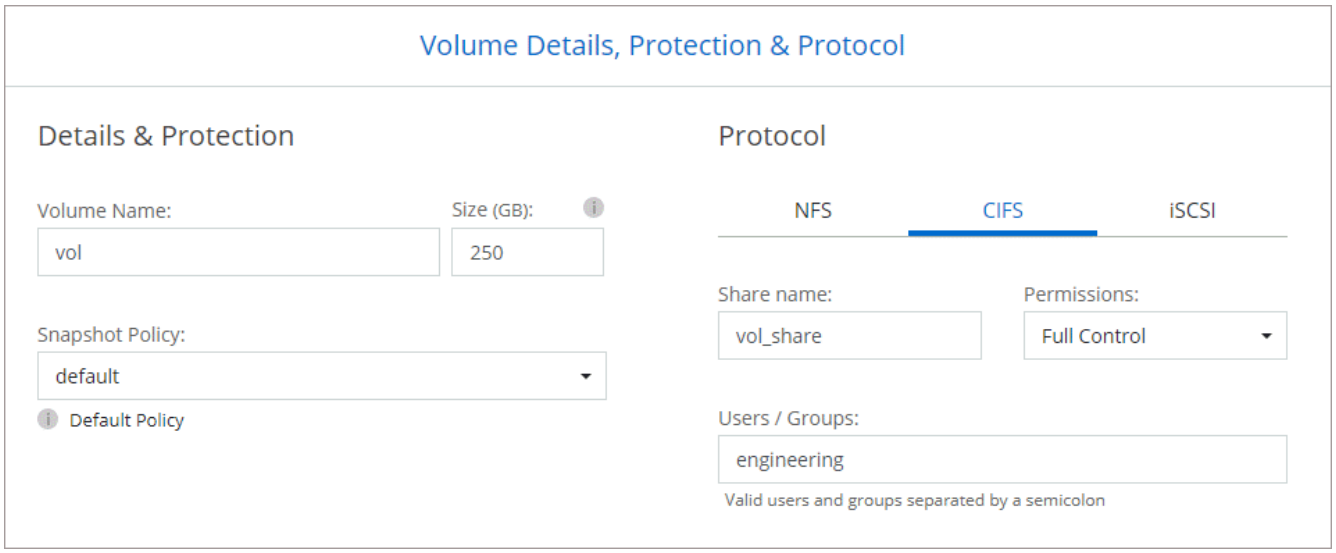
    "En savoir plus sur le stockage WORM".

17. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, Cloud Manager entre une valeur qui donne accès à toutes les instances du sous-réseau.
Autorisations et utilisateurs/groupes (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur à l'aide du format domaine\nom d'utilisateur.
Stratégie Snapshot	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de buste hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".

L'image suivante montre la page Volume remplie pour le protocole CIFS :



18. **Configuration CIFS** : si vous avez sélectionné le protocole CIFS, configurez un serveur CIFS.

Champ	Description
Adresse IP principale et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS.
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Nom de serveur CIFS unique dans le domaine AD.
Unité organisationnelle	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Si vous configurez AWS Managed Microsoft AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer **ou=ordinateurs,ou=corp** dans ce champ.
Domaine DNS	Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD.
Serveur NTP	Sélectionnez **utiliser le domaine Active Directory** pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la "Guide du développeur de l'API Cloud Manager" pour plus d'informations.

19. **Profil d'utilisation, type de disque et règle de hiérarchisation** : choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifiez la règle de hiérarchisation du volume, si nécessaire.

    Pour plus d'informations, voir "Présentation des profils d'utilisation des volumes" et "Vue d'ensemble du hiérarchisation des données".

20. **Revue et approbation** : consultez et confirmez vos choix.

a. Consultez les détails de la configuration.

b. Cliquez sur **plus d'informations** pour en savoir plus sur le support et les ressources AWS que Cloud Manager achètera.

c. Cochez les cases **Je comprends…**.

d. Cliquez sur **Go**.

Résultat

Cloud Manager lance la paire Cloud Volumes ONTAP HA. Vous pouvez suivre la progression dans la chronologie.

Si vous rencontrez des problèmes lors du lancement de la paire HA, consultez le message d'échec. Vous pouvez également sélectionner l'environnement de travail et cliquer sur Re-create environment.

Pour obtenir de l'aide supplémentaire, consultez la page "Prise en charge de NetApp Cloud Volumes ONTAP".

Une fois que vous avez terminé

- Si vous avez provisionné un partage CIFS, donnez aux utilisateurs ou aux groupes des autorisations sur les fichiers et les dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier.
- Si vous souhaitez appliquer des quotas aux volumes, utilisez System Manager ou l'interface de ligne de commande.

  Les quotas vous permettent de restreindre ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree.

Commencez à Azure

Mise en route de Cloud Volumes ONTAP pour Azure

Découvrez Cloud Volumes ONTAP pour Azure en quelques étapes.

Créer un connecteur

Si vous n'avez pas de "Connecteur" Cependant, un administrateur de compte doit en créer un. "Découvrez comment créer un connecteur dans Azure".

Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à déployer un connecteur si vous n'en possédez pas encore.

Planification de la configuration

Cloud Manager propose des packages préconfigurés qui répondent aux exigences de vos workloads, ou vous pouvez créer votre propre configuration. Dans ce dernier cas, il est important de connaître les options dont vous disposez. "En savoir plus >>".

Configurez votre réseau

1. Assurez-vous que votre VNet et vos sous-réseaux prennent en charge la connectivité entre le connecteur et Cloud Volumes ONTAP.
2. Activez l'accès Internet sortant à partir du réseau vnet cible de sorte que le connecteur et Cloud Volumes ONTAP puissent contacter plusieurs noeuds finaux.

   Cette étape est importante car le connecteur ne peut pas gérer Cloud Volumes ONTAP sans accès Internet sortant. Si vous devez limiter la connectivité sortante, reportez-vous à la liste des noeuds finaux pour "Le connecteur et le Cloud Volumes ONTAP".

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

Lancez Cloud Volumes ONTAP à l'aide de Cloud Manager

Cliquez sur **Ajouter un environnement de travail**, sélectionnez le type de système que vous souhaitez déployer et suivez les étapes de l'assistant. "Lisez les instructions détaillées".

Liens connexes

- "L'évaluation"
- "Création d'un connecteur depuis Cloud Manager"
- "Création d'un connecteur à partir d'Azure Marketplace"
- "Installation du logiciel du connecteur sur un hôte Linux"
- "Ce que fait Cloud Manager avec les autorisations Azure"

Planification de votre configuration Cloud Volumes ONTAP dans Azure

Lorsque vous déployez Cloud Volumes ONTAP dans Azure, vous pouvez soit choisir un système préconfiguré qui correspond aux exigences de vos workloads, soit créer votre propre configuration. Dans ce dernier cas, il est important de connaître les options dont vous disposez.

Choix d'un type de licence

Deux options de tarification sont disponibles pour Cloud Volumes ONTAP : le paiement à l'utilisation ou le modèle BYOL (où vous apportez votre propre licence). Le paiement basé sur l'utilisation vous permet de choisir entre trois licences : explore, Standard ou Premium. Chacune d'elles fournit une capacité distincte et des options de calcul différentes.

"Configurations prises en charge pour Cloud Volumes ONTAP 9.7 dans Azure"

Compréhension des limites de stockage

La limite de capacité brute d'un système Cloud Volumes ONTAP dépend de la licence. Des limites supplémentaires ont un impact sur la taille des agrégats et des volumes. Il est important de connaître ces dernières lors de la planification de la configuration.

"Limites de stockage pour Cloud Volumes ONTAP 9.7 dans Azure"

Dimensionnement du système dans Azure

Le dimensionnement du système Cloud Volumes ONTAP permet de répondre à vos besoins de performance et de capacité. Quelques points clés sont à noter lors de la sélection d'un type de VM, d'un type de disque et d'une taille de disque :

Type de machine virtuelle

Examinez les types de machines virtuelles prises en charge dans le "Notes de version de Cloud Volumes ONTAP" Examinez ensuite toutes les informations sur chaque type de machine virtuelle pris en charge. Notez que chaque type de VM prend en charge un nombre spécifique de disques de données.

- "Documentation Azure : tailles de machine virtuelle à usage général"
- "Documentation Azure : tailles de machines virtuelles optimisées pour la mémoire"

Type de disque Azure

Lorsque vous créez des volumes pour Cloud Volumes ONTAP, vous devez choisir le stockage cloud sous-jacent utilisé par Cloud Volumes ONTAP comme disque.

Les systèmes HAUTE DISPONIBILITÉ utilisent des objets blob de pages Premium. En parallèle, les systèmes à un seul nœud peuvent utiliser deux types de disques gérés Azure :

- *Des disques gérés SSD de premier choix* fournir des performances élevées aux charges de travail exigeantes en E/S à un coût plus élevé.
- *Des disques gérés SSD standard* assurent des performances prévisibles pour les charges de travail nécessitant un faible niveau d'IOPS.
- *Les disques gérés HDD standard* sont un bon choix si vous n'avez pas besoin d'IOPS élevées et souhaitez réduire vos coûts.

  Pour plus d'informations sur les cas d'utilisation de ces disques, reportez-vous à la section "Documentation Microsoft Azure : quels types de disques sont disponibles dans Azure ?".

Taille des disques Azure

Lorsque vous lancez des instances Cloud Volumes ONTAP, vous devez choisir la taille de disque par défaut des agrégats. Cloud Manager utilise cette taille de disque pour l'agrégat initial, et pour tous les agrégats supplémentaires que vous créez lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente de la taille par défaut "utilisation de l'option d'allocation avancée".

Tous les disques qui composent un agrégat doivent être de la même taille.

Lorsque vous choisissez une taille de disque, vous devez prendre en compte plusieurs facteurs. La taille des disques a une incidence sur le montant de vos frais de stockage, la taille des volumes que vous pouvez créer au sein d'un agrégat, la capacité totale disponible pour Cloud Volumes ONTAP et les performances de stockage.

Les performances du stockage Azure Premium sont liées à la taille des disques. Les disques de grande taille offrent des IOPS et un débit plus élevés. Par exemple, le choix de disques de 1 To peut fournir des performances supérieures à celles des disques de 500 Go, pour un coût plus élevé.

Avec un stockage standard, les performances sont les mêmes pour toutes les tailles de disques.

Choisissez la taille de disque en fonction de la capacité dont vous avez besoin.

Pour les IOPS et le débit par taille de disque, consultez Azure :

- "Microsoft Azure : tarification des disques gérés"
- "Microsoft Azure : tarification Blobs de page"

Choix d'une configuration qui prend en charge Flash cache

Une configuration Cloud Volumes ONTAP dans Azure inclut un stockage NVMe local, que Cloud Volumes ONTAP utilise comme *Flash cache* pour de meilleures performances. "En savoir plus sur Flash cache".

Fiche d'informations sur le réseau Azure

Lorsque vous déployez Cloud Volumes ONTAP dans Azure, vous devez spécifier des informations concernant votre réseau virtuel. Vous pouvez utiliser un modèle pour recueillir ces informations auprès de votre administrateur.

Informations sur Azure	Votre valeur
Région	
Réseau virtuel (vnet)	
Sous-réseau	
Groupe de sécurité réseau (s'il s'agit du vôtre)	

Sélection d'une vitesse d'écriture

Cloud Manager permet de choisir un paramètre de vitesse d'écriture pour les systèmes Cloud Volumes ONTAP à un seul nœud. Avant de choisir une vitesse d'écriture, vous devez comprendre les différences entre les paramètres normaux et élevés et les risques et les recommandations lors de l'utilisation de la vitesse d'écriture élevée.

Différence entre une vitesse d'écriture standard et une vitesse d'écriture élevée

Lorsque vous choisissez la vitesse d'écriture standard, les données sont écrites directement sur le disque, réduisant ainsi le risque de perte de données en cas d'interruption imprévue du système.

Lorsque vous choisissez la vitesse d'écriture élevée, les données sont mises en tampon dans la mémoire avant d'être écrites sur le disque, ce qui accélère les performances d'écriture. Toutefois, la mise en cache peut entraîner une perte de données en cas de panne système.

Le volume de données pouvant être perdues en cas de panne système correspond à l'étendue des deux derniers points de cohérence. Le point de cohérence consiste à écrire des données mises en tampon sur le disque. Un point de cohérence se produit lorsque le journal d'écriture est plein ou après 10 secondes (selon la première éventualité). Cependant, la performance des volumes AWS EBS peut affecter le temps de traitement des points de cohérence.

Quand utiliser une vitesse d'écriture élevée

Optez pour la vitesse d'écriture élevée si vos workloads nécessitent des performances d'écriture rapides et que vous ne craignez pas de perdre des données.

Recommandations lors de l'utilisation d'une vitesse d'écriture élevée

Si vous activez la vitesse d'écriture élevée, vous devez assurer la protection de l'écriture au niveau de la couche applicative.

Choix d'un profil d'utilisation du volume

ONTAP comprend plusieurs fonctionnalités d'efficacité du stockage qui permettent de réduire la quantité totale de stockage nécessaire. Lorsque vous créez un volume dans Cloud Manager, vous pouvez choisir un profil qui active ou désactive ces fonctionnalités. Vous devez en savoir plus sur ces fonctionnalités pour vous aider à choisir le profil à utiliser.

Les fonctionnalités d'efficacité du stockage NetApp offrent les avantages suivants :

Provisionnement fin
: Met à la disposition des hôtes ou des utilisateurs une quantité de stockage logique supérieure au stockage effectivement présent dans votre pool physique. L'espace de stockage est alloué de manière dynamique, et non au préalable, à chaque volume lors de l'écriture des données.

Déduplication
: Améliore l'efficacité en identifiant les blocs de données identiques et en les remplaçant par des références à un seul bloc partagé. Cette technique réduit les besoins de stockage en éliminant les blocs de données redondants qui résident dans le même volume.

Compression
: Réduit la capacité physique requise pour stocker les données en les compressant dans un volume sur un stockage primaire, secondaire ou d'archivage.

Exigences réseau pour déployer et gérer Cloud Volumes ONTAP dans Azure

Configurez votre réseau Azure de façon à ce que les systèmes Cloud Volumes ONTAP puissent fonctionner correctement. Cela inclut la mise en réseau pour le connecteur et le Cloud Volumes ONTAP.

Conditions requises pour Cloud Volumes ONTAP

Les exigences réseau suivantes doivent être satisfaites dans Azure.

Accès Internet sortant pour Cloud Volumes ONTAP
: Cloud Volumes ONTAP requiert un accès Internet sortant pour envoyer des messages à NetApp AutoSupport, qui surveille de façon proactive l'état de votre stockage.

  Les règles de routage et de pare-feu doivent autoriser le trafic HTTP/HTTPS vers les terminaux suivants pour que Cloud Volumes ONTAP puisse envoyer les messages AutoSupport :

  - https://support.netapp.com/aods/asupmessage
  - https://support.netapp.com/asupprod/post/1.0/postAsup

  "Découvrez comment configurer AutoSupport".

Groupes de sécurité

Vous n'avez pas besoin de créer de groupes de sécurité car Cloud Manager le fait pour vous. Si vous devez utiliser votre propre système, reportez-vous aux règles du groupe de sécurité répertoriées ci-dessous.

Nombre d'adresses IP

Cloud Manager attribue le nombre suivant d'adresses IP à Cloud Volumes ONTAP dans Azure :

- Un seul nœud : 5 adresses IP
- Paire HA : 16 adresses IP

Notez que Cloud Manager crée une LIF de gestion des SVM sur des paires haute disponibilité, mais pas sur des systèmes à un seul nœud dans Azure.

Une LIF est une adresse IP associée à un port physique. Une LIF de gestion SVM est nécessaire pour les outils de gestion tels que SnapCenter.

Connexion de Cloud Volumes ONTAP au stockage Azure Blob pour le hiérarchisation des données

Si vous souhaitez transférer les données inactives vers un stockage Azure Blob, vous n'avez pas besoin de configurer de connexion entre le Tier de performance et le Tier de capacité tant que Cloud Manager dispose des autorisations nécessaires. Cloud Manager active un terminal de service VNet pour vous si la règle Cloud Manager dispose des autorisations suivantes :

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

Ces autorisations sont incluses dans la dernière version "Politique de Cloud Manager".

Pour plus d'informations sur la configuration du Tiering des données, voir "Tiering des données inactives vers un stockage objet à faible coût".

Connexions aux systèmes ONTAP dans d'autres réseaux

Pour répliquer des données entre un système Cloud Volumes ONTAP sur les systèmes Azure et ONTAP sur d'autres réseaux, vous devez disposer d'une connexion VPN entre Azure VNet et l'autre réseau, par exemple un VPC AWS ou votre réseau d'entreprise.

Pour obtenir des instructions, reportez-vous à la section "Documentation Microsoft Azure : créez une connexion de site à site dans le portail Azure".

Configuration requise pour le connecteur

Configurez votre réseau afin que le connecteur puisse gérer les ressources et les processus au sein de votre environnement de cloud public. L'étape la plus importante consiste à garantir l'accès Internet sortant à différents terminaux.

Si votre réseau utilise un serveur proxy pour toutes les communications vers Internet, vous pouvez spécifier le serveur proxy à partir de la page Paramètres. Reportez-vous à la section "Configuration du connecteur pour utiliser un serveur proxy".

Connexions aux réseaux cibles

Un connecteur nécessite une connexion réseau aux VPC et VNets dans lesquels vous souhaitez déployer Cloud Volumes ONTAP.

Par exemple, si vous installez un connecteur sur le réseau de votre entreprise, vous devez configurer une connexion VPN sur le VPC ou le vnet dans lequel vous lancez Cloud Volumes ONTAP.

Accès Internet sortant

Le connecteur nécessite un accès Internet sortant pour gérer les ressources et les processus au sein de votre environnement de cloud public. Lors de la gestion des ressources dans Azure, un connecteur contacte les terminaux suivants :

Terminaux	Objectif
https://management.azure.com https://login.microsoftonline.com	Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans la plupart des régions d'Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans les régions d'Azure Allemagne.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans les régions d'Azure US Gov.
https://api.services.cloud.netapp.com:443	Demandes d'API à NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Permet d'accéder aux images logicielles, aux manifestes et aux modèles.
https://repo.cloud.support.netapp.com	Permet de télécharger les dépendances de Cloud Manager.
http://repo.mysql.com/	Utilisé pour télécharger MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Permet à Cloud Manager d'accéder aux manifestes, aux modèles et aux images de mise à niveau Cloud Volumes ONTAP et de les télécharger.
https://cloudmanagerinfraprod.azurecr.io	Accédez aux images logicielles des composants de conteneur pour une infrastructure exécutant Docker et fournie une solution pour les intégrations des services avec Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.
https://cloudmanager.cloud.netapp.com	Communication avec le service Cloud Manager, notamment les comptes Cloud Central.
https://netapp-cloud-account.auth0.com	Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs.
https://mysupport.netapp.com	Communication avec NetApp AutoSupport.

Terminaux	Objectif
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Communication avec NetApp pour les licences système et l'inscription au support.
https://ipa-signer.cloudmanager.netapp.com	Génération des licences par Cloud Manager (par exemple, une licence FlexCache pour Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Nécessaire pour connecter des systèmes Cloud Volumes ONTAP avec un cluster Kubernetes. Les terminaux permettent l'installation de NetApp Trident.
*.blob.core.windows.net	Requis pour les paires haute disponibilité lors de l'utilisation d'un proxy.
Divers sites tiers, par exemple : • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Les emplacements tiers sont sujets à modification.	Lors des mises à niveau, Cloud Manager télécharge les derniers packages pour les dépendances tierces.

Bien que vous devriez effectuer presque toutes les tâches à partir de l'interface utilisateur SaaS, une interface utilisateur locale est toujours disponible sur le connecteur. La machine exécutant le navigateur Web doit disposer de connexions aux terminaux suivants :

Terminaux	Objectif
L'hôte du connecteur	Vous devez entrer l'adresse IP de l'hôte depuis un navigateur Web pour charger la console Cloud Manager. En fonction de votre connectivité avec votre fournisseur de cloud, vous pouvez utiliser l'IP privée ou une adresse IP publique attribuée à l'hôte : • Une adresse IP privée fonctionne si vous disposez d'un VPN et d'un accès direct à votre réseau virtuel • Un IP public fonctionne dans tous les scénarios de mise en réseau Dans tous les cas, vous devez sécuriser l'accès au réseau en vous assurant que les règles du groupe de sécurité autorisent l'accès à partir des adresses IP ou des sous-réseaux autorisés uniquement.

Terminaux	Objectif
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Votre navigateur Web se connecte à ces terminaux pour une authentification centralisée des utilisateurs via NetApp Cloud Central.
https://widget.intercom.io	Vous bénéficiez d'un chat en ligne pour discuter avec des experts du cloud NetApp.

Règles de groupe de sécurité pour Cloud Volumes ONTAP

Cloud Manager crée des groupes de sécurité Azure qui incluent les règles entrantes et sortantes nécessaires au fonctionnement de Cloud Volumes ONTAP. Vous pouvez vous référer aux ports à des fins de test ou si vous préférez que votre utilise ses propres groupes de sécurité.

Le groupe de sécurité pour Cloud Volumes ONTAP requiert des règles entrantes et sortantes.

Règles entrantes pour les systèmes à nœud unique

Les règles énumérées ci-dessous autorisent le trafic, sauf si la description indique qu'il bloque un trafic entrant spécifique.

Priorité et nom	Port et protocole	Source et destination	Description
1000 inbound_ssh	22 TCP	De tous les types à tous	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
1001 inbound_http	80 TCP	De tous les types à tous	Accès HTTP à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
1002 inbound_111_tcp	111 TCP	De tous les types à tous	Appel de procédure à distance pour NFS
1003 inbound_111_udp	111 UDP	De tous les types à tous	Appel de procédure à distance pour NFS
1004 entrant_139	139 TCP	De tous les types à tous	Session de service NetBIOS pour CIFS
1005 inbound_161-162 _tcp	161-162 TCP	De tous les types à tous	Protocole de gestion de réseau simple
1006 inbound_161-162 _udp	161-162 UDP	De tous les types à tous	Protocole de gestion de réseau simple
1007 entrant_443	443 TCP	De tous les types à tous	Accès HTTPS à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
1008 entrant_445	445 TCP	De tous les types à tous	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS

Priorité et nom	Port et protocole	Source et destination	Description
1009 inbound_635_tcp	635 TCP	De tous les types à tous	Montage NFS
1010 inbound_635_udp	635 UDP	De tous les types à tous	Montage NFS
1011 entrant_749	749 TCP	De tous les types à tous	Kerberos
1012 inbound_2049_tcp	2049 TCP	De tous les types à tous	Démon du serveur NFS
1013 inbound_2049_udp	2049 UDP	De tous les types à tous	Démon du serveur NFS
1014 entrant_3260	3260 TCP	De tous les types à tous	Accès iSCSI via le LIF de données iSCSI
1015 inbound_4045-4046_tcp	4045-4046 TCP	De tous les types à tous	Démon de verrouillage NFS et contrôle de l'état du réseau
1016 inbound_4045-4046_udp	4045-4046 UDP	De tous les types à tous	Démon de verrouillage NFS et contrôle de l'état du réseau
1017 entrant_10000	10000 TCP	De tous les types à tous	Sauvegarde avec NDMP
1018 entrant_11104-11105	11104-11105 TCP	De tous les types à tous	Transfert de données SnapMirror
3000 inbound_deny _all_tcp	Tout port TCP	De tous les types à tous	Bloquer tout autre trafic TCP entrant
3001 inbound_deny _all_udp	Tout port UDP	De tous les types à tous	Bloquer tout autre trafic entrant UDP
65000 AllowVnetInBound	N'importe quel protocole	VirtualNetwork à VirtualNetwork	Trafic entrant depuis le réseau VNet
65001 AllowAzureLoad BalancerInBound	N'importe quel protocole	AzureLoadBalancer à tout	Le trafic de données à partir d'Azure Standard Load Balancer
65500 DenyAllInBound	N'importe quel protocole	De tous les types à tous	Bloquer tout autre trafic entrant

Règles entrantes pour les systèmes HA

Les règles énumérées ci-dessous autorisent le trafic, sauf si la description indique qu'il bloque un trafic entrant spécifique.

Les systèmes HAUTE DISPONIBILITÉ disposent de règles entrantes moins strictes que les systèmes à un seul nœud, car le trafic des données entrantes transite par Azure Standard Load Balancer. Pour cette raison, le trafic provenant du Load Balancer doit être ouvert, comme indiqué dans la règle AllowAzureLoadBalancerInBound.

Priorité et nom	Port et protocole	Source et destination	Description
100 entrant_443	443 tout protocole	De tous les types à tous	Accès HTTPS à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
101 inbound_111_tcp	111 tout protocole	De tous les types à tous	Appel de procédure à distance pour NFS
102 inbound_2049_tcp	2049 tout protocole	De tous les types à tous	Démon du serveur NFS
111 inbound_ssh	22 tout protocole	De tous les types à tous	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
121 entrant_53	53 tout protocole	De tous les types à tous	DNS et CIFS
65000 AllowVnetInBound	N'importe quel protocole	VirtualNetwork à VirtualNetwork	Trafic entrant depuis le réseau VNet
65001 AllowAzureLoad BalancerInBound	N'importe quel protocole	AzureLoadBalancer à tout	Le trafic de données à partir d'Azure Standard Load Balancer
65500 DenyAllInBound	N'importe quel protocole	De tous les types à tous	Bloquer tout autre trafic entrant

Règles de sortie

Le groupe de sécurité prédéfini pour Cloud Volumes ONTAP ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour Cloud Volumes ONTAP inclut les règles de sortie suivantes.

Port	Protocole	Objectif
Tout	Tous les protocoles TCP	Tout le trafic sortant
Tout	Tous les protocoles UDP	Tout le trafic sortant

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par Cloud Volumes ONTAP.

La source est l'interface (adresse IP) du système Cloud Volumes ONTAP.

Service	Port	Protocole	Source	Destination	Objectif
Active Directory	88	TCP	FRV de gestion des nœuds	Forêt Active Directory	Authentification Kerberos V.
	137	UDP	FRV de gestion des nœuds	Forêt Active Directory	Service de noms NetBIOS
	138	UDP	FRV de gestion des nœuds	Forêt Active Directory	Service de datagrammes NetBIOS
	139	TCP	FRV de gestion des nœuds	Forêt Active Directory	Session de service NetBIOS
	389	TCP ET UDP	FRV de gestion des nœuds	Forêt Active Directory	LDAP
	445	TCP	FRV de gestion des nœuds	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	464	TCP	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	464	UDP	FRV de gestion des nœuds	Forêt Active Directory	Administration des clés Kerberos
	749	TCP	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)
	88	TCP	LIF de données (NFS, CIFS, iSCSI)	Forêt Active Directory	Authentification Kerberos V.
	137	UDP	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de noms NetBIOS
	138	UDP	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de datagrammes NetBIOS
	139	TCP	FRV de données (NFS, CIFS)	Forêt Active Directory	Session de service NetBIOS
	389	TCP ET UDP	FRV de données (NFS, CIFS)	Forêt Active Directory	LDAP
	445	TCP	FRV de données (NFS, CIFS)	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	464	TCP	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	464	UDP	FRV de données (NFS, CIFS)	Forêt Active Directory	Administration des clés Kerberos
	749	TCP	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)
DHCP	68	UDP	FRV de gestion des nœuds	DHCP	Client DHCP pour la première configuration

Service	Port	Protocole	Source	Destination	Objectif
DHCPS	67	UDP	FRV de gestion des nœuds	DHCP	Serveur DHCP
DNS	53	UDP	FRV de gestion des nœuds et FRV de données (NFS, CIFS)	DNS	DNS
NDMP	18600-18699	TCP	FRV de gestion des nœuds	Serveurs de destination	Copie NDMP
SMTP	25	TCP	FRV de gestion des nœuds	Serveur de messagerie	Les alertes SMTP peuvent être utilisées pour AutoSupport
SNMP	161	TCP	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	161	UDP	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	162	TCP	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	162	UDP	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
SnapMirror	11104	TCP	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Gestion des sessions de communication intercluster pour SnapMirror
	11105	TCP	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Transfert de données SnapMirror
Syslog	514	UDP	FRV de gestion des nœuds	Serveur Syslog	Messages de transfert syslog

Règles de groupe de sécurité pour le connecteur

Le groupe de sécurité du connecteur nécessite à la fois des règles entrantes et sortantes.

Règles entrantes

La source des règles entrantes dans le groupe de sécurité prédéfini est 0.0.0.0/0.

Port	Protocole	Objectif
22	SSH	Fournit un accès SSH à l'hôte du connecteur
80	HTTP	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale

Port	Protocole	Objectif
443	HTTPS	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale

Règles de sortie

Le groupe de sécurité prédéfini pour le connecteur ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour le connecteur inclut les règles de trafic sortant suivantes.

Port	Protocole	Objectif
Tout	Tous les protocoles TCP	Tout le trafic sortant
Tout	Tous les protocoles UDP	Tout le trafic sortant

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par le connecteur.

L'adresse IP source est l'hôte du connecteur.

Service	Port	Protocole	Destination	Objectif
Active Directory	88	TCP	Forêt Active Directory	Authentification Kerberos V.
	139	TCP	Forêt Active Directory	Session de service NetBIOS
	389	TCP	Forêt Active Directory	LDAP
	445	TCP	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	464	TCP	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	749	TCP	Forêt Active Directory	Modification et définition du mot de passe de Kerberos V Active Directory (RPCSEC_GSS)
	137	UDP	Forêt Active Directory	Service de noms NetBIOS
	138	UDP	Forêt Active Directory	Service de datagrammes NetBIOS
	464	UDP	Forêt Active Directory	Administration des clés Kerberos
Appels API et AutoSupport	443	HTTPS	LIF de gestion de cluster ONTAP et Internet sortant	API appelle AWS et ONTAP et envoie des messages AutoSupport à NetApp
Appels API	3000	TCP	LIF de gestion de cluster ONTAP	Appels API vers ONTAP
DNS	53	UDP	DNS	Utilisé pour la résolution DNS par Cloud Manager

Lancement d'Cloud Volumes ONTAP dans Azure

Vous pouvez lancer un système à un seul nœud ou une paire HA dans Azure en créant un environnement de travail Cloud Volumes ONTAP dans Cloud Manager.

Avant de commencer

- Vous devez avoir un "Connecteur associé à votre espace de travail".

Vous devez être un administrateur de compte pour créer un connecteur. Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l'avez pas encore fait.

- "Vous devez être prêt à laisser le connecteur fonctionner en permanence".
- Vous devez avoir choisi une configuration et obtenir des informations de mise en réseau Azure auprès de votre administrateur. Pour plus de détails, voir "Planification de votre configuration Cloud Volumes ONTAP".
- Pour déployer un système BYOL, vous devez disposer du numéro de série à 20 chiffres (clé de licence) pour chaque nœud.

Description de la tâche

Lorsque Cloud Manager crée un système Cloud Volumes ONTAP dans Azure, il crée plusieurs objets Azure, comme un groupe de ressources, des interfaces réseau et des comptes de stockage. Vous pouvez consulter un résumé des ressources à la fin de l'assistant.

Risque de perte de données

Le déploiement d'Cloud Volumes ONTAP dans un groupe de ressources existant et partagées n'est pas recommandé en raison du risque de perte de données. Lorsque la restauration est actuellement désactivée par défaut lors de l'utilisation de l'API pour le déploiement dans un groupe de ressources existant, la suppression de Cloud Volumes ONTAP risque de supprimer d'autres ressources de ce groupe partagé.

Il est recommandé d'utiliser un nouveau groupe de ressources dédié pour Cloud Volumes ONTAP. Il s'agit de l'option par défaut et uniquement recommandée pour le déploiement de Cloud Volumes ONTAP dans Azure à partir de Cloud Manager.

Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
2. **Choisissez un emplacement** : sélectionnez **Microsoft Azure** et **Cloud Volumes ONTAP nœud unique** ou **Cloud Volumes ONTAP haute disponibilité**.
3. **Détails et informations d'identification** : modifiez éventuellement les informations d'identification et l'abonnement Azure, spécifiez un nom de cluster et de groupe de ressources, ajoutez des balises si nécessaire, puis spécifiez des informations d'identification.

   Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Nom de l'environnement de travail	Cloud Manager utilise le nom de l'environnement de travail pour nommer à la fois le système Cloud Volumes ONTAP et la machine virtuelle Azure. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.

Champ	Description
Nom du groupe de ressources	Conservez le nom par défaut du nouveau groupe de ressources ou décochez **utiliser par défaut** et entrez votre propre nom pour le nouveau groupe de ressources. Il est recommandé d'utiliser un nouveau groupe de ressources dédié pour Cloud Volumes ONTAP. S'il est possible de déployer Cloud Volumes ONTAP dans un groupe de ressources existant et partagé à l'aide de l'API, il n'est pas recommandé en raison du risque de perte de données. Voir l'avertissement ci-dessus pour plus de détails.
Étiquettes	Les étiquettes sont des métadonnées pour vos ressources Azure. Lorsque vous saisissez des balises dans ce champ, Cloud Manager les ajoute au groupe de ressources associé au système Cloud Volumes ONTAP. Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section "Documentation Microsoft Azure : utilisation des balises pour organiser vos ressources Azure".
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte d'administration du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via OnCommand System Manager ou sa CLI.
Modifier les informations d'identification	Vous pouvez choisir plusieurs identifiants Azure et un autre abonnement Azure à utiliser avec ce système Cloud Volumes ONTAP. Vous devez associer un abonnement Azure Marketplace à l'abonnement Azure sélectionné pour déployer un système Cloud Volumes ONTAP basé sur l'utilisation. "Apprenez à ajouter des informations d'identification".

La vidéo suivante explique comment associer un abonnement Marketplace à un abonnement Azure :

► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_azure.mp4 *(video)*

4. **Services** : conservez les services activés ou désactivez les services individuels que vous ne souhaitez pas utiliser avec Cloud Volumes ONTAP.
   - "En savoir plus sur Cloud Compliance".
   - "En savoir plus sur la sauvegarde dans le cloud".
5. **Localisation et connectivité** : sélectionnez un emplacement et un groupe de sécurité et cochez la case pour confirmer la connectivité réseau entre Cloud Manager et l'emplacement cible.
6. **Compte sur le site de licence et de support** : indiquez si vous souhaitez utiliser le paiement à l'utilisation ou BYOL, puis indiquez un compte sur le site de support NetApp.

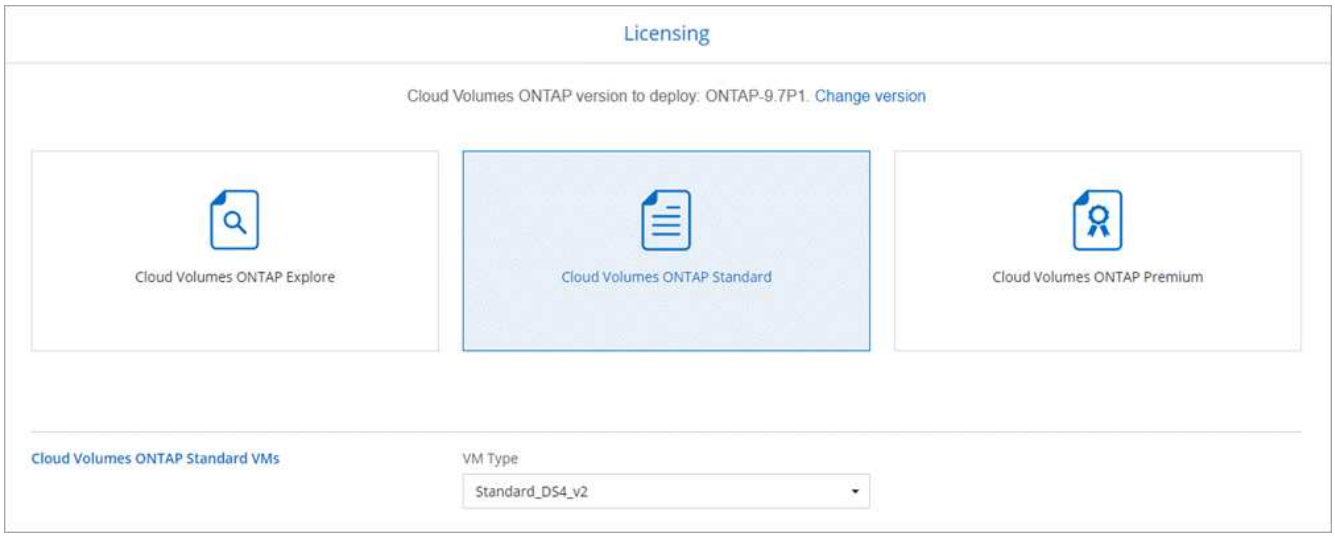
   Pour comprendre le fonctionnement des licences, reportez-vous à la section "Licences".

   Un compte sur le site de support NetApp est facultatif afin de bénéficier d'un paiement à l'utilisation, mais requis pour les systèmes BYOL. "Découvrez comment ajouter des comptes au site de support NetApp".

7. **Packages préconfigurés** : Shelect un des packages pour déployer rapidement un système Cloud Volumes ONTAP, ou cliquez sur **Créer ma propre configuration**.

   Si vous choisissez l'un des packages, vous n'avez qu'à spécifier un volume, puis à revoir et approuver la configuration.

8. **Licence** : modifiez la version de Cloud Volumes ONTAP selon vos besoins, sélectionnez une licence et sélectionnez un type de machine virtuelle.



Si vos besoins changent après le lancement du système, vous pouvez modifier la licence ou le type de machine virtuelle ultérieurement.

> Si une version plus récente de Release Candidate, General Availability ou patch est disponible pour la version sélectionnée, Cloud Manager met à jour le système à cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.6 RC1 et 9.6 GA est disponible. La mise à jour ne se produit pas d'une version à l'autre, par exemple de 9.6 à 9.7.

9. **Abonnez-vous à partir d'Azure Marketplace**: Suivez les étapes si Cloud Manager n'a pas pu activer les déploiements programmatiques de Cloud Volumes ONTAP.
10. **Ressources de stockage sous-jacentes** : Choisissez les paramètres de l'agrégat initial : un type de disque, une taille pour chaque disque et si le Tiering des données vers stockage Blob doit être activé.

    Notez ce qui suit :

    - Le type de disque correspond au volume initial. Vous pouvez choisir un autre type de disque pour les volumes suivants.
    - La taille du disque correspond à tous les disques de l'agrégat initial et à tous les agrégats supplémentaires créés par Cloud Manager lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente à l'aide de l'option d'allocation avancée.

      Pour obtenir de l'aide sur le choix du type et de la taille d'un disque, reportez-vous à la section "Dimensionnement du système dans Azure".

    - Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
    - Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants.

      "En savoir plus sur le Tiering des données".

11. **Vitesse d'écriture et WORM** (systèmes à un seul nœud uniquement) : choisissez **Normal** ou **vitesse d'écriture élevée** et activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

La sélection d'une vitesse d'écriture est prise en charge avec les systèmes à un seul nœud uniquement.

"En savoir plus sur la vitesse d'écriture".

IMPOSSIBLE D'activer WORM si le Tiering des données était activé.

"En savoir plus sur le stockage WORM".

12. **Secure communication to Storage & WORM** (HA uniquement) : permet d'activer ou non une connexion HTTPS aux comptes de stockage Azure et d'activer le stockage WORM (Write Once, Read Many), si nécessaire.

    La connexion HTTPS est établie depuis une paire HA Cloud Volumes ONTAP 9.7 vers les comptes de stockage Azure. Notez que l'activation de cette option peut avoir un impact sur les performances d'écriture. Vous ne pouvez pas modifier le paramètre après avoir créé l'environnement de travail.

    "En savoir plus sur le stockage WORM".

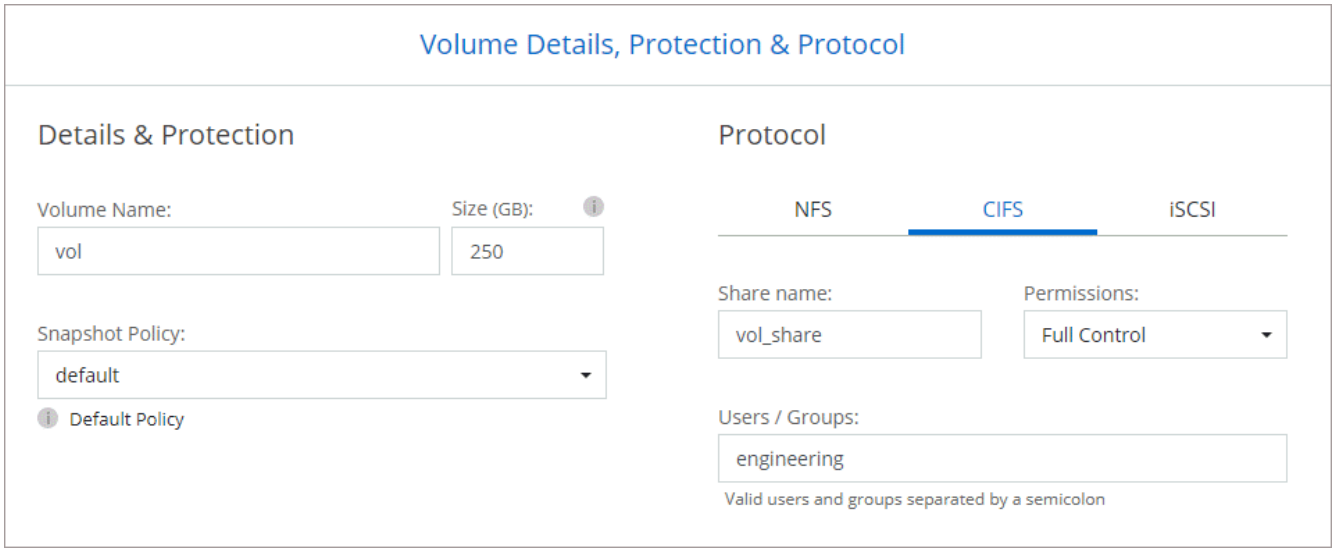
13. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

    Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, Cloud Manager entre une valeur qui donne accès à toutes les instances du sous-réseau.
Autorisations et utilisateurs/groupes (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur à l'aide du format domaine\nom d'utilisateur.
Stratégie Snapshot	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.

Champ	Description
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de buste hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".

L'image suivante montre la page Volume remplie pour le protocole CIFS :



14. **Configuration CIFS** : si vous choisissez le protocole CIFS, configurez un serveur CIFS.

Champ	Description
Adresse IP principale et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS.
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Nom de serveur CIFS unique dans le domaine AD.

Champ	Description
Unité organisationnelle	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Pour configurer les services de domaine Azure AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer **ou=ordinateurs ADDC** ou **ou=utilisateurs ADDC** dans ce champ.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentation Azure : créez une unité organisationnelle dans un domaine géré Azure AD Domain Services"^]
Domaine DNS	Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD.
Serveur NTP	Sélectionnez **utiliser le domaine Active Directory** pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la "Guide du développeur de l'API Cloud Manager" pour plus d'informations.

15. **Profil d'utilisation, type de disque et règle de hiérarchisation** : choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifiez la règle de hiérarchisation du volume, si nécessaire.

    Pour plus d'informations, voir "Présentation des profils d'utilisation des volumes" et "Vue d'ensemble du hiérarchisation des données".

16. **Revue et approbation** : consultez et confirmez vos choix.
    a. Consultez les détails de la configuration.
    b. Cliquez sur **plus d'informations** pour en savoir plus sur le support et les ressources Azure que Cloud Manager achètera.
    c. Cochez les cases **Je comprends…**.
    d. Cliquez sur **Go**.

Résultat

Cloud Manager déploie le système Cloud Volumes ONTAP. Vous pouvez suivre la progression dans la chronologie.

Si vous rencontrez des problèmes lors du déploiement du système Cloud Volumes ONTAP, consultez le message d'échec. Vous pouvez également sélectionner l'environnement de travail et cliquer sur **recréer l'environnement**.

Pour obtenir de l'aide supplémentaire, consultez la page "Prise en charge de NetApp Cloud Volumes ONTAP".

Une fois que vous avez terminé

- Si vous avez provisionné un partage CIFS, donnez aux utilisateurs ou aux groupes des autorisations sur les fichiers et les dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier.
- Si vous souhaitez appliquer des quotas aux volumes, utilisez System Manager ou l'interface de ligne de commande.

  Les quotas vous permettent de restreindre ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree.

Lancez-vous dans GCP

Mise en route avec Cloud Volumes ONTAP pour Google Cloud

Lancez-vous avec Cloud Volumes ONTAP pour GCP en quelques étapes.

Créer un connecteur

Si vous n'avez pas de "Connecteur" Cependant, un administrateur de compte doit en créer un. "Découvrez comment créer un connecteur dans GCP".

Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à déployer un connecteur si vous n'en possédez pas encore.

Planification de la configuration

Cloud Manager propose des packages préconfigurés qui répondent aux exigences de vos workloads, ou vous pouvez créer votre propre configuration. Dans ce dernier cas, il est important de connaître les options dont vous disposez. "En savoir plus >>".

Configurez votre réseau

1. Vérifiez que votre VPC et vos sous-réseaux prennent en charge la connectivité entre le connecteur et Cloud Volumes ONTAP.
2. Activez l'accès Internet sortant à partir du VPC cible de sorte que le connecteur et le Cloud Volumes ONTAP puissent contacter plusieurs terminaux.

   Cette étape est importante car le connecteur ne peut pas gérer Cloud Volumes ONTAP sans accès Internet sortant. Si vous devez limiter la connectivité sortante, reportez-vous à la liste des noeuds finaux pour "Le connecteur et le Cloud Volumes ONTAP".

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

Configuration de GCP pour le Tiering des données

Deux exigences doivent être remplies pour transférer les données inactives de Cloud Volumes ONTAP vers un stockage objet à faible coût (un compartiment Google Cloud Storage) :

1. "Configurez le sous-réseau Cloud Volumes ONTAP pour un accès privé à Google".
2. "Configurez un compte de service pour le Tiering des données":
   - Attribuez le rôle *Storage Admin* prédéfini au compte de service de hiérarchisation.
   - Ajoutez le compte de service Connector en tant que *Service Account User* au compte de service Tiering.

Vous pouvez indiquer le rôle d'utilisateur "à l'étape 3 de l'assistant lorsque vous créez le compte de service de tiering", ou "attribuez le rôle après la création du compte de service".

Lorsque vous créez un environnement de travail Cloud Volumes ONTAP, vous devrez sélectionner le compte de service de Tiering.

Si vous n'activez pas le Tiering des données et sélectionnez un compte de service lorsque vous créez le système Cloud Volumes ONTAP, vous devrez désactiver le système et ajouter le compte de service à Cloud Volumes ONTAP à partir de la console GCP.

Activez les API Google Cloud

"Activez les API Google Cloud suivantes dans votre projet". Ces API sont nécessaires pour déployer le connecteur et Cloud Volumes ONTAP.

- API Cloud Deployment Manager V2
- API de journalisation cloud
- API Cloud Resource Manager
- API du moteur de calcul
- API de gestion des identités et des accès

Lancez Cloud Volumes ONTAP à l'aide de Cloud Manager

Cliquez sur **Ajouter un environnement de travail**, sélectionnez le type de système que vous souhaitez déployer et suivez les étapes de l'assistant. "Lisez les instructions détaillées".

Liens connexes

- "L'évaluation"
- "Création d'un connecteur depuis Cloud Manager"
- "Installation du logiciel du connecteur sur un hôte Linux"
- "Avantages de Cloud Manager avec les autorisations GCP"

Planification de votre configuration Cloud Volumes ONTAP dans Google Cloud

Lorsque vous déployez Cloud Volumes ONTAP dans Google Cloud, vous pouvez soit choisir un système préconfiguré qui correspond aux exigences de vos workloads, soit créer votre propre configuration. Dans ce dernier cas, il est important de connaître les options dont vous disposez.

Choix d'un type de licence

Deux options de tarification sont disponibles pour Cloud Volumes ONTAP : le paiement à l'utilisation ou le modèle BYOL (où vous apportez votre propre licence). Le paiement basé sur l'utilisation vous permet de choisir entre trois licences : explore, Standard ou Premium. Chacune d'elles fournit une capacité distincte et des options de calcul différentes.

"Configurations prises en charge pour Cloud Volumes ONTAP 9.7 dans GCP"

Compréhension des limites de stockage

La limite de capacité brute d'un système Cloud Volumes ONTAP dépend de la licence. Des limites supplémentaires ont un impact sur la taille des agrégats et des volumes. Il est important de connaître ces dernières lors de la planification de la configuration.

"Limites de stockage pour Cloud Volumes ONTAP 9.7 dans GCP"

Dimensionnement du système dans GCP

Le dimensionnement du système Cloud Volumes ONTAP permet de répondre à vos besoins de performance et de capacité. Quelques points clés sont à noter lors de la sélection d'un type de machine, d'un type de disque et d'une taille de disque :

Type de machine

Examiner les types de machine pris en charge dans le "Notes de version de Cloud Volumes ONTAP" Puis passez en revue les détails de Google concernant chaque type de machine pris en charge. Faites correspondre les exigences de vos charges de travail au nombre de CPU virtuels et à la mémoire correspondant au type de machine. Notez que chaque cœur de processeur augmente les performances réseau.

Pour plus de détails, reportez-vous aux sections suivantes :

- "Documentation Google Cloud : types de machine standard N1"
- "Documentation Google Cloud : performances"

Type de disque GCP

Lorsque vous créez des volumes pour Cloud Volumes ONTAP, vous devez choisir le stockage cloud sous-jacent utilisé par Cloud Volumes ONTAP pour un disque. Le type de disque peut être soit *Zonal SSD persistent disks* soit *Zonal standard persistent disks*.

Les disques persistants des disques SSD sont parfaitement adaptés aux charges de travail qui exigent des taux élevés d'IOPS aléatoires, tandis que les disques persistants standard sont économiques et peuvent prendre en charge des opérations de lecture/écriture séquentielles. Pour plus de détails, voir "Documentation Google Cloud : disques persistants zonés (standard et SSD)".

Taille des disques GCP

Lorsque vous déployez un système Cloud Volumes ONTAP, vous devez choisir la taille de disque initiale. Après cela, Cloud Manager vous permet de gérer la capacité d'un système, mais si vous souhaitez créer vous-même des agrégats, sachez que :

- Tous les disques qui composent un agrégat doivent être de la même taille.
- Déterminez l'espace dont vous avez besoin tout en prenant en compte les performances.
- Les performances des disques persistants évoluent automatiquement en fonction de la taille des disques et du nombre de CPU virtuels disponibles pour le système.

  Pour plus de détails, reportez-vous aux sections suivantes :

  - "Documentation Google Cloud : disques persistants zonés (standard et SSD)"
  - "Documentation Google Cloud : optimisation des performances des disques persistants et des SSD locaux"

Fiche technique d'informations réseau GCP

Lorsque vous déployez Cloud Volumes ONTAP dans GCP, vous devez spécifier des informations relatives à votre réseau virtuel. Vous pouvez utiliser un modèle pour recueillir ces informations auprès de votre administrateur.

Informations GCP	Votre valeur
Région	
Zone	
Réseau VPC	
Sous-réseau	
Politique de pare-feu (s'il s'agit du vôtre)	

Sélection d'une vitesse d'écriture

Cloud Manager permet de choisir un paramètre de vitesse d'écriture pour les systèmes Cloud Volumes ONTAP à un seul nœud. Avant de choisir une vitesse d'écriture, vous devez comprendre les différences entre les paramètres normaux et élevés et les risques et les recommandations lors de l'utilisation de la vitesse d'écriture élevée.

Différence entre une vitesse d'écriture standard et une vitesse d'écriture élevée

Lorsque vous choisissez la vitesse d'écriture standard, les données sont écrites directement sur le disque, réduisant ainsi le risque de perte de données en cas d'interruption imprévue du système.

Lorsque vous choisissez la vitesse d'écriture élevée, les données sont mises en tampon dans la mémoire avant d'être écrites sur le disque, ce qui accélère les performances d'écriture. Toutefois, la mise en cache peut entraîner une perte de données en cas de panne système.

Le volume de données pouvant être perdues en cas de panne système correspond à l'étendue des deux derniers points de cohérence. Le point de cohérence consiste à écrire des données mises en tampon sur le disque. Un point de cohérence se produit lorsque le journal d'écriture est plein ou après 10 secondes (selon la première éventualité). Cependant, la performance des volumes AWS EBS peut affecter le temps de traitement des points de cohérence.

Quand utiliser une vitesse d'écriture élevée

Optez pour la vitesse d'écriture élevée si vos workloads nécessitent des performances d'écriture rapides et que vous ne craignez pas de perdre des données.

Recommandations lors de l'utilisation d'une vitesse d'écriture élevée

Si vous activez la vitesse d'écriture élevée, vous devez assurer la protection de l'écriture au niveau de la couche applicative.

Choix d'un profil d'utilisation du volume

ONTAP comprend plusieurs fonctionnalités d'efficacité du stockage qui permettent de réduire la quantité totale de stockage nécessaire. Lorsque vous créez un volume dans Cloud Manager, vous pouvez choisir un profil qui active ou désactive ces fonctionnalités. Vous devez en savoir plus sur ces fonctionnalités pour vous aider à

choisir le profil à utiliser.

Les fonctionnalités d'efficacité du stockage NetApp offrent les avantages suivants :

Provisionnement fin

Met à la disposition des hôtes ou des utilisateurs une quantité de stockage logique supérieure au stockage effectivement présent dans votre pool physique. L'espace de stockage est alloué de manière dynamique, et non au préalable, à chaque volume lors de l'écriture des données.

Déduplication

Améliore l'efficacité en identifiant les blocs de données identiques et en les remplaçant par des références à un seul bloc partagé. Cette technique réduit les besoins de stockage en éliminant les blocs de données redondants qui résident dans le même volume.

Compression

Réduit la capacité physique requise pour stocker les données en les compressant dans un volume sur un stockage primaire, secondaire ou d'archivage.

Exigences de mise en réseau pour le déploiement et la gestion de Cloud Volumes ONTAP dans GCP

Configurez votre réseau Google Cloud Platform de manière à ce que les systèmes Cloud Volumes ONTAP puissent fonctionner correctement. Cela inclut la mise en réseau pour le connecteur et le Cloud Volumes ONTAP.

Conditions requises pour Cloud Volumes ONTAP

Les exigences suivantes doivent être satisfaites dans GCP.

Cloud privé virtuel

Cloud Volumes ONTAP et le connecteur sont pris en charge dans un VPC partagé par Google Cloud et dans des VPC non partagés.

Un VPC partagé vous permet de configurer et de gérer de manière centralisée les réseaux virtuels dans plusieurs projets. Vous pouvez configurer des réseaux VPC partagés dans le projet *host* et déployer les instances de machines virtuelles Connector et Cloud Volumes ONTAP dans un projet *service*. "Documentation Google Cloud : présentation du VPC partagé".

La seule exigence concernant l'utilisation d'un VPC partagé est de fournir le "Rôle utilisateur du réseau de calcul" Vers le compte de service Connector. Cloud Manager a besoin de ces autorisations pour interroger les pare-feu, le VPC et les sous-réseaux du projet hôte.

Accès Internet sortant pour Cloud Volumes ONTAP

Cloud Volumes ONTAP requiert un accès Internet sortant pour envoyer des messages à NetApp AutoSupport, qui surveille de façon proactive l'état de votre stockage.

Les règles de routage et de pare-feu doivent autoriser le trafic HTTP/HTTPS vers les terminaux suivants pour que Cloud Volumes ONTAP puisse envoyer les messages AutoSupport :

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

"Découvrez comment configurer AutoSupport".

Nombre d'adresses IP

Cloud Manager attribue 5 adresses IP à Cloud Volumes ONTAP dans GCP.

Notez que Cloud Manager ne crée pas de LIF de gestion des SVM pour Cloud Volumes ONTAP dans GCP.

Une LIF est une adresse IP associée à un port physique. Une LIF de gestion SVM est nécessaire pour les outils de gestion tels que SnapCenter.

Règles de pare-feu

Inutile de créer des règles de pare-feu, car Cloud Manager le fait pour vous. Si vous devez vous en servir, reportez-vous aux règles de pare-feu répertoriées ci-dessous.

Connexion de Cloud Volumes ONTAP à Google Cloud Storage pour le Tiering des données

Pour transférer des données inactives vers un compartiment Google Cloud Storage, le sous-réseau dans lequel réside Cloud Volumes ONTAP doit être configuré pour un accès Google privé. Pour obtenir des instructions, reportez-vous à la section "Documentation Google Cloud : configuration de Private Google Access".

Pour connaître les étapes supplémentaires requises pour la configuration du Tiering des données dans Cloud Manager, consultez la section "Tiering des données inactives vers un stockage objet à faible coût".

Connexions aux systèmes ONTAP dans d'autres réseaux

Pour répliquer les données entre un système Cloud Volumes ONTAP dans GCP et des systèmes ONTAP d'autres réseaux, vous devez disposer d'une connexion VPN entre le VPC et l'autre réseau, par exemple votre réseau d'entreprise.

Pour obtenir des instructions, reportez-vous à la section "Documentation Google Cloud : présentation de Cloud VPN".

Configuration requise pour le connecteur

Configurez votre réseau afin que le connecteur puisse gérer les ressources et les processus au sein de votre environnement de cloud public. L'étape la plus importante consiste à garantir l'accès Internet sortant à différents terminaux.

Si votre réseau utilise un serveur proxy pour toutes les communications vers Internet, vous pouvez spécifier le serveur proxy à partir de la page Paramètres. Reportez-vous à la section "Configuration du connecteur pour utiliser un serveur proxy".

Connexion aux réseaux cibles

Un connecteur nécessite une connexion réseau aux VPC et VNets dans lesquels vous souhaitez déployer Cloud Volumes ONTAP.

Par exemple, si vous installez un connecteur sur le réseau de votre entreprise, vous devez configurer une connexion VPN sur le VPC ou le vnet dans lequel vous lancez Cloud Volumes ONTAP.

Accès Internet sortant

Le connecteur nécessite un accès Internet sortant pour gérer les ressources et les processus au sein de votre environnement de cloud public. Lors de la gestion des ressources dans GCP, un connecteur contacte les terminaux suivants :

Terminaux	Objectif
https://www.googleapis.com	Permet au connecteur de contacter les API Google pour le déploiement et la gestion de Cloud Volumes ONTAP dans GCP.
https://api.services.cloud.netapp.com:443	Demandes d'API à NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Permet d'accéder aux images logicielles, aux manifestes et aux modèles.
https://repo.cloud.support.netapp.com	Permet de télécharger les dépendances de Cloud Manager.
http://repo.mysql.com/	Utilisé pour télécharger MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Permet au connecteur d'accéder aux manifestes, aux modèles et aux images de mise à niveau Cloud Volumes ONTAP et de les télécharger.
https://cloudmanagerinfraprod.azurecr.io	Accédez aux images logicielles des composants de conteneur pour une infrastructure exécutant Docker et fournie une solution pour les intégrations des services avec Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.
https://cloudmanager.cloud.netapp.com	Communication avec le service Cloud Manager, notamment les comptes Cloud Central.
https://netapp-cloud-account.auth0.com	Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs.
https://mysupport.netapp.com	Communication avec NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Communication avec NetApp pour les licences système et l'inscription au support.
https://ipa-signer.cloudmanager.netapp.com	Génération des licences par Cloud Manager (par exemple, une licence FlexCache pour Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Nécessaire pour connecter des systèmes Cloud Volumes ONTAP avec un cluster Kubernetes. Les terminaux permettent l'installation de NetApp Trident.

Terminaux	Objectif
Divers sites tiers, par exemple : • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Les emplacements tiers sont sujets à modification.	Lors des mises à niveau, Cloud Manager télécharge les derniers packages pour les dépendances tierces.

Bien que vous devriez effectuer presque toutes les tâches à partir de l'interface utilisateur SaaS, une interface utilisateur locale est toujours disponible sur le connecteur. La machine exécutant le navigateur Web doit disposer de connexions aux terminaux suivants :

Terminaux	Objectif
L'hôte du connecteur	Vous devez entrer l'adresse IP de l'hôte depuis un navigateur Web pour charger la console Cloud Manager. En fonction de votre connectivité avec votre fournisseur de cloud, vous pouvez utiliser l'IP privée ou une adresse IP publique attribuée à l'hôte : • Une adresse IP privée fonctionne si vous disposez d'un VPN et d'un accès direct à votre réseau virtuel • Un IP public fonctionne dans tous les scénarios de mise en réseau Dans tous les cas, vous devez sécuriser l'accès au réseau en vous assurant que les règles du groupe de sécurité autorisent l'accès à partir des adresses IP ou des sous-réseaux autorisés uniquement.
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Votre navigateur Web se connecte à ces terminaux pour une authentification centralisée des utilisateurs via NetApp Cloud Central.
https://widget.intercom.io	Vous bénéficiez d'un chat en ligne pour discuter avec des experts du cloud NetApp.

Règles de pare-feu pour Cloud Volumes ONTAP

Cloud Manager crée des règles de pare-feu GCP qui incluent les règles entrantes et sortantes nécessaires au bon fonctionnement de Cloud Manager et d'Cloud Volumes ONTAP. Vous pouvez vous référer aux ports à des fins de test ou si vous préférez que votre utilise ses propres groupes de sécurité.

Les règles de pare-feu de Cloud Volumes ONTAP requièrent des règles entrantes et sortantes.

Règles entrantes

La source des règles entrantes dans le groupe de sécurité prédéfini est 0.0.0.0/0.

Protocole	Port	Objectif
Tous les protocoles ICMP	Tout	Envoi d'une requête ping à l'instance
HTTP	80	Accès HTTP à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
HTTPS	443	Accès HTTPS à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
SSH	22	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
TCP	111	Appel de procédure à distance pour NFS
TCP	139	Session de service NetBIOS pour CIFS
TCP	161-162	Protocole de gestion de réseau simple
TCP	445	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
TCP	658	Montage NFS
TCP	749	Kerberos
TCP	2049	Démon du serveur NFS
TCP	3260	Accès iSCSI via le LIF de données iSCSI
TCP	4045	Démon de verrouillage NFS
TCP	4046	Surveillance de l'état du réseau pour NFS
TCP	10000	Sauvegarde avec NDMP
TCP	11104	Gestion des sessions de communication intercluster pour SnapMirror
TCP	11105	Transfert de données SnapMirror à l'aide de LIF intercluster
UDP	111	Appel de procédure à distance pour NFS
UDP	161-162	Protocole de gestion de réseau simple
UDP	658	Montage NFS
UDP	2049	Démon du serveur NFS
UDP	4045	Démon de verrouillage NFS
UDP	4046	Surveillance de l'état du réseau pour NFS
UDP	4049	Protocole NFS rquotad

Règles de sortie

Le groupe de sécurité prédéfini pour Cloud Volumes ONTAP ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour Cloud Volumes ONTAP inclut les règles de sortie suivantes.

Protocole	Port	Objectif
Tous les protocoles ICMP	Tout	Tout le trafic sortant
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles UDP	Tout	Tout le trafic sortant

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par Cloud Volumes ONTAP.

La source est l'interface (adresse IP) du système Cloud Volumes ONTAP.

Service	Protocole	Port	Source	Destination	Objectif
Active Directory	TCP	88	FRV de gestion des nœuds	Forêt Active Directory	Authentification Kerberos V.
	UDP	137	FRV de gestion des nœuds	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	FRV de gestion des nœuds	Forêt Active Directory	Service de datagrammes NetBIOS
	TCP	139	FRV de gestion des nœuds	Forêt Active Directory	Session de service NetBIOS
	TCP ET UDP	389	FRV de gestion des nœuds	Forêt Active Directory	LDAP
	TCP	445	FRV de gestion des nœuds	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	UDP	464	FRV de gestion des nœuds	Forêt Active Directory	Administration des clés Kerberos
	TCP	749	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)
	TCP	88	LIF de données (NFS, CIFS, iSCSI)	Forêt Active Directory	Authentification Kerberos V.
	UDP	137	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de datagrammes NetBIOS
	TCP	139	FRV de données (NFS, CIFS)	Forêt Active Directory	Session de service NetBIOS
	TCP ET UDP	389	FRV de données (NFS, CIFS)	Forêt Active Directory	LDAP
	TCP	445	FRV de données (NFS, CIFS)	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	UDP	464	FRV de données (NFS, CIFS)	Forêt Active Directory	Administration des clés Kerberos
	TCP	749	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)

Service	Protocole	Port	Source	Destination	Objectif
Cluster	Tout le trafic	Tout le trafic	Tous les LIF sur un nœud	Tous les LIF de l'autre nœud	Communications InterCluster (Cloud Volumes ONTAP HA uniquement)
	TCP	3000	FRV de gestion des nœuds	Ha médiateur	Appels ZAPI (Cloud Volumes ONTAP HA uniquement)
	ICMP	1	FRV de gestion des nœuds	Ha médiateur	Rester en vie (Cloud Volumes ONTAP HA uniquement)
DHCP	UDP	68	FRV de gestion des nœuds	DHCP	Client DHCP pour la première configuration
DHCPS	UDP	67	FRV de gestion des nœuds	DHCP	Serveur DHCP
DNS	UDP	53	FRV de gestion des nœuds et FRV de données (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600-18699	FRV de gestion des nœuds	Serveurs de destination	Copie NDMP
SMTP	TCP	25	FRV de gestion des nœuds	Serveur de messagerie	Les alertes SMTP peuvent être utilisées pour AutoSupport
SNMP	TCP	161	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	UDP	161	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	TCP	162	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	UDP	162	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
SnapMirror	TCP	11104	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Gestion des sessions de communication intercluster pour SnapMirror
	TCP	11105	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Transfert de données SnapMirror
Syslog	UDP	514	FRV de gestion des nœuds	Serveur Syslog	Messages de transfert syslog

Règles de pare-feu pour le connecteur

Les règles de pare-feu du connecteur exigent à la fois des règles entrantes et sortantes.

Règles entrantes

La source des règles entrantes dans les règles de pare-feu prédéfinies est 0.0.0.0/0.

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale

Règles de sortie

Les règles de pare-feu prédéfinies pour le connecteur ouvrent tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

Les règles de pare-feu prédéfinies pour le connecteur comprennent les règles de trafic sortant suivantes.

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles UDP	Tout	Tout le trafic sortant

Règles de sortie avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par le connecteur.

L'adresse IP source est l'hôte du connecteur.

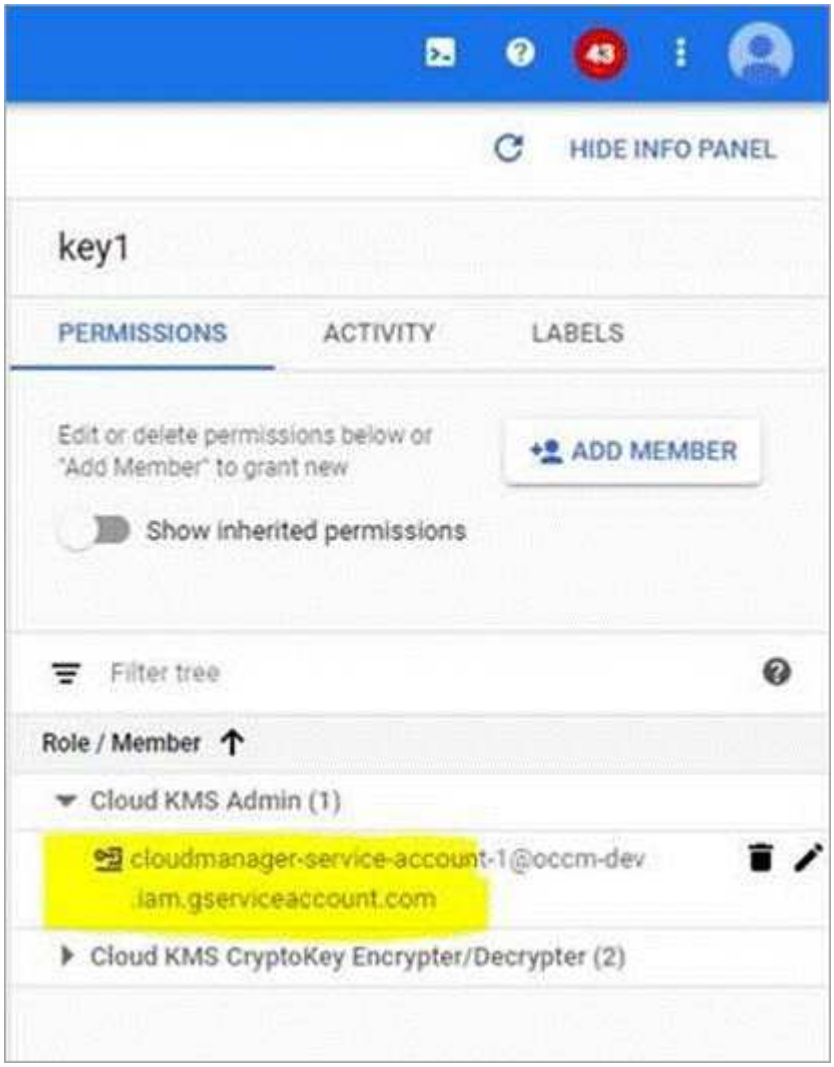
Service	Protocole	Port	Destination	Objectif
Active Directory	TCP	88	Forêt Active Directory	Authentification Kerberos V.
	TCP	139	Forêt Active Directory	Session de service NetBIOS
	TCP	389	Forêt Active Directory	LDAP
	TCP	445	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	TCP	749	Forêt Active Directory	Modification et définition du mot de passe de Kerberos V Active Directory (RPCSEC_GSS)
	UDP	137	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	Forêt Active Directory	Service de datagrammes NetBIOS
	UDP	464	Forêt Active Directory	Administration des clés Kerberos
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	Par des appels d'API à GCP et à ONTAP, et par l'envoi de messages AutoSupport à NetApp
Appels API	TCP	3000	LIF de gestion de cluster ONTAP	Appels API vers ONTAP
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par Cloud Manager

Grâce à des clés de chiffrement gérées par le client avec Cloud Volumes ONTAP

Google Cloud Storage chiffre toujours vos données avant leur écriture sur le disque, mais vous pouvez utiliser les API Cloud Manager pour créer un système Cloud Volumes ONTAP qui utilise des clés de chiffrement *gérées par le client*. Il s'agit des clés que vous créez et gérez dans GCP à l'aide du service Cloud Key Management.

Étapes

1. Donnez au compte de service Connector l'autorisation d'utiliser la clé de cryptage.



2. Obtenir l'ID de la clé en invoquant la commande GET pour l'API /gcp/vsa/Metadata/gcp-Encryption-keys
3. Utilisez le paramètre "GcpEncryption" avec votre requête API lors de la création d'un environnement de travail.

Exemple

```
"gcpEncryptionParameters": {
    "key": "projects/tlv-support/locations/us-
east4/keyRings/Nikiskeys/cryptoKeys/generatedkey1"
  }
```

Reportez-vous à la "Guide du développeur API" Pour plus d'informations sur l'utilisation du paramètre "GcpEncryption".

Lancement d'Cloud Volumes ONTAP dans GCP

Vous pouvez lancer un système Cloud Volumes ONTAP à nœud unique dans GCP en créant un environnement de travail.

Ce dont vous avez besoin

- Vous devez avoir un "Connecteur associé à votre espace de travail".

> Vous devez être un administrateur de compte pour créer un connecteur. Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l'avez pas encore fait.

- "Vous devez être prêt à laisser le connecteur fonctionner en permanence".
- Vous devez avoir choisi une configuration et obtenir des informations de mise en réseau GCP auprès de votre administrateur. Pour plus de détails, voir "Planification de votre configuration Cloud Volumes ONTAP".
- Pour déployer un système BYOL, vous devez disposer du numéro de série à 20 chiffres (clé de licence) pour chaque nœud.
- Il convient de définir les API Google Cloud suivantes "activé dans votre projet":
  - API Cloud Deployment Manager V2
  - API de journalisation cloud
  - API Cloud Resource Manager
  - API du moteur de calcul
  - API de gestion des identités et des accès

Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
2. **Choisissez un emplacement** : sélectionnez **Google Cloud** et **Cloud Volumes ONTAP**.
3. **Détails et informations d'identification** : sélectionnez un projet, spécifiez un nom de cluster, ajoutez éventuellement des étiquettes, puis spécifiez les informations d'identification.

   Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Nom de l'environnement de travail	Cloud Manager utilise le nom de l'environnement de travail pour nommer le système Cloud Volumes ONTAP et l'instance de machine virtuelle GCP. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.

Champ	Description
Ajouter des étiquettes	Les étiquettes sont des métadonnées pour les ressources GCP. Cloud Manager ajoute les étiquettes au système Cloud Volumes ONTAP et aux ressources GCP associées au système. Vous pouvez ajouter jusqu'à quatre étiquettes à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis vous pouvez en ajouter d'autres une fois qu'elles ont été créées. Notez que l'API ne vous limite pas à quatre étiquettes lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section "Documentation Google Cloud : étiquetage des ressources".
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte d'administration du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces identifiants pour vous connecter à Cloud Volumes ONTAP via System Manager ou son interface de ligne de commandes.
Modifier le projet	Sélectionnez le projet dans lequel vous souhaitez que Cloud Volumes ONTAP réside. Le projet par défaut est le projet sur lequel réside Cloud Manager. Si d'autres projets ne s'affichent pas dans la liste déroulante, le compte de service Cloud Manager n'est pas encore associé à d'autres projets. Accédez à la console Google Cloud, ouvrez le service IAM et sélectionnez le projet. Ajoutez le compte de service avec le rôle Cloud Manager à ce projet. Vous devrez répéter cette étape pour chaque projet. Il s'agit du compte de service que vous configurez pour Cloud Manager, "comme décrit à l'étape 2b sur cette page". Cliquez sur **Ajouter un abonnement** pour associer les informations d'identification sélectionnées à un abonnement. Pour créer un système Cloud Volumes ONTAP de paiement basé sur l'utilisation, vous devez sélectionner un projet GCP associé à un abonnement à Cloud Volumes ONTAP depuis GCP Marketplace.

Découvrez dans cette vidéo comment associer un abonnement Marketplace basé sur l'utilisation à votre projet GCP :

► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_gcp.mp4 *(video)*

4. **Localisation et connectivité** : sélectionnez un emplacement, choisissez une stratégie de pare-feu et cochez la case pour confirmer la connectivité réseau au stockage Google Cloud pour le Tiering des données.

   Pour transférer des données inactives vers un compartiment Google Cloud Storage, le sous-réseau dans lequel réside Cloud Volumes ONTAP doit être configuré pour un accès Google privé. Pour obtenir des instructions, reportez-vous à la section "Documentation Google Cloud : configuration de Private Google Access".

5. **Compte du site de licence et de support** : indiquez si vous souhaitez utiliser le paiement à l'utilisation ou BYOL, puis indiquez un compte sur le site de support NetApp.

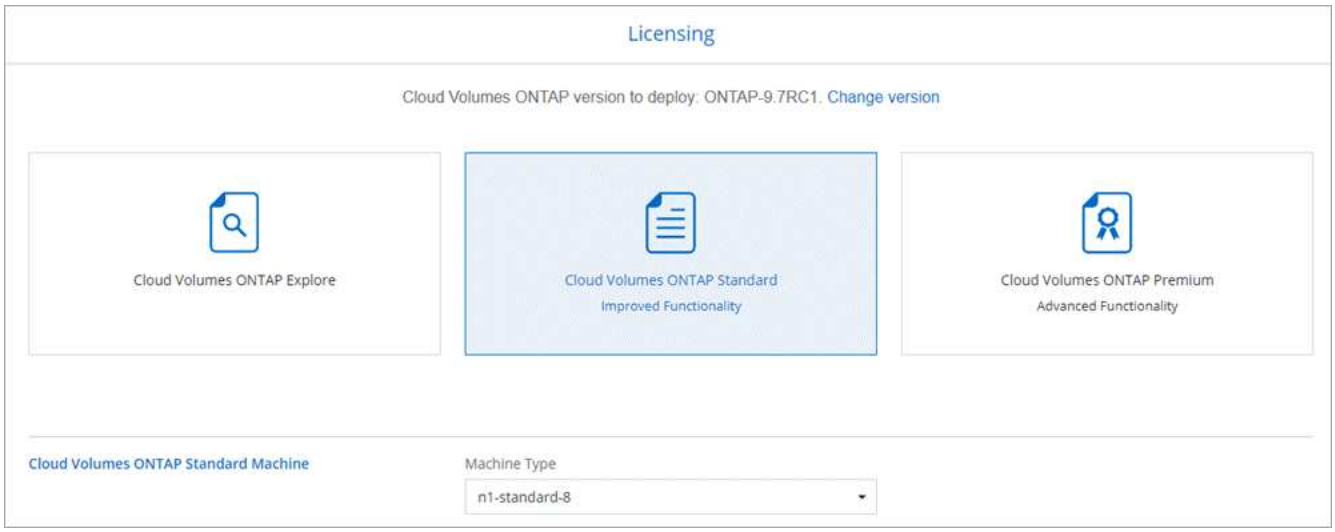
   Pour comprendre le fonctionnement des licences, reportez-vous à la section "Licences".

Un compte sur le site de support NetApp est facultatif afin de bénéficier d'un paiement à l'utilisation, mais requis pour les systèmes BYOL. "Découvrez comment ajouter des comptes au site de support NetApp".

6. **Packages préconfigurés** : sélectionnez un des packages pour déployer rapidement un système Cloud Volumes ONTAP ou cliquez sur **Créer ma propre configuration**.

   Si vous choisissez l'un des packages, vous n'avez qu'à spécifier un volume, puis à revoir et approuver la configuration.

7. **Licence** : modifiez la version de Cloud Volumes ONTAP selon vos besoins, sélectionnez une licence et sélectionnez un type de machine virtuelle.



   Si vos besoins changent après le lancement du système, vous pouvez modifier la licence ou le type de machine virtuelle ultérieurement.

   > Si une version plus récente de Release Candidate, General Availability ou patch est disponible pour la version sélectionnée, Cloud Manager met à jour le système à cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.6 RC1 et 9.6 GA est disponible. La mise à jour ne se produit pas d'une version à l'autre, par exemple de 9.6 à 9.7.

8. **Ressources de stockage sous-jacentes** : Choisissez les paramètres de l'agrégat initial : un type de disque et la taille de chaque disque.

   Le type de disque correspond au volume initial. Vous pouvez choisir un autre type de disque pour les volumes suivants.

   La taille du disque correspond à tous les disques de l'agrégat initial et à tous les agrégats supplémentaires créés par Cloud Manager lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente à l'aide de l'option d'allocation avancée.

   Pour obtenir de l'aide sur le choix du type et de la taille d'un disque, reportez-vous à la section "Dimensionnement du système dans GCP".

9. **Vitesse d'écriture et WORM** : choisissez **Normal** ou **vitesse d'écriture élevée**, et activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

   La sélection d'une vitesse d'écriture est prise en charge avec les systèmes à un seul nœud uniquement.

"En savoir plus sur la vitesse d'écriture".

IMPOSSIBLE D'activer WORM si le Tiering des données était activé.

"En savoir plus sur le stockage WORM".

10. **Tiering de données dans Google Cloud Platform**: Choisissez d'activer ou non le Tiering des données sur l'agrégat initial, de choisir une classe de stockage pour les données hiérarchisées, puis de sélectionner un compte de service disposant du rôle d'administrateur de stockage prédéfini (requis pour Cloud Volumes ONTAP 9.7) ou de sélectionner un compte GCP (requis pour Cloud Volumes ONTAP 9.6).

    Notez ce qui suit :

    - Cloud Manager définit le compte de service sur l'instance Cloud Volumes ONTAP. Ce compte de service fournit des autorisations de Tiering des données vers un compartiment Google Cloud Storage. N'oubliez pas d'ajouter le compte de service Cloud Manager en tant qu'utilisateur du compte de service de Tiering ou bien ne pouvez pas le sélectionner depuis Cloud Manager.
    - Pour obtenir de l'aide sur l'ajout d'un compte GCP, reportez-vous à "Configuration et ajout de comptes GCP pour le Tiering des données avec la version 9.6".
    - Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
    - Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants, mais vous devrez désactiver le système et ajouter un compte de service à partir de la console GCP.

      "En savoir plus sur le Tiering des données".

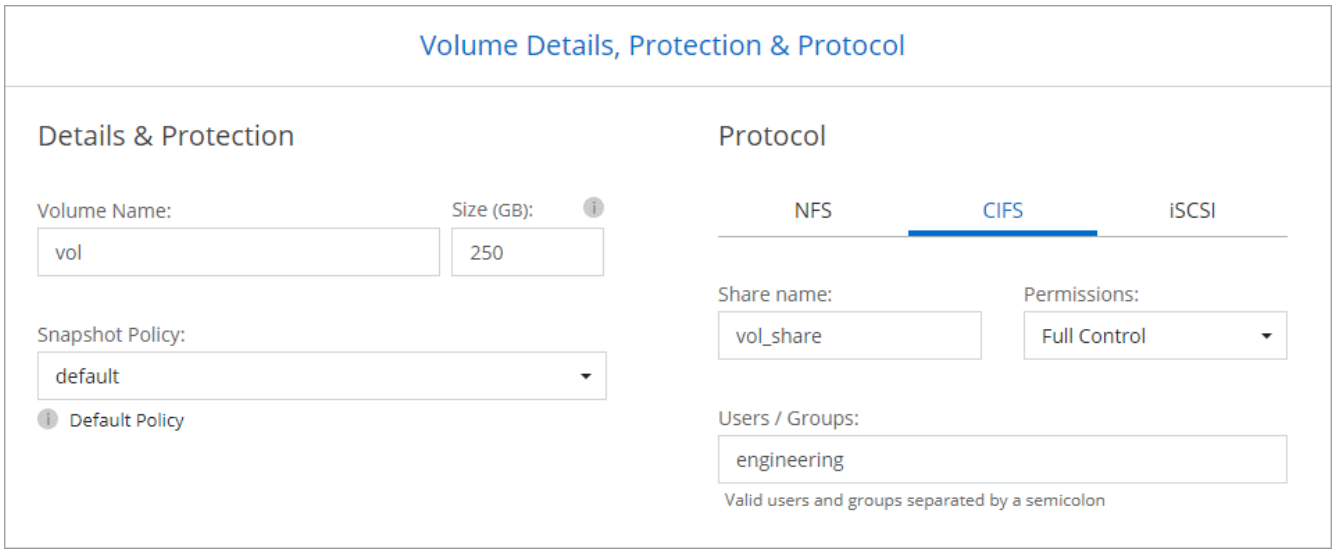
11. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

    Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, Cloud Manager entre une valeur qui donne accès à toutes les instances du sous-réseau.
Autorisations et utilisateurs/groupes (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur à l'aide du format domaine\nom d'utilisateur.
Stratégie Snapshot	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.

Champ	Description
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de buste hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".

L'image suivante montre la page Volume remplie pour le protocole CIFS :



12. **Configuration CIFS** : si vous choisissez le protocole CIFS, configurez un serveur CIFS.

Champ	Description
Adresse IP principale et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS.
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Nom de serveur CIFS unique dans le domaine AD.

Champ	Description
Unité organisationnelle	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers.
Domaine DNS	Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD.
Serveur NTP	Sélectionnez **utiliser le domaine Active Directory** pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la "Guide du développeur de l'API Cloud Manager" pour plus d'informations.

13. **Profil d'utilisation, type de disque et règle de hiérarchisation** : choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifiez la règle de hiérarchisation du volume, si nécessaire.

    Pour plus d'informations, voir "Présentation des profils d'utilisation des volumes" et "Vue d'ensemble du hiérarchisation des données".

14. **Revue et approbation** : consultez et confirmez vos choix.
    a. Consultez les détails de la configuration.
    b. Cliquez sur **plus d'informations** pour en savoir plus sur le support et les ressources GCP que Cloud Manager achètera.
    c. Cochez les cases **Je comprends…**.
    d. Cliquez sur **Go**.

Résultat

Cloud Manager déploie le système Cloud Volumes ONTAP. Vous pouvez suivre la progression dans la chronologie.

Si vous rencontrez des problèmes lors du déploiement du système Cloud Volumes ONTAP, consultez le message d'échec. Vous pouvez également sélectionner l'environnement de travail et cliquer sur **recréer l'environnement**.

Pour obtenir de l'aide supplémentaire, consultez la page "Prise en charge de NetApp Cloud Volumes ONTAP".

Une fois que vous avez terminé

- Si vous avez provisionné un partage CIFS, donnez aux utilisateurs ou aux groupes des autorisations sur les fichiers et les dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier.
- Si vous souhaitez appliquer des quotas aux volumes, utilisez System Manager ou l'interface de ligne de commande.

  Les quotas vous permettent de restreindre ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree.

Provisionner et gérer le stockage

Provisionnement du stockage

Vous pouvez provisionner du stockage supplémentaire pour vos systèmes Cloud Volumes ONTAP depuis Cloud Manager en gérant les volumes et les agrégats.

Tous les disques et agrégats doivent être créés et supprimés directement de Cloud Manager. Vous ne devez pas effectuer ces actions à partir d'un autre outil de gestion. Cela peut avoir un impact sur la stabilité du système, entraver la possibilité d'ajouter des disques à l'avenir et générer potentiellement des frais de fournisseur de cloud redondant.

Création de volumes FlexVol

Si vous avez besoin de plus de stockage après le lancement d'un système Cloud Volumes ONTAP, vous pouvez créer de nouveaux volumes FlexVol pour NFS, CIFS ou iSCSI à partir de Cloud Manager.

Description de la tâche

Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes.

Vous pouvez créer des LUN supplémentaires depuis System Manager ou l'interface de ligne de commandes.

Avant de commencer

Si vous souhaitez utiliser CIFS dans AWS, vous devez avoir configuré DNS et Active Directory. Pour plus de détails, voir "Configuration réseau requise pour Cloud Volumes ONTAP pour AWS".

Étapes

1. Sur la page Working Environments, double-cliquez sur le nom du système Cloud Volumes ONTAP sur lequel vous souhaitez provisionner les volumes FlexVol.
2. Créez un nouveau volume sur un agrégat ou sur un agrégat spécifique :

Action	Étapes
Créez un nouveau volume et laissez Cloud Manager choisir l'agrégat contenant	Cliquez sur **Ajouter nouveau volume**.
Créez un nouveau volume sur un agrégat spécifique	a. Cliquez sur l'icône du menu, puis sur **Avancé > attribution avancée**. b. Cliquez sur le menu correspondant à un agrégat. c. Cliquez sur **Créer un volume**.

3. Entrez les détails du nouveau volume, puis cliquez sur **Continuer**.

   Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, Cloud Manager entre une valeur qui donne accès à toutes les instances du sous-réseau.

Champ	Description
Autorisations et utilisateurs/groupes (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur à l'aide du format domaine\nom d'utilisateur.
Stratégie Snapshot	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de buste hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".

4. Si vous avez choisi le protocole CIFS et que le serveur CIFS n'a pas été configuré, spécifiez les détails du serveur dans la boîte de dialogue Créer un serveur CIFS, puis cliquez sur **Enregistrer et continuer** :

Champ	Description
Adresse IP principale et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS.
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Nom de serveur CIFS unique dans le domaine AD.

Champ	Description
Unité organisationnelle	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. • Pour configurer Microsoft AD géré par AWS en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer **ou=ordinateurs,ou=corp** dans ce champ. • Pour configurer les services de domaine Azure AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer **ou=ordinateurs ADDC** ou **ou=utilisateurs ADDC** dans ce champ.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentation Azure : créez une unité organisationnelle dans un domaine géré Azure AD Domain Services"^]
Domaine DNS	Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD.
Serveur NTP	Sélectionnez **utiliser le domaine Active Directory** pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la "Guide du développeur de l'API Cloud Manager" pour plus d'informations.

5. Sur la page profil d'utilisation, type de disque et règle de Tiering, choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage, choisissez un type de disque et modifiez la règle de Tiering, si nécessaire.

   Pour obtenir de l'aide, reportez-vous aux documents suivants :

   - "Présentation des profils d'utilisation des volumes"
   - "Dimensionnement de votre système dans AWS"
   - "Dimensionnement du système dans Azure"
   - "Vue d'ensemble du hiérarchisation des données"

6. Cliquez sur **Go**.

Résultat

Cloud Volumes ONTAP en assure la gestion.

Une fois que vous avez terminé

Si vous avez provisionné un partage CIFS, donnez aux utilisateurs ou aux groupes des autorisations sur les fichiers et les dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier.

Si vous souhaitez appliquer des quotas aux volumes, vous devez utiliser System Manager ou l'interface de ligne de commande. Les quotas vous permettent de restreindre ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree.

Création de volumes FlexVol sur le second nœud dans une configuration haute disponibilité

Par défaut, Cloud Manager crée des volumes sur le premier nœud d'une configuration HA. Si vous avez besoin d'une configuration active-active, dans laquelle les deux nœuds servent les données aux clients, vous devez créer des agrégats et des volumes sur le second nœud.

Étapes

1. Sur la page Working Environments, double-cliquez sur le nom de l'environnement de travail Cloud Volumes ONTAP sur lequel vous souhaitez gérer les agrégats.
2. Cliquez sur l'icône du menu, puis sur **Avancé > attribution avancée**.
3. Cliquez sur **Ajouter agrégat**, puis créez l'agrégat.
4. Pour le nœud principal, choisissez le second nœud dans la paire HA.
5. Une fois que Cloud Manager a créé l'agrégat, sélectionnez-le, puis cliquez sur **Create volume**.
6. Entrez les détails du nouveau volume, puis cliquez sur **Créer**.

Une fois que vous avez terminé

Vous pouvez créer des volumes supplémentaires sur cet agrégat si nécessaire.

Pour les paires HA déployées dans plusieurs zones de disponibilité AWS, vous devez monter le volume sur les clients en utilisant l'adresse IP flottante du nœud sur lequel réside le volume.

Création d'agrégats

Vous pouvez créer des agrégats vous-même ou laisser Cloud Manager le faire lorsque vous créez des volumes. L'avantage de créer des agrégats vous-même est de choisir la taille du disque sous-jacent, ce qui vous permet de dimensionner l'agrégat en fonction de la capacité ou des performances requises.

Étapes

1. Sur la page Working Environments, double-cliquez sur le nom de l'instance Cloud Volumes ONTAP sur laquelle vous souhaitez gérer les agrégats.
2. Cliquez sur l'icône du menu, puis sur **Avancé > attribution avancée**.
3. Cliquez sur **Ajouter agrégat**, puis spécifiez les détails de l'agrégat.

   Pour obtenir de l'aide sur le type et la taille du disque, reportez-vous à la section "Planification de votre configuration".

4. Cliquez sur **Go**, puis sur **approuver et acheter**.

Connexion d'une LUN à un hôte

Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes.

Notez ce qui suit :

1. La gestion automatique de la capacité de Cloud Manager ne s'applique pas aux LUN. Lorsque Cloud Manager crée un LUN, il désactive la fonctionnalité de croissance automatique.
2. Vous pouvez créer des LUN supplémentaires depuis System Manager ou l'interface de ligne de commandes.

Étapes

1. Sur la page Working Environments, double-cliquez sur l'environnement de travail Cloud Volumes ONTAP sur lequel vous souhaitez gérer les volumes.
2. Sélectionnez un volume, puis cliquez sur **IQN cible**.
3. Cliquez sur **Copy** pour copier le nom IQN.
4. Configurez une connexion iSCSI de l'hôte vers le LUN.
    - "Configuration iSCSI express ONTAP 9 pour Red Hat Enterprise Linux : démarrage des sessions iSCSI avec la cible"
    - "Configuration iSCSI express de ONTAP 9 pour Windows : démarrage des sessions iSCSI avec la cible"

Utilisation de volumes FlexCache pour accélérer l'accès aux données

Un volume FlexCache est un volume de stockage qui met en cache les données lues par NFS à partir d'un volume d'origine (ou source). Les lectures suivantes des données mises en cache permettent un accès plus rapide à ces données.

Les volumes FlexCache peuvent être utilisés pour accélérer l'accès aux données ou pour décharger le trafic des volumes fortement sollicités. Les volumes FlexCache contribuent à améliorer les performances, en particulier lorsque les clients doivent accéder de façon répétée aux mêmes données, car elles peuvent être servies directement sans avoir à accéder au volume d'origine. Les volumes FlexCache fonctionnent parfaitement pour les charges de travail système intensives en lecture.

Cloud Manager n'assure pas la gestion des volumes FlexCache pour le moment, mais vous pouvez utiliser l'interface de ligne de commande ONTAP ou ONTAP System Manager pour créer et gérer des volumes FlexCache :

- "Guide de puissance des volumes FlexCache pour un accès plus rapide aux données"
- "Création de volumes FlexCache dans System Manager"

À partir de la version 3.7.2, Cloud Manager génère une licence FlexCache pour tous les nouveaux systèmes Cloud Volumes ONTAP. La licence inclut une limite d'utilisation de 500 Go.

Pour générer la licence, Cloud Manager doit accéder au https://ipa-signer.cloudmanager.netapp.com. Assurez-vous que cette URL est accessible à partir de votre pare-feu.

Gestion du stockage existant

Cloud Manager vous permet de gérer les volumes, les agrégats et les serveurs CIFS. Il vous invite également à déplacer des volumes afin d'éviter les problèmes de capacité.

Gestion des volumes existants

Vous pouvez gérer les volumes existants à mesure que vos besoins de stockage changent. Vous pouvez afficher, modifier, cloner, restaurer et supprimer des volumes.

Étapes

1. Sur la page Working Environments, double-cliquez sur l'environnement de travail Cloud Volumes ONTAP sur lequel vous souhaitez gérer les volumes.
2. Gérez vos volumes :

Tâche	Action
Afficher des informations sur un volume	Sélectionnez un volume, puis cliquez sur **Info**.
Modifier un volume (volumes en lecture-écriture uniquement)	a. Sélectionnez un volume, puis cliquez sur **Modifier**. b. Modifiez la stratégie Snapshot du volume, la version du protocole NFS, la liste de contrôle d'accès NFS ou les autorisations de partage, puis cliquez sur **Update**. Si vous avez besoin de règles Snapshot personnalisées, vous pouvez les créer à l'aide de System Manager.

Tâche	Action
Clonez un volume	a. Sélectionnez un volume, puis cliquez sur **Clone**. b. Modifiez le nom du clone selon vos besoins, puis cliquez sur **Clone**. Ce processus crée un volume FlexClone. Un volume FlexClone est une copie inscriptible, ponctuelle et efficace dans l'espace, car il utilise une petite quantité d'espace pour les métadonnées, puis ne consomme que de l'espace supplémentaire lorsque les données sont modifiées ou ajoutées. Pour en savoir plus sur les volumes FlexClone, consultez le "Guide de gestion du stockage logique ONTAP 9".
Restaurer les données d'une copie Snapshot vers un nouveau volume	a. Sélectionnez un volume, puis cliquez sur **Restaurer à partir de la copie Snapshot**. b. Sélectionnez une copie Snapshot, indiquez le nom du nouveau volume, puis cliquez sur **Restore**.
Créez une copie Snapshot à la demande	a. Sélectionnez un volume, puis cliquez sur **Créer une copie snapshot**. b. Modifiez le nom, si nécessaire, puis cliquez sur **Créer**.
Obtenez la commande NFS mount	a. Sélectionnez un volume, puis cliquez sur **Mount Command**. b. Cliquez sur **Copier**.
Afficher l'IQN cible d'un volume iSCSI	a. Sélectionnez un volume, puis cliquez sur **IQN cible**. b. Cliquez sur **Copier**. c. "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".
Modifiez le type de disque sous-jacent	a. Sélectionnez un volume, puis cliquez sur **Modifier le type de disque et la stratégie de hiérarchisation**. b. Sélectionnez le type de disque, puis cliquez sur **changer**. Cloud Manager déplace le volume vers un agrégat existant qui utilise le type de disque sélectionné ou crée un nouvel agrégat pour le volume.
Modifiez la stratégie de hiérarchisation	a. Sélectionnez un volume, puis cliquez sur **Modifier le type de disque et la stratégie de hiérarchisation**. b. Cliquez sur **Modifier la stratégie**. c. Sélectionnez une autre stratégie et cliquez sur **Modifier**. Cloud Manager déplace le volume vers un agrégat existant qui utilise le type de disque sélectionné avec hiérarchisation ou crée un nouvel agrégat pour le volume.

Tâche	Action
Supprimer un volume	a. Sélectionnez un volume, puis cliquez sur **Supprimer**. b. Cliquez à nouveau sur **Supprimer** pour confirmer.

Gestion des agrégats existants

Gérez vous-même les agrégats en ajoutant des disques, en affichant les informations sur les agrégats et en les supprimant.

Avant de commencer

Si vous souhaitez supprimer un agrégat, vous devez d'abord supprimer les volumes de l'agrégat.

Description de la tâche

Si un agrégat manque d'espace, vous pouvez déplacer des volumes vers un autre agrégat à l'aide d'OnCommand System Manager.

Étapes

1. Sur la page Working Environments, double-cliquez sur l'environnement de travail Cloud Volumes ONTAP sur lequel vous souhaitez gérer les agrégats.
2. Cliquez sur l'icône du menu, puis sur **Avancé > attribution avancée**.
3. Gérez vos agrégats :

Tâche	Action
Afficher des informations sur un agrégat	Sélectionnez un agrégat et cliquez sur **Info**.
Créez un volume sur un agrégat spécifique	Sélectionnez un agrégat et cliquez sur **Create volume**.
Ajoutez des disques à un agrégat	a. Sélectionnez un agrégat et cliquez sur **Ajouter des disques AWS** ou **Ajouter des disques Azure**. b. Sélectionnez le nombre de disques que vous souhaitez ajouter et cliquez sur **Ajouter**.  Tous les disques qui composent un agrégat doivent être de la même taille.
Supprimer un agrégat	a. Sélectionnez un agrégat qui ne contient aucun volume et cliquez sur **Supprimer**. b. Cliquez à nouveau sur **Supprimer** pour confirmer.

Modification du serveur CIFS

Si vous modifiez vos serveurs DNS ou votre domaine Active Directory, vous devez modifier le serveur CIFS dans Cloud Volumes ONTAP pour pouvoir continuer à servir le stockage aux clients.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > Configuration CIFS**.
2. Spécifiez les paramètres du serveur CIFS :

Tâche	Action
Adresse IP principale et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS.
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Nom de serveur CIFS unique dans le domaine AD.
Unité organisationnelle	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Si vous configurez AWS Managed Microsoft AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer **ou=ordinateurs,ou=corp** dans ce champ.
Domaine DNS	Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD.
Serveur NTP	Sélectionnez **utiliser le domaine Active Directory** pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la "Guide du développeur de l'API Cloud Manager" pour plus d'informations.

3. Cliquez sur **Enregistrer**.

Résultat

Cloud Volumes ONTAP met à jour le serveur CIFS avec les modifications.

Déplacement d'un volume

Déplacer les volumes pour optimiser l'utilisation de la capacité et les performances, et satisfaire les contrats de niveau de service.

Vous pouvez déplacer un volume dans System Manager en sélectionnant un volume et l'agrégat de destination, en commençant l'opération de déplacement de volume et, éventuellement, en surveillant la tâche de déplacement de volume. Avec System Manager, une opération de déplacement de volume se termine automatiquement.

Étapes

1. Utilisez System Manager ou l'interface de ligne de commande pour déplacer les volumes vers l'agrégat.

   Dans la plupart des cas, vous pouvez utiliser System Manager pour déplacer des volumes.

Pour obtenir des instructions, reportez-vous au "Guide de migration de volumes ONTAP 9 Express".

Déplacement d'un volume lorsque Cloud Manager affiche un message action requise

Cloud Manager peut afficher un message Action requise indiquant que le déplacement d'un volume est nécessaire pour éviter les problèmes de capacité, mais qu'il ne peut pas fournir de recommandations pour corriger le problème. Dans ce cas, vous devez identifier comment corriger le problème, puis déplacer un ou plusieurs volumes.

Étapes

1. Identifier la manière de corriger le problème.
2. En fonction de votre analyse, déplacez les volumes pour éviter les problèmes de capacité :
   - Déplacement des volumes vers un autre système.
   - Déplacement des volumes vers un autre agrégat du même système.

Identifier comment corriger les problèmes de capacité

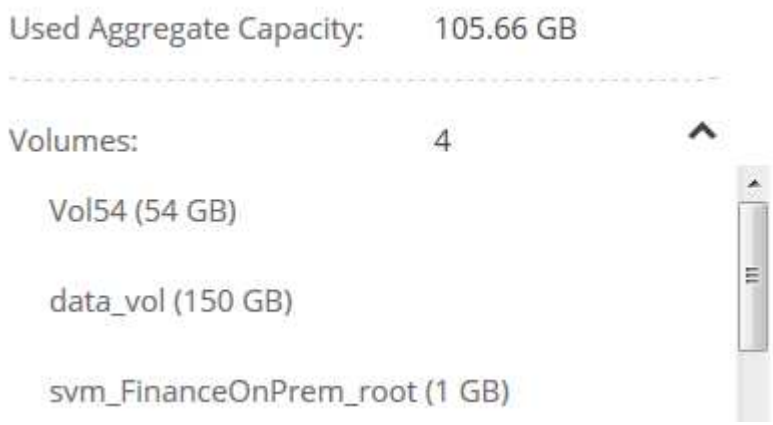
Si Cloud Manager ne peut pas fournir de recommandations pour le déplacement d'un volume afin d'éviter les problèmes de capacité, vous devez identifier les volumes que vous devez déplacer et indiquer si vous devez les déplacer vers un autre agrégat sur le même système ou vers un autre système.

Étapes

1. Consultez les informations avancées du message Action requise pour identifier l'agrégat ayant atteint sa limite de capacité.

   Par exemple, l'information avancée devrait dire quelque chose de similaire à ce qui suit : aggr1 global a atteint sa limite de capacité.

2. Identifiez un ou plusieurs volumes à sortir de l'agrégat :
   a. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > allocation avancée**.
   b. Sélectionnez l'agrégat, puis cliquez sur **Info**.
   c. Développez la liste des volumes.



   d. Passez en revue la taille de chaque volume et choisissez un ou plusieurs volumes pour sortir de l'agrégat.

      Vous devez choisir des volumes suffisamment volumineux pour libérer de l'espace dans l'agrégat afin

d'éviter d'autres problèmes de capacité à l'avenir.

3. Si le système n'a pas atteint la limite de disque, vous devez déplacer les volumes vers un agrégat existant ou vers un nouvel agrégat sur le même système.

   Pour plus de détails, voir "Déplacement des volumes vers un autre agrégat pour éviter les problèmes de capacité".

4. Si le système a atteint la limite de disque, effectuez l'une des opérations suivantes :
   a. Supprimez tous les volumes inutilisés.
   b. Réorganiser les volumes pour libérer de l'espace sur un agrégat.

      Pour plus de détails, voir "Déplacement des volumes vers un autre agrégat pour éviter les problèmes de capacité".

   c. Déplacez deux volumes ou plus vers un autre système disposant d'espace.

      Pour plus de détails, voir "Déplacement des volumes vers un autre système pour éviter les problèmes de capacité".

Déplacement des volumes vers un autre système pour éviter les problèmes de capacité

Vous pouvez déplacer un ou plusieurs volumes vers un autre système Cloud Volumes ONTAP pour éviter les problèmes de capacité. Vous devrez peut-être le faire si le système a atteint sa limite de disque.

Description de la tâche

Vous pouvez suivre les étapes de cette tâche pour corriger le message Action requise suivant :

```
 Moving a volume is necessary to avoid capacity issues; however, Cloud
Manager cannot perform this action for you because the system has reached
the disk limit.
.Étapes
. Identifiez un système Cloud Volumes ONTAP doté de la capacité disponible
ou déployez un nouveau système.
. Faites glisser et déposez l'environnement de travail source sur
l'environnement de travail cible pour effectuer une réplication unique du
volume.
```

+
Pour plus de détails, voir "Réplication des données entre les systèmes".

1. Accédez à la page Etat de la réplication, puis rompez la relation SnapMirror pour convertir le volume répliqué d'un volume de protection des données en volume en lecture/écriture.

   Pour plus de détails, voir "Gestion des planifications et des relations de réplication des données".

2. Configurez le volume pour l'accès aux données.

   Pour plus d'informations sur la configuration d'un volume de destination pour l'accès aux données, reportez-vous à la section "Guide rapide de reprise après incident de volumes ONTAP 9".

3. Supprimez le volume d'origine.

   Pour plus de détails, voir "Gestion des volumes existants".

Déplacement des volumes vers un autre agrégat pour éviter les problèmes de capacité

Vous pouvez déplacer un ou plusieurs volumes vers un autre agrégat pour éviter les problèmes de capacité.

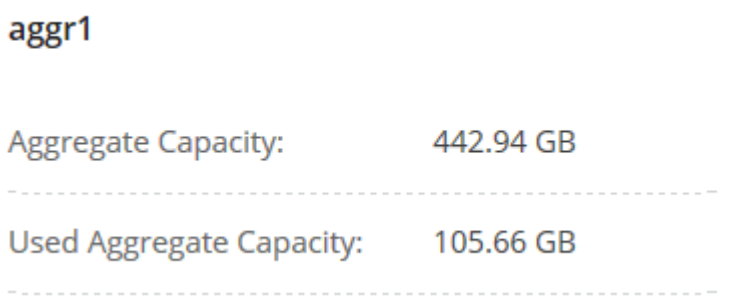
Description de la tâche

Vous pouvez suivre les étapes de cette tâche pour corriger le message Action requise suivant :

```
 Moving two or more volumes is necessary to avoid capacity issues;
however, Cloud Manager cannot perform this action for you.
.Étapes
. Vérifiez si un agrégat existant a la capacité disponible pour les
volumes que vous devez déplacer :
```

+
.. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > allocation avancée**.
.. Sélectionnez chaque agrégat, cliquez sur **Info**, puis affichez la capacité disponible (capacité d'agrégat moins la capacité d'agrégat utilisée).

+



1. Si nécessaire, ajoutez des disques à un agrégat existant :
   a. Sélectionner l'agrégat, puis cliquer sur **Add disks**.
   b. Sélectionnez le nombre de disques à ajouter, puis cliquez sur **Ajouter**.
2. Si aucun agrégat n'a de capacité disponible, créez un nouvel agrégat.

   Pour plus de détails, voir "Création d'agrégats".

3. Utilisez System Manager ou l'interface de ligne de commande pour déplacer les volumes vers l'agrégat.
4. Dans la plupart des cas, vous pouvez utiliser System Manager pour déplacer des volumes.

   Pour obtenir des instructions, reportez-vous au "Guide de migration de volumes ONTAP 9 Express".

Raisons de la lenteur d'un déplacement de volume

Le déplacement d'un volume peut prendre plus de temps que ce que vous attendez si l'une des conditions suivantes est vraie pour Cloud Volumes ONTAP :

- Le volume est un clone.
- Le volume est parent d'un clone.
- L'agrégat source ou de destination dispose d'un seul disque dur (st1) à débit optimisé.
- Le système Cloud Volumes ONTAP est dans AWS et un agrégat utilise une ancienne approche de nommage des objets. Les deux agrégats doivent utiliser le même format de nom.

  Une ancienne méthode de nommage est utilisée si le Tiering des données était activé sur un agrégat dans la version 9.4 ou antérieure.

- Les paramètres de chiffrement ne correspondent pas aux agrégats source et de destination, ou une nouvelle clé est en cours.
- L'option *-Tiering-policy* a été spécifiée sur le déplacement de volumes pour modifier la règle de Tiering.
- L'option *-generate-destination-key* a été spécifiée lors du déplacement du volume.

Tiering des données inactives vers un stockage objet à faible coût

Vous pouvez réduire les coûts de stockage pour Cloud Volumes ONTAP en combinant un Tier de performance SSD ou HDD pour les données actives avec un Tier de capacité de stockage objet pour les données inactives. Pour une vue d'ensemble de haut niveau, voir "Vue d'ensemble du hiérarchisation des données".

Pour configurer le tiering des données, il vous suffit d'effectuer les opérations suivantes :

Choisissez une configuration prise en charge

La plupart des configurations sont prises en charge. Si votre système Cloud Volumes ONTAP Standard, Premium ou BYOL exécute la version la plus récente, il est préférable de passer à la version précédente. "En savoir plus >>".

Assurez la connectivité entre le Cloud Volumes ONTAP et le stockage objet

- Pour AWS, vous avez besoin d'un terminal VPC vers S3. En savoir plus >>.
- Pour Azure, vous n'aurez rien à faire tant que Cloud Manager dispose des autorisations requises. En savoir plus >>.
- Pour GCP, vous devez configurer le sous-réseau pour Private Google Access et configurer un compte de service. En savoir plus >>.

Choisissez une règle de Tiering lors de la création, de la modification ou de la réplication d'un volume

Cloud Manager vous invite à choisir une règle de Tiering lors de la création, de la modification ou de la réplication d'un volume.

- "Hiérarchisation des données sur les volumes en lecture-écriture"
- "Hiérarchisation des données sur les volumes de protection des données"

Quelles sont les’s non requis pour le Tiering des données

- Vous n’avez pas besoin d’installer une licence pour activer le Tiering des données.
- Inutile de créer un Tier de capacité (un compartiment S3, un conteneur Azure Blob ou un compartiment GCP). Cloud Manager le fait pour vous.

Configurations prenant en charge le tiering des données

Vous pouvez activer le tiering des données lors de l’utilisation de configurations et de fonctionnalités spécifiques :

- Le Tiering des données est pris en charge avec Cloud Volumes ONTAP Standard, Premium ou BYOL, à partir des versions suivantes :
  - Version 9.2 dans AWS
  - Version 9.4 dans Azure avec des systèmes à un seul nœud
  - Version 9.6 dans Azure avec paires HA
  - Version 9.6 dans GCP

  Le tiering des données n’est pas pris en charge dans Azure avec le type de machine virtuelle DS3_v2.

- Dans AWS, le niveau de performance peut être des disques SSD à usage général, des disques SSD IOPS provisionnés ou des disques durs optimisés pour le débit.
- Dans Azure, le Tier de performance peut être soit des disques gérés par SSD premium, soit des disques gérés par SSD standard, soit des disques gérés par des disques durs standard.
- Dans GCP, le Tier de performance peut être équipé de disques SSD ou HDD (disques standard).
- Le Tiering des données est pris en charge grâce aux technologies de chiffrement.
- Le provisionnement fin doit être activé sur les volumes.

Conditions requises pour le Tiering des données inactives vers AWS S3

Assurez-vous que Cloud Volumes ONTAP dispose d’une connexion à S3. La meilleure façon de fournir cette connexion est de créer un terminal VPC vers le service S3. Pour obtenir des instructions, reportez-vous à la section "Documentation AWS : création d’un terminal de passerelle".

Lorsque vous créez le terminal VPC, veillez à sélectionner la région, le VPC et la table de routage correspondant à l’instance Cloud Volumes ONTAP. Vous devez également modifier le groupe de sécurité pour ajouter une règle HTTPS sortante qui active le trafic vers le terminal S3. Dans le cas contraire, Cloud Volumes ONTAP ne peut pas se connecter au service S3.

Si vous rencontrez des problèmes, reportez-vous à la section "Centre de connaissances du support AWS : pourquoi ne puis-je pas me connecter à un compartiment S3 à l’aide d’un terminal VPC de passerelle ?".

Il est nécessaire de déplacer les données inactives vers le stockage Azure Blob

Vous n’avez pas besoin de configurer de connexion entre le Tier de performance et le Tier de capacité tant que Cloud Manager dispose des autorisations requises. Cloud Manager active un terminal de service VNet pour vous si la règle Cloud Manager dispose des autorisations suivantes :

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

Les autorisations sont incluses dans le dernier "Politique de Cloud Manager".

Il est donc nécessaire de transférer les données inactives vers un compartiment Google Cloud Storage

- Le sous-réseau dans lequel réside Cloud Volumes ONTAP doit être configuré pour un accès privé à Google. Pour obtenir des instructions, reportez-vous à la section "Documentation Google Cloud : configuration de Private Google Access".
- Vous devez disposer d'un compte de service avec le rôle d'administrateur de stockage prédéfini. Vous devez sélectionner ce compte de service lors de la création d'un environnement de travail Cloud Volumes ONTAP.

  "Configurez ce compte de service de Tiering comme suit":

  a. Attribuez le rôle *Storage Admin* prédéfini au compte de service de hiérarchisation.
  b. Ajoutez le compte de service Connector en tant que *Service Account User* au compte de service Tiering.

     Vous pouvez indiquer le rôle d'utilisateur "à l'étape 3 de l'assistant lorsque vous créez le compte de service de tiering", ou "attribuez le rôle après la création du compte de service".

     Lorsque vous créez un environnement de travail Cloud Volumes ONTAP, vous devrez sélectionner le compte de service de Tiering.

  Si vous n'activez pas le Tiering des données et sélectionnez un compte de service lorsque vous créez le système Cloud Volumes ONTAP, vous devrez désactiver le système et ajouter le compte de service à Cloud Volumes ONTAP à partir de la console GCP.

Tiering des données à partir de volumes en lecture/écriture

Cloud Volumes ONTAP peut déplacer les données inactives sur des volumes en lecture/écriture vers un stockage objet économique, libérant ainsi le Tier de performance pour les données actives.

Étapes

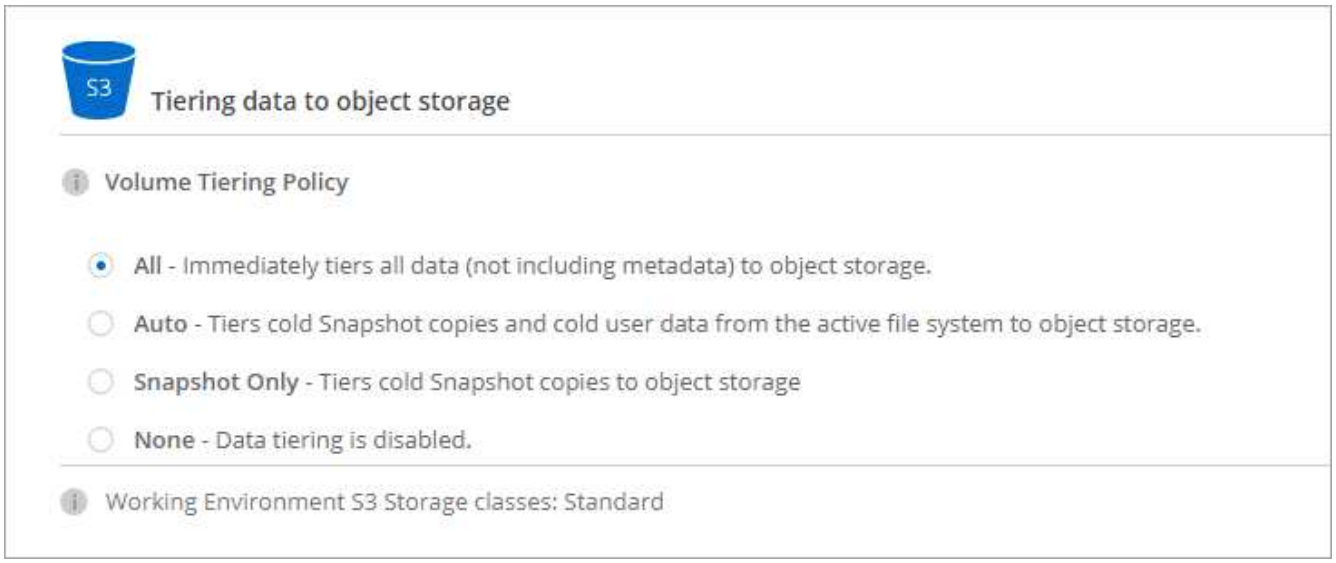
1. Dans l'environnement de travail, créez un nouveau volume ou modifiez le niveau d'un volume existant :

Tâche	Action
Créez un nouveau volume	Cliquez sur **Ajouter nouveau volume**.
Modifier un volume existant	Sélectionnez le volume et cliquez sur **Modifier le type de disque et la stratégie de hiérarchisation**.

2. Sélectionnez une règle de hiérarchisation.

   Pour obtenir une description de ces politiques, reportez-vous à la section "Vue d'ensemble du hiérarchisation des données".

   Exemple



Cloud Manager crée un nouvel agrégat pour le volume si un agrégat compatible avec le hiérarchisation des données n'existe pas déjà.

Si vous préférez créer vous-même des agrégats, vous pouvez activer le tiering des données sur les agrégats lorsque vous les créez.

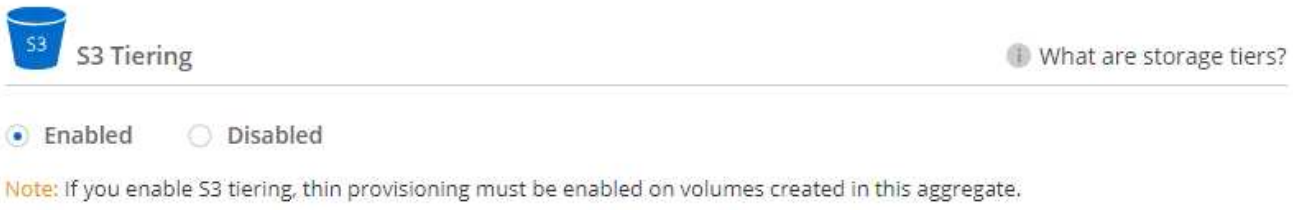
Tiering des données à partir des volumes de protection des données

Cloud Volumes ONTAP permet de hiérarchiser les données d'un volume de protection des données vers un niveau de capacité. Si vous activez le volume de destination, les données passent progressivement au niveau de performance tel qu'il est lu.

Étapes

1. Sur la page Working Environments (Environnements de travail), sélectionnez l'environnement de travail qui contient le volume source, puis faites-le glisser vers l'environnement de travail vers lequel vous souhaitez répliquer le volume.
2. Suivez les invites jusqu'à ce que vous atteigniez la page de hiérarchisation et que vous activiez le tiering des données vers le stockage d'objets.

Exemple



Pour obtenir de l'aide sur la réplication des données, voir "Réplication des données depuis et vers le cloud".

Modification de la classe de stockage pour les données hiérarchisées

Une fois déployé Cloud Volumes ONTAP, vous pouvez réduire les coûts de stockage en modifiant la classe de

stockage pour les données inactives inutilisées depuis 30 jours. Les coûts d'accès sont plus élevés si vous accédez aux données. Vous devez donc prendre en compte ces coûts avant de changer de classe de stockage.

it stockage des données hiérarchisées est disponible dans l'ensemble du système, et non dans chaque volume.

Pour plus d'informations sur les classes de stockage prises en charge, reportez-vous à la section "Vue d'ensemble du hiérarchisation des données".

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **classes de stockage** ou **stockage Blob Storage Tiering**.
2. Choisissez une classe de stockage, puis cliquez sur **Enregistrer**.

Puis-je activer le Tiering des données sur un agrégat existant ?

Non, vous ne pouvez pas activer le Tiering des données sur un agrégat existant. Vous pouvez uniquement activer le Tiering sur les nouveaux agrégats.

Vous pouvez activer le Tiering des données sur un nouvel agrégat "en créant un agrégat vous-même" ou en créant un nouveau volume sur lequel le tiering des données est activé. Cloud Manager crée ensuite un nouvel agrégat pour le volume si un agrégat compatible avec le Tiering des données n'existe pas déjà.

Gestion des machines virtuelles de stockage

Une VM de stockage est une machine virtuelle exécutée dans ONTAP, qui fournit des services de données et de stockage à vos clients. Vous pouvez le connaître comme *SVM* ou *vserver*. La solution Cloud Volumes ONTAP est configurée par défaut avec une seule machine virtuelle de stockage, mais certaines configurations prennent en charge des machines virtuelles de stockage supplémentaires.

Nombre de machines virtuelles de stockage pris en charge

Cloud Volumes ONTAP 9.7 prend en charge plusieurs machines virtuelles de stockage dans AWS avec certaines configurations et une licence d'extension. "Afficher le nombre de machines virtuelles de stockage prises en charge dans AWS". Contactez l'équipe en charge de votre compte pour obtenir une licence d'extension SVM.

Toutes les autres configurations Cloud Volumes ONTAP prennent en charge une VM de stockage servant aux données et une VM de stockage de destination utilisée pour la reprise après incident. Vous pouvez activer la machine virtuelle de stockage de destination pour l'accès aux données en cas de panne sur la machine virtuelle de stockage source.

Une machine virtuelle de stockage s'étend sur l'ensemble du système Cloud Volumes ONTAP (paire haute disponibilité ou nœud unique).

Création de machines virtuelles de stockage supplémentaires

Si votre configuration prend en charge, vous pouvez créer des VM de stockage supplémentaires à l'aide de "System Manager ou l'interface de ligne de commandes".

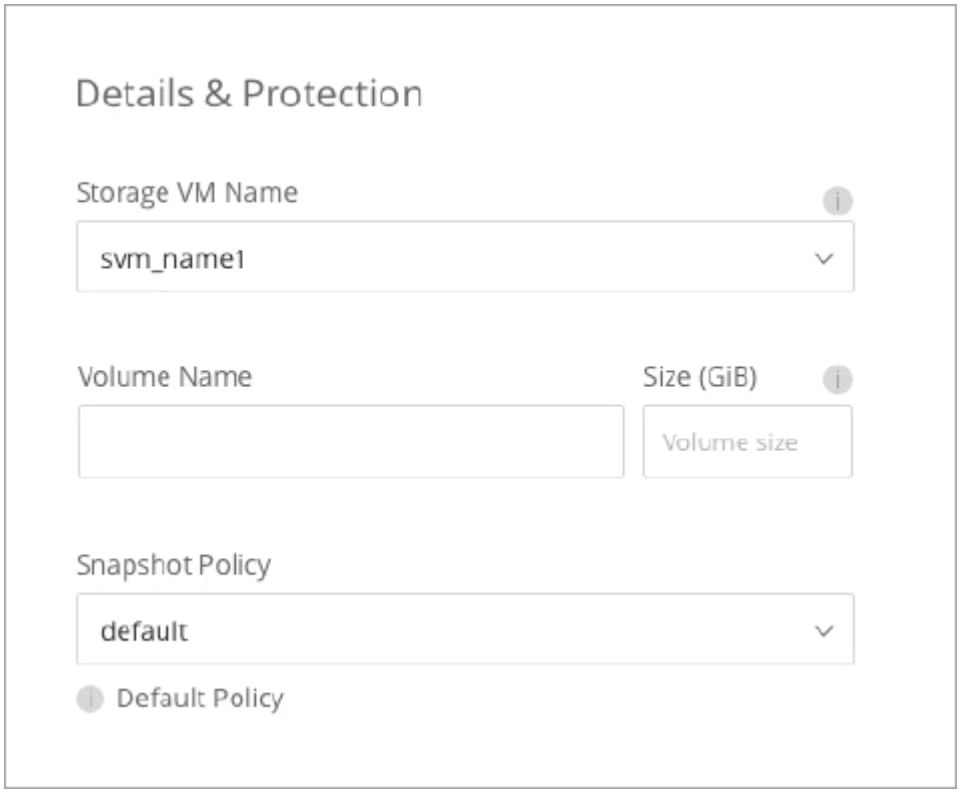
- "Création d'un SVM pour l'accès SMB"

- "Création d'un SVM pour l'accès NFS"
- "Création d'un SVM pour l'accès iSCSI"
- "Création d'un SVM de destination pour la reprise après incident"

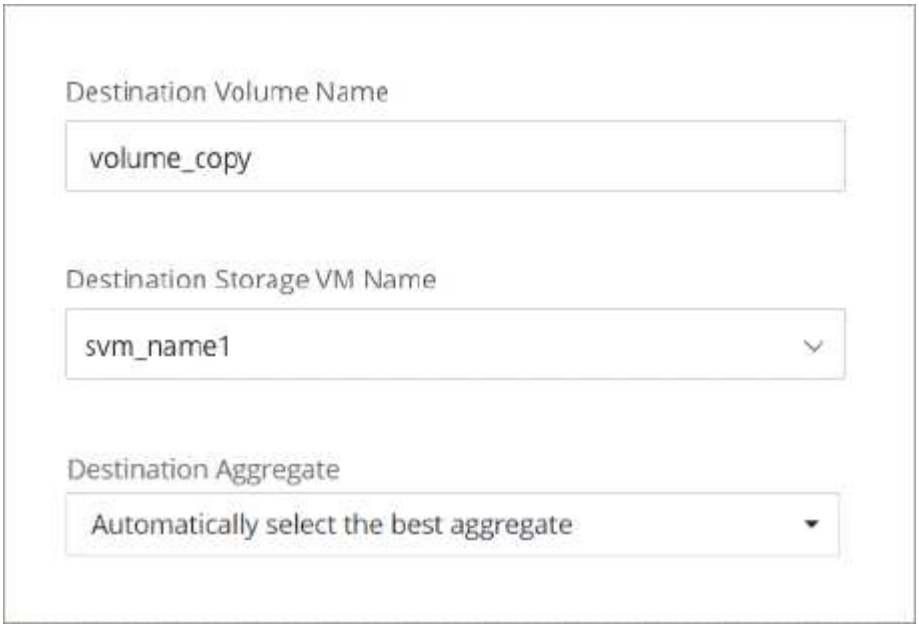
Utilisation de plusieurs VM de stockage dans Cloud Manager

Cloud Manager prend en charge toutes les machines virtuelles de stockage supplémentaires que vous créez à partir de System Manager ou de l'interface de ligne de commandes.

Par exemple, l'image suivante montre comment choisir une VM de stockage lors de la création d'un volume.



L'image suivante montre comment choisir une VM de stockage lors de la réplication d'un volume sur un autre système.



Gestion de la reprise après incident des machines virtuelles de stockage

Cloud Manager ne prend pas en charge la configuration ou l'orchestration pour la reprise d'activité des machines virtuelles de stockage. Vous devez utiliser System Manager ou l'interface de ligne de commandes.

- "Guide de préparation rapide pour la reprise après incident du SVM"
- "Guide de reprise après incident de SVM Express"

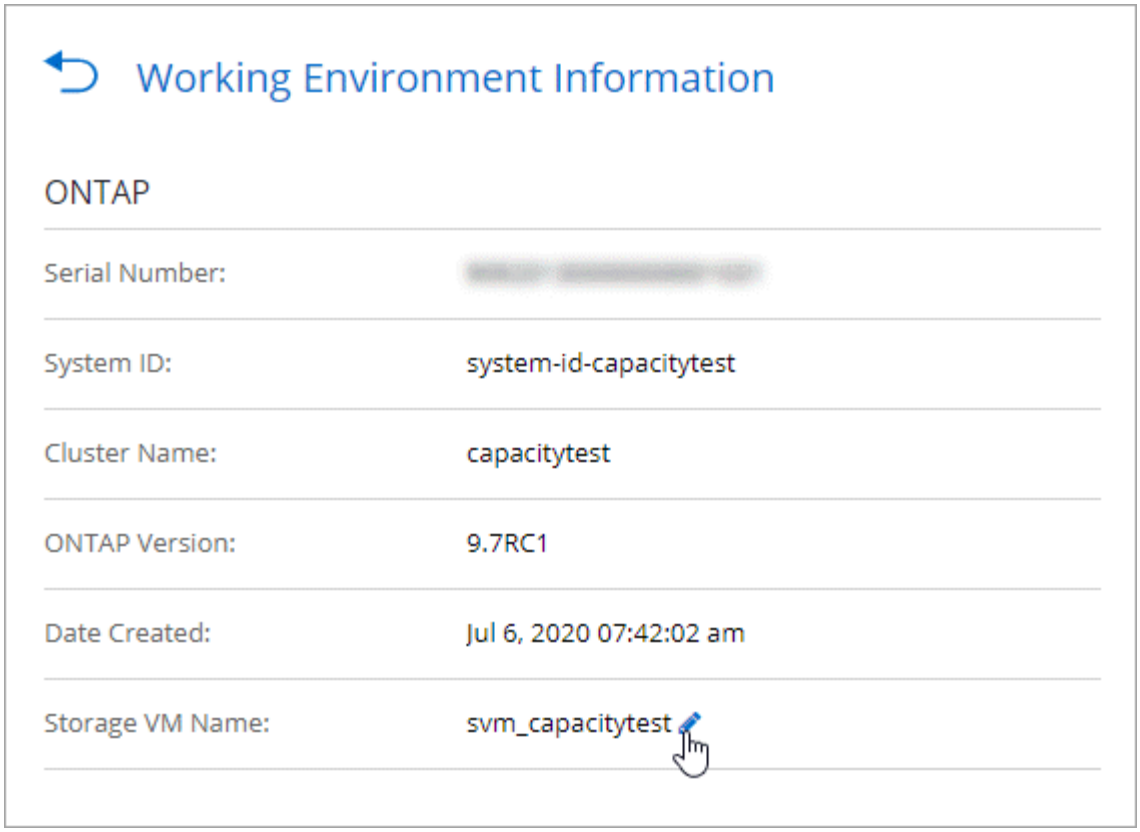
Modification du nom de la machine virtuelle de stockage

Cloud Manager attribue automatiquement la VM de stockage créée pour Cloud Volumes ONTAP. Si vous avez des normes de nommage très strictes, vous pouvez modifier le nom de la machine virtuelle de stockage. Par exemple, vous pouvez indiquer le nom des machines virtuelles de stockage dans vos clusters ONTAP.

Si vous avez créé des machines virtuelles de stockage supplémentaires pour Cloud Volumes ONTAP, vous ne pouvez pas les renommer à partir de Cloud Manager. Pour ce faire, vous devez utiliser System Manager ou l'interface de ligne de commandes directement dans Cloud Volumes ONTAP.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **informations**.
2. Cliquez sur l'icône d'édition située à droite du nom de la VM de stockage.



3. Dans la boîte de dialogue Modifier le nom du SVM, modifiez le nom, puis cliquez sur **Enregistrer**.

Avec Cloud Volumes ONTAP comme stockage persistant pour Kubernetes

Cloud Manager peut automatiser le déploiement de NetApp Trident sur les clusters Kubernetes afin d'utiliser Cloud Volumes ONTAP comme stockage persistant pour les conteneurs.

Trident est un projet open source entièrement pris en charge et géré par NetApp. Trident s'intègre de manière native avec Kubernetes et son framework de volumes persistants pour provisionner et gérer de manière transparente les volumes des systèmes qui exécutent toutes les combinaisons de plateformes de stockage NetApp. "En savoir plus sur Trident".

La fonctionnalité Kubernetes n'est pas prise en charge avec les clusters ONTAP sur site. Elle est prise en charge avec Cloud Volumes ONTAP uniquement.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

1 Passer en revue les prérequis

Assurez-vous que votre environnement peut répondre aux prérequis, qui inclut la connectivité entre les clusters Kubernetes et Cloud Volumes ONTAP, la connectivité entre les clusters Kubernetes et un connecteur, une version minimale de Kubernetes de 1.14, au moins un nœud worker dans un cluster et plus. Voir la liste

complète.

Ajoutez vos clusters Kubernetes à Cloud Manager

Dans Cloud Manager, cliquez sur **Kubernetes** et découvrez les clusters directement depuis le service géré de votre fournisseur cloud ou importez un cluster en fournissant un fichier kubeconfig.

Connectez vos clusters à Cloud Volumes ONTAP

Après avoir ajouté un cluster Kubernetes, cliquez sur **connexion à l'environnement de travail** pour connecter le cluster à un ou plusieurs systèmes Cloud Volumes ONTAP.

Commencez le provisionnement des volumes persistants

Demandez et gérez les volumes persistants à l'aide d'interfaces et de constructions Kubernetes natives. Cloud Manager crée des classes de stockage NFS et iSCSI que vous pouvez utiliser pour le provisionnement de volumes persistants.

"En savoir plus sur le provisionnement de votre premier volume avec Trident pour Kubernetes".

Vérification des prérequis

Avant de commencer, assurez-vous que vos clusters Kubernetes et votre connecteur répondent à des exigences spécifiques.

Exigences relatives aux clusters Kubernetes

- La connectivité réseau est requise entre un cluster Kubernetes et le connecteur et entre un cluster Kubernetes et Cloud Volumes ONTAP.

  Le connecteur et Cloud Volumes ONTAP doivent tous deux se connecter au terminal de l'API Kubernetes :

  - Pour les clusters gérés, configurez une route entre le VPC d'un cluster et le VPC où résident le connecteur et le Cloud Volumes ONTAP.
  - Pour les autres clusters, l'adresse IP du nœud maître ou de l'équilibreur de charge (indiquée dans le fichier kubecconfig) doit être accessible par le connecteur et Cloud Volumes ONTAP, et il doit présenter un certificat TLS valide.
- Un cluster Kubernetes peut se trouver sur n'importe quel emplacement qui dispose de la connectivité réseau indiquée ci-dessus.
- Un cluster Kubernetes doit exécuter la version 1.14 au moins.

  La version maximale prise en charge est définie par Trident. "Cliquez ici pour voir la version Kubernetes maximale prise en charge".
- Un cluster Kubernetes doit disposer d'au moins un nœud worker.
- Pour les clusters exécutés dans Amazon Elastic Kubernetes Service (Amazon EKS), chaque cluster a besoin d'un rôle IAM ajouté afin de résoudre une erreur d'autorisation. Une fois le cluster ajouté, Cloud Manager vous invite à utiliser la commande eksctl exacte qui résout l'erreur.

"En savoir plus sur les limites des autorisations IAM".

- Pour les clusters exécutés dans Azure Kubernetes Service (AKS), ces clusters doivent avoir le rôle *Azure Kubernetes Service RBAC Cluster Admin*. Ceci est nécessaire afin que Cloud Manager puisse installer Trident et configurer des classes de stockage sur le cluster.
- Pour les clusters exécutés dans Google Kubernetes Engine (GKE), ces clusters ne doivent pas utiliser le système d'exploitation optimisé par défaut pour les conteneurs. Vous devez les changer pour utiliser Ubuntu.

  GKE utilise par défaut Google "image optimisée pour les conteneurs", Qui ne dispose pas des utilitaires dont Trident a besoin pour monter des volumes.

Exigences relatives au connecteur

Assurez-vous que la mise en réseau et les autorisations suivantes sont en place pour le connecteur.

Mise en réseau

- Lors de l'installation de Trident, le connecteur doit disposer d'une connexion Internet sortante pour accéder aux terminaux suivants :

  https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/

  Cloud Manager installe Trident sur un cluster Kubernetes lorsque vous connectez un environnement de travail au cluster.

Autorisations requises pour détecter et gérer les clusters EKS

Pour détecter et gérer les clusters Kubernetes exécutés dans Amazon Elastic Kubernetes Service (EKS), le connecteur a besoin d'autorisations d'administration :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "eks:*",
            "Resource": "*"
        }
    ]
}
```

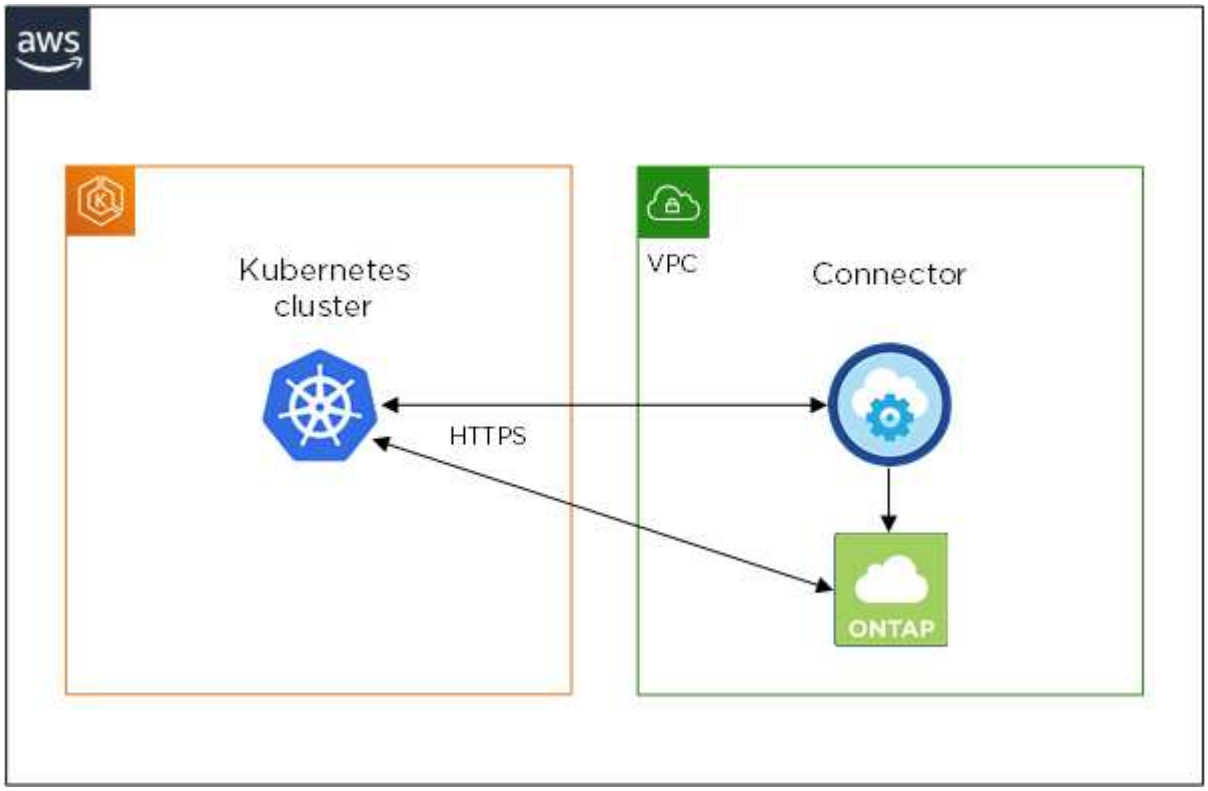
Autorisations requises pour détecter et gérer les clusters GKE

Le connecteur a besoin des autorisations suivantes pour détecter et gérer les clusters Kubernetes exécutés dans Google Kubernetes Engine (GKE) :

```
container.*
```

Exemple de configuration

L'image suivante montre un exemple de cluster Kubernetes exécuté dans Amazon Elastic Kubernetes Service (Amazon EKS) et ses connexions au connecteur et à Cloud Volumes ONTAP.



Ajout des clusters Kubernetes

Ajoutez des clusters Kubernetes à Cloud Manager en découvrant les clusters exécutés dans le service Kubernetes géré de votre fournisseur cloud ou en important le fichier kubeconfig d'un cluster.

Étapes

1. En haut de Cloud Manager, cliquez sur **Kubernetes**.
2. Cliquez sur **Ajouter un cluster**.
3. Choisissez l'une des options disponibles :
   - Cliquez sur **découvrir les clusters** pour découvrir les clusters gérés auxquels Cloud Manager a accès en fonction des autorisations que vous avez fournies au connecteur.

     Par exemple, si votre connecteur est exécuté dans Google Cloud, Cloud Manager utilise les autorisations du compte de service du connecteur pour détecter les clusters exécutés dans Google Kubernetes Engine (GKE).

   - Cliquez sur **Import Cluster** pour importer un cluster à l'aide d'un fichier kubeconfig.

     Une fois le fichier téléchargé, Cloud Manager vérifie la connexion au cluster et enregistre une copie chiffrée du fichier kubeconfig.

Résultat

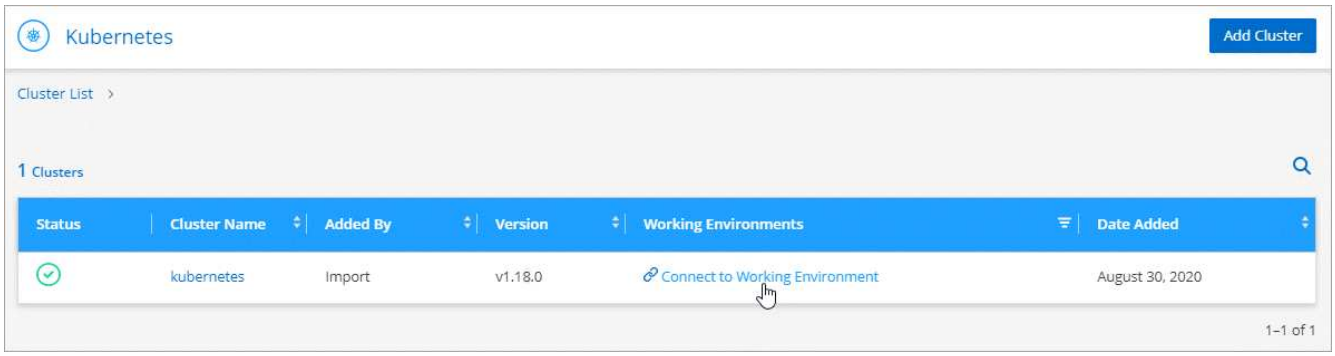
Cloud Manager ajoute le cluster Kubernetes. Vous pouvez désormais connecter le cluster à Cloud Volumes ONTAP.

Connexion d'un cluster à Cloud Volumes ONTAP

Connectez un cluster Kubernetes à Cloud Volumes ONTAP afin d'utiliser Cloud Volumes ONTAP comme stockage persistant pour les conteneurs.

Étapes

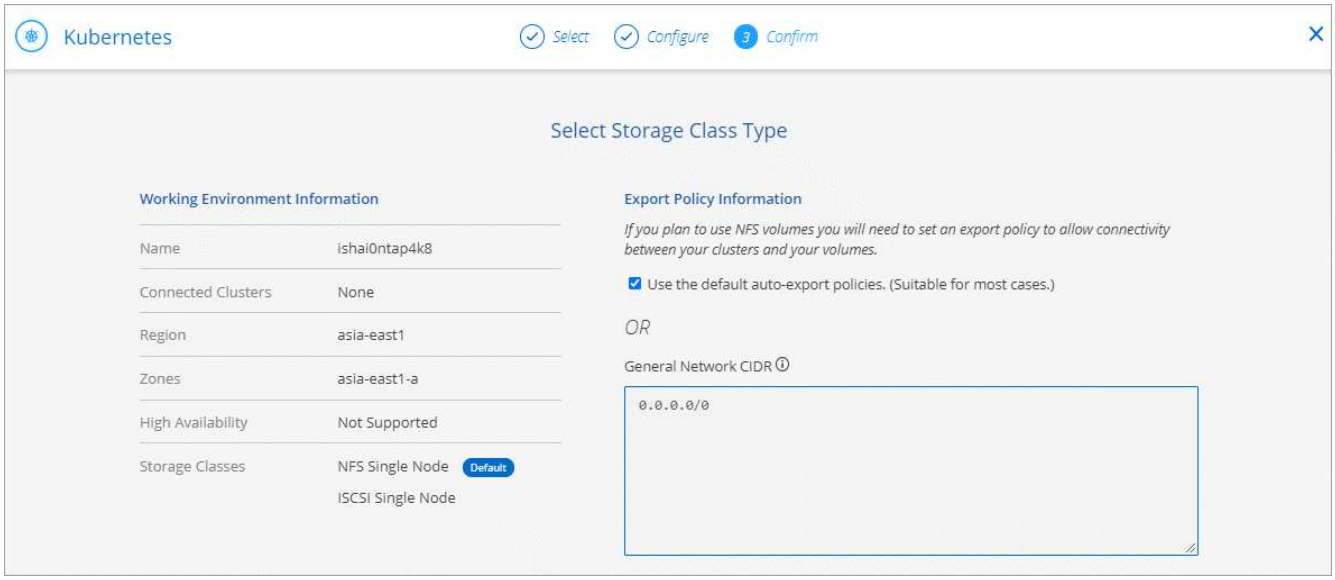
1. En haut de Cloud Manager, cliquez sur **Kubernetes**.
2. Cliquez sur **connexion à l'environnement de travail** pour le cluster que vous venez d'ajouter.



3. Sélectionnez un environnement de travail et cliquez sur **Continuer**.
4. Sélectionnez la classe de stockage NetApp à utiliser comme classe de stockage par défaut pour le cluster Kubernetes, puis cliquez sur **Continuer**.

   Lorsqu'un utilisateur crée un volume persistant, le cluster Kubernetes peut utiliser cette classe de stockage comme stockage back-end par défaut.

5. Choisissez d'utiliser les règles d'exportation automatique par défaut ou d'ajouter un bloc CIDR personnalisé.



6. Cliquez sur **Ajouter un environnement de travail**.

Résultat

Cloud Manager connecte l'environnement de travail au cluster, qui peut prendre jusqu'à 15 minutes.

Gestion des clusters

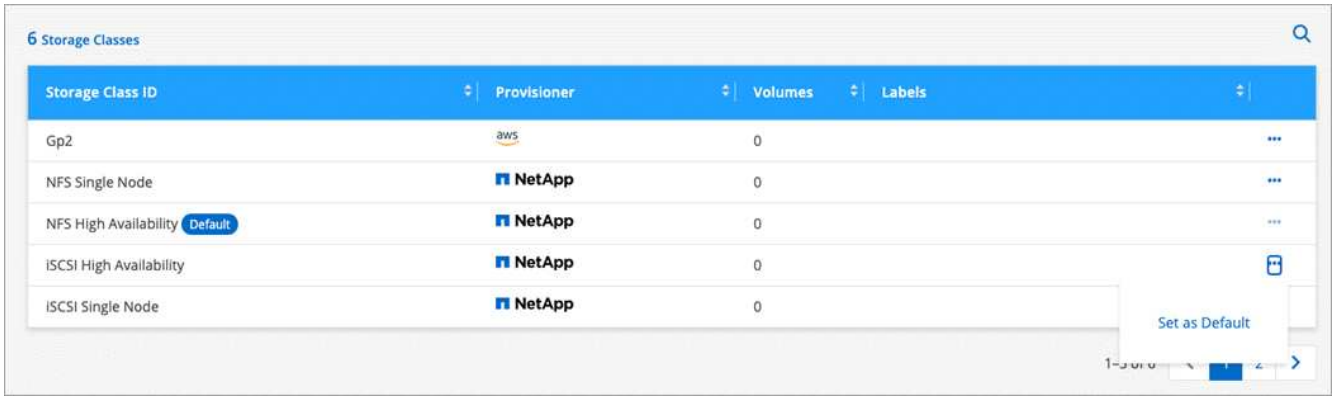
Cloud Manager vous permet de gérer vos clusters Kubernetes en modifiant la classe de stockage par défaut, en mettant à niveau Trident, etc.

Modification de la classe de stockage par défaut

Assurez-vous d'avoir défini une classe de stockage Cloud Volumes ONTAP comme classe de stockage par défaut, de sorte que les clusters utilisent Cloud Volumes ONTAP comme système de stockage back-end.

Étapes

1. En haut de Cloud Manager, cliquez sur **Kubernetes**.
2. Cliquez sur le nom du cluster Kubernetes.
3. Dans le tableau **classes de stockage**, cliquez sur le menu actions à l'extrême droite de la classe de stockage que vous souhaitez définir comme valeur par défaut.



4. Cliquez sur **définir comme valeur par défaut**.

Mise à niveau de Trident

Vous pouvez mettre à niveau Trident depuis Cloud Manager lorsqu'une nouvelle version de Trident est disponible.

Étapes

1. En haut de Cloud Manager, cliquez sur **Kubernetes**.
2. Cliquez sur le nom du cluster Kubernetes.
3. Si une nouvelle version est disponible, cliquez sur **Upgrade** en regard de la version de Trident.

Mise à jour du fichier kubeconfig

Si vous avez ajouté votre cluster à Cloud Manager en important le fichier kubeconfig, vous pouvez télécharger le dernier fichier kubeconfig vers Cloud Manager à tout moment. Vous pouvez le faire si vous avez mis à jour les identifiants, si vous avez modifié des utilisateurs ou des rôles, ou si un changement affecte le cluster, l'utilisateur, l'espace de noms ou l'authentification.

Étapes

1. En haut de Cloud Manager, cliquez sur **Kubernetes**.
2. Cliquez sur le nom du cluster Kubernetes.
3. Cliquez sur **mettre à jour Kubeconfig**.
4. Lorsque vous y êtes invité par l'intermédiaire de votre navigateur Web, sélectionnez le fichier mis à jour kubeconfig et cliquez sur **Ouvrir**.

Résultat

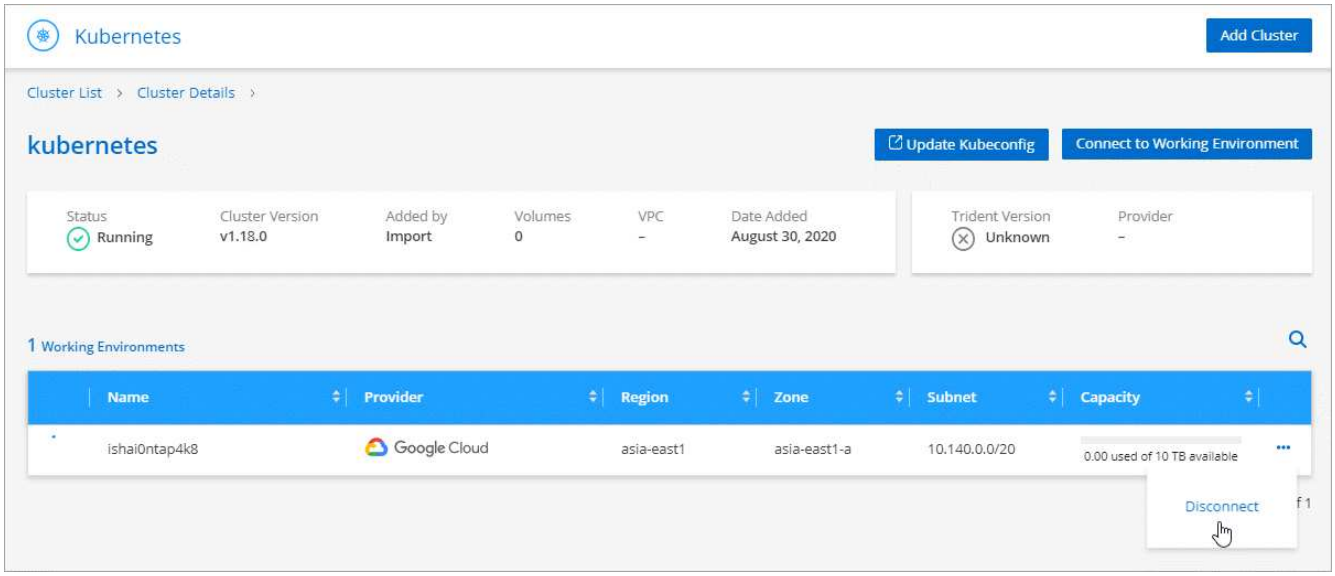
Cloud Manager met à jour des informations concernant le cluster Kubernetes d'après le dernier fichier kubeconfig.

Déconnexion d'un cluster

Lorsque vous déconnectez un cluster de Cloud Volumes ONTAP, vous ne pouvez plus utiliser ce système Cloud Volumes ONTAP comme stockage persistant pour les conteneurs. Les volumes persistants existants ne sont pas supprimés.

Étapes

1. En haut de Cloud Manager, cliquez sur **Kubernetes**.
2. Cliquez sur le nom du cluster Kubernetes.
3. Dans le tableau **environnements de travail**, cliquez sur le menu actions à l'extrême droite de l'environnement de travail que vous souhaitez déconnecter.



4. Cliquez sur **déconnecter**.

Résultat

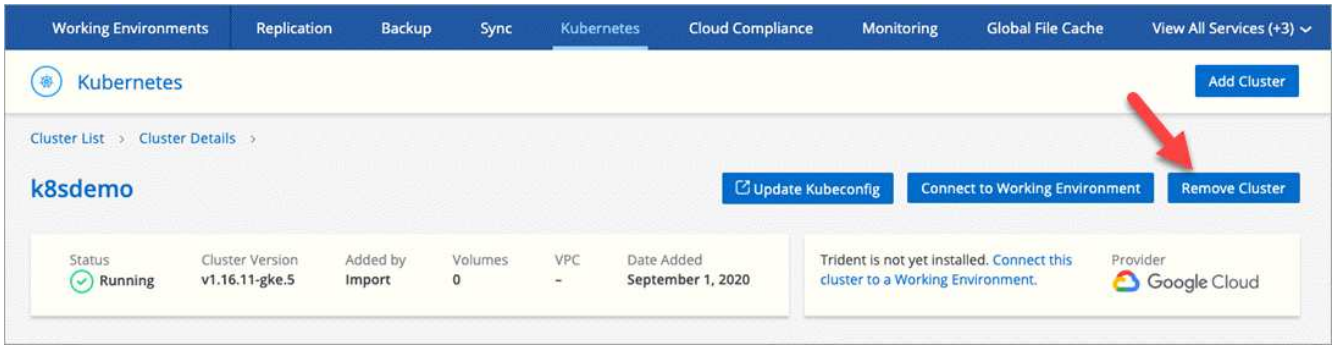
Cloud Manager déconnecte le cluster du système Cloud Volumes ONTAP.

Suppression d'un cluster

Retirez les clusters désaffectés de Cloud Manager après avoir déconnecté tous les environnements de travail du cluster.

Étapes

1. En haut de Cloud Manager, cliquez sur **Kubernetes**.
2. Cliquez sur le nom du cluster Kubernetes.
3. Cliquez sur **Supprimer le cluster**.



Cryptage de volumes grâce aux solutions de cryptage NetApp

Cloud Volumes ONTAP prend en charge NVE (NetApp Volume Encryption) et NAE (NetApp Aggregate Encryption) avec un gestionnaire de clés externe. NVE et NAE sont des solutions logicielles qui permettent le chiffrement des données au repos (conformes à la norme FIPS) de volumes 140-2. "En savoir plus sur ces solutions de cryptage".

NAE est activé par défaut sur les nouveaux agrégats depuis Cloud Volumes ONTAP 9.7 après la configuration d'un gestionnaire de clés externe. NVE est activé par défaut sur les nouveaux volumes qui ne font pas partie d'un agrégat NAE (par exemple, si des agrégats existants ont été créés avant de configurer un gestionnaire de clés externe).

Cloud Volumes ONTAP ne prend pas en charge la gestion intégrée des clés.

Ce dont vous avez besoin

Votre système Cloud Volumes ONTAP doit être enregistré auprès du support NetApp. Depuis la version Cloud Manager 3.7.1, une licence NetApp Volume Encryption est automatiquement installée sur chaque système Cloud Volumes ONTAP enregistré auprès du support NetApp.

- "Ajout de comptes du site de support NetApp à Cloud Manager"
- "Enregistrement des systèmes de paiement à l'utilisation"

Cloud Manager n'installe pas la licence NVE sur les systèmes de la région Chine.

Étapes

1. Consultez la liste des gestionnaires de clés pris en charge dans le "Matrice d'interopérabilité NetApp".

   Recherchez la solution **gestionnaires de clés**.

2. "Connectez-vous à l'interface de ligne de commandes de Cloud Volumes ONTAP".
3. Installez les certificats SSL et connectez-vous aux serveurs de gestion des clés externes.

   "Guide d'alimentation du cryptage ONTAP 9 NetApp : configuration de la gestion externe des clés"

Réplication des données entre les systèmes

Vous pouvez répliquer des données entre des environnements de travail en choisissant une réplication de données unique pour le transfert de données, ou un planning récurrent pour la reprise sur incident ou la conservation à long terme. Par exemple, vous pouvez configurer la réplication des données depuis un système ONTAP sur site vers Cloud Volumes ONTAP pour la reprise après incident.

Cloud Manager simplifie la réplication des données entre les volumes sur des systèmes distincts à l'aide des technologies SnapMirror et SnapVault. Il vous suffit d'identifier le volume source et le volume de destination, puis de choisir une stratégie et un planning de réplication. Cloud Manager achète les disques requis, configure les relations, applique la stratégie de réplication, puis lance le transfert de base entre les volumes.

Le transfert de base inclut une copie complète des données source. Les transferts ultérieurs contiennent des copies différentielles des données source.

Cloud Manager permet la réplication des données entre différents types d'environnements de travail :

- D'un système Cloud Volumes ONTAP à un autre système Cloud Volumes ONTAP
- Entre un système Cloud Volumes ONTAP et un cluster ONTAP sur site
- D'un cluster ONTAP sur site vers un autre cluster ONTAP sur site

Exigences de réplication des données

Avant de pouvoir répliquer des données, vous devez confirmer que des exigences spécifiques sont respectées pour les systèmes Cloud Volumes ONTAP et les clusters ONTAP.

Exigences de version

Vérifiez que les volumes source et de destination exécutent des versions ONTAP compatibles avant de répliquer les données. Pour plus d'informations, reportez-vous à la "Guide d'alimentation de la protection des données".

Exigences spécifiques à Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'ICMP et les ports 11104 et 11105.

  Ces règles sont incluses dans le groupe de sécurité prédéfini.

- Pour répliquer des données entre deux systèmes Cloud Volumes ONTAP dans différents sous-réseaux, les sous-réseaux doivent être routés ensemble (paramètre par défaut).
- Pour répliquer des données entre un système Cloud Volumes ONTAP dans AWS et un système dans Azure, vous devez disposer d'une connexion VPN entre AWS VPC et Azure VNet.

Exigences spécifiques aux clusters ONTAP

- Une licence SnapMirror active doit être installée.
- Si le cluster se trouve sur votre site, vous devez disposer d'une connexion entre votre réseau d'entreprise et AWS ou Azure, qui est généralement une connexion VPN.
- Les clusters ONTAP doivent répondre à des exigences supplémentaires en termes de sous-réseau, de port, de pare-feu et de cluster.

  Pour plus d'informations, reportez-vous au Cluster and SVM Peering Express Guide de votre version d'ONTAP.

Configuration de la réplication des données entre les systèmes

Vous pouvez répliquer des données entre les systèmes Cloud Volumes ONTAP et les clusters ONTAP en choisissant une réplication de données unique, qui peut vous aider à déplacer des données vers et depuis le cloud, ou un planning récurrent, qui peut vous aider à la reprise sur incident ou à la conservation à long terme.

Description de la tâche

Cloud Manager prend en charge des configurations de protection des données simples, en panne et en cascade :

- Dans une configuration simple, la réplication s'effectue du volume A au volume B.
- Dans une configuration en panne, la réplication se produit du volume A vers plusieurs destinations.
- Dans une configuration en cascade, la réplication s'effectue du volume A au volume B et du volume B au volume C.

Vous pouvez configurer les configurations en cascade et en panne dans Cloud Manager en configurant plusieurs réplications de données entre les systèmes. Par exemple, en répliquant un volume du système A vers le système B, puis en répliquant le même volume du système B vers le système C.

Étapes

1. Sur la page Working Environments (Environnements de travail), sélectionnez l'environnement de travail qui contient le volume source, puis faites-le glisser vers l'environnement de travail vers lequel vous souhaitez répliquer le volume :

2. Si les pages Configuration de la mise en valeur de la source et de la destination s'affichent, sélectionnez tous les LIF intercluster pour la relation d'homologues du cluster.

   Le réseau intercluster doit être configuré de sorte que les pairs de cluster disposent d'une connectivité « full-mesh » au niveau des paires, ce qui signifie que chaque paire de clusters d'une relation cluster peer-to-peer dispose d'une connectivité parmi l'ensemble de leurs LIFs intercluster.

Ces pages s'affichent si un cluster ONTAP disposant de plusieurs LIF est la source ou la destination.

3. Sur la page Sélection du volume source, sélectionnez le volume que vous souhaitez répliquer.
4. Sur la page Nom du volume de destination et Tiering, spécifiez le nom du volume de destination, choisissez un type de disque sous-jacent, modifiez l'une des options avancées, puis cliquez sur **Continuer**.

   Si la destination est un cluster ONTAP, vous devez également spécifier le SVM de destination et l'agrégat.

5. Sur la page Taux de transfert maximal, spécifiez le débit maximal (en mégaoctets par seconde) auquel les données peuvent être transférées.
6. Sur la page Stratégie de réplication, choisissez l'une des stratégies par défaut ou cliquez sur **stratégies supplémentaires**, puis sélectionnez l'une des stratégies avancées.

   Pour obtenir de l'aide, voir "Choix d'une stratégie de réplication".

   Si vous choisissez une stratégie de sauvegarde personnalisée (SnapVault), les étiquettes associées à la stratégie doivent correspondre aux étiquettes des copies Snapshot sur le volume source. Pour plus d'informations, voir "Fonctionnement des stratégies de sauvegarde".

7. Sur la page Programmation, choisissez une copie unique ou un planning récurrent.

   Plusieurs plannings par défaut sont disponibles. Si vous souhaitez un autre planning, vous devez créer une nouvelle planification sur le cluster *destination* à l'aide de System Manager.

8. Sur la page Revue, vérifiez vos sélections, puis cliquez sur **Go**.

Résultat

Cloud Manager démarre le processus de réplication des données. Vous pouvez afficher des informations détaillées sur la réplication dans la page Etat de la réplication.

Gestion des planifications et des relations de réplication des données

Après avoir configuré la réplication des données entre deux systèmes, vous pouvez gérer le planning et la relation de réplication des données à partir de Cloud Manager.

Étapes

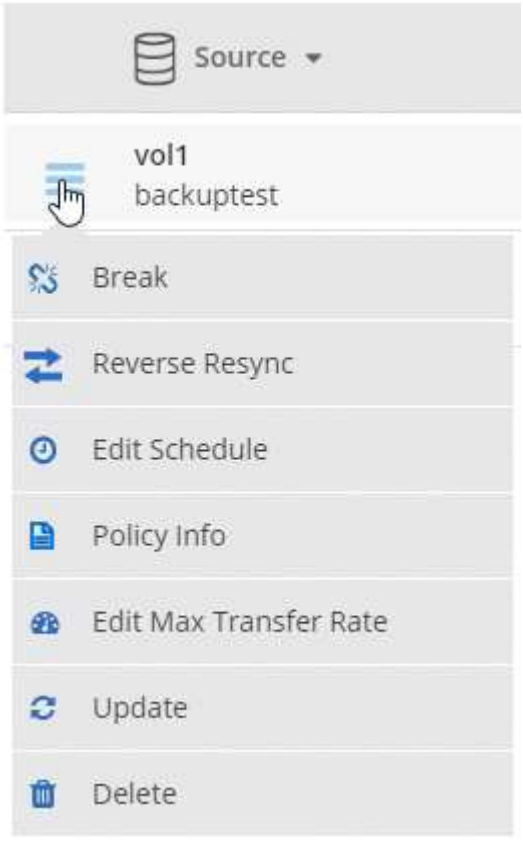
1. Sur la page environnements de travail, affichez l'état de réplication de tous les environnements de travail de l'espace de travail ou d'un environnement de travail spécifique :

Option	Action
Tous les environnements de travail de l'espace de travail	En haut de Cloud Manager, cliquez sur **Replication**.
Un environnement de travail spécifique	Ouvrez l'environnement de travail et cliquez sur **réplications**.

2. Vérifiez l'état des relations de réplication des données pour vérifier qu'elles sont en bon état.

Si l'état d'une relation est inactif et que l'état Miroir n'est pas initialisé, vous devez initialiser la relation à partir du système de destination pour que la réplication des données se produise selon le planning défini. Vous pouvez initialiser la relation à l'aide de System Manager ou de l'interface de ligne de commande (CLI). Ces états peuvent apparaître en cas de défaillance du système de destination, puis revenir en ligne.

3. Sélectionnez l'icône de menu située en regard du volume source, puis choisissez l'une des actions disponibles.



Le tableau suivant décrit les actions disponibles :

Action	Description
Pause	Rompt la relation entre les volumes source et de destination et active le volume de destination pour l'accès aux données. Cette option est généralement utilisée lorsque le volume source ne peut pas servir de données en raison d'événements tels que la corruption des données, la suppression accidentelle ou un état hors ligne. Pour plus d'informations sur la configuration d'un volume de destination pour l'accès aux données et la réactivation d'un volume source, reportez-vous au Guide ONTAP 9 Volume Disaster Recovery Express Guide.

Action	Description
Resynchroniser	Rétablit une relation interrompue entre les volumes et reprend la réplication des données selon le planning défini. Lorsque vous resynchronisez les volumes, le contenu du volume de destination est remplacé par le contenu du volume source. Pour effectuer une resynchronisation inverse, qui resynchronise les données du volume de destination vers le volume source, consultez la "Guide rapide de reprise après incident de volumes ONTAP 9".
Resynchronisation inverse	Inverse les rôles des volumes source et de destination. Le contenu du volume source d'origine est remplacé par le contenu du volume de destination. Ceci est utile lorsque vous souhaitez réactiver un volume source hors ligne. Toutes les données écrites sur le volume source d'origine entre la dernière réplication de données et l'heure à laquelle le volume source a été désactivé ne sont pas conservées.
Modifier le planning	Vous permet de choisir un planning différent pour la réplication des données.
Informations sur les règles	Affiche la stratégie de protection attribuée à la relation de réplication des données.
Modifier le taux de transfert maximal	Permet de modifier le taux maximal (en kilo-octets par seconde) auquel les données peuvent être transférées.
Mise à jour	Lance un transfert incrémentiel pour mettre à jour le volume de destination.
Supprimer	Supprime la relation de protection des données entre les volumes source et de destination, ce qui signifie que la réplication des données n'a plus lieu entre les volumes. Cette action n'active pas le volume de destination pour l'accès aux données. Cette action supprime également la relation d'homologues de cluster et la relation d'homologues de la machine virtuelle de stockage (SVM), si aucune autre relation de protection des données n'existe entre les systèmes.

Résultat

Après avoir sélectionné une action, Cloud Manager met à jour la relation ou le planning.

Choix d'une stratégie de réplication

Vous aurez peut-être besoin d'aide pour choisir une règle de réplication lorsque vous configurez la réplication des données dans Cloud Manager. Une stratégie de réplication définit la manière dont le système de stockage réplique les données d'un volume source vers un volume de destination.

Quelles sont les règles de réplication

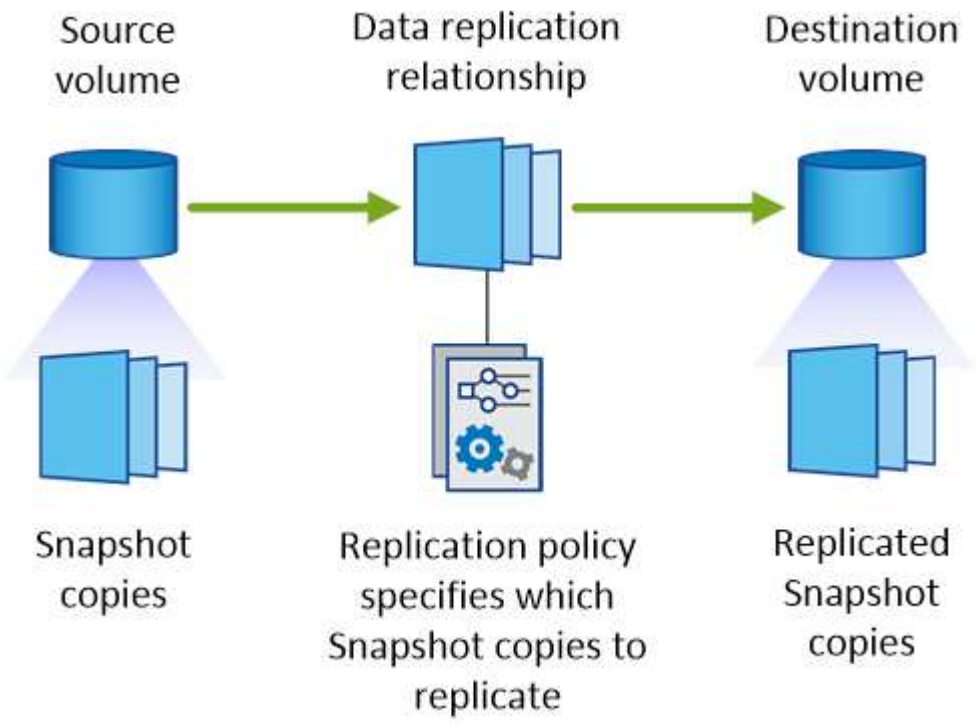
Le système d'exploitation ONTAP crée automatiquement des sauvegardes appelées copies Snapshot. Une copie Snapshot est une image en lecture seule d'un volume qui capture l'état du système de fichiers à un moment donné.

Lorsque vous répliquez des données entre des systèmes, vous répliquez des copies Snapshot d'un volume source vers un volume de destination. Une stratégie de réplication spécifie les copies Snapshot à répliquer du

volume source vers le volume de destination.

Les règles de réplication sont également appelées « stratégies de protection_ car elles sont optimisées par les technologies SnapMirror et SnapVault, qui assurent la protection de la reprise après incident ainsi que la sauvegarde et la restauration disque à disque.

L'image suivante montre la relation entre les copies Snapshot et les règles de réplication :



Types de règles de réplication

Il existe trois types de règles de réplication :

- Une règle *Mirror* réplique les copies Snapshot nouvellement créées vers un volume de destination.

  Vous pouvez utiliser ces copies Snapshot pour protéger le volume source en vue de la reprise après incident ou de la réplication de données unique. Vous pouvez activer le volume de destination pour l'accès aux données à tout moment.

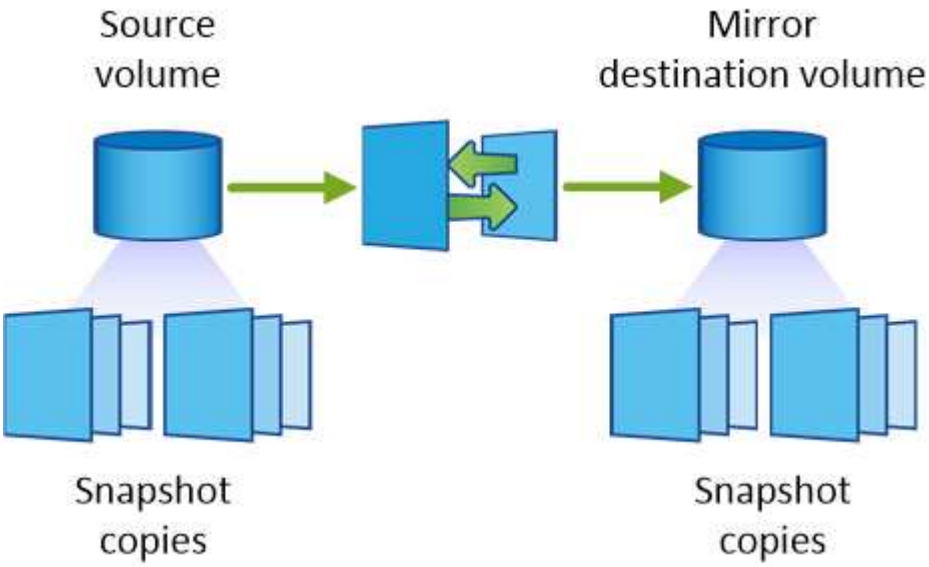
- Une règle *Backup* réplique des copies Snapshot spécifiques sur un volume de destination et les conserve généralement pendant une période plus longue que sur le volume source.

  Vous pouvez restaurer des données à partir de ces copies Snapshot lorsque les données sont corrompues ou perdues, et les conserver à des fins de conformité aux normes et à d'autres fins liées à la gouvernance.

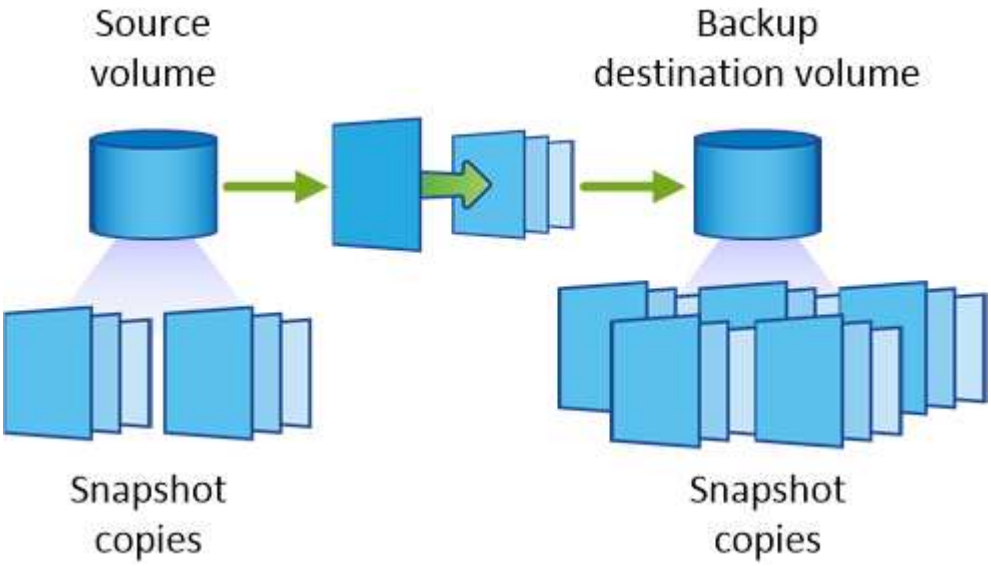
- Une politique *Mirror et Backup* permet la reprise sur incident et la conservation à long terme.

  Chaque système inclut une stratégie de mise en miroir et de sauvegarde par défaut, qui fonctionne bien dans de nombreuses situations. Si vous avez besoin de règles personnalisées, vous pouvez créer vos propres règles à l'aide de System Manager.

Les images suivantes montrent la différence entre les stratégies Miroir et Sauvegarde. Une stratégie Miroir reflète les copies Snapshot disponibles sur le volume source.



Une stratégie de sauvegarde conserve généralement les copies Snapshot plus longtemps qu'elles ne sont conservées sur le volume source :



Fonctionnement des stratégies de sauvegarde

Contrairement aux stratégies Mirror, les stratégies de sauvegarde (SnapVault) répliquent des copies Snapshot spécifiques vers un volume de destination. Il est important de comprendre le fonctionnement des stratégies de sauvegarde si vous souhaitez utiliser vos propres règles au lieu des règles par défaut.

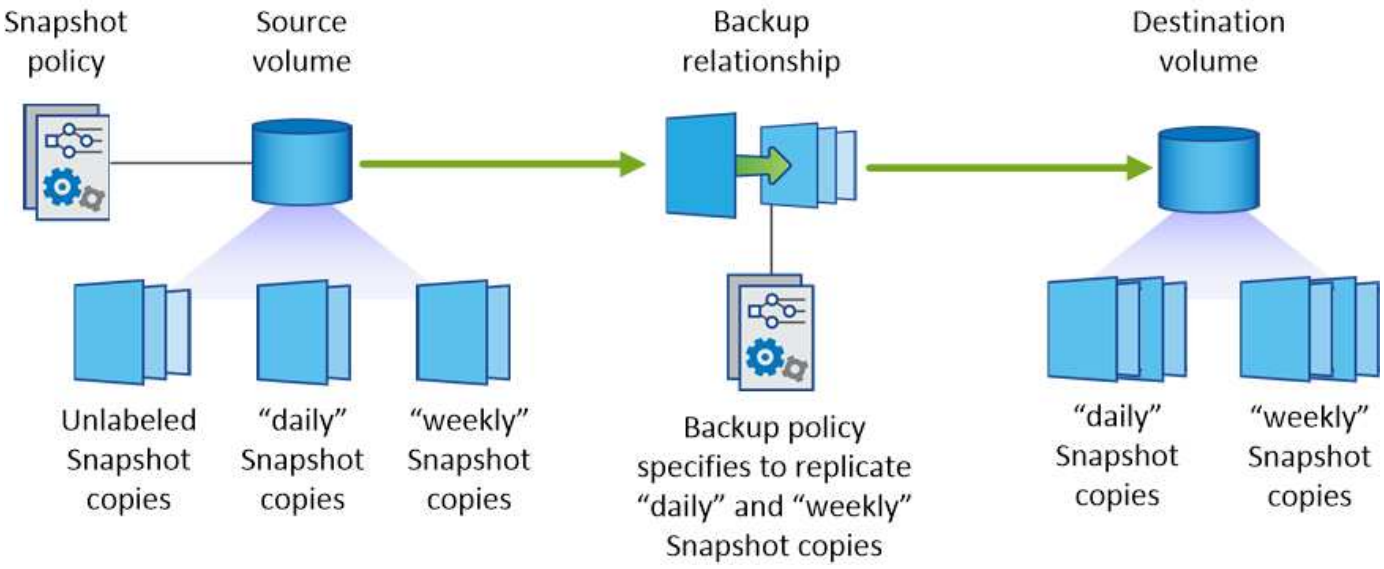
Comprendre la relation entre les étiquettes de copie Snapshot et les stratégies de sauvegarde

Une stratégie Snapshot définit la façon dont le système crée des copies Snapshot de volumes. La stratégie indique quand créer les copies Snapshot, le nombre de copies à conserver et comment les étiqueter. Par exemple, un système peut créer une copie Snapshot tous les jours à 12 h 10, conserver les deux copies les plus récentes et les étiqueter " quotidiennement ".

Une stratégie de sauvegarde inclut des règles qui spécifient les copies Snapshot à répliquer sur un volume de destination et le nombre de copies à conserver. Les étiquettes définies dans une stratégie de sauvegarde doivent correspondre à une ou plusieurs étiquettes définies dans une stratégie Snapshot. Dans le cas

contraire, le système ne peut pas répliquer de copies Snapshot.

Par exemple, une stratégie de sauvegarde qui inclut les étiquettes " quotidiennes " et " hebdomadaires " entraîne la réplication des copies Snapshot qui n'incluent que ces étiquettes. Aucune autre copie Snapshot n'est répliquée, comme illustré dans l'image suivante :



Règles par défaut et règles personnalisées

La stratégie Snapshot par défaut crée des copies Snapshot toutes les heures, quotidiennes et hebdomadaires, conservant six copies Snapshot toutes les heures, deux copies quotidiennes et deux copies Snapshot hebdomadaires.

Vous pouvez facilement utiliser une stratégie de sauvegarde par défaut avec la stratégie Snapshot par défaut. Les règles de sauvegarde par défaut répliquent les copies Snapshot quotidiennes et hebdomadaires, en conservant sept copies Snapshot quotidiennes et 52 copies Snapshot hebdomadaires.

Si vous créez des règles personnalisées, les étiquettes définies par ces règles doivent correspondre. Vous pouvez créer des règles personnalisées à l'aide de System Manager.

Réplication des données de NetApp HCI vers Cloud Volumes ONTAP

Si vous essayez de répliquer des données de NetApp HCI vers Cloud Volumes ONTAP, vous pouvez le faire sur un système NetApp HCI exécutant le logiciel NetApp Element à l'aide de SnapMirror. Vous pouvez également répliquer les données sur des volumes créés sur un système ONTAP Select, qui s'exécute en tant qu'invité virtuel dans une solution NetApp HCI vers Cloud Volumes ONTAP.

Pour plus d'informations, reportez-vous aux rapports techniques suivants :

- "Rapport technique 4641 : protection des données NetApp HCI"
- "Rapport technique 4651 : architecture et configuration de NetApp SolidFire SnapMirror"

Contrôle des performances

Découvrez le service surveillance

En exploitant la "Service NetApp Cloud Insights", Cloud Manager vous donne des informations sur l'état et les performances de vos instances Cloud Volumes ONTAP et vous aide à dépanner et à optimiser les performances de votre environnement de stockage cloud.

Caractéristiques

- Surveillance automatique de tous les volumes
- Affichez les données de performances de volumes en termes d'IOPS, de débit et de latence
- Identifiez les problèmes de performances pour minimiser l'impact sur vos utilisateurs et vos applications

Fournisseurs cloud pris en charge

Le service de contrôle est pris en charge par Cloud Volumes ONTAP pour AWS.

Le coût

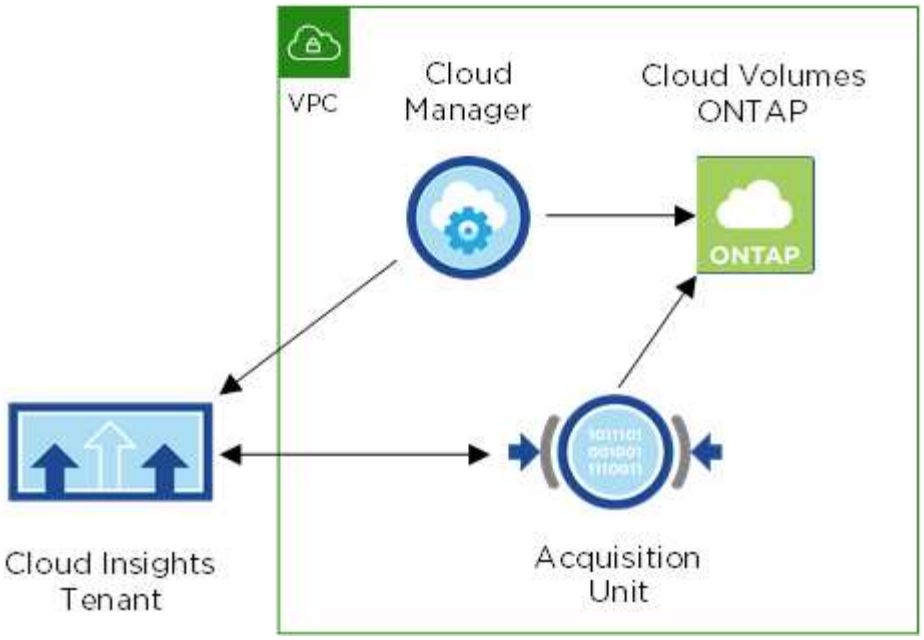
La surveillance est actuellement disponible sous forme d'aperçu. L'activation est gratuite, mais Cloud Manager lance une machine virtuelle dans votre VPC pour faciliter le contrôle. Cette machine virtuelle entraîne des frais supplémentaires de la part de votre fournisseur cloud.

Fonctionnement de Cloud Insights avec Cloud Manager

À un niveau élevé, l'intégration d'Cloud Insights avec Cloud Manager fonctionne comme suit :

1. Vous activez le service de surveillance sur Cloud Volumes ONTAP.
2. Cloud Manager configure votre environnement. Il effectue les opérations suivantes :
    a. Crée un locataire Cloud Insights (également appelé *environnement*) et associe tous les utilisateurs de votre compte Cloud Central au locataire.
    b. Offre une version d'essai gratuite de 30 jours d'Cloud Insights.
    c. Déploie une machine virtuelle dans votre VPC appelé unité d'acquisition, ce qui facilite la surveillance des volumes (il s'agit de la machine virtuelle mentionnée dans la section de coût ci-dessus).
    d. Connecte l'unité d'acquisition à Cloud Volumes ONTAP et au locataire Cloud Insights.
3. Dans Cloud Manager, vous cliquez sur surveillance et utilisez les données de performance pour résoudre les problèmes et optimiser les performances.

L'image suivante montre la relation entre ces composants :



L'unité d'acquisition

Lorsque vous activez surveillance, Cloud Manager déploie une unité d'acquisition dans le même sous-réseau que le connecteur.

Une *unité d'acquisition* collecte les données de performances de Cloud Volumes ONTAP et les envoie au locataire Cloud Insights. Cloud Manager interroge ensuite les données et les présente à votre place.

Notez ce qui suit à propos de l'instance d'unité d'acquisition :

- L'unité d'acquisition fonctionne sur une instance t3.XLarge avec un volume GP2 de 100 Go.
- L'instance s'appelle *AcquisitionUnit* avec un hachage (UUID) généré concaténé. Par exemple : *AcquisitionUnit-FAN7FqeH*
- Une seule unité d'acquisition est déployée par connecteur.
- L'instance doit être en cours d'exécution pour accéder aux informations de performances dans l'onglet surveillance.

Locataire Cloud Insights

Cloud Manager configure un *tenant* lorsque vous activez la surveillance. Un locataire Cloud Insights vous permet d'accéder aux données de performance collectées par l'unité d'acquisition. Le locataire est une partition de données sécurisée au sein du service NetApp Cloud Insights.

Interface Web de Cloud Insights

L'onglet Monitoring de Cloud Manager fournit des données de performance de base pour vos volumes. Vous pouvez accéder à l'interface Web de Cloud Insights depuis votre navigateur pour effectuer un contrôle plus approfondi et configurer des alertes pour vos systèmes Cloud Volumes ONTAP.

Essai gratuit et abonnement

Cloud Manager propose une version d'évaluation gratuite de 30 jours de Cloud Insights. Elle vous permet de fournir des données de performances dans Cloud Manager et d'explorer les fonctionnalités proposées par Cloud Insights Standard Edition.

Vous devez vous abonner d'ici la fin de la période d'essai gratuite ; sinon, votre locataire Cloud Insights finira par être supprimé. Vous pouvez vous abonner à l'édition Basic, Standard ou Premium pour continuer à utiliser la fonctionnalité Monitoring dans Cloud Manager.

"Découvrez comment vous inscrire à Cloud Insights".

Contrôle d'Cloud Volumes ONTAP dans AWS

Suivez quelques étapes pour contrôler les performances d'Cloud Volumes ONTAP.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

Vérifiez la prise en charge de votre configuration

Vous devez avoir installé Cloud Manager 3.8.4 ou une version ultérieure dans AWS et Cloud Volumes ONTAP dans AWS. Vous devez également être un nouveau client Cloud Insights.

Activez la surveillance sur votre système nouveau ou existant

- Nouveaux environnements de travail : assurez-vous de maintenir l'option surveillance activée lorsque vous créez l'environnement de travail (activé par défaut).
- Environnements de travail existants : sélectionnez un environnement de travail et cliquez sur **Démarrer la surveillance**.

Afficher les données de performances

Cliquez sur **Monitoring** et affichez les données de performances de vos volumes.

Abonnez-vous à Cloud Insights

Abonnez-vous avant la fin de votre essai gratuit de 30 jours pour continuer à consulter les données de performances dans Cloud Manager et Cloud Insights. "Découvrez comment vous inscrire".

De formation

Lisez les informations suivantes pour vous assurer que votre configuration est prise en charge.

Versions de Cloud Manager prises en charge

Vous devez installer Cloud Manager 3.8.4 ou une version ultérieure. Une nouvelle installation est nécessaire car une nouvelle infrastructure est requise pour activer le service de surveillance. Cette infrastructure est disponible en commençant par les nouvelles installations de Cloud Manager 3.8.4.

Versions de Cloud Volumes ONTAP prises en charge

Toute version d'Cloud Volumes ONTAP dans AWS.

Condition Cloud Insights

Vous devez être un nouveau client de Cloud Insights. La surveillance n'est pas prise en charge si vous disposez déjà d'un locataire Cloud Insights.

Adresse e-mail pour Cloud Central

L'adresse e-mail de votre compte utilisateur Cloud Central doit être l'adresse e-mail professionnelle. Les domaines de messagerie gratuits tels que gmail et hotmail ne sont pas pris en charge lors de la création d'un locataire Cloud Insights.

Mise en réseau pour l'unité d'acquisition

L'unité d'acquisition utilise une authentification bidirectionnelle/mutuelle pour se connecter au serveur Cloud Insights. Le certificat client doit être transmis au serveur Cloud Insights pour être authentifié. Pour ce faire, le proxy doit être configuré pour transférer la requête http au serveur Cloud Insights sans décrypter les données.

L'unité d'acquisition utilise les deux noeuds finaux suivants pour communiquer avec Cloud Insights. Si vous disposez d'un pare-feu entre le serveur de l'unité d'acquisition et Cloud Insights, vous avez besoin de ces noeuds finaux lors de la configuration des règles de pare-feu :

```
https://aulogin.<Cloud Insights Domain>
https://<your-tenant-ID>.<Cloud Insights Domain>
```

Par exemple :

```
https://aulogin.c01.cloudinsights.netapp.com
https://cg0c586a-ee05-45rb-a5ac-
333b5ae7718d7.c01.cloudinsights.netapp.com
```

Contactez-nous via la discussion interne si vous avez besoin d'aide pour identifier votre domaine Cloud Insights et votre identifiant de locataire.

Mise en réseau du connecteur

Comme pour l'unité d'acquisition, le connecteur doit disposer d'une connectivité sortante avec le locataire Cloud Insights. Mais le point d'extrémité que les contacts du connecteur sont légèrement différents. Il contacte l'URL de l'hôte du locataire à l'aide de l'ID de locataire raccourci :

```
 https://<your-short-tenant-ID>.<Cloud Insights Domain>
Par exemple :
```

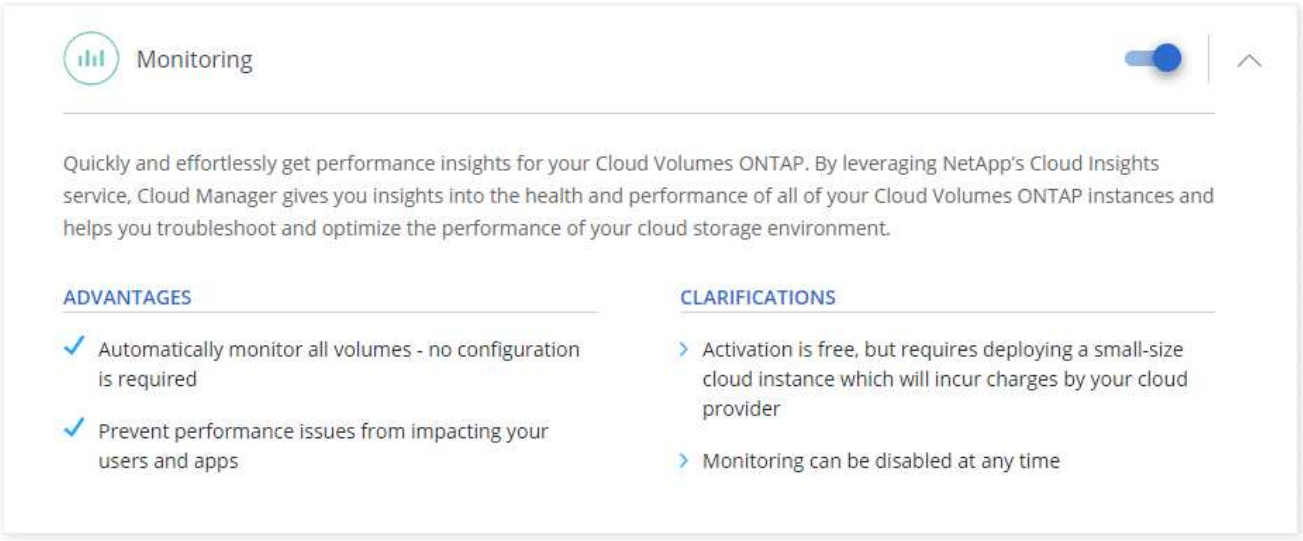
```
 https://abcd12345.c01.cloudinsights.netapp.com
Encore une fois, vous pouvez nous contacter par le biais de la
discussion sur le produit si vous avez besoin d'aide pour identifier
l'URL d'hôte du locataire.
```

Activation de la surveillance sur un nouveau système

Le service de surveillance est activé par défaut dans l'assistant de l'environnement de travail. Assurez-vous de conserver l'option activée.

Étapes

1. Cliquez sur **Créer Cloud Volumes ONTAP**.
2. Sélectionnez Amazon Web Services en tant que fournisseur cloud, puis choisissez un système à un seul nœud ou haute disponibilité.
3. Remplissez la page Détails et références.
4. Sur la page Services, laissez le service activé et cliquez sur **Continuer**.

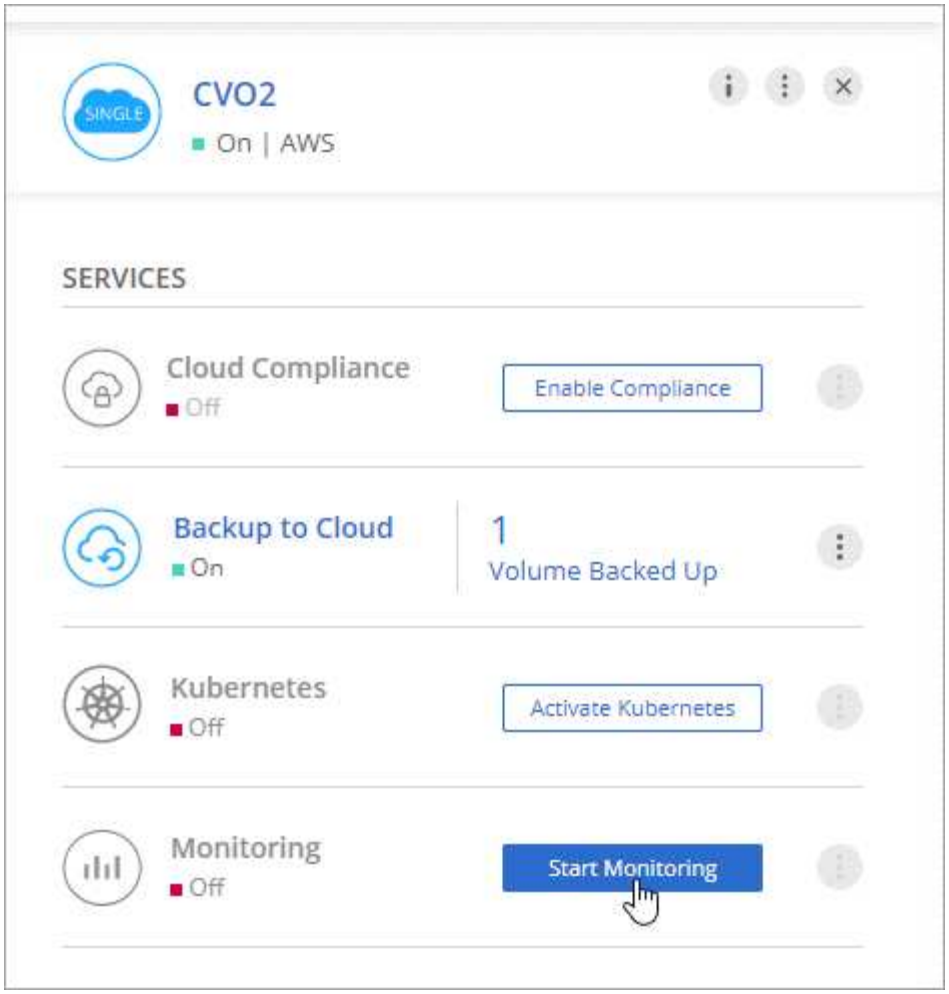


Activation de la surveillance sur un système existant

Activez la surveillance à tout moment à partir de l'environnement de travail.

Étapes

1. En haut de Cloud Manager, cliquez sur **environnements de travail**.
2. Sélectionnez un environnement de travail.
3. Dans le volet de droite, cliquez sur **Démarrer la surveillance**.



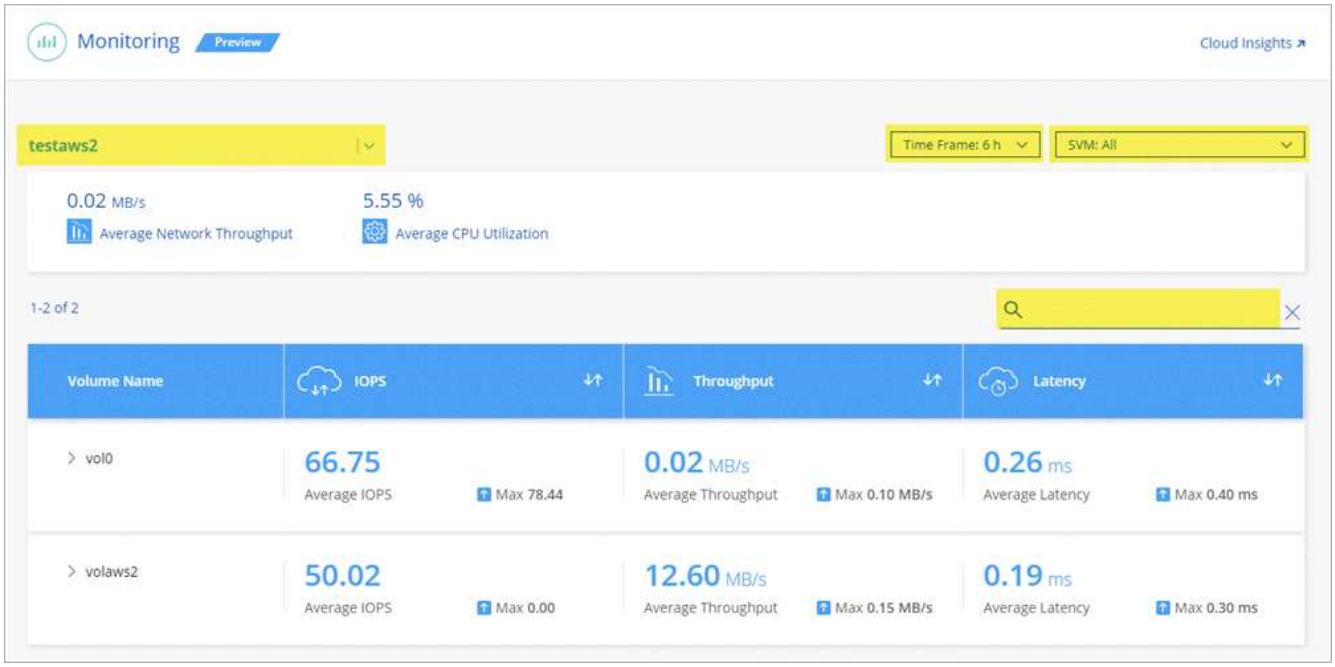
Surveillance de vos volumes

Surveillez les performances en affichant les IOPS, le débit et la latence de chacun de vos volumes.

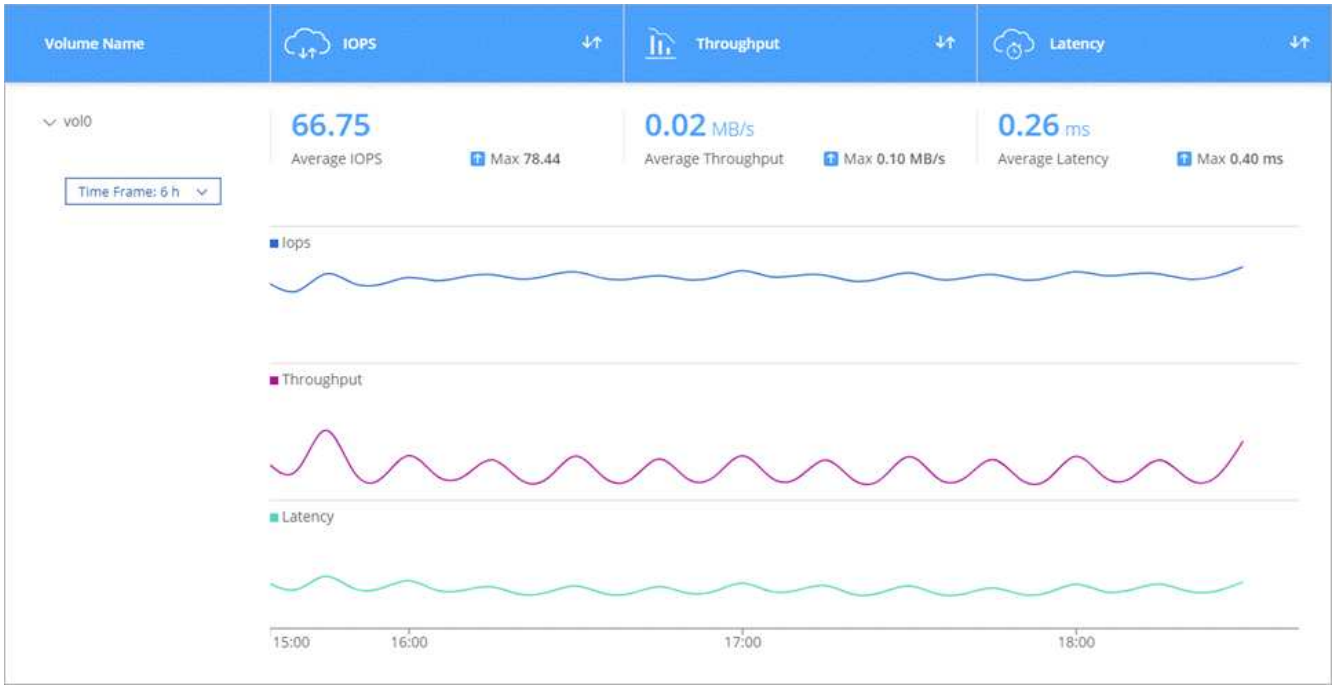
Étapes

1. En haut de Cloud Manager, cliquez sur **Monitoring**.
2. Filtrez le contenu du tableau de bord pour afficher les informations dont vous avez besoin.
    - Sélectionnez un environnement de travail spécifique.
    - Sélectionnez une autre période.
    - Sélectionnez un SVM spécifique.
    - Rechercher un volume spécifique.

    L'image suivante met en évidence chacune de ces options :



3. Cliquez sur un volume dans le tableau pour développer la ligne et afficher une chronologie pour les IOPS, le débit et la latence.



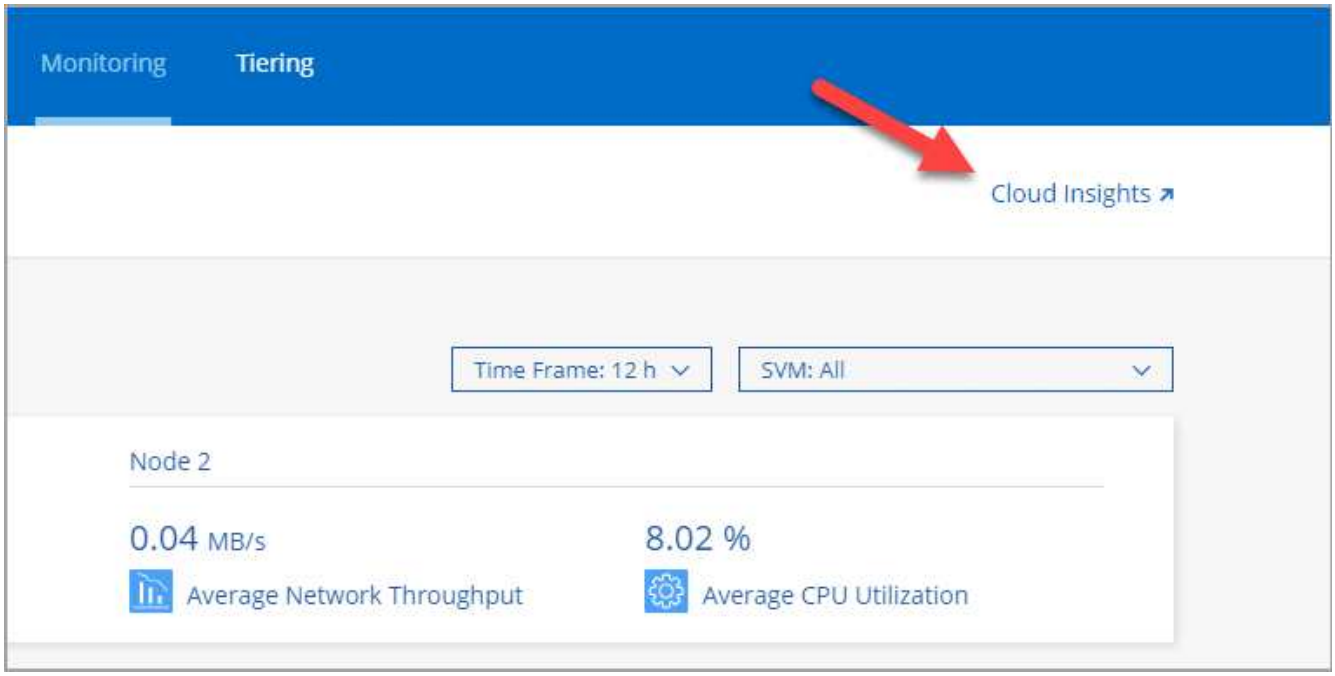
4. Utilisez ces données pour identifier les problèmes de performances et minimiser l'impact sur les utilisateurs et les applications.

Obtenir de plus amples informations sur Cloud Insights

L'onglet Monitoring de Cloud Manager fournit des données de performance de base pour vos volumes. Vous pouvez accéder à l'interface Web de Cloud Insights depuis votre navigateur pour effectuer un contrôle plus approfondi et configurer des alertes pour vos systèmes Cloud Volumes ONTAP.

Étapes

1. En haut de Cloud Manager, cliquez sur **Monitoring**.
2. Cliquez sur le lien **Cloud Insights**.



Résultat

Cloud Insights s'ouvre dans un nouvel onglet du navigateur. Si vous avez besoin d'aide, reportez-vous au "Documentation Cloud Insights".

Désactivation de la surveillance

Si vous ne souhaitez plus surveiller Cloud Volumes ONTAP, vous pouvez désactiver le service à tout moment.

> Si vous désactivez la surveillance de chacun de vos environnements de travail, vous devrez supprimer vous-même l'instance EC2. L'instance s'appelle *AcquisitionUnit* avec un hachage (UUID) généré concaténé. Par exemple : *AcquisitionUnit-FAN7FqeH*

Étapes

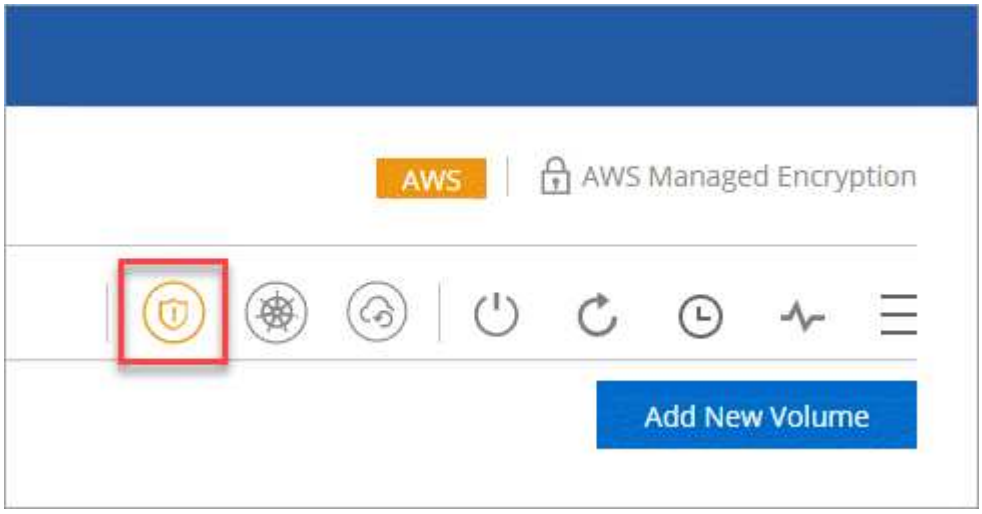
1. En haut de Cloud Manager, cliquez sur **environnements de travail**.
2. Sélectionnez un environnement de travail.
3. Dans le volet de droite, cliquez sur Et sélectionnez **Désactiver l'acquisition**.

Renforcer la protection contre les attaques par ransomware

Les attaques par ransomware peuvent coûter du temps, des ressources et de la réputation à l'entreprise. Cloud Manager vous permet d'implémenter la solution NetApp contre les attaques par ransomware qui fournit des outils efficaces pour la visibilité, la détection et la résolution de problèmes.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône **ransomware**.

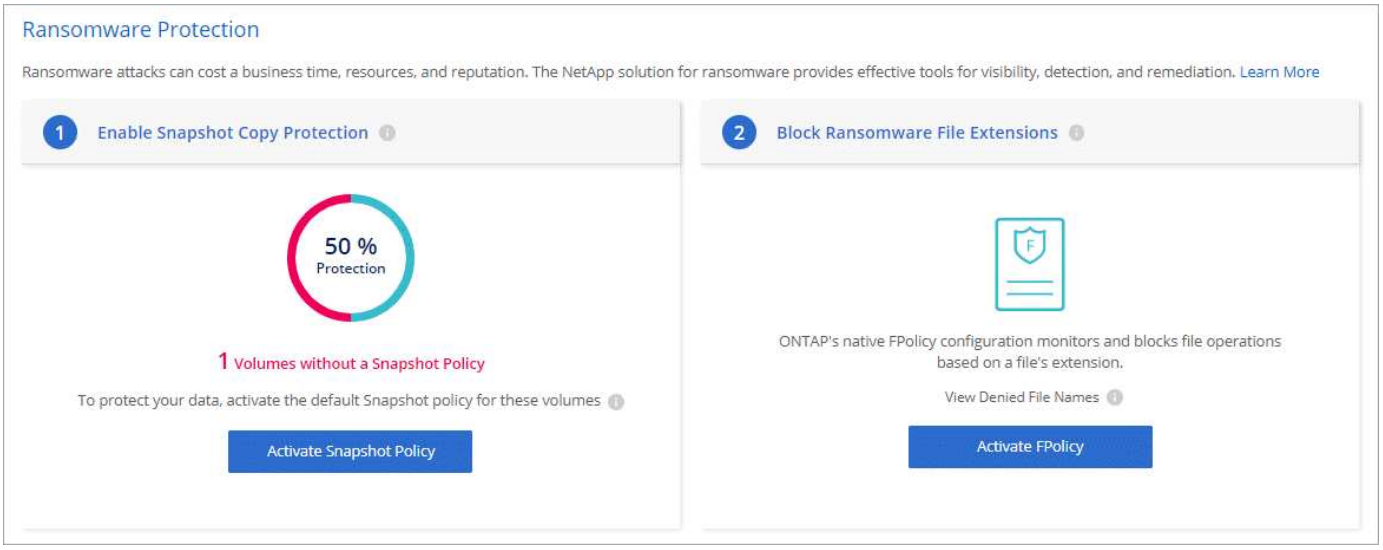


2. Implémentez la solution NetApp en cas d'attaque par ransomware :
   a. Cliquez sur **Activer la stratégie de snapshot**, si des volumes n'ont pas de règle de snapshot activée.

      La technologie Snapshot de NetApp offre la meilleure solution du secteur pour résoudre les problèmes liés aux attaques par ransomware. Le mieux pour réussir la récupération est d'effectuer une restauration à partir de sauvegardes non infectées. Les copies Snapshot sont en lecture seule, ce qui empêche la corruption par ransomware. Ils peuvent également assurer la granularité pour créer des images d'une copie de fichiers unique ou d'une solution complète de reprise après incident.

   b. Cliquez sur **Activer FPolicy** pour activer la solution FPolicy d'ONTAP, qui peut bloquer les opérations de fichiers en fonction de l'extension d'un fichier.

      Cette solution préventive améliore la protection contre les attaques par ransomware en bloquant les types de fichiers généralement utilisés.



Administration

Enregistrement des systèmes de paiement à l'utilisation

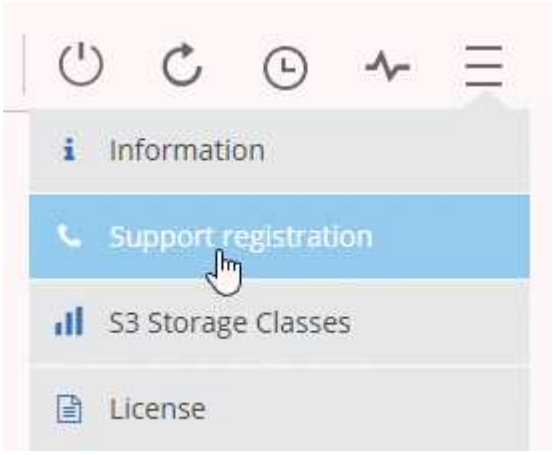
Le support de NetApp est inclus avec les systèmes Cloud Volumes ONTAP Explore, Standard et Premium, mais vous devez au préalable activer le support en enregistrant les systèmes à NetApp.

Étapes

1. Si vous n'avez pas encore ajouté votre compte du site de support NetApp à Cloud Manager, accédez à **Paramètres de compte** et ajoutez-le maintenant.

   "Découvrez comment ajouter des comptes au site de support NetApp".

2. Sur la page Working Environments, double-cliquez sur le nom du système que vous souhaitez enregistrer.
3. Cliquez sur l'icône du menu, puis sur **support Registration** :



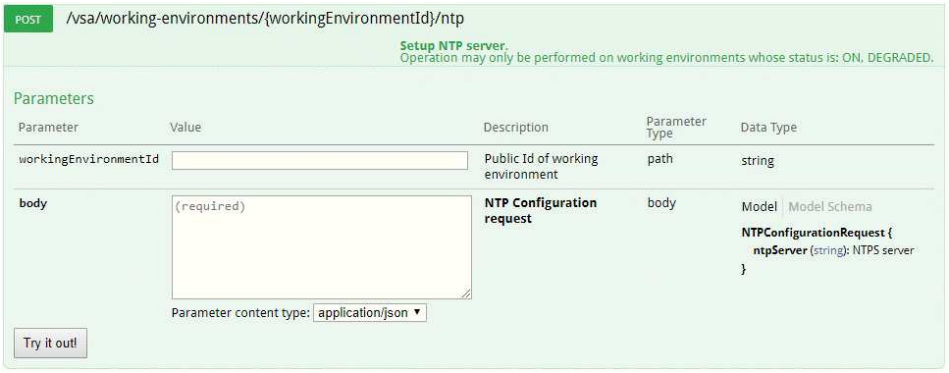
4. Sélectionnez un compte sur le site de support NetApp et cliquez sur **Register**.

Résultat

Cloud Manager enregistre le système avec NetApp.

Configuration de Cloud Volumes ONTAP

Après avoir déployé Cloud Volumes ONTAP, vous pouvez le configurer en synchronisant l'heure du système à l'aide de NTP et en effectuant quelques tâches facultatives à partir de System Manager ou de l'interface de ligne de commande.

Tâche	Description
Synchronisez l'heure du système à l'aide du protocole NTP	La spécification d'un serveur NTP synchronise l'heure entre les systèmes de votre réseau, ce qui peut aider à éviter les problèmes dus aux différences de temps. Spécifiez un serveur NTP via l'API Cloud Manager ou depuis l'interface utilisateur lors de la configuration d'un serveur CIFS. • "Modification du serveur CIFS" • "Guide du développeur de l'API Cloud Manager" Par exemple, voici l'API d'un système à un seul nœud dans AWS : 
Facultatif : configuration d'AutoSupport	AutoSupport surveille de manière proactive l'état de votre système et envoie automatiquement des messages au support technique NetApp par défaut. Si l'administrateur de comptes a ajouté un serveur proxy à Cloud Manager avant de lancer votre instance, Cloud Volumes ONTAP est configuré pour utiliser ce serveur proxy pour les messages AutoSupport. Vous devez tester AutoSupport pour vous assurer qu'il peut envoyer des messages. Pour obtenir ces instructions, consultez l'aide de System Manager ou le "Référence de l'administration du système ONTAP 9".
Facultatif : configurez Cloud Manager en tant que proxy AutoSupport	Si votre environnement requiert un serveur proxy pour envoyer des messages AutoSupport, vous pouvez configurer Cloud Manager pour qu'il fonctionne comme proxy. Aucune configuration de Cloud Manager n'est requise, autre que l'accès Internet. Il vous suffit de accéder à l'interface de ligne de commandes pour Cloud Volumes ONTAP et d'exécuter la commande suivante : `system node autosupport modify -proxy-url <cloud-manager-ip-address>`

Tâche	Description
En option : Configurer EMS	Le système de gestion des événements (EMS) collecte et affiche des informations sur les événements qui se produisent sur les systèmes Cloud Volumes ONTAP. Pour recevoir des notifications d'événements, vous pouvez définir des destinations d'événements (adresses e-mail, hôtes de trap SNMP ou serveurs syslog) et des routes d'événements pour un événement particulier. Vous pouvez configurer EMS à l'aide de l'interface de ligne de commande. Pour obtenir des instructions, reportez-vous au "Guide de configuration rapide de ONTAP 9 EMS".
Facultatif : créez une interface réseau de gestion SVM (LIF) pour les systèmes HA dans plusieurs zones de disponibilité AWS	Une interface de réseau de gestion de machine virtuelle de stockage (LIF) est requise si vous souhaitez utiliser SnapCenter ou SnapDrive pour Windows avec une paire haute disponibilité. La LIF de gestion du SVM doit utiliser une adresse IP *flottante* lors de l'utilisation d'une paire HA sur plusieurs zones de disponibilité AWS. Cloud Manager vous invite à spécifier l'adresse IP flottante lors du lancement de la paire HA. Si vous n'avez pas spécifié l'adresse IP, vous pouvez créer le LIF de gestion SVM vous-même à partir de System Manager ou de l'interface de ligne de commande. L'exemple suivant montre comment créer le LIF à partir de l'interface de ligne de commande : `network interface create -vserver svm_cloud -lif svm_mgmt -role data -data-protocol none -home-node cloud-01 -home-port e0a -address 10.0.2.126 -netmask 255.255.255.0 -status-admin up -firewall -policy mgmt`
Facultatif : modifiez l'emplacement de sauvegarde des fichiers de configuration	Cloud Volumes ONTAP crée automatiquement des fichiers de sauvegarde de la configuration qui contiennent des informations sur les options configurables dont il a besoin pour fonctionner correctement. Par défaut, Cloud Volumes ONTAP sauvegarde les fichiers sur l'hôte Connector toutes les huit heures. Si vous souhaitez envoyer les sauvegardes à un autre emplacement, vous pouvez modifier l'emplacement vers un serveur FTP ou HTTP dans votre data center ou dans AWS. Par exemple, vous pouvez déjà disposer d'un emplacement de sauvegarde pour vos systèmes de stockage FAS. Vous pouvez modifier l'emplacement de sauvegarde à l'aide de l'interface de ligne de commande. Voir la "Référence de l'administration du système ONTAP 9".

Gestion des licences BYOL pour Cloud Volumes ONTAP

Ajoutez une licence système BYOL Cloud Volumes ONTAP pour ajouter de la capacité, mettre à jour une licence système existante et gérer les licences BYOL pour la sauvegarde dans le cloud.

Gestion des licences système

Vous pouvez acheter plusieurs licences pour un système Cloud Volumes ONTAP BYOL pour allouer plus de 368 To de capacité. Par exemple, vous pouvez acheter deux licences pour allouer une capacité allant jusqu'à

736 To à Cloud Volumes ONTAP. Vous pouvez également acheter quatre licences pour obtenir jusqu'à 1.4 po.

Le nombre de licences que vous pouvez acheter pour un système à un seul nœud ou une paire HA est illimité.

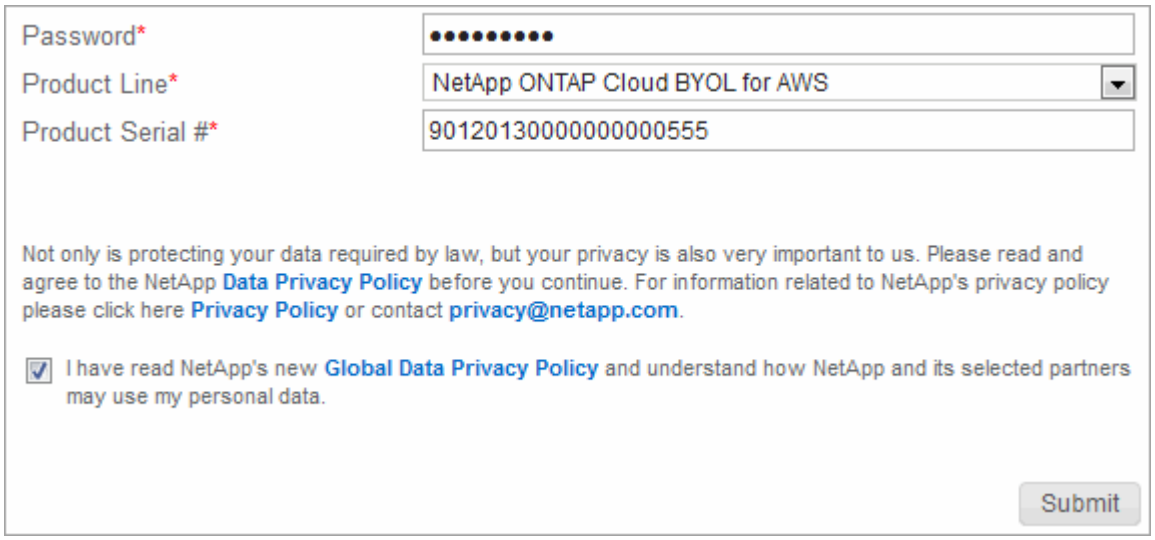
Obtention d'un fichier de licence système

Dans la plupart des cas, Cloud Manager peut obtenir automatiquement votre fichier de licence en utilisant votre compte sur le site de support NetApp. Si ce n'est pas le cas, vous devrez charger manuellement le fichier de licence. Si vous n'avez pas le fichier de licence, vous pouvez l'obtenir sur netapp.com.

Étapes

1. Accédez au "Générateur de fichiers de licences NetApp" Et connectez-vous en utilisant vos identifiants du site du support NetApp.
2. Entrez votre mot de passe, choisissez votre produit, entrez le numéro de série, confirmez que vous avez lu et accepté la politique de confidentialité, puis cliquez sur **Envoyer**.

   Exemple



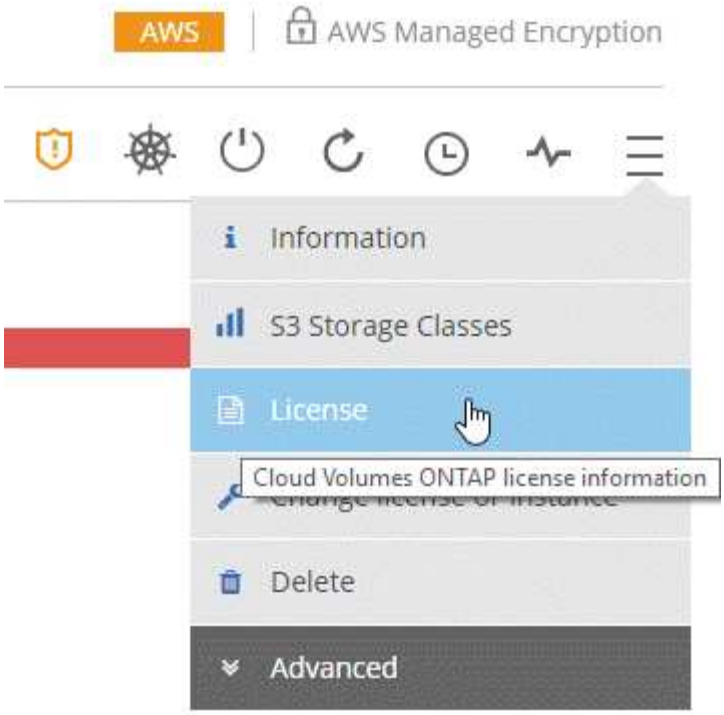
3. Choisissez si vous souhaitez recevoir le fichier numéro de série.NLF JSON par e-mail ou par téléchargement direct.

Ajout d'une nouvelle licence système

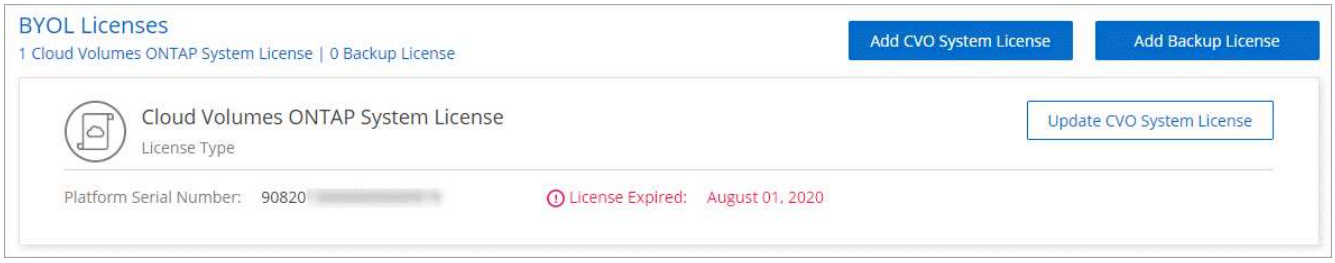
Ajoutez une nouvelle licence système BYOL à tout moment pour allouer une capacité supplémentaire de 368 To à votre système Cloud Volumes ONTAP BYOL.

Étapes

1. Dans Cloud Manager, ouvrez l'environnement de travail Cloud Volumes ONTAP BYOL.
2. Cliquez sur l'icône du menu, puis sur **Licence**.



3. Cliquez sur **Ajouter la licence système CVO**.



4. Indiquez le numéro de série ou téléchargez le fichier de licence.
5. Cliquez sur **Ajouter une licence**.

Résultat

Cloud Manager installe le nouveau fichier de licence sur le système Cloud Volumes ONTAP.

Mise à jour d'une licence système

Lorsque vous renouvelez un abonnement BYOL en contactant un représentant NetApp, Cloud Manager obtient automatiquement la nouvelle licence auprès de NetApp et l'installe sur le système Cloud Volumes ONTAP.

Si Cloud Manager ne peut pas accéder au fichier de licence via la connexion Internet sécurisée, vous pouvez obtenir le fichier vous-même, puis le charger manuellement dans Cloud Manager.

Étapes

1. Dans Cloud Manager, ouvrez l'environnement de travail Cloud Volumes ONTAP BYOL.
2. Cliquez sur l'icône du menu, puis sur **Licence**.
3. Cliquez sur **mettre à jour la licence système CVO**.

4. Cliquez sur **Télécharger le fichier** et sélectionnez le fichier de licence.
5. Cliquez sur **mettre à jour la licence**.

Résultat

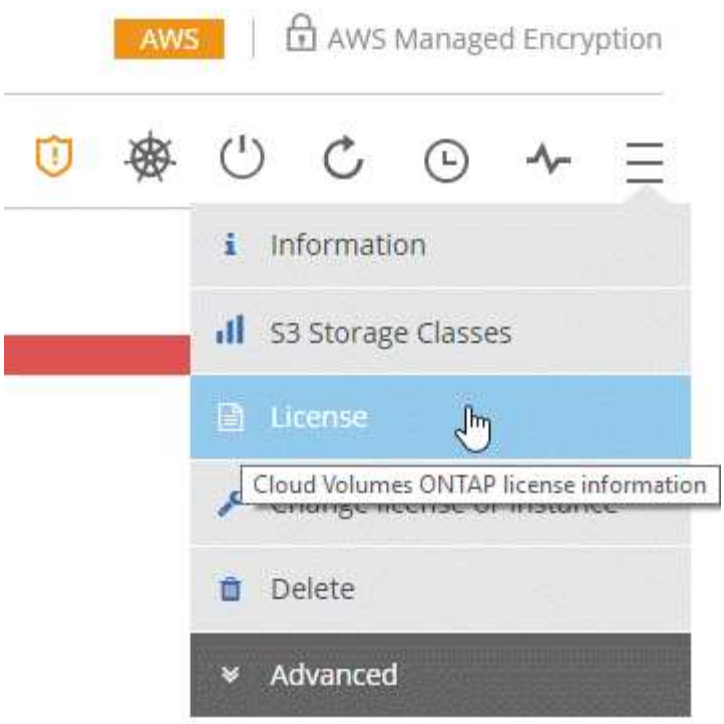
Cloud Manager met à jour la licence sur le système Cloud Volumes ONTAP.

Ajout et mise à jour de votre licence Backup BYOL

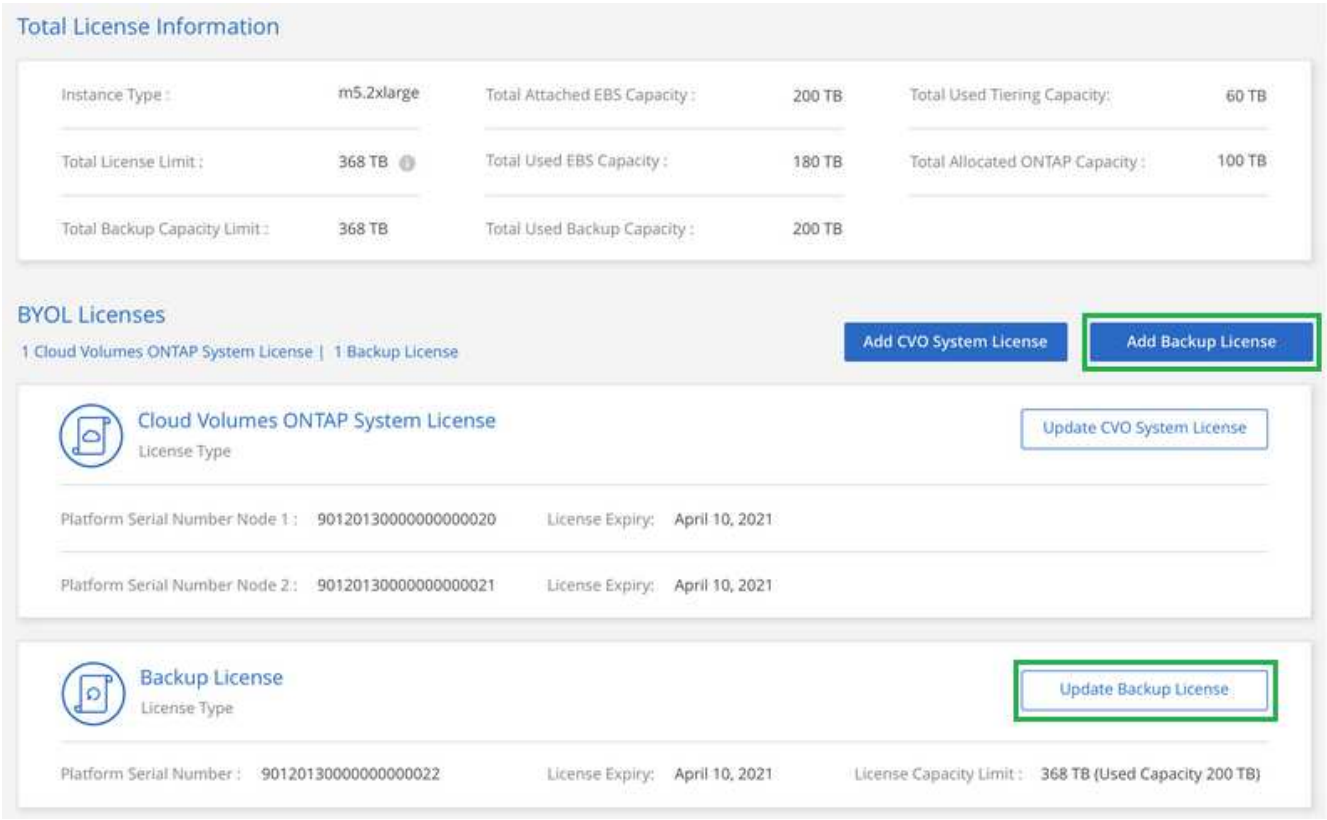
La page des licences BYOL permet d'ajouter ou de mettre à jour votre licence Backup BYOL.

Étapes

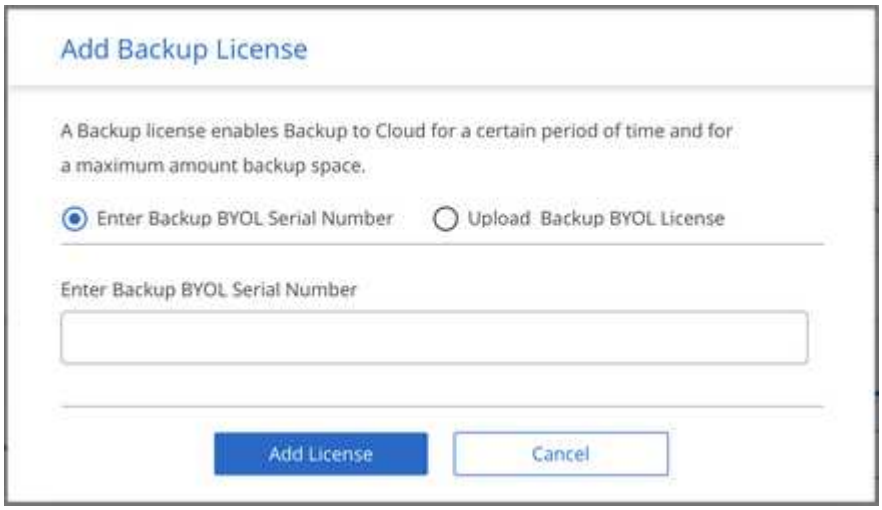
1. Dans Cloud Manager, ouvrez l'environnement de travail Cloud Volumes ONTAP BYOL.
2. Cliquez sur l'icône du menu, puis sur **Licence**.



3. Cliquez sur **Ajouter une licence de sauvegarde** ou **mettre à jour la licence de sauvegarde** selon que vous ajoutez une nouvelle licence ou mettez à jour une licence existante.



4. Entrez les informations de licence et cliquez sur **Ajouter une licence** :
   - Si vous disposez du numéro de série, sélectionnez l'option **entrer le numéro de série BYOL** et entrez le numéro de série.
   - Si vous disposez du fichier de licence de sauvegarde, sélectionnez l'option **Télécharger la licence BYOL** de sauvegarde et suivez les invites pour joindre le fichier.



Résultat

Cloud Manager ajoute ou met à jour la licence pour que votre service Backup vers Cloud soit actif.

Mise à jour du logiciel Cloud Volumes ONTAP

Cloud Manager inclut plusieurs options que vous pouvez utiliser pour mettre à niveau

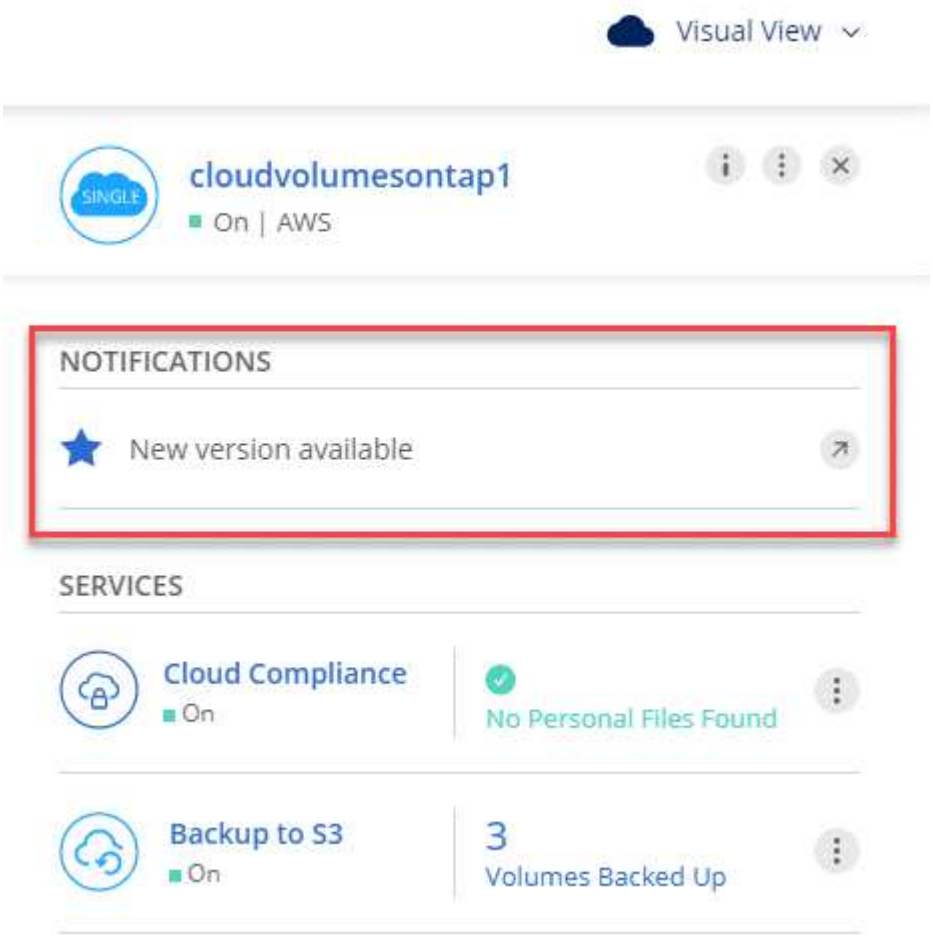
vers la version actuelle de Cloud Volumes ONTAP ou pour mettre à niveau Cloud Volumes ONTAP vers une version antérieure. Vous devez préparer les systèmes Cloud Volumes ONTAP avant de mettre à niveau ou de mettre à niveau le logiciel.

Les mises à jour logicielles doivent être effectuées par Cloud Manager

La mise à niveau d'Cloud Volumes ONTAP doit être effectuée depuis Cloud Manager. Vous ne devez pas mettre à niveau Cloud Volumes ONTAP à l'aide de System Manager ou de l'interface de ligne de commandes. Cela peut affecter la stabilité du système.

Méthodes de mise à jour de Cloud Volumes ONTAP

Cloud Manager affiche une notification dans les environnements de travail Cloud Volumes ONTAP lorsqu'une nouvelle version de Cloud Volumes ONTAP est disponible :



Vous pouvez lancer le processus de mise à niveau à partir de cette notification, qui automatise le processus en obtenant l'image logicielle à partir d'un compartiment S3, en installant l'image, puis en redémarrant le système. Pour plus de détails, voir Mise à niveau d'Cloud Volumes ONTAP à partir des notifications Cloud Manager.

Pour les systèmes HA dans AWS, Cloud Manager peut mettre à niveau le médiateur HA dans le cadre du processus de mise à niveau.

Options avancées pour les mises à jour logicielles

Cloud Manager propose également les options avancées suivantes pour la mise à jour du logiciel Cloud Volumes ONTAP :

- Mises à jour logicielles à l'aide d'une image sur une URL externe

  Cette option est utile si Cloud Manager ne peut pas accéder à la rubrique S3 pour mettre à niveau le logiciel, si un correctif vous a été fourni, ou si vous souhaitez rétrograder le logiciel vers une version spécifique.

  Pour plus de détails, voir Mise à niveau ou mise à niveau vers une version antérieure de Cloud Volumes ONTAP à l'aide d'un serveur HTTP ou FTP.

- Mises à jour logicielles à l'aide de l'autre image du système

  Vous pouvez utiliser cette option pour revenir à la version précédente en faisant de l'image logicielle alternative l'image par défaut. Cette option n'est pas disponible pour les paires HA.

  Pour plus de détails, voir Déclassement de Cloud Volumes ONTAP à l'aide d'une image locale.

Préparation de la mise à jour du logiciel Cloud Volumes ONTAP

Avant d'effectuer une mise à niveau ou une mise à niveau vers une version antérieure, vous devez vérifier que vos systèmes sont prêts et apporter les modifications de configuration requises.

- Planifier des temps d'indisponibilité
- Révision des exigences de version
- Vérifier que le rétablissement automatique est toujours activé
- Suspension des transferts SnapMirror
- Vérifier que les agrégats sont en ligne

Planifier des temps d'indisponibilité

Lorsque vous mettez à niveau un système à un seul nœud, le processus de mise à niveau met le système hors ligne pendant 25 minutes au cours desquelles les E/S sont interrompues.

La mise à niveau d'une paire haute disponibilité s'effectue sans interruption et les E/S sont continues. Au cours de ce processus de mise à niveau sans interruption, chaque nœud est mis à niveau en tandem afin de continuer à traiter les E/S aux clients.

Révision des exigences de version

La version de ONTAP que vous pouvez mettre à niveau ou rétrograder varie en fonction de la version de ONTAP actuellement exécutée sur votre système.

Pour comprendre les exigences de version, reportez-vous à la section "Documentation ONTAP 9 : configuration requise pour la mise à jour du cluster".

Vérifier que le rétablissement automatique est toujours activé

Le rétablissement automatique doit être activé sur une paire Cloud Volumes ONTAP HA (paramètre par défaut). Si ce n'est pas le cas, l'opération échouera.

"Documentation ONTAP 9 : commandes pour la configuration du rétablissement automatique"

Suspension des transferts SnapMirror

Si un système Cloud Volumes ONTAP a des relations SnapMirror actives, il est préférable de suspendre les transferts avant de mettre à jour le logiciel Cloud Volumes ONTAP. La suspension des transferts empêche les défaillances de SnapMirror. Vous devez suspendre les transferts depuis le système de destination.

Description de la tâche

Ces étapes décrivent l'utilisation de System Manager pour la version 9.3 et ultérieure.

Étapes

1. "Connectez-vous à System Manager" à partir du système de destination.
2. Cliquez sur **protection > relations**.
3. Sélectionnez la relation et cliquez sur **opérations > Quiesce**.

Vérifier que les agrégats sont en ligne

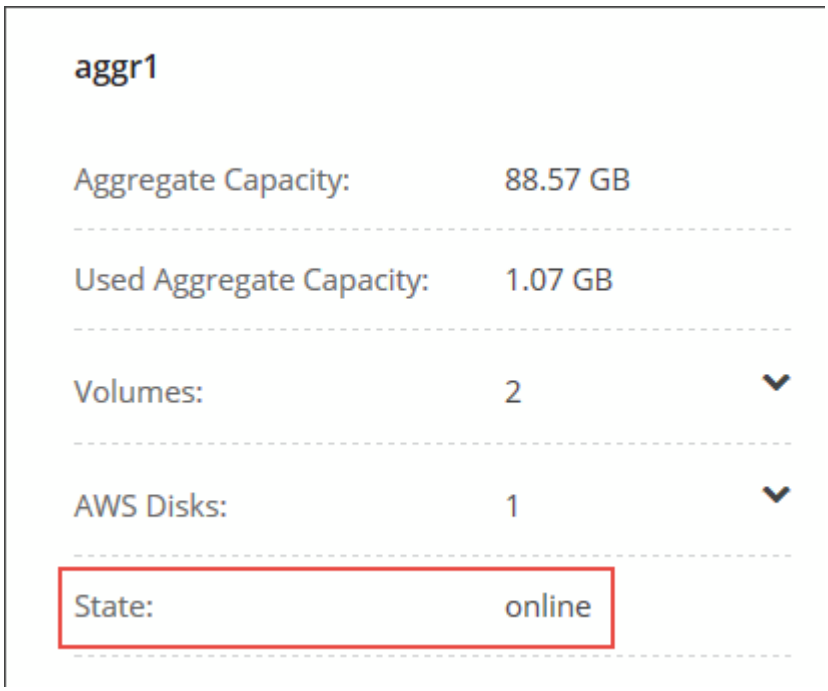
Les agrégats pour Cloud Volumes ONTAP doivent être en ligne avant de mettre à jour le logiciel. Les agrégats doivent être en ligne dans la plupart des configurations, mais si ce n'est pas le cas, vous devez les mettre en ligne.

Description de la tâche

Ces étapes décrivent l'utilisation de System Manager pour la version 9.3 et ultérieure.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > allocation avancée**.
2. Sélectionnez un agrégat, cliquez sur **Info**, puis vérifiez que l'état est en ligne.



3. Si l'agrégat est hors ligne, utilisez System Manager pour mettre l'agrégat en ligne :
   a. "Connectez-vous à System Manager".

b. Cliquez sur **stockage > agrégats et disques > agrégats**.

c. Sélectionnez l'agrégat, puis cliquez sur **plus d'actions > État > en ligne**.

Mise à niveau d'Cloud Volumes ONTAP à partir des notifications Cloud Manager

Cloud Manager vous avertit lorsqu'une nouvelle version d'Cloud Volumes ONTAP est disponible. Cliquez sur la notification pour lancer le processus de mise à niveau.

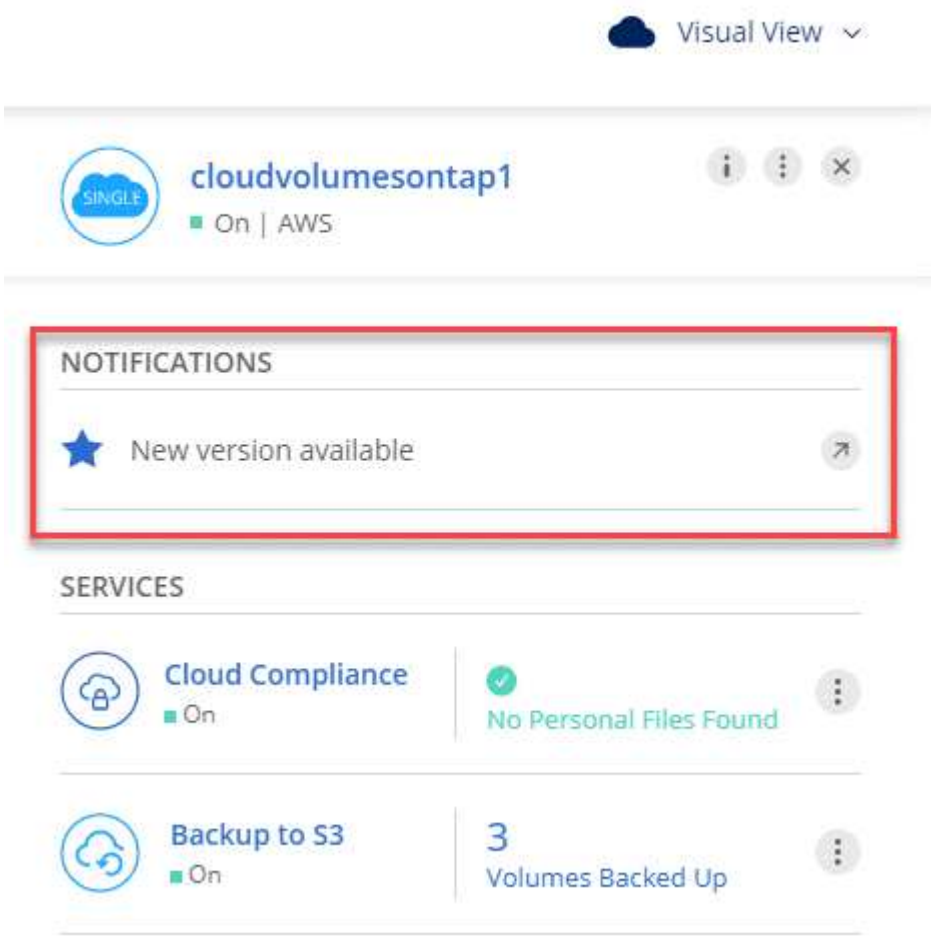
Avant de commencer

Les opérations de Cloud Manager telles que la création de volumes ou d'agrégats ne doivent pas être en cours pour le système Cloud Volumes ONTAP.

Étapes

1. Cliquez sur **environnements de travail**.
2. Sélectionnez un environnement de travail.

   Une notification s'affiche dans le volet droit si une nouvelle version est disponible :



3. Si une nouvelle version est disponible, cliquez sur **Upgrade**.
4. Dans la page informations sur la version, cliquez sur le lien pour lire les notes de version de la version spécifiée, puis cochez la case **J'ai lu…**.

5. Dans la page du contrat de licence utilisateur final (CLUF), lisez le CLUF, puis sélectionnez **J'ai lu et approuvé le CLUF**.
6. Dans la page Revue et approbation, lisez les notes importantes, sélectionnez **Je comprends…**, puis cliquez sur **Go**.

Résultat

Cloud Manager démarre la mise à niveau logicielle. Vous pouvez effectuer des actions sur l'environnement de travail une fois la mise à jour logicielle terminée.

Une fois que vous avez terminé

Si vous avez suspendu les transferts SnapMirror, utilisez System Manager pour reprendre les transferts.

Mise à niveau ou mise à niveau vers une version antérieure de Cloud Volumes ONTAP à l'aide d'un serveur HTTP ou FTP

Vous pouvez placer l'image du logiciel Cloud Volumes ONTAP sur un serveur HTTP ou FTP, puis lancer la mise à jour du logiciel à partir de Cloud Manager. Vous pouvez utiliser cette option si Cloud Manager ne peut pas accéder à la rubrique S3 pour mettre à niveau le logiciel ou si vous souhaitez mettre à niveau le logiciel.

Étapes

1. Configurez un serveur HTTP ou FTP pouvant héberger l'image du logiciel Cloud Volumes ONTAP.
2. Si vous disposez d'une connexion VPN au réseau virtuel, vous pouvez placer l'image logicielle Cloud Volumes ONTAP sur un serveur HTTP ou un serveur FTP de votre propre réseau. Sinon, vous devez placer le fichier sur un serveur HTTP ou FTP dans le cloud.
3. Si vous utilisez votre propre groupe de sécurité pour Cloud Volumes ONTAP, assurez-vous que les règles de sortie autorisent les connexions HTTP ou FTP pour que Cloud Volumes ONTAP puisse accéder à l'image logicielle.

   Le groupe de sécurité Cloud Volumes ONTAP prédéfini autorise les connexions HTTP et FTP sortantes par défaut.

4. Obtenez l'image logicielle de "Le site de support NetApp".
5. Copiez l'image du logiciel dans le répertoire du serveur HTTP ou FTP à partir duquel le fichier sera servi.
6. Dans l'environnement de travail de Cloud Manager, cliquez sur l'icône de menu, puis sur **Avancé > mettre à jour Cloud Volumes ONTAP**.
7. Sur la page de mise à jour du logiciel, choisissez **sélectionnez une image disponible à partir d'une URL**, saisissez l'URL, puis cliquez sur **Modifier l'image**.
8. Cliquez sur **Continuer** pour confirmer.

Résultat

Cloud Manager démarre la mise à jour logicielle. Vous pouvez effectuer des actions sur l'environnement de travail une fois la mise à jour logicielle terminée.

Une fois que vous avez terminé

Si vous avez suspendu les transferts SnapMirror, utilisez System Manager pour reprendre les transferts.

Déclassement de Cloud Volumes ONTAP à l'aide d'une image locale

Le passage de Cloud Volumes ONTAP à une version antérieure dans la même famille de versions (par exemple, 9.5 à 9.4) est appelé une version antérieure. Vous pouvez rétrograder sans assistance lors de la

rétrogradation de clusters nouveaux ou de tests, mais vous devez contacter le support technique si vous souhaitez rétrograder un cluster de production.

Chaque système Cloud Volumes ONTAP peut contenir deux images logicielles : l'image en cours d'exécution et une autre image que vous pouvez démarrer. Cloud Manager peut modifier l'image alternative comme image par défaut. Vous pouvez utiliser cette option pour revenir à la version précédente de Cloud Volumes ONTAP, si vous rencontrez des problèmes avec l'image actuelle.

Description de la tâche

Ce processus de mise à niveau vers une version antérieure est uniquement disponible pour les systèmes Cloud Volumes ONTAP. Il n'est pas disponible pour les paires HA.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > mettre à jour Cloud Volumes ONTAP**.
2. Sur la page mise à jour du logiciel, sélectionnez l'image de remplacement, puis cliquez sur **changer l'image**.
3. Cliquez sur **Continuer** pour confirmer.

Résultat

Cloud Manager démarre la mise à jour logicielle. Vous pouvez effectuer des actions sur l'environnement de travail une fois la mise à jour logicielle terminée.

Une fois que vous avez terminé

Si vous avez suspendu les transferts SnapMirror, utilisez System Manager pour reprendre les transferts.

Modification des systèmes Cloud Volumes ONTAP

Il peut être nécessaire de modifier la configuration des systèmes Cloud Volumes ONTAP au fur et à mesure de l'évolution de vos besoins de stockage. Vous pouvez, par exemple, choisir entre les configurations de paiement à l'utilisation, modifier le type d'instance ou d'ordinateur virtuel, et bien plus encore.

Modification de l'instance ou du type de machine pour Cloud Volumes ONTAP

Vous pouvez choisir parmi plusieurs types d'instances ou de machines lors du lancement d'Cloud Volumes ONTAP dans AWS, Azure ou GCP. Vous pouvez modifier l'instance ou le type de machine à tout moment si vous déterminez qu'elle est sous-dimensionnée ou surdimensionnée en fonction de vos besoins.

Description de la tâche

- Le rétablissement automatique doit être activé sur une paire Cloud Volumes ONTAP HA (paramètre par défaut). Si ce n'est pas le cas, l'opération échouera.

  "Documentation ONTAP 9 : commandes pour la configuration du rétablissement automatique"

- La modification de l'instance ou du type de machine affecte les frais de service du fournisseur cloud.
- L'opération redémarre Cloud Volumes ONTAP.

  Pour les systèmes à nœud unique, les E/S sont interrompues.

  Pour les paires HA, le changement n'est pas perturbateur. Les paires HA continuent de servir les données.

Cloud Manager modifie aisément un nœud à la fois en lançant le basculement et en attendant les frais de retour. L'équipe d'assurance qualité de NetApp a testé l'écriture et la lecture des fichiers pendant ce processus et n'a rencontré aucun problème côté client. Au fur et à mesure des changements de connexion, nous avons constaté des tentatives d'E/S au niveau des E/S, mais la couche applicative a pu faire face à ces courtes « connexions » NFS/CIFS.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **changer la licence ou l'instance** pour AWS, **changer la licence ou VM** pour Azure ou **changer la licence ou la machine** pour GCP.
2. Si vous utilisez une configuration payante, vous pouvez choisir une licence différente.
3. Sélectionnez une instance ou un type de machine, cochez la case pour confirmer que vous comprenez les implications du changement, puis cliquez sur **OK**.

Résultat

Cloud Volumes ONTAP redémarre avec la nouvelle configuration.

Changement entre les configurations de paiement à la demande

Une fois que vous avez lancé les systèmes Cloud Volumes ONTAP à la demande, vous pouvez modifier les configurations Explorer, Standard et Premium à tout moment en modifiant la licence. La modification de la licence augmente ou réduit la limite de capacité brute et vous permet de choisir entre différents types d'instances AWS ou de machines virtuelles Azure.

Dans GCP, un seul type de machine est disponible pour chaque configuration avec paiement à l'utilisation. Vous ne pouvez pas choisir entre différents types de machine.

Description de la tâche

Notez ce qui suit au sujet de la modification entre les licences de paiement à la demande :

- L'opération redémarre Cloud Volumes ONTAP.

  Pour les systèmes à nœud unique, les E/S sont interrompues.

  Pour les paires HA, le changement n'est pas perturbateur. Les paires HA continuent de servir les données.

- La modification de l'instance ou du type de machine affecte les frais de service du fournisseur cloud.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **changer la licence ou l'instance** pour AWS, **changer la licence ou VM** pour Azure ou **changer la licence ou la machine** pour GCP.
2. Sélectionnez un type de licence et un type d'instance ou de machine, cochez la case pour confirmer que vous comprenez les implications du changement, puis cliquez sur **OK**.

Résultat

Cloud Volumes ONTAP redémarre avec la nouvelle licence, le type d'instance, le type de machine ou les deux.

Passage à une autre configuration Cloud Volumes ONTAP

Si vous souhaitez basculer entre un abonnement avec paiement à l'utilisation et un abonnement BYOL, ou entre un système Cloud Volumes ONTAP unique et une paire haute disponibilité, vous devez déployer un

nouveau système avant de répliquer les données depuis le système existant vers le nouveau système.

Étapes

1. Créez un nouvel environnement de travail Cloud Volumes ONTAP.

   "Lancement d'Cloud Volumes ONTAP dans AWS"
   "Lancement d'Cloud Volumes ONTAP dans Azure"
   "Lancement d'Cloud Volumes ONTAP dans GCP"

2. "Configuration de la réplication des données unique" entre les systèmes pour chaque volume que vous devez répliquer.
3. Terminez le système Cloud Volumes ONTAP dont vous n'avez plus besoin par "suppression de l'environnement de travail d'origine".

Modification de la vitesse d'écriture sur normale ou élevée

Cloud Manager permet de choisir un paramètre de vitesse d'écriture pour les systèmes Cloud Volumes ONTAP à un seul nœud. La vitesse d'écriture par défaut est normale. Vous pouvez passer à une vitesse d'écriture élevée si vos workloads nécessitent des performances d'écriture rapides. Avant de modifier la vitesse d'écriture, vous devez "comprendre les différences entre les réglages normaux et élevés".

Description de la tâche

- Assurez-vous que les opérations telles que la création de volume ou d'agrégat ne sont pas en cours.
- Notez que cette modification redémarre Cloud Volumes ONTAP, ce qui signifie que les E/S sont interrompues.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > vitesse d'écriture**.
2. Sélectionnez **Normal** ou **Haut**.

   Si vous choisissez Haut, vous devrez lire l'énoncé « Je comprends… » et confirmer en cochant la case.

3. Cliquez sur **Enregistrer**, vérifiez le message de confirmation, puis cliquez sur **Continuer**.

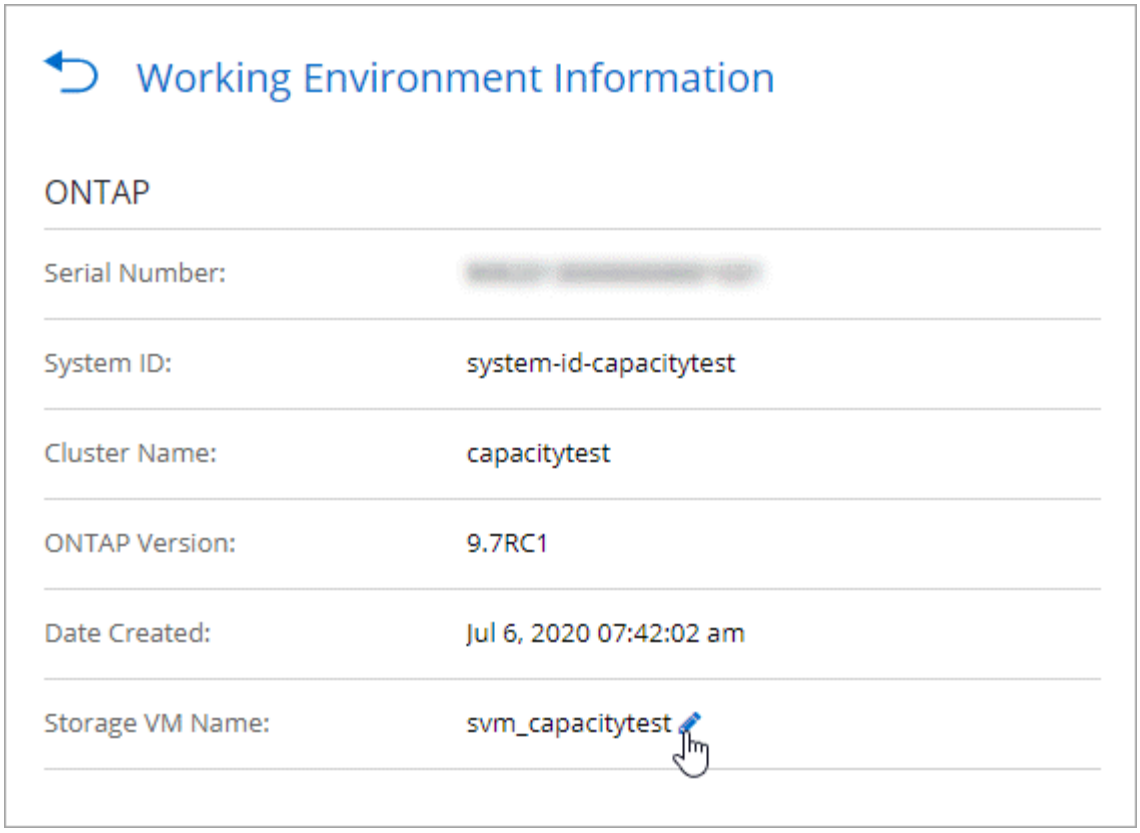
Modification du nom de la machine virtuelle de stockage

Cloud Manager nomme automatiquement la machine virtuelle de stockage (SVM) créée pour Cloud Volumes ONTAP. Vous pouvez modifier le nom du SVM si vous disposez de normes strictes en matière de nommage. Par exemple, vous pouvez indiquer le nom des SVM dans vos clusters ONTAP.

Mais si vous avez créé des SVM supplémentaires pour Cloud Volumes ONTAP, vous ne pouvez pas renommer les SVM de Cloud Manager. Pour ce faire, vous devez utiliser System Manager ou l'interface de ligne de commandes directement dans Cloud Volumes ONTAP.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **informations**.
2. Cliquez sur l'icône d'édition située à droite du nom de la VM de stockage.



3. Dans la boîte de dialogue Modifier le nom du SVM, modifiez le nom, puis cliquez sur **Enregistrer**.

Modification du mot de passe de Cloud Volumes ONTAP

Cloud Volumes ONTAP inclut un compte d'administration de cluster. Si nécessaire, vous pouvez modifier le mot de passe de ce compte à partir de Cloud Manager.

> Vous ne devez pas modifier le mot de passe du compte admin via System Manager ou l'interface de ligne de commande. Le mot de passe ne sera pas pris en compte dans Cloud Manager. Par conséquent, Cloud Manager ne peut pas contrôler l'instance correctement.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > définir mot de passe**.
2. Saisissez le nouveau mot de passe deux fois, puis cliquez sur **Enregistrer**.

   Le nouveau mot de passe doit être différent de l'un des six derniers mots de passe utilisés.

Modification de la MTU réseau pour les instances c4.4xlarge et c4.8xlarge

Par défaut, Cloud Volumes ONTAP est configuré pour utiliser 9 000 MTU (également appelés trames Jumbo) lorsque vous choisissez l'instance c4.4xlarge ou l'instance c4.8xlarge dans AWS. Vous pouvez modifier la MTU réseau à 1 500 octets si cela est plus approprié pour votre configuration réseau.

Description de la tâche

Une unité de transmission réseau maximale (MTU) de 9 000 octets peut fournir le débit réseau maximal le plus élevé possible pour des configurations spécifiques.

9 000 MTU sont un bon choix si les clients du même VPC communiquent avec le système Cloud Volumes

ONTAP et que certains ou tous ces clients prennent également en charge 9 000 MTU. Si le trafic quitte le VPC, la fragmentation des paquets peut se produire, ce qui dégrade les performances.

Un MTU réseau de 1 500 octets est un bon choix si les clients ou les systèmes extérieurs au VPC communiquent avec le système Cloud Volumes ONTAP.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > utilisation du réseau**.
2. Sélectionnez **Standard** ou **Jumbo Frames**.
3. Cliquez sur **Modifier**.

Modification des tables de routage associées aux paires HA dans plusieurs AZS d'AWS

Vous pouvez modifier les tables de routage AWS incluant des routes vers les adresses IP flottantes pour une paire haute disponibilité. Vous pouvez le faire si les nouveaux clients NFS ou CIFS ont besoin d'accéder à une paire haute disponibilité dans AWS.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **informations**.
2. Cliquez sur **tables de routage**.
3. Modifiez la liste des tables de routage sélectionnées, puis cliquez sur **Enregistrer**.

Résultat

Cloud Manager envoie une requête AWS pour modifier les tables de routage.

Gestion de l'état du Cloud Volumes ONTAP

Vous pouvez arrêter et lancer Cloud Volumes ONTAP depuis Cloud Manager pour gérer les coûts de calcul du cloud.

Planification des arrêts automatiques de Cloud Volumes ONTAP

Vous pouvez arrêter Cloud Volumes ONTAP à des intervalles réguliers afin de réduire les coûts de calcul. Au lieu de le faire manuellement, vous pouvez configurer Cloud Manager de sorte qu'il s'arrête automatiquement, puis redémarre les systèmes à des moments spécifiques.

Description de la tâche

Lorsque vous planifiez un arrêt automatique de votre système Cloud Volumes ONTAP, Cloud Manager reporte l'arrêt du système si un transfert de données actif est en cours. Cloud Manager arrête le système une fois le transfert terminé.

Cette tâche planifie les arrêts automatiques des deux nœuds d'une paire haute disponibilité.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône horloge :

2. Spécifiez la planification de l'arrêt :

a. Choisissez si vous souhaitez arrêter le système tous les jours, tous les jours de semaine, tous les week-ends ou toute combinaison des trois options.

b. Indiquez quand vous souhaitez désactiver le système et pendant combien de temps vous voulez le désactiver.

Exemple

L'image suivante montre un calendrier qui indique à Cloud Manager d'arrêter le système tous les samedis à 12:00 pendant 48 heures. Cloud Manager redémarre le système tous les lundis à 12:00

3. Cliquez sur **Enregistrer**.

Résultat

Cloud Manager enregistre la planification. L'icône de l'horloge change pour indiquer qu'un programme est défini : 

Arrêt d'Cloud Volumes ONTAP

L'arrêt de Cloud Volumes ONTAP vous permet d'économiser de l'espace de calcul et de créer des snapshots des disques racines et de démarrage, ce qui peut être utile pour la résolution des problèmes.

Description de la tâche

Lorsque vous arrêtez une paire HA, Cloud Manager arrête les deux nœuds.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône **Désactiver**.

2. Conservez l'option de création de snapshots activés car les snapshots peuvent activer la récupération du système.
3. Cliquez sur **Désactiver**.

   L'arrêt du système peut prendre jusqu'à quelques minutes. Vous pouvez redémarrer les systèmes ultérieurement à partir de la page de l'environnement de travail.

Contrôle des coûts des ressources AWS

Avec Cloud Manager, vous pouvez consulter les coûts associés aux ressources pour l'exécution de Cloud Volumes ONTAP dans AWS. Vous pouvez également voir les économies réalisées grâce aux fonctionnalités NetApp qui permettent de réduire les coûts de stockage.

Description de la tâche

Cloud Manager met à jour les coûts lorsque vous actualisez la page. Vous devez vous référer à AWS pour plus de détails sur le coût final.

Étape

1. Vérifiez que Cloud Manager peut obtenir des informations de coûts depuis AWS :
   a. Assurez-vous que la politique IAM qui fournit les autorisations à Cloud Manager inclut les actions suivantes :

      ```
      "ce:GetReservationUtilization",
      "ce:GetDimensionValues",
      "ce:GetCostAndUsage",
      "ce:GetTags"
      ```

      Ces actions sont incluses dans la dernière "Politique de Cloud Manager". Les nouveaux systèmes déployés à partir de NetApp Cloud Central incluent automatiquement ces autorisations.

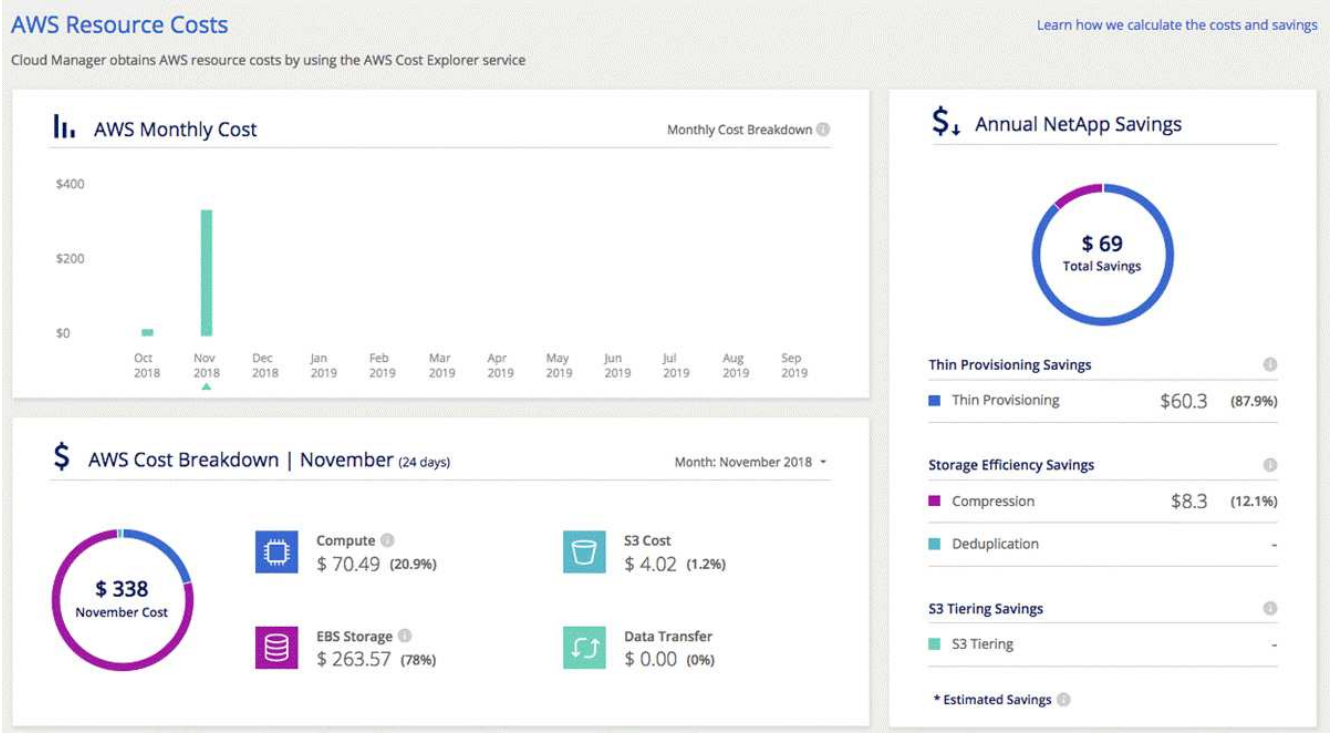
   b. "Activer la balise **WorkingEnvironnement**".

      Pour suivre vos coûts AWS, Cloud Manager attribue une balise d'allocation des coûts aux instances Cloud Volumes ONTAP. Après avoir créé votre premier environnement de travail, activez la balise **WorkingEnvironment,Id**. Les balises définies par l'utilisateur n'apparaissent pas dans les rapports de facturation AWS tant que vous ne les activez pas dans la console de facturation et de gestion des coûts.

2. Sur la page environnements de travail, sélectionnez un environnement de travail Cloud Volumes ONTAP, puis cliquez sur **coût**.

   La page coûts affiche les coûts des mois actuels et précédents et présente vos économies annuelles sur les produits NetApp, si vous avez activé les fonctions d'économies de volumes offertes par NetApp.

   L'image suivante montre un exemple de page de coût :



Connexion à Cloud Volumes ONTAP

Si vous avez besoin d'une gestion avancée de Cloud Volumes ONTAP, vous pouvez le faire à l'aide d'OnCommand System Manager ou de l'interface de ligne de commande.

Connexion à System Manager

Vous devrez peut-être effectuer certaines tâches Cloud Volumes ONTAP à partir de System Manager, un outil de gestion basé sur un navigateur qui s'exécute sur le système Cloud Volumes ONTAP. Par exemple, vous devez utiliser System Manager pour créer des LUN.

Avant de commencer

L'ordinateur à partir duquel vous accédez à Cloud Manager doit disposer d'une connexion réseau à Cloud Volumes ONTAP. Par exemple, vous devrez peut-être vous connecter à Cloud Manager à partir d'un hôte de saut dans AWS ou Azure.

Lorsqu'elles sont déployées dans plusieurs zones de disponibilité AWS, les configurations Cloud Volumes ONTAP HA utilisent une adresse IP flottante pour l'interface de gestion de cluster, ce qui signifie que le routage externe n'est pas disponible. Vous devez vous connecter à partir d'un hôte faisant partie du même domaine de routage.

Étapes

1. Sur la page Working Environments, double-cliquez sur le système Cloud Volumes ONTAP que vous souhaitez gérer avec System Manager.
2. Cliquez sur l'icône de menu, puis sur **Avancé > System Manager**.
3. Cliquez sur **lancer**.

   System Manager se charge dans un nouvel onglet de navigateur.

4. Sur l'écran de connexion, saisissez **admin** dans le champ Nom d'utilisateur, saisissez le mot de passe que vous avez spécifié lors de la création de l'environnement de travail, puis cliquez sur **connexion**.

Résultat

La console System Manager se charge. Vous pouvez désormais l'utiliser pour gérer Cloud Volumes ONTAP.

Connexion à l'interface de ligne de commande Cloud Volumes ONTAP

L'interface de ligne de commande Cloud Volumes ONTAP vous permet d'exécuter toutes les commandes administratives et constitue un bon choix pour les tâches avancées ou si vous êtes plus à l'aise avec l'interface de ligne de commande. Vous pouvez vous connecter à l'interface de ligne de commande à l'aide de Secure Shell (SSH).

Avant de commencer

L'hôte à partir duquel vous utilisez SSH pour vous connecter à Cloud Volumes ONTAP doit disposer d'une connexion réseau à Cloud Volumes ONTAP. Par exemple, vous devrez peut-être utiliser SSH à partir d'un hôte de saut dans AWS ou Azure.

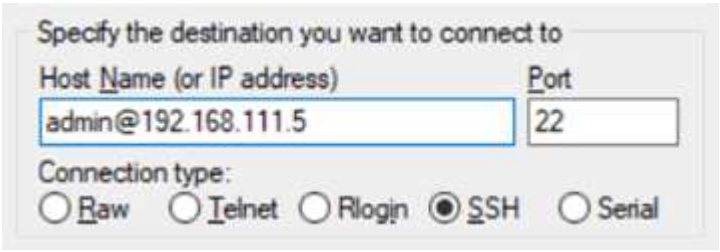
Lorsqu'elles sont déployées dans plusieurs environnements AZS, les configurations Cloud Volumes ONTAP HA utilisent une adresse IP flottante pour l'interface de gestion de cluster, ce qui signifie que le routage externe n'est pas disponible. Vous devez vous connecter à partir d'un hôte faisant partie du même domaine de routage.

Étapes

1. Dans Cloud Manager, identifiez l'adresse IP de l'interface de gestion du cluster :
   a. Sur la page Working Environments, sélectionnez le système Cloud Volumes ONTAP.
   b. Copiez l'adresse IP de gestion du cluster qui apparaît dans le volet droit.
2. Utilisez SSH pour vous connecter à l'adresse IP de l'interface de gestion du cluster à l'aide du compte admin.

   Exemple

   L'image suivante montre un exemple utilisant PuTTY :



3. À l'invite de connexion, entrez le mot de passe du compte admin.

   Exemple

```
Password: ********
COT2::>
```

Ajout de systèmes Cloud Volumes ONTAP existants à Cloud Manager

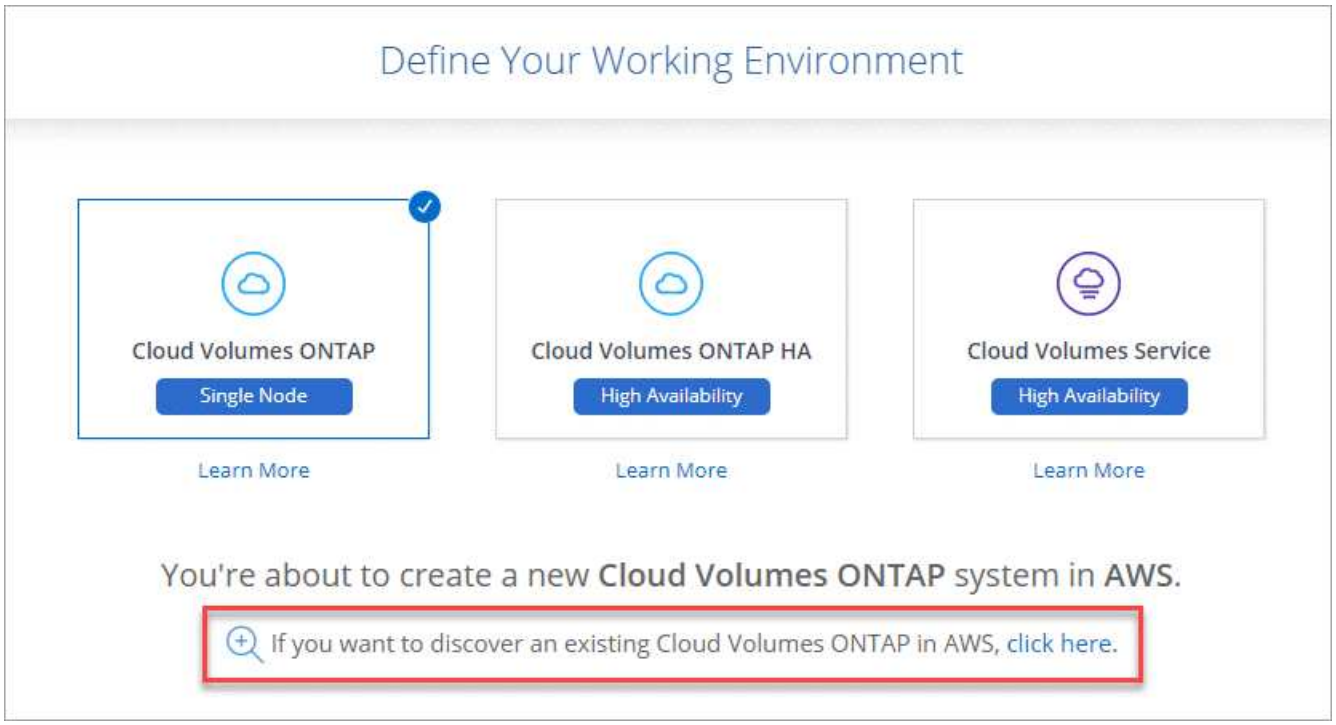
Vous pouvez découvrir et ajouter des systèmes Cloud Volumes ONTAP existants à Cloud Manager. Cette opération peut être possible si vous avez déployé un nouveau système Cloud Manager.

Avant de commencer

Vous devez connaître le mot de passe du compte d'administrateur Cloud Volumes ONTAP.

Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail**.
2. Sélectionnez le fournisseur de cloud dans lequel réside le système.
3. Choisissez le type de système Cloud Volumes ONTAP.
4. Cliquez sur le lien pour découvrir un système existant.



5. Sur la page Région, choisissez la région dans laquelle les instances sont exécutées, puis sélectionnez les instances.
6. Sur la page informations d'identification, entrez le mot de passe de l'utilisateur administrateur Cloud Volumes ONTAP, puis cliquez sur **Go**.

Résultat

Cloud Manager ajoute les instances Cloud Volumes ONTAP à l'espace de travail.

Suppression d'un environnement de travail Cloud Volumes ONTAP

Il est préférable de supprimer les systèmes Cloud Volumes ONTAP de Cloud Manager, plutôt que de la console de votre fournisseur cloud. Par exemple, si vous mettez fin à une instance Cloud Volumes ONTAP sous licence depuis AWS, vous ne pouvez pas utiliser la

clé de licence pour une autre instance. Vous devez supprimer l'environnement de travail de Cloud Manager pour libérer la licence.

Description de la tâche

Lorsque vous supprimez un environnement de travail, Cloud Manager met fin aux instances, supprime les disques et les snapshots.

> Les instances de Cloud Volumes ONTAP bénéficient d'une protection de terminaison pour empêcher la fermeture accidentelle d'AWS. Cependant, si vous arrêtez une instance Cloud Volumes ONTAP d'AWS, vous devez accéder à la console AWS CloudFormation et supprimer la pile de l'instance. Le nom de la pile est le nom de l'environnement de travail.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Supprimer**.
2. Saisissez le nom de l'environnement de travail, puis cliquez sur **Supprimer**.

   La suppression de l'environnement de travail peut prendre jusqu'à 5 minutes.

Provisionner des volumes à l'aide d'un service de fichiers

Azure NetApp Files

Découvrez Azure NetApp Files

Azure NetApp Files permet aux entreprises de migrer et d'exécuter leurs applications stratégiques, stratégiques ou stratégiques, gourmandes en performances et en latence, dans Azure sans remaniement pour le cloud.

Caractéristiques

- La prise en charge de plusieurs protocoles permet d'exécuter les applications Linux et Windows de façon transparente dans Azure.
- Plusieurs tiers de performance permettent un alignement étroit avec les exigences de performances des charges de travail.
- Les certifications les plus exigeantes, telles que SAP HANA, le RGPD et HIPPA, permettent la migration des charges de travail les plus exigeantes vers Azure.

Fonctionnalités supplémentaires dans Cloud Manager

- Migrez des données NFS ou SMB vers Azure NetApp Files directement à partir de Cloud Manager. Les migrations de données sont optimisées par le service Cloud Sync de NetApp. "En savoir plus >>".
- Avec la technologie d'intelligence artificielle (IA), Cloud Compliance vous aide à comprendre le contexte des données et à identifier les données sensibles qui résident sur vos comptes Azure NetApp Files. "En savoir plus >>".

Le coût

"Voir la tarification Azure NetApp Files".

Notez que votre abonnement et vos frais sont gérés par le service Azure NetApp Files et non par Cloud Manager.

Régions prises en charge

"Affichez les régions Azure prises en charge".

Demande d'accès

Vous devez obtenir l'accès à Azure NetApp Files par "envoi d'une demande en ligne". Vous devrez attendre l'approbation de l'équipe Azure NetApp Files pour pouvoir continuer.

Obtenir de l'aide

Pour tout problème de support technique lié à Azure NetApp Files, utilisez le portail Azure pour enregistrer une demande de support auprès de Microsoft. Sélectionnez votre abonnement Microsoft associé et sélectionnez le nom de service **Azure NetApp Files** sous **stockage**. Fournissez les informations restantes nécessaires pour créer votre demande d'assistance Microsoft.

Pour les problèmes liés à Cloud Sync et à Azure NetApp Files, vous pouvez commencer par utiliser votre numéro de série Cloud Sync directement depuis le service Cloud Sync. Vous devez accéder au service Cloud Sync via le lien dans Cloud Manager. "Affichez le processus d'activation du support Cloud Sync".

Liens connexes

- "NetApp Cloud Central : Azure NetApp Files"
- "Documentation Azure NetApp Files"
- "Documentation Cloud Sync"

Configuration de Azure NetApp Files

Créez un environnement de travail Azure NetApp Files dans Cloud Manager pour créer et gérer les comptes NetApp, les pools de capacité, les volumes et les copies Snapshot.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

Demander l'accès

"Envoyez une demande en ligne" Pour avoir accès à Azure NetApp Files.

Configurez une application Azure AD

À partir d'Azure, accordez des autorisations à une application Azure AD, puis copiez l'ID d'application (client), l'ID de répertoire (locataire) et la valeur d'un secret client.

Créer un environnement de travail Azure NetApp Files

Dans Cloud Manager, cliquez sur **Ajouter un environnement de travail** > **Microsoft Azure** > **Azure NetApp Files**, puis donnez des détails sur l'application AD.

Demande d'accès

Vous devez obtenir l'accès à Azure NetApp Files par "envoi d'une demande en ligne". Vous devrez attendre l'approbation de l'équipe Azure NetApp Files pour pouvoir continuer.

Configuration d'une application Azure AD

Cloud Manager doit disposer d'autorisations pour configurer et gérer Azure NetApp Files. Vous pouvez accorder les autorisations requises à un compte Azure en créant et en configurant une application Azure AD et en obtenant les identifiants Azure requis par Cloud Manager.

Création de l'application AD

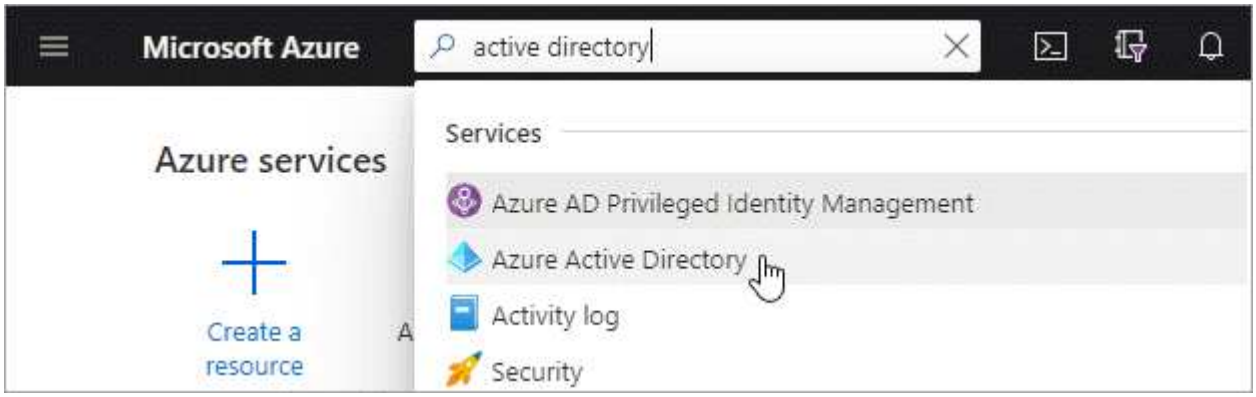
Créez une application Azure Active Directory (AD) et une entité de service que Cloud Manager peut utiliser pour le contrôle d'accès basé sur des rôles.

Avant de commencer

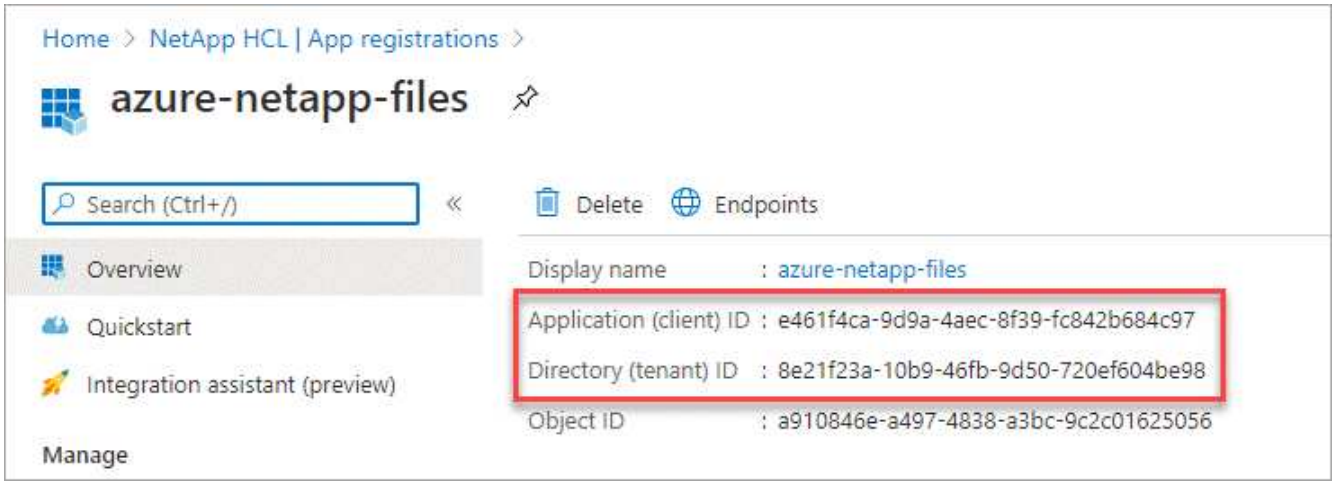
Vous devez disposer des droits d'accès dans Azure pour créer une application Active Directory et attribuer l'application à un rôle. Pour plus de détails, reportez-vous à "Documentation Microsoft Azure : autorisations requises".

Étapes

1. À partir du portail Azure, ouvrez le service **Azure Active Directory**.



2. Dans le menu, cliquez sur **enregistrements d'applications**.
3. Créez l'application :
   a. Cliquez sur **Nouvelle inscription**.
   b. Spécifiez les détails de l'application :
      - **Nom** : saisissez un nom pour l'application.
      - **Type de compte** : sélectionnez un type de compte (tout fonctionne avec Cloud Manager).
      - **URI de redirection**: Vous pouvez laisser ce blanc.
   c. Cliquez sur **Enregistrer**.
4. Copiez l'ID **application (client)** et l'ID **Directory (tenant)**.



Lorsque vous créez l'environnement de travail Azure NetApp Files dans Cloud Manager, vous devez fournir l'ID d'application (client) et l'ID de répertoire (locataire) de l'application. Cloud Manager utilise ces identifiants pour vous connecter automatiquement.

5. Créez un code secret client pour l'application afin que Cloud Manager puisse l'utiliser pour l'authentification avec Azure AD :
   a. Cliquez sur **certificats et secrets > Nouveau secret client**.
   b. Fournissez une description du secret et une durée.
   c. Cliquez sur **Ajouter**.
   d. Copier la valeur du secret client.

Résultat

Votre application AD est maintenant configurée et vous devez avoir copié l'ID de l'application (client), l'ID du répertoire (tenant) et la valeur du secret client. Ces informations doivent être saisies dans Cloud Manager lorsque vous ajoutez un environnement de travail Azure NetApp Files.

Attribution de l'application à un rôle

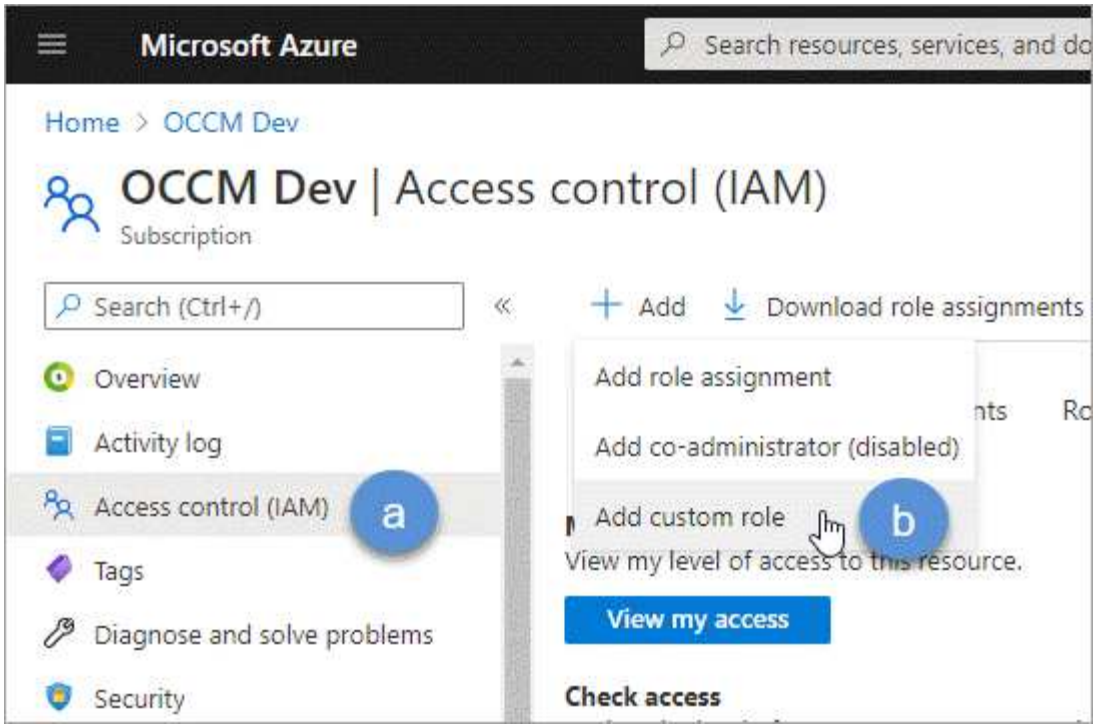
Vous devez lier l'entité de service à votre abonnement Azure et lui attribuer un rôle personnalisé qui dispose des autorisations requises.

Étapes

1. "Créez un rôle personnalisé dans Azure".

   La procédure de création du rôle dans le portail Azure s'explique par la procédure suivante.

   a. Ouvrez l'abonnement et cliquez sur **contrôle d'accès (IAM)**.
   b. Cliquez sur **Ajouter > Ajouter un rôle personnalisé**.



c. Dans l'onglet **Basics**, saisissez un nom et une description pour le rôle.

d. Cliquez sur **JSON** et cliquez sur **Edit** qui apparaît en haut à droite du format JSON.

e. Ajoutez les autorisations suivantes sous *actions* :

```
"actions": [
    "Microsoft.NetApp/*",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Insights/Metrics/Read"
    ],
```

f. Cliquez sur **Enregistrer**, cliquez sur **Suivant**, puis sur **Créer**.

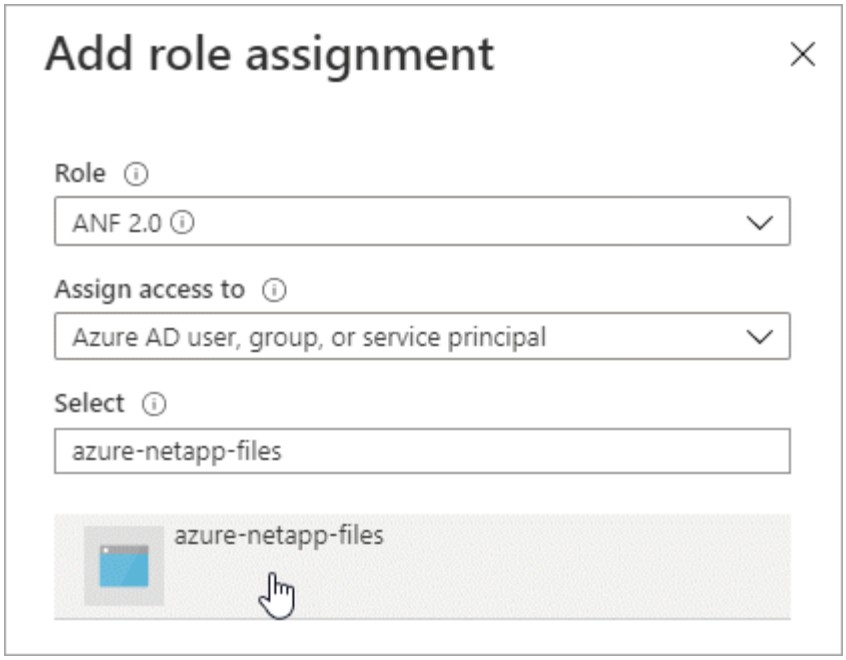
2. Attribuez maintenant l'application au rôle que vous venez de créer :

a. Sur le portail Azure, ouvrez l'abonnement et cliquez sur **contrôle d'accès (IAM) > Ajouter > Ajouter une affectation de rôle**.

b. Sélectionnez le rôle personnalisé que vous avez créé.

c. Conserver *l'utilisateur, le groupe ou le principal de service AD d'Azure sélectionné.

d. Recherchez le nom de l'application (vous ne pouvez pas le trouver dans la liste en faisant défiler la liste).



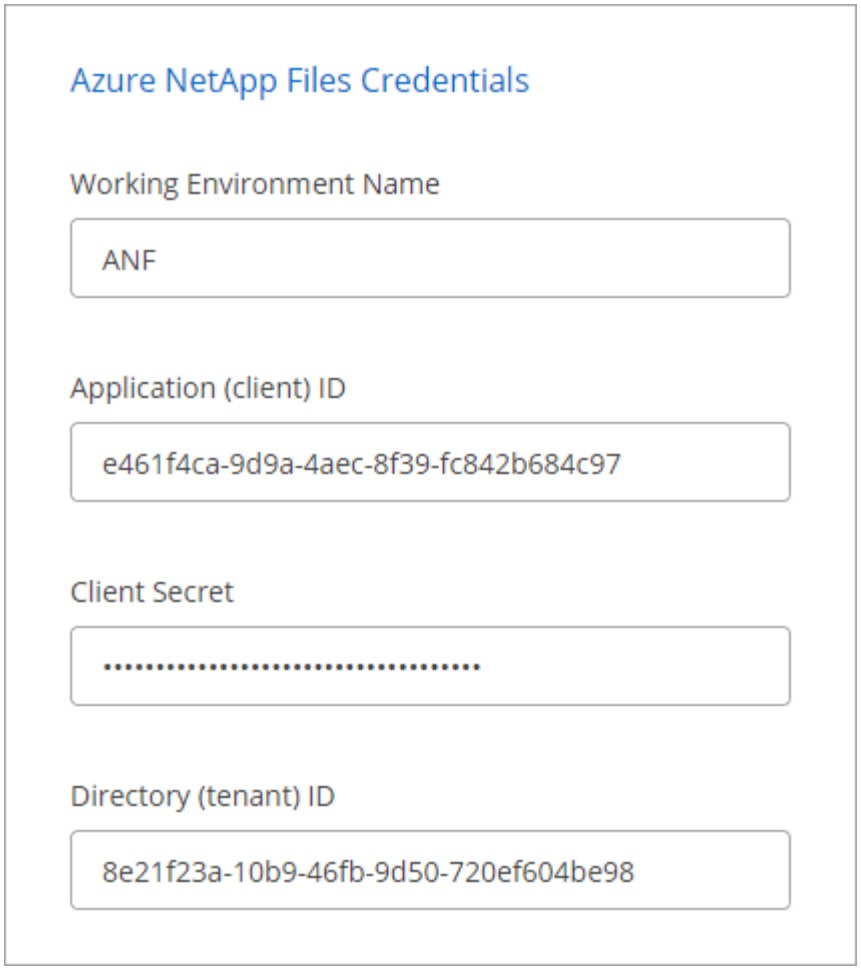
e. Sélectionnez l'application et cliquez sur **Enregistrer**.

   Le principal de service de Cloud Manager dispose désormais des autorisations Azure requises pour cet abonnement.

Création d'un environnement de travail Azure NetApp Files

Configurez un environnement de travail Azure NetApp Files dans Cloud Manager pour que vous puissiez commencer à créer des volumes.

1. Dans la page environnements de travail, cliquez sur **Ajouter un environnement de travail**.
2. Sélectionnez **Microsoft Azure**, puis **Azure NetApp Files**.
3. Fournissez des détails sur l'application AD que vous avez configurée précédemment.



4. Cliquez sur **Ajouter**.

Résultat

Vous devriez maintenant avoir un environnement de travail Azure NetApp Files.

Et la suite ?

"Démarrage de la création et de la gestion des volumes".

Création et gestion de volumes pour Azure NetApp Files

Une fois l'environnement de travail configuré, vous pouvez créer et gérer des comptes Azure NetApp Files, des pools de capacité, des volumes et des copies Snapshot.

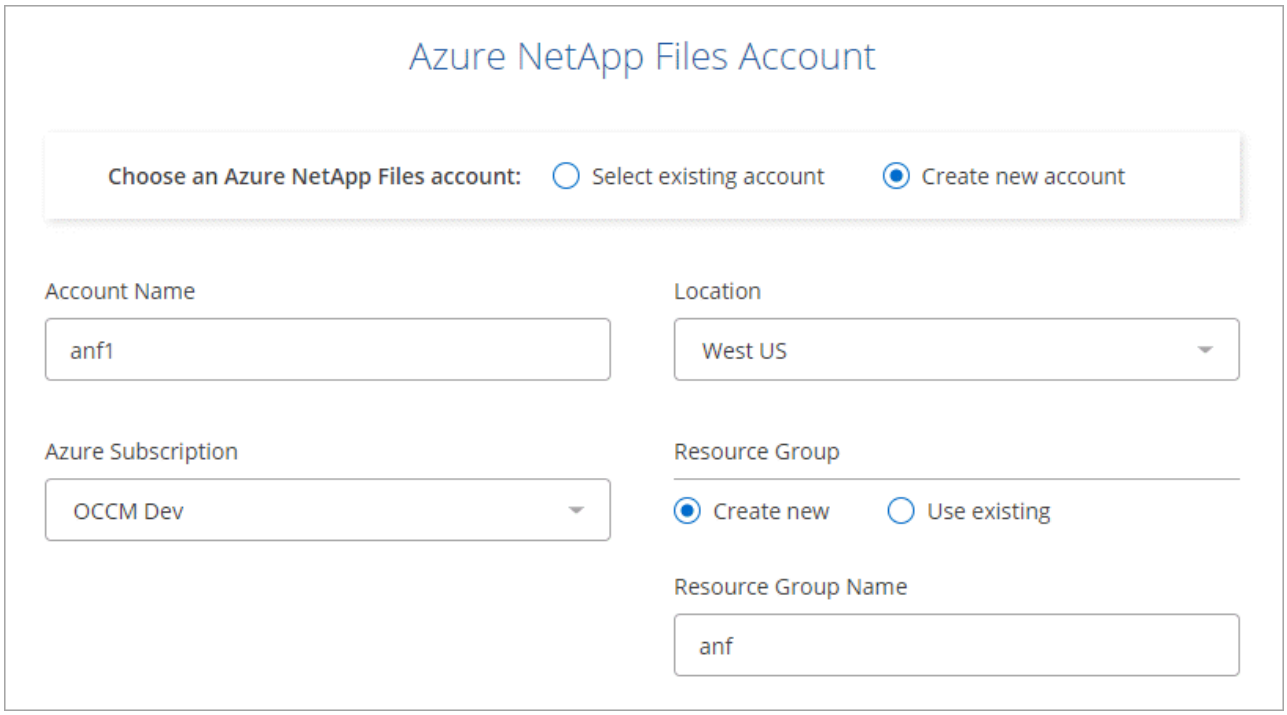
Création de volumes

Vous pouvez créer des volumes NFS ou SMB dans un compte Azure NetApp Files existant ou nouveau.

Étapes

1. Ouvrez l'environnement de travail Azure NetApp Files.
2. Cliquez sur **Ajouter nouveau volume**.
3. Fournissez les informations requises sur chaque page :

   - **Compte Azure NetApp Files** : Choisissez un compte Azure NetApp Files existant ou créez un nouveau compte.



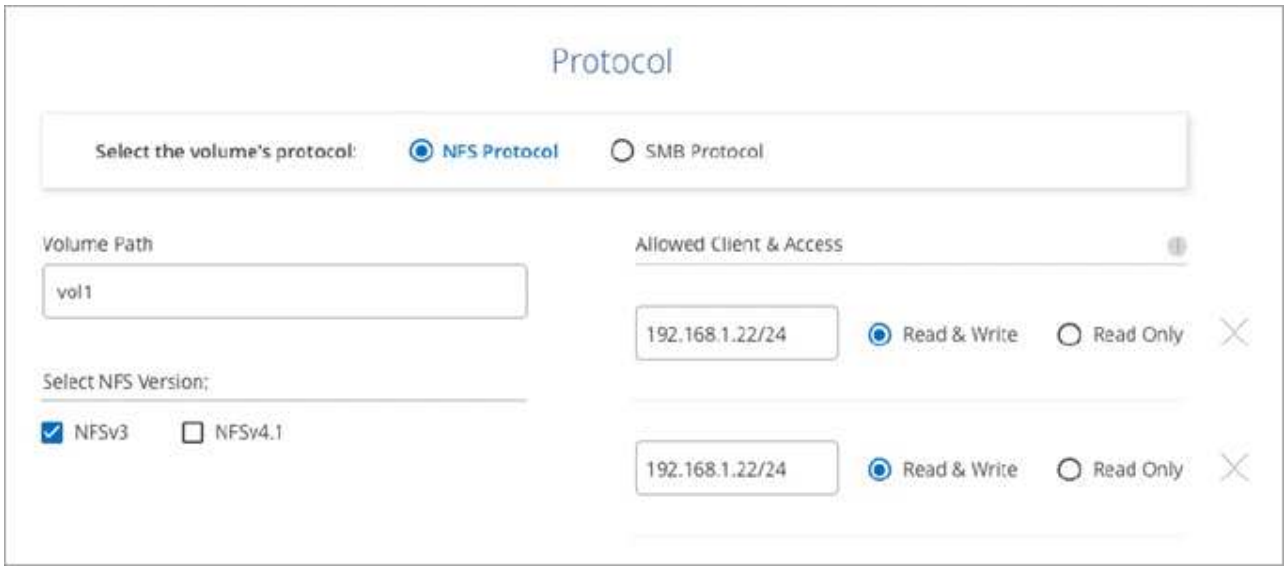
   - **Pool de capacité** : sélectionnez un pool de capacité existant ou créez un nouveau pool de capacité.

     Si vous créez un nouveau pool de capacité, vous devez spécifier une taille et sélectionner un "niveau de service".

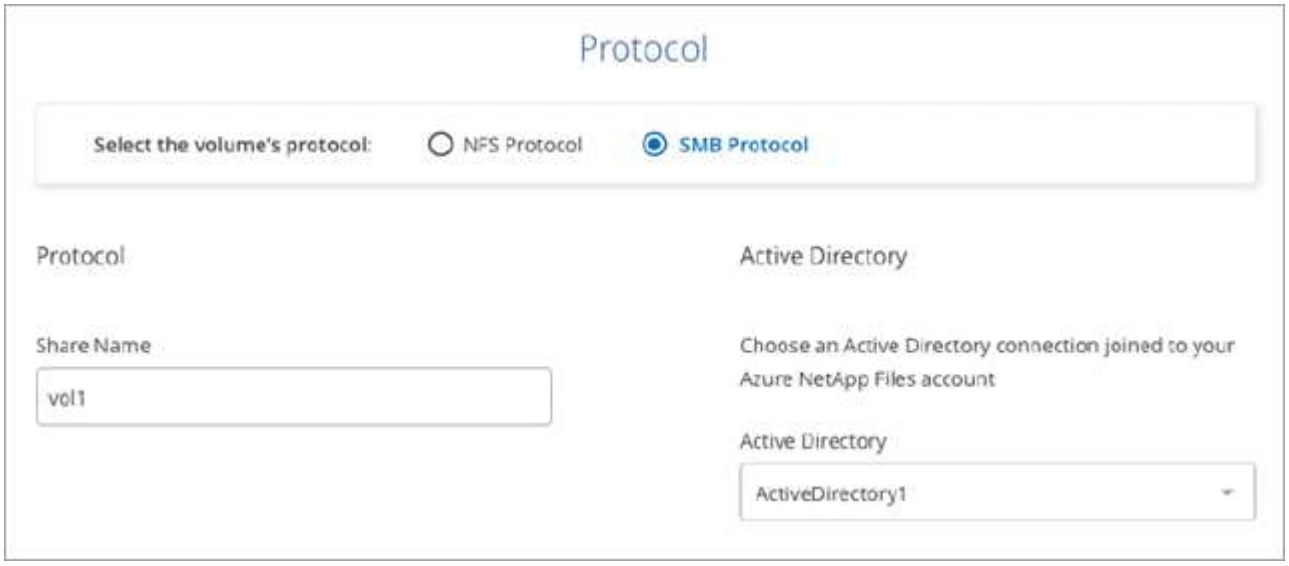
     La taille minimale du pool de capacité est de 4 To. Vous pouvez spécifier une taille en multiples de 4 To.

   - **Détails et étiquettes** : saisissez un nom et une taille de volume, le vnet et le sous-réseau où le volume doit résider, et spécifiez éventuellement des balises pour le volume.
   - **Protocole** : Choisissez le protocole NFS ou SMB et entrez les informations requises.

     Voici un exemple de détails sur NFS.



Voici un exemple de détails pour les PME. Vous devrez fournir des informations Active Directory lors de la configuration de votre premier volume SMB.



4. Cliquez sur **Ajouter un volume**.

Volumes de montage

Accédez aux instructions de montage depuis Cloud Manager, afin de monter le volume sur un hôte.

Étapes

1. Ouvrir l'environnement de travail.
2. Passez le curseur sur le volume et sélectionnez **Monter le volume**.

3. Suivez les instructions de montage du volume.

Modification de la taille et des balises d'un volume

Après avoir créé un volume, vous pouvez modifier sa taille et ses balises à tout moment.

Étapes

1. Ouvrir l'environnement de travail.
2. Placez le pointeur de la souris sur le volume et sélectionnez **Modifier**.
3. Modifiez la taille et les étiquettes si nécessaire.
4. Cliquez sur **appliquer**.

Gestion des copies Snapshot

Les copies Snapshot fournissent une copie instantanée de votre volume. Création de copies Snapshot, restauration des données sur un nouveau volume et suppression des copies Snapshot

Étapes

1. Ouvrir l'environnement de travail.
2. Placez le pointeur de la souris sur le volume et choisissez l'une des options disponibles pour la gestion des copies Snapshot :
   - **Créer une copie snapshot**
   - **Restaurer sur un nouveau volume**
   - **Supprimer une copie snapshot**
3. Suivez les invites pour terminer l'action sélectionnée.

Suppression de volumes

Supprimez les volumes dont vous n'avez plus besoin.

Étapes

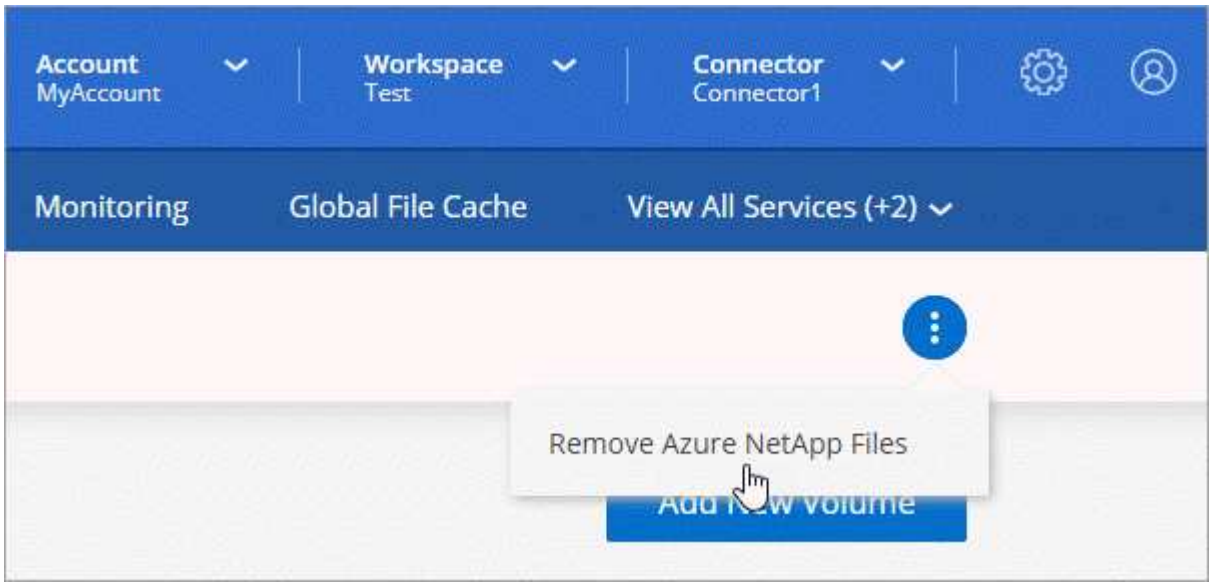
1. Ouvrir l'environnement de travail.
2. Placez le pointeur de la souris sur le volume et cliquez sur **Supprimer**.
3. Confirmez la suppression du volume.

Suppression de Azure NetApp Files

Cette action supprime Azure NetApp Files de Cloud Manager. Elle ne supprime pas votre compte ou volumes Azure NetApp Files. Vous pouvez à tout moment ajouter Azure NetApp Files à Cloud Manager.

Étapes

1. Ouvrez l'environnement de travail Azure NetApp Files.
2. Dans le coin supérieur droit de la page, sélectionnez le menu actions et cliquez sur **Supprimer Azure NetApp Files**.



3. Cliquez sur **Supprimer** pour confirmer.

Cloud Volumes Service pour AWS

En savoir plus sur Cloud Volumes Service pour AWS

NetApp Cloud Volumes Service pour AWS est un service de fichiers cloud natif qui fournit des volumes NAS sur NFS et SMB avec des performances 100 % Flash. Ce service permet l'exécution de tout workload, y compris les applications héritées, dans le cloud AWS.

Avantages d'Cloud Volumes Service pour AWS

Cloud Volumes Service pour AWS offre plusieurs avantages :

- Service entièrement géré, il n'est donc pas nécessaire de configurer ou de gérer les périphériques de stockage
- Prise en charge des protocoles NFS v3 et NFS v4.1, et des protocoles NAS SMB 3.0 et 3.1.1
- Accès sécurisé aux instances Linux et Windows Elastic Container Service (ECS), avec prise en charge notamment :
  - Amazon Linux 2, Red Hat Enterprise Linux 7.5, SLES 12 SP3 et Ubuntu 16.04 LTS
  - Windows Server 2008 R2, Windows Server 2012 R2 et Windows Server 2016

- Vous avez le choix entre un bundle et une facturation à l'utilisation

Le coût

Les volumes créés par Cloud Volumes Service pour AWS sont facturés en fonction de l'abonnement que vous avez souscrit au service, et non via Cloud Manager.

Il n'y a aucun frais pour découvrir une région ou un volume Cloud Volumes Service pour AWS depuis Cloud Manager.

Avant de commencer

- Cloud Manager peut découvrir les abonnements et volumes Cloud Volumes Service pour AWS. Voir la "Guide de configuration de compte NetApp Cloud Volumes Service pour AWS" si vous n'avez pas encore configuré votre abonnement. Vous devez suivre cette procédure d'installation pour chaque région avant de pouvoir ajouter les abonnements et volumes AWS à Cloud Manager.
- Vous devez obtenir la clé API Cloud volumes et une clé secrète pour les fournir à Cloud Manager. "Pour en savoir plus, consultez la documentation Cloud Volumes Service pour AWS".

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou passez à la section suivante pour obtenir plus d'informations.

Vérifiez la prise en charge de votre configuration

Vous avez configuré AWS pour Cloud Volumes Service et vous devez vous être abonné à l'un de ces "Offres NetApp Cloud Volumes Service sur AWS Marketplace".

Ajoutez votre abonnement Cloud Volumes Service pour AWS

Vous devez créer un environnement de travail pour les volumes basés sur votre abonnement Cloud Volumes Service pour AWS.

Créer des volumes cloud

Les volumes Cloud qui existent déjà pour cet abonnement apparaissent dans le nouvel environnement de travail. Sinon, vous créez de nouveaux volumes à partir de Cloud Manager.

Montez un volume cloud

Montez de nouveaux volumes cloud sur votre instance AWS pour que les utilisateurs puissent commencer à utiliser le stockage.

Obtenir de l'aide

Utilisez la discussion de chat Cloud Manager pour toute question générale sur les services.

Pour les problèmes de support technique associés à vos volumes Cloud, utilisez votre numéro de série à 20 chiffres « 930 » dans l'onglet « support » de l'interface utilisateur Cloud Volumes Service. Utilisez cet ID de support lors de l'ouverture d'un ticket Web ou lorsque vous appelez pour obtenir de l'aide. N'oubliez pas d'activer votre numéro de série Cloud Volumes Service pour le support depuis l'interface utilisateur de Cloud Volumes Service. "Ces étapes sont expliquées ici".

Limites

- Cloud Manager ne prend pas en charge la réplication des données entre les environnements de travail lors de l'utilisation de volumes Cloud Volumes Service.
- La suppression de votre abonnement Cloud Volumes Service pour AWS de Cloud Manager n'est pas prise en charge. Pour ce faire, vous devez utiliser l'interface Cloud Volumes Service pour AWS.

Liens connexes

- "NetApp Cloud Central : Cloud Volumes Service pour AWS"
- "Documentation sur NetApp Cloud Volumes Service pour AWS"

Gestion d'Cloud Volumes Service pour AWS

Cloud Manager vous permet de créer des volumes cloud basés sur votre "Cloud Volumes Service pour AWS" abonnement. Vous pouvez également découvrir les volumes cloud que vous avez déjà créés à partir de l'interface Cloud Volumes Service et les ajouter à un environnement de travail.

Ajoutez votre abonnement Cloud Volumes Service pour AWS

Que vous ayez déjà créé des volumes depuis l'interface utilisateur Cloud Volumes Service ou que vous venez de vous inscrire à Cloud Volumes Service pour AWS et qu'aucun volume n'a encore été créé, la première étape consiste à créer un environnement de travail pour les volumes basés sur votre abonnement AWS.

Si des volumes Cloud existent déjà pour cet abonnement, les volumes sont automatiquement ajoutés au nouvel environnement de travail. Si vous n'avez pas encore ajouté de volumes cloud pour l'abonnement AWS, cela fait une fois que vous avez créé le nouvel environnement de travail.

Si vous disposez d'abonnements et de volumes dans plusieurs régions AWS, vous devez effectuer cette tâche pour chaque région.

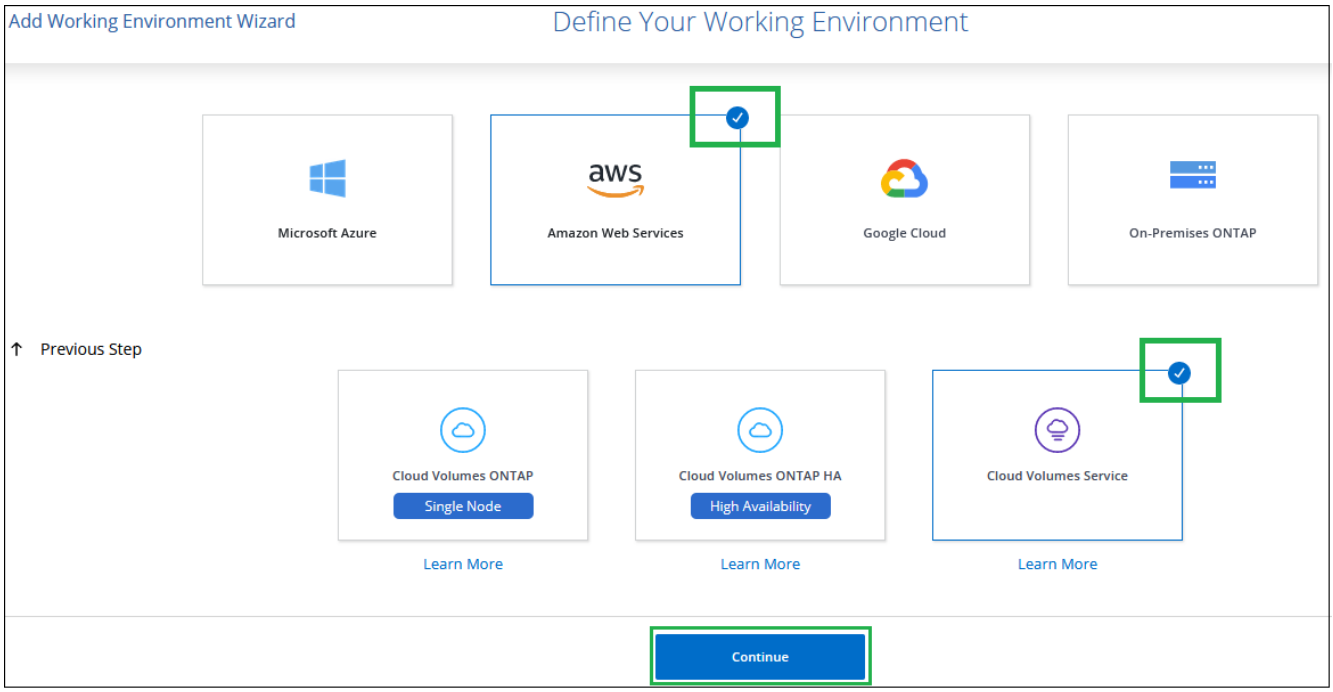
Avant de commencer

Vous devez disposer des informations suivantes lors de l'ajout d'un abonnement dans chaque région :

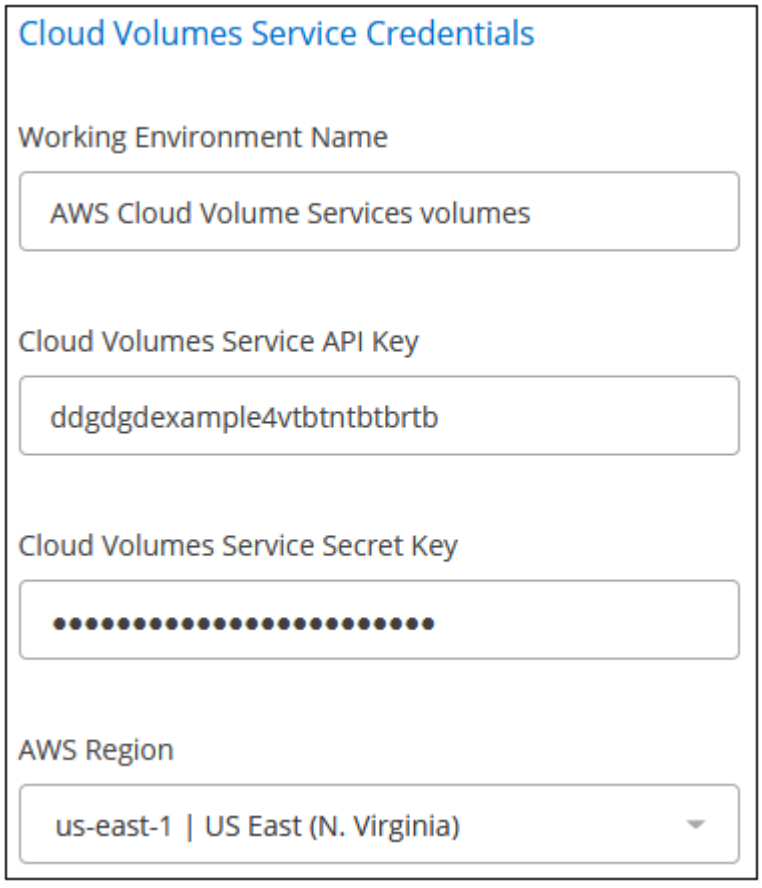
- Clé API et clé secrète de Cloud volumes : "Consultez la documentation sur Cloud Volumes Service pour AWS pour obtenir ces informations".
- Région AWS où l'abonnement a été créé.

Étapes

1. Dans Cloud Manager, ajoutez un nouvel environnement de travail, sélectionnez l'emplacement **Amazon Web Services**, puis cliquez sur **Continuer**.
2. Sélectionnez **Cloud Volumes Service** et cliquez sur **Continuer**.



3. Fournir des informations sur votre abonnement Cloud Volumes Service :
   a. Entrez le nom de l'environnement de travail que vous souhaitez utiliser.
   b. Entrez la clé API Cloud Volumes Service et la clé secrète.
   c. Sélectionnez la région AWS où résident vos volumes cloud ou où ils seront déployés.
   d. Cliquez sur **Ajouter**.



Résultat

Cloud Manager affiche votre configuration Cloud Volumes Service pour AWS sur la page Working Environments.

Si des volumes cloud existent déjà pour cet abonnement, ils sont automatiquement ajoutés au nouvel environnement de travail, comme indiqué dans la capture d'écran. Vous pouvez ajouter des volumes cloud supplémentaires à partir de Cloud Manager.

Si aucun volume de Cloud n'existe pour cet abonnement, vous pouvez les créer maintenant.

Création de volumes cloud

Pour les configurations dans lesquelles des volumes existent déjà dans l'environnement de travail Cloud Volumes Service, vous pouvez utiliser ces étapes pour ajouter de nouveaux volumes.

Pour les configurations dans lesquelles aucun volume n'existe, vous pouvez créer votre premier volume directement depuis Cloud Manager après avoir configuré votre abonnement Cloud Volumes Service pour AWS. Auparavant, le premier volume devait être créé directement dans l'interface utilisateur de Cloud Volumes Service.

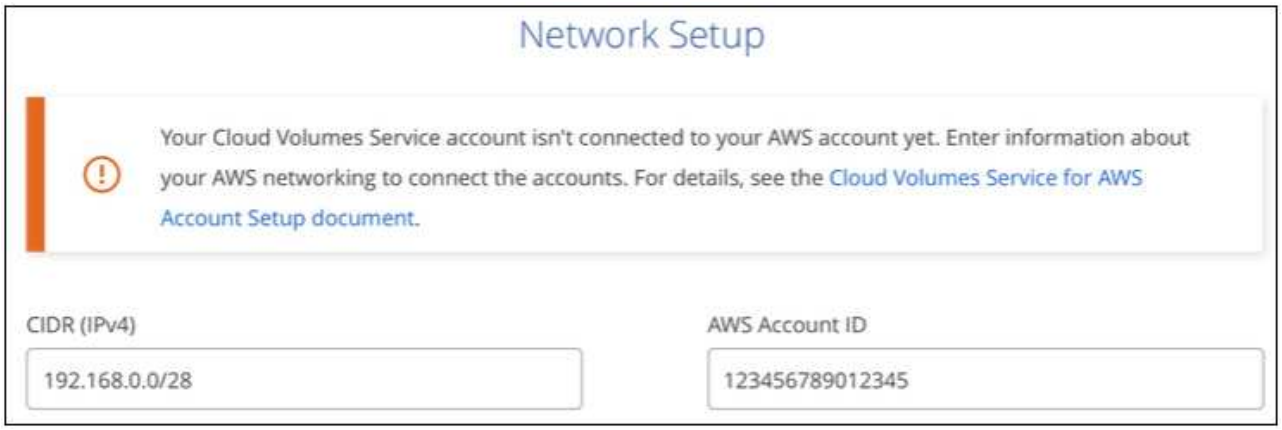
Avant de commencer

- Si vous souhaitez utiliser SMB dans AWS, vous devez avoir configuré DNS et Active Directory.
- Lorsque vous prévoyez de créer un volume SMB, vous devez disposer d'un serveur Windows Active Directory disponible auquel vous pouvez vous connecter. Vous entrez ces informations lors de la création du volume. Assurez-vous également que l'utilisateur administrateur peut créer un compte machine dans le chemin d'unité organisationnelle spécifié.
- Vous aurez besoin de ces informations lors de la création du premier volume dans une nouvelle région/environnement de travail :
  - ID de compte AWS : identifiant de compte Amazon à 12 chiffres sans tirets. Pour connaître votre ID de compte, reportez-vous à ce document "Rubrique AWS".
  - Blocage de routage inter-domaines (CIDR) sans classe : un bloc CIDR IPv4 non utilisé. Le préfixe réseau doit être compris entre /16 et /28 et doit également se trouver dans les plages réservées aux réseaux privés (RFC 1918). Ne choisissez pas un réseau qui chevauche vos allocations VPC CIDR.

Étapes

1. Sélectionnez le nouvel environnement de travail et cliquez sur **Ajouter un nouveau volume**.
2. Si vous ajoutez le premier volume à l'environnement de travail de la région, vous devez ajouter les informations de mise en réseau AWS.
   a. Saisissez la plage IPv4 (CIDR) pour la région.
   b. Entrez l'ID de compte AWS à 12 chiffres (sans tiret) pour connecter votre compte Cloud volumes à votre compte AWS.

c. Cliquez sur **Continuer**.



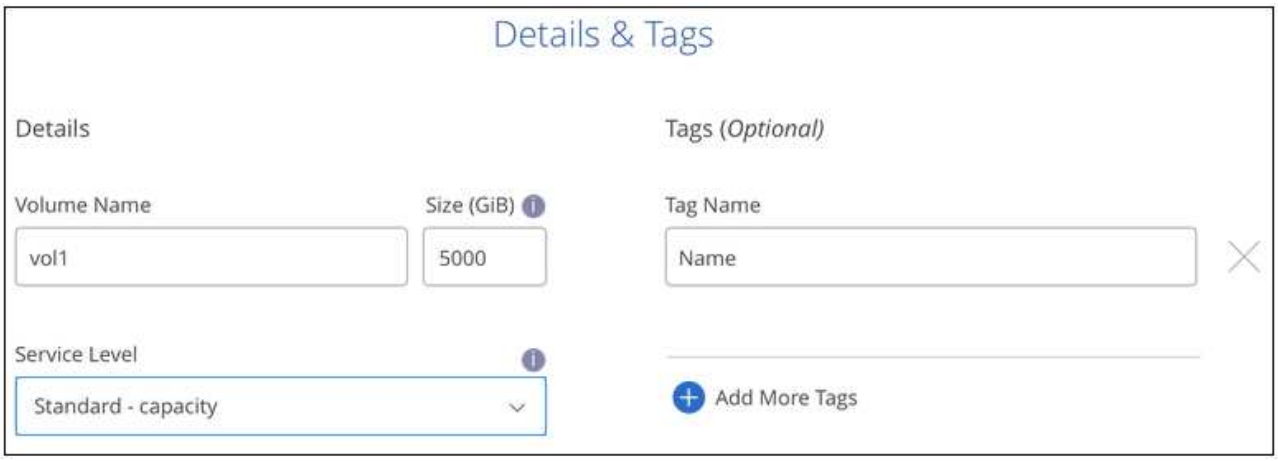
3. La page accepter les interfaces virtuelles décrit certaines étapes que vous devrez effectuer après avoir ajouté le volume pour que vous soyez prêt à effectuer cette étape. Cliquez à nouveau sur **Continuer**.
4. Dans la page Détails et étiquettes, entrez les détails du volume :
   a. Entrez un nom pour le volume.
   b. Spécifiez une taille comprise entre 100 Gio et 90,000 Gio (équivalent à 88 Tibs).

      "En savoir plus sur la capacité allouée".

   c. Spécifier un niveau de service : standard, Premium ou Extreme.

      "En savoir plus sur les niveaux de service".

   d. Entrez un ou plusieurs noms d'étiquettes pour classer le volume si vous le souhaitez.
   e. Cliquez sur **Continuer**.



5. Sur la page Protocol, sélectionnez NFS, SMB ou Dual Protocol, puis définissez les détails. Les entrées requises pour NFS et SMB sont répertoriées dans les sections ci-après.
6. Dans le champ chemin du volume, indiquez le nom de l'exportation de volume que vous verrez lors du montage du volume.
7. Si vous sélectionnez Protocole double, vous pouvez sélectionner le style de sécurité en sélectionnant NTFS ou UNIX. Les styles de sécurité affectent le type d'autorisation de fichier utilisé et la manière dont les autorisations peuvent être modifiées.

- UNIX utilise les bits du mode NFSv3 et seuls les clients NFS peuvent modifier les autorisations.
- NTFS utilise les listes de contrôle d'accès NTFS et seuls les clients SMB peuvent modifier les autorisations.

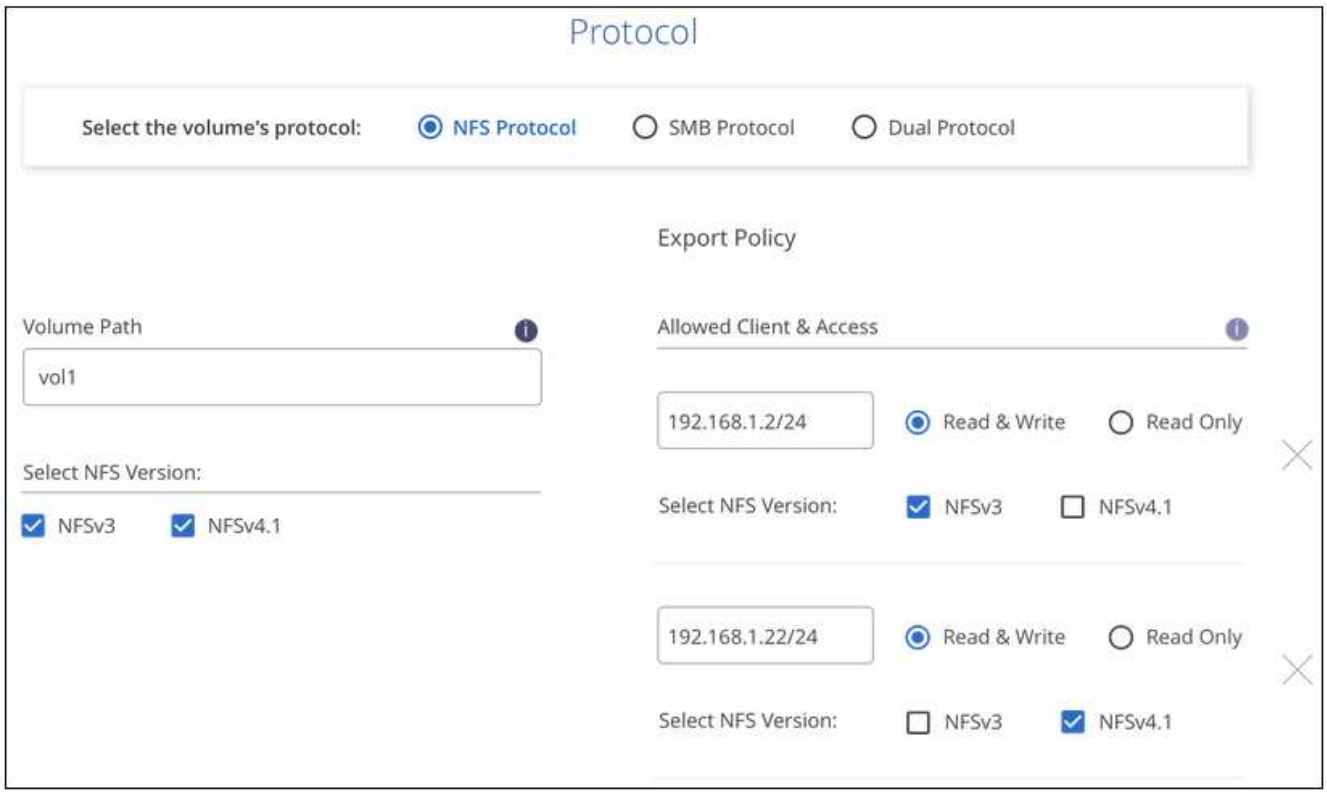
8. Pour NFS :

   a. Dans le champ version NFS, sélectionnez NFS v3, NFS v4.1 ou les deux en fonction de vos exigences.

   b. Vous pouvez également créer une export-policy pour identifier les clients pouvant accéder au volume. Spécifiez :

      - Clients autorisés à l'aide d'une adresse IP ou d'un routage inter-domaines sans classe (CIDR).
      - Droits d'accès en lecture et écriture ou lecture seule.
      - Protocole d'accès (ou protocoles si le volume autorise l'accès NFS v3 et NFS v4.1) utilisé pour les utilisateurs.
      - Cliquez sur **+ Ajouter règle de stratégie d'exportation** si vous souhaitez définir des règles de stratégie d'exportation supplémentaires.

        L'image suivante montre la page Volume remplie pour le protocole NFS :



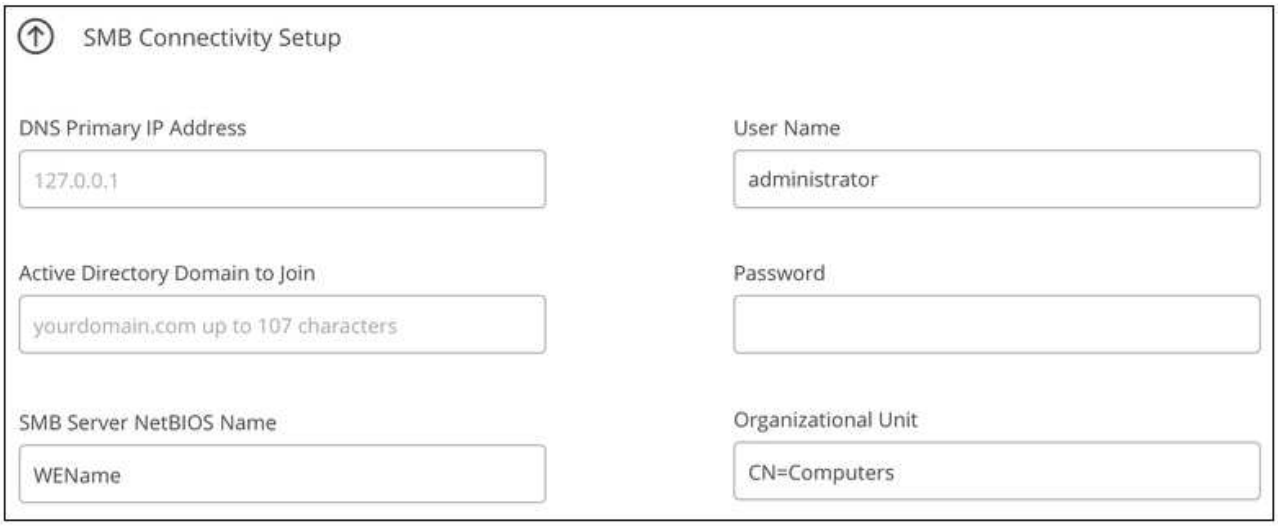
9. Pour SMB :

   a. Vous pouvez activer le chiffrement de session SMB en cochant la case SMB Protocol Encryption.

   b. Vous pouvez intégrer le volume à un serveur Windows Active Directory existant en remplissant les champs de la section Active Directory :

Champ	Description
Adresse IP principale DNS	Les adresses IP des serveurs DNS qui fournissent une résolution de nom pour le serveur SMB. Utilisez une virgule pour séparer les adresses IP lorsque vous faites référence à plusieurs serveurs, par exemple 172.31.25.223, 172.31.2.74.
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) que vous souhaitez que le serveur SMB rejoint. Si vous utilisez AWS Managed Microsoft AD, utilisez la valeur du champ « Directory DNS name ».
Nom NetBIOS du serveur SMB	Nom NetBIOS du serveur SMB qui sera créé.
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Unité organisationnelle	Unité organisationnelle au sein du domaine AD à associer au serveur SMB. La valeur par défaut est CN=Computers pour les connexions à votre propre serveur Windows Active Directory. Si vous configurez AWS Managed Microsoft AD en tant que serveur AD pour Cloud Volumes Service, vous devez entrer **ou=ordinateurs,ou=corp** dans ce champ.

L'image suivante montre la page Volume remplie pour le protocole SMB :



Suivez les recommandations relatives aux paramètres des groupes de sécurité AWS pour permettre l'intégration correcte des volumes cloud avec les serveurs Windows Active Directory. Voir "Paramètres des groupes de sécurité AWS pour les serveurs Windows AD" pour en savoir plus.

10. Sur la page Volume à partir de Snapshot, si vous souhaitez créer ce volume en fonction d'un snapshot d'un volume existant, sélectionnez l'instantané dans la liste déroulante Nom de l'instantané.
11. Sur la page règle Snapshot, vous pouvez activer Cloud Volumes Service pour créer des copies snapshot de vos volumes selon un planning. Vous pouvez le faire maintenant ou le modifier ultérieurement pour définir la stratégie de snapshot.

    Voir "Création d'une règle Snapshot" pour plus d'informations sur la fonctionnalité de snapshot.

12. Cliquez sur **Ajouter un volume**.

Le nouveau volume est ajouté à l'environnement de travail.

Une fois que vous avez terminé

S'il s'agit du premier volume créé dans cet abonnement AWS, vous devez lancer la console de gestion AWS pour accepter les deux interfaces virtuelles qui seront utilisées dans cette région AWS pour connecter l'ensemble de vos volumes cloud. Voir la "Guide de configuration de compte NetApp Cloud Volumes Service pour AWS" pour plus d'informations.

Vous devez accepter les interfaces dans les 10 minutes après avoir cliqué sur le bouton **Ajouter un volume** pour que le système se déchaîne. Dans ce cas, envoyez un e-mail à cvs-support@netapp.com avec votre ID client AWS et votre numéro de série NetApp. Le support corrigera le problème et vous pourrez redémarrer le processus d'intégration.

Puis continuer avec "Montage du volume cloud".

Montez le volume cloud

Vous pouvez monter un volume cloud sur votre instance AWS. Les volumes cloud prennent actuellement en charge NFSv3 et NFSv4.1 pour les clients Linux et UNIX, ainsi que SMB 3.0 et 3.1.1 pour les clients Windows.

Remarque : Veuillez utiliser le protocole/dialecte mis en évidence pris en charge par votre client.

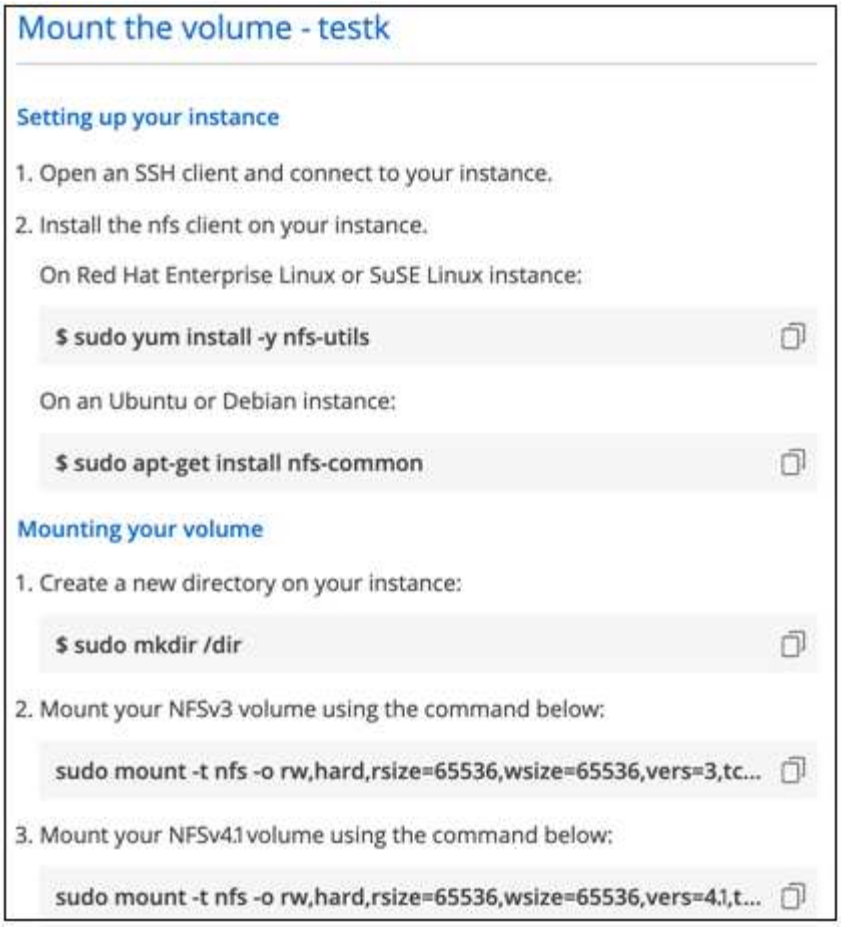
Étapes

1. Ouvrir l'environnement de travail.
2. Placez le pointeur de la souris sur le volume et cliquez sur **montez le volume**.

   Les volumes NFS et SMB affichent des instructions de montage pour ce protocole. Les volumes à double protocole fournissent ces deux ensembles d'instructions.

3. Placez le pointeur de la souris sur les commandes et copiez-les dans le presse-papiers pour faciliter ce processus. Ajoutez simplement le répertoire de destination/point de montage à la fin de la commande.

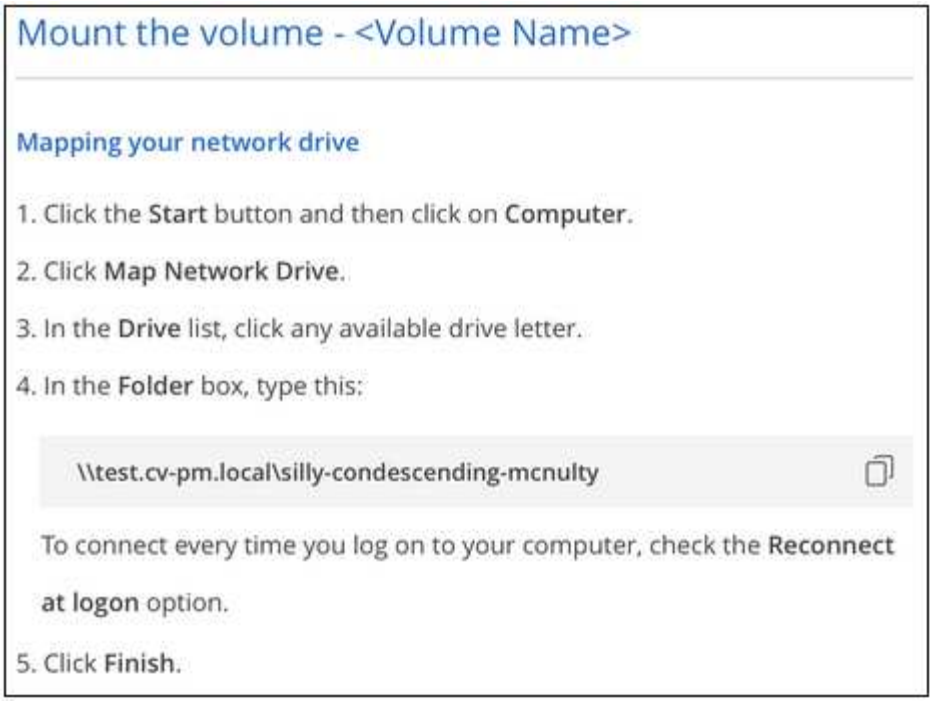
   Exemple NFS:



La taille d'E/S maximale définie par le `rsize` et `wsize` les options sont 1048576. cependant, la version 65536 est la valeur par défaut recommandée pour la plupart des cas d'utilisation.

Notez que les clients Linux seront par défaut sur NFSv4.1 à moins que la version soit spécifiée avec `vers=<nfs_version>` option.

Exemple SMB:



4. Connectez-vous à votre instance Amazon Elastic Compute Cloud (EC2) à l'aide d'un client SSH ou RDP, puis suivez les instructions de montage pour votre instance.

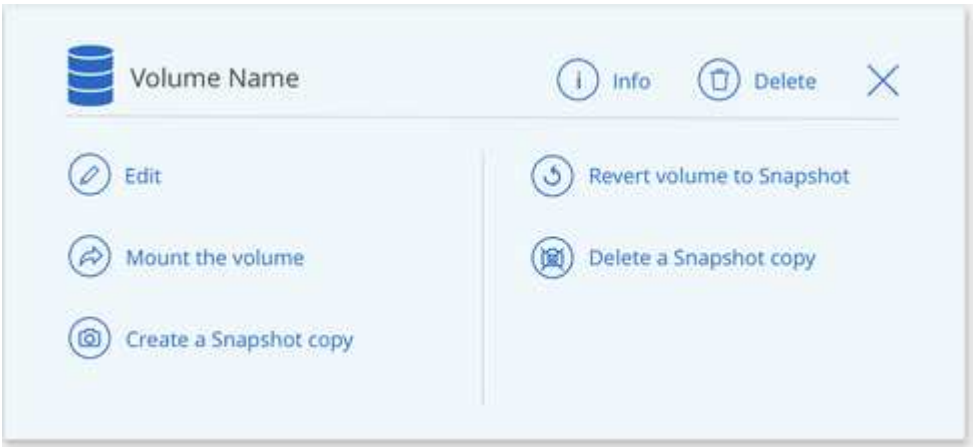
   Après avoir terminé les étapes des instructions de montage, vous avez correctement monté le volume cloud sur votre instance AWS.

Gestion des volumes existants

Vous pouvez gérer les volumes existants à mesure que vos besoins de stockage changent. Vous pouvez afficher, modifier, restaurer et supprimer des volumes.

Étapes

1. Ouvrir l'environnement de travail.
2. Placez le pointeur de la souris sur le volume.



3. Gérez vos volumes :

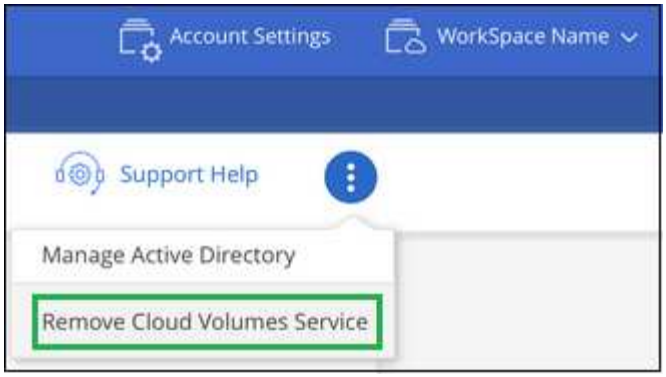
Tâche	Action
Afficher des informations sur un volume	Sélectionnez un volume, puis cliquez sur **Info**.
Modification d'un volume (y compris la règle Snapshot)	a. Sélectionnez un volume, puis cliquez sur **Modifier**. b. Modifiez les propriétés du volume, puis cliquez sur **mettre à jour**.
Procurez-vous la commande NFS ou SMB mount	a. Sélectionnez un volume, puis cliquez sur **Monter le volume**. b. Cliquez sur **Copier** pour copier la ou les commandes.
Créez une copie Snapshot à la demande	a. Sélectionnez un volume, puis cliquez sur **Créer une copie snapshot**. b. Modifiez le nom de l'instantané, si nécessaire, puis cliquez sur **Créer**.
Remplacez le volume par le contenu d'une copie Snapshot	a. Sélectionnez un volume, puis cliquez sur **revenir au snapshot**. b. Sélectionnez une copie Snapshot et cliquez sur **Revert**.
Supprimez une copie Snapshot	a. Sélectionnez un volume, puis cliquez sur **Supprimer une copie snapshot**. b. Sélectionnez la copie Snapshot à supprimer et cliquez sur **Supprimer**. c. Cliquez à nouveau sur **Supprimer** pour confirmer.
Supprimer un volume	a. Démonter le volume de tous les clients : ◦ Sur les clients Linux, utilisez `umount` commande. ◦ Sur les clients Windows, cliquez sur **déconnecter le lecteur réseau**. b. Sélectionnez un volume, puis cliquez sur **Supprimer**. c. Cliquez à nouveau sur **Supprimer** pour confirmer.

Supprimez Cloud Volumes Service de Cloud Manager

Vous pouvez supprimer un abonnement Cloud Volumes Service pour AWS et tous les volumes existants depuis Cloud Manager. Les volumes ne sont pas supprimés, mais ils sont simplement supprimés de l'interface Cloud Manager.

Étapes

1. Ouvrir l'environnement de travail.



2. Cliquez sur le bouton En haut de la page, cliquez sur **Supprimer Cloud Volumes Service**.
3. Dans la boîte de dialogue de confirmation, cliquez sur **Supprimer**.

Gérer la configuration d'Active Directory

Si vous modifiez vos serveurs DNS ou votre domaine Active Directory, vous devez modifier le serveur SMB dans Cloud volumes Services afin qu'il puisse continuer à fournir du stockage aux clients.

Vous pouvez également supprimer le lien vers un Active Directory si vous n'en avez plus besoin.

Étapes

1. Ouvrir l'environnement de travail.
2. Cliquez sur le bouton En haut de la page, cliquez sur **gérer Active Directory**.
3. Si aucun Active Directory n'est configuré, vous pouvez en ajouter un maintenant. Si l'un d'eux est configuré, vous pouvez modifier les paramètres ou le supprimer à l'aide du bouton.
4. Spécifiez les paramètres de l'Active Directory que vous souhaitez joindre :

Champ	Description
Adresse IP principale DNS	Les adresses IP des serveurs DNS qui fournissent une résolution de nom pour le serveur SMB. Utilisez une virgule pour séparer les adresses IP lorsque vous faites référence à plusieurs serveurs, par exemple 172.31.25.223, 172.31.2.74.
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) que vous souhaitez que le serveur SMB rejoint. Si vous utilisez AWS Managed Microsoft AD, utilisez la valeur du champ « Directory DNS name ».
Nom NetBIOS du serveur SMB	Nom NetBIOS du serveur SMB qui sera créé.
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Unité organisationnelle	Unité organisationnelle au sein du domaine AD à associer au serveur SMB. La valeur par défaut est CN=Computers pour les connexions à votre propre serveur Windows Active Directory. Si vous configurez AWS Managed Microsoft AD en tant que serveur AD pour Cloud Volumes Service, vous devez entrer **ou=ordinateurs,ou=corp** dans ce champ.

5. Cliquez sur **Enregistrer** pour enregistrer vos paramètres.

Gestion des copies Snapshot de Cloud volumes

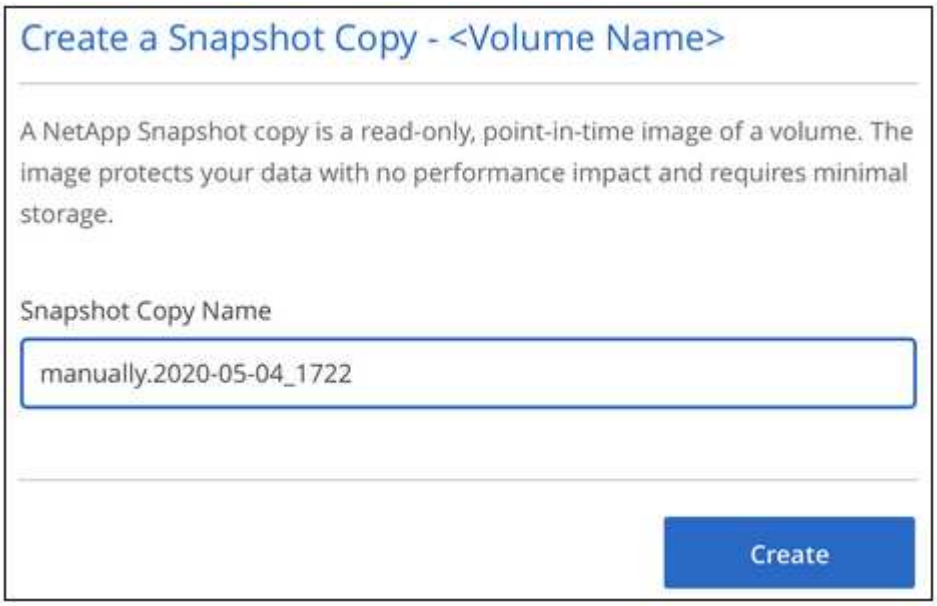
Vous pouvez créer une règle Snapshot pour chaque volume, de sorte que vous puissiez récupérer ou restaurer l'intégralité du contenu d'un volume à partir d'une version antérieure. Vous pouvez également créer un snapshot à la demande d'un volume cloud, si nécessaire.

Créer un snapshot à la demande

Vous pouvez créer un snapshot à la demande d'un volume cloud si vous souhaitez créer un snapshot avec l'état actuel du volume.

Étapes

1. Ouvrir l'environnement de travail.
2. Placez le pointeur de la souris sur le volume et cliquez sur **Créer une copie snapshot**.
3. Entrez un nom pour le snapshot ou utilisez le nom généré automatiquement, puis cliquez sur **Créer**.



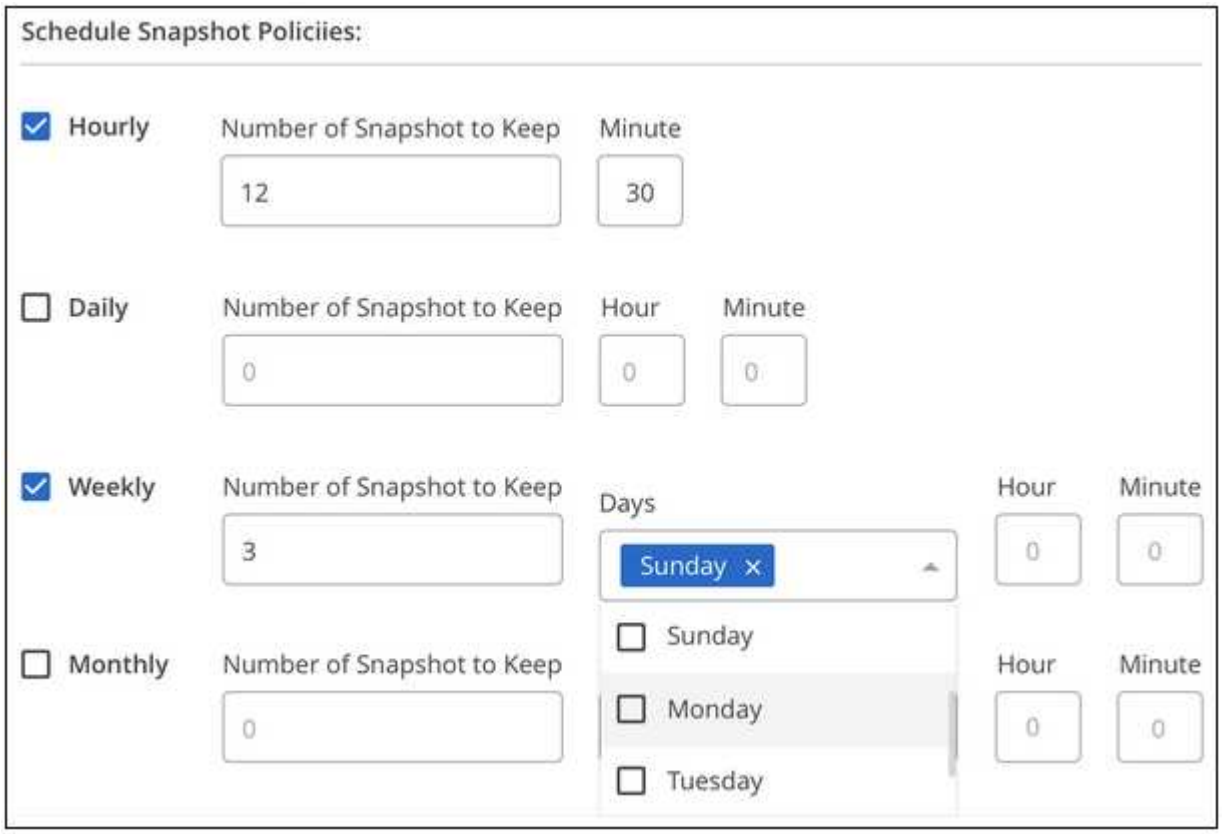
Créez ou modifiez une policy de snapshots

Vous pouvez créer ou modifier une règle Snapshot si nécessaire pour un volume cloud. Vous définissez la stratégie de snapshot à partir de l'onglet *Snapshot Policy* lors de la création d'un volume ou lors de la modification d'un volume.

Étapes

1. Ouvrir l'environnement de travail.
2. Placez le pointeur de la souris sur le volume et cliquez sur **Modifier**.
3. Dans l'onglet *Snapshot Policy*, déplacez le curseur activer les snapshots vers la droite.
4. Définir la planification des snapshots :
   a. Sélectionnez la fréquence : **horaire**, **quotidien**, **hebdomadaire** ou **mensuel**

b. Sélectionnez le nombre de snapshots que vous souhaitez conserver.
c. Sélectionnez le jour, l'heure et la minute où l'instantané doit être pris.



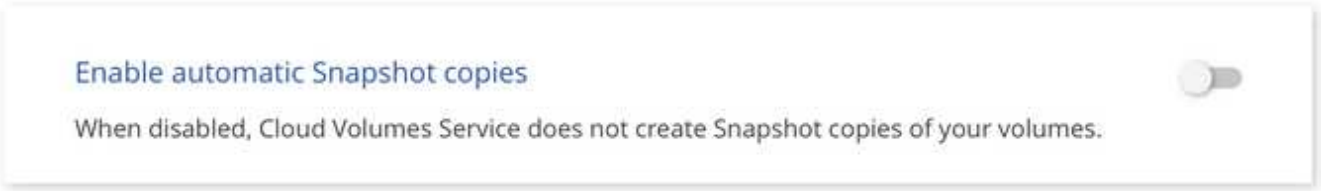
5. Cliquez sur **Ajouter volume** ou **mettre à jour volume** pour enregistrer les paramètres de votre stratégie.

Désactiver une règle Snapshot

Vous pouvez désactiver une stratégie de snapshot pour empêcher la création de snapshots pendant une courte période tout en conservant les paramètres de votre stratégie de snapshot.

Étapes

1. Ouvrir l'environnement de travail.
2. Placez le pointeur de la souris sur le volume et cliquez sur **Modifier**.
3. Dans l'onglet *Snapshot Policy*, déplacez le curseur activer les snapshots vers la gauche.



4. Cliquez sur **mettre à jour le volume**.

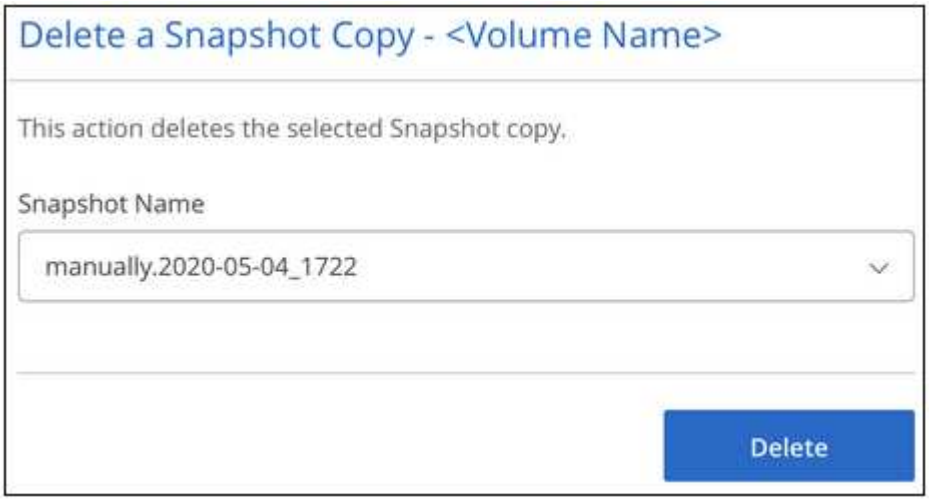
Lorsque vous souhaitez réactiver la stratégie de snapshot, déplacez le curseur d'activation des snapshots vers la droite et cliquez sur **mettre à jour le volume**.

Supprime un snapshot

Vous pouvez supprimer un snapshot de la page volumes.

Étapes

1. Ouvrir l'environnement de travail.
2. Placez le pointeur de la souris sur le volume et cliquez sur **Supprimer une copie snapshot**.
3. Sélectionnez l'instantané dans la liste déroulante et cliquez sur **Supprimer**.



4. Dans la boîte de dialogue de confirmation, cliquez sur **Supprimer**.

Restaurez un volume à partir d'un snapshot

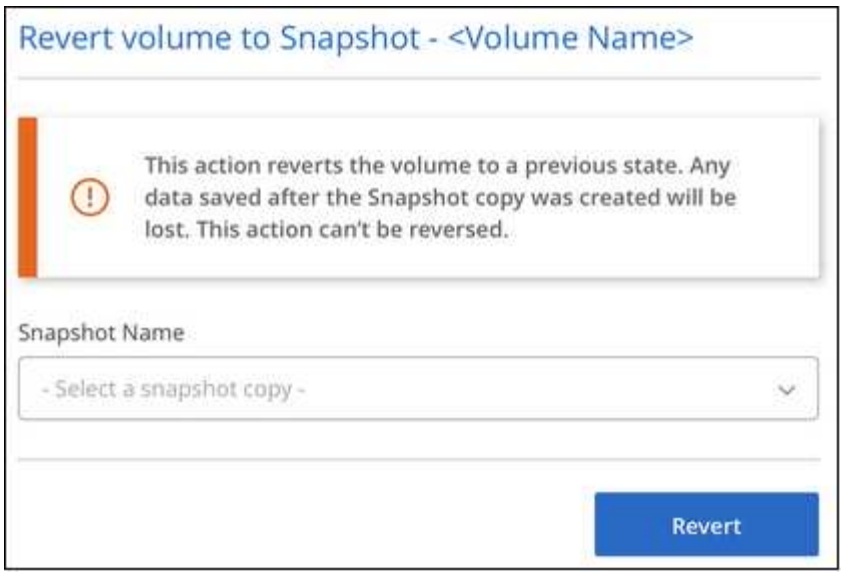
Vous pouvez restaurer un volume à un point antérieur à partir d'un snapshot existant.

Lorsque vous restaurez un volume, le contenu de l'instantané remplace la configuration de volume existante. Toute modification apportée aux données du volume après la création de la copie Snapshot est perdue.

Notez que les clients n'ont pas besoin de remonter le volume après la restauration.

Étapes

1. Ouvrir l'environnement de travail.
2. Placez le pointeur de la souris sur le volume et cliquez sur **Revert volume to Snapshot**.
3. Sélectionnez le snapshot que vous souhaitez utiliser pour restaurer le volume existant dans la liste déroulante et cliquez sur **Revert**.



Référence

Les niveaux de service et la capacité allouée

Le coût de Cloud Volumes Service pour AWS repose sur *niveau de service* et sur la *capacité* allouée que vous avez sélectionnées. Le choix du niveau de service et de la capacité adaptés vous aide à répondre à vos besoins de stockage à moindre coût.

Considérations

Les besoins en matière de stockage sont les suivants :

- Capacité_de_stockage_ pour le stockage des données
- Le stockage *Bandwidth* pour l'interaction avec les données

Si vous utilisez plus d'espace de stockage que la capacité sélectionnée pour ce volume, les considérations suivantes s'appliquent :

- Vous serez facturé pour la capacité de stockage supplémentaire que vous consommez au prix défini par votre niveau de service.
- La quantité de bande passante de stockage disponible pour le volume n'augmente que lorsque vous augmentez la taille de la capacité allouée ou modifiez le niveau de service.

Niveaux de services

Cloud Volumes Service pour AWS prend en charge trois niveaux de service. Vous spécifiez votre niveau de service lors de la création ou de la modification du volume.

Les niveaux de service répondent à différents besoins en capacité de stockage et bande passante de stockage :

- **Standard** (capacité)

  Si vous souhaitez obtenir de la capacité au coût le plus faible et que vos besoins en bande passante sont limités, le niveau de service Standard peut vous convenir le mieux. C'est un exemple en utilisant le volume

comme cible de sauvegarde.

    - Bande passante : 16 Ko de bande passante par Go capacité provisionnée

- **Premium** (équilibre entre capacités et performances)

  Si votre application a un besoin équilibré en capacité de stockage et en bande passante, le niveau de service Premium peut vous être le plus adapté. Ce niveau coûte moins cher par Mo/s que le niveau de service standard, et il est également moins cher par Go de capacité de stockage que le niveau de service extrême.

    - Bande passante : 64 Ko de bande passante par Go capacité provisionnée

- **Extrême** (performances)

  Le niveau de service extrême est le moins cher en bande passante de stockage. Si votre application exige de la bande passante de stockage sans les besoins associés en capacité de stockage importante, le niveau de service extrême peut vous convenir.

    - Bande passante : 128 Ko de bande passante par Go capacité provisionnée

Capacité allouée

Vous spécifiez la capacité allouée au volume lors de la création ou de la modification du volume.

Même si vous sélectionnez votre niveau de service en fonction de vos besoins généraux, vous devez sélectionner la taille de votre capacité allouée en fonction des besoins spécifiques des applications, par exemple :

- Quantité d'espace de stockage dont les applications ont besoin
- La bande passante de stockage requise par seconde pour les applications ou les utilisateurs

La capacité allouée est spécifiée en GB. La capacité allouée d'un volume peut être réglée dans la plage de 100 Go à 100,000 Go (soit 100 To).

Nombre d'inodes

Les volumes inférieurs ou égaux à 1 To peuvent utiliser jusqu'à 20 millions d'inodes. Le nombre d'inodes augmente de 20 millions pour chaque To que vous allouez, jusqu'à un maximum de 100 millions d'inodes.

- <= 1 To = 20 millions d'inodes
- Environ 1 To à 2 To = 40 millions d'inodes
- Pour environ 2 To à 3 To = 60 millions d'inodes
- Pour 3 To à 4 To = 80 millions d'inodes
- Pour 4 To à 100 To = 100 millions d'inodes

La bande passante

La combinaison du niveau de service et de la capacité allouée que vous sélectionnez détermine la bande passante maximale du volume.

Si vos applications ou utilisateurs ont besoin de plus de bande passante que vos sélections, vous pouvez modifier le niveau de service ou augmenter la capacité allouée. Les modifications n'affectent pas l'accès aux données.

Sélection du niveau de service et de la capacité allouée

Pour sélectionner le niveau de service le plus approprié et la capacité allouée à vos besoins, vous devez connaître la capacité et la bande passante dont vous avez besoin au maximum ou à la périphérie.

Liste des niveaux de service et des capacités allouées

La colonne la plus à gauche indique la capacité, et les autres colonnes définissent les Mo/s disponibles à chaque point de capacité en fonction du niveau de service.

Voir "Tarification de l'abonnement aux contrats" et "Facturation des abonnements" pour en savoir plus sur les prix.

Capacité (To)	Standard (Mo/s)	Premium (Mo/s)	Extreme (Mbit/s)
0.1 (100 GO)	1.6	6.4	12.8
1	16	64	128
2	32	128	256
3	48	192	384
4	64	256	512
5	80	320	640
6	96	384	768
7	112	448	896
8	128	512	1,024
9	144	576	1,152
10	160	640	1,280
11	176	704	1,408
12	192	768	1,536
13	208	832	1,664
14	224	896	1,792
15	240	960	1,920
16	256	1,024	2,048
17	272	1,088	2,176
18	288	1,152	2,304
19	304	1,216	2,432
20	320	1,280	2,560
21	336	1,344	2,688
22	352	1,408	2,816
23	368	1,472	2,944
24	384	1,536	3,072

Capacité (To)	Standard (Mo/s)	Premium (Mo/s)	Extreme (Mbit/s)
25	400	1,600	3,200
26	416	1,664	3,328
27	432	1,728	3,456
28	448	1,792	3,584
29	464	1,856	3,712
30	480	1,920	3,840
31	496	1,984	3,968
32	512	2,048	4,096
33	528	2,112	4,224
34	544	2,176	4,352
35	560	2,240	4,480
36	576	2,304	4,500
37	592	2,368	4,500
38	608	2,432	4,500
39	624	2,496	4,500
40	640	2,560	4,500
41	656	2,624	4,500
42	672	2,688	4,500
43	688	2,752	4,500
44	704	2,816	4,500
45	720	2,880	4,500
46	736	2,944	4,500
47	752	3,008	4,500
48	768	3,072	4,500
49	784	3,136	4,500
50	800	3,200	4,500
51	816	3,264	4,500
52	832	3,328	4,500
53	848	3,392	4,500
54	864	3,456	4,500
55	880	3,520	4,500
56	896	3,584	4,500
57	912	3,648	4,500

Capacité (To)	Standard (Mo/s)	Premium (Mo/s)	Extreme (Mbit/s)
58	928	3,712	4,500
59	944	3,776	4,500
60	960	3,840	4,500
61	976	3,904	4,500
62	992	3,968	4,500
63	1,008	4,032	4,500
64	1,024	4,096	4,500
65	1,040	4,160	4,500
66	1,056	4,224	4,500
67	1,072	4,288	4,500
68	1,088	4,352	4,500
69	1,104	4,416	4,500
70	1,120	4,480	4,500
71	1,136	4,500	4,500
72	1,152	4,500	4,500
73	1,168	4,500	4,500
74	1,184	4,500	4,500
75	1,200	4,500	4,500
76	1,216	4,500	4,500
77	1,232	4,500	4,500
78	1,248	4,500	4,500
79	1,264	4,500	4,500
80	1,280	4,500	4,500
81	1,296	4,500	4,500
82	1,312	4,500	4,500
83	1,328	4,500	4,500
84	1,344	4,500	4,500
85	1,360	4,500	4,500
86	1,376	4,500	4,500
87	1,392	4,500	4,500
88	1,408	4,500	4,500
89	1,424	4,500	4,500
90	1,440	4,500	4,500

Capacité (To)	Standard (Mo/s)	Premium (Mo/s)	Extreme (Mbit/s)
91	1,456	4,500	4,500
92	1,472	4,500	4,500
93	1,488	4,500	4,500
94	1,504	4,500	4,500
95	1,520	4,500	4,500
96	1,536	4,500	4,500
97	1,552	4,500	4,500
98	1,568	4,500	4,500
99	1,584	4,500	4,500
100	1,600	4,500	4,500

Exemple 1

Par exemple, votre application requiert une capacité de 25 To et 100 Mo/s de bande passante. Avec une capacité de 25 To, le niveau de service standard fournira 400 Mo/s de bande passante pour un coût de 2,500 $ (estimation : voir la tarification actuelle), faisant de Standard le niveau de service le plus approprié dans ce cas.

	Standard		Premium		Extreme	
capacity TB	Bandwidth MB/s	Cost	Bandwidth MB/s	Cost	Bandwidth MB/s	Cost
24	384	$2,400	1,536	$4,800	3,072	$7,200
25	400	$2,500	1,600	$5,000	3,200	$7,500
26	416	$2,600	1,664	$5,200	3,328	$7,800

Exemple 2

Par exemple, votre application a besoin d'une capacité de 12 To et de 800 Mo/s de bande passante maximale. Même si le niveau de service extrême peut satisfaire aux exigences de l'application avec le seuil de 12 To, il est plus économique (estimation : voir la tarification actuelle) de sélectionner 13 To au niveau de service Premium.

	Standard		Premium		Extreme	
capacity TB	Bandwidth MB/s	Cost	Bandwidth MB/s	Cost	Bandwidth MB/s	Cost
12	192	$1,200	768	$2,400	1,536	$3,600
13	208	$1,300	832	$2,600	1,664	$3,900
14	224	$1,400	896	$2,800	1,792	$4,200

Paramètres des groupes de sécurité AWS pour les serveurs Windows AD

Si vous utilisez des serveurs Windows Active Directory (AD) avec des volumes clouds,

vous devez vous familiariser avec les paramètres des groupes de sécurité AWS. Les paramètres permettent aux volumes cloud de s'intégrer correctement avec AD.

Par défaut, le groupe de sécurité AWS appliqué à une instance Windows EC2 ne contient aucune règle entrante pour un protocole sauf RDP. Vous devez ajouter des règles aux groupes de sécurité associés à chaque instance Windows AD afin d'activer la communication entrante à partir de Cloud Volumes Service. Les ports requis sont les suivants :

Service	Port	Protocole
SERVICES Web PUBLICITAIRES	9389	TCP
DNS	53	TCP
DNS	53	UDP
ICMPv4	S/O	Réponse écho
Kerberos	464	TCP
Kerberos	464	UDP
Kerberos	88	TCP
Kerberos	88	UDP
LDAP	389	TCP
LDAP	389	UDP
LDAP	3268	TCP
Nom NetBIOS	138	UDP
SAM/LSA	445	TCP
SAM/LSA	445	UDP
Sécurité LDAP	636	TCP
Sécurité LDAP	3269	TCP
w32time	123	UDP

Si vous déployez et gérez vos contrôleurs de domaine d'installation AD et vos serveurs membres sur une instance AWS EC2, vous aurez besoin de plusieurs règles de groupe de sécurité pour autoriser le trafic de Cloud Volumes Service. Voici un exemple de mise en œuvre de ces règles pour les applications AD dans le modèle AWS CloudFormation.

```
{
    "AWSTemplateFormatVersion" : "2010-09-09",
    "Description" : "Security Group for AD",
    "Parameters" :
    {
        "VPC" :
        {
            "Type" : "AWS::EC2::VPC::Id",
            "Description" : "VPC where the Security Group will belong:"
```

```
        },
        "Name" :
        {
            "Type" : "String",
            "Description" : "Name Tag of the Security Group:"
        },
        "Description" :
        {
            "Type" : "String",
            "Description" : "Description Tag of the Security Group:",
            "Default" : "Security Group for Active Directory for CVS "
        },
        "CIDRrangeforTCPandUDP" :
        {
            "Type" : "String",
            "Description" : "CIDR Range for the UDP ports
445,138,464,389,53,123 and for the TCP ports
464,339,3389,3268,88,636,9389,445 and 0-65535: *CIDR range format:
10.0.0.0/24"
        }
    },
    "Resources" :
    {
        "ADSGWest" :
        {
            "Type" : "AWS::EC2::SecurityGroup",
            "Properties" :
            {
                "GroupDescription" : {"Ref" : "Description"},
                "VpcId" : { "Ref" : "VPC" },
                "SecurityGroupIngress" : [
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "445",
                        "ToPort" : "445"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "138",
                        "ToPort" : "138"
                    },
                    {
                        "IpProtocol" : "udp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
```

```
                    "FromPort" : "464",
                    "ToPort" : "464"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "464",
                    "ToPort" : "464"
                },
                {
                    "IpProtocol" : "udp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "389",
                    "ToPort" : "389"
                },
                {
                    "IpProtocol" : "udp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "53",
                    "ToPort" : "53"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "339",
                    "ToPort" : "339"
                },
                {
                    "IpProtocol" : "udp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "123",
                    "ToPort" : "123"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "3389",
                    "ToPort" : "3389"
                },
                {
                    "IpProtocol" : "tcp",
                    "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                    "FromPort" : "3268",
                    "ToPort" : "3268"
                },
                {
```

```
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "88",
                        "ToPort" : "88"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "636",
                        "ToPort" : "636"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "3269",
                        "ToPort" : "3269"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "53",
                        "ToPort" : "53"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "0",
                        "ToPort" : "65535"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "9389",
                        "ToPort" : "9389"
                    },
                    {
                        "IpProtocol" : "tcp",
                        "CidrIp" : {"Ref" : "CIDRrangeforTCPandUDP"},
                        "FromPort" : "445",
                        "ToPort" : "445"
                    }
                ]
            }
        }
    },
    "Outputs" :
```

```
    {
        "SecurityGroupID" :
        {
            "Description" : "Security Group ID",
            "Value" : { "Ref" : "ADSGWest" }
        }
    }
}
```

Cloud Volumes Service pour GCP

En savoir plus sur Cloud Volumes Service pour Google Cloud

NetApp Cloud Volumes Service pour Google Cloud vous permet d'ajouter rapidement des workloads multiprotocoles et de créer et déployer aussi bien des applications Windows que UNIX.

Fonctionnalités clés :

- Migrez les données entre votre infrastructure sur site et Google Cloud.
- Provisionnez des volumes de 1 à 100 Tio en quelques secondes.
- Prise en charge multiprotocole (vous pouvez créer un volume NFS ou SMB).
- Protection des données grâce à des copies Snapshot automatisées et efficaces
- Accélérez le développement d'applications grâce au clonage rapide.

Le coût

Les volumes créés par Cloud Volumes Service pour Google Cloud sont facturés pour votre abonnement au service, et non par l'intermédiaire de Cloud Manager.

"Voir les prix"

Il n'y a aucun frais pour découvrir une région ou un volume Cloud Volumes Service pour Google Cloud depuis Cloud Manager.

Régions prises en charge

"Consultez les régions Google Cloud prises en charge."

Avant de commencer

Cloud Manager peut découvrir les abonnements et volumes Cloud Volumes Service pour GCP existants. Voir la "Documentation NetApp Cloud Volumes Service pour Google Cloud" si vous n'avez pas encore configuré votre abonnement.

Obtenir de l'aide

Utilisez la discussion de chat Cloud Manager pour toute question d'ordre général sur le fonctionnement de Cloud Volumes Service dans Cloud Manager.

Pour toute question d'ordre général sur Cloud Volumes Service pour Google Cloud, envoyez un e-mail à l'équipe Google Cloud de NetApp à l'adresse gcinfo@netapp.com.

Pour tout problème technique lié à vos volumes cloud, vous pouvez créer un dossier de support technique à partir de Google Cloud Console. Voir "obtenir de l'aide" pour plus d'informations.

Limites

- Cloud Manager ne prend pas en charge la réplication des données entre les environnements de travail lors de l'utilisation de volumes Cloud Volumes Service.
- La suppression de votre abonnement Cloud Volumes Service pour Google Cloud de Cloud Manager n'est pas prise en charge. Pour ce faire, vous pouvez utiliser la console Google Cloud.

Liens connexes

- "NetApp Cloud Central : Cloud Volumes Service pour Google Cloud"
- "Documentation NetApp Cloud Volumes Service pour Google Cloud"

Configuration de Cloud Volumes Service pour Google Cloud

Créez et gérez des volumes et des snapshots à partir d'un environnement de travail Cloud Volumes Service pour Google Cloud dans Cloud Manager.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou passez à la section suivante pour obtenir plus d'informations.

Activez l'API Cloud Volumes Service

Depuis Google, activez l'API Cloud Volumes Service pour GCP afin que Cloud Manager puisse gérer l'abonnement et les volumes cloud.

Créez un compte de service GCP et téléchargez les identifiants

Depuis Google, créez un compte de service GCP et un rôle afin de permettre à Cloud Manager d'accéder à votre compte Cloud Volumes Service pour GCP.

Créez un environnement de travail Cloud Volumes Service pour GCP

Dans Cloud Manager, cliquez sur **Ajouter un environnement de travail** > **Google Cloud** > **Cloud Volumes Service**, puis donnez des détails sur le compte de service et le projet Google Cloud.

Activez l'API Cloud Volumes Service

Dans Google Cloud Shell, exécutez la commande suivante pour activer l'API Cloud Volumes Service :

```
gcloud --project=<my-cvs-project> services enable cloudvolumesgcp-api.netapp.com
```

Donnez un accès à Cloud Manager au compte Cloud Volumes Service pour GCP

Pour que Cloud Manager puisse accéder à votre projet Google Cloud, vous devez effectuer les tâches suivantes :

- Créez un nouveau compte de service
- Ajoutez le nouveau membre du compte de service à votre projet et attribuez-lui des rôles (autorisations) spécifiques.
- Créez et téléchargez une paire de clés pour le compte de service utilisé pour s'authentifier auprès de Google

Étapes

1. Dans Google Cloud Console, accédez à la page **Service Accounts**.
2. Cliquez sur **sélectionnez un projet**, choisissez votre projet et cliquez sur **Ouvrir**.
3. Cliquez sur **Créer un compte de service**, entrez le nom du compte de service (nom d'affichage convivial) et la description, puis cliquez sur **Créer**.
4. Dans la page *IAM*, cliquez sur **Ajouter** et remplissez les champs de la page *Ajouter des membres* :
   a. Dans le champ nouveaux membres, saisissez l'ID de compte de service complet, par exemple user1-service-account-cvs@project1.iam.gserviceaccount.com.
   b. Ajouter ces rôles :
      - *NetApp Cloud volumes Admin*
      - *Compute Network Viewer*
      - *Visualiseur de dossiers*
   c. Cliquez sur **Enregistrer**.
5. Dans la page *Service account details*, cliquez sur **Add key > Create New key**.
6. Sélectionnez **JSON** comme type de clé et cliquez sur **Create**.

   En cliquant sur **Créer**, votre nouvelle paire de clés publique/privée est générée et téléchargée sur votre système. Il sert de seule copie de la clé privée. Stockez ce fichier de façon sécurisée car il peut être utilisé pour s'authentifier en tant que compte de service.

Pour obtenir des instructions détaillées, consultez les rubriques relatives à Google Cloud "Création et gestion des comptes de service", "Octroi, modification et révocation de l'accès aux ressources", et "Création et gestion des clés de compte de service".

Créez un environnement de travail Cloud Volumes Service pour GCP

Configuration d'un environnement de travail Cloud Volumes Service pour GCP dans Cloud Manager, pour que vous puissiez commencer à créer des volumes

Que vous ayez déjà créé des volumes depuis Google Cloud Console ou que vous vous abonnez à Cloud Volumes Service pour GCP et que vous ne possédez pas encore de volumes, la première étape consiste à créer un environnement de travail pour les volumes basés sur votre abonnement GCP.

Si des volumes cloud existent déjà pour cet abonnement, les volumes apparaîtront dans le nouvel environnement de travail. Si vous n'avez pas encore ajouté de volumes cloud pour l'abonnement GCP, cela se produit une fois que vous avez créé le nouvel environnement de travail.

Si vous disposez d'abonnements et de volumes dans plusieurs projets GCP, vous devez effectuer cette tâche pour chaque projet.

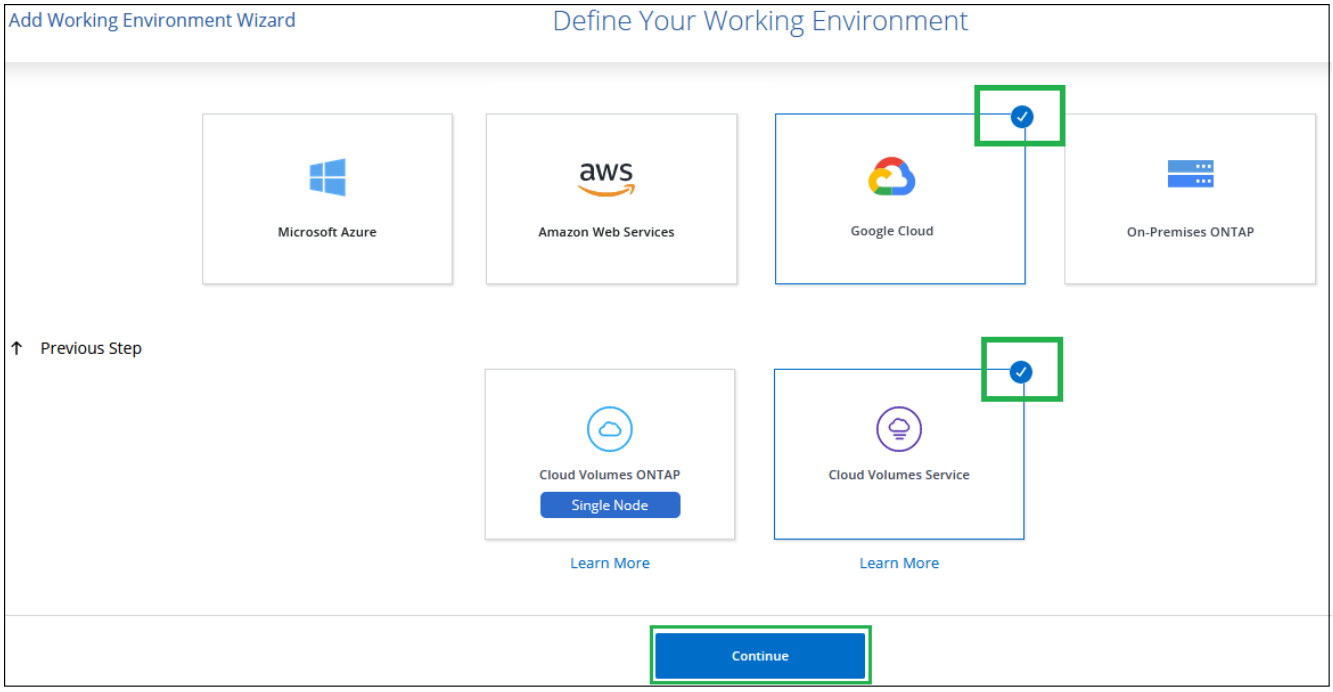
Avant de commencer

Vous devez disposer des informations suivantes lors de l'ajout d'un abonnement pour chaque projet :

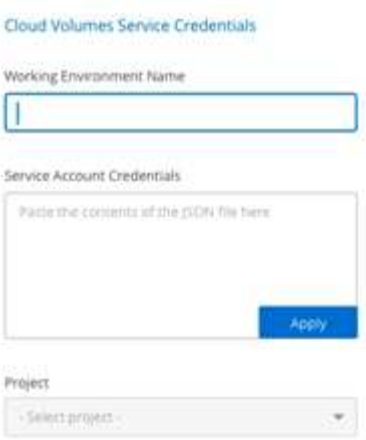
- Identifiants de compte de service (clé privée JSON que vous avez téléchargée)
- Nom du projet

Étapes

1. Dans Cloud Manager, ajoutez un nouvel environnement de travail, sélectionnez l'emplacement **Google Cloud**, puis cliquez sur **Continuer**.
2. Sélectionnez **Cloud Volumes Service** et cliquez sur **Continuer**.



3. Fournir des informations sur votre abonnement Cloud Volumes Service :
   a. Entrez le nom de l'environnement de travail que vous souhaitez utiliser.
   b. Copiez/collez la clé privée JSON que vous avez téléchargée au cours des étapes précédentes.
   c. Sélectionnez le nom de votre projet Google Cloud.
   d. Cliquez sur **Ajouter**.



Résultat

Cloud Manager affiche votre environnement de travail Cloud Volumes Service pour Google Cloud.

Si des volumes cloud existent déjà pour cet abonnement, ils apparaissent dans le nouvel environnement de travail, comme indiqué dans la capture d'écran. Vous pouvez ajouter des volumes cloud supplémentaires à partir de Cloud Manager.

Si aucun volume cloud n'existe pour cet abonnement, créez-les dès maintenant.

Et la suite ?

"Démarrage de la création et de la gestion des volumes".

Création et gestion de volumes pour Cloud Volumes Service pour Google Cloud

Cloud Manager vous permet de créer des volumes cloud basés sur votre "Cloud Volumes Service pour Google Cloud" abonnement. Vous pouvez également modifier certains attributs d'un volume, obtenir les commandes de montage appropriées, créer des copies Snapshot et supprimer des volumes cloud.

Création de volumes cloud

Vous pouvez créer des volumes NFS ou SMB dans un compte Cloud Volumes Service pour Google Cloud existant ou nouveau. Les volumes cloud prennent actuellement en charge NFSv3 et NFSv4.1 pour les clients Linux et UNIX, et SMB 3.x pour les clients Windows.

Avant de commencer

- Si vous souhaitez utiliser SMB dans GCP, vous devez avoir configuré DNS et Active Directory.
- Lorsque vous prévoyez de créer un volume SMB, vous devez disposer d'un serveur Windows Active Directory disponible auquel vous pouvez vous connecter. Vous entrez ces informations lors de la création

du volume. Assurez-vous également que l'utilisateur administrateur peut créer un compte machine dans le chemin d'unité organisationnelle spécifié.

Étapes

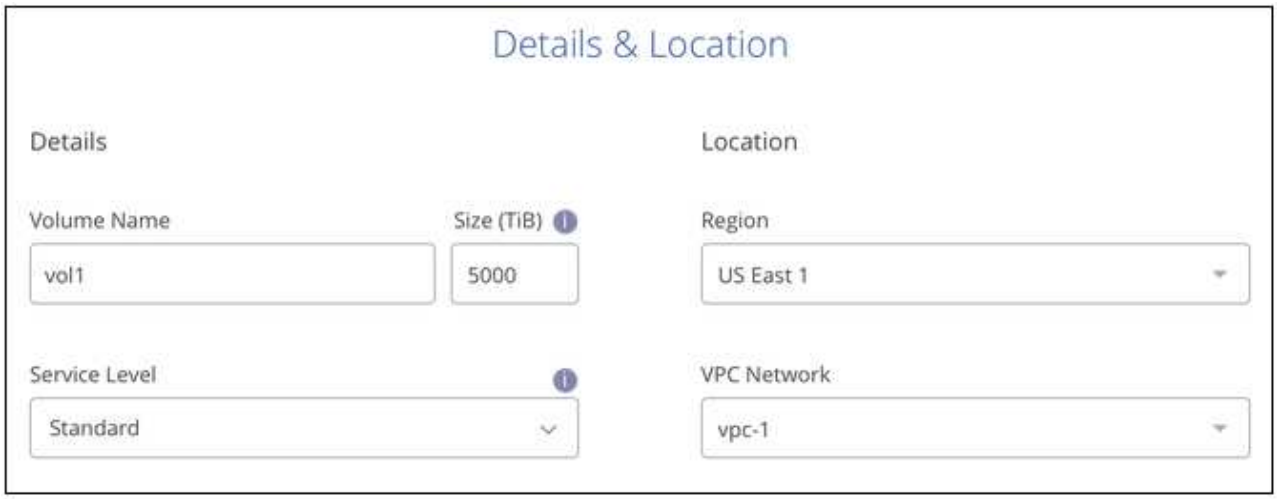
1. Sélectionnez l'environnement de travail et cliquez sur **Ajouter un nouveau volume**.
2. Sur la page Détails et emplacement, saisissez les détails du volume :
   a. Entrez un nom pour le volume.
   b. Spécifiez une taille dans la plage de 1 Tio (1024 Gio) à 100 Tio.

      "En savoir plus sur la capacité allouée".

   c. Spécifier un niveau de service : standard, Premium ou Extreme.

      "En savoir plus sur les niveaux de service".

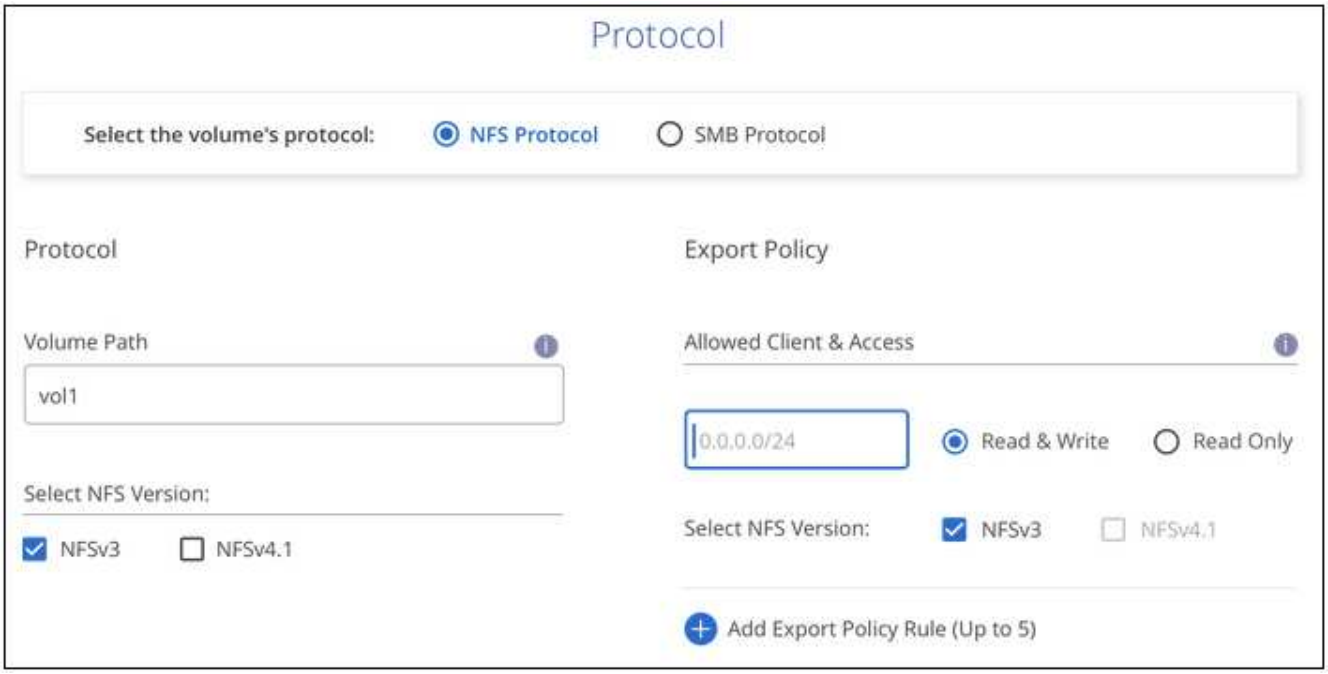
   d. Sélectionnez la région Google Cloud.
   e. Sélectionnez le réseau VPC à partir duquel le volume sera accessible. Notez que le VPC ne peut pas être modifié ou modifié une fois le volume créé.
   f. Cliquez sur **Continuer**.



3. Sur la page Protocol, sélectionnez NFS ou SMB, puis définissez les détails. Les entrées requises pour NFS et SMB sont répertoriées dans les sections ci-après.
4. Pour NFS :
   a. Dans le champ chemin du volume, indiquez le nom de l'exportation de volume que vous verrez lors du montage du volume.
   b. Sélectionnez NFS v3, NFS v4.1 ou les deux en fonction de vos exigences.
   c. Vous pouvez également créer une export-policy pour identifier les clients pouvant accéder au volume. Spécifiez :
      - Clients autorisés à l'aide d'une adresse IP ou d'un routage inter-domaines sans classe (CIDR).
      - Droits d'accès en lecture et écriture ou lecture seule.
      - Protocole d'accès (ou protocoles si le volume autorise l'accès NFS v3 et NFS v4.1) utilisé pour les utilisateurs.

- Cliquez sur **+ Ajouter règle de stratégie d'exportation** si vous souhaitez définir des règles de stratégie d'exportation supplémentaires.

  L'image suivante montre la page Volume remplie pour le protocole NFS :



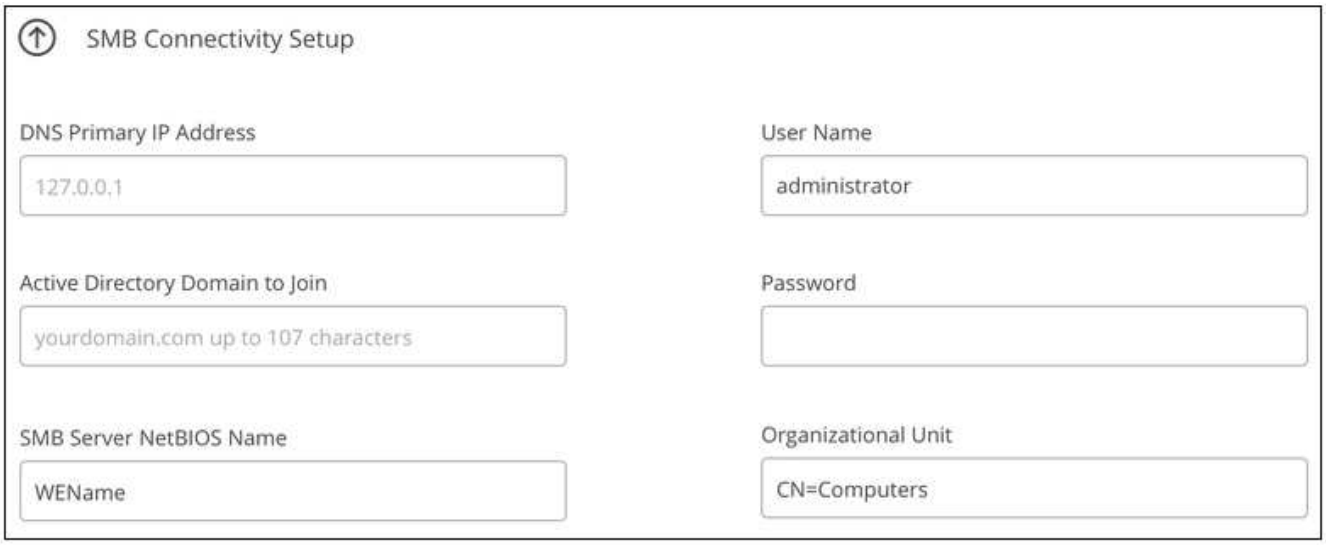
5. Pour SMB :

   a. Dans le champ chemin du volume, indiquez le nom de l'exportation de volume que vous verrez lorsque vous montez le volume et cliquez sur **Continuer**.

   b. Si Active Directory a été configuré, la configuration s'affiche. S'il s'agit du premier volume en cours de configuration et qu'aucun Active Directory n'a été configuré, vous pouvez activer le chiffrement de session SMB dans la page d'installation de la connectivité SMB :

Champ	Description
Adresse IP principale DNS	Les adresses IP des serveurs DNS qui fournissent une résolution de nom pour le serveur SMB. Utilisez une virgule pour séparer les adresses IP lorsque vous faites référence à plusieurs serveurs, par exemple 172.31.25.223, 172.31.2.74.
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) que vous souhaitez que le serveur SMB rejoint.
Nom NetBIOS du serveur SMB	Nom NetBIOS du serveur SMB qui sera créé.
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Unité organisationnelle	Unité organisationnelle au sein du domaine AD à associer au serveur SMB. La valeur par défaut est CN=Computers pour les connexions à votre propre serveur Windows Active Directory.

L'image suivante montre la page Volume remplie pour le protocole SMB :



6. Cliquez sur **Continuer**.
7. Si vous souhaitez créer le volume à partir d'un snapshot d'un volume existant, sélectionnez-le dans la liste déroulante Nom de snapshot. Sinon, cliquez simplement sur **Continuer**.
8. Sur la page règle Snapshot, vous pouvez activer Cloud Volumes Service pour créer des copies snapshot de vos volumes selon un planning. Pour ce faire, vous pouvez déplacer le sélecteur vers la droite ou modifier le volume ultérieurement pour définir la stratégie de snapshots.

   Voir "Création d'une règle Snapshot" pour plus d'informations sur la fonctionnalité de snapshot.

9. Cliquez sur **Ajouter un volume**.

Le nouveau volume est ajouté à l'environnement de travail.

Passez à "Montage du volume cloud".

Montez les volumes cloud

Accédez aux instructions de montage depuis Cloud Manager, afin de monter le volume sur un hôte.

Remarque : Veuillez utiliser le protocole/dialecte mis en évidence pris en charge par votre client.

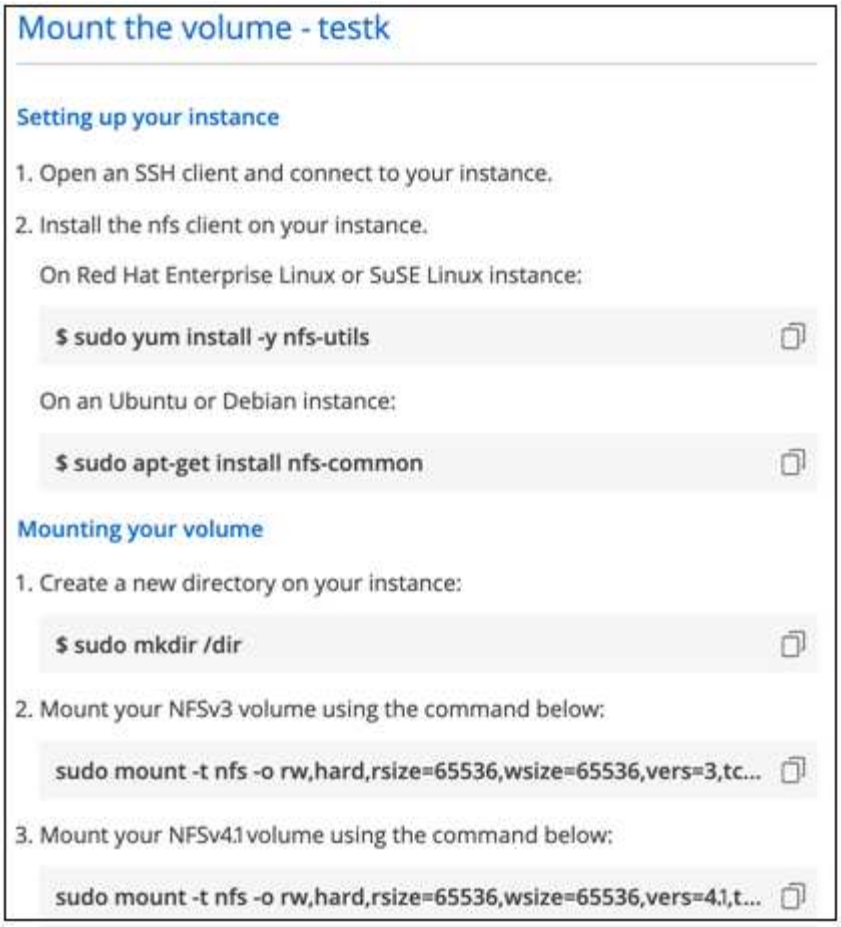
Étapes

1. Ouvrir l'environnement de travail.
2. Placez le pointeur de la souris sur le volume et cliquez sur **montez le volume**.

   Les volumes NFS et SMB affichent des instructions de montage pour ce protocole.

3. Placez le pointeur de la souris sur les commandes et copiez-les dans le presse-papiers pour faciliter ce processus. Ajoutez simplement le répertoire de destination/point de montage à la fin de la commande.

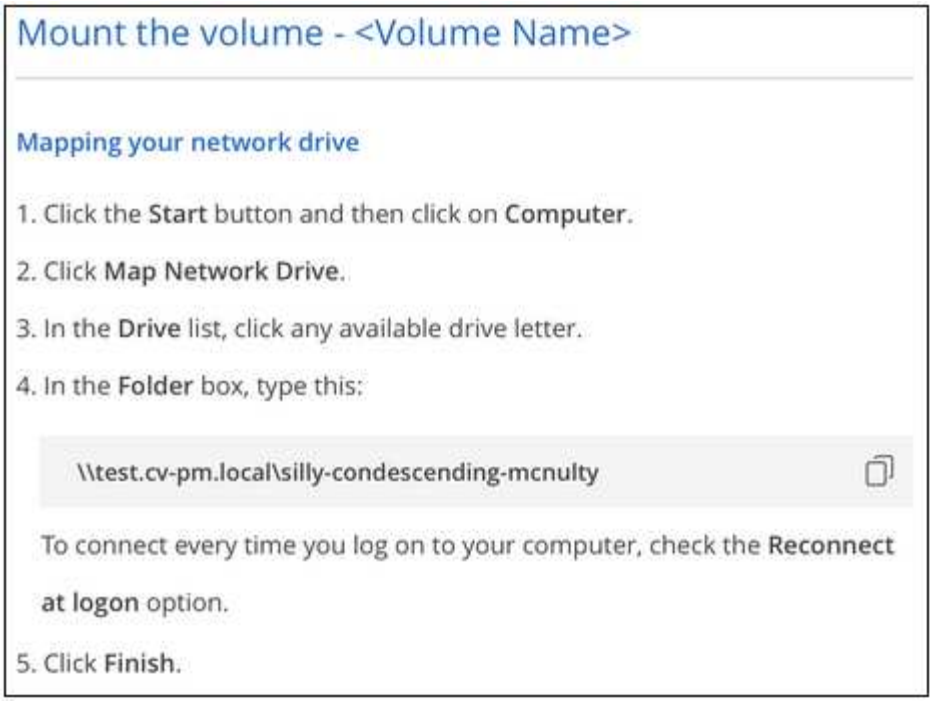
   Exemple NFS:



La taille d'E/S maximale définie par le `rsize` et `wsize` les options sont 1048576. cependant, la version 65536 est la valeur par défaut recommandée pour la plupart des cas d'utilisation.

Notez que les clients Linux seront par défaut sur NFSv4.1 à moins que la version soit spécifiée avec `vers=<nfs_version>` option.

Exemple SMB:



4. Mappez votre lecteur réseau en suivant les instructions de montage de votre instance.

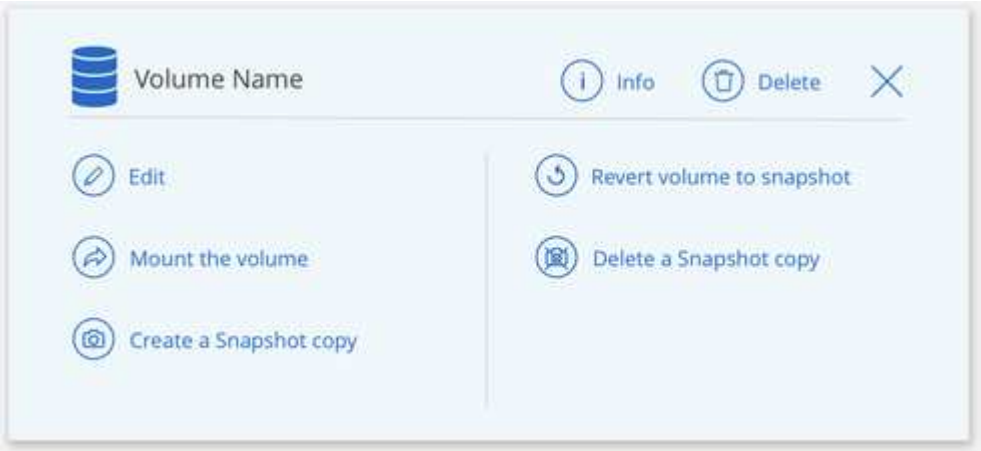
   Après avoir terminé les étapes des instructions de montage, vous avez correctement monté le volume cloud sur votre instance GCP.

Gérer les volumes existants

Vous pouvez gérer les volumes existants à mesure que vos besoins de stockage changent. Vous pouvez afficher, modifier, restaurer et supprimer des volumes.

Étapes

1. Ouvrir l'environnement de travail.
2. Placez le pointeur de la souris sur le volume.



3. Gérez vos volumes :

Tâche	Action
Afficher des informations sur un volume	Cliquez sur **Info**.
Modification d'un volume (y compris la règle Snapshot)	a. Cliquez sur **Modifier**. b. Modifiez les propriétés du volume, puis cliquez sur **mettre à jour**.
Procurez-vous la commande NFS ou SMB mount	a. Cliquez sur **montez le volume**. b. Cliquez sur **Copier** pour copier la ou les commandes.
Créez une copie Snapshot à la demande	a. Cliquez sur **Créer une copie snapshot**. b. Modifiez le nom, si nécessaire, puis cliquez sur **Créer**.
Remplacez le volume par le contenu d'une copie Snapshot	a. Cliquez sur **revenir au snapshot**. b. Sélectionnez une copie Snapshot et cliquez sur **Restaurer**.
Supprimez une copie Snapshot	a. Cliquez sur **Supprimer une copie snapshot**. b. Sélectionnez l'instantané et cliquez sur **Supprimer**. c. Cliquez à nouveau sur **Supprimer** lorsque vous êtes invité à confirmer.
Supprimer un volume	a. Démonter le volume de tous les clients : ◦ Sur les clients Linux, utilisez `umount` commande. ◦ Sur les clients Windows, cliquez sur **déconnecter le lecteur réseau**. b. Sélectionnez un volume, puis cliquez sur **Supprimer**. c. Cliquez à nouveau sur **Supprimer** pour confirmer.

Supprimez Cloud Volumes Service de Cloud Manager

Vous pouvez supprimer un abonnement Cloud Volumes Service pour Google Cloud et tous les volumes existants depuis Cloud Manager. Les volumes ne sont pas supprimés, mais ils sont simplement supprimés de l'interface Cloud Manager.

Étapes

1. Ouvrir l'environnement de travail.
2. Cliquez sur le bouton En haut de la page, cliquez sur **Supprimer Cloud Volumes Service**.
3. Dans la boîte de dialogue de confirmation, cliquez sur **Supprimer**.

Gérer la configuration d'Active Directory

Si vous modifiez vos serveurs DNS ou votre domaine Active Directory, vous devez modifier le serveur SMB dans Cloud volumes Services afin qu'il puisse continuer à fournir du stockage aux clients.

Étapes

1. Ouvrir l'environnement de travail.
2. Cliquez sur le bouton En haut de la page, cliquez sur **gérer Active Directory**. Si aucun Active Directory n'est configuré, vous pouvez en ajouter un maintenant. Si l'un d'eux est configuré, vous pouvez modifier ou supprimer les paramètres à l'aide du bouton.
3. Spécifiez les paramètres du serveur SMB :

Champ	Description
Adresse IP principale DNS	Les adresses IP des serveurs DNS qui fournissent une résolution de nom pour le serveur SMB. Utilisez une virgule pour séparer les adresses IP lorsque vous faites référence à plusieurs serveurs, par exemple 172.31.25.223, 172.31.2.74.
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) que vous souhaitez que le serveur SMB rejoint.
Nom NetBIOS du serveur SMB	Nom NetBIOS du serveur SMB qui sera créé.
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Unité organisationnelle	Unité organisationnelle au sein du domaine AD à associer au serveur SMB. La valeur par défaut est CN=Computers pour les connexions à votre propre serveur Windows Active Directory.

4. Cliquez sur **Enregistrer** pour enregistrer vos paramètres.

Gestion des copies Snapshot de Cloud volumes

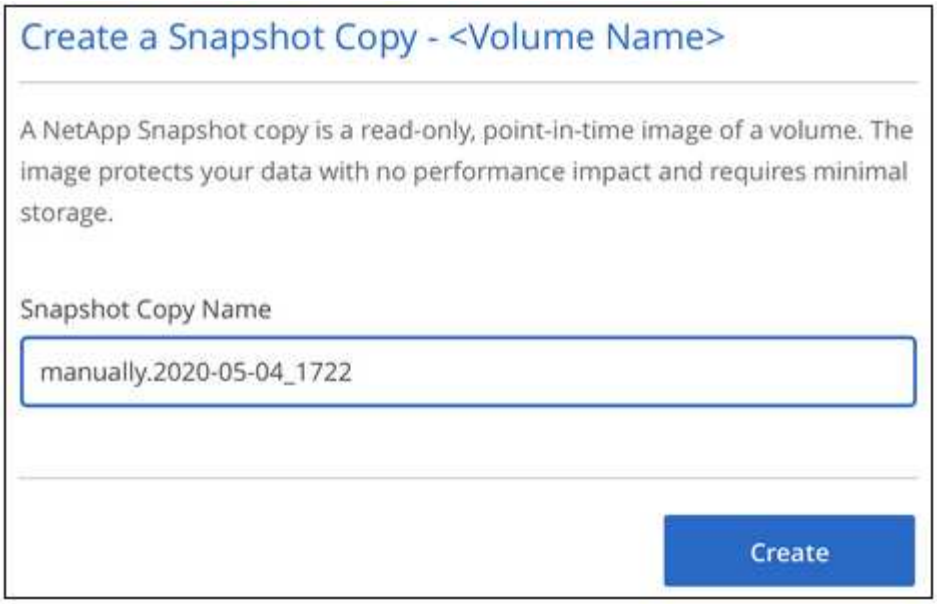
Vous pouvez créer une règle Snapshot pour chaque volume, de sorte que vous puissiez récupérer ou restaurer l'intégralité du contenu d'un volume à partir d'une version antérieure. Vous pouvez également créer un snapshot à la demande d'un volume cloud, si nécessaire.

Créer un snapshot à la demande

Vous pouvez créer un snapshot à la demande d'un volume cloud si vous souhaitez créer un snapshot avec l'état actuel du volume.

Étapes

1. Ouvrir l'environnement de travail.
2. Placez le pointeur de la souris sur le volume et cliquez sur **Créer une copie snapshot**.
3. Entrez un nom pour le snapshot ou utilisez le nom généré automatiquement, puis cliquez sur **Créer**.



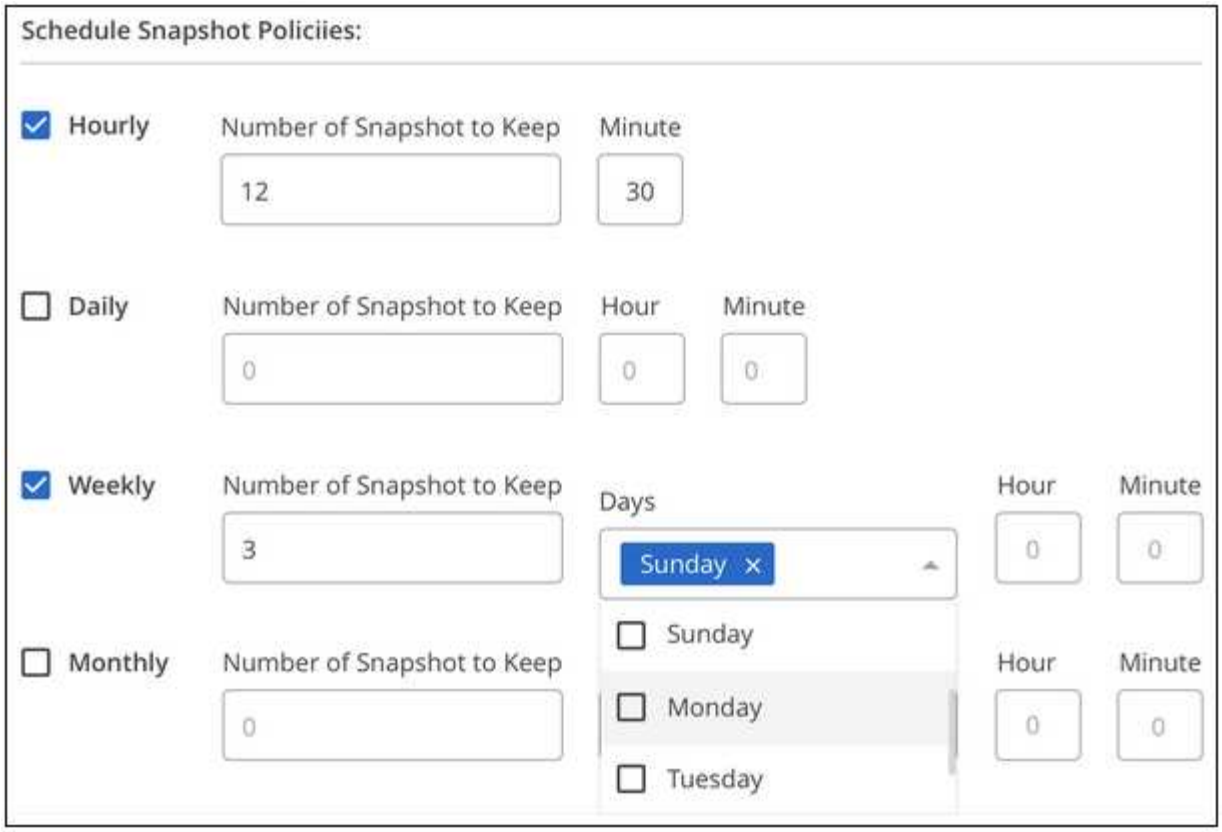
Le snapshot est créé.

Créez ou modifiez une policy de snapshots

Vous pouvez créer ou modifier une règle Snapshot si nécessaire pour un volume cloud. Vous définissez la stratégie de snapshot à partir de l'onglet *Snapshot Policy* lors de la création d'un volume ou lors de la modification d'un volume.

Étapes

1. Ouvrir l'environnement de travail.
2. Placez le pointeur de la souris sur le volume et cliquez sur **Modifier**.
3. Dans l'onglet *Snapshot Policy*, déplacez le curseur activer les snapshots vers la droite.
4. Définir la planification des snapshots :
   a. Sélectionnez la fréquence : **horaire**, **quotidien**, **hebdomadaire** ou **mensuel**
   b. Sélectionnez le nombre de snapshots que vous souhaitez conserver.
   c. Sélectionnez le jour, l'heure et la minute où l'instantané doit être pris.



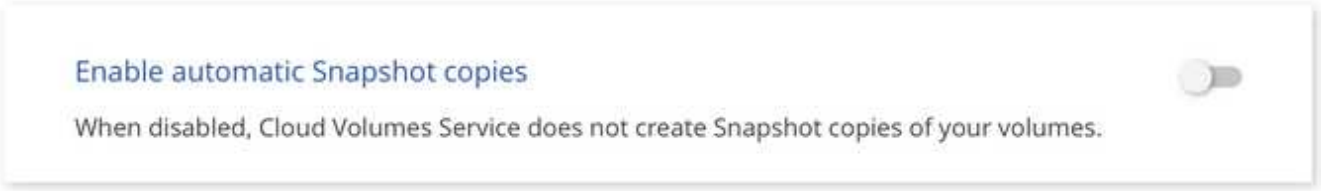
5. Cliquez sur **Ajouter volume** ou **mettre à jour volume** pour enregistrer les paramètres de votre stratégie.

Désactiver une règle Snapshot

Vous pouvez désactiver une stratégie de snapshot pour empêcher la création de snapshots pendant une courte période tout en conservant les paramètres de votre stratégie de snapshot.

Étapes

1. Ouvrir l'environnement de travail.
2. Placez le pointeur de la souris sur le volume et cliquez sur **Modifier**.
3. Dans l'onglet *Snapshot Policy*, déplacez le curseur activer les snapshots vers la gauche.



4. Cliquez sur **mettre à jour le volume**.

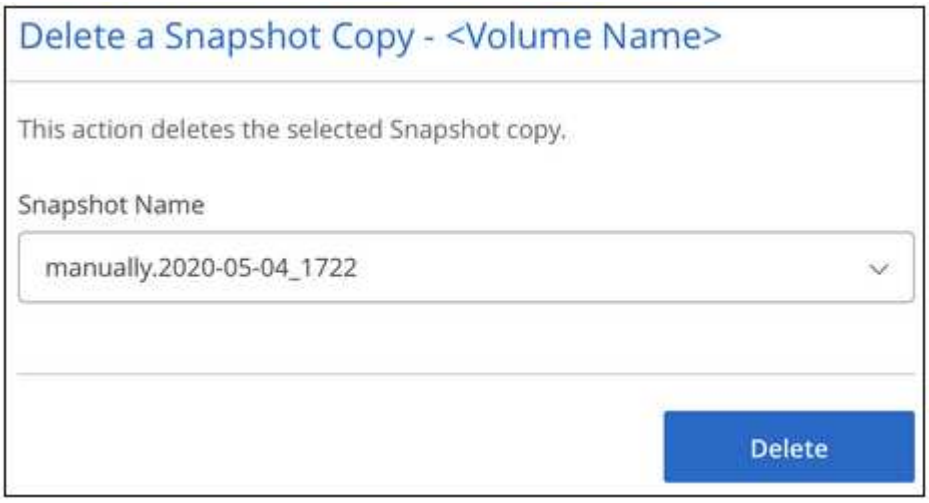
Lorsque vous souhaitez réactiver la stratégie de snapshot, déplacez le curseur d'activation des snapshots vers la droite et cliquez sur **mettre à jour le volume**.

Supprime un snapshot

Vous pouvez supprimer un instantané s'il n'est plus nécessaire.

Étapes

1. Ouvrir l'environnement de travail.
2. Placez le pointeur de la souris sur le volume et cliquez sur **Supprimer une copie snapshot**.
3. Sélectionnez l'instantané dans la liste déroulante et cliquez sur **Supprimer**.



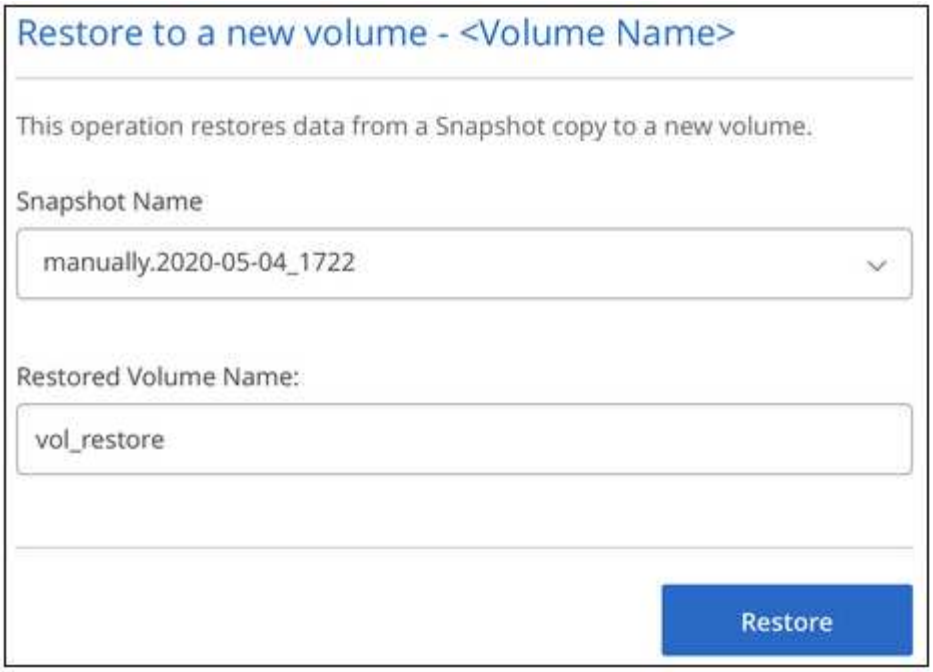
4. Dans la boîte de dialogue de confirmation, cliquez sur **Supprimer**.

Restaurer un snapshot vers un nouveau volume

Vous pouvez restaurer un snapshot vers un nouveau volume si nécessaire.

Étapes

1. Ouvrir l'environnement de travail.
2. Placez le pointeur de la souris sur le volume et cliquez sur **Restaurer un nouveau volume**.
3. Sélectionnez l'instantané que vous souhaitez utiliser pour créer le nouveau volume dans la liste déroulante.
4. Entrez un nom pour le nouveau volume et cliquez sur **Restaurer**.



Le volume est créé dans l'environnement de travail.

5. Si vous devez modifier l'un des attributs de volume, tels que le chemin de volume ou le niveau de service :
   a. Placez le pointeur de la souris sur le volume et cliquez sur **Modifier**.
   b. Effectuez vos modifications et cliquez sur **mettre à jour le volume**.

Une fois que vous avez terminé

Passez à "Montage du volume cloud".

Gérer les clusters ONTAP

Découverte des clusters ONTAP

Cloud Manager peut découvrir les clusters ONTAP dans votre environnement sur site, dans une configuration de stockage privé NetApp et dans IBM Cloud. Il vous permet de ONTAP provisionner le stockage, de répliquer les données, de sauvegarder et de déplacer les données inactives dans le cloud à partir d'un cluster sur site.

Ce dont vous avez besoin

- Connecteur installé dans un fournisseur cloud ou sur site.

  Si vous voulez transférer les données inactives vers le cloud, consultez les conditions du connecteur en fonction de l'emplacement où vous prévoyez d'effectuer le Tiering des données inactives.

  - "En savoir plus sur les connecteurs"
  - "Basculement entre les connecteurs"
  - "Découvrez NetApp Cloud Tiering"
- L'adresse IP de gestion du cluster et le mot de passe du compte utilisateur admin pour ajouter le cluster à Cloud Manager.

  Cloud Manager détecte les clusters ONTAP à l'aide de HTTPS. Si vous utilisez des stratégies de pare-feu personnalisées, elles doivent répondre aux exigences suivantes :

  - L'hôte du connecteur doit autoriser l'accès HTTPS sortant via le port 443.

    Si le connecteur est dans le Cloud, toutes les communications sortantes sont autorisées par le groupe de sécurité prédéfini.

  - Le cluster ONTAP doit autoriser l'accès HTTPS entrant via le port 443.

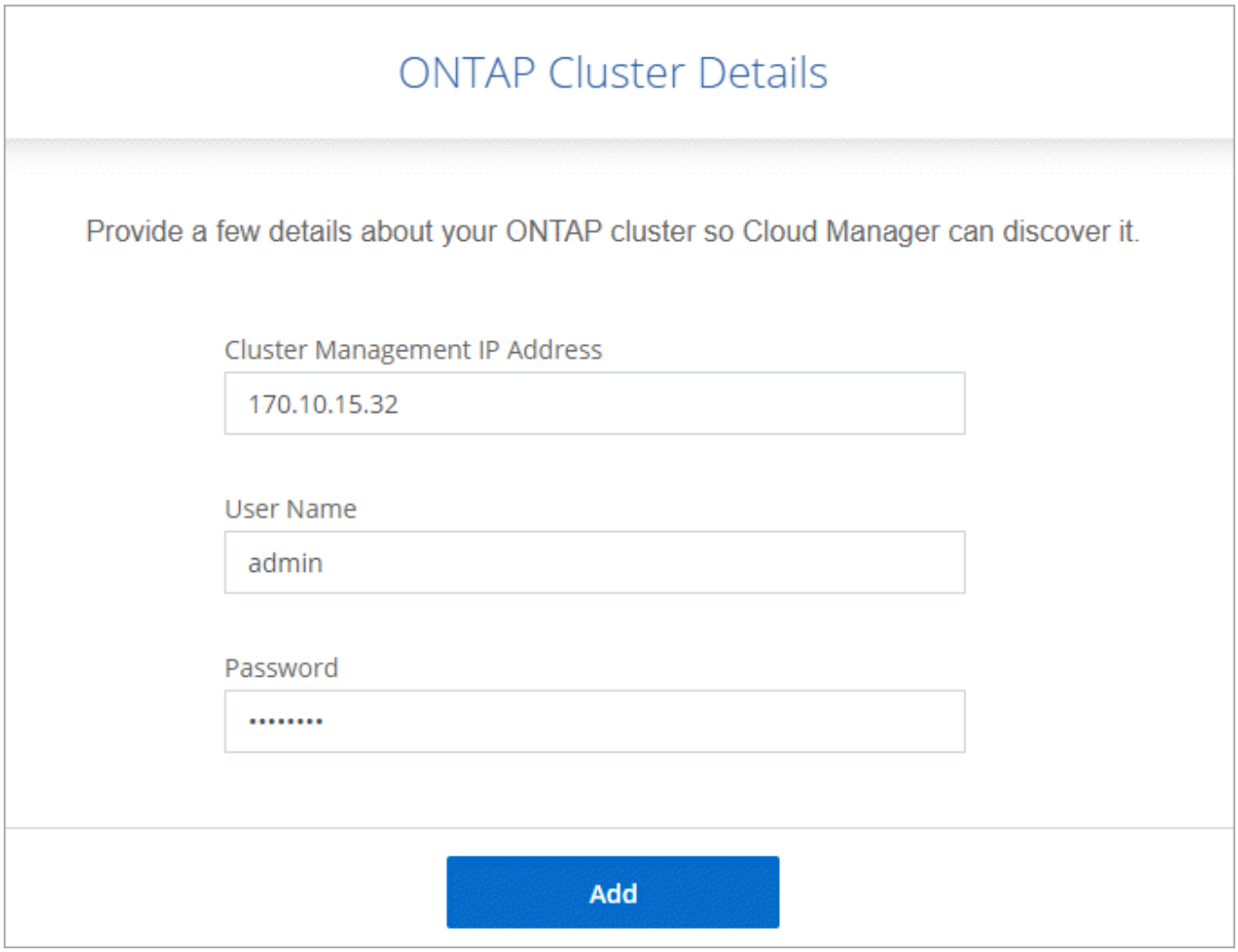
    La stratégie de pare-feu " mgmt " par défaut permet l'accès HTTPS entrant à partir de toutes les adresses IP. Si vous avez modifié cette stratégie par défaut ou si vous avez créé votre propre stratégie de pare-feu, vous devez associer le protocole HTTPS à cette politique et activer l'accès à partir de l'hôte du connecteur.

Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail** et sélectionnez **ONTAP sur site**.
2. Si vous y êtes invité, créez un connecteur.

   Reportez-vous aux liens ci-dessus pour plus de détails.

3. Sur la page **ONTAP Détails du cluster**, entrez l'adresse IP de gestion du cluster, le mot de passe du compte utilisateur admin et l'emplacement du cluster.



4. Sur la page Détails, entrez un nom et une description pour l'environnement de travail, puis cliquez sur **Go**.

Résultat

Cloud Manager détecte le cluster. Vous pouvez désormais créer des volumes, répliquer les données depuis et vers le cluster, configurer le Tiering des données dans le cloud, sauvegarder des volumes dans le cloud et lancer System Manager pour exécuter des tâches avancées.

Gestion du stockage pour les clusters ONTAP

Une fois que vous avez découvert votre cluster ONTAP depuis Cloud Manager, vous pouvez ouvrir l'environnement de travail afin de provisionner et de gérer le stockage.

Création de volumes pour les clusters ONTAP

Cloud Manager vous permet de provisionner des volumes NFS, CIFS et iSCSI sur les clusters ONTAP.

Avant de commencer

Les protocoles de données doivent être définis sur le cluster, à l'aide de System Manager ou de l'interface de ligne de commandes.

Description de la tâche

Vous pouvez créer des volumes sur des agrégats existants. Vous ne pouvez pas créer de nouveaux agrégats

depuis Cloud Manager.

Étapes

1. Sur la page Working Environments, double-cliquez sur le nom du cluster ONTAP sur lequel vous souhaitez provisionner des volumes.
2. Cliquez sur **Ajouter nouveau volume**.
3. Sur la page Créer un nouveau volume, entrez les détails du volume, puis cliquez sur **Créer**.

   Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Stratégie Snapshot	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.
Contrôle d'accès (pour NFS uniquement)	Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, Cloud Manager entre une valeur qui donne accès à toutes les instances du sous-réseau.
Autorisations et utilisateurs/groupes (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur à l'aide du format domaine\nom d'utilisateur.
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de buste hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, sélectionnez-le, cliquez sur IQN cible, puis utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes.
Profil d'utilisation	Les profils d'utilisation définissent les fonctionnalités d'efficacité du stockage NetApp qui sont activées pour un volume.

Réplication des données

Vous pouvez répliquer des données entre les systèmes Cloud Volumes ONTAP et les clusters ONTAP en choisissant une réplication de données unique, qui peut vous aider à déplacer des données vers et depuis le cloud, ou un planning récurrent, qui peut vous aider à la reprise sur incident ou à la conservation à long terme.

"Cliquez ici pour en savoir plus".

Sauvegarde des données

Vous pouvez sauvegarder les données stockées dans votre système ONTAP sur site vers un stockage objet à faible coût dans le cloud à l'aide du service Cloud Manager Backup vers le cloud. Ce service offre des fonctionnalités de sauvegarde et de restauration pour la protection et l'archivage à long terme de vos données cloud.

"Cliquez ici pour en savoir plus".

Tiering des données dans le cloud

Étendez votre data Center au cloud en transférant automatiquement les données inactives des clusters ONTAP au stockage objet.

"Cliquez ici pour en savoir plus".

Sauvegarder dans le cloud

Découvrez la sauvegarde dans le cloud

La sauvegarde dans le cloud est un service complémentaire pour les clusters Cloud Volumes ONTAP et ONTAP sur site qui offre des fonctionnalités de sauvegarde et de restauration pour la protection, ainsi que l'archivage à long terme de vos données cloud. Les sauvegardes sont stockées dans un magasin d'objets de votre compte cloud, indépendamment des copies Snapshot de volume utilisées pour la restauration à court terme ou le clonage.

Sauvegarde dans le cloud est optimisée par "Cloud Backup Service".

> Vous devez utiliser Cloud Manager pour toutes les opérations de sauvegarde et de restauration. Toute action réalisée directement auprès de ONTAP ou de votre fournisseur cloud ne prend pas en charge la configuration.

Caractéristiques

- Sauvegardez des copies indépendantes de vos volumes de données dans un stockage objet économique dans le cloud.
- Les données de sauvegarde sont sécurisées par chiffrement AES 256 bits au repos et TLS 1.2 HTTPS en transit.
- Sauvegarde depuis le cloud, et depuis les systèmes ONTAP sur site vers le cloud.
- Prise en charge de 1,019 sauvegardes maximum d'un seul volume.
- Restauration des données à partir d'un point dans le temps spécifique
- Restaurez les données vers un volume du système source ou vers un autre système.

Environnements de travail et fournisseurs de stockage objet pris en charge

La sauvegarde dans le cloud est prise en charge avec plusieurs types d'environnements de travail :

- Cloud Volumes ONTAP dans AWS
- Cloud Volumes ONTAP dans Azure
- Clusters ONTAP sur site

Le coût

Deux options de tarification sont disponibles pour la sauvegarde dans le cloud : BYOL (Bring Your Own License) et le paiement à l'utilisation (PAYGO).

BYOL, vous payez NetApp pour une utilisation du service pendant une période de temps, disons de 6 mois, ainsi qu'une quantité maximale de capacité de sauvegarde, d'environ 10 Go (avant fonctionnalités d'efficacité du stockage). Vous devrez alors payer votre fournisseur cloud pour les coûts de stockage objet. Vous recevrez un numéro de série indiqué dans la page des licences Cloud Manager pour activer le service. Lorsque l'une ou l'autre limite est atteinte, vous devez renouveler la licence. Voir "Ajout et mise à jour de votre licence Backup BYOL". La licence de sauvegarde BYOL s'applique à tous les systèmes Cloud Volumes ONTAP associés à

votre "Compte Cloud Central".

Facturation à l'utilisation de PAYGO, vous devrez payer votre fournisseur cloud pour le stockage objet et NetApp pour les coûts de licence de sauvegarde. Les coûts de licence dépendent de la capacité utilisée (avant l'efficacité du stockage) :

- AWS : "Rendez-vous sur l'offre Cloud Manager Marketplace pour obtenir des informations sur leurs prix".
- Azure : "Rendez-vous sur l'offre Cloud Manager Marketplace pour obtenir des informations sur leurs prix".

Essai gratuit

Un essai gratuit de 30 jours est disponible. Lorsque vous utilisez la version d'essai, vous êtes averti du nombre de jours d'essai gratuits restants. À la fin de votre essai gratuit, les sauvegardes cessent d'être créées. Vous devez vous abonner au service ou acheter une licence pour continuer à utiliser le service.

La sauvegarde n'est pas supprimée lorsque le service est désactivé. Votre fournisseur cloud continuera de vous facturer les coûts de stockage objet pour la capacité de vos sauvegardes, à moins de supprimer les sauvegardes.

Fonctionnement de la sauvegarde dans le cloud

Lorsque vous activez la sauvegarde dans le cloud sur un système ONTAP Cloud Volumes ONTAP ou sur site, le service effectue une sauvegarde complète de vos données. Les instantanés de volume ne sont pas inclus dans l'image de sauvegarde. Après la sauvegarde initiale, toutes les sauvegardes supplémentaires sont incrémentielles, ce qui signifie que seuls les blocs modifiés et les nouveaux blocs sont sauvegardés.

L'emplacement des sauvegardes

Les copies de sauvegarde sont stockées dans un compartiment S3 ou dans un conteneur Azure Blob créé par Cloud Manager dans votre compte cloud. Pour les systèmes Cloud Volumes ONTAP, le magasin d'objets est créé dans la même région où se trouve le système Cloud Volumes ONTAP. Pour les systèmes ONTAP sur site, vous identifiez la région lorsque vous activez le service.

Il existe un magasin d'objets par système Cloud Volumes ONTAP ou ONTAP sur site. Cloud Manager nomme le magasin d'objets comme suit : netapp-Backup-*clusterUUID*

Veillez à ne pas supprimer ce magasin d'objets.

Remarques :

- Dans AWS, Cloud Manager permet d'utiliser "Fonctionnalité d'accès public aux blocs Amazon S3" Sur le compartiment S3.
- Dans Azure, Cloud Manager utilise un groupe de ressources nouveau ou existant avec un compte de stockage pour le conteneur Blob.

Classes de stockage S3 prises en charge

Dans Amazon S3, les sauvegardes commencent dans la classe de stockage *Standard* et la transition vers la classe de stockage *Standard-Infrequent Access* après 30 jours.

Tiers d'accès Azure Blob pris en charge

Dans Azure, chaque sauvegarde est associée au niveau d'accès *Cold*.

Les paramètres de sauvegarde sont disponibles dans tout le système

Lorsque vous activez la sauvegarde dans le cloud, tous les volumes que vous identifiez sur le système sont sauvegardés dans le cloud.

La planification et le nombre de sauvegardes à conserver sont définis au niveau du système. Les paramètres de sauvegarde affectent tous les volumes du système.

L'horaire est quotidien, hebdomadaire, mensuel ou une combinaison

Vous pouvez choisir des sauvegardes quotidiennes, hebdomadaires ou mensuelles de tous les volumes. Vous pouvez également sélectionner l'une des stratégies définies par le système qui assure les sauvegardes et la conservation pendant 3 mois, 1 an et 7 ans. Ces règles sont les suivantes :

Nom de la règle	Sauvegardes par intervalle…			Capacité Sauvegardes
	Tous les jours	Hebdomadaire	Mensuel	
Netap3MonthsRetention	30	13	3	46
Fidélisation Netapp1YearRetention	30	13	12	55
Netapp7YearsRetention	30	53	84	167

Lorsque vous avez atteint le nombre maximal de sauvegardes pour une catégorie ou un intervalle, les anciennes sauvegardes sont supprimées, ce qui vous permet d'avoir toujours les sauvegardes les plus récentes.

Notez que la période de conservation pour les sauvegardes de volumes de protection des données est identique à celle définie dans la relation SnapMirror source. Vous pouvez le modifier si vous le souhaitez à l'aide de l'API.

Les sauvegardes sont effectuées à minuit

- Les sauvegardes quotidiennes commencent juste après minuit chaque jour.
- Les sauvegardes hebdomadaires commencent juste après minuit le dimanche matin.
- Les sauvegardes mensuelles commencent juste après minuit le premier de chaque mois.

Pour le moment, vous ne pouvez pas planifier les opérations de sauvegarde à un moment spécifié par l'utilisateur.

Les copies de sauvegarde sont associées à votre compte Cloud Central

Les copies de sauvegarde sont associées à l' "Compte Cloud Central" Où réside Cloud Manager.

Si plusieurs systèmes Cloud Manager se trouvent dans le même compte Cloud Central, chaque système Cloud Manager affiche la même liste de sauvegardes. Cela inclut les sauvegardes associées à Cloud Volumes ONTAP et aux instances ONTAP sur site à partir d'autres systèmes Cloud Manager.

Considérations relatives aux licences BYOL

Lorsque vous utilisez la licence Backup vers Cloud BYOL, Cloud Manager vous informe que les sauvegardes approchent de la limite de capacité ou près de la date d'expiration de la licence. Vous recevez les notifications suivantes :

- lorsque les sauvegardes atteignent 80 % de la capacité sous licence, et lorsque vous en avez atteint la limite
- 30 jours avant l'expiration d'une licence, et encore une fois à l'expiration de celle-ci

Utilisez l'icône de chat située en bas à droite de l'interface Cloud Manager pour renouveler votre licence lorsque vous recevez ces notifications.

Deux éléments peuvent se produire à l'expiration de votre licence :

- Si le compte que vous utilisez pour vos systèmes ONTAP possède un compte Marketplace, le service de sauvegarde continue de s'exécuter, mais vous avez basculé vers un modèle de licence PAYGO. Vous êtes facturé par votre fournisseur cloud pour les coûts de stockage objet, et par NetApp pour les coûts de licence de sauvegarde, en fonction de la capacité utilisée par vos sauvegardes.
- Si le compte que vous utilisez pour vos systèmes ONTAP ne dispose pas d'un compte Marketplace, le service de sauvegarde continue de fonctionner, mais vous continuerez à recevoir le message d'expiration.

Une fois que vous renouvelez votre abonnement BYOL, Cloud Manager obtient automatiquement la nouvelle licence auprès de NetApp et l'installe. Si Cloud Manager ne peut pas accéder au fichier de licence via la connexion Internet sécurisée, vous pouvez obtenir le fichier vous-même et le télécharger manuellement dans Cloud Manager. Pour obtenir des instructions, reportez-vous à la section "Ajout et mise à jour de votre licence Backup BYOL".

Les systèmes qui ont basculé vers une licence PAYGO sont automatiquement renvoyés vers la licence BYOL. De plus, les systèmes qui étaient en cours d'exécution sans licence cessent de recevoir le message d'avertissement et seront facturés pour les sauvegardes qui se sont produites pendant l'expiration de la licence.

Volumes pris en charge

La sauvegarde dans le cloud prend en charge les volumes en lecture/écriture et les volumes de protection des données (DP).

Les volumes FlexGroup ne sont pas pris en charge actuellement.

Limites

- Le stockage WORM (SnapLock) n'est pas pris en charge sur un système Cloud Volumes ONTAP ou sur site lorsque la sauvegarde vers le cloud est activée.
- Restrictions liées à la sauvegarde dans le cloud pour les sauvegardes à partir de systèmes ONTAP sur site :
  - Le cluster sur site doit exécuter ONTAP 9.7P5 ou une version ultérieure.
  - Cloud Manager doit être déployé sur Azure. Les déploiements Cloud Manager sur site ne sont pas pris en charge.
  - L'emplacement de destination des sauvegardes n'est que le stockage objet sur Azure.
  - Les sauvegardes ne peuvent être restaurées que sur des systèmes Cloud Volumes ONTAP déployés sur Azure. Vous ne pouvez pas restaurer une sauvegarde vers un système ONTAP sur site ou vers un système Cloud Volumes ONTAP qui utilise un autre fournisseur cloud.
- Lors de la sauvegarde de volumes de protection des données (DP), la règle définie pour la règle SnapMirror sur le volume source doit utiliser une étiquette qui correspond aux noms de stratégie de sauvegarde dans le cloud définis : **quotidien**, **hebdomadaire** ou **mensuel**. Dans le cas contraire, la sauvegarde échouera pour ce volume DP.

- Dans Azure, si vous activez l'option sauvegarde dans le cloud lorsque Cloud Volumes ONTAP est déployé, Cloud Manager crée le groupe de ressources pour vous et vous ne pouvez pas le modifier. Si vous souhaitez choisir votre propre groupe de ressources lors de l'activation de la sauvegarde dans le cloud, **désactiver** la sauvegarde dans le cloud lors du déploiement de Cloud Volumes ONTAP, puis activer la sauvegarde dans le cloud et choisir le groupe de ressources dans la page Paramètres de sauvegarde dans le cloud.
- Lorsque vous sauvegardez des volumes à partir de systèmes Cloud Volumes ONTAP, la sauvegarde des volumes que vous créez en dehors de Cloud Manager n'est pas automatique.

  Par exemple, si vous créez un volume depuis l'interface de ligne de commandes ONTAP, l'API ONTAP ou System Manager, le volume ne sera pas automatiquement sauvegardé.

  Si vous souhaitez sauvegarder ces volumes, désactivez sauvegarde dans le cloud, puis activez-les à nouveau.

Commencez

Sauvegarde des données dans Amazon S3

Commencez à sauvegarder des données d'Cloud Volumes ONTAP vers Amazon S3 en quelques étapes.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

Vérifiez la prise en charge de votre configuration

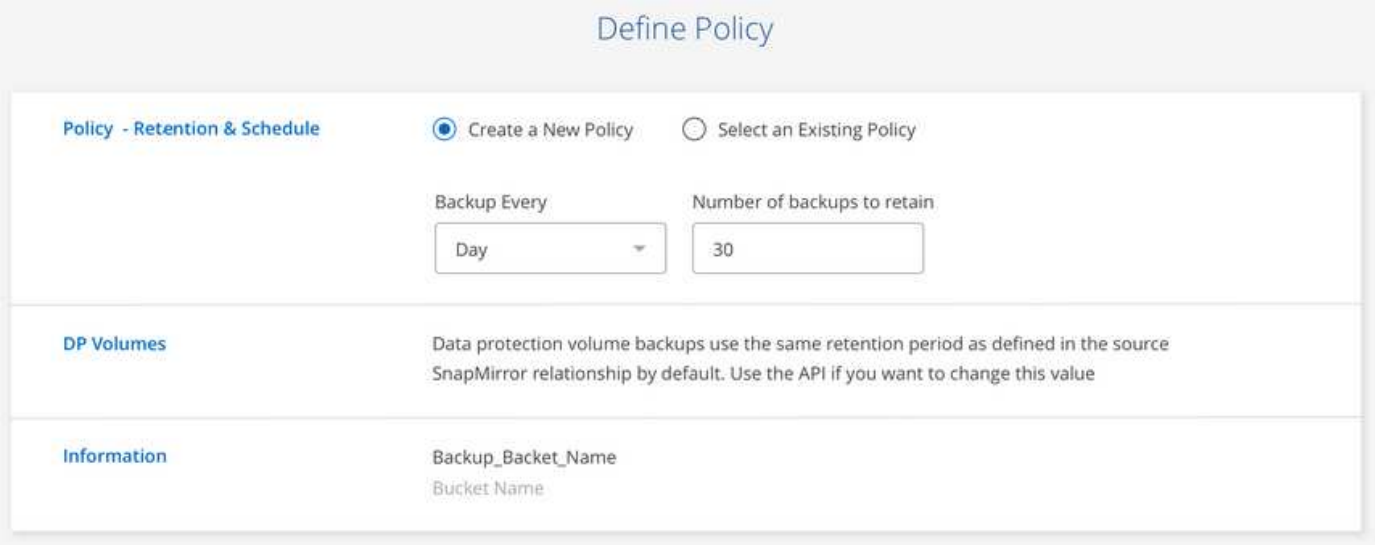
- Vous exécutez Cloud Volumes ONTAP 9.6 ou une version ultérieure dans AWS.
- Vous avez souscrit au "Offre Cloud Manager Marketplace Backup", ou vous avez acheté "et activé" Licence BYOL pour la sauvegarde dans le cloud de NetApp.
- Le rôle IAM qui fournit des autorisations Cloud Manager inclut les autorisations S3 à partir de la dernière version "Politique de Cloud Manager".

Activation de la sauvegarde dans le cloud sur votre système nouveau ou existant

- Nouveaux systèmes : la sauvegarde dans le cloud est activée par défaut dans l'assistant de l'environnement de travail. Assurez-vous de conserver l'option activée.
- Systèmes existants : sélectionnez l'environnement de travail et cliquez sur **Activer** en regard du service sauvegarde dans le cloud dans le panneau de droite, puis suivez l'assistant d'installation.

Définissez la stratégie de sauvegarde

La règle par défaut sauvegarde les volumes tous les jours et conserve les 30 copies de sauvegarde les plus récentes de chaque volume. Passez aux sauvegardes hebdomadaires ou mensuelles ou sélectionnez l'une des règles définies par le système qui offrent plus d'options. Vous pouvez également modifier le nombre de copies de sauvegarde à conserver.

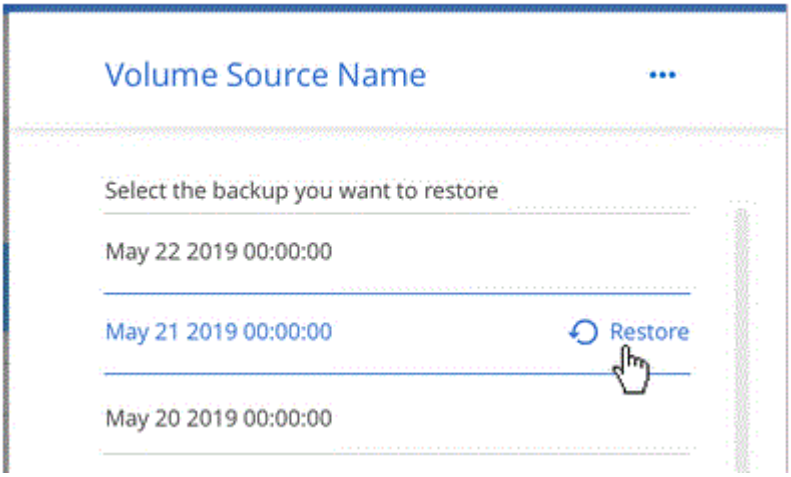


Sélectionnez les volumes à sauvegarder

Identifiez les volumes à sauvegarder dans la page Sélectionner les volumes.

Restaurez vos données à la demande

Dans la liste de sauvegarde, sélectionnez un volume, sélectionnez une sauvegarde, puis restaurez les données de la sauvegarde vers un nouveau volume.



De formation

Avant de commencer à sauvegarder des volumes sur S3, lisez les informations suivantes pour vous assurer que votre configuration est prise en charge.

Versions de ONTAP prises en charge

Cloud Volumes ONTAP 9.6 et versions ultérieures

Régions AWS prises en charge

Backup vers le cloud est pris en charge dans toutes les régions AWS "Dans ce cas, Cloud Volumes ONTAP est pris en charge".

Conditions de licence

Pour le modèle de licence PAYGO pour la sauvegarde dans le cloud, un abonnement Cloud Manager est disponible sur AWS Marketplace qui permet de déployer Cloud Volumes ONTAP 9.6 et versions ultérieures (PAYGO) et la solution de sauvegarde dans le cloud. Vous devez le faire "Abonnez-vous à cet abonnement Cloud Manager" Avant d'activer la sauvegarde dans le cloud. La facturation pour la sauvegarde dans le cloud se fait via cet abonnement.

Pour les licences BYOL pour la sauvegarde dans le cloud, vous n'avez pas besoin d'un abonnement AWS Backup vers Cloud. Vous avez besoin du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité de la licence. Voir "Ajout et mise à jour de votre licence Backup BYOL".

Vous devez également disposer d'un abonnement AWS pour l'espace de stockage où vos sauvegardes seront stockées.

Autorisations AWS requises

Le rôle IAM qui fournit des autorisations à Cloud Manager doit inclure les autorisations S3 les plus récentes "Politique de Cloud Manager".

Voici les autorisations spécifiques de la stratégie :

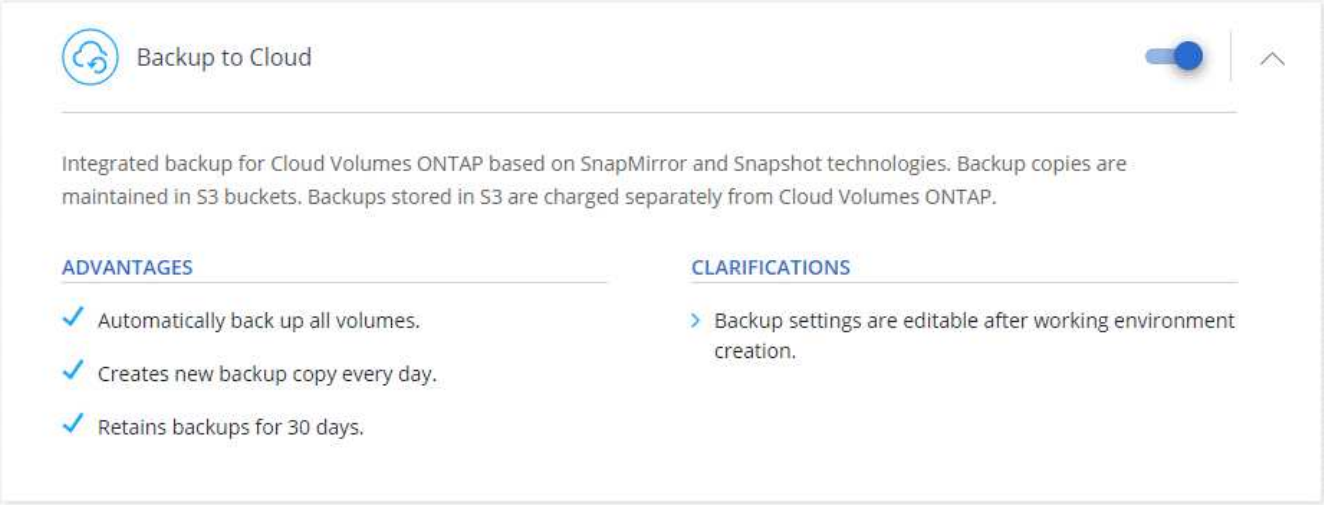
```
{
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "Action": [
                "s3:DeleteBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetObject",
                "s3:ListBucket",
                "s3:ListAllMyBuckets",
                "s3:GetBucketTagging",
                "s3:GetBucketLocation",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
            ]
        },
```

Activation de la sauvegarde dans le cloud sur un nouveau système

La sauvegarde dans le cloud est activée par défaut dans l'assistant de l'environnement de travail. Assurez-vous de conserver l'option activée.

Étapes

1. Cliquez sur **Créer Cloud Volumes ONTAP**.
2. Sélectionnez Amazon Web Services en tant que fournisseur cloud, puis choisissez un système à un seul nœud ou haute disponibilité.
3. Remplissez la page Détails et références.
4. Sur la page Services, laissez le service activé et cliquez sur **Continuer**.



5. Complétez les pages de l'assistant pour déployer le système.

Résultat

La sauvegarde dans le cloud est activée sur le système. Elle sauvegarde les volumes tous les jours et conserve les 30 copies de sauvegarde les plus récentes.

Et la suite ?

"Vous pouvez gérer les sauvegardes en modifiant la planification des sauvegardes, en restaurant des volumes, etc".

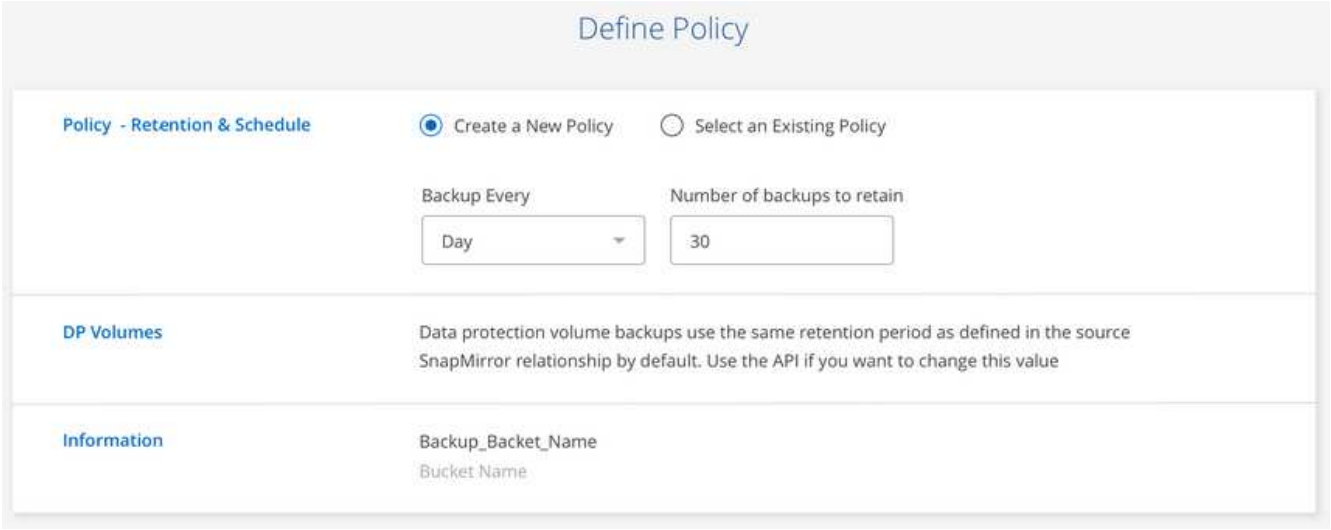
Activation de la sauvegarde dans le cloud sur un système existant

Activation de la sauvegarde dans le cloud à tout moment directement depuis l'environnement de travail

Étapes

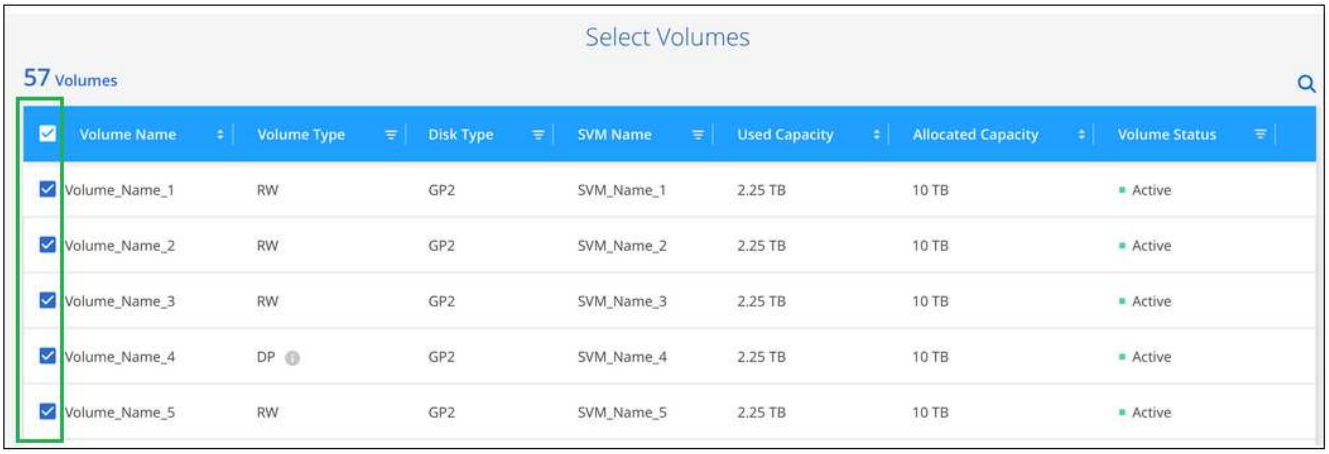
1. Sélectionnez l'environnement de travail et cliquez sur **Activer** en regard du service sauvegarde dans le cloud dans le panneau de droite.

2. Définissez le programme de sauvegarde et la valeur de conservation, puis cliquez sur **Continuer**.



Voir "liste des stratégies existantes".

3. Sélectionnez les volumes à sauvegarder et cliquez sur **Activer**.



Résultat

La sauvegarde dans le cloud commence à effectuer les sauvegardes initiales de chaque volume sélectionné.

Et la suite ?

"Vous pouvez gérer les sauvegardes en modifiant la planification des sauvegardes, en restaurant des volumes, etc".

Sauvegarde des données dans le stockage Azure Blob

Réalisez quelques étapes pour commencer à sauvegarder des données de Cloud Volumes ONTAP vers le stockage Azure Blob.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

Vérifiez la prise en charge de votre configuration

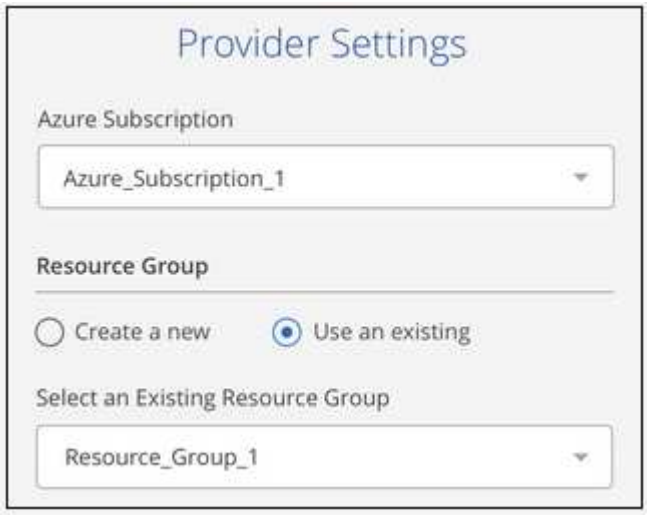
- Vous exécutez Cloud Volumes ONTAP 9.7 ou une version ultérieure dans Azure.
- Vous disposez d'un abonnement valide au fournisseur cloud pour l'espace de stockage où vos sauvegardes seront stockées.
- Vous avez souscrit au "Offre Cloud Manager Marketplace Backup", ou vous avez acheté "et activé" Licence BYOL pour la sauvegarde dans le cloud de NetApp.

Activation de la sauvegarde dans le cloud sur votre système nouveau ou existant

- Nouveaux systèmes : la sauvegarde dans le cloud est activée par défaut dans l'assistant de l'environnement de travail. Assurez-vous de conserver l'option activée.
- Systèmes existants : sélectionnez l'environnement de travail et cliquez sur **Activer** en regard du service sauvegarde dans le cloud dans le panneau de droite, puis suivez l'assistant d'installation.

Entrez les détails du fournisseur

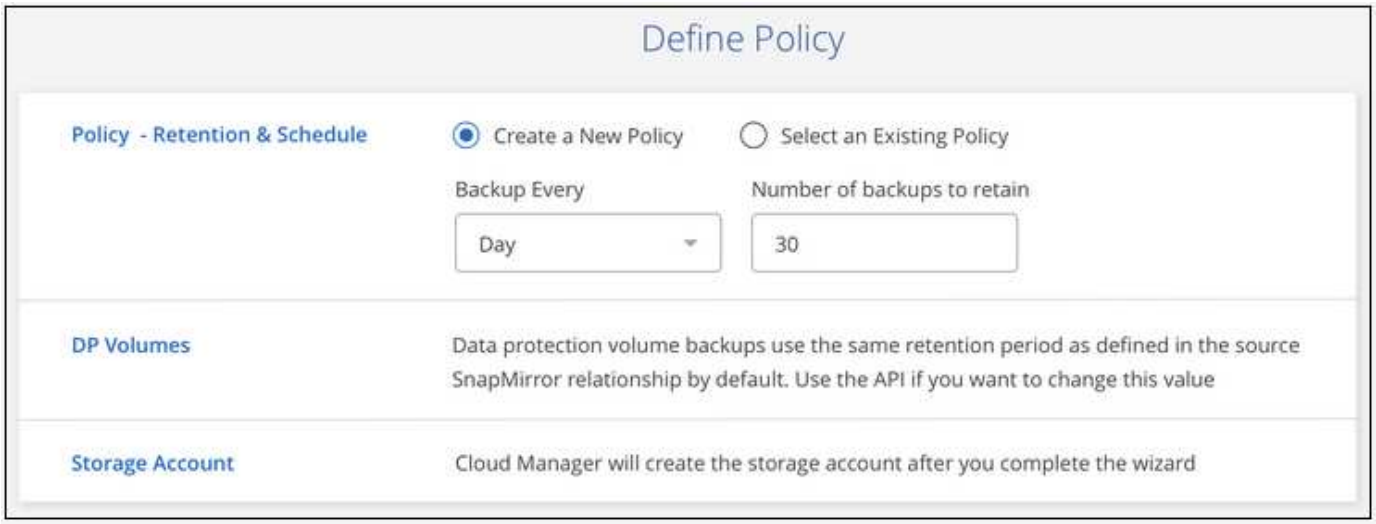
Sélectionnez l'abonnement du fournisseur et choisissez si vous souhaitez créer un nouveau groupe de ressources ou utiliser un groupe de ressources existant.



Définissez la stratégie de sauvegarde

La règle par défaut sauvegarde les volumes tous les jours et conserve les 30 copies de sauvegarde les plus récentes de chaque volume. Passez aux sauvegardes hebdomadaires ou mensuelles ou sélectionnez l'une

des règles définies par le système qui offrent plus d'options.

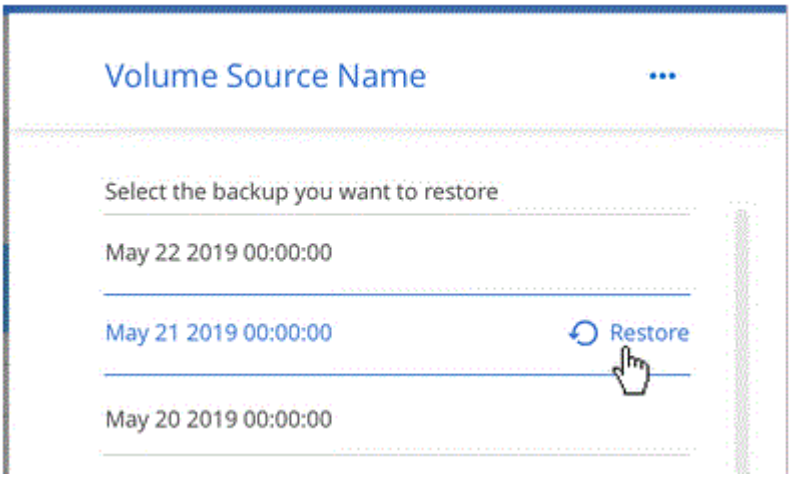


5 Sélectionnez les volumes à sauvegarder

Identifiez les volumes à sauvegarder dans la page Sélectionner les volumes.

6 Restaurez vos données à la demande

Dans la liste de sauvegarde, sélectionnez un volume, sélectionnez une sauvegarde, puis restaurez les données de la sauvegarde vers un nouveau volume.



De formation

Avant de commencer à sauvegarder les volumes sur le stockage Azure Blob, lisez les informations suivantes pour vous assurer que la configuration est prise en charge.

Versions de ONTAP prises en charge

Cloud Volumes ONTAP 9.7 et versions ultérieures

Régions Azure prises en charge

Backup dans le cloud est pris en charge dans toutes les régions Azure "Dans ce cas, Cloud Volumes ONTAP est pris en charge".

Conditions de licence

Pour le modèle de licence PAYGO pour la sauvegarde dans le cloud, un abonnement via Azure Marketplace est requis avant d'activer la sauvegarde dans le cloud. La facturation pour la sauvegarde dans le cloud se fait via cet abonnement. "Vous pouvez vous abonner à la page Détails et amp ; informations d'identification de l'assistant de l'environnement de travail".

Pour les licences BYOL pour la sauvegarde dans le cloud, vous avez besoin du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité du contrat. Voir "Ajout et mise à jour de votre licence Backup BYOL".

Vous devez également disposer d'un abonnement Microsoft Azure pour l'espace de stockage où vos sauvegardes seront stockées.

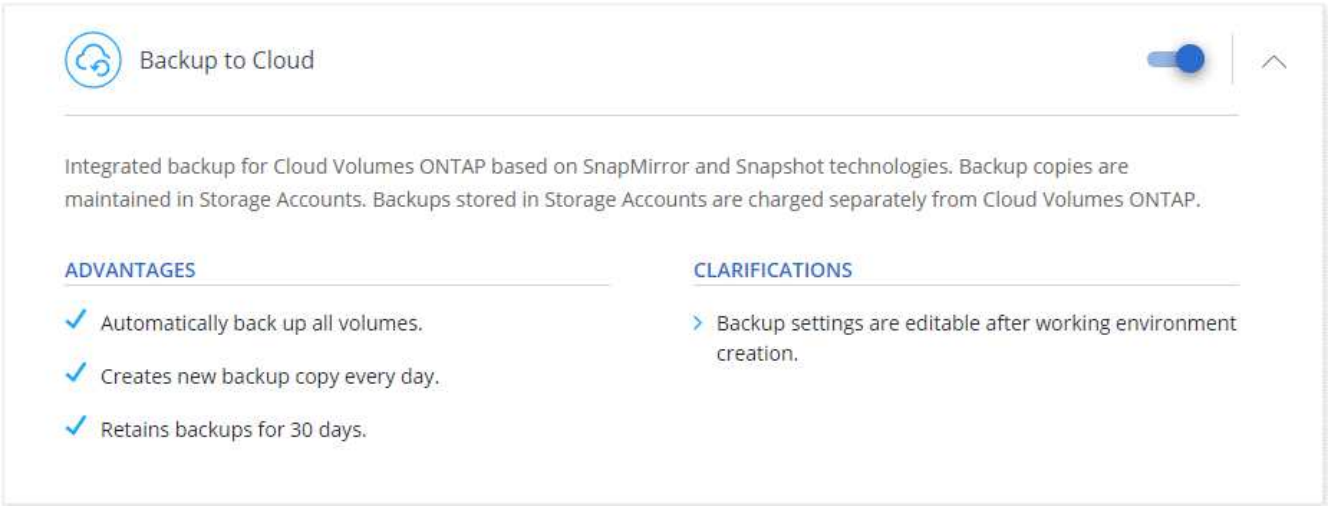
Activation de la sauvegarde dans le cloud sur un nouveau système

La sauvegarde dans le cloud est activée par défaut dans l'assistant de l'environnement de travail. Assurez-vous de conserver l'option activée.

Si vous souhaitez choisir le nom du groupe de ressources, **disable** sauvegarde dans le cloud lors du déploiement de Cloud Volumes ONTAP. Suivez les étapes de la section activation de la sauvegarde dans le cloud sur un système en place Pour activer la sauvegarde dans le cloud et choisir le groupe de ressources.

Étapes

1. Cliquez sur **Créer Cloud Volumes ONTAP**.
2. Sélectionnez Microsoft Azure comme fournisseur cloud, puis choisissez un système HA ou un seul nœud.
3. Remplissez la page Détails et identifiants pour qu'un abonnement Azure Marketplace soit en place.
4. Sur la page Services, laissez le service activé et cliquez sur **Continuer**.



5. Complétez les pages de l'assistant pour déployer le système.

Résultat

La sauvegarde dans le cloud est activée sur le système. Elle sauvegarde les volumes tous les jours et conserve les 30 copies de sauvegarde les plus récentes.

Et la suite ?

"Vous pouvez gérer les sauvegardes en modifiant la planification des sauvegardes, en restaurant des volumes, etc".

Activation de la sauvegarde dans le cloud sur un système existant

Activation de la sauvegarde dans le cloud à tout moment directement depuis l'environnement de travail

Étapes

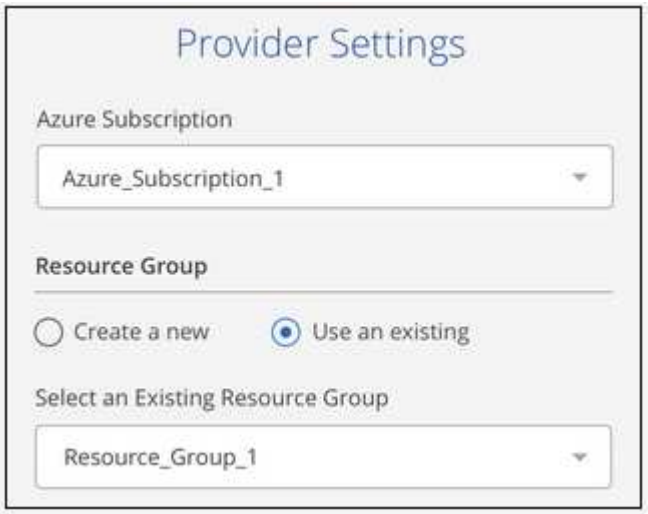
1. Sélectionnez l'environnement de travail et cliquez sur **Activer** en regard du service sauvegarde dans le cloud dans le panneau de droite.

2. Sélectionnez les détails du fournisseur :

   a. L'abonnement Azure utilisé pour stocker les sauvegardes.

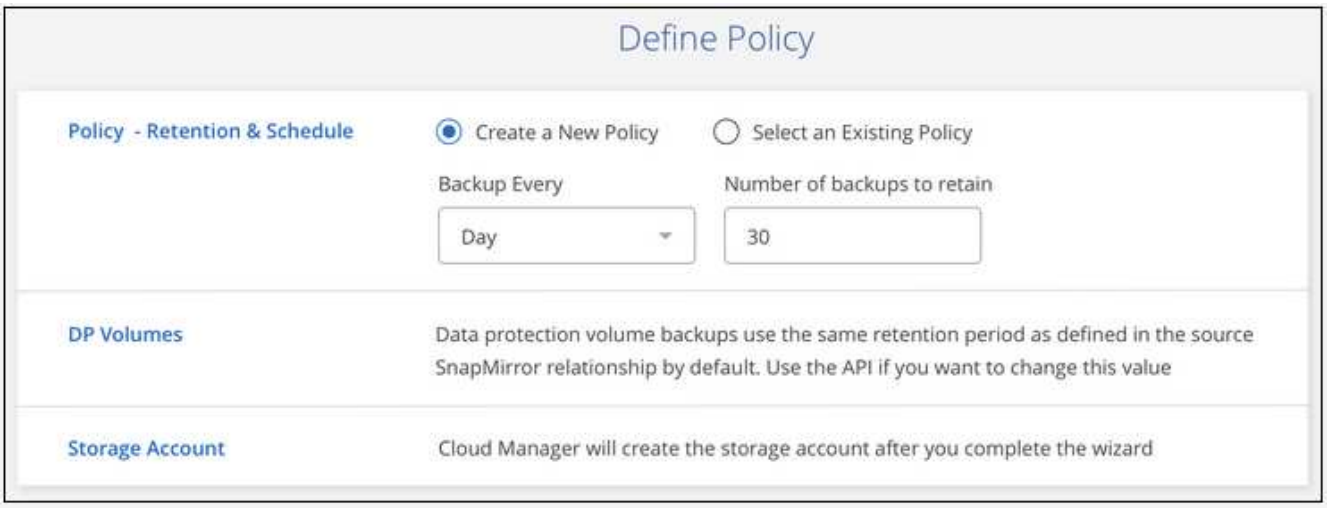
   b. Le groupe de ressources - vous pouvez créer un nouveau groupe de ressources ou sélectionner et un groupe de ressources existant.

   c. Puis cliquez sur **Continuer**.



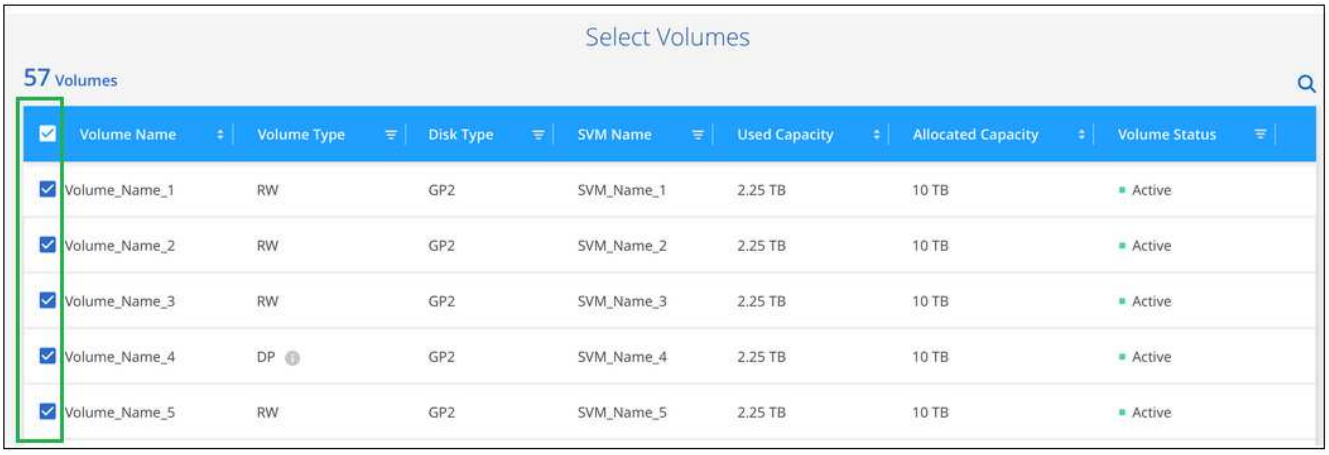
   Notez que vous ne pouvez pas modifier l'abonnement ou le groupe de ressources après le démarrage des services.

3. Dans la page *Define Policy*, sélectionnez le programme de sauvegarde et la valeur de conservation, puis cliquez sur **Continuer**.



Voir "liste des stratégies existantes".

4. Sélectionnez les volumes à sauvegarder et cliquez sur **Activer**.



Résultat

La sauvegarde dans le cloud commence à effectuer les sauvegardes initiales de chaque volume sélectionné.

Et la suite ?

"Vous pouvez gérer les sauvegardes en modifiant la planification des sauvegardes, en restaurant des volumes, etc".

Sauvegarde des données à partir d'un système ONTAP sur site vers le cloud

Procédez comme suit pour commencer à sauvegarder les données à partir de votre système ONTAP sur site vers un stockage objet à faible coût dans le cloud.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

Vérifiez la prise en charge de votre configuration

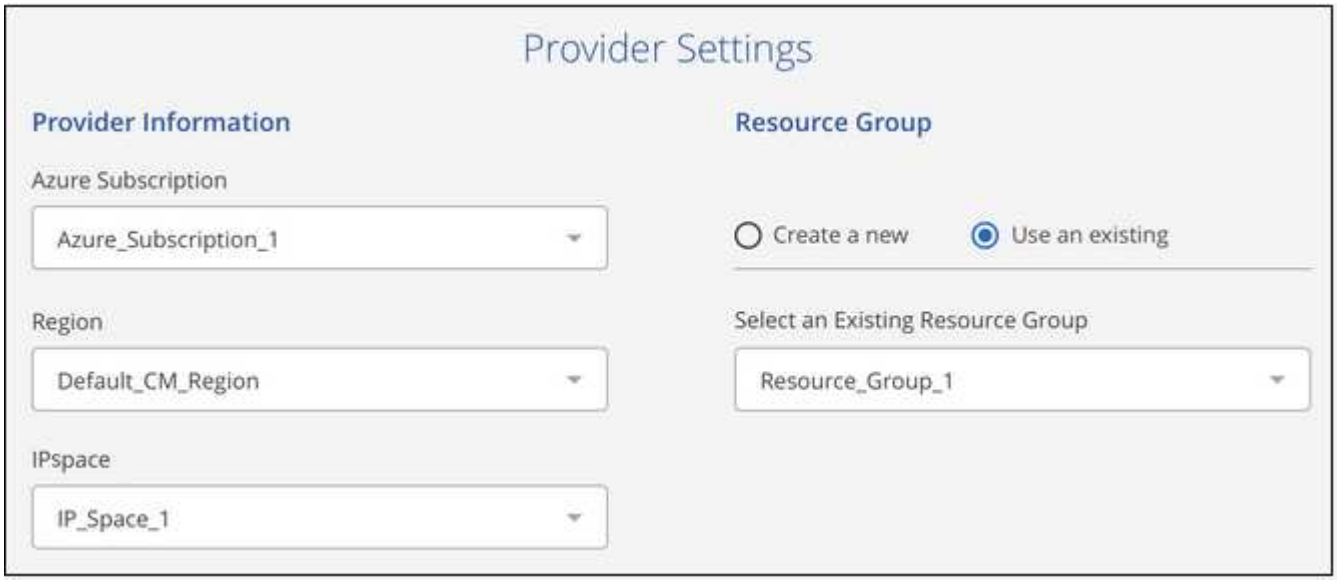
- Vous avez découvert le cluster sur site et l'avez ajouté à un environnement de travail dans Cloud Manager. Voir "Découverte des clusters ONTAP" pour plus d'informations.
- Vous exécutez ONTAP 9.7P5 ou version ultérieure sur le cluster.
- Vous disposez d'un abonnement valide au fournisseur cloud pour l'espace de stockage où vos sauvegardes seront stockées.
- Vous avez souscrit au "Offre Cloud Manager Marketplace Backup", ou vous avez acheté "et activé" Licence BYOL pour la sauvegarde dans le cloud de NetApp.

Activez la sauvegarde dans le cloud sur le système

Sélectionnez l'environnement de travail et cliquez sur **Activer** en regard du service sauvegarde vers le cloud dans le panneau de droite, puis suivez l'assistant d'installation.

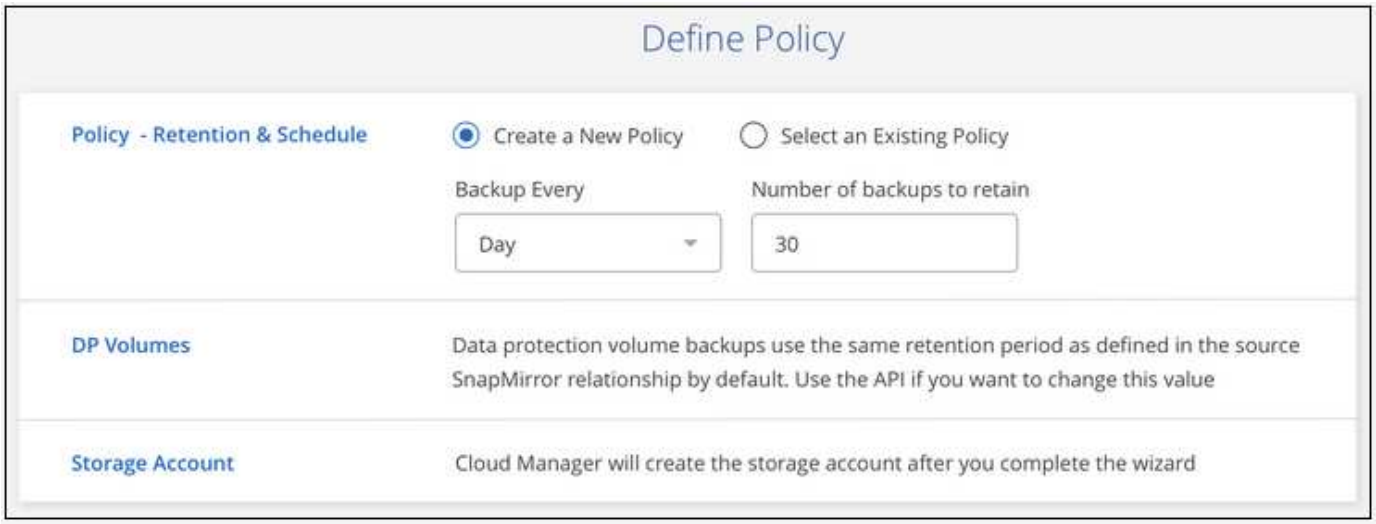
Sélectionnez le fournisseur de services clouds et entrez les informations relatives au fournisseur

Sélectionnez le fournisseur, puis sélectionnez l'abonnement du fournisseur, la région et le groupe de ressources. Vous devez également spécifier l'IPspace dans le cluster ONTAP où les volumes résident.



Définissez la stratégie de sauvegarde

La règle par défaut sauvegarde les volumes tous les jours et conserve les 30 copies de sauvegarde les plus récentes de chaque volume. Passez aux sauvegardes hebdomadaires ou mensuelles ou sélectionnez l'une des règles définies par le système qui offrent plus d'options.

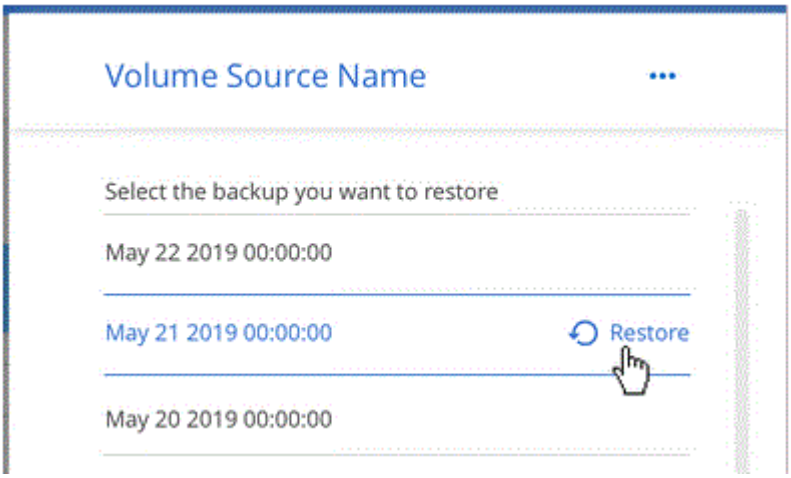


Sélectionnez les volumes à sauvegarder

Identifiez les volumes à sauvegarder depuis le cluster.

Restaurez vos données à la demande

Dans la liste des sauvegardes, sélectionnez un volume, sélectionnez une sauvegarde, puis restaurez les données depuis la sauvegarde vers un nouveau volume d'un système Cloud Volumes ONTAP qui utilise le même fournisseur cloud.



De formation

Avant de commencer à sauvegarder des volumes sur le stockage Azure Blob, lisez les informations suivantes pour vous assurer que votre configuration est prise en charge.

Versions de ONTAP prises en charge

ONTAP 9.7P5 et version ultérieure.

Configuration requise pour la mise en réseau des clusters

Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge les volumes que vous souhaitez sauvegarder. La LIF doit être associée au *IPspace* que ONTAP doit utiliser pour se connecter au stockage objet. Le SVM Admin doit résider sur l'IPspace. "En savoir plus sur les IPspaces".

Lorsque vous configurez la sauvegarde dans le cloud, vous êtes invité à utiliser l'IPspace. Vous devez choisir l'IPspace auquel chaque LIF est associée. Il peut s'agir de l'IPspace par défaut ou d'un IPspace personnalisé que vous avez créé.

Régions Azure prises en charge

Backup dans le cloud est pris en charge dans toutes les régions Azure "et des volumes cloud pris en charge".

Conditions de licence

Pour le modèle de licence PAYGO pour la sauvegarde dans le cloud, un abonnement à la solution "Offre Azure Marketplace Cloud Manager Backup" Sont indispensables avant d'activer la sauvegarde vers le cloud. La facturation pour la sauvegarde dans le cloud se fait via cet abonnement.

Pour les licences BYOL pour la sauvegarde dans le cloud, vous avez besoin du numéro de série de NetApp qui vous permet d'utiliser le service pendant la durée et la capacité du contrat. Voir "Ajout et mise à jour de votre licence Backup BYOL".

Vous devez également disposer d'un abonnement Microsoft Azure pour l'espace de stockage où vos sauvegardes seront stockées.

Activation de la sauvegarde dans le cloud

Activation de la sauvegarde dans le cloud à tout moment directement depuis l'environnement de travail

Étapes

1. Sélectionnez l'environnement de travail et cliquez sur **Activer** en regard du service sauvegarde dans le cloud dans le panneau de droite.

2. Sélectionnez le fournisseur, puis entrez les informations sur le fournisseur :

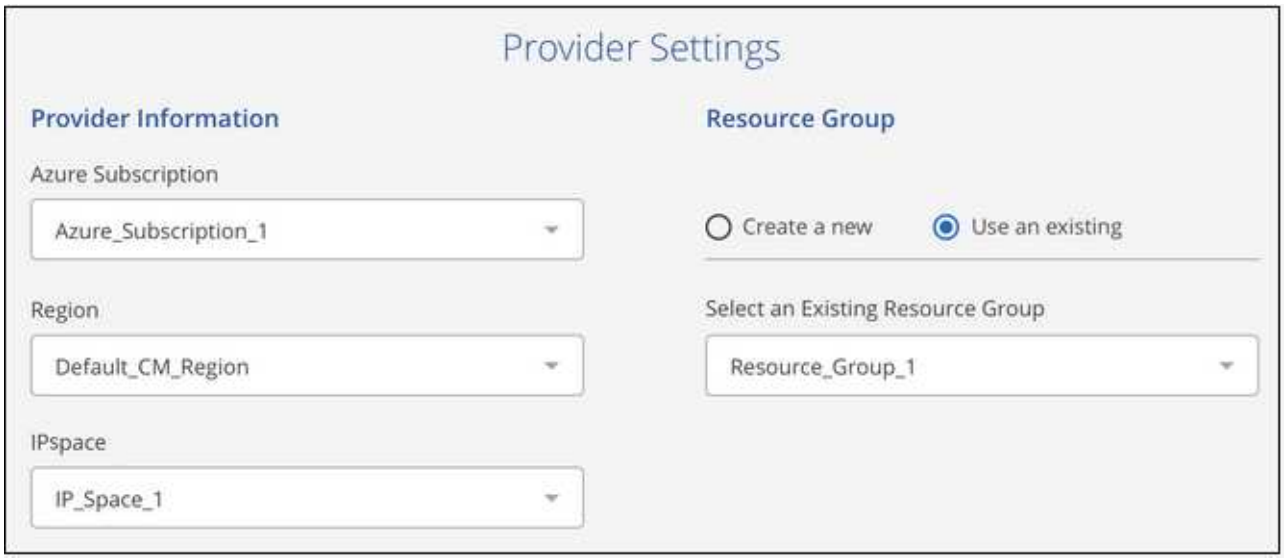
   a. L'abonnement Azure utilisé pour stocker les sauvegardes.

   b. Région Azure.

   c. Le groupe de ressources - vous pouvez créer un nouveau groupe de ressources ou sélectionner et un groupe de ressources existant.

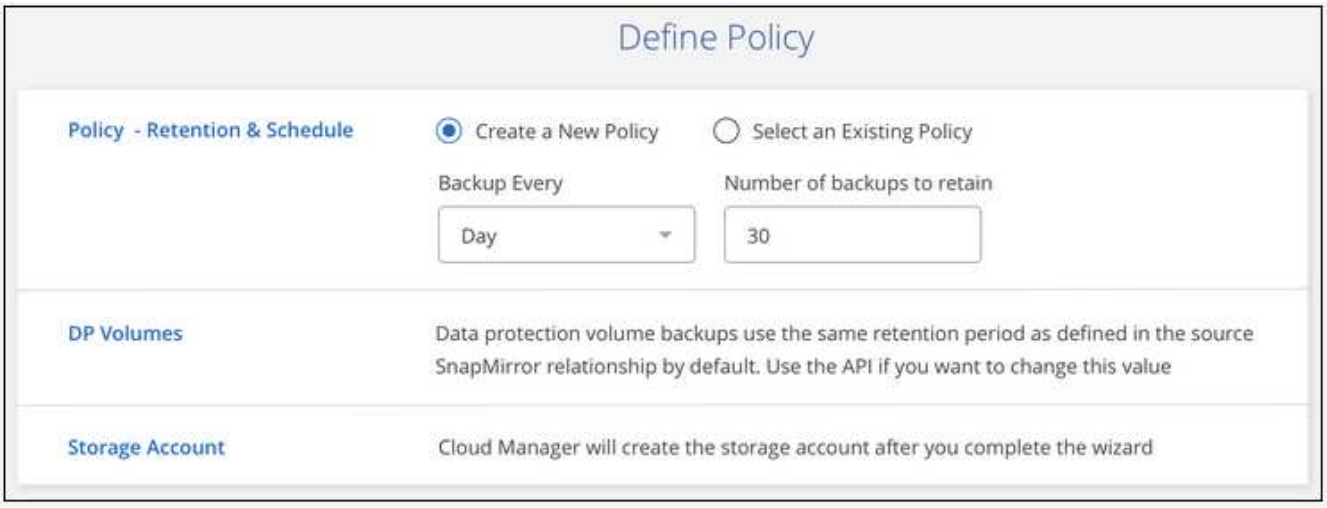
d. L'IPspace dans le cluster ONTAP où les volumes à sauvegarder résident.

e. Puis cliquez sur **Continuer**.



Notez que vous ne pouvez pas modifier l'abonnement ou le groupe de ressources après le démarrage des services.

3. Dans la page *Define Policy*, sélectionnez le programme de sauvegarde et la valeur de conservation, puis cliquez sur **Continuer**.



Voir "liste des stratégies existantes".

4. Sélectionnez les volumes à sauvegarder et cliquez sur **Activer**.

Résultat

La sauvegarde dans le cloud commence à effectuer les sauvegardes initiales de chaque volume sélectionné.

Et la suite ?

"Vous pouvez gérer les sauvegardes en modifiant la planification des sauvegardes, en restaurant des volumes, etc".

Gestion des sauvegardes pour les systèmes Cloud Volumes ONTAP et ONTAP sur site

Gérez les sauvegardes pour Cloud Volumes ONTAP et les systèmes ONTAP sur site en modifiant la planification des sauvegardes, en restaurant des volumes, en supprimant les sauvegardes, etc.

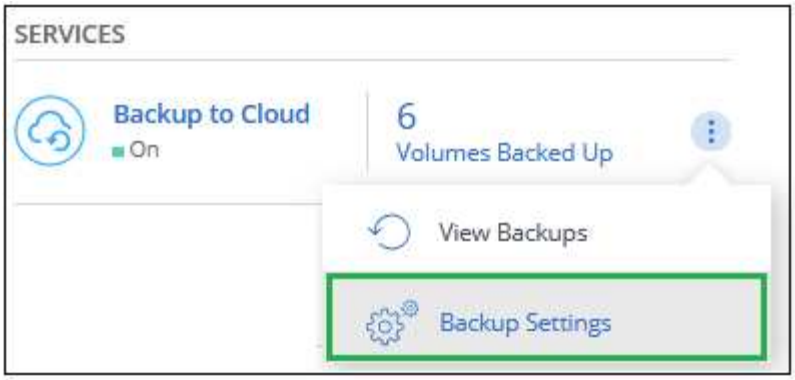
Modification de la planification et de la conservation des sauvegardes

La règle par défaut sauvegarde les volumes tous les jours et conserve les 30 copies de sauvegarde les plus récentes de chaque volume. Vous pouvez passer à des sauvegardes hebdomadaires ou mensuelles et modifier le nombre de copies de sauvegarde à conserver. Vous pouvez également sélectionner l'une des stratégies définies par le système qui fournissent des sauvegardes planifiées pour 3 mois, 1 an et 7 ans.

La modification de la règle de sauvegarde affecte uniquement les nouveaux volumes créés après que vous avez modifié la planification. Elle n'affecte pas la planification des volumes existants.

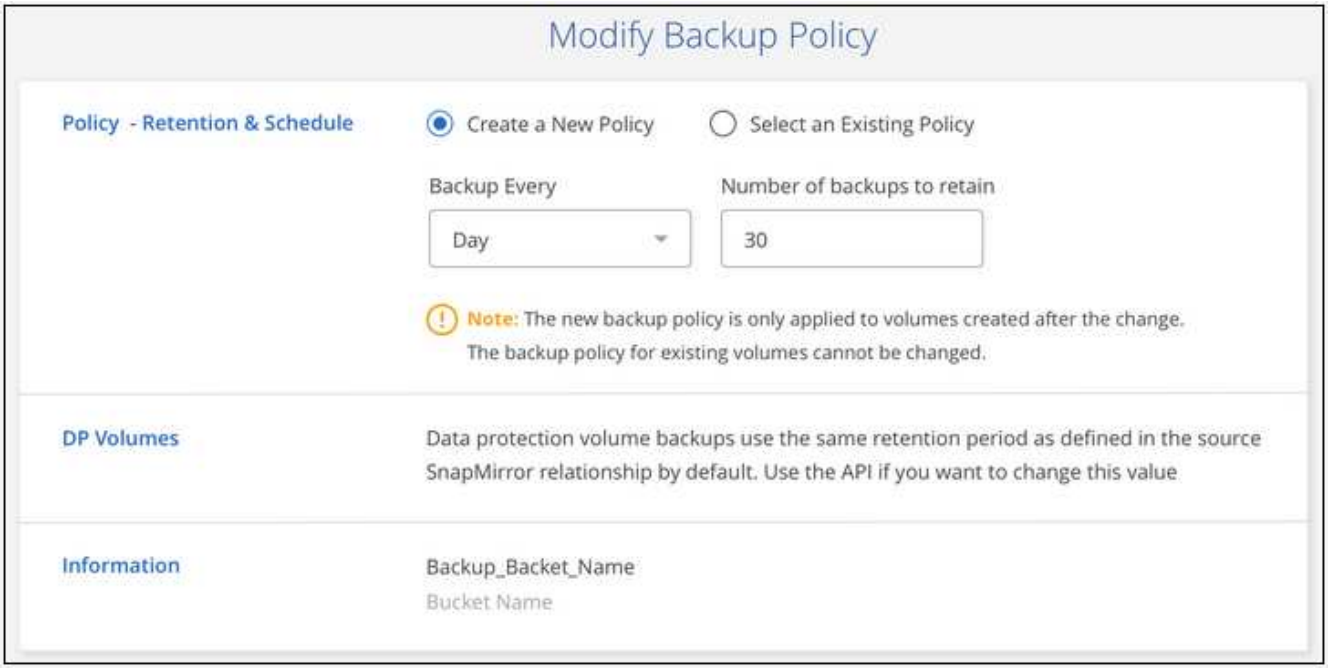
Étapes

1. Sélectionnez l'environnement de travail.
2. Cliquez sur Et sélectionnez **Paramètres de sauvegarde**.



3. Dans la page *Backup Settings*, cliquez sur ••• Pour l'environnement de travail et sélectionnez **Modifier la stratégie de sauvegarde**.

4. Dans la page *Modify Backup Policy*, modifiez le planning et la rétention des sauvegardes, puis cliquez sur **Save**.

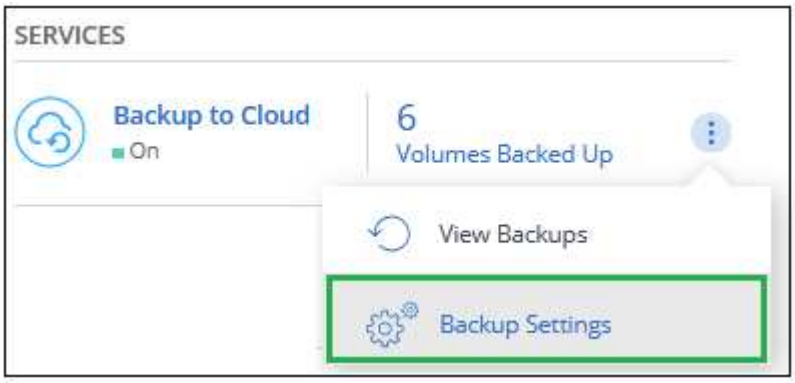


Démarrage et arrêt des sauvegardes de volumes

Vous pouvez arrêter la sauvegarde d'un volume si vous n'avez pas besoin de copies de sauvegarde de ce volume et si vous ne voulez pas payer pour le coût de stockage des sauvegardes. Vous pouvez également ajouter un nouveau volume à la liste des sauvegardes si ce n'est pas actuellement le cas.

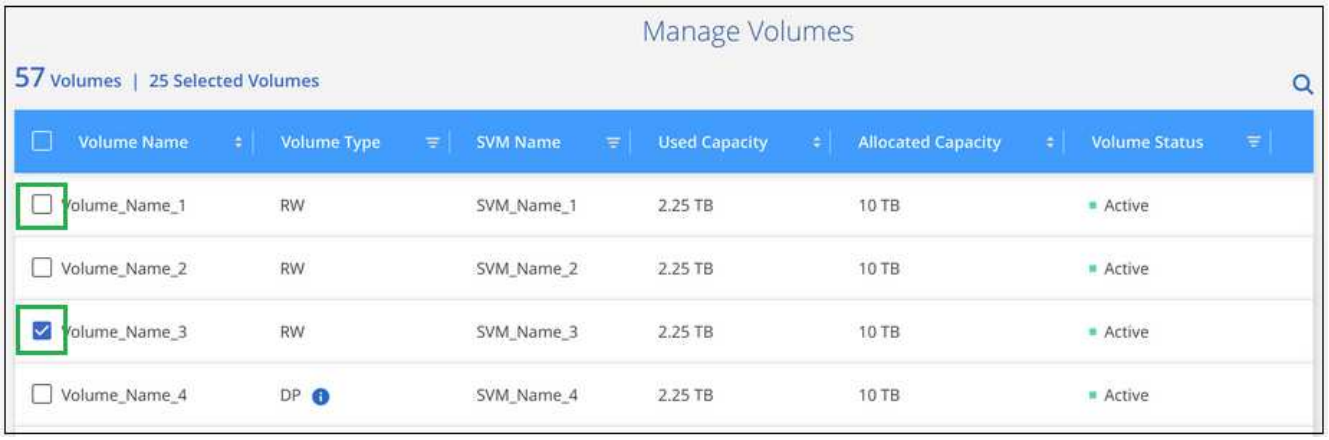
Étapes

1. Sélectionnez l'environnement de travail.
2. Cliquez sur ⋮ Et sélectionnez **Paramètres de sauvegarde**.



3. Dans la page *Backup Settings*, cliquez sur ••• Pour l'environnement de travail et sélectionnez **gérer les volumes**.

4. Cochez la case des volumes que vous souhaitez démarrer la sauvegarde et décochez la case des volumes que vous souhaitez arrêter la sauvegarde.



Remarque : lors de l'arrêt de la sauvegarde d'un volume, vous continuerez à être facturé par votre fournisseur de cloud pour les coûts de stockage objet pour la capacité que les sauvegardes utilisent, sauf si vous supprimez les sauvegardes.

Restauration d'un volume à partir d'une sauvegarde

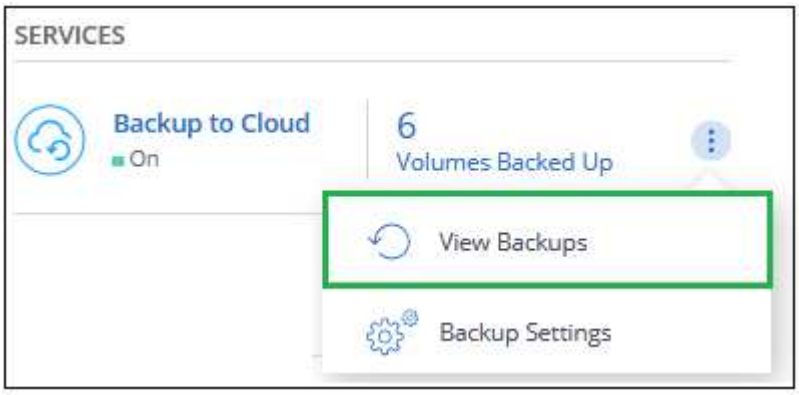
Lorsque vous restaurez les données à partir d'une sauvegarde, Cloud Manager crée un *nouveau* volume en

utilisant les données de la sauvegarde. Vous pouvez restaurer les données vers un volume dans le même environnement de travail ou vers un autre environnement de travail situé dans le même compte cloud que l'environnement de travail source. Comme la sauvegarde ne contient aucun instantané, le volume récemment restauré n'en contient pas non plus.

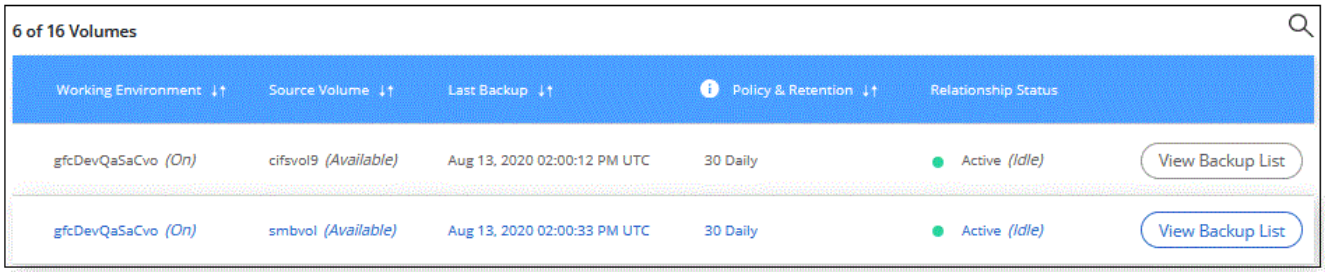
Les sauvegardes créées à partir des systèmes ONTAP sur site ne peuvent être restaurées que sur des systèmes Cloud Volumes ONTAP qui utilisent le même fournisseur cloud que où résident la sauvegarde.

Étapes

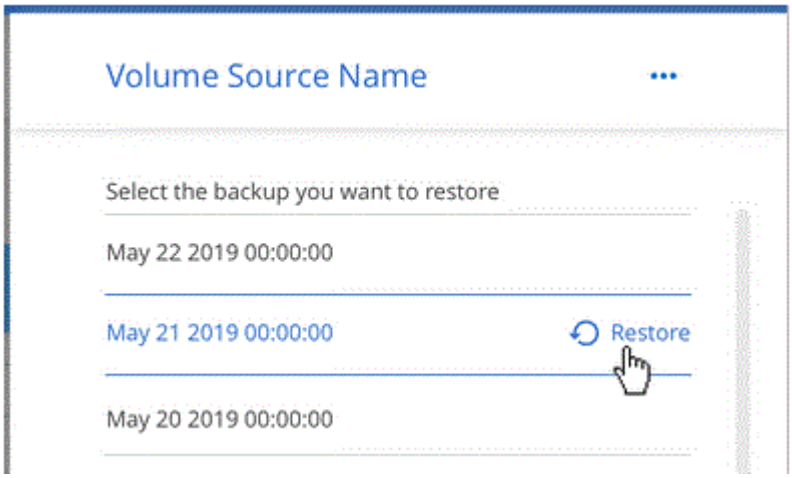
1. Sélectionnez l'environnement de travail.
2. Cliquez sur Et sélectionnez **Afficher les sauvegardes**.



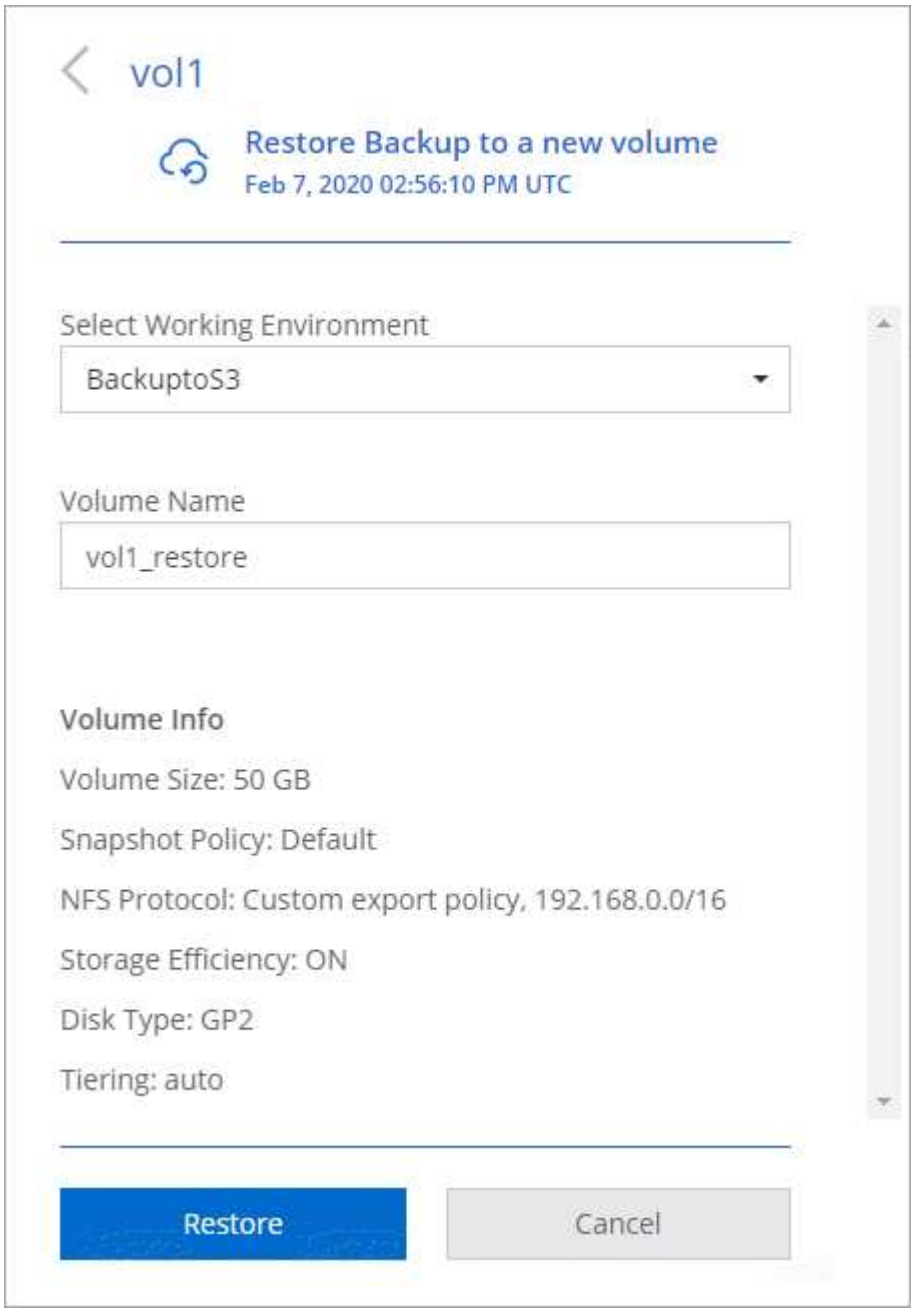
3. Sélectionnez la ligne du volume à restaurer et cliquez sur **Afficher la liste de sauvegarde**.



4. Recherchez la sauvegarde à restaurer et cliquez sur l'icône **Restaurer**.



5. Remplissez la *Restore Backup to New volume* page:
   a. Sélectionnez l'environnement de travail dans lequel vous souhaitez restaurer le volume.
   b. Entrez un nom pour le volume.
   c. Cliquez sur **Restaurer**.



Résultat

Cloud Manager crée un nouveau volume en fonction de la sauvegarde que vous avez sélectionnée. C'est possible "gestion de ce nouveau volume" selon les besoins.

Suppression de sauvegardes

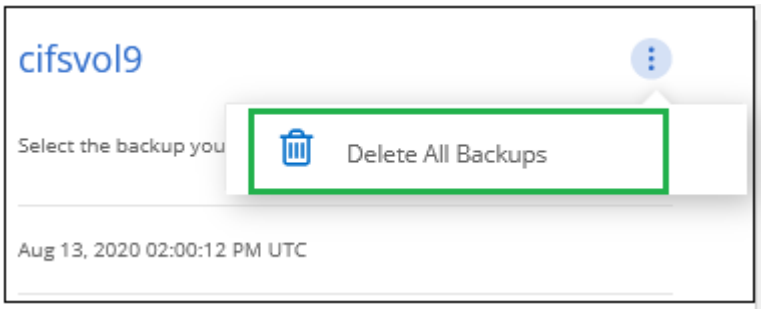
La sauvegarde dans le cloud vous permet de supprimer toutes les *sauvegardes d'un volume spécifique. Vous ne pouvez pas supprimer des _sauvegardes* individuelles.

Vous pouvez le faire si vous n'avez plus besoin des sauvegardes ou si vous avez supprimé le volume source et que vous souhaitez supprimer toutes les sauvegardes.

> Si vous prévoyez de supprimer un système Cloud Volumes ONTAP ou ONTAP sur site qui dispose de sauvegardes, vous devez supprimer les sauvegardes **avant** de supprimer le système. La sauvegarde dans le cloud ne supprime pas automatiquement les sauvegardes lorsque vous supprimez un système et l'interface utilisateur ne prend pas en charge la suppression des sauvegardes après la suppression du système.

Étapes

1. En haut de Cloud Manager, cliquez sur **Backup**.
2. Dans la liste des volumes, recherchez le volume et cliquez sur **Afficher la liste de sauvegarde**.
3. Cliquez sur ••• Et sélectionnez **Supprimer toutes les sauvegardes**.



4. Dans la boîte de dialogue de confirmation, cliquez sur **Supprimer**.

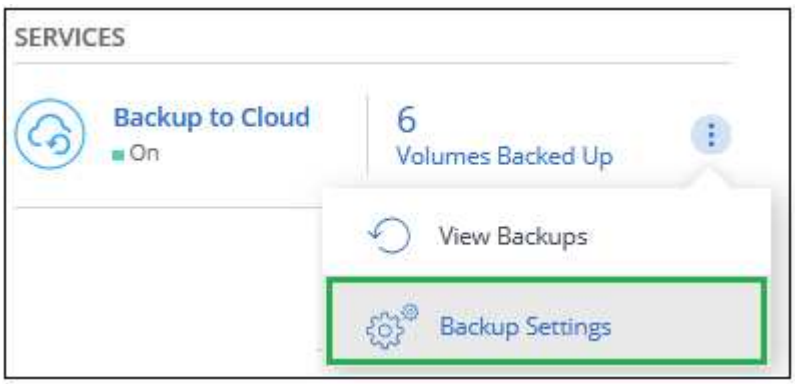
Désactivation de la sauvegarde dans le cloud

La désactivation de la sauvegarde dans le cloud pour un environnement de travail désactive les sauvegardes de chaque volume du système. Elle désactive également la restauration d'un volume. Les sauvegardes existantes ne seront pas supprimées.

Notez que vous continuerez d'être facturé par votre fournisseur cloud pour les coûts de stockage objet correspondant à la capacité que vos sauvegardes utilisent, à moins que vous ne supprimiez les sauvegardes.

Étapes

1. Sélectionnez l'environnement de travail.
2. Cliquez sur ⋮ Et sélectionnez **Paramètres de sauvegarde**.



3. Dans la page *Backup Settings*, cliquez sur ••• Pour l'environnement de travail et sélectionnez **Désactiver la sauvegarde dans le cloud**.

4. Dans la boîte de dialogue de confirmation, cliquez sur **Désactiver**.

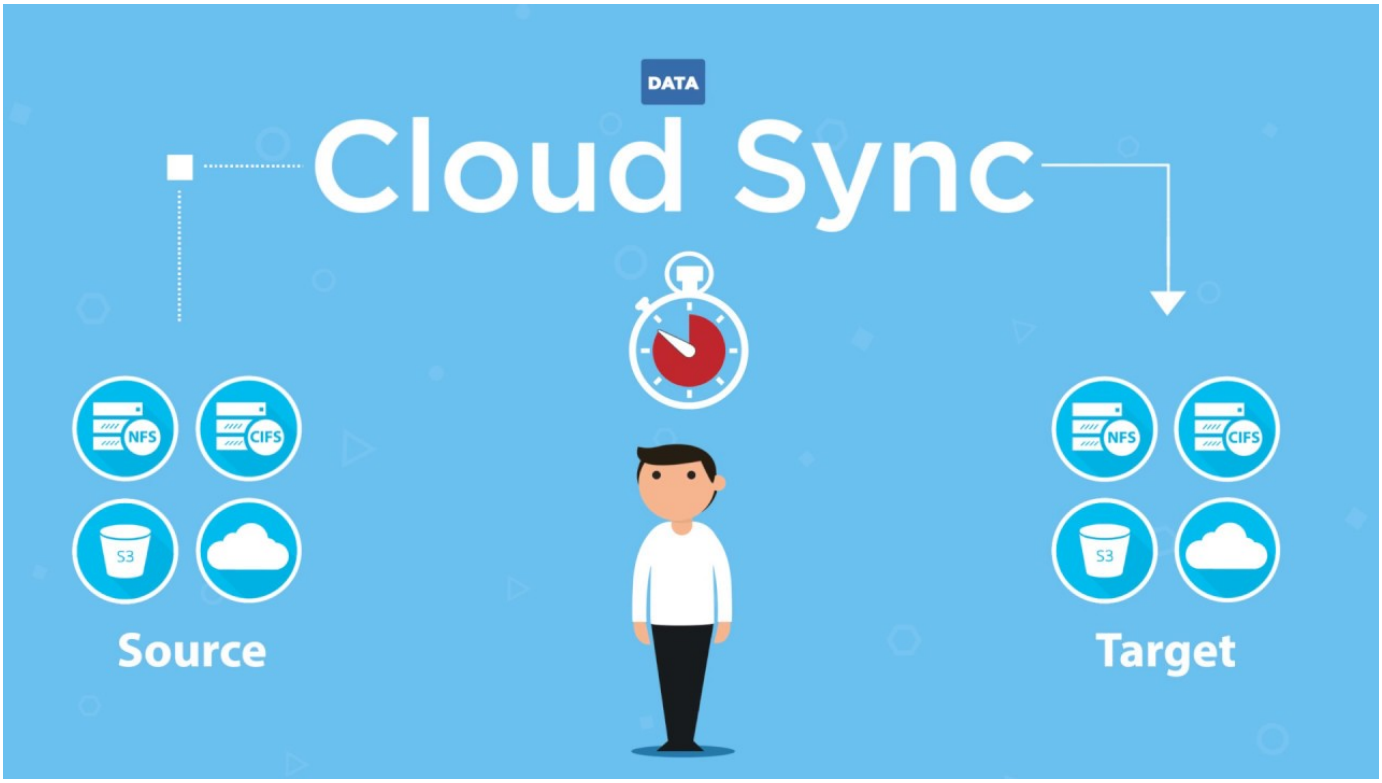
Copiez et synchronisez les données

Présentation de Cloud Sync

Le service NetApp Cloud Sync offre un moyen simple, sécurisé et automatisé de migrer vos données vers n'importe quelle cible, dans le cloud ou sur votre site. Qu'il s'agisse d'un dataset NAS basé sur fichiers (NFS ou SMB), d'un format d'objet Amazon simple Storage Service (S3), d'une appliance NetApp StorageGRID® ou de tout magasin d'objets d'un autre fournisseur cloud, Cloud Sync peut la convertir et la déplacer pour vous.

Caractéristiques

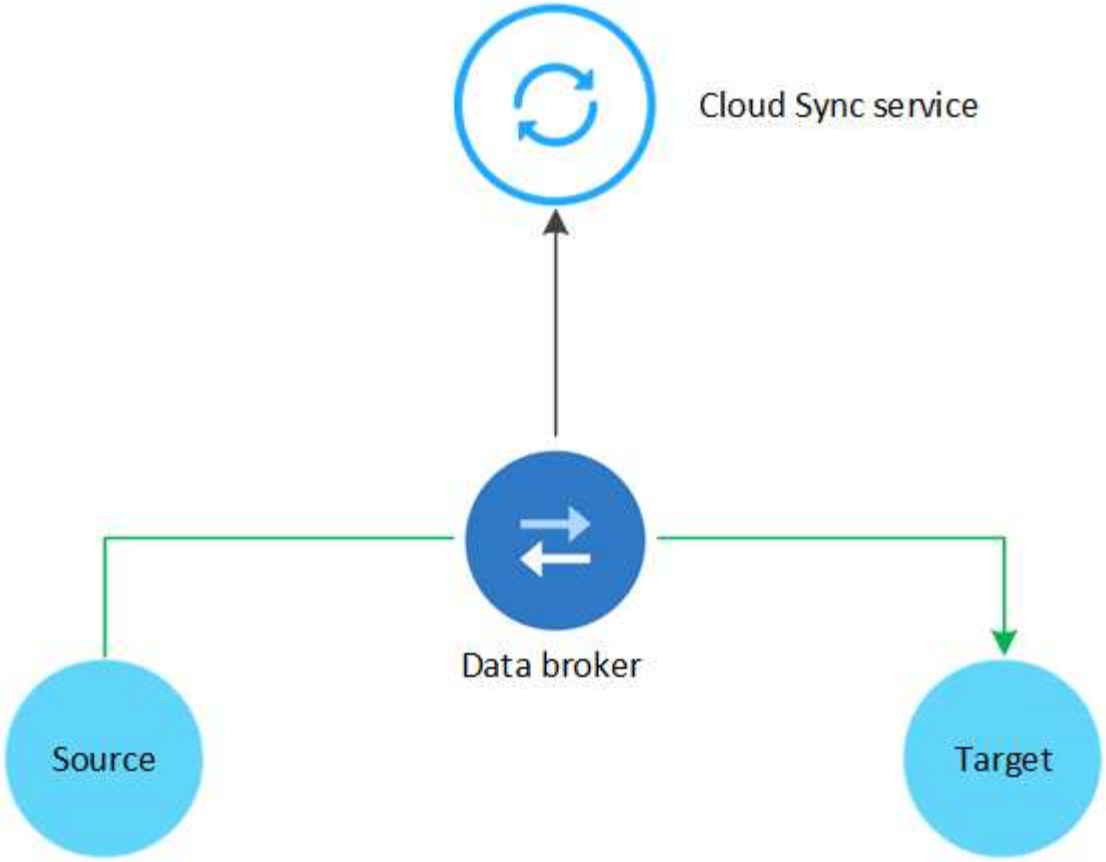
Regardez la vidéo suivante pour une présentation de Cloud Sync :



Fonctionnement de Cloud Sync

Cloud Sync est une plateforme de services à la demande (SaaS), qui consiste en un courtier en données, une interface cloud disponible via Cloud Manager, ainsi qu'une source et une cible.

L'image suivante montre la relation entre les composants Cloud Sync :



Le logiciel de courtier de données NetApp synchronise les données d'une source vers une cible (appelée « relation synchrone »). Vous pouvez exécuter le data broker dans AWS, Azure, Google Cloud Platform ou sur votre site. Le courtier de données a besoin d'une connexion Internet sortante sur le port 443 pour pouvoir communiquer avec le service Cloud Sync et contacter quelques autres services et référentiels. "Afficher la liste des noeuds finaux".

Après la copie initiale, le service synchronise toutes les données modifiées en fonction de la planification que vous avez définie.

Types de stockage pris en charge

Cloud Sync prend en charge les types de stockage suivants :

- Tout serveur NFS
- Tout serveur SMB
- EFS AWS
- AWS S3
- Blob d'Azure
- Azure NetApp Files
- Cloud Volumes Service
- Cloud Volumes ONTAP
- Google Cloud Storage
- IBM Cloud Object Storage

- Cluster ONTAP sur site
- Stockage ONTAP S3
- StorageGRID

"Vérifiez les relations de synchronisation prises en charge".

Le coût

Il existe deux types de coûts associés à l'utilisation de Cloud Sync : les frais de ressources et les frais de service.

Frais de ressources

Les coûts en ressources sont liés aux coûts de calcul et de stockage pour l'exécution du courtier en données dans le cloud.

Frais de service

Il existe deux façons de payer les relations de synchronisation après la fin de votre essai gratuit de 14 jours. La première option consiste à vous abonner à AWS ou à Azure, ce qui vous permet de payer une heure ou une année. La deuxième option consiste à acheter des licences directement auprès de NetApp. Pour plus d'informations, lisez les sections suivantes.

Abonnement Marketplace

L'abonnement au service Cloud Sync d'AWS ou d'Azure vous permet de payer à un tarif horaire ou de payer annuellement. "Vous pouvez vous abonner via AWS ou Azure", selon l'endroit où vous voulez être facturé.

Abonnements horaires

Avec un abonnement au paiement à l'utilisation à l'heure, le service Cloud Sync facture l'heure en fonction du nombre de relations de synchronisation créées.

- "Voir les tarifs à Azure"
- "Consultez les tarifs à la carte dans AWS"

Abonnements annuels

Un abonnement annuel fournit une licence pour 20 relations de synchronisation que vous payez avant. Si vous utilisez plus de 20 relations synchronisées et que vous vous êtes abonné à Azure, vous payez les relations supplémentaires à l'heure.

"Voir les tarifs annuels dans AWS"

Licences de NetApp

L'achat de licences directement auprès de NetApp constitue une autre façon de payer les relations de synchronisation. Chaque licence vous permet de créer jusqu'à 20 relations de synchronisation.

Vous pouvez utiliser ces licences avec un abonnement AWS ou Azure. Par exemple, si vous disposez de 25 relations de synchronisation, vous pouvez payer les 20 premières relations de synchronisation à l'aide d'une licence, puis effectuer des opérations de paiement à la demande à partir d'AWS ou d'Azure avec les 5 autres relations de synchronisation.

"Découvrez comment acheter des licences et les ajouter à Cloud Sync".

Termes de la licence

Les clients qui achètent une licence BYOL (Bring Your Own License) au service Cloud Sync doivent être conscients des limites associées au droit de licence.

- Les clients ont le droit de tirer parti de la licence BYOL pour une durée maximale d'un an à compter de la date de livraison.
- Les clients ont le droit de tirer parti de la licence BYOL pour établir et ne pas dépasser un total de 20 connexions individuelles entre une source et une cible (chaque " relation de synchronisation ").
- Le droit d'un client expire à la fin de la période d'un an de licence, que le Client ait atteint la limite de 20 relations de synchronisation.
- Si le Client choisit de renouveler sa licence, les relations de synchronisation non utilisées associées à l'octroi de licence précédent ne passent PAS au renouvellement de la licence.

Confidentialité des données

NetApp n'a pas accès aux identifiants que vous indiquez lors de l'utilisation du service Cloud Sync. Les informations d'identification sont stockées directement sur l'ordinateur du courtier de données, qui réside dans votre réseau.

Selon la configuration choisie, Cloud Sync peut vous demander des informations d'identification lorsque vous créez une nouvelle relation. Par exemple, lors de la configuration d'une relation qui inclut un serveur SMB, ou lors du déploiement du courtier en données dans AWS.

Ces informations d'identification sont toujours enregistrées directement dans le data broker lui-même. Le courtier en données réside sur une machine de votre réseau, qu'elle soit hébergée sur site ou dans votre compte cloud. Les informations d'identification ne sont jamais mises à la disposition de NetApp.

Les informations d'identification sont chiffrées localement sur la machine du courtier de données à l'aide de HashiCorp Vault.

Limites

- Cloud Sync n'est pas pris en charge en Chine.
- Outre la Chine, le courtier de données Cloud Sync n'est pas pris en charge dans les régions suivantes :
  - AWS GovCloud (États-Unis)
  - Azure US Gov
  - Azure US DoD

Commencez

Démarrage rapide de Cloud Sync

La mise en route du service Cloud Sync comprend quelques étapes.

Préparez votre source et votre cible

Vérifiez que la source et la cible sont prises en charge et configurées. L'exigence la plus importante est de vérifier la connectivité entre le courtier de données et les emplacements source et cible. "En savoir plus >>".

Préparez un emplacement pour le data broker NetApp

Le logiciel de courtier de données NetApp synchronise les données d'une source vers une cible (appelée « relation synchrone »). Vous pouvez exécuter le data broker dans AWS, Azure, Google Cloud Platform ou sur votre site. Le courtier de données a besoin d'une connexion Internet sortante sur le port 443 pour pouvoir communiquer avec le service Cloud Sync et contacter quelques autres services et référentiels. "Afficher la liste des noeuds finaux".

Cloud Sync vous guide tout au long du processus d'installation lorsque vous créez une relation de synchronisation, à quel point vous pouvez déployer le data broker dans le cloud ou télécharger un script d'installation pour votre propre hôte Linux.

- "Consultez l'installation d'AWS"
- "Vérifiez l'installation d'Azure"
- "Vérifiez l'installation de GCP"
- "Vérifiez l'installation de l'hôte Linux"

Créez votre première relation de synchronisation

Connectez-vous à "Le gestionnaire Cloud", Cliquez sur **Sync**, puis faites glisser et déposez vos sélections pour la source et la cible. Suivez les invites pour terminer la configuration. "En savoir plus >>".

Payez vos relations de synchronisation après la fin de votre essai gratuit

Abonnez-vous à AWS ou Azure pour payer à votre gré ou pour payer chaque année. Ou achetez des licences directement auprès de NetApp. Il vous suffit d'aller à la page Paramètres de licence de Cloud Sync pour la configurer. "En savoir plus >>".

Préparation de la source et de la cible

Préparez la synchronisation des données en vérifiant que votre source et votre cible sont prises en charge et configurées.

Relations de synchronisation prises en charge

Cloud Sync vous permet de synchroniser des données d'une source vers une cible (appelée *sync relationship*). Vous devez comprendre les relations prises en charge avant de commencer.

Emplacement de la source	Emplacements cibles pris en charge
EFS AWS	• EFS AWS • AWS S3 • Blob d'Azure • Fichiers NetApp Azure (NFS) • Cloud Volumes ONTAP (NFS) • Service de volumes cloud (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Serveur NFS • Cluster ONTAP sur site • StorageGRID
AWS S3	• EFS AWS • AWS S3 • Blob d'Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • IBM Cloud Object Storage • Google Cloud Storage • Serveur NFS • Cluster ONTAP sur site • Serveur SMB • StorageGRID

Emplacement de la source	Emplacements cibles pris en charge
Blob d'Azure	• EFS AWS • AWS S3 • Blob d'Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • IBM Cloud Object Storage • Serveur NFS • Cluster ONTAP sur site • Serveur SMB • StorageGRID
Fichiers NetApp Azure (NFS)	• EFS AWS • AWS S3 • Blob d'Azure • Fichiers NetApp Azure (NFS) • Cloud Volumes ONTAP (NFS) • Service de volumes cloud (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Serveur NFS • Cluster ONTAP sur site • StorageGRID
Azure NetApp Files (PME)	• AWS S3 • Blob d'Azure • Azure NetApp Files (PME) • Cloud Volumes ONTAP (PME) • Cloud Volumes Service (PME) • Google Cloud Storage • IBM Cloud Object Storage • Cluster ONTAP sur site • Serveur SMB • StorageGRID

Emplacement de la source	Emplacements cibles pris en charge
Cloud Volumes ONTAP (NFS)	• EFS AWS • AWS S3 • Blob d'Azure • Fichiers NetApp Azure (NFS) • Cloud Volumes ONTAP (NFS) • Service de volumes cloud (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Serveur NFS • Cluster ONTAP sur site • StorageGRID
Cloud Volumes ONTAP (PME)	• AWS S3 • Blob d'Azure • Azure NetApp Files (PME) • Cloud Volumes ONTAP (PME) • Cloud Volumes Service (PME) • Google Cloud Storage • IBM Cloud Object Storage • Cluster ONTAP sur site • Serveur SMB • StorageGRID
Service de volumes cloud (NFS)	• EFS AWS • AWS S3 • Blob d'Azure • Fichiers NetApp Azure (NFS) • Cloud Volumes ONTAP (NFS) • Service de volumes cloud (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Serveur NFS • Cluster ONTAP sur site • StorageGRID

Emplacement de la source	Emplacements cibles pris en charge
Cloud Volumes Service (PME)	• AWS S3 • Blob d'Azure • Azure NetApp Files (PME) • Cloud Volumes ONTAP (PME) • Cloud Volumes Service (PME) • Google Cloud Storage • IBM Cloud Object Storage • Cluster ONTAP sur site • Serveur SMB • StorageGRID
Google Cloud Storage	• EFS AWS • AWS S3 • Blob d'Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • IBM Cloud Object Storage • Serveur NFS • Cluster ONTAP sur site • Serveur SMB • StorageGRID
IBM Cloud Object Storage	• EFS AWS • AWS S3 • Blob d'Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • Google Cloud Storage • IBM Cloud Object Storage • Serveur NFS • Cluster ONTAP sur site • Serveur SMB • StorageGRID

Emplacement de la source	Emplacements cibles pris en charge
Serveur NFS	• EFS AWS • AWS S3 • Blob d'Azure • Fichiers NetApp Azure (NFS) • Cloud Volumes ONTAP (NFS) • Service de volumes cloud (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Serveur NFS • Cluster ONTAP sur site • StorageGRID
Cluster ONTAP sur site (NFS)	• EFS AWS • AWS S3 • Blob d'Azure • Fichiers NetApp Azure (NFS) • Cloud Volumes ONTAP (NFS) • Service de volumes cloud (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Serveur NFS • Cluster ONTAP sur site • StorageGRID
Cluster ONTAP sur site (PME)	• AWS S3 • Blob d'Azure • Azure NetApp Files (PME) • Cloud Volumes ONTAP (PME) • Cloud Volumes Service (PME) • Google Cloud Storage • IBM Cloud Object Storage • Cluster ONTAP sur site • Serveur SMB • StorageGRID
Stockage ONTAP S3	• StorageGRID

Emplacement de la source	Emplacements cibles pris en charge
Serveur SMB	• AWS S3 • Blob d'Azure • Azure NetApp Files (PME) • Cloud Volumes ONTAP (NFS) • Service de volumes cloud (NFS) • IBM Cloud Object Storage • Google Cloud Storage • Cluster ONTAP sur site • Serveur SMB • StorageGRID
StorageGRID	• EFS AWS • AWS S3 • Blob d'Azure • Azure NetApp Files • Cloud Volumes ONTAP • Cloud Volumes Service • IBM Cloud Object Storage • Google Cloud Storage • Serveur NFS • Cluster ONTAP sur site • Stockage ONTAP S3 • Serveur SMB • StorageGRID

Remarques :

1. Vous pouvez choisir un niveau de stockage spécifique à Azure Blob lorsqu'un conteneur Blob est la cible :
    - Stockage à chaud
    - Stockage cool
2. lorsque AWS S3 est la cible, vous pouvez choisir une classe de stockage S3 spécifique :
    - Standard (il s'agit de la classe par défaut)
    - Le Tiering intelligent
    - Accès autonome et peu fréquent
    - Un seul accès à Zone-Infrequent
    - Glacier
    - Archives profondes des Glaciers

Mise en réseau de la source et de la cible

- La source et la cible doivent disposer d'une connexion réseau au data broker.

  Par exemple, si un serveur NFS se trouve dans votre data center et que le data broker est dans AWS, vous avez besoin d'une connexion réseau (VPN ou Direct Connect) entre votre réseau et le VPC.

- NetApp recommande de configurer la source, la cible et le courtier de données pour qu'ils utilisent un service NTP (Network Time Protocol). La différence de temps entre les trois composants ne doit pas dépasser 5 minutes.

Exigences source et cible

Vérifiez que votre source et vos cibles répondent aux exigences suivantes.

exigences du compartiment AWS S3

Assurez-vous que votre seau AWS S3 répond aux exigences suivantes.

Emplacements des courtiers de données pris en charge pour AWS S3

Les relations de synchronisation qui incluent le stockage S3 nécessitent un data broker déployé dans AWS ou sur votre site. Dans les deux cas, Cloud Sync vous invite à associer le courtier de données à un compte AWS lors de l'installation.

- "Découvrez comment déployer le courtier de données AWS"
- "Découvrez comment installer le courtier de données sur un hôte Linux"

Régions AWS prises en charge

Toutes les régions sont prises en charge à l'exception des régions Chine et GovCloud (États-Unis).

Autorisations requises pour les compartiments S3 dans d'autres comptes AWS

Lors de la configuration d'une relation de synchronisation, vous pouvez spécifier un compartiment S3 qui réside dans un compte AWS non associé au courtier de données.

"Les autorisations incluses dans ce fichier JSON" Doit être appliqué au compartiment S3 pour que le courtier de données puisse y accéder. Ces autorisations permettent au courtier de copier des données depuis et vers la rubrique et de lister les objets dans la rubrique.

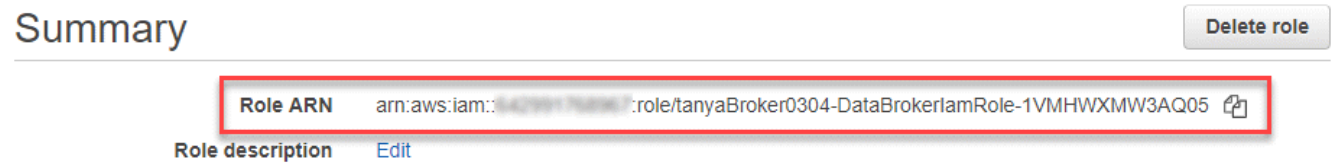
Notez les informations suivantes sur les autorisations incluses dans le fichier JSON :

1. *<BucketName>* est le nom du compartiment qui réside dans le compte AWS non associé au courtier en données.
2. *<RoleARN>* doit être remplacé par l'un des éléments suivants :

   - Si le courtier de données a été installé manuellement sur un hôte Linux, *RoleARN* doit être l'ARN de l'utilisateur AWS pour lequel vous avez fourni des informations d'identification AWS lors du déploiement du courtier de données.
   - Si le courtier de données a été déployé dans AWS à l'aide du modèle CloudFormation, *RoleARN* doit être l'ARN du rôle IAM créé par le modèle.

     Vous pouvez trouver le nom ARN du rôle en accédant à la console EC2, en sélectionnant l'instance du

courtier de données et en cliquant sur le rôle IAM dans l'onglet Description. La page Résumé de la console IAM qui contient le numéro de référence du rôle doit apparaître.



exigences de stockage Azure Blob

Assurez-vous que votre stockage Azure Blob répond aux exigences suivantes.

Emplacements des courtiers de données pris en charge pour Azure Blob

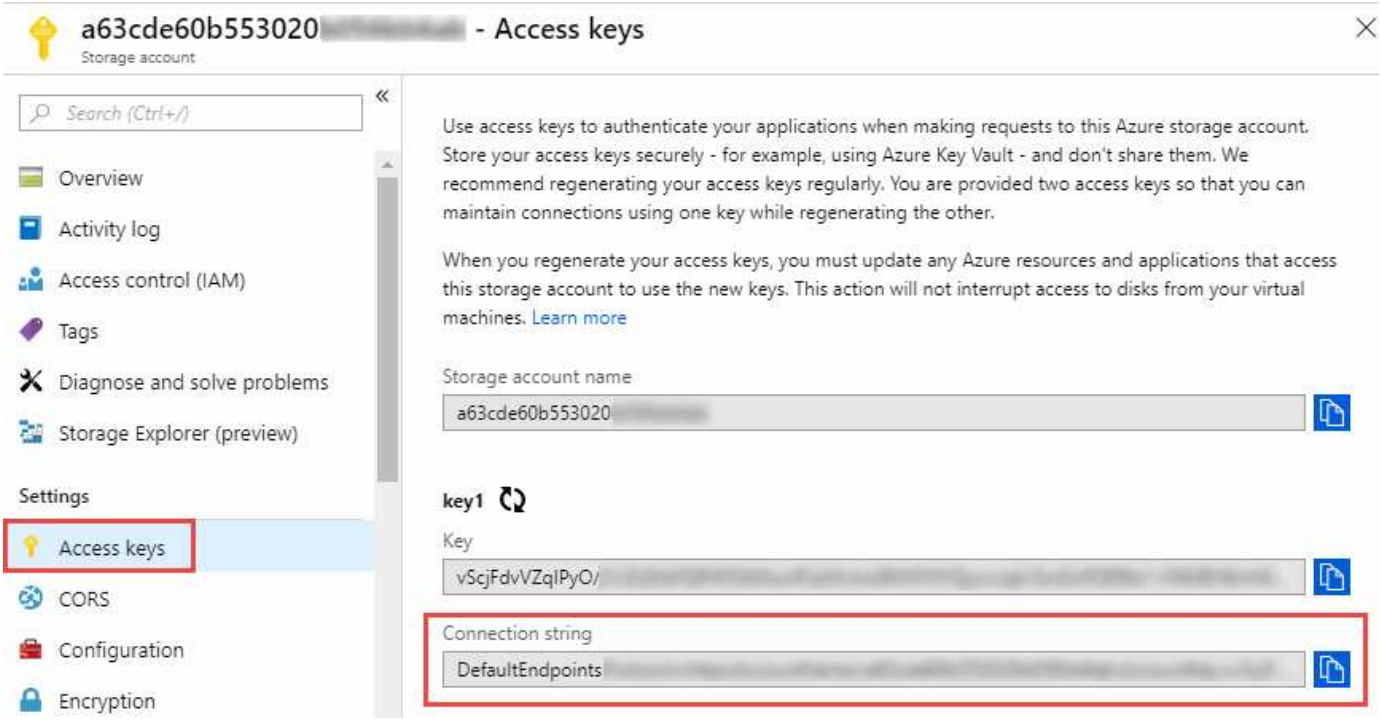
Le courtier de données peut résider dans n'importe quel emplacement lorsqu'une relation de synchronisation inclut le stockage Blob d'Azure.

Régions Azure prises en charge

Toutes les régions sont prises en charge à l'exception des régions China, US Gov et US DoD.

Chaîne de connexion requise pour les relations qui incluent Azure Blob et NFS/SMB

Lors de la création d'une relation synchrone entre un conteneur Azure Blob et un serveur NFS ou SMB, vous devez fournir à Cloud Sync la chaîne de connexion du compte de stockage :

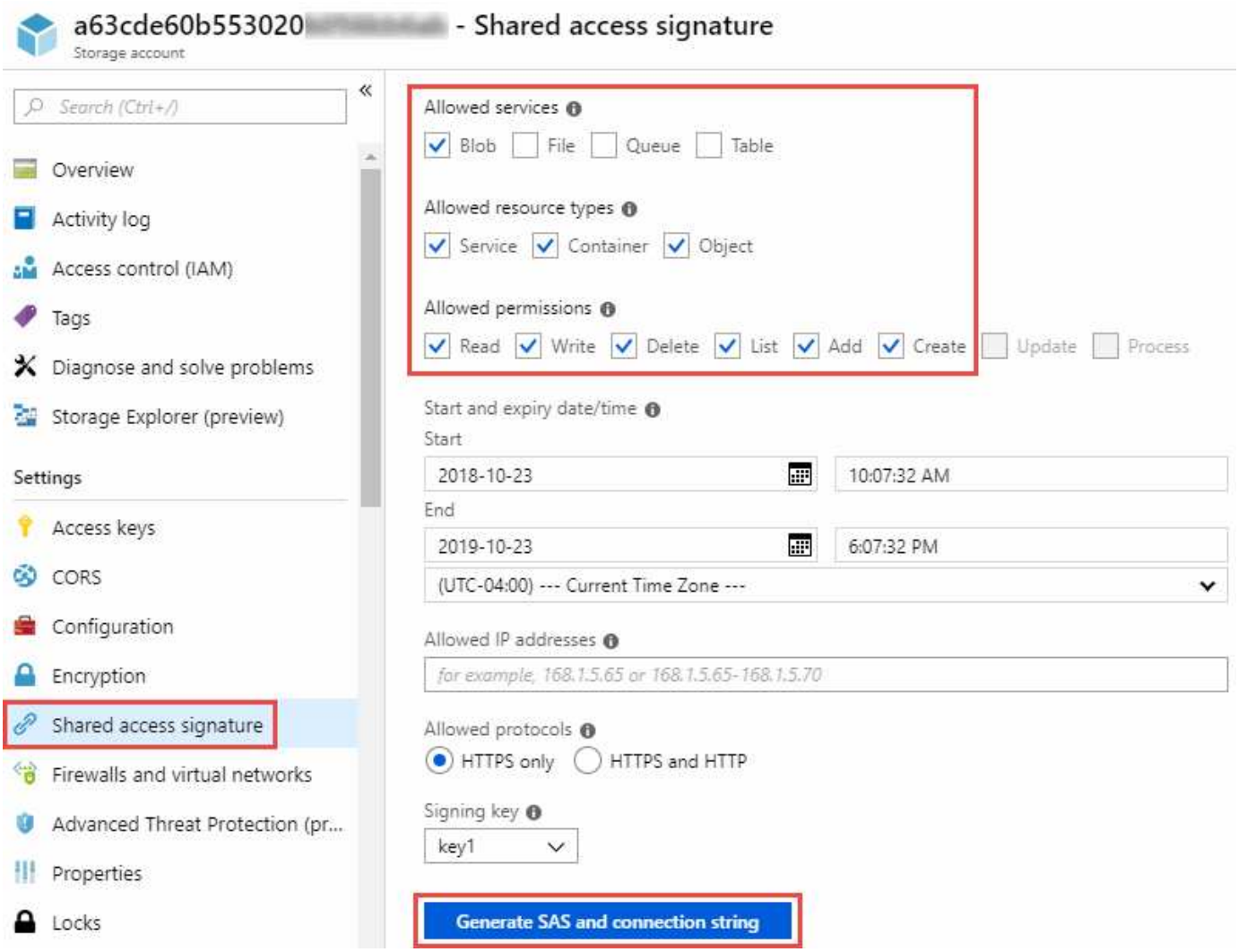


Pour synchroniser les données entre deux conteneurs Azure Blob, la chaîne de connexion doit inclure une "signature d'accès partagé" (SAS). Vous avez également la possibilité d'utiliser un SAS lors de la synchronisation entre un conteneur Blob et un serveur NFS ou SMB.

Le SAS doit autoriser l'accès au service Blob et à tous les types de ressources (Service, Conteneur et Objet).

Le SAS doit également inclure les autorisations suivantes :

- Pour le conteneur Blob source : Lecture et liste
- Pour le conteneur Blob cible : lecture, écriture, liste, ajout et création



Condition Azure NetApp Files

Utilisez le niveau de service Premium ou Ultra lorsque vous synchronisez des données vers ou depuis Azure NetApp Files. Vous risquez de rencontrer des défaillances et des problèmes de performances si le niveau de service des disques est standard.

Consultez un architecte de solutions si vous avez besoin d'aide pour déterminer le niveau de service adapté à vos besoins. La taille et le niveau de volume déterminent le débit pouvant être optimal.

"En savoir plus sur le débit et les niveaux de service de Azure NetApp Files".

Exigences relatives au compartiment de stockage Google Cloud

Assurez-vous que votre rayon de stockage Google Cloud Storage répond aux exigences suivantes.

Emplacements des courtiers de données pris en charge pour Google Cloud Storage

Les relations de synchronisation qui incluent Google Cloud Storage nécessitent un data broker déployé dans GCP ou sur votre site. Cloud Sync vous guide tout au long du processus d'installation du courtier de données lorsque vous créez une relation de synchronisation.

- "Découvrez comment déployer le courtier de données GCP"
- "Découvrez comment installer le courtier de données sur un hôte Linux"

Régions GCP prises en charge

Toutes les régions sont prises en charge.

Configuration requise pour le serveur NFS

- Le serveur NFS peut être un système NetApp ou un système non NetApp.
- Le serveur de fichiers doit permettre à l'hôte du courtier de données d'accéder aux exportations.
- Les versions NFS 3, 4.0, 4.1 et 4.2 sont prises en charge.

  La version souhaitée doit être activée sur le serveur.

- Si vous souhaitez synchroniser les données NFS à partir d'un système ONTAP, assurez-vous que l'accès à la liste d'export NFS pour un SVM est activé (vserver nfs modify -vserver *svm_name* -showmount activé).

  Le paramètre par défaut de showmount est *Enabled* commençant par ONTAP 9.2.

Exigences du stockage ONTAP S3

ONTAP 9.7 prend en charge Amazon simple Storage Service (Amazon S3) comme préversion publique. "En savoir plus sur la prise en charge d'ONTAP pour Amazon S3".

Lorsque vous configurez une relation de synchronisation incluant le stockage ONTAP S3, vous devez fournir les éléments suivants :

- L'adresse IP du LIF connecté à ONTAP S3
- La clé d'accès et la clé secrète que ONTAP est configuré pour utiliser

Configuration requise pour le serveur SMB

- Le serveur SMB peut être un système NetApp ou un système non NetApp.
- Le serveur de fichiers doit permettre à l'hôte du courtier de données d'accéder aux exportations.
- Les versions SMB 1.0, 2.0, 2.1, 3.0 et 3.11 sont prises en charge.
- Accordez au groupe « administrateurs » les autorisations « contrôle total » aux dossiers source et cible.

  Si vous n'accordez pas cette autorisation, le courtier de données peut ne pas disposer des autorisations suffisantes pour obtenir les listes de contrôle d'accès sur un fichier ou un répertoire. Si cela se produit, vous recevrez l'erreur suivante : "erreur getxattr 95"

Limitation SMB pour les répertoires et les fichiers cachés

Une limitation SMB affecte les répertoires et les fichiers masqués lors de la synchronisation des données entre les serveurs SMB. Si l'un des répertoires ou des fichiers du serveur SMB source était masqué par Windows, l'attribut masqué n'est pas copié sur le serveur SMB cible.

Comportement de la synchronisation SMB en raison d'une limitation de la sensibilité au cas

Le protocole SMB n'est pas sensible à la casse, ce qui signifie que les lettres majuscules et minuscules sont traitées comme étant les mêmes. Ce comportement peut entraîner un écrasement des fichiers et des erreurs de copie de répertoire si une relation de synchronisation inclut un serveur SMB et que des données existent déjà sur la cible.

Par exemple, disons qu'il y a un fichier nommé « a » sur la source et un fichier nommé « A » sur la cible. Lorsque Cloud Sync copie le fichier nommé « a » sur la cible, le fichier « A » est remplacé par le fichier « a » de la source.

Dans le cas des répertoires, disons qu'il y a un répertoire nommé "b" sur la source et un répertoire nommé "B" sur la cible. Lorsque Cloud Sync tente de copier le répertoire nommé « b » vers la cible, Cloud Sync reçoit une erreur indiquant que le répertoire existe déjà. Par conséquent, Cloud Sync ne parvient toujours pas à copier le répertoire nommé "b."

La meilleure façon d'éviter cette limitation est de garantir la synchronisation des données vers un répertoire vide.

Autorisations d'accès à une destination SnapMirror

Si la source d'une relation de synchronisation est une destination SnapMirror (en lecture seule), des autorisations « read/list » suffisent pour synchroniser les données de la source vers une cible.

Présentation de la mise en réseau pour Cloud Sync

La mise en réseau pour Cloud Sync inclut la connectivité entre le courtier de données et les emplacements source et cible, ainsi qu'une connexion Internet sortante du courtier de données sur le port 443.

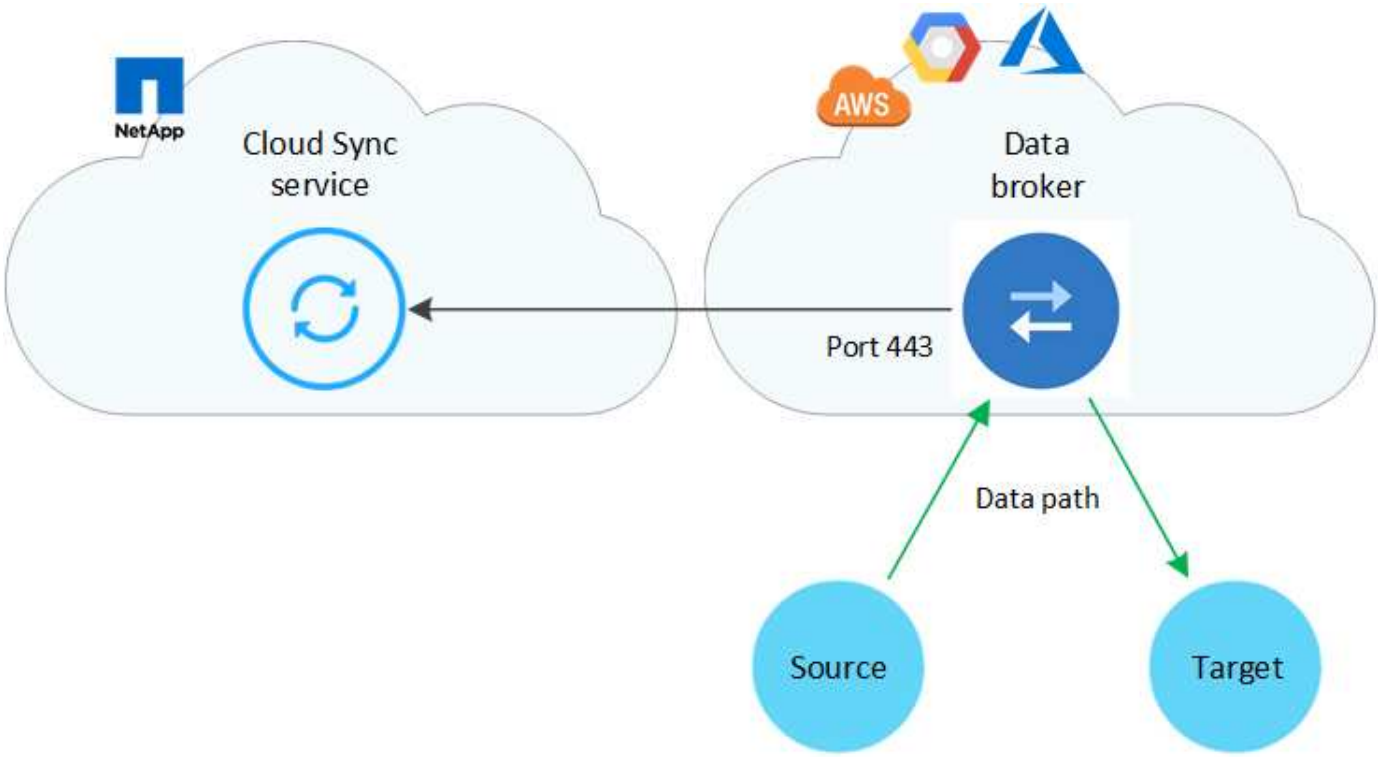
Emplacement du courtier en données

Vous pouvez installer le courtier en données dans le cloud ou sur site.

Data broker dans le cloud

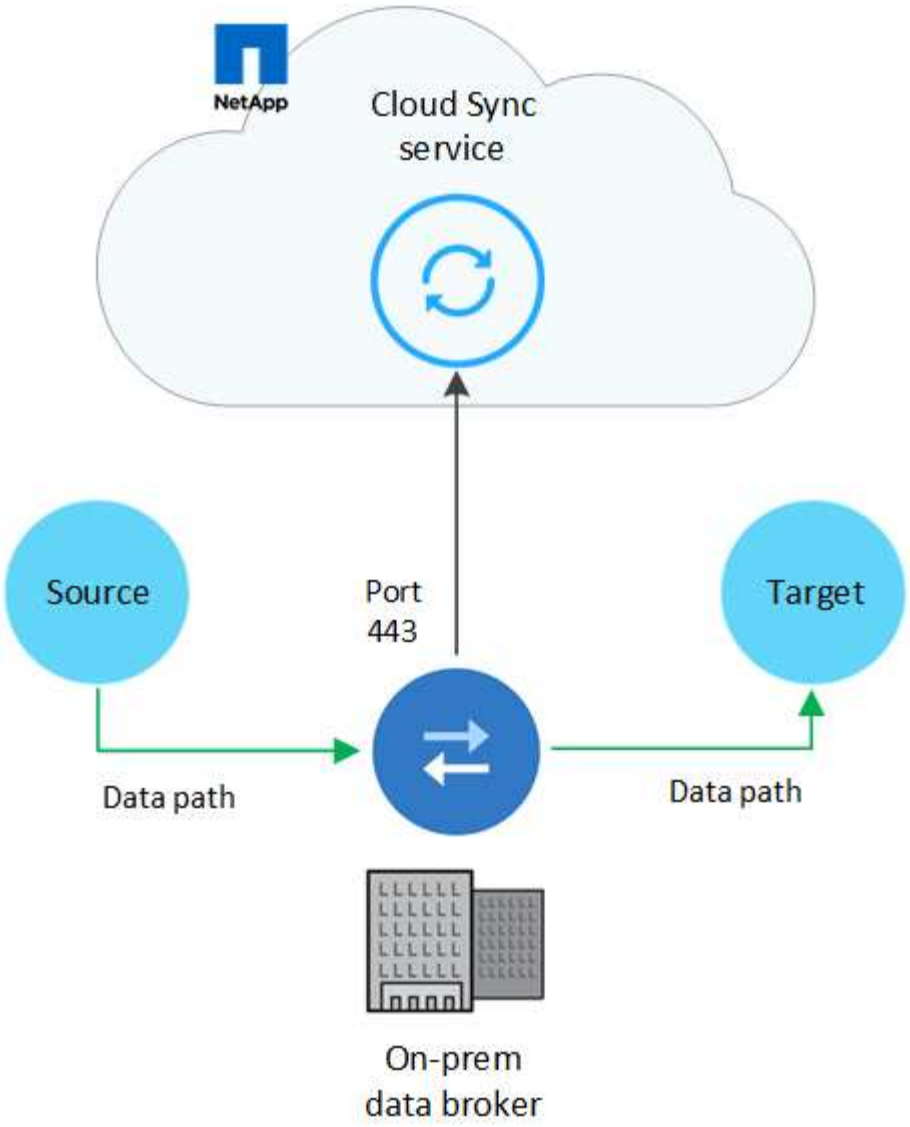
L'image suivante montre le courtier en données qui s'exécute dans le cloud, soit dans AWS, GCP ou Azure. La source et la cible peuvent être hébergées quel que soit le lieu, à condition que le courtier soit connecté. Par exemple, vous pouvez disposer d'une connexion VPN entre votre data center et votre fournisseur de cloud.

Lorsque Cloud Sync déploie le courtier de données dans AWS, Azure ou GCP, il crée un groupe de sécurité qui active la communication sortante requise.



Data broker sur votre site

L'image suivante montre le courtier de données qui s'exécute sur-prem, dans un data center. Là encore, la source et la cible peuvent être hébergées quel que soit le lieu, tant qu'il y a une connexion avec le courtier de données.



Configuration réseau requise

- La source et la cible doivent disposer d'une connexion réseau au data broker.

  Par exemple, si un serveur NFS se trouve dans votre data center et que le data broker est dans AWS, vous avez besoin d'une connexion réseau (VPN ou Direct Connect) entre votre réseau et le VPC.

- Le courtier de données a besoin d'une connexion Internet sortante pour pouvoir interroger le service Cloud Sync sur le port 443.
- NetApp recommande de configurer la source, la cible et le courtier de données pour qu'ils utilisent un service NTP (Network Time Protocol). La différence de temps entre les trois composants ne doit pas dépasser 5 minutes.

Terminaux de mise en réseau

Pour communiquer avec le service Cloud Sync et contacter quelques autres services et référentiels, le courtier de données NetApp a besoin d'un accès Internet sortant sur le port 443. Votre navigateur Web local nécessite également l'accès aux points de terminaison pour certaines actions. Si vous devez limiter la connectivité sortante, reportez-vous à la liste de terminaux suivante lors de la configuration de votre pare-feu pour le trafic sortant.

Terminaux du courtier de données

Le courtier de données contacte les terminaux suivants :

Terminaux	Objectif
Olcentgbl.trafficmanager.net:443	Pour contacter un référentiel de mise à jour des packages CentOS pour l'hôte du data broker. Ce noeud final n'est contacté que si vous installez manuellement le courtier de données sur un hôte CentOS.
Rpm.nodesource.com:443 registry.npmjs.org:443 nodejs.org:443	Pour contacter des référentiels pour mettre à jour Node.js, npm et d'autres packages tiers utilisés dans le développement.
Tgz.pm2.io:443	Pour accéder à un référentiel de mise à jour de PM2, un package tiers utilisé pour surveiller Cloud Sync.
Www.myrc.com/fr/ www.myrc.com/fr/ www.myrc.com/fr/ www.myrc.com/fr/	Pour contacter les services AWS utilisés par Cloud Sync pour les opérations (mise en file d'attente de fichiers, enregistrement d'actions et mise à jour du data broker).
s3.*region*.amazonaws.com:443 par exemple : s3.us-east-2.amazonaws.com:443https://docs.aws.amazon.com/general/latest/gr/rande.html#s3_region["Consultez la documentation AWS pour obtenir la liste des terminaux S3"^]	Pour contacter Amazon S3 lorsqu'une relation de synchronisation inclut une rubrique S3.
Cf.cloudsync.netapp.com:443 repo.cloudsync.netapp.com:443	Pour contacter le service Cloud Sync.
Support.netapp.com:443	Pour contacter le support NetApp lors de l'utilisation d'une licence BYOL pour les relations de synchronisation.
fedoraproject.org:443	Pour installer 7z sur la machine virtuelle du courtier de données pendant l'installation et les mises à jour. 7z est nécessaire pour envoyer des messages AutoSupport au support technique NetApp.

Terminaux de navigateur Web

Votre navigateur Web doit accéder au point final suivant pour télécharger les journaux à des fins de dépannage :

logs.cloudsync.netapp.com:443

Comment installer un courtier de données

Installation du courtier de données dans AWS

Lorsque vous créez une relation de synchronisation, choisissez l'option AWS Data Broker pour déployer le logiciel Data Broker sur une nouvelle instance EC2 dans un VPC. Cloud Sync vous guide tout au long du processus d'installation, mais les exigences et les étapes sont répétées sur cette page pour vous aider à vous préparer à l'installation.

Vous avez également la possibilité d'installer le courtier de données sur un hôte Linux existant dans le cloud ou sur votre site. "En savoir plus >>".

Régions AWS prises en charge

Toutes les régions sont prises en charge à l'exception des régions Chine et GovCloud (États-Unis).

Configuration réseau requise

- Le courtier de données a besoin d'une connexion Internet sortante pour pouvoir interroger le service Cloud Sync sur le port 443.

  Lorsque Cloud Sync déploie le courtier de données dans AWS, il crée un groupe de sécurité qui active la communication sortante requise. Notez que vous pouvez configurer le courtier de données pour qu'il utilise un serveur proxy pendant le processus d'installation.

  Si vous devez limiter la connectivité sortante, reportez-vous à la section "liste des noeuds finaux que le courtier de données contacte".

- NetApp recommande de configurer la source, la cible et le courtier de données pour qu'ils utilisent un service NTP (Network Time Protocol). La différence de temps entre les trois composants ne doit pas dépasser 5 minutes.

Autorisations requises pour déployer le courtier de données dans AWS

Le compte utilisateur AWS que vous utilisez pour déployer le courtier de données doit disposer des autorisations incluses dans "Politique fournie par NetApp".

pour utiliser votre propre rôle IAM avec le courtier de données AWS

Lorsque Cloud Sync déploie le data broker, il crée un rôle IAM pour l'instance du data broker. Si vous le souhaitez, vous pouvez déployer le data broker à l'aide de votre propre rôle IAM. Vous pouvez utiliser cette option si votre entreprise dispose de règles de sécurité strictes.

Le rôle IAM doit répondre aux exigences suivantes :

- Le service EC2 doit être autorisé à assumer le rôle IAM en tant qu'entité de confiance.
- "Les autorisations définies dans ce fichier JSON" Doit être attaché au rôle IAM pour que le courtier de données puisse fonctionner correctement.

Suivez les étapes ci-dessous pour spécifier le rôle IAM lors du déploiement du courtier de données.

Installation du data broker

Vous pouvez installer un courtier de données dans AWS lorsque vous créez une relation de synchronisation.

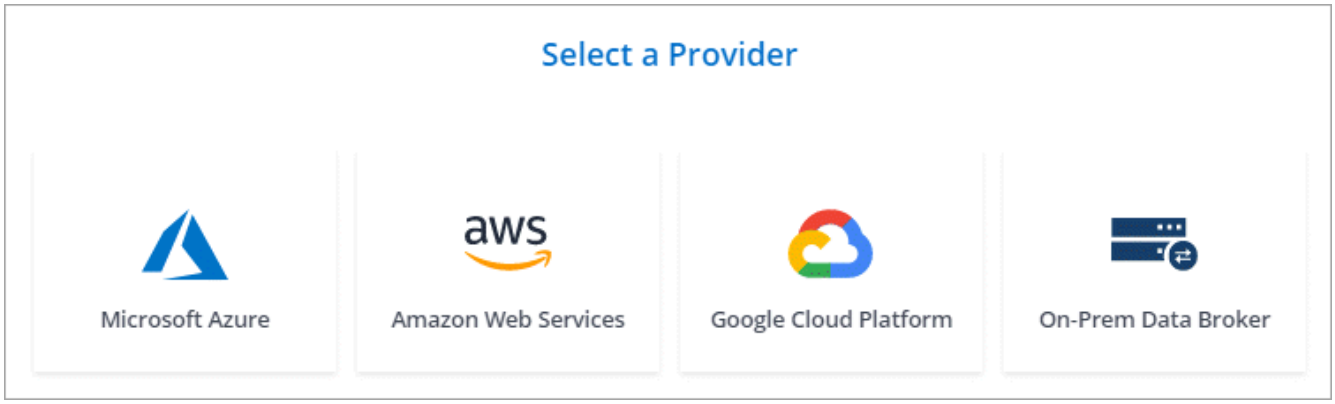
Étapes

1. Cliquez sur **Créer une nouvelle synchronisation**.
2. Sur la page **Define Sync Relationship**, choisissez une source et une cible et cliquez sur **Continuer**.

   Suivez les étapes jusqu'à ce que vous atteiez la page **Data Broker**.

3. Sur la page **Data Broker**, cliquez sur **Create Data Broker**, puis sélectionnez **Amazon Web Services**.

   Si vous avez déjà un courtier de données, vous devez cliquer sur le + icône en premier.



4. Entrez un nom pour le courtier de données et cliquez sur **Continuer**.
5. Entrez une clé d'accès AWS pour que Cloud Sync crée le courtier en données dans AWS.

   Les touches ne sont pas enregistrées ou utilisées à d'autres fins.

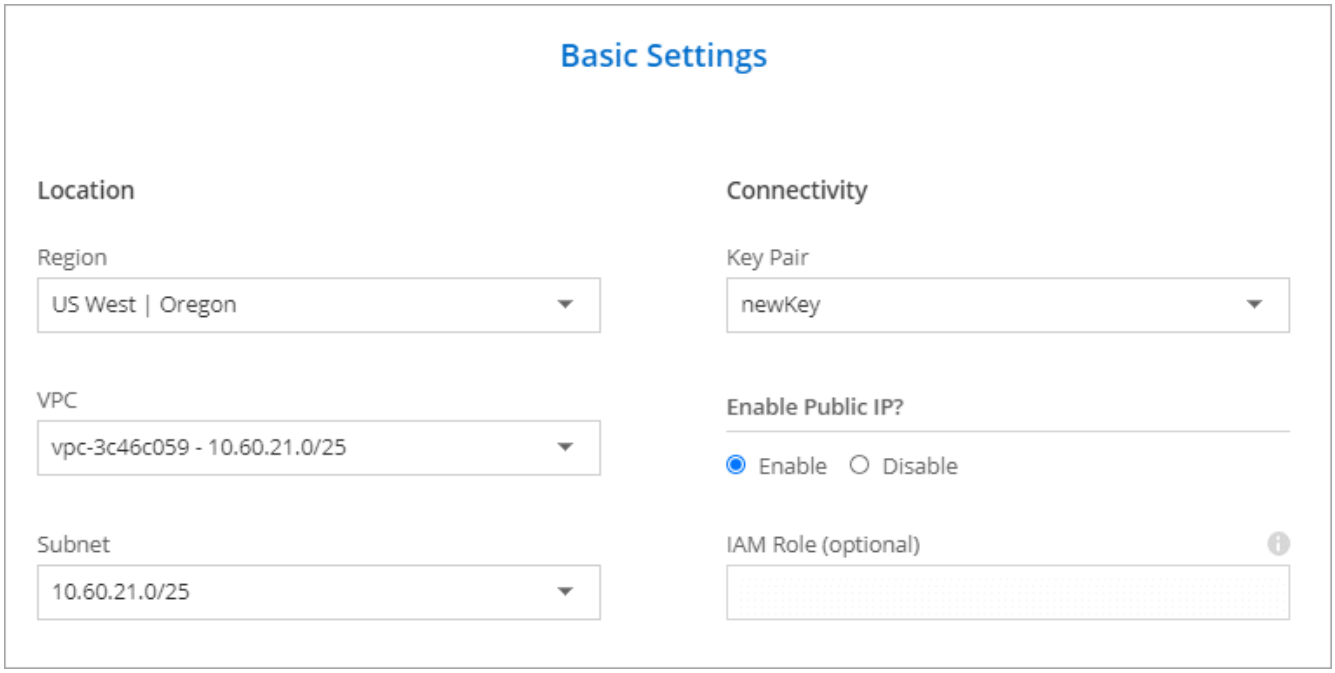
   Si vous préférez ne pas fournir de touches d'accès, cliquez sur le lien en bas de la page pour utiliser un modèle CloudFormation. Lorsque vous utilisez cette option, vous n'avez pas besoin de fournir des identifiants, car vous vous connectez directement à AWS.

   la vidéo suivante montre comment lancer l'instance de courtier de données à l'aide d'un modèle CloudFormation :

   ► https://docs.netapp.com/fr-fr/occm38//media/video_cloud_sync.mp4 *(video)*

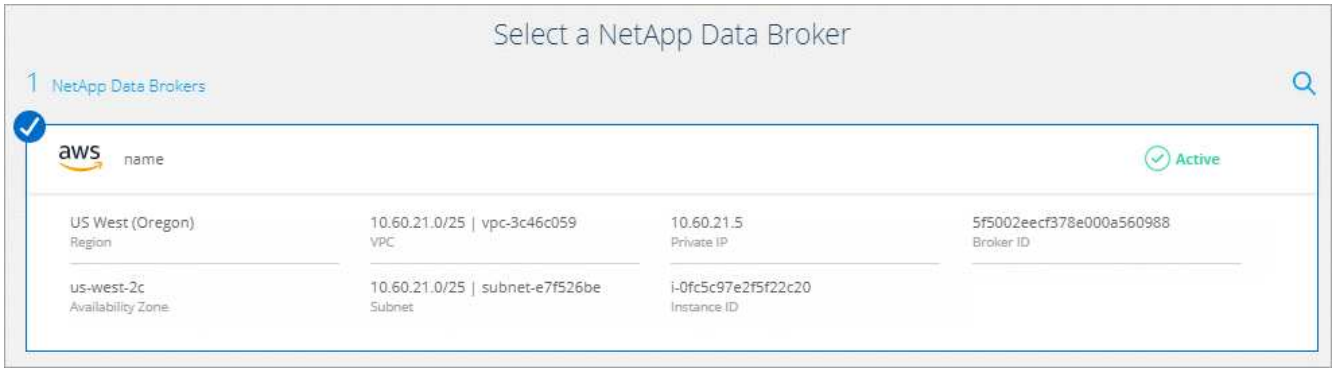
6. Si vous avez saisi une clé d'accès AWS, sélectionnez un emplacement pour l'instance, sélectionnez une paire de clés, choisissez d'activer ou non une adresse IP publique, puis sélectionnez un rôle IAM existant, ou laissez le champ vide afin que Cloud Sync crée le rôle pour vous.

   Si vous choisissez votre propre rôle IAM, vous devrez fournir les autorisations requises.



7. Une fois le courtier de données disponible, cliquez sur **Continuer** dans Cloud Sync.

L'image suivante montre une instance déployée avec succès dans AWS :



8. Complétez les pages de l'assistant pour créer la nouvelle relation de synchronisation.

Résultat

Vous avez déployé un courtier de données dans AWS et créé une nouvelle relation de synchronisation. Vous pouvez utiliser ce data broker avec des relations de synchronisation supplémentaires.

Installation du data broker dans Azure

Lorsque vous créez une relation de synchronisation, choisissez l'option Azure Data Broker pour déployer le logiciel Data Broker sur une nouvelle machine virtuelle dans un VNet. Cloud Sync vous guide tout au long du processus d'installation, mais les exigences et les étapes sont répétées sur cette page pour vous aider à vous préparer à l'installation.

Vous avez également la possibilité d'installer le courtier de données sur un hôte Linux existant dans le cloud ou sur votre site. "En savoir plus >>".

Régions Azure prises en charge

Toutes les régions sont prises en charge à l'exception des régions China, US Gov et US DoD.

Configuration réseau requise

- Le courtier de données a besoin d'une connexion Internet sortante pour pouvoir interroger le service Cloud Sync sur le port 443.

  Lorsque Cloud Sync déploie le courtier de données dans Azure, il crée un groupe de sécurité qui active la communication sortante requise.

  Si vous devez limiter la connectivité sortante, reportez-vous à la section "liste des noeuds finaux que le courtier de données contacte".

- NetApp recommande de configurer la source, la cible et le courtier de données pour qu'ils utilisent un service NTP (Network Time Protocol). La différence de temps entre les trois composants ne doit pas dépasser 5 minutes.

METHODE d'authentification

Lorsque vous déployez le courtier de données, vous devrez choisir une méthode d'authentification : un mot de passe ou une paire de clés publiques-privées SSH.

Pour obtenir de l'aide sur la création d'une paire de clés, reportez-vous à la section "Documentation Azure : créez et utilisez une paire de clés publiques-privées SSH pour les machines virtuelles Linux dans Azure".

Installation du data broker

Vous pouvez installer un courtier de données dans Azure lorsque vous créez une relation de synchronisation.

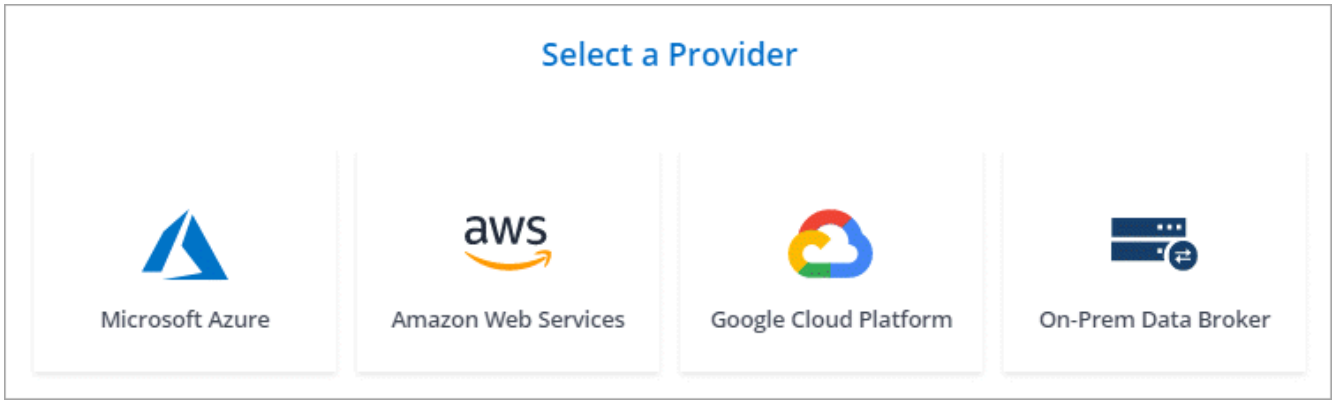
Étapes

1. Cliquez sur **Créer une nouvelle synchronisation**.
2. Sur la page **Define Sync Relationship**, choisissez une source et une cible et cliquez sur **Continuer**.

   Complétez les pages jusqu'à ce que vous atteiez la page **Data Broker**.

3. Sur la page **Data Broker**, cliquez sur **Create Data Broker**, puis sélectionnez **Microsoft Azure**.

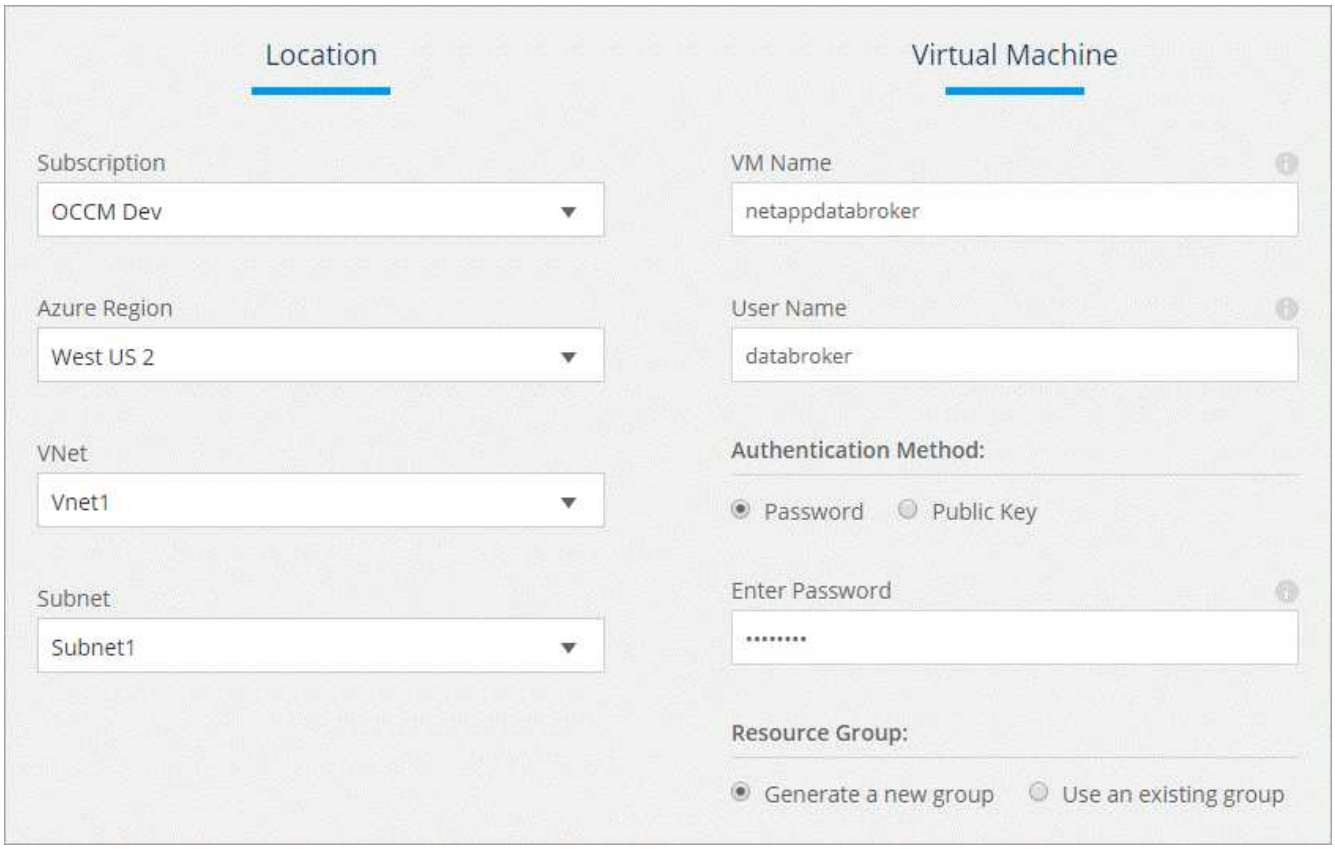
   Si vous avez déjà un courtier de données, vous devez cliquer sur le + icône en premier.



4. Entrez un nom pour le courtier de données et cliquez sur **Continuer**.
5. Si vous y êtes invité, connectez-vous à votre compte Microsoft. Si vous n'êtes pas invité, cliquez sur **connexion à Azure**.

   Ce formulaire est détenu et hébergé par Microsoft. Vos identifiants ne sont pas fournis à NetApp.

6. Choisissez un emplacement pour le courtier de données et entrez les informations de base sur la machine virtuelle.



7. Cliquez sur **Continuer** et maintenez la page ouverte jusqu'à ce que le déploiement soit terminé.

   Ce processus peut prendre jusqu'à 7 minutes.

8. Dans Cloud Sync, cliquez sur **Continuer** une fois le courtier de données disponible.
9. Complétez les pages de l'assistant pour créer la nouvelle relation de synchronisation.

Résultat

Vous avez déployé un courtier en données dans Azure et créé une nouvelle relation de synchronisation. Vous pouvez utiliser ce data broker avec des relations de synchronisation supplémentaires.

Vous obtenez un message sur le besoin d'un consentement de l'administrateur ?

Si Microsoft vous informe que l'administrateur doit être approuvé, car Cloud Sync doit disposer d'une autorisation d'accès aux ressources de votre entreprise pour votre compte, vous disposez de deux options :

1. Demandez à votre administrateur AD de vous fournir l'autorisation suivante :

   Dans Azure, accédez à **Admin Centers > Azure AD > utilisateurs et groupes > User Settings** et activez **les utilisateurs peuvent autoriser les applications à accéder aux données de l'entreprise en leur nom**.

2. Demandez à votre administrateur AD de consentir en votre nom à **CloudSync-AzureDataBrokerCreator** à l'aide de l'URL suivante (il s'agit du point de terminaison du consentement de l'administrateur) :

   https://login.microsoftonline.com/{FILL ICI VOTRE identifiant DE LOCATAIRE}/v2.0/adminConcey?client_ID=8ee4ca3a-bafa-4831-97cc-5a38923cab85&redirect_uri=https://cloudsync.netapp.com&scope=https://management.azure.com/user_impersonationhttps://graph.microsoft.com/User.Read

   Comme indiqué dans l'URL, notre URL d'application est https://cloudsync.netapp.com et l'ID client de l'application est 8ee4ca3a-bafa-4831-97cc-5a38923cab85.

Installation du courtier en données dans Google Cloud Platform

Lorsque vous créez une relation de synchronisation, choisissez l'option GCP Data Broker pour déployer le logiciel Data Broker sur une nouvelle instance de machine virtuelle dans un VPC. Cloud Sync vous guide tout au long du processus d'installation, mais les exigences et les étapes sont répétées sur cette page pour vous aider à vous préparer à l'installation.

Vous avez également la possibilité d'installer le courtier de données sur un hôte Linux existant dans le cloud ou sur votre site. "En savoir plus >>".

Régions GCP prises en charge

Toutes les régions sont prises en charge.

Configuration réseau requise

- Le courtier de données a besoin d'une connexion Internet sortante pour pouvoir interroger le service Cloud Sync sur le port 443.

  Lorsque Cloud Sync déploie le courtier de données dans GCP, il crée un groupe de sécurité qui active la communication sortante requise.

  Si vous devez limiter la connectivité sortante, reportez-vous à la section "liste des noeuds finaux que le courtier de données contacte".

- NetApp recommande de configurer la source, la cible et le courtier de données pour qu'ils utilisent un service NTP (Network Time Protocol). La différence de temps entre les trois composants ne doit pas dépasser 5 minutes.

Autorisations requises pour déployer le courtier de données dans GCP

Assurez-vous que l'utilisateur GCP qui déploie le courtier de données dispose des autorisations suivantes :

```
- compute.networks.list
- compute.regions.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.operations.get
- iam.serviceAccounts.list
```

Autorisations requises pour le compte de service

Lorsque vous déployez le courtier de données, vous devez sélectionner un compte de service disposant des autorisations suivantes :

```
- logging.logEntries.create
- resourcemanager.projects.get
- storage.buckets.get
- storage.buckets.list
- storage.objects.*
```

Installation du data broker

Vous pouvez installer un courtier de données dans GCP lorsque vous créez une relation de synchronisation.

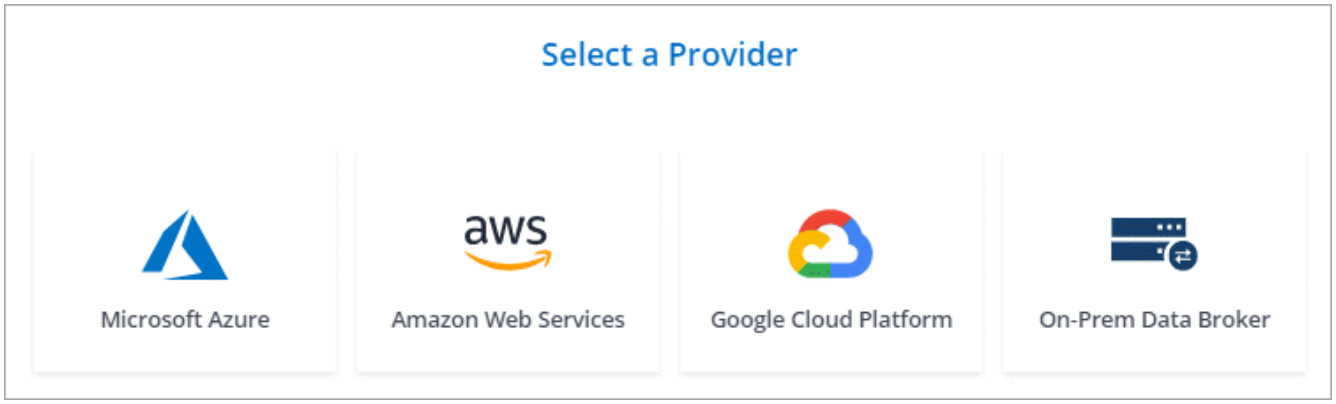
Étapes

1. Cliquez sur **Créer une nouvelle synchronisation**.
2. Sur la page **Define Sync Relationship**, choisissez une source et une cible et cliquez sur **Continuer**.

   Suivez les étapes jusqu'à ce que vous atteiez la page **Data Broker**.

3. Sur la page **Data Broker**, cliquez sur **Create Data Broker**, puis sélectionnez **Google Cloud Platform**.

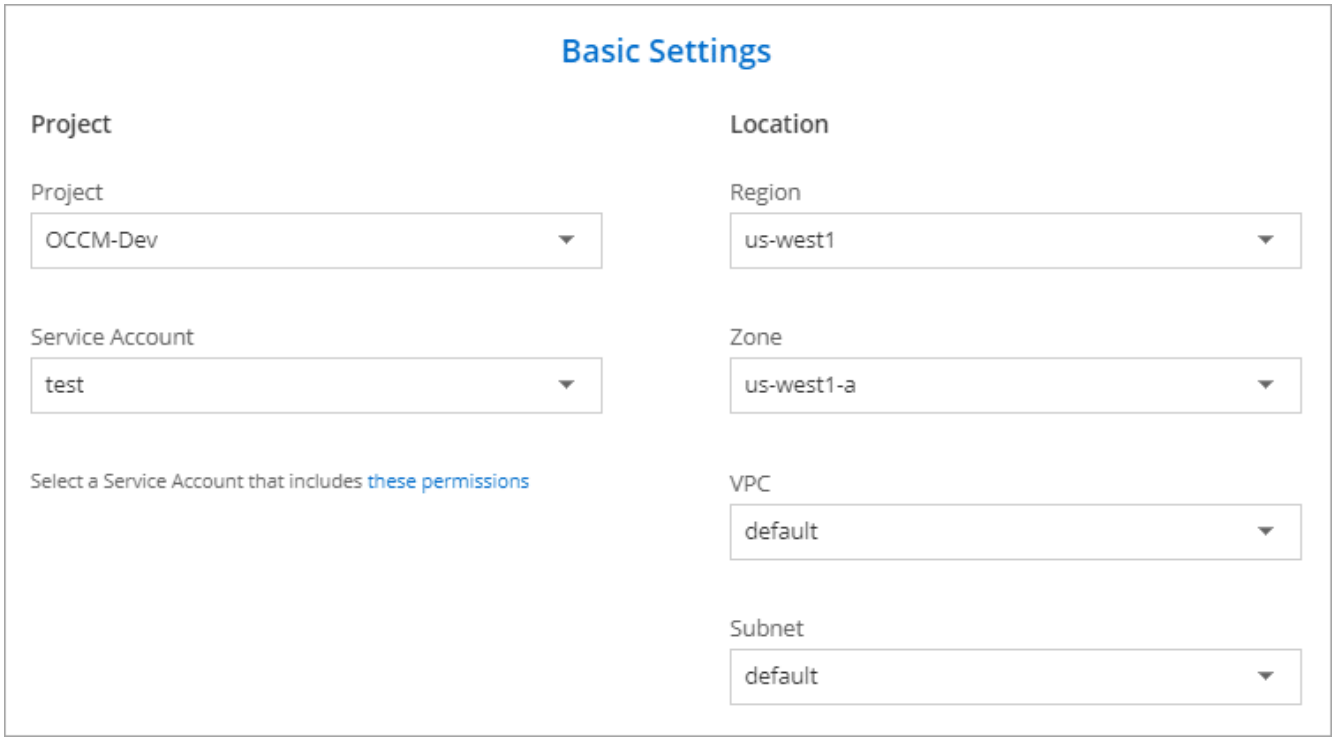
   Si vous avez déjà un courtier de données, vous devez cliquer sur le  icône en premier.



4. Entrez un nom pour le courtier de données et cliquez sur **Continuer**.
5. Si vous y êtes invité, connectez-vous à l'aide de votre compte Google.

   Le formulaire est détenu et hébergé par Google. Vos identifiants ne sont pas fournis à NetApp.

6. Sélectionnez un compte de projet et de service, puis choisissez un emplacement pour le courtier de données.



7. Une fois le courtier de données disponible, cliquez sur **Continuer** dans Cloud Sync.

   Le déploiement de l'instance dure environ 5 à 10 minutes. Vous pouvez contrôler la progression à partir du service Cloud Sync, qui est automatiquement actualisé lorsque l'instance est disponible.

8. Complétez les pages de l'assistant pour créer la nouvelle relation de synchronisation.

Résultat

Vous avez déployé un courtier en données dans GCP et avez créé une nouvelle relation de synchronisation. Vous pouvez utiliser ce data broker avec des relations de synchronisation supplémentaires.

Installation du data broker sur un hôte Linux

Lorsque vous créez une relation de synchronisation, choisissez l'option On-Pem Data Broker pour installer le logiciel de courtier de données sur un hôte Linux sur site ou sur un hôte Linux existant dans le cloud. Cloud Sync vous guide tout au long du processus d'installation, mais les exigences et les étapes sont répétées sur cette page pour vous aider à vous préparer à l'installation.

Configuration requise pour l'hôte Linux

- **Système d'exploitation** :
  - CentOS 7.0, 7.7 et 8.0
  - Red Hat Enterprise Linux 7.7 et 8.0
  - Ubuntu Server 18.04 LTS
  - SUSE Linux Enterprise Server 15 SP1

    La commande `yum update all` doit être exécuté sur l'hôte avant d'installer le courtier de données.

  Un système Red Hat Enterprise Linux doit être enregistré avec Red Hat Subscription Management. S'il n'est pas enregistré, le système ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis pendant l'installation.

- **RAM** : 16 GO
- **CPU** : 4 cœurs
- **Espace disque disponible**: 10 Go
- **SELinux**: Nous vous recommandons de désactiver "SELinux" sur l'hôte.

  SELinux applique une stratégie qui bloque les mises à jour logicielles des courtiers de données et peut empêcher le courtier de données de contacter les terminaux requis pour un fonctionnement normal.

- **OpenSSL** : OpenSSL doit être installé sur l'hôte Linux.

Configuration réseau requise

- L'hôte Linux doit être connecté à la source et à la cible.
- Le serveur de fichiers doit autoriser l'hôte Linux à accéder aux exportations.
- Le port 443 doit être ouvert sur l'hôte Linux pour le trafic sortant vers AWS (le courtier communique en permanence avec le service Amazon SQS).
- NetApp recommande de configurer la source, la cible et le courtier de données pour qu'ils utilisent un service NTP (Network Time Protocol). La différence de temps entre les trois composants ne doit pas dépasser 5 minutes.

Activation de l'accès à AWS

Si vous prévoyez d'utiliser le courtier de données avec une relation de synchronisation incluant un compartiment S3, préparez l'hôte Linux pour l'accès AWS. Lorsque vous installez le courtier en données, vous devrez fournir les clés AWS pour un utilisateur AWS qui dispose d'un accès aux programmes et d'autorisations spécifiques.

Étapes

1. Créer une règle IAM à l'aide de "Politique fournie par NetApp". "Consultez les instructions AWS".
2. Créez un utilisateur IAM disposant d'un accès programmatique. "Consultez les instructions AWS".

   Assurez-vous de copier les clés AWS car vous devez les spécifier lors de l'installation du logiciel Data Broker.

Activation de l'accès à Google Cloud

Si vous prévoyez d'utiliser le courtier de données avec une relation de synchronisation incluant un compartiment Google Cloud Storage, préparez l'hôte Linux pour l'accès GCP. Lorsque vous installez le courtier de données, vous devez fournir une clé pour un compte de service disposant d'autorisations spécifiques.

Étapes

1. Créez un compte de service GCP avec des autorisations d'administration du stockage, si vous n'en possédez pas déjà un.
2. Créez une clé de compte de service enregistrée au format JSON. "Affichez les instructions GCP".

   Le fichier doit contenir au moins les propriétés suivantes : "Project_ID", "Private_key" et "client_email"

   Lorsque vous créez une clé, le fichier est généré et téléchargé sur votre machine.

3. Enregistrez le fichier JSON sur l'hôte Linux.

Activation de l'accès à Microsoft Azure

L'accès à Azure est défini par relation en fournissant un compte de stockage et une chaîne de connexion dans l'assistant de synchronisation.

Installation du data broker

Vous pouvez installer un courtier de données sur un hôte Linux lorsque vous créez une relation de synchronisation.

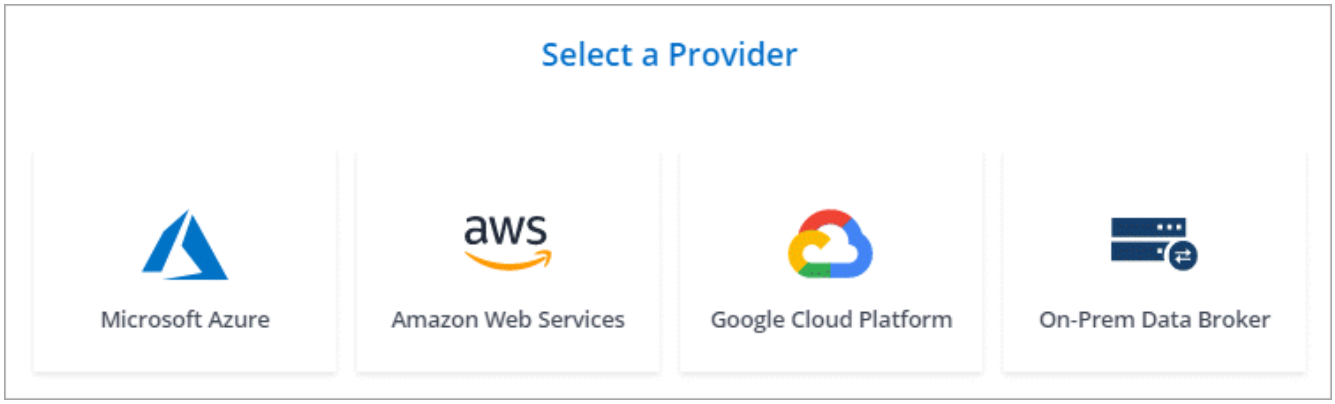
Étapes

1. Cliquez sur **Créer une nouvelle synchronisation**.
2. Sur la page **Define Sync Relationship**, choisissez une source et une cible et cliquez sur **Continuer**.

   Suivez les étapes jusqu'à ce que vous atteiez la page **Data Broker**.

3. Sur la page **Data Broker**, cliquez sur **Create Data Broker**, puis sélectionnez **On-site Data Broker**.

   Si vous avez déjà un courtier de données, vous devez cliquer sur le + icône en premier.



Bien que cette option soit ***sur site*** **Data Broker**, elle s'applique à un hôte Linux sur site ou dans le cloud.

4. Entrez un nom pour le courtier de données et cliquez sur **Continuer**.

   La page d'instructions se charge sous peu. Vous devez suivre ces instructions --elles comprennent un lien unique pour télécharger le programme d'installation.

5. Sur la page d'instructions :
   a. Indiquez si vous souhaitez activer l'accès à **AWS**, **Google Cloud** ou aux deux.
   b. Sélectionnez une option d'installation : **pas de proxy**, **utilisez le serveur proxy** ou **utilisez le serveur proxy avec authentification**.
   c. Utilisez les commandes pour télécharger et installer le courtier de données.

      Les étapes suivantes fournissent des détails sur chaque option d'installation possible. Suivez la page d'instructions pour obtenir la commande exacte en fonction de votre option d'installation.

   d. Téléchargez le programme d'installation :
      - Aucun proxy :

        ```
        curl <URI> -o data_broker_installer.sh
        ```

      - Utiliser le serveur proxy :

        ```
        curl <URI> -o data_broker_installer.sh -x <proxy_host>:<proxy_port>
        ```

      - Utilisez le serveur proxy avec l'authentification :

        ```
        curl <URI> -o data_broker_installer.sh -x
        <proxy_username>:<proxy_password>@<proxy_host>:<proxy_port>
        ```

        URI

        Cloud Sync affiche l'URI du fichier d'installation sur la page d'instructions, qui se charge lorsque vous suivez les invites de déploiement du courtier de données sur site. Cet URI ne se répète pas ici car le lien est généré de manière dynamique et ne peut être utilisé qu'une seule fois. Procédez comme suit pour obtenir l'URI de Cloud Sync.

   e. Passez en mode superutilisateur, rendez le programme d'installation exécutable et installez le logiciel :

Chaque commande indiquée ci-dessous inclut des paramètres d'accès AWS et d'accès GCP. Suivez la page d'instructions pour obtenir la commande exacte en fonction de votre option d'installation.

- Pas de configuration proxy :

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file>
```

- Configuration du proxy :

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port>
```

- Configuration proxy avec authentification :

```
sudo -s
chmod +x data_broker_installer.sh
./data_broker_installer.sh -a <aws_access_key> -s <aws_secret_key> -g
<absolute_path_to_the_json_file> -h <proxy_host> -p <proxy_port> -u
<proxy_username> -w <proxy_password>
```

Clés AWS

Il s'agit des clés que vous devriez avoir préparées pour l'utilisateur voici la procédure à suivre. Les clés AWS sont stockées sur le courtier en données, qui s'exécute sur votre réseau sur site ou dans le cloud. NetApp n'utilise pas les clés en dehors du courtier en données.

Fichier JSON

Il s'agit du fichier JSON qui contient une clé de compte de service que vous devez avoir préparée voici la procédure à suivre.

6. Une fois le courtier de données disponible, cliquez sur **Continuer** dans Cloud Sync.
7. Complétez les pages de l'assistant pour créer la nouvelle relation de synchronisation.

Création d'une relation de synchronisation

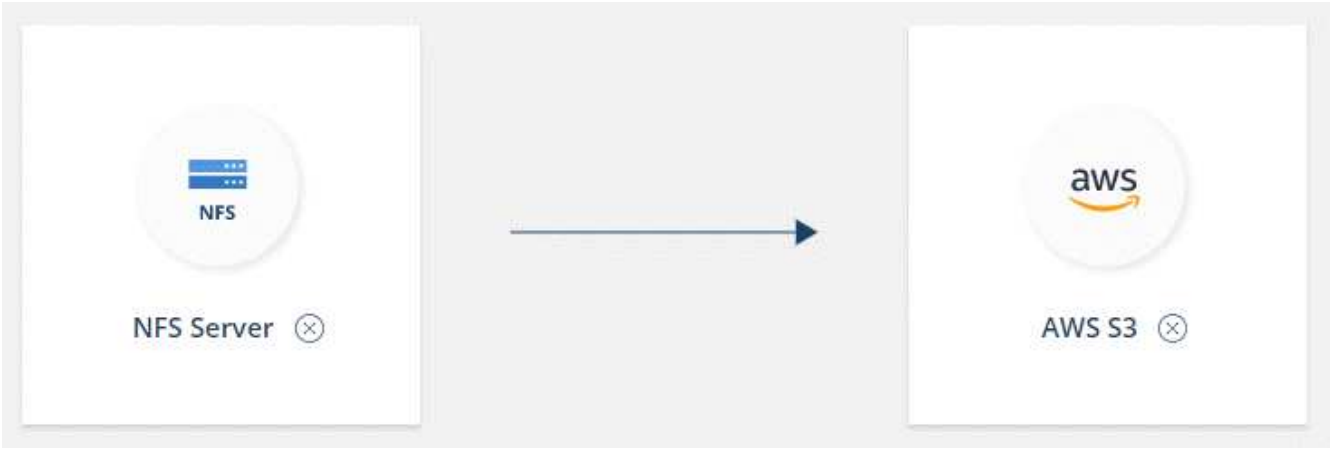
Lorsque vous créez une relation de synchronisation, le service Cloud Sync copie les fichiers de la source vers la cible. Après la copie initiale, le service synchronise les données modifiées toutes les 24 heures.

Les étapes ci-dessous fournissent un exemple de configuration d'une relation de synchronisation à partir d'un serveur NFS vers un compartiment S3.

Étapes

1. Dans Cloud Manager, cliquez sur **Sync**.
2. Sur la page **Define Sync Relationship**, choisissez une source et une cible.

Les étapes suivantes fournissent un exemple de création d'une relation de synchronisation entre un serveur NFS et un compartiment S3.

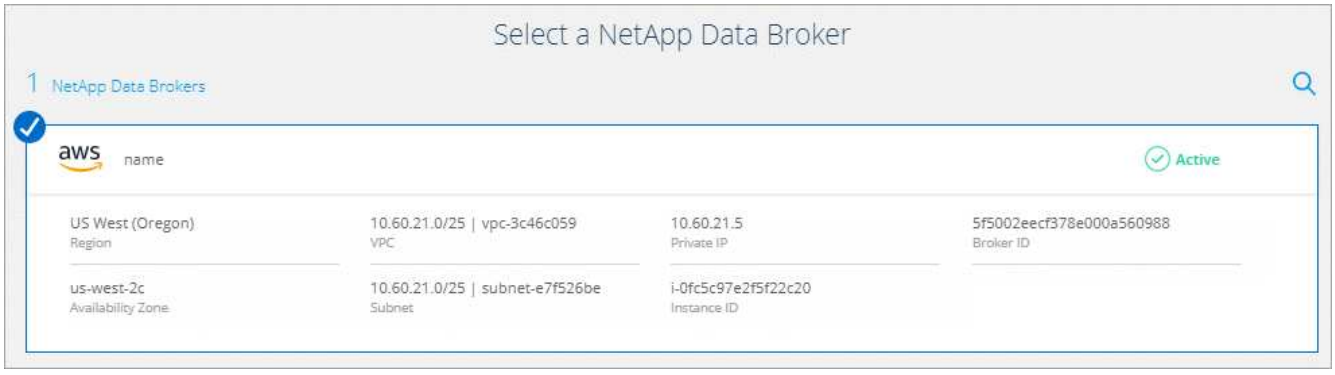


3. Sur la page **NFS Server**, entrez l'adresse IP ou le nom de domaine complet du serveur NFS que vous souhaitez synchroniser avec AWS.
4. Sur la page **Data Broker**, suivez les invites pour créer une machine virtuelle de courtier de données dans AWS, Azure ou Google Cloud Platform, ou pour installer le logiciel de courtier de données sur un hôte Linux existant.

   Pour plus de détails, reportez-vous aux pages suivantes :

   - "Installation du courtier de données dans AWS"
   - "Installation du data broker dans Azure"
   - "Installation du courtier de données dans GCP"
   - "Installation du data broker sur un hôte Linux"
5. Après avoir installé le courtier de données, cliquez sur **Continuer**.

   L'image suivante montre le déploiement réussi d'un courtier de données dans AWS :

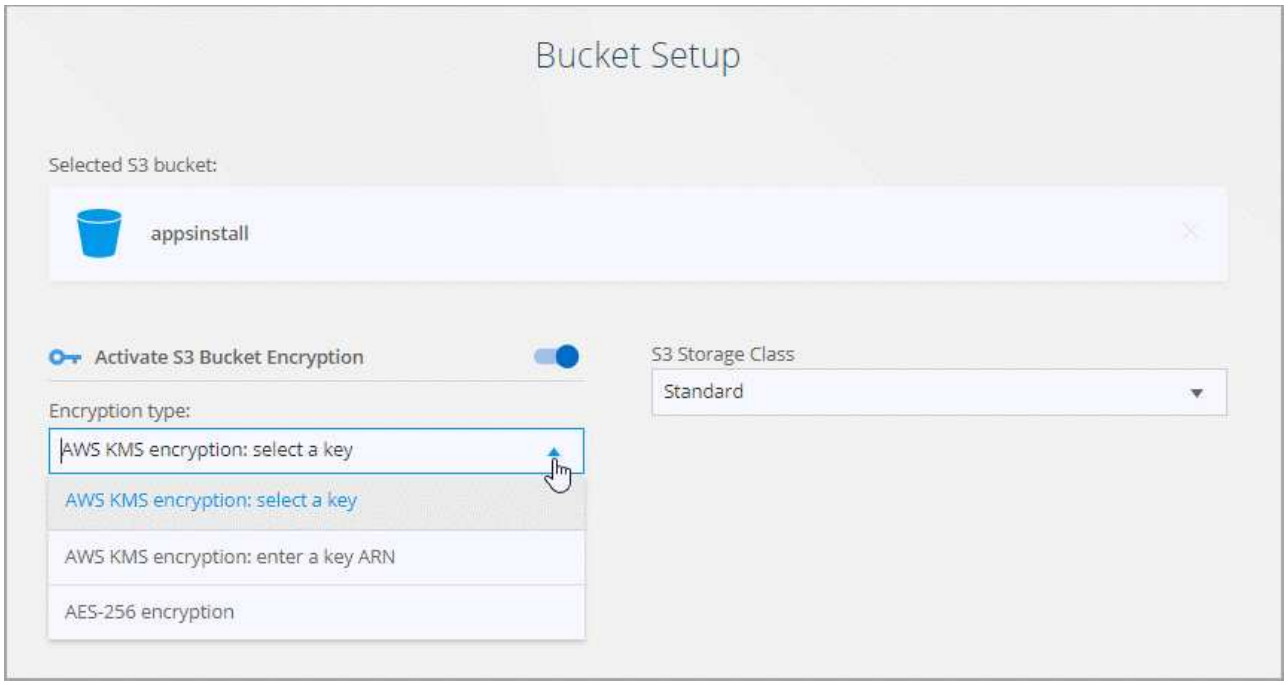


6. sur la page **répertoires**, sélectionnez un répertoire ou un sous-répertoire de niveau supérieur.

   Si Cloud Sync ne parvient pas à récupérer les exportations, cliquez sur **Ajouter une exportation manuelle** et entrez le nom d'une exportation NFS.

   Si vous souhaitez synchroniser plusieurs répertoires sur le serveur NFS, vous devez créer des relations de synchronisation supplémentaires après avoir terminé.

7. Sur la page **AWS S3 Bucket**, sélectionnez un compartiment :
   - Allez vers le bas pour sélectionner un dossier existant dans la rubrique ou pour sélectionner un nouveau dossier que vous créez dans la rubrique.
   - Cliquez sur **Ajouter à la liste** pour sélectionner un compartiment S3 qui n'est pas associé à votre compte AWS. "Des autorisations spécifiques doivent être appliquées au compartiment S3".
8. Sur la page **Configuration godet**, configurez le compartiment :
   - Optez pour l'activation du chiffrement des compartiments S3, puis sélectionnez une clé KMS AWS, saisissez l'ARN d'une clé KMS ou sélectionnez le chiffrement AES-256.
   - Sélectionnez une classe de stockage S3. "Afficher les classes de stockage prises en charge".



9. Sur la page **Paramètres**, définissez comment les fichiers et dossiers source sont synchronisés et gérés à l'emplacement cible :

Planification

Choisissez un programme récurrent pour les synchronisations ultérieures ou désactivez la planification de synchronisation. Vous pouvez planifier une relation pour synchroniser les données aussi souvent que toutes les 1 minute.

Tentatives

Définissez le nombre de tentatives de synchronisation d'un fichier par Cloud Sync avant de l'ignorer.

Fichiers récemment modifiés

Choisissez d'exclure les fichiers récemment modifiés avant la synchronisation planifiée.

Supprimer des fichiers sur la source

Choisissez de supprimer des fichiers de l'emplacement source une fois que Cloud Sync a copier les fichiers vers l'emplacement cible. Cette option inclut le risque de perte de données car les fichiers source sont supprimés après leur copie.

Si vous activez cette option, vous devez également modifier un paramètre dans le fichier local.json du courtier de données. Ouvrez le fichier et remplacez le paramètre nommé *workers.transferrer.delete-on-*

source par **true**.

Supprimer des fichiers sur la cible

Choisissez de supprimer des fichiers de l'emplacement cible, s'ils ont été supprimés de la source. La valeur par défaut est de ne jamais supprimer de fichiers de l'emplacement cible.

Balisage d'objets

Lorsque AWS S3 est la cible d'une relation de synchronisation, Cloud Sync balise les objets S3 avec des métadonnées pertinentes pour l'opération de synchronisation. Vous pouvez désactiver le balisage des objets S3 si ce n'est pas le cas dans votre environnement. Il n'y a aucun impact sur Cloud Sync si vous désactivez le balisage : Cloud Sync stocke simplement les métadonnées synchronisées d'une autre façon.

Types de fichiers

Définissez les types de fichiers à inclure dans chaque synchronisation : fichiers, répertoires et liens symboliques.

Exclure les extensions de fichier

Spécifiez les extensions de fichier à exclure de la synchronisation en tapant l'extension de fichier et en appuyant sur **entrée**. Par exemple, tapez *log* ou *.log* pour exclure les fichiers *.log. Un séparateur n'est pas nécessaire pour les extensions multiples. La vidéo suivante présente une courte démonstration :

► https://docs.netapp.com/fr-fr/occm38//media/video_file_extensions.mp4 *(video)*

Taille du fichier

Choisissez de synchroniser tous les fichiers, quelle que soit leur taille ou uniquement les fichiers qui se trouvent dans une plage de taille spécifique.

Date de modification

Choisissez tous les fichiers quelle que soit leur date de dernière modification, les fichiers modifiés après une date spécifique, avant une date spécifique ou entre une plage de temps.

10. Sur la page **Relationship Tags**, saisissez jusqu'à 9 balises de relation, puis cliquez sur **Continuer**.

    Le service Cloud Sync attribue les balises à chaque objet qu'il synchronise avec le compartiment S3.

11. Vérifiez les détails de la relation de synchronisation, puis cliquez sur **Créer une relation**.

Résultat

Cloud Sync démarre la synchronisation des données entre la source et la cible.

Payer pour la synchronisation après la fin de votre essai gratuit

Il existe deux façons de payer les relations de synchronisation après la fin de votre essai gratuit de 14 jours. La première option consiste à vous abonner à AWS ou Azure pour payer à votre gré ou à payer annuellement. La deuxième option consiste à acheter des licences directement auprès de NetApp.

Vous pouvez utiliser les licences de NetApp avec un abonnement AWS ou Azure. Par exemple, si vous disposez de 25 relations de synchronisation, vous pouvez payer les 20 premières relations de synchronisation à l'aide d'une licence, puis effectuer des opérations de paiement à la demande à partir d'AWS ou d'Azure avec les 5 autres relations de synchronisation.

"En savoir plus sur le fonctionnement des licences".

Que dois-je payer immédiatement après 8217 la fin de mon essai gratuit ?

Vous ne pourrez pas créer de relations supplémentaires. Les relations existantes ne sont pas supprimées, mais vous ne pouvez pas y apporter de modifications tant que vous n'êtes pas abonné ou que vous n'avez pas saisi de licence.

abonnement d'AWS

AWS vous permet de payer à votre gré ou de payer chaque année.

Les étapes à payer en tant que vous-même

1. Cliquez sur **Sync > licences**.
2. Sélectionnez **AWS**
3. Cliquez sur **s'abonner**, puis sur **Continuer**.
4. Abonnez-vous à AWS Marketplace, puis connectez-vous au service Cloud Sync pour terminer l'enregistrement.

   La vidéo suivante montre le processus :

   ► https://docs.netapp.com/fr-fr/occm38//media/video_cloud_sync_registering.mp4 *(video)*

Étapes à payer annuellement

1. "Accédez à la page AWS Marketplace".
2. Cliquez sur **Continuer pour s'inscrire**.
3. Sélectionnez vos options de contrat et cliquez sur **Créer contrat**.

abonnement d'Azure

Azure vous permet de payer à votre gré ou de payer chaque année.

Ce dont vous avez besoin

Un compte utilisateur Azure disposant des autorisations Contributeur ou Propriétaire dans l'abonnement correspondant.

Étapes

1. Cliquez sur **Sync > licences**.
2. Sélectionnez **Azure**.
3. Cliquez sur **s'abonner**, puis sur **Continuer**.
4. Dans le portail Azure, cliquez sur **Créer**, sélectionnez vos options et cliquez sur **s'abonner**.

   Sélectionnez **mensuel** pour payer par heure, ou **annuel** pour payer une année avant.

5. Une fois le déploiement terminé, cliquez sur le nom de la ressource SaaS dans le menu contextuel de notification.
6. Cliquez sur **configurer le compte** pour revenir à Cloud Sync.

   La vidéo suivante montre le processus :

► https://docs.netapp.com/fr-fr/occm38//media/video_cloud_sync_registering_azure.mp4 *(video)*

achat de licences de NetApp et leur ajout à Cloud Sync

Pour payer vos relations de synchronisation, vous devez acheter une ou plusieurs licences et les ajouter au service Cloud Sync.

Étapes

1. Achetez une licence par contacter NetApp.
2. Dans Cloud Manager, cliquez sur **Sync > licences**.
3. Cliquez sur **Ajouter une licence** et ajoutez la licence.

Tutoriels

Copie de listes de contrôle d'accès entre partages SMB

Cloud Sync peut copier les listes de contrôle d'accès (ACL) entre un partage SMB source et un partage SMB cible. Si nécessaire, vous pouvez conserver manuellement les listes de contrôle d'accès vous-même en utilisant robocopy.

Choix

- Configurez Cloud Sync pour copier automatiquement les ACL
- Copiez manuellement les ACL vous-même

Configuration de Cloud Sync pour copier les ACL entre les serveurs SMB

Copiez les ACL entre serveurs SMB en activant un paramètre lors de la création d'une relation ou après la création d'une relation.

Notez que cette fonction est disponible pour les nouvelles relations de synchronisation créées après la version du 23 février 2020. Si vous souhaitez utiliser cette fonction avec des relations existantes créées avant cette date, vous devrez recréer la relation.

Ce dont vous avez besoin

- Une nouvelle relation de synchronisation ou une relation de synchronisation existante créée après la version 23 février 2020.
- Tout type de courtier en données.

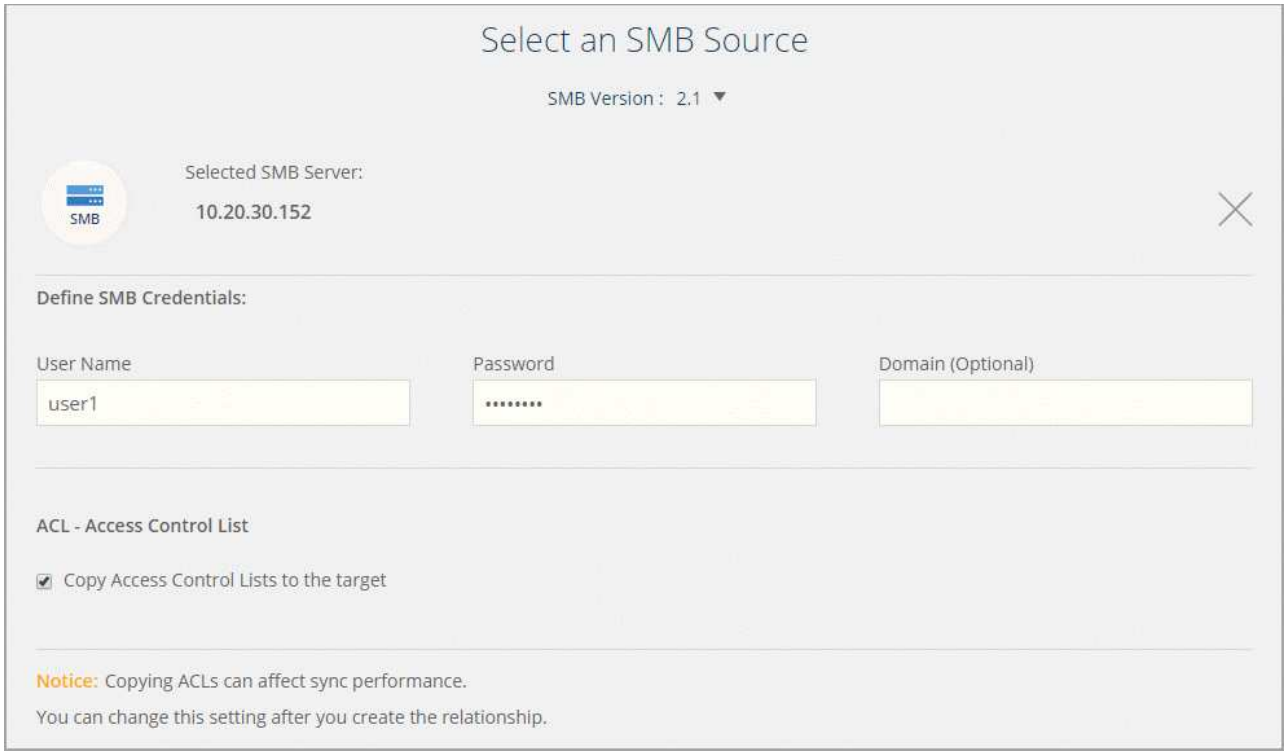
  Cette fonctionnalité fonctionne avec *tout* type de courtier en données : AWS, Azure, Google Cloud Platform ou comme courtier en données sur site. Le courtier en données sur site peut être exécuté "tout système d'exploitation pris en charge".

Étapes d'une nouvelle relation

1. Dans Cloud Sync, cliquez sur **Créer une nouvelle synchronisation**.
2. Faites glisser **SMB Server** vers la source et la cible et cliquez sur **Continuer**.
3. Sur la page **SMB Server** :
   a. Entrez un nouveau serveur SMB ou sélectionnez un serveur existant et cliquez sur **Continuer**.

b. Saisissez les informations d'identification du serveur SMB.

c. Sélectionnez **Copier les listes de contrôle d'accès vers la cible** et cliquez sur **Continuer**.



4. Suivez les autres invites pour créer la relation de synchronisation.

Étapes d'une relation existante

1. Survolez la relation de synchronisation et cliquez sur le menu d'action.
2. Cliquez sur **Paramètres**.
3. Sélectionnez **Copier les listes de contrôle d'accès vers la cible**.
4. Cliquez sur **Enregistrer les paramètres**.

Résultat

Lors de la synchronisation des données, Cloud Sync préserve les ACL entre les partages SMB source et cible.

Copie manuelle des ACL

Vous pouvez conserver manuellement les listes de contrôle d'accès entre les partages SMB à l'aide de la commande Windows robocopy.

Étapes

1. Identifiez un hôte Windows qui dispose d'un accès complet aux deux partages SMB.
2. Si l'un des noeuds finaux nécessite une authentification, utilisez la commande **net use** pour vous connecter aux noeuds finaux à partir de l'hôte Windows.

   Vous devez effectuer cette étape avant d'utiliser Robocopy.

3. Dans Cloud Sync, créez une nouvelle relation entre les partages SMB source et cible ou synchronisez une relation existante.

4. Une fois la synchronisation des données terminée, exécutez la commande suivante à partir de l'hôte Windows pour synchroniser les ACL et la propriété :

```
robocopy /E /COPY:SOU /secfix [source] [target] /w:0 /r:0 /XD ~snapshots
/UNILOG:"[logfilepath]
```

Source et *target* doivent être spécifiés à l'aide du format UNC. Par exemple : \\<serveur>\<partage>\<chemin>

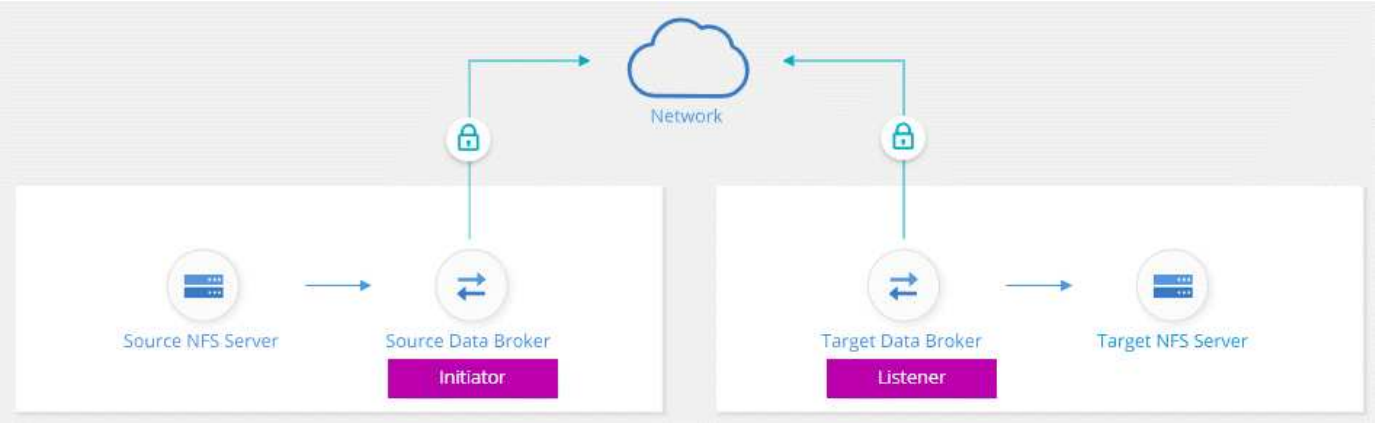
Synchronisation des données NFS à l'aide du chiffrement des données à la volée

Si votre entreprise dispose de règles de sécurité strictes, vous pouvez synchroniser les données NFS à l'aide du chiffrement des données à la volée. Cette fonctionnalité est prise en charge d'un serveur NFS vers un autre serveur NFS et de Azure NetApp Files vers Azure NetApp Files.

Par exemple, vous pouvez synchroniser des données entre deux serveurs NFS situés sur des réseaux différents. Ou bien vous devrez peut-être transférer des données sur Azure NetApp Files de manière sécurisée entre plusieurs sous-réseaux ou régions.

Fonctionnement du chiffrement des données en vol.

Le chiffrement des données à la volée crypte les données NFS lorsqu'elles sont transmises sur le réseau entre deux courtiers de données. L'image suivante montre une relation entre deux serveurs NFS et deux courtiers de données :



Un courtier de données fonctionne comme *initiator*. Lorsqu'il est temps de synchroniser des données, il envoie une demande de connexion à l'autre courtier de données, qui est le *listener*. Ce courtier de données écoute les demandes sur le port 443. Vous pouvez utiliser un autre port, si nécessaire, mais assurez-vous que le port n'est pas utilisé par un autre service.

Par exemple, si vous synchronisez des données d'un serveur NFS sur site vers un serveur NFS basé sur le cloud, vous pouvez choisir le courtier de données qui écoute les demandes de connexion et qui les envoie.

Voici le fonctionnement du chiffrement à la volée :

1. Après avoir créé la relation de synchronisation, l'initiateur démarre une connexion chiffrée avec l'autre courtier de données.
2. Le courtier de données source crypte les données à partir de la source à l'aide de TLS 1.3.

3. Il envoie ensuite les données via le réseau au data broker cible.
4. Le courtier de données cible décrypte les données avant de les envoyer à la cible.
5. Après la copie initiale, le service synchronise les données modifiées toutes les 24 heures. S'il y a des données à synchroniser, le processus commence par l'initiateur qui ouvre une connexion chiffrée avec l'autre courtier de données.

   Si vous préférez synchroniser les données plus fréquemment, "vous pouvez modifier le planning après avoir créé la relation".

Versions NFS prises en charge

- Pour les serveurs NFS, le chiffrement des données à la volée est pris en charge avec les versions 3, 4.0, 4.1 et 4.2 de NFS.
- Pour Azure NetApp Files, le chiffrement des données à la volée est pris en charge avec les versions 3 et 4.1 de NFS.

Ce dont vous avez besoin pour commencer

Assurez-vous d'avoir les éléments suivants :

- Deux serveurs NFS qui sont équipés "exigences source et cible" Ou Azure NetApp Files dans deux sous-réseaux ou régions.
- Les adresses IP ou noms de domaine complets des serveurs.
- Emplacements réseau pour deux courtiers de données.

  Vous pouvez sélectionner un courtier de données existant, mais il doit fonctionner comme initiateur. Le courtier de données de l'écouteur doit être un courtier de données *New*.

  Si vous n'avez pas encore déployé de courtier de données, consultez les exigences du courtier de données. Comme vous disposez de règles de sécurité strictes, passez en revue les exigences de mise en réseau, notamment le trafic sortant à partir du port 443 et du "terminaux internet" que le courtier de données contacte.

  - "Consultez l'installation d'AWS"
  - "Vérifiez l'installation d'Azure"
  - "Vérifiez l'installation de GCP"
  - "Vérifiez l'installation de l'hôte Linux"

Synchronisation des données NFS à l'aide du chiffrement des données à la volée

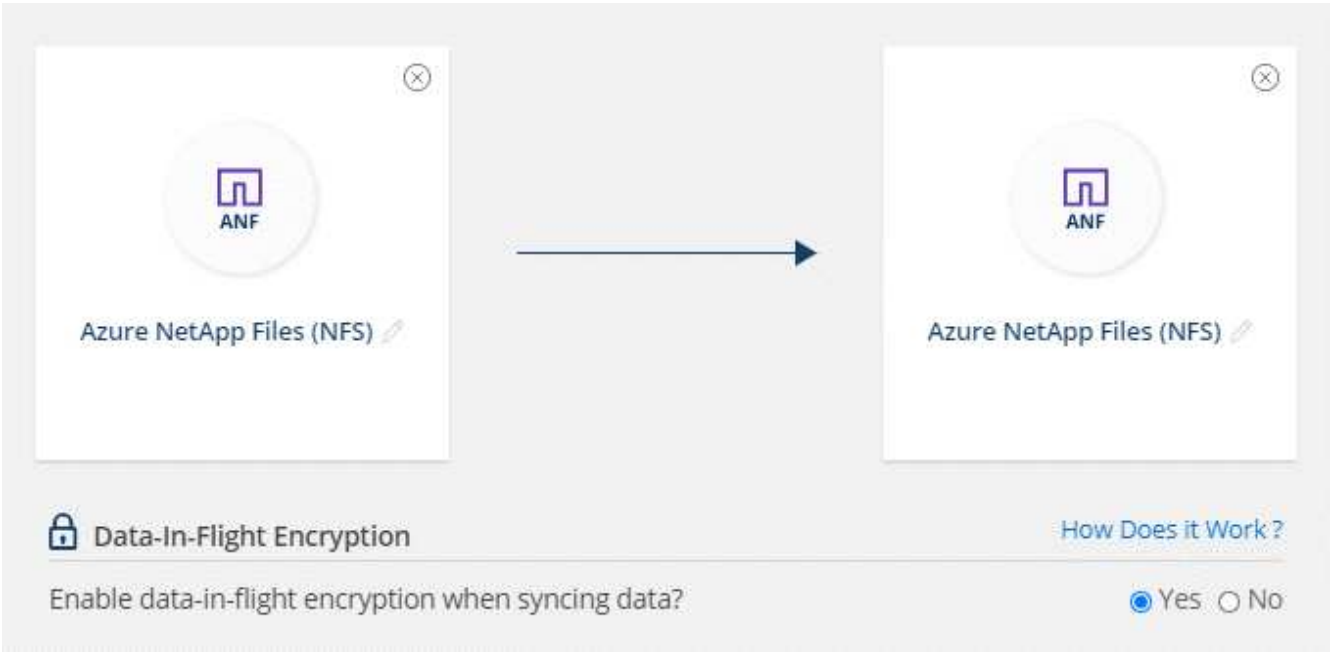
Créez une nouvelle relation de synchronisation entre deux serveurs NFS ou entre Azure NetApp Files, activez l'option de chiffrement à la volée et suivez les invites.

Étapes

1. Cliquez sur **Créer une nouvelle synchronisation**.
2. Faites glisser **serveur NFS** vers les emplacements source et cible ou **Azure NetApp Files** vers les emplacements source et cible et sélectionnez **Oui** pour activer le cryptage des données en transit.

   L'image suivante montre ce que vous sélectionnez pour synchroniser des données entre deux serveurs NFS :

L'image suivante montre ce que vous choisissez de synchroniser des données entre Azure NetApp Files :



3. Suivez les invites pour créer la relation :

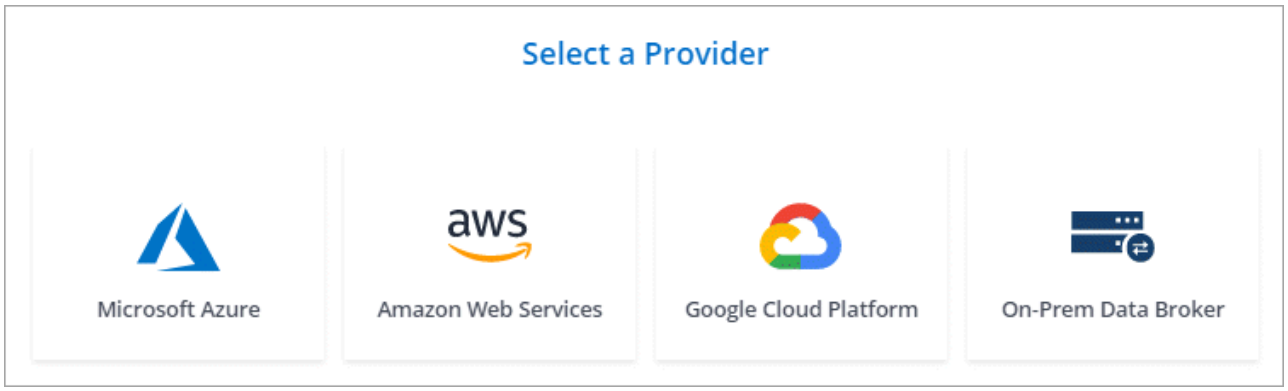
   a. **NFS Server/Azure NetApp Files** : Choisissez la version NFS, puis spécifiez une nouvelle source NFS ou sélectionnez un serveur existant.

   b. **Définir la fonctionnalité de Data Broker** : définissez le courtier de données *écoute* pour les demandes de connexion sur un port et lequel *lance* la connexion. Faites votre choix en fonction de vos besoins en matière de mise en réseau.

   c. **Data Broker** : suivez les invites pour ajouter un nouveau courtier de données source ou sélectionner un courtier de données existant.

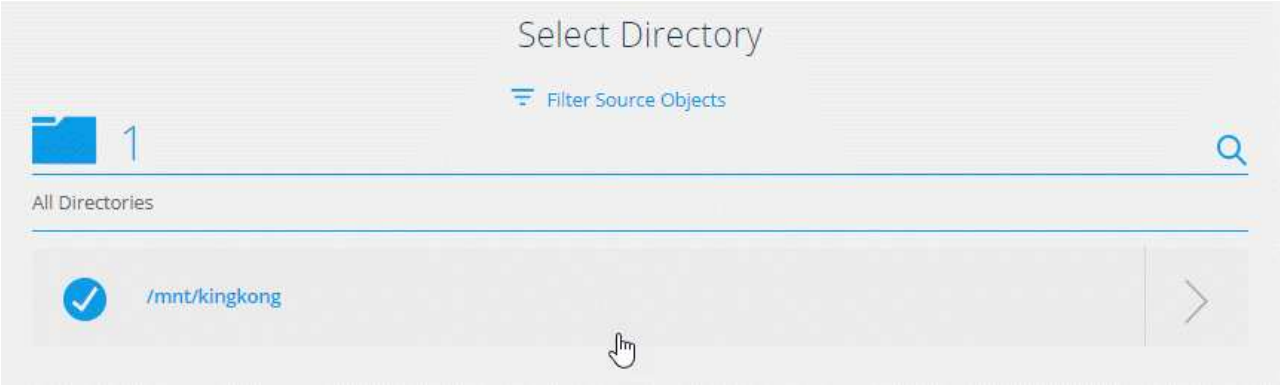
      Si le courtier de données source agit en tant qu'auditeur, il doit alors être un nouveau courtier de données.

Si vous avez besoin d'un nouveau courtier de données, Cloud Sync vous invite à suivre les instructions d'installation. Vous pouvez déployer le data broker dans le cloud ou télécharger un script d'installation pour votre propre hôte Linux.



d. **Répertoires** : Choisissez les répertoires que vous souhaitez synchroniser en sélectionnant tous les répertoires ou en descendant et en sélectionnant un sous-répertoire.

   Cliquez sur **Filtrer les objets source** pour modifier les paramètres qui définissent la synchronisation et la gestion des fichiers et dossiers source à l'emplacement cible.

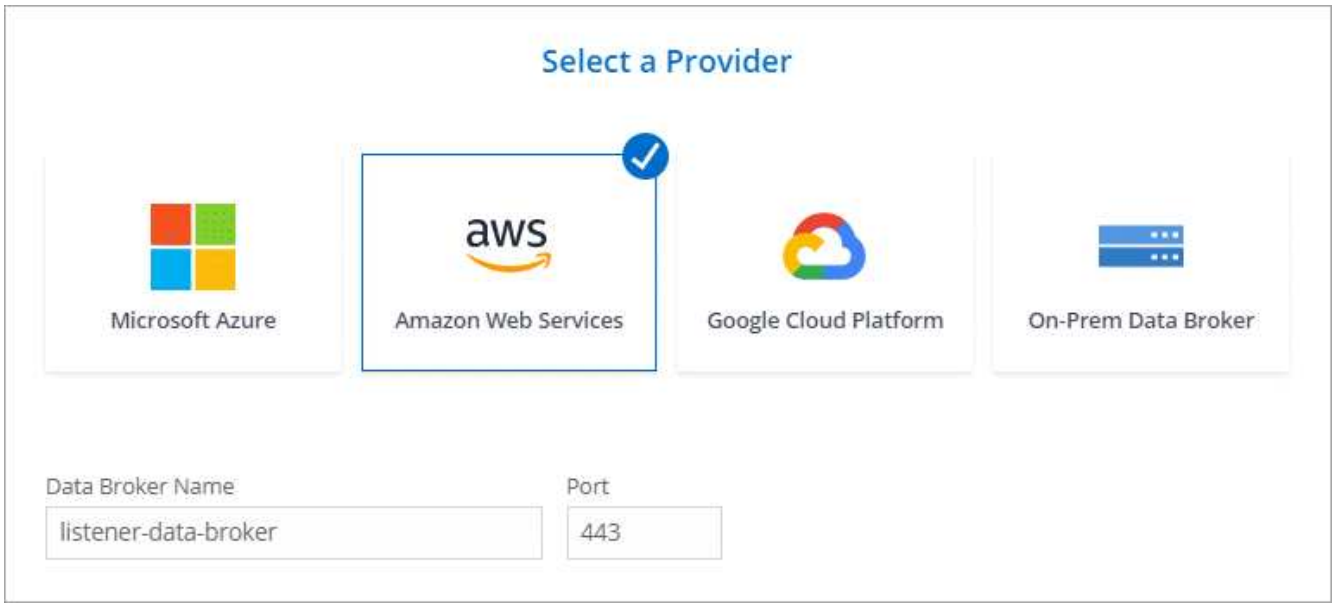


e. **Serveur NFS cible/Azure NetApp Files cible** : Choisissez la version NFS, puis entrez une nouvelle cible NFS ou sélectionnez un serveur existant.

f. **Courtier de données cible** : suivez les invites pour ajouter un nouveau courtier de données source ou sélectionner un courtier de données existant.

   Si le courtier de données cible agit en tant qu'auditeur, il doit alors être un nouveau courtier de données.

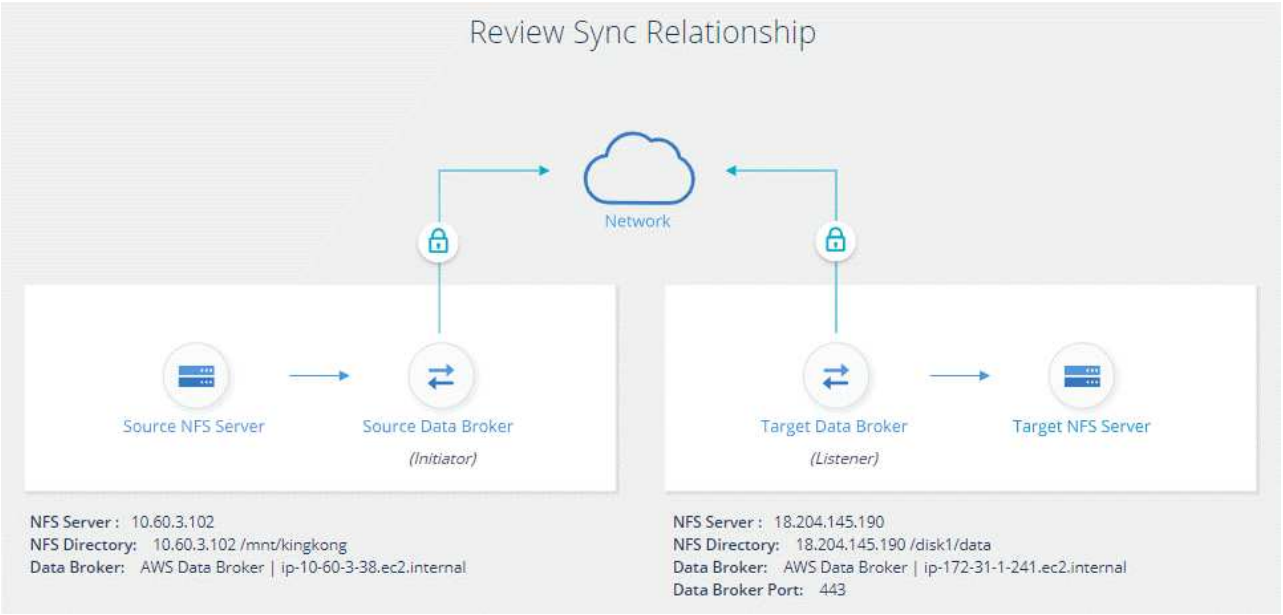
   Voici un exemple d'invite lorsque le courtier de données cible fonctionne comme écouteur. Notez l'option permettant de spécifier le port.



a. **Répertoires cibles** : sélectionnez un répertoire de niveau supérieur ou accédez à la recherche pour sélectionner un sous-répertoire existant ou créer un nouveau dossier à l'intérieur d'une exportation.

b. **Paramètres** : définissez comment les fichiers et dossiers source sont synchronisés et gérés à l'emplacement cible.

c. **Revue** : consultez les détails de la relation de synchronisation, puis cliquez sur **Créer une relation**.



Résultat

Cloud Sync commence à créer la nouvelle relation de synchronisation. Lorsque vous avez terminé, cliquez sur **Afficher dans le tableau de bord** pour afficher les détails de la nouvelle relation.

Gestion des relations de synchronisation

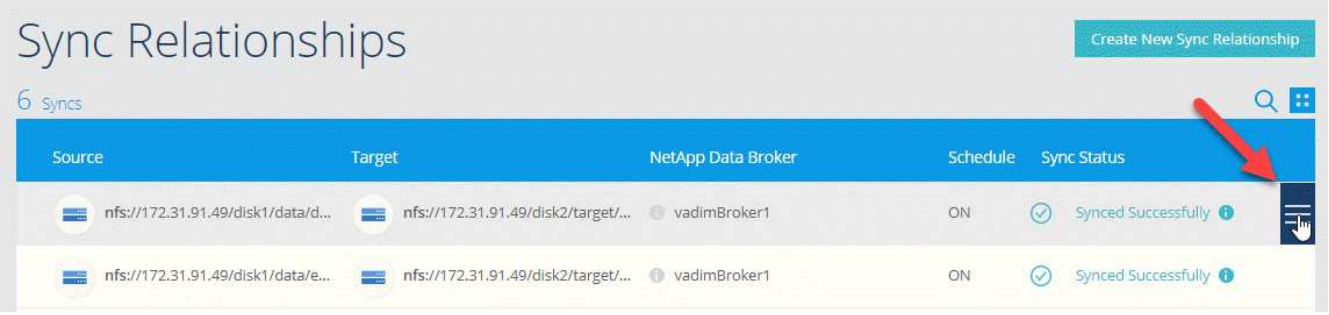
Vous pouvez gérer les relations de synchronisation à tout moment en synchronisant immédiatement les données, en modifiant les horaires, etc.

Effectuer une synchronisation immédiate des données

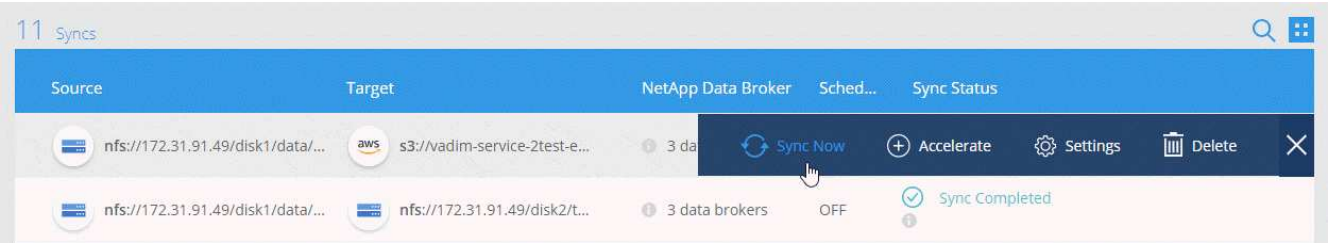
Au lieu d'attendre la synchronisation planifiée suivante, vous pouvez appuyer sur un bouton pour synchroniser immédiatement les données entre la source et la cible.

Étapes

1. Dans le tableau de bord **Sync**, survolez la relation de synchronisation et cliquez sur le menu d'action.



2. Cliquez sur **Synchroniser maintenant**, puis sur **Sync** pour confirmer.



Résultat

Cloud Sync démarre le processus de synchronisation des données pour la relation.

Accélération des performances de synchronisation

Accélérez les performances d'une relation de synchronisation en ajoutant un courtier de données supplémentaire à la relation. Le courtier de données supplémentaire doit être un *New* Data broker.

Comment cela fonctionne

Si les courtiers de données existants dans la relation sont utilisés dans d'autres relations de synchronisation, Cloud Sync ajoute automatiquement le nouveau courtier de données à ces relations.

Imaginons par exemple que vous ayez trois relations :

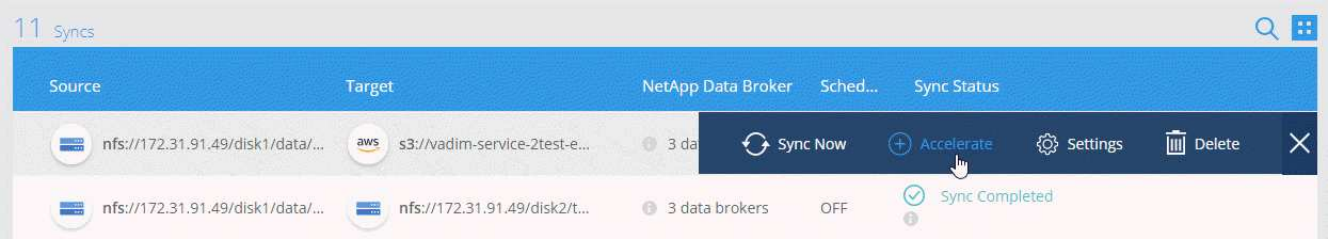
- La relation 1 utilise le courtier de données A
- La relation 2 utilise le courtier de données B
- La relation 3 utilise le courtier de données A

Vous souhaitez accélérer la performance de la relation 1 afin d'ajouter un nouveau courtier de données à cette relation (data broker C). Comme le courtier de données A est également utilisé dans la relation 3, le nouveau courtier de données est également automatiquement ajouté à la relation 3.

Étapes

1. Assurez-vous qu'au moins un des courtiers de données existants dans la relation est en ligne.

2. Survolez la relation de synchronisation et cliquez sur le menu d'action.
3. Cliquez sur **accélérer**.



4. Suivez les invites pour créer un nouveau courtier de données.

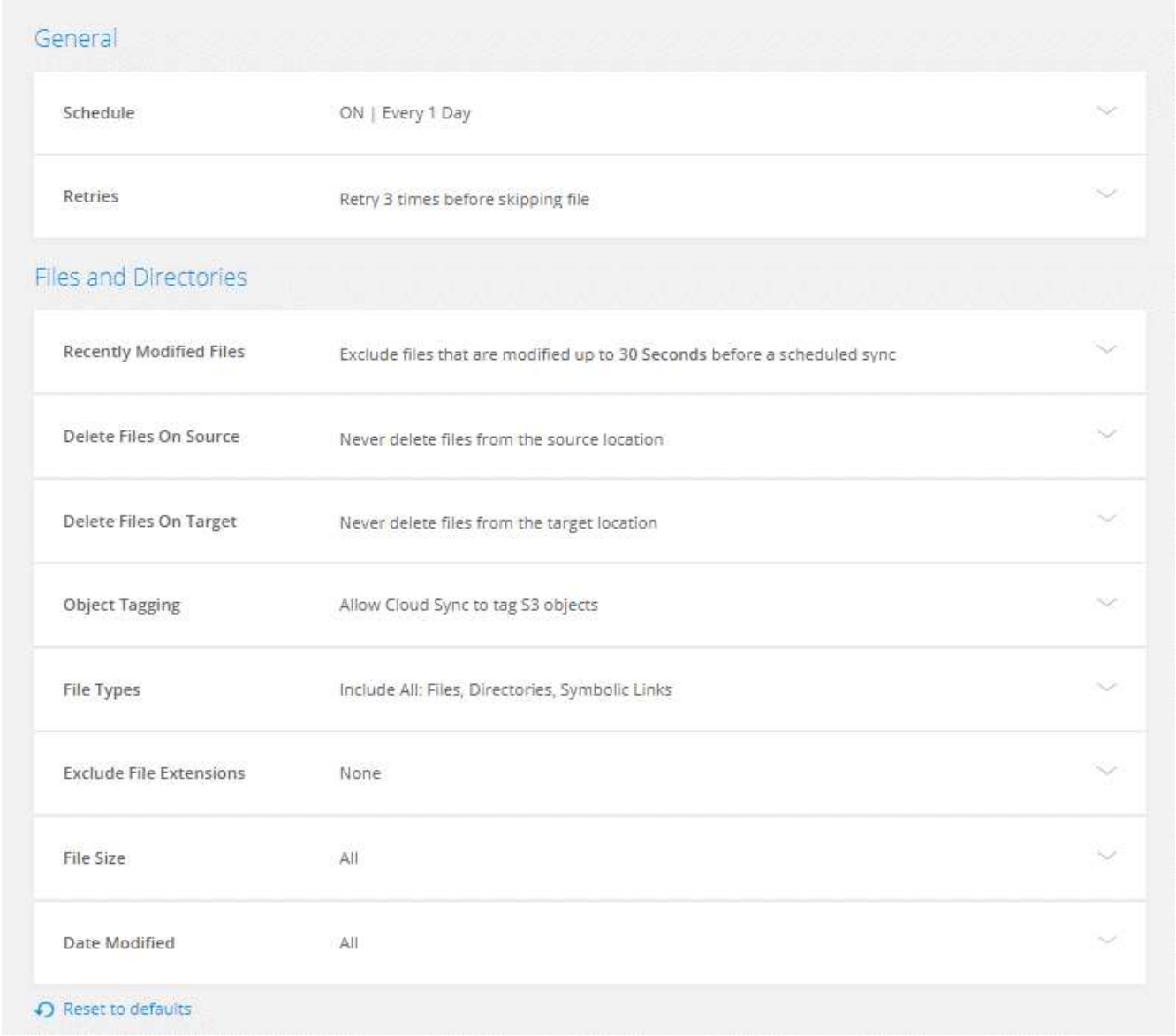
Résultat

Cloud Sync ajoute le nouveau courtier de données aux relations de synchronisation. Les performances de la prochaine synchronisation des données doivent être accélérées.

Modification des paramètres d'une relation de synchronisation

Modifiez les paramètres qui définissent la façon dont les fichiers et dossiers source sont synchronisés et gérés à l'emplacement cible.

1. Survolez la relation de synchronisation et cliquez sur le menu d'action.
2. Cliquez sur **Paramètres**.
3. Modifiez l'un des paramètres.



Voici une brève description de chaque paramètre :

Planification

Choisissez un programme récurrent pour les synchronisations ultérieures ou désactivez la planification de synchronisation. Vous pouvez planifier une relation pour synchroniser les données aussi souvent que toutes les 1 minute.

Tentatives

Définissez le nombre de tentatives de synchronisation d'un fichier par Cloud Sync avant de l'ignorer.

Fichiers récemment modifiés

Choisissez d'exclure les fichiers récemment modifiés avant la synchronisation planifiée.

Supprimer des fichiers sur la source

Choisissez de supprimer des fichiers de l'emplacement source une fois que Cloud Sync a copier les fichiers vers l'emplacement cible. Cette option inclut le risque de perte de données car les fichiers source sont supprimés après leur copie.

Si vous activez cette option, vous devez également modifier un paramètre dans le fichier local.json du

courtier de données. Ouvrez le fichier et remplacez le paramètre nommé *workers.transferrer.delete-on-source* par **true**.

Supprimer des fichiers sur la cible

Choisissez de supprimer des fichiers de l'emplacement cible, s'ils ont été supprimés de la source. La valeur par défaut est de ne jamais supprimer de fichiers de l'emplacement cible.

Balisage d'objets

Lorsque AWS S3 est la cible d'une relation de synchronisation, Cloud Sync balise les objets S3 avec des métadonnées pertinentes pour l'opération de synchronisation. Vous pouvez désactiver le balisage des objets S3 si ce n'est pas le cas dans votre environnement. Il n'y a aucun impact sur Cloud Sync si vous désactivez le balisage : Cloud Sync stocke simplement les métadonnées synchronisées d'une autre façon.

Types de fichiers

Définissez les types de fichiers à inclure dans chaque synchronisation : fichiers, répertoires et liens symboliques.

Exclure les extensions de fichier

Spécifiez les extensions de fichier à exclure de la synchronisation en tapant l'extension de fichier et en appuyant sur **entrée**. Par exemple, tapez *log* ou *.log* pour exclure les fichiers *.log. Un séparateur n'est pas nécessaire pour les extensions multiples. La vidéo suivante présente une courte démonstration :

► https://docs.netapp.com/fr-fr/occm38//media/video_file_extensions.mp4 *(video)*

Taille du fichier

Choisissez de synchroniser tous les fichiers, quelle que soit leur taille ou uniquement les fichiers qui se trouvent dans une plage de taille spécifique.

Date de modification

Choisissez tous les fichiers quelle que soit leur date de dernière modification, les fichiers modifiés après une date spécifique, avant une date spécifique ou entre une plage de temps.

Copier les listes de contrôle d'accès sur la cible

Choisir de copier les listes de contrôle d'accès (ACL) entre les partages SMB source et les partages SMB cibles. Notez que cette option n'est disponible que pour les relations de synchronisation créées après la version du 23 février 2020.

4. Cliquez sur **Enregistrer les paramètres**.

Résultat

Cloud Sync modifie la relation de synchronisation avec les nouveaux paramètres.

Suppression de relations

Vous pouvez supprimer une relation de synchronisation si vous n'avez plus besoin de synchroniser les données entre la source et la cible. Cette action ne supprime pas l'instance du courtier de données et ne supprime pas les données de la cible.

Étapes

1. Survolez la relation de synchronisation et cliquez sur le menu d'action.
2. Cliquez sur **Supprimer**, puis cliquez à nouveau sur **Supprimer** pour confirmer.

Résultat

Cloud Sync supprime la relation de synchronisation.

API Cloud Sync

Les fonctionnalités Cloud Sync disponibles via l'interface utilisateur Web sont également disponibles via les API RESTful.

Pour commencer

Pour commencer à utiliser les API Cloud Sync, vous devez obtenir un jeton d'utilisateur et votre identifiant de compte Cloud Central. Vous devrez ajouter le jeton et l'ID de compte à l'en-tête autorisation lorsque vous passez des appels API.

Étapes

1. Obtenez un jeton utilisateur auprès de NetApp Cloud Central.

```
POST https://netapp-cloud-account.auth0.com/oauth/token
Header: Content-Type: application/json
Body:
{
                "username": "<user_email>",
                "scope": "profile",
                "audience": "https://api.cloud.netapp.com",
                "client_id": "UaVhOIXMWQs5i1WdDxauXe5Mqkb34NJQ",
                "grant_type": "password",
                "password": "<user_password>"
}
```

2. Obtenez votre ID de compte Cloud Central.

```
GET https://cloudsync.netapp.com/api/accounts
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
```

Cette API renvoie une réponse comme suit :

```
[
  {
    "accountId": "account-JeL97Ry3",
    "name": "Test"
  }
]
```

3. Ajoutez le jeton utilisateur et l'ID de compte dans l'en-tête autorisation de chaque appel d'API.

   Exemple

   L'exemple suivant montre un appel API pour créer un courtier de données dans Microsoft Azure. Il vous suffit de remplacer <user_token> et <AccountID> par le jeton et l'ID obtenus lors des étapes précédentes.

```
POST https://cloudsync.netapp.com/api/data-brokers
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
Body: { "name": "databroker1", "type": "AZURE" }
```

Que dois-je faire lorsque le jeton expire ?

Le jeton utilisateur de NetApp Cloud Central a une date d'expiration. Pour actualiser le jeton, vous devez à nouveau appeler l'API à partir de l'étape 1.

La réponse de l'API inclut un champ " expire_in " qui indique la date d'expiration du jeton.

Référence API

La documentation de chaque API Cloud Sync est disponible à partir de "NetApp Cloud Central".

Utilisation d'API de liste

Les API de liste sont des API asynchrones. Les résultats ne reviennent donc pas immédiatement (par exemple : `GET /data-brokers/{id}/list-nfs-export-folders` et `GET /data-brokers/{id}/list-s3-buckets`). La seule réponse du serveur est l'état HTTP 202. Pour obtenir le résultat réel, vous devez utiliser le `GET /messages/client` API.

Étapes

1. Appelez l'API de liste que vous souhaitez utiliser.
2. Utilisez le `GET /messages/client` API pour afficher le résultat de l'opération.
3. Utilisez la même API en l'ajoutant avec l'ID que vous venez de recevoir : `GET http://cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>`

   Notez que l'ID change chaque fois que vous appelez le `GET /messages/client` API.

Exemple

Lorsque vous appelez le `list-s3-buckets` API, le résultat n'est pas immédiatement renvoyé :

```
GET http://cloudsync.netapp.com/api/data-brokers/<data-broker-id>/list-s3-buckets
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

Le résultat est le code d'état HTTP 202, ce qui signifie que le message a été accepté, mais qu'il n'a pas encore été traité.

Pour obtenir le résultat de l'opération, vous devez utiliser l'API suivante :

```
GET http://cloudsync.netapp.com/api/messages/client
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

Le résultat est un tableau avec un objet qui inclut un champ ID. Le champ ID représente le dernier message envoyé par le serveur. Par exemple :

```
[
    {
        "header": {
            "requestId": "init",
            "clientId": "init",
            "agentId": "init"
        },
        "payload": {
            "init": {}
        },
        "id": "5801"
    }
]
```

Vous devez maintenant passer l'appel API suivant à l'aide de l'ID que vous venez de recevoir :

```
GET http://cloudsync.netapp.com/api/messages/client?last=<id_from_step_2>
Headers: Authorization: Bearer <user_token>
Content-Type: application/json
x-account-id: <accountId>
```

Le résultat est un tableau de messages. Dans chaque message se trouve un objet Payload, qui se compose du nom de l'opération (en tant que clé) et de son résultat (en valeur). Par exemple :

```
[
    {
        "payload": {
            "list-s3-buckets": [
                {
                    "tags": [
                        {
                            "Value": "100$",
                            "Key": "price"
                        }
                    ],
                    "region": {
                        "displayName": "US West (Oregon)",
                        "name": "us-west-2"
                    },
                    "name": "small"
                }
            ]
        },
        "header": {
            "requestId": "f687ac55-2f0c-40e3-9fa6-57fb8c4094a3",
            "clientId": "5beb032f548e6e35f4ed1ba9",
            "agentId": "5bed61f4489fb04e34a9aac6"
        },
        "id": "5802"
    }
]
```


FAQ technique sur Cloud Sync

Cette FAQ peut vous aider si vous cherchez simplement une réponse rapide à une question.

Pour commencer

Les questions suivantes concernent le démarrage avec Cloud Sync.

Comment fonctionne Cloud Sync ?

Cloud Sync, qui utilise le logiciel de courtier de données NetApp, synchronise les données d'une source vers une cible (appelée « relation synchrone »).

Le courtier de données contrôle les relations de synchronisation entre vos sources et vos cibles. Après avoir configuré une relation de synchronisation, Cloud Sync analyse votre système source et le décompose en plusieurs flux de réplication afin de les transmettre aux données cible sélectionnées.

Après la copie initiale, le service synchronise toutes les données modifiées en fonction de la planification que

vous avez définie.

Comment fonctionne l'essai gratuit de 14 jours ?

L'essai gratuit de 14 jours commence lorsque vous vous inscrivez au service Cloud Sync. Vous n'êtes pas sujet aux frais NetApp liés aux relations Cloud Sync que vous créez pendant 14 jours. Cependant, tous les frais de ressources pour tout courtier de données que vous déployez s'appliquent toujours.

Combien coûte Cloud Sync ?

Il existe deux types de coûts associés à l'utilisation de Cloud Sync : les frais de service et les frais de ressources.

Frais de service

Pour les tarifs à la demande, les frais de service Cloud Sync sont horaires, en fonction du nombre de relations de synchronisation que vous créez.

- "Consultez les tarifs à la carte dans AWS"
- "Voir les tarifs annuels dans AWS"
- "Voir les tarifs à Azure"

Les licences Cloud Sync sont également disponibles auprès de votre représentant NetApp. Chaque licence permet 20 relations de synchronisation pendant 12 mois.

"En savoir plus sur les licences".

Frais de ressources

Les frais de ressources sont liés aux coûts de calcul et de stockage pour l'exécution du courtier de données dans le cloud.

Comment le service Cloud Sync est-il facturé ?

Il existe deux façons de payer les relations de synchronisation après la fin de votre essai gratuit de 14 jours. La première option consiste à vous abonner à AWS ou Azure, ce qui vous permet de payer à votre gré ou de payer chaque année. La deuxième option consiste à acheter des licences directement auprès de NetApp.

Puis-je utiliser Cloud Sync en dehors du cloud ?

Oui, vous pouvez utiliser Cloud Sync dans une architecture non cloud. La source et la cible peuvent résider sur site et ainsi de suite, le courtier de données.

Notez les points clés suivants sur l'utilisation de Cloud Sync en dehors du cloud :

- Pour la synchronisation sur site, un compartiment privé Amazon S3 est disponible via NetApp StorageGRID.
- Le courtier de données a besoin d'une connexion Internet pour communiquer avec le service Cloud Sync.
- Si vous n'achetez pas de licence directement auprès de NetApp, vous devrez acquérir un compte AWS ou Azure pour la facturation du service PAYGO Cloud Sync.

Comment accéder à Cloud Sync ?

Cloud Sync est disponible depuis Cloud Manager dans l'onglet **Sync**.

Sources et cibles prises en charge

Les questions suivantes concernent la source et les cibles prises en charge dans une relation de synchronisation.

Quelles sources et cibles Cloud Sync prend-il en charge ?

Cloud Sync prend en charge de nombreux types de relations de synchronisation. "Afficher la liste complète".

Quelles sont les versions de NFS et SMB prises en charge par Cloud Sync ?

Cloud Sync prend en charge NFS version 3 et ultérieure et SMB version 1 et ultérieure.

"En savoir plus sur les exigences de synchronisation".

Quand Amazon S3 est la cible, les données peuvent-elles être hiérarchisées vers une classe de stockage S3 spécifique ?

Oui, vous pouvez choisir une classe de stockage S3 spécifique lorsque AWS S3 est la cible :

- Standard (il s'agit de la classe par défaut)
- Le Tiering intelligent
- Accès autonome et peu fréquent
- Un seul accès à Zone-Infrequent
- Glacier
- Archives profondes des Glaciers

Qu'en est-il des niveaux de stockage pour le stockage Azure Blob ?

Vous pouvez choisir un niveau de stockage spécifique à Azure Blob lorsqu'un conteneur Blob est la cible :

- Stockage à chaud
- Stockage cool

Mise en réseau

Les questions suivantes concernent les exigences de mise en réseau pour Cloud Sync.

Quelles sont les exigences de mise en réseau pour Cloud Sync ?

L'environnement Cloud Sync requiert que le courtier de données soit connecté à la source et à la cible via le protocole sélectionné (NFS, SMB, EFS) ou l'API de stockage objet (Amazon S3, Azure Blob, IBM Cloud Object Storage).

En outre, le courtier de données a besoin d'une connexion Internet sortante sur le port 443 pour pouvoir communiquer avec le service Cloud Sync et contacter quelques autres services et référentiels.

Pour en savoir plus, "examiner les besoins en matière de mise en réseau".

Y a-t-il des limites de mise en réseau liées à la connectivité des courtiers de données ?

Les courtiers de données ont besoin d'un accès Internet. Nous ne prenons pas en charge un serveur proxy lors du déploiement d'un courtier en données dans Azure ou dans Google Cloud Platform.

Synchronisation des données

Les questions suivantes concernent le fonctionnement de la synchronisation des données.

À quelle fréquence la synchronisation se produit-elle ?

Le planning par défaut est défini pour la synchronisation quotidienne. Après la synchronisation initiale, vous pouvez :

- Modifiez le programme de synchronisation en fonction du nombre de jours, d'heures ou de minutes souhaité
- Désactivez le programme de synchronisation
- Supprimer le programme de synchronisation (aucune donnée ne sera perdue ; seule la relation de synchronisation sera supprimée)

Quel est le programme de synchronisation minimal ?

Vous pouvez planifier une relation pour synchroniser les données aussi souvent que toutes les 1 minute.

Le courtier de données essaie-t-il lorsqu'un fichier ne parvient pas à se synchroniser ? Ou est-ce que ce délai ?

Le courtier de données n'expire pas lorsqu'un seul fichier ne parvient pas à être transféré. Au lieu de cela, le courtier de données essaie à nouveau 3 fois avant de sauter le fichier. La valeur de la nouvelle tentative est configurable dans les paramètres d'une relation de synchronisation.

"Découvrez comment modifier les paramètres d'une relation de synchronisation".

Que se passe-t-il si j'ai un très grand jeu de données ?

Si un seul répertoire contient 600,000 fichiers ou plus, contactez-nous afin que nous puissions vous aider à configurer le courtier de données pour gérer la charge utile. Il est possible que nous devions ajouter de la mémoire supplémentaire à la machine du courtier de données.

Sécurité

Les questions suivantes ont trait à la sécurité.

Cloud Sync est-il sécurisé ?

Oui. Toute la connectivité réseau des services Cloud Sync est utilisée "Service SQS (simple Queue) d'Amazon".

Toutes les communications entre le data broker et Amazon S3, Azure Blob, Google Cloud Storage et IBM Cloud Object Storage sont effectuées via le protocole HTTPS.

Si vous utilisez Cloud Sync avec des systèmes sur site (source ou destination), voici quelques options de connectivité recommandées :

- Une connexion AWS Direct Connect, Azure ExpressRoute ou Google Cloud Interconnect, qui n'est pas routée par Internet (et ne peut communiquer qu'avec les réseaux cloud que vous spécifiez)
- Une connexion VPN entre votre passerelle sur site et vos réseaux cloud
- Pour un transfert de données plus sécurisé avec des compartiments S3, le stockage Azure Blob ou Google Cloud Storage, un terminal Amazon Private S3, des terminaux de service Azure Virtual Network ou Private Google Access peuvent être établis.

L'une de ces méthodes établit une connexion sécurisée entre vos serveurs NAS sur site et un courtier de données Cloud Sync.

Les données sont-elles chiffrées par Cloud Sync ?

- Cloud Sync prend en charge le chiffrement des données en vol entre les serveurs NFS source et cible. "En savoir plus >>".
- Le chiffrement n'est pas pris en charge avec SMB.
- Lorsqu'un compartiment Amazon S3 est la cible d'une relation synchrone, vous pouvez choisir d'activer le chiffrement des données à l'aide du chiffrement AWS KMS ou AES-256.

Autorisations

Les questions suivantes concernent les autorisations de données.

Les autorisations de données SMB sont-elles synchronisées vers l'emplacement cible ?

Vous pouvez configurer Cloud Sync pour préserver les listes de contrôle d'accès (ACL) entre un partage SMB source et un partage SMB cible. Vous pouvez également copier manuellement les ACL vous-même. "Découvrez comment copier des listes de contrôle d'accès entre partages SMB".

Les autorisations de données NFS sont-elles synchronisées vers l'emplacement cible ?

Cloud Sync copie automatiquement les autorisations NFS entre les serveurs NFS comme suit :

- NFS version 3 : Cloud Sync copie les autorisations et le propriétaire du groupe d'utilisateurs.
- NFS version 4 : Cloud Sync copie les ACL.

Performance

Les questions suivantes concernent les performances de Cloud Sync.

Que représente l'indicateur de progression d'une relation de synchronisation ?

La relation de synchronisation indique le débit de l'adaptateur réseau du courtier de données. Si vous accélérez les performances de synchronisation en utilisant plusieurs courtiers de données, le débit est la somme de tout le trafic. Ce débit est actualisé toutes les 20 secondes.

J'ai des problèmes de performances. Pouvons-nous limiter le nombre de transferts simultanés ?

Le courtier de données peut synchroniser 4 fichiers à la fois. Si vous avez des fichiers de très grande taille (plusieurs To chacun), il peut prendre beaucoup de temps pour terminer le processus de transfert et les performances peuvent être affectées.

Limiter le nombre de transferts simultanés peut vous aider. Mailto:ng-cloudsync-

support@netapp.com[Contactez-nous pour obtenir de l'aide].

Pourquoi les performances avec Azure NetApp Files sont-elles faibles ?

Lorsque vous synchronisez les données depuis ou vers Azure NetApp Files, vous risquez de subir des défaillances et des problèmes de performances si le niveau de service des disques est Standard.

Définissez le niveau de service sur Premium ou Ultra pour améliorer les performances de synchronisation.

"En savoir plus sur le débit et les niveaux de service de Azure NetApp Files".

Pourquoi est-ce que j'ai de faibles performances avec Cloud Volumes Service pour AWS ?

Lorsque vous synchronisez des données vers ou à partir d'un volume cloud, vous risquez de rencontrer des problèmes de performances et de panne si le niveau de performance du volume cloud est Standard.

Définissez le niveau de service sur Premium ou Extreme pour améliorer les performances de synchronisation.

Combien de courtiers de données sont requis ?

Lorsque vous créez une nouvelle relation, vous commencez par un seul courtier de données (sauf si vous avez sélectionné un courtier de données existant qui appartient à une relation de synchronisation accélérée). Dans de nombreux cas, un seul courtier de données peut répondre aux exigences de performance d'une relation de synchronisation. Si ce n'est pas le cas, l'ajout de courtiers de données supplémentaires permet d'accélérer la synchronisation. Mais vous devez d'abord vérifier d'autres facteurs qui peuvent avoir un impact sur les performances de synchronisation.

Plusieurs facteurs peuvent avoir un impact sur les performances de transfert de données. Les performances globales de la synchronisation peuvent être affectées en raison de la bande passante du réseau, de la latence et de la topologie du réseau, ainsi que des spécifications des VM du courtier de données et des performances du système de stockage. Par exemple, un seul courtier de données dans une relation de synchronisation peut atteindre 100 Mo/s, tandis que le débit du disque sur la cible peut uniquement permettre 64 Mo/s. Par conséquent, le courtier en données essaie de copier les données, mais la cible ne peut pas répondre aux besoins de performances du courtier.

Assurez-vous donc de vérifier les performances de votre réseau et le débit du disque sur la cible.

Vous pouvez ensuite envisager d'accélérer les performances de synchronisation en ajoutant un courtier de données supplémentaire pour partager la charge de cette relation. "Découvrez comment accélérer les performances de synchronisation".

Suppression de choses

Les questions suivantes concernent la suppression des relations de synchronisation et des données des sources et des cibles.

Que se passe-t-il si je supprime ma relation Cloud Sync ?

La suppression d'une relation arrête toutes les synchronisations de données futures et met fin au paiement. Toutes les données synchronisées sur la cible restent en l'état.

Que se passe-t-il si je supprime quelque chose de mon serveur source ? Est-il également supprimé de la cible ?

Par défaut, si vous disposez d'une relation de synchronisation active, l'élément supprimé sur le serveur source n'est pas supprimé de la cible lors de la prochaine synchronisation. Il existe toutefois une option dans les paramètres de synchronisation pour chaque relation, dans laquelle vous pouvez définir que Cloud Sync supprimera les fichiers de l'emplacement cible s'ils ont été supprimés de la source.

"Découvrez comment modifier les paramètres d'une relation de synchronisation".

Que se passe-t-il si je supprime quelque chose de ma cible ? Est-il supprimé de ma source ?

Si un élément est supprimé de la cible, il ne sera pas supprimé de la source. La relation est unidirectionnelle, de la source à la cible. Au cours du cycle de synchronisation suivant, Cloud Sync compare la source à la cible, identifie que l'élément est manquant et Cloud Sync le copie à nouveau de la source à la cible.

Dépannage

"Base de connaissances NetApp : FAQ Cloud Sync : support et dépannage"

Data broker plongez en profondeur

La question suivante concerne le courtier de données.

Pouvez-vous expliquer l'architecture du data broker ?

Bien sûr. Voici les points les plus importants :

- Le courtier de données est une application node.js exécutée sur un hôte Linux.
- Cloud Sync déploie le courtier de données comme suit :
  - AWS : à partir d'un modèle AWS CloudFormation
  - Azure : d'Azure Resource Manager
  - Google : à partir de Google Cloud Deployment Manager
  - Si vous utilisez votre propre hôte Linux, vous devez installer manuellement le logiciel
- Le logiciel Data Broker se met automatiquement à niveau vers la dernière version.
- Le data broker utilise AWS SQS comme canal de communication fiable et sécurisé et pour le contrôle et la surveillance. Les LP fournissent également une couche de persistance.
- Vous pouvez ajouter des courtiers de données supplémentaires à une relation pour augmenter la vitesse de transfert et augmenter la haute disponibilité. La résilience des services est assurée en cas de défaillance d'un courtier de données.

Améliorez la confidentialité des données

Découvrez Cloud Compliance

Cloud Compliance est un service de confidentialité et de conformité des données conçu pour Cloud Manager qui analyse les volumes, les compartiments Amazon S3 et les bases de données afin d'identifier les données personnelles et sensibles qui résident dans ces fichiers. Avec la technologie d'intelligence artificielle (IA), Cloud Compliance aide les entreprises à comprendre le contexte des données et à identifier les données sensibles.

"Découvrez les utilisations de Cloud Compliance".

Caractéristiques

Cloud Compliance fournit plusieurs outils qui vous aideront dans vos efforts de conformité. Vous pouvez utiliser Cloud Compliance pour :

- Identifier les informations à caractère personnel
- Identifier une vaste gamme d'informations sensibles, conformément aux réglementations en matière de confidentialité RGPD, CCPA, PCI et HIPAA
- Répondre aux demandes d'accès aux données (DSAR, Data Subject Access Requests)

Environnements de travail et sources de données pris en charge

Cloud Compliance peut analyser les données à partir de plusieurs types de sources :

- Cloud Volumes ONTAP dans AWS
- Cloud Volumes ONTAP dans Azure
- Azure NetApp Files
- Amazon S3
- Bases de données résidant où que vous soyez (elles ne nécessitent pas que la base de données réside dans un environnement de travail)

Remarque : pour Azure NetApp Files, Cloud Compliance peut analyser tous les volumes se trouvant dans la même région que Cloud Manager.

Le coût

- Le coût d'utilisation de la conformité dans le cloud dépend de la quantité de données à analyser. Depuis le 7 octobre 2020, les 1 premiers To de données analysés par Cloud Compliance dans un espace de travail Cloud Manager sont gratuits. Cela inclut les données des volumes Cloud Volumes ONTAP, des volumes Azure NetApp Files, des compartiments Amazon S3 et des schémas de base de données. Un abonnement à AWS ou Azure Marketplace est nécessaire pour poursuivre l'analyse des données après ce point. Voir "tarifs" pour plus d'informations.

  "Découvrez comment vous inscrire".

- L'installation de Cloud Compliance nécessite le déploiement d'une instance cloud, ce qui entraîne des frais supplémentaires du fournisseur cloud sur lequel elle est déployée. Voir la type d'instance déployé pour chaque fournisseur cloud
- Cloud Compliance requiert que vous ayez déployé un connecteur. Dans la plupart des cas, vous disposez déjà d'un connecteur en raison des autres services et stockages que vous utilisez dans Cloud Manager. L'instance de connecteur entraîne des frais supplémentaires du fournisseur cloud sur lequel elle est déployée. Voir la "type d'instance déployé pour chaque fournisseur cloud".

Coûts de transfert de données

Les coûts de transfert de données dépendent de votre configuration. Si l'instance Cloud Compliance et la source de données se trouvent dans la même zone de disponibilité et la même région, aucun coût de transfert de données n'est observé. Mais si la source de données, telle qu'un cluster Cloud Volumes ONTAP ou un compartiment S3, se trouve dans une zone ou une région *différente* disponibilité, vous serez facturé par votre fournisseur cloud pour les coûts de transfert de données. Consultez ces liens pour en savoir plus :

- "AWS : tarification Amazon EC2"
- "Microsoft Azure : détails de la tarification de la bande passante"

Fonctionnement de Cloud Compliance

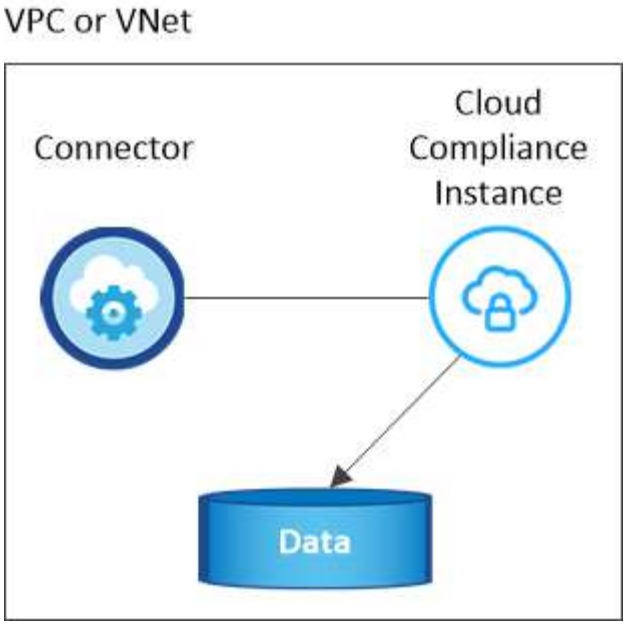
À un niveau élevé, Cloud Compliance fonctionne comme ceci :

1. Vous déployez une instance de Cloud Compliance dans Cloud Manager.
2. Vous l'activez sur un ou plusieurs environnements de travail, ou sur vos bases de données.
3. Cloud Compliance analyse les données à l'aide d'un processus de formation d'IA.
4. Dans Cloud Manager, vous cliquez sur **Compliance** et utilisez le tableau de bord et les outils de reporting fournis pour vous aider dans vos efforts de conformité.

Instance Cloud Compliance

Lorsque vous activez Cloud Compliance, Cloud Manager déploie une instance Cloud Compliance dans le même sous-réseau que le connecteur. "En savoir plus sur les connecteurs."

Si le connecteur est installé sur site, il déploie l'instance Cloud Compliance dans le même VPC ou vNet que le premier système Cloud Volumes ONTAP de la demande.



Notez les points suivants sur l'instance :

- Dans Azure, Cloud Compliance s'exécute sur une machine virtuelle standard_D16s_v3 avec un disque de 512 Go.
- Dans AWS, Cloud Compliance s'exécute sur une instance m5.4xlarge avec un disque GP2 de 500 Go.

  Dans les régions où m5.4xlarge n'est pas disponible, Cloud Compliance s'exécute sur une instance m4.4xlarge.

  La modification ou le redimensionnement du type d'instance/de VM n'est pas prise en charge. Vous devez utiliser la taille fournie.

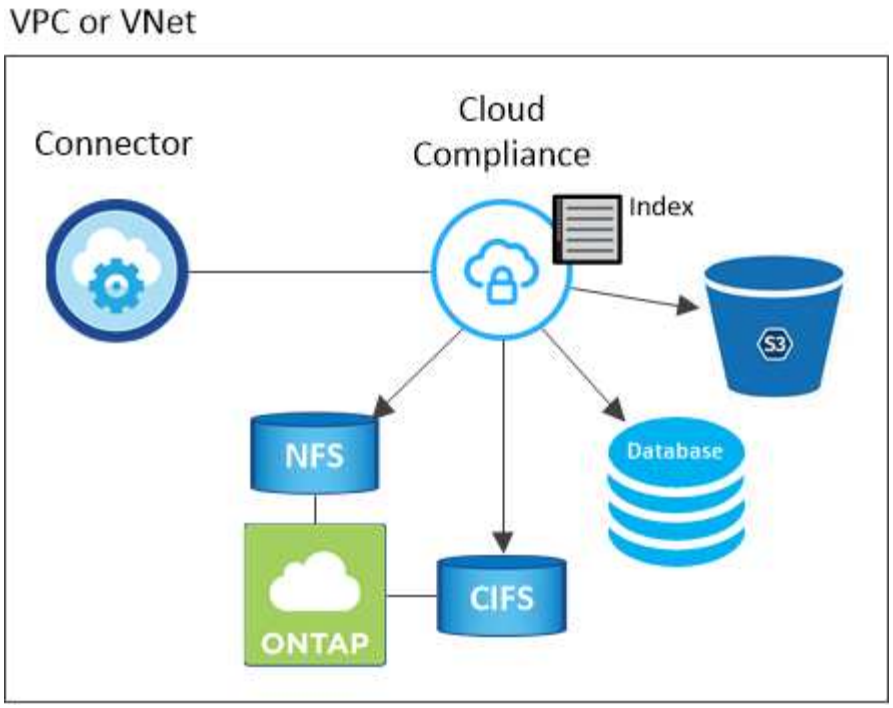
- L'instance s'appelle *CloudCompliance* avec un hachage (UUID) généré concaténé. Par exemple : *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*
- Une seule instance Cloud Compliance est déployée par connecteur.
- Les mises à niveau du logiciel Cloud Compliance sont automatisées ; vous n'avez plus à vous inquiéter.

L'instance doit rester en cours d'exécution en permanence car Cloud Compliance analyse les données en continu.

Fonctionnement des acquisitions

Une fois que vous avez activé Cloud Compliance et sélectionné les volumes, compartiments ou schémas de base de données que vous souhaitez numériser, il commence immédiatement à analyser les données pour identifier les données personnelles et sensibles. Il mappe les données de votre organisation, classe chaque fichier et identifie et extrait des entités et des modèles prédéfinis dans les données. Cette analyse permet d'obtenir un index des données personnelles, des données personnelles sensibles et des catégories de données.

Cloud Compliance se connecte aux données comme tout autre client en montant les volumes NFS et CIFS. Les volumes NFS sont automatiquement accessibles en lecture seule, tandis que vous devez fournir des identifiants Active Directory pour analyser les volumes CIFS.



Après l'analyse initiale, Cloud Compliance analyse en continu chaque volume pour détecter les modifications incrémentielles (c'est pourquoi il est important de maintenir l'exécution de l'instance).

Vous pouvez activer et désactiver les analyses au niveau du "niveau du volume", au "niveau du godet", et au "niveau du schéma de base de données".

Informations index par Cloud Compliance

Cloud Compliance collecte, index et attribue des catégories aux données non structurées (fichiers). Les données index Cloud Compliance incluent les éléments suivants :

Métadonnées standard

Cloud Compliance collecte des métadonnées standard sur les fichiers : le type de fichier, sa taille, ses dates de création et de modification, etc.

Données personnelles

Informations personnelles identifiables telles que les adresses électroniques, les numéros d'identification ou les numéros de carte de crédit. "En savoir plus sur les données personnelles".

Données personnelles sensibles

Des types spéciaux d'informations sensibles, comme les données de santé, l'origine ethnique ou les opinions politiques, tels que définis par le RGPD et d'autres réglementations sur la confidentialité. "En savoir plus sur les données personnelles sensibles".

Catégories

Cloud Compliance divise les données analysées et les divise en plusieurs types de catégories. Les catégories sont des rubriques basées sur l'analyse par IA du contenu et des métadonnées de chaque fichier. "En savoir plus sur les catégories".

Reconnaissance de l'entité de nom

Cloud Compliance utilise l'IA pour extraire les noms des personnes physiques des documents. "Découvrez comment répondre aux demandes d'accès aux données".

Présentation du réseau

Cloud Manager déploie l'instance Cloud Compliance avec un groupe de sécurité qui active les connexions HTTP entrantes à partir de l'instance de connecteur.

Lorsque vous utilisez Cloud Manager en mode SaaS, la connexion à Cloud Manager est assurée par HTTPS. Les données privées envoyées entre votre navigateur et l'instance Cloud Compliance sont sécurisées par un chiffrement de bout en bout, ce qui signifie que NetApp et des tiers ne peuvent pas les lire.

Si vous devez utiliser l'interface utilisateur locale plutôt que l'interface utilisateur SaaS pour quelque raison que ce soit, vous pouvez toujours "Accédez à l'interface utilisateur locale".

Les règles sortantes sont complètement ouvertes. Un accès Internet est nécessaire pour installer et mettre à niveau le logiciel Cloud Compliance et pour envoyer des metrics d'utilisation.

Si vous avez des exigences de mise en réseau strictes, "Découvrez les terminaux contacts par Cloud Compliance".

Accès des utilisateurs aux informations de conformité

Le rôle attribué à chaque utilisateur donne accès à différentes fonctionnalités dans Cloud Manager et dans Cloud Compliance :

- **Les administrateurs de compte** peuvent gérer les paramètres de conformité et afficher les informations de conformité pour tous les environnements de travail.
- **Les administrateurs d'espace de travail** peuvent gérer les paramètres de conformité et afficher les informations de conformité uniquement pour les systèmes auxquels ils ont des autorisations d'accès. Si un administrateur d'espace de travail ne parvient pas à accéder à un environnement de travail dans Cloud Manager, il ne peut pas voir les informations de conformité de l'environnement de travail dans l'onglet conformité.
- Les utilisateurs disposant du rôle **Cloud Compliance Viewer** peuvent uniquement afficher les informations de conformité et générer des rapports pour les systèmes auxquels ils sont autorisés à accéder. Ces utilisateurs ne peuvent pas activer/désactiver la lecture des volumes, compartiments ou schémas de base de données.

"En savoir plus sur les rôles de Cloud Manager" et comment "ajoutez des utilisateurs avec des rôles spécifiques".

Commencez

Déployez Cloud Compliance

Suivez quelques étapes pour déployer l'instance Cloud Compliance dans votre espace de travail Cloud Manager.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

Créer un connecteur

Si vous n'avez pas encore de connecteur, créez-en un dans Azure ou AWS. Voir "Création d'un connecteur dans AWS" ou "Création d'un connecteur dans Azure".

Passer en revue les prérequis

Assurez-vous que votre environnement cloud peut répondre aux conditions préalables, dont 16 vCPU pour l'instance Cloud Compliance, l'accès Internet sortant pour l'instance, la connectivité entre le connecteur et Cloud Compliance sur le port 80, etc. Voir la liste complète.

Déployez Cloud Compliance

Lancez l'assistant d'installation pour déployer l'instance Cloud Compliance dans Cloud Manager.

Abonnez-vous au service Cloud Compliance

Les 1 premiers To de données analysés par Cloud Compliance dans Cloud Manager sont gratuits. Un abonnement à AWS ou Azure Marketplace est nécessaire pour poursuivre l'analyse des données après ce point.

Création d'un connecteur

Si vous n'avez pas encore de connecteur, créez-en un dans Azure ou AWS. Voir "Création d'un connecteur dans AWS" ou "Création d'un connecteur dans Azure". Dans la plupart des cas, un connecteur sera probablement configuré avant d'essayer d'activer Cloud Compliance, car la plupart du temps "Les fonctionnalités de Cloud Manager nécessitent un connecteur", mais il y a des cas où vous devez en configurer un maintenant.

Il existe certains cas où vous devez utiliser un connecteur dans AWS ou Azure pour Cloud Compliance.

- Pour analyser les données dans Cloud Volumes ONTAP dans AWS ou dans des compartiments AWS S3, vous utilisez un connecteur dans AWS.
- Pour analyser les données dans Cloud Volumes ONTAP dans Azure ou dans Azure NetApp Files, vous utilisez un connecteur dans Azure.
- Les bases de données peuvent être scannées à l'aide d'un connecteur.

Comme vous pouvez le voir, il peut y avoir des situations où vous devez utiliser "Plusieurs connecteurs".

Si vous envisagez d'analyser Azure NetApp Files, vous devez vous assurer que vous déployez dans la même région que les volumes que vous souhaitez analyser.

Vérification des prérequis

Avant de déployer Cloud Compliance, consultez les conditions préalables suivantes pour vous assurer que la configuration est prise en charge.

Activer l'accès Internet sortant

Cloud Compliance requiert un accès Internet sortant. Si votre réseau virtuel utilise un serveur proxy pour l'accès Internet, assurez-vous que l'instance Cloud Compliance dispose d'un accès Internet sortant pour contacter les points de terminaison suivants. Notez que Cloud Manager déploie l'instance Cloud Compliance dans le même sous-réseau que le connecteur.

Terminaux	Objectif
https://cloudmanager.cloud.netapp.com	Communication avec le service Cloud Manager, notamment les comptes Cloud Central.
https://netapp-cloud-account.auth0.com https://auth0.com	Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs.
https://cloud-compliance-support-netapp.s3.us-west-2.amazonaws.com https://hub.docker.com https://auth.docker.io https://registry-1.docker.io https://index.docker.io/ https://dseasb33srnrn.cloudfront.net/ https://production.cloudflare.docker.com/	Permet d'accéder aux images logicielles, aux manifestes et aux modèles.
https://kinesis.us-east-1.amazonaws.com	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com	Permet à Cloud Compliance d'accéder aux manifestes et aux modèles, à l'envoi de journaux et de metrics, et de les télécharger.

Assurez-vous que Cloud Manager dispose des autorisations requises

Assurez-vous que Cloud Manager dispose des autorisations nécessaires pour déployer des ressources et créer des groupes de sécurité pour l'instance Cloud Compliance. Vous trouverez les dernières autorisations Cloud Manager dans "Règles fournies par NetApp".

Vérifiez les limites de vos CPU virtuels

Assurez-vous que la limite de vCPU de votre fournisseur de cloud permet de déployer une instance de 16 cœurs. Vous devez vérifier la limite de CPU virtuels pour la famille d'instances appropriée dans la région où Cloud Manager fonctionne.

Dans AWS, la famille d'instances est *On-Demand Standard instances*. Dans Azure, la famille d'instances est *Standard DSv3 Family*.

Pour plus de détails sur les limites des CPU virtuels, consultez les documents suivants :

- "Documentation AWS : limites du service Amazon EC2"
- "Documentation Azure : quotas de vCPU de machine virtuelle"

Assurez-vous que Cloud Manager peut accéder à Cloud Compliance

Assurez la connectivité entre le connecteur et l'instance Cloud Compliance. Le groupe de sécurité du connecteur doit autoriser le trafic entrant et sortant via le port 80 vers et depuis l'instance Cloud Compliance.

Cette connexion permet le déploiement de l'instance Cloud Compliance et vous permet d'afficher des informations dans l'onglet conformité.

Configurer la découverte de Azure NetApp Files

Avant de pouvoir analyser des volumes pour Azure NetApp Files, "Cloud Manager doit être configuré pour détecter la configuration".

Assurez-vous que vous pouvez assurer que Cloud Compliance est en cours d'exécution

L'instance Cloud Compliance doit rester active pour analyser vos données en continu.

Assurez la connectivité du navigateur Web à Cloud Compliance

Une fois que Cloud Compliance est activé, assurez-vous que les utilisateurs accèdent à l'interface Cloud Manager à partir d'un hôte connecté à l'instance Cloud Compliance.

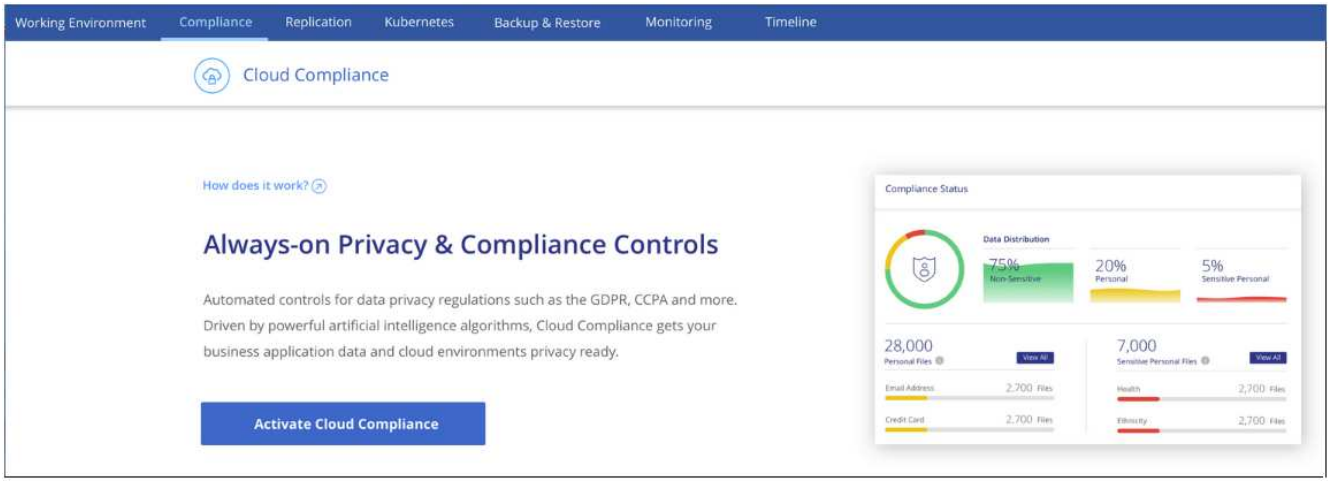
L'instance Cloud Compliance utilise une adresse IP privée pour s'assurer que les données indexées ne sont pas accessibles sur Internet. Par conséquent, le navigateur Web que vous utilisez pour accéder à Cloud Manager doit disposer d'une connexion à cette adresse IP privée. Cette connexion peut s'établir directement auprès d'AWS ou d'Azure (par exemple, un VPN), ou depuis un hôte situé dans le même réseau que l'instance Cloud Compliance.

Déploiement de l'instance Cloud Compliance

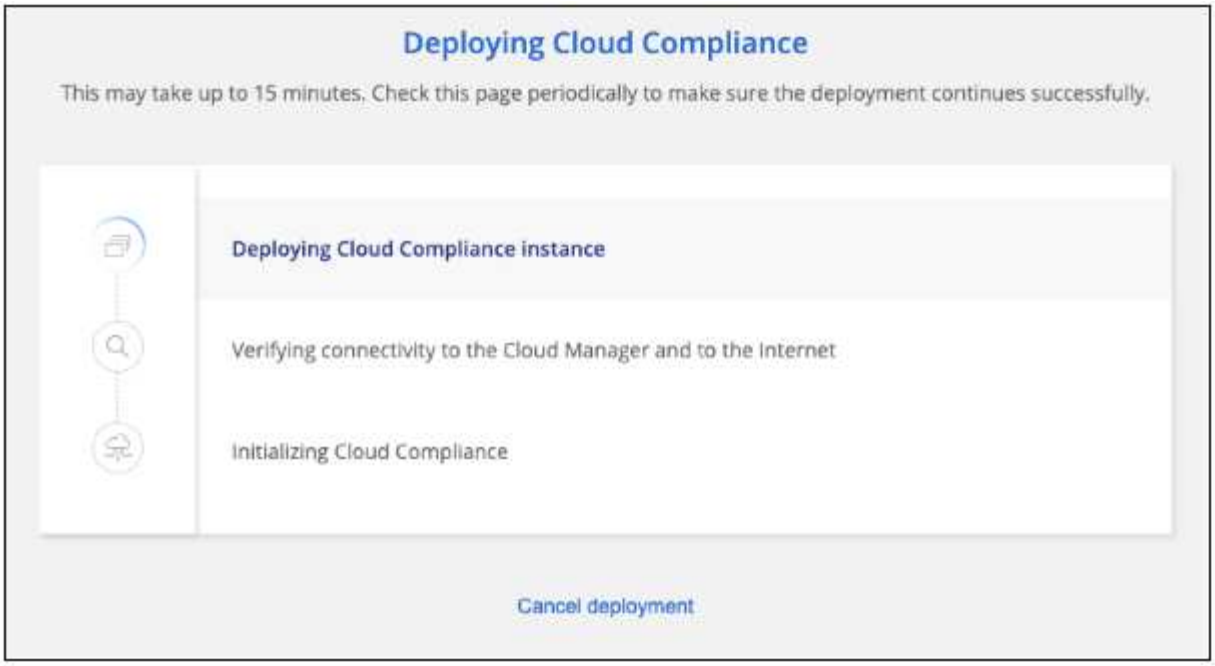
Vous déployez une instance de Cloud Compliance pour chaque instance Cloud Manager.

Étapes

1. Dans Cloud Manager, cliquez sur **Cloud Compliance**.
2. Cliquez sur **Activer Cloud Compliance** pour démarrer l'assistant de déploiement.



3. L'assistant affiche la progression au fur et à mesure des étapes de déploiement. Il s'arrête et demande des commentaires s'il n'y a pas de problème.



4. Lorsque l'instance est déployée, cliquez sur **Continuer la configuration** pour accéder à la page *Scan Configuration*.

Résultat

Cloud Manager déploie l'instance Cloud Compliance dans votre fournisseur cloud.

Et la suite

Dans la page Configuration de la numérisation, vous pouvez sélectionner les environnements de travail, les volumes et les compartiments que vous souhaitez rechercher pour la conformité. Vous pouvez également vous connecter à un serveur de base de données afin de scanner des schémas de base de données spécifiques. Activez Cloud Compliance sur l'une de ces sources de données.

Abonnement au service Cloud Compliance

Les 1 premiers To de données analysés par Cloud Compliance dans un espace de travail Cloud Manager sont gratuits. Un abonnement à AWS ou Azure Marketplace est nécessaire pour poursuivre l'analyse des données après ce point.

Vous pouvez vous abonner à tout moment et vous ne serez facturé que lorsque la quantité de données dépasse 1 To. La quantité totale de données analysées à partir du tableau de bord de conformité cloud est toujours visible. Et le bouton *Subscribe Now* permet de vous abonner facilement lorsque vous êtes prêt.

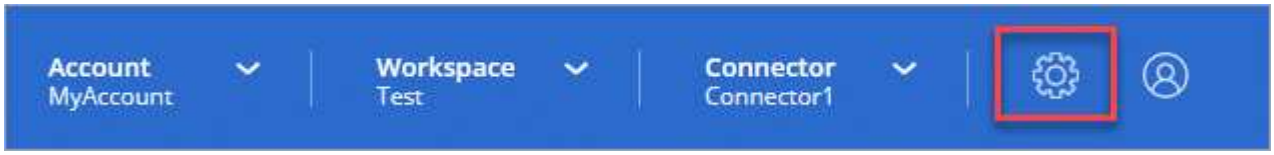
Remarque : si vous êtes invité par Cloud Compliance à vous abonner, mais que vous disposez déjà d'un abonnement Azure, vous utilisez probablement l'ancien abonnement **Cloud Manager** et vous devez passer au nouvel abonnement **NetApp Cloud Manager**. VoirModification du nouveau plan NetApp Cloud Manager dans

Azure pour plus d'informations.

Étapes

Ces étapes doivent être effectuées par un utilisateur qui a le rôle *Account Admin*.

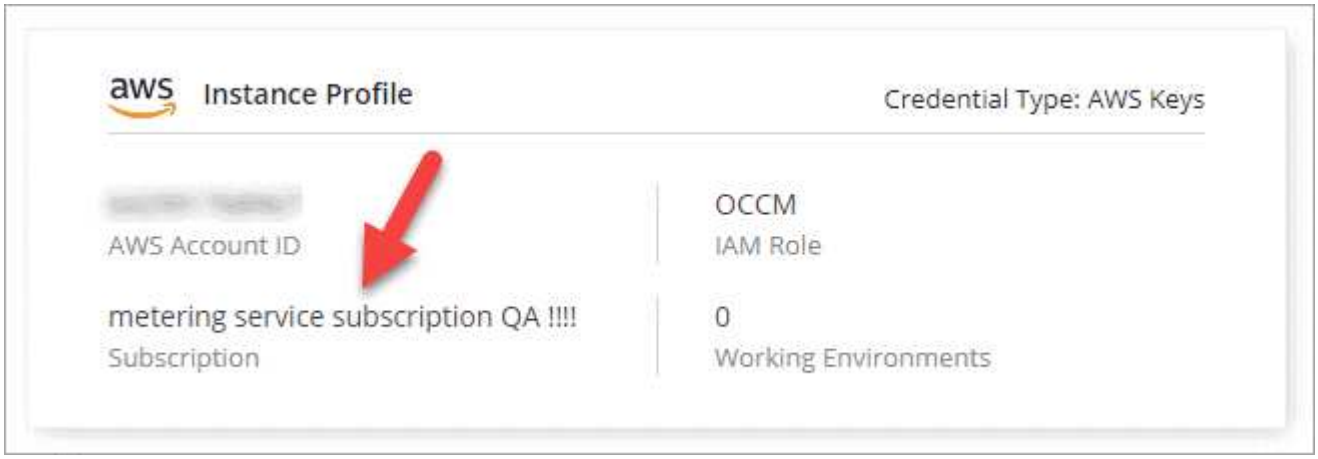
1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.



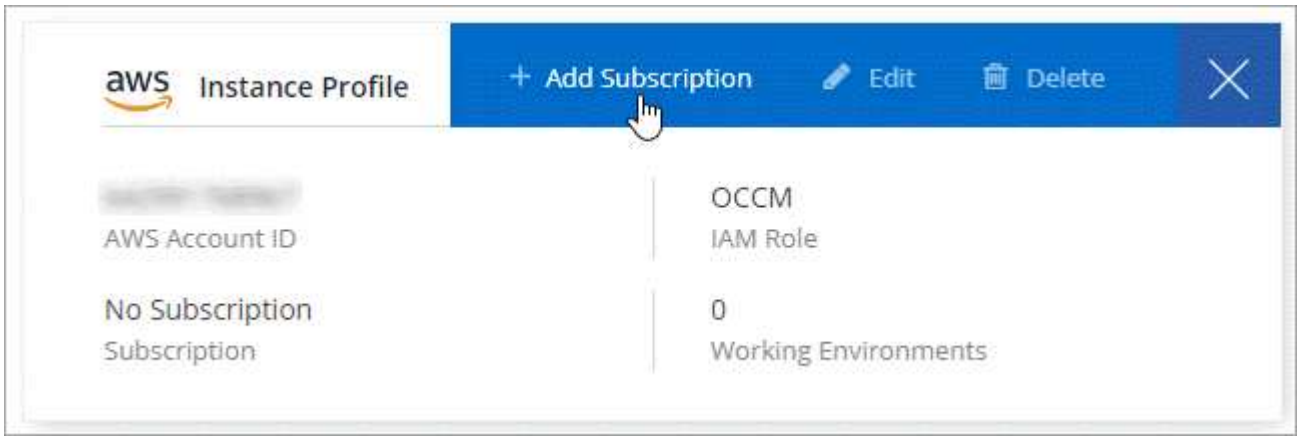
2. Recherchez les identifiants du profil d'instance AWS ou de l'identité de service géré Azure.

   L'abonnement doit être ajouté au profil d'instance ou à l'identité de service géré. La charge ne fonctionnera pas autrement.

   Si vous avez déjà un abonnement, alors vous êtes tout configuré - il n'y a rien d'autre que vous devez faire.



3. Si vous n'avez pas encore d'abonnement, passez le curseur sur les informations d'identification et cliquez sur le menu d'action.
4. Cliquez sur **Ajouter un abonnement**.



5. Cliquez sur **Ajouter un abonnement**, cliquez sur **Continuer** et suivez les étapes.

Découvrez dans la vidéo comment associer un abonnement Marketplace à un abonnement AWS :

► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_aws.mp4 *(video)*

La vidéo suivante explique comment associer un abonnement Marketplace à un abonnement Azure :

► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_azure.mp4 *(video)*

Modification du nouveau plan Cloud Manager dans Azure

Cloud Compliance a été ajouté à l'abonnement Azure Marketplace nommé **NetApp Cloud Manager** au 7 octobre 2020. Si vous disposez déjà de l'abonnement d'Azure **Cloud Manager** d'origine, il ne vous permettra pas d'utiliser Cloud Compliance.

Suivez ces étapes et sélectionnez le nouvel abonnement **NetApp Cloud Manager**, puis supprimez l'ancien abonnement **Cloud Manager**.

Si votre abonnement existant a été délivré avec une offre privée spéciale, vous devez contacter NetApp afin de pouvoir émettre une nouvelle offre privée spéciale avec conformité incluse.

Étapes

Ces étapes sont similaires à l'ajout d'un nouvel abonnement comme décrit ci-dessus, mais varient en quelques endroits.

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.
2. Recherchez les informations d'identification pour l'identité de service géré Azure pour laquelle vous souhaitez modifier l'abonnement et passez le curseur sur les informations d'identification, puis cliquez sur **associer l'abonnement**.

   Les détails de votre abonnement Marketplace actuel s'affichent.

3. Cliquez sur **Ajouter un abonnement**, cliquez sur **Continuer** et suivez les étapes. Vous êtes redirigé vers le portail Azure pour créer votre abonnement.
4. Veillez à sélectionner le plan **NetApp Cloud Manager** qui donne accès à Cloud Compliance et non **Cloud Manager**.
5. Suivez les étapes de la vidéo pour associer un abonnement Marketplace à un abonnement Azure :

   ► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_azure.mp4 *(video)*

6. Revenez à Cloud Manager, sélectionnez le nouvel abonnement et cliquez sur **Associate**.
7. Pour vérifier que votre abonnement a changé, passez le curseur sur « i » ci-dessus dans la carte d'informations d'identification.

   Vous pouvez désormais annuler votre abonnement précédent sur le portail Azure.

8. Sur le portail Azure, accédez à Software as a Service (SaaS), sélectionnez l'abonnement, puis cliquez sur **Unsubscribe**.

Activez la numérisation sur vos sources de données

Mise en route de Cloud Compliance pour Cloud Volumes ONTAP et Azure NetApp Files

Découvrez comment utiliser Cloud Compliance pour Cloud Volumes ONTAP ou Azure NetApp Files en quelques étapes.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

Déployez l'instance Cloud Compliance

"Déployez Cloud Compliance dans Cloud Manager" si aucune instance n'est déjà déployée.

Intégrez Cloud Compliance dans vos environnements de travail

Cliquez sur **Cloud Compliance**, sélectionnez l'onglet **Configuration** et activez les analyses de conformité pour des environnements de travail spécifiques.

Vérifiez l'accès aux volumes

Lorsque Cloud Compliance est activé, assurez-vous que le service informatique peut accéder aux volumes.

- L'instance Cloud Compliance doit disposer d'une connexion réseau à chaque sous-réseau Cloud Volumes ONTAP ou sous-réseau Azure NetApp Files.
- Les groupes de sécurité pour Cloud Volumes ONTAP doivent autoriser les connexions entrantes depuis l'instance Cloud Compliance.
- Les règles d'exportation de volumes NFS doivent autoriser l'accès à partir de l'instance Cloud Compliance.
- Pour analyser les volumes CIFS, Cloud Compliance a besoin d'identifiants Active Directory.

  Cliquez sur **Cloud Compliance** > **Scan Configuration** > **Edit CIFS Credentials** et indiquez les informations d'identification. Ces identifiants peuvent être en lecture seule, mais fournir des informations d'identification administrateur garantit que Cloud Compliance peut lire les données qui requièrent des autorisations élevées.

Configurez les volumes à analyser

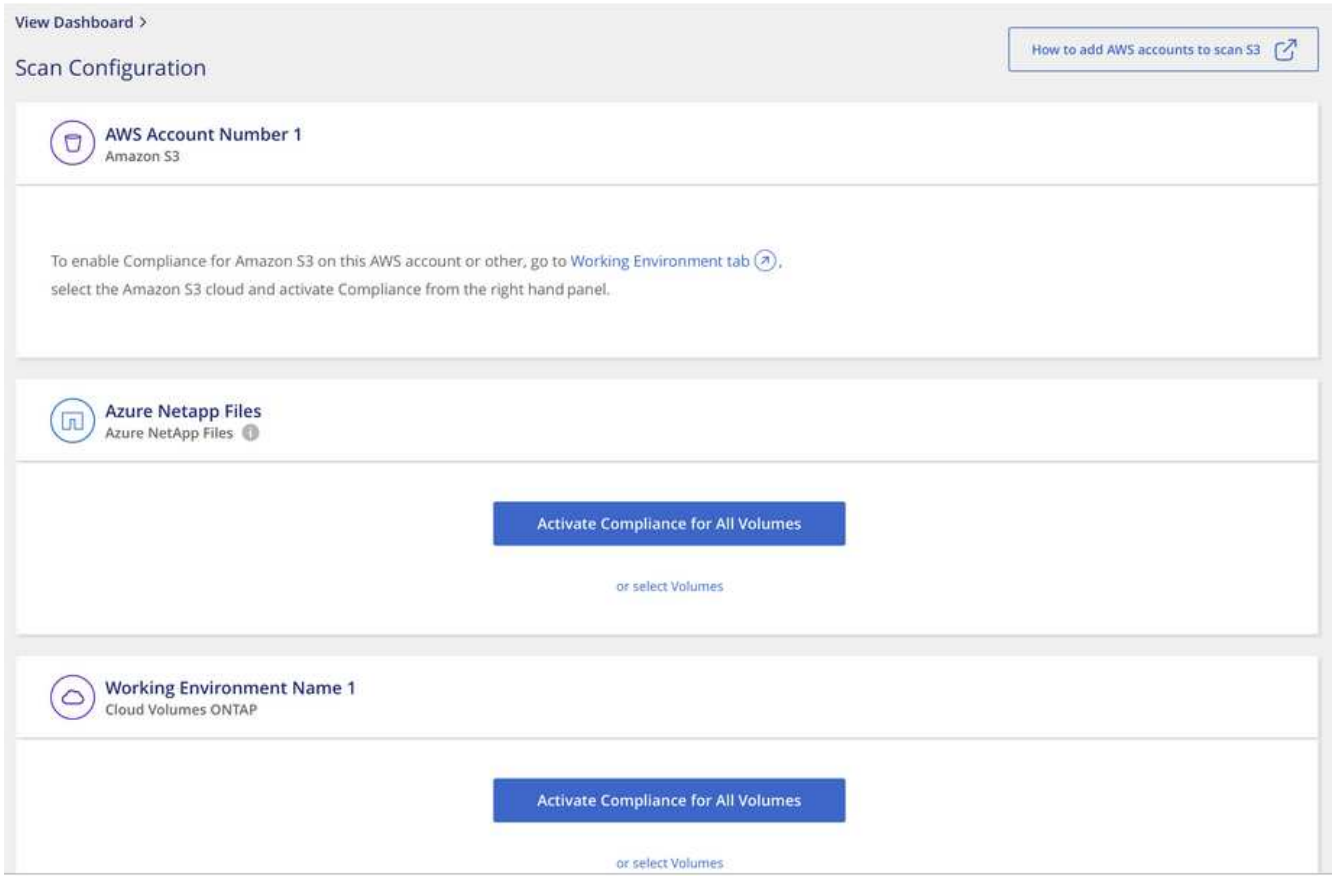
Sélectionnez les volumes que vous souhaitez analyser et Cloud Compliance commence à les analyser.

Déploiement de l'instance Cloud Compliance

"Déployez Cloud Compliance dans Cloud Manager" si aucune instance n'est déjà déployée.

Activation de la conformité cloud dans vos environnements de travail

1. En haut de Cloud Manager, cliquez sur **Cloud Compliance**, puis sélectionnez l'onglet **Configuration**.



2. Pour analyser tous les volumes d'un environnement de travail, cliquez sur **Activer la conformité pour tous les volumes**.

   Pour analyser uniquement certains volumes dans un environnement de travail, cliquez sur **ou sélectionnez volumes**, puis choisissez les volumes que vous souhaitez analyser.

Voir Activation et désactivation des analyses de conformité sur les volumes pour plus d'informations.

Résultat

Cloud Compliance commence l'analyse des données sur chaque environnement de travail. Les résultats seront disponibles dans le tableau de bord de conformité dès que Cloud Compliance termine les analyses initiales. Le temps nécessaire dépend de la quantité de données—il peut être de quelques minutes ou heures.

Vérification de l'accès aux volumes par Cloud Compliance

Assurez-vous que Cloud Compliance peut accéder aux volumes en vérifiant vos groupes de sécurité et vos règles d'exportation. Vous devez fournir des identifiants CIFS à Cloud Compliance pour pouvoir accéder aux volumes CIFS.

Étapes

1. Vérifiez qu'il existe une connexion réseau entre l'instance Cloud Compliance et chaque réseau qui inclut des volumes pour Cloud Volumes ONTAP ou Azure NetApp Files.

Pour Azure NetApp Files, Cloud Compliance ne peut analyser que les volumes qui se trouvent dans la même région que Cloud Manager.

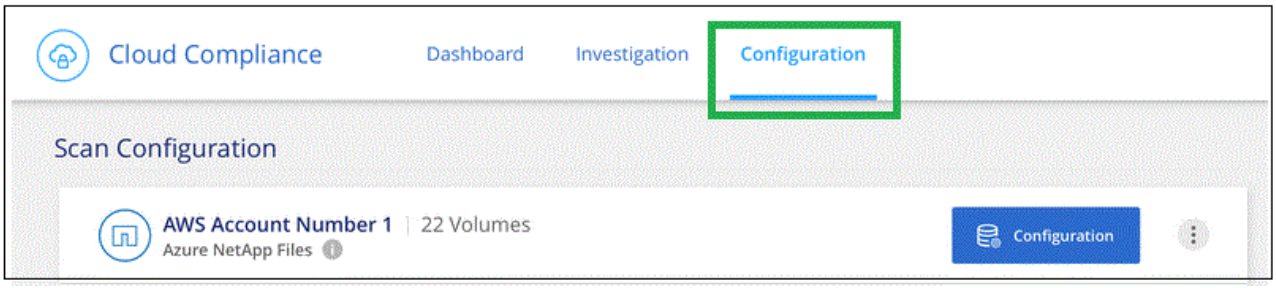
2. Assurez-vous que le groupe de sécurité pour Cloud Volumes ONTAP autorise le trafic entrant depuis l'instance Cloud Compliance.

   Vous pouvez soit ouvrir le groupe de sécurité pour le trafic à partir de l'adresse IP de l'instance Cloud Compliance, soit ouvrir le groupe de sécurité pour tout le trafic à partir du réseau virtuel.

3. Assurez-vous que les règles d'exportation de volume NFS incluent l'adresse IP de l'instance Cloud Compliance afin que les services IT puissent accéder aux données de chaque volume.
4. Si vous utilisez CIFS, fournissez Cloud Compliance avec des identifiants Active Directory pour qu'il puisse analyser les volumes CIFS.

   a. En haut de Cloud Manager, cliquez sur **Cloud Compliance**.

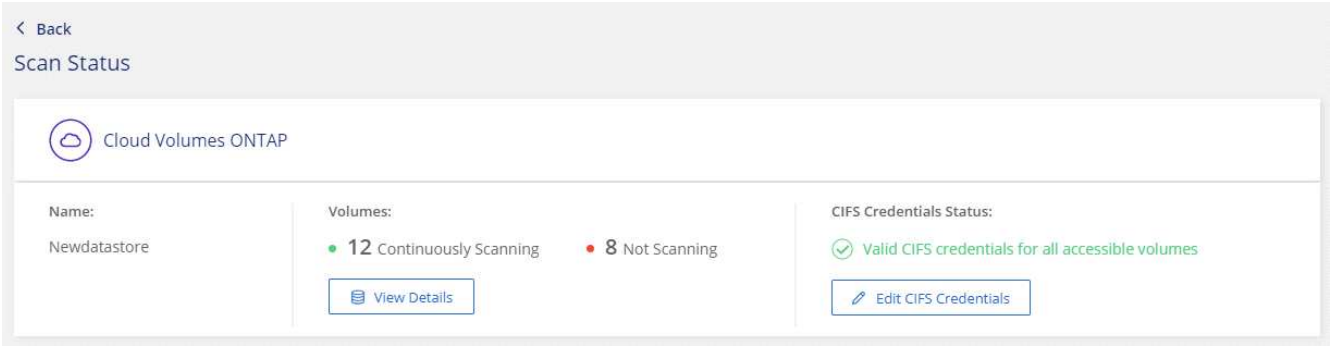
   b. Cliquez sur l'onglet **Configuration**.



   c. Pour chaque environnement de travail, cliquez sur **Modifier les informations d'identification CIFS** et entrez le nom d'utilisateur et le mot de passe requis par Cloud Compliance pour accéder aux volumes CIFS sur le système.

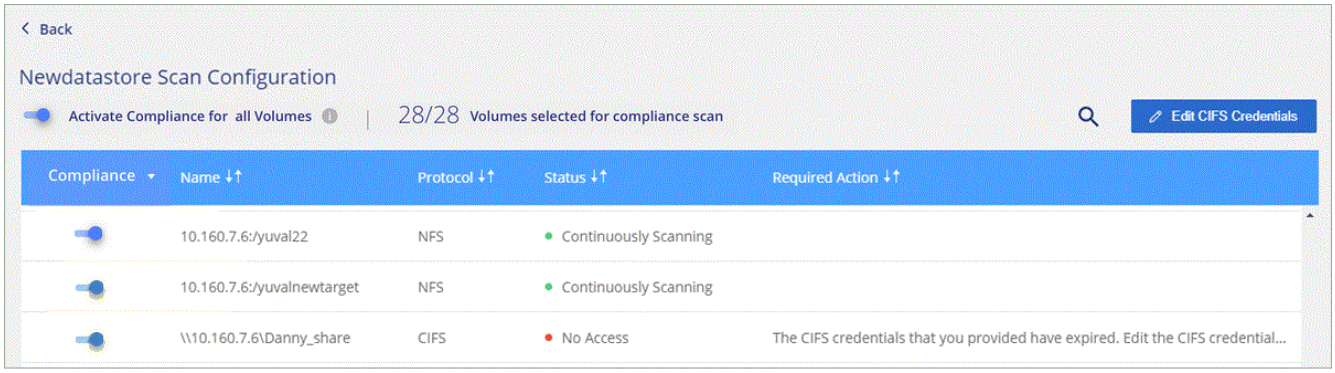
      Les identifiants peuvent être en lecture seule, mais fournir des informations d'identification administrateur garantit que Cloud Compliance peut lire toutes les données qui requièrent des autorisations élevées. Les identifiants sont stockés sur l'instance Cloud Compliance.

      Une fois les informations d'identification saisies, un message indiquant que tous les volumes CIFS ont été authentifiés avec succès s'affiche.



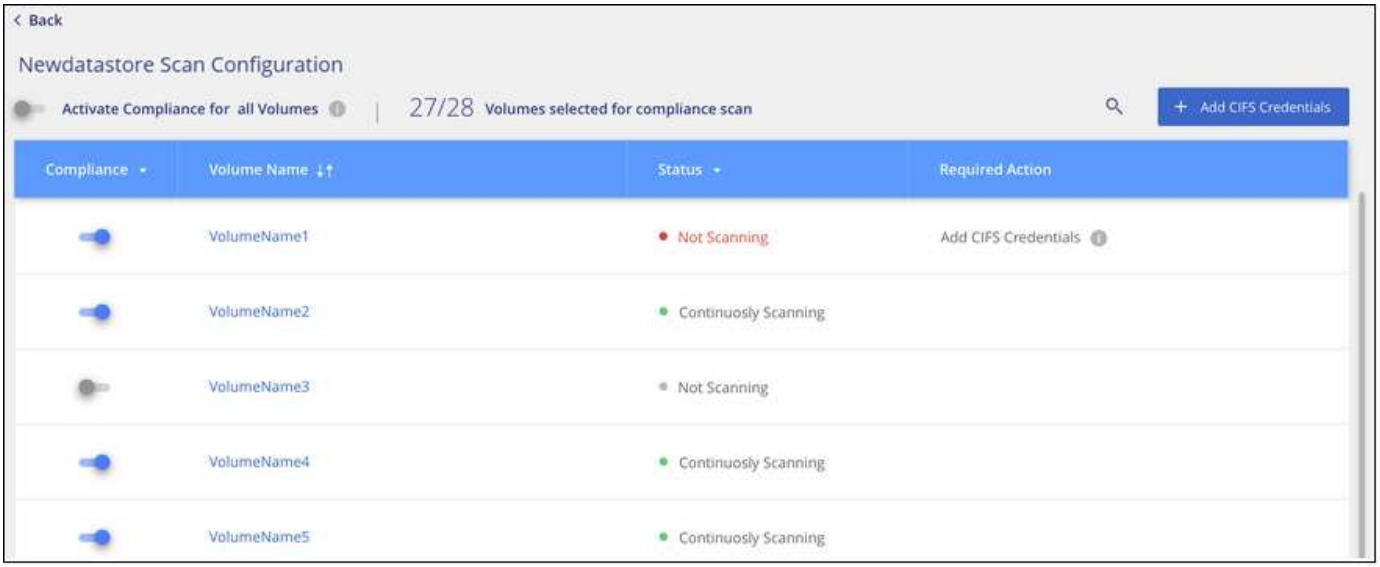
5. Sur la page *Scan Configuration*, cliquez sur **View Details** pour vérifier l'état de chaque volume CIFS et NFS et corriger les erreurs éventuelles.

   L'image suivante montre par exemple trois volumes dont l'un ne peut pas se numériser en raison de problèmes de connectivité réseau entre l'instance Cloud Compliance et le volume.



Activation et désactivation des analyses de conformité sur les volumes

Vous pouvez arrêter ou démarrer la numérisation de volumes dans un environnement de travail à tout moment à partir de la page Configuration de la numérisation. Nous vous recommandons de scanner tous les volumes.



À :	Procédez comme suit :
Désactiver la recherche d'un volume	Déplacez le curseur de volume vers la gauche
Désactiver l'analyse de tous les volumes	Déplacez le curseur **Activer la conformité pour tous les volumes** vers la gauche
Activer la recherche d'un volume	Déplacez le curseur de volume vers la droite
Activer la recherche de tous les volumes	Déplacez le curseur **Activer la conformité pour tous les volumes** vers la droite

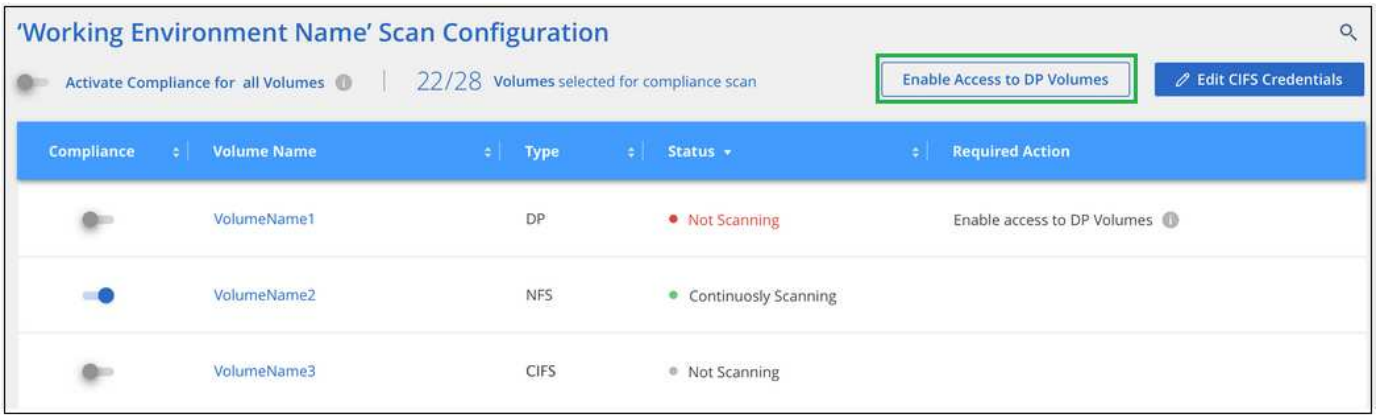
Les nouveaux volumes ajoutés à l'environnement de travail sont automatiquement analysés uniquement lorsque le paramètre **Activer la conformité pour tous les volumes** est activé. Lorsque ce paramètre est désactivé, vous devez activer la numérisation sur chaque nouveau volume créé dans l'environnement de travail.

Analyse des volumes de protection des données

Par défaut, les volumes de protection des données (DP) ne sont pas analysés parce qu'ils ne sont pas

exposés à des ressources externes et que Cloud Compliance ne peut pas y accéder. Ces volumes sont généralement les volumes de destination des opérations SnapMirror à partir d'un cluster ONTAP sur site.

Initialement, la liste de volumes Cloud Compliance identifie ces volumes comme *Type* **DP** avec *Status* **Not Scanning** et la *Requited action* **Enable Access to DP volumes**.



Étapes

Pour analyser ces volumes de protection des données :

1. Cliquez sur le bouton **Activer l'accès aux volumes DP** en haut de la page.
2. Activez chaque volume DP que vous souhaitez analyser ou utilisez le contrôle **Activer la conformité pour tous les volumes** pour activer tous les volumes, y compris tous les volumes DP.

Une fois activé, Cloud Compliance crée un partage NFS à partir de chaque volume DP activé pour la conformité, afin de pouvoir l'analyser. Les règles d'exportation de partage n'autorisent l'accès qu'à partir de l'instance Cloud Compliance.

Seuls les volumes initialement créés en tant que volumes NFS dans le système ONTAP source sont affichés dans la liste des volumes. Les volumes source qui ont été créés initialement en tant que CIFS n'apparaissent pas actuellement dans Cloud Compliance.

Mise en route de Cloud Compliance pour Amazon S3

Cloud Compliance peut analyser vos compartiments Amazon S3 pour identifier les données personnelles et sensibles qui résident dans le stockage objet S3. Cloud Compliance peut analyser n'importe quel compartiment du compte, quel que soit son origine pour une solution NetApp.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir de plus amples informations.

1 Configurez les exigences S3 dans votre environnement cloud

Assurez-vous que votre environnement cloud répond aux exigences de Cloud Compliance, y compris la préparation d'un rôle IAM et la configuration de la connectivité Cloud Compliance vers S3. Voir la liste complète.

Déployez l'instance Cloud Compliance

"Déployez Cloud Compliance dans Cloud Manager" si aucune instance n'est déjà déployée.

Activez la conformité sur votre environnement de travail S3

Sélectionnez l'environnement de travail Amazon S3, cliquez sur **Activer la conformité** et sélectionnez un rôle IAM qui inclut les autorisations requises.

Sélectionnez les compartiments à numériser

Sélectionnez les compartiments que vous souhaitez analyser et Cloud Compliance commence à les analyser.

Vérification des prérequis S3

Les exigences suivantes sont spécifiques à l'analyse des compartiments S3.

Configurez un rôle IAM pour l'instance Cloud Compliance

Cloud Compliance doit disposer d'autorisations pour se connecter aux compartiments S3 de votre compte et pour les analyser. Configurez un rôle IAM qui inclut les autorisations répertoriées ci-dessous. Cloud Manager vous invite à sélectionner un rôle IAM lorsque vous activez Cloud Compliance dans l'environnement de travail Amazon S3.

```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:HeadBucket"
          ],
          "Resource": "*"
      },
      {
          "Effect": "Allow",
          "Action": [
              "iam:GetPolicyVersion",
              "iam:GetPolicy",
              "iam:ListAttachedRolePolicies"
          ],
          "Resource": [
              "arn:aws:iam::*:policy/*",
              "arn:aws:iam::*:role/*"
          ]
      }
  ]
}
```

Connectivité entre Cloud Compliance et Amazon S3

Cloud Compliance a besoin d'une connexion à Amazon S3. Pour assurer cette connexion, le meilleur moyen consiste à utiliser un terminal VPC pour le service S3. Pour obtenir des instructions, reportez-vous à la section "Documentation AWS : création d'un terminal de passerelle".

Lorsque vous créez le point de terminaison VPC, veillez à sélectionner la région, le VPC et la table de routage correspondant à l'instance Cloud Compliance. Vous devez également modifier le groupe de sécurité pour ajouter une règle HTTPS sortante qui active le trafic vers le terminal S3. Dans le cas contraire, Cloud Compliance ne peut pas se connecter au service S3.

Si vous rencontrez des problèmes, reportez-vous à la section "Centre de connaissances du support AWS : pourquoi ne puis-je pas me connecter à un compartiment S3 à l'aide d'un terminal VPC de passerelle ?"

Une alternative consiste à fournir la connexion à l'aide d'une passerelle NAT.

Vous ne pouvez pas utiliser de proxy pour accéder à S3 sur Internet.

Déploiement de l'instance Cloud Compliance

"Déployez Cloud Compliance dans Cloud Manager" si aucune instance n'est déjà déployée.

Vous devez déployer l'instance dans un connecteur AWS, pour que Cloud Manager détecte automatiquement les compartiments S3 dans ce compte AWS et les affiche dans un environnement de travail Amazon S3.

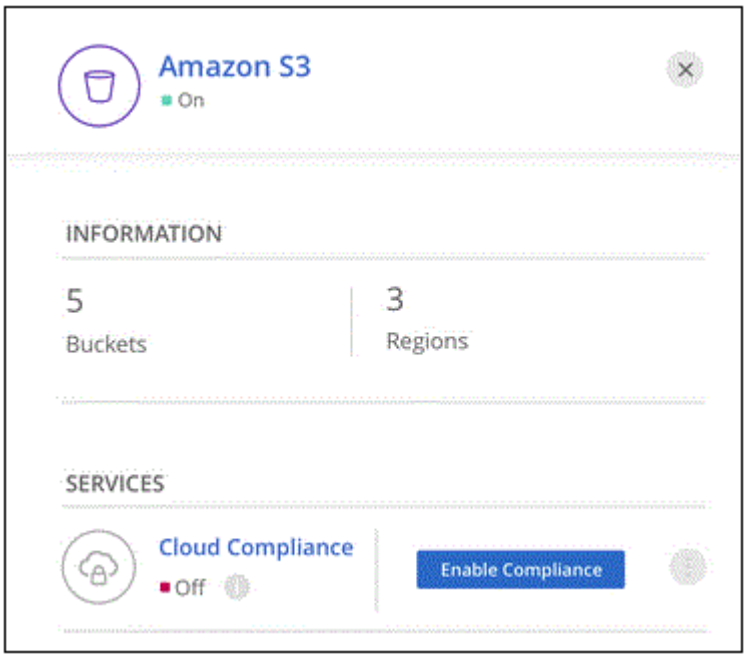
Activation de la conformité sur votre environnement de travail S3

Activez Cloud Compliance sur Amazon S3 après avoir vérifié les prérequis.

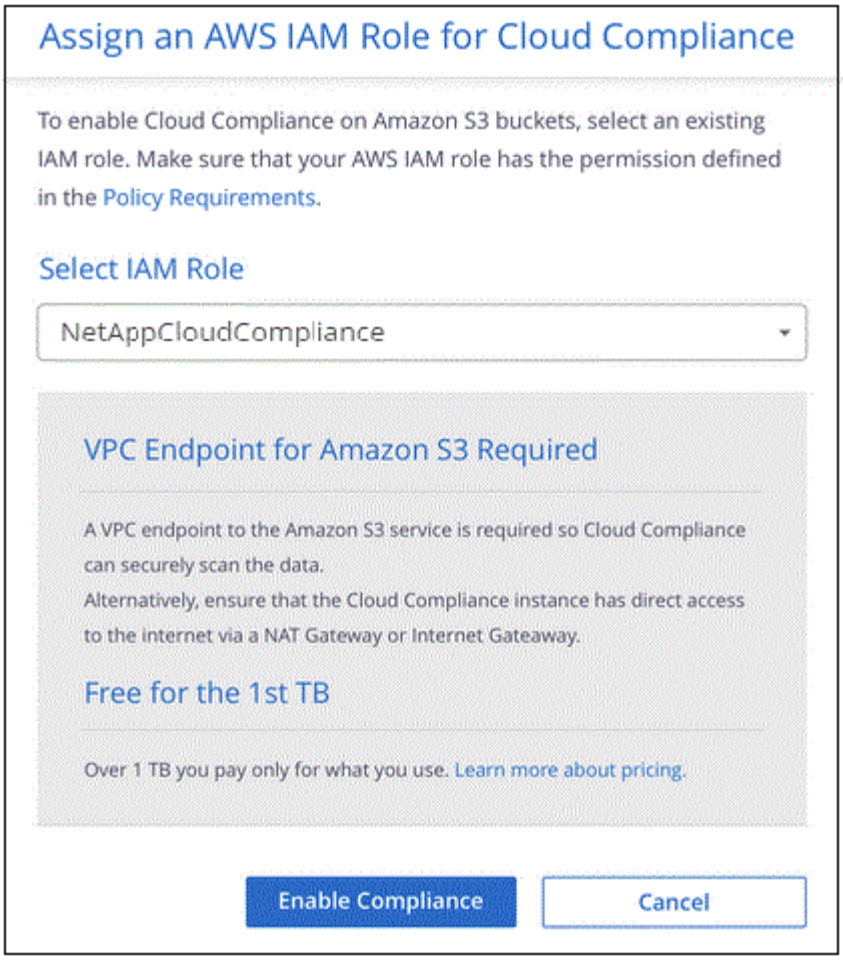
Étapes

1. En haut de Cloud Manager, cliquez sur **environnements de travail**.
2. Sélectionnez l'environnement de travail Amazon S3.

3. Dans le volet de droite, cliquez sur **Activer la conformité**.



4. Lorsque vous y êtes invité, attribuez un rôle IAM à l'instance Cloud Compliance qui possède les autorisations requises.



5. Cliquez sur **Activer la conformité**.

Vous pouvez également activer les analyses de conformité pour un environnement de travail à partir de la page Configuration de la numérisation en cliquant sur le bouton Et en sélectionnant **Activer la conformité**.

Résultat

Cloud Manager attribue le rôle IAM à l'instance.

Activation et désactivation des analyses de conformité dans les compartiments S3

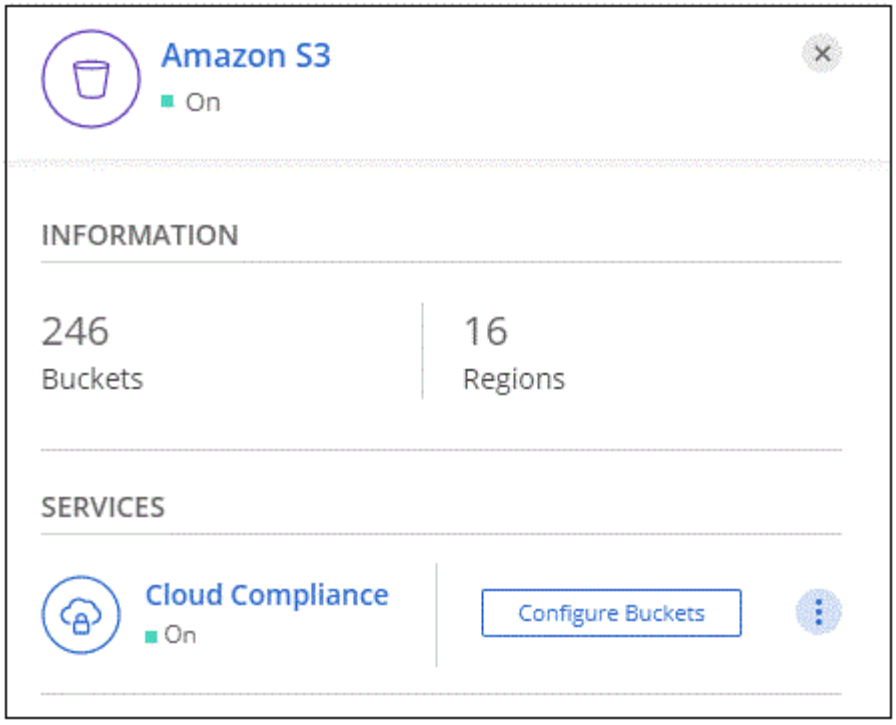
Une fois que Cloud Manager active Cloud Compliance sur Amazon S3, l'étape suivante consiste à configurer les compartiments à analyser.

Lorsque Cloud Manager s'exécute sur le compte AWS possédant les compartiments S3 que vous souhaitez analyser, il détecte ces compartiments et les affiche dans un environnement de travail Amazon S3.

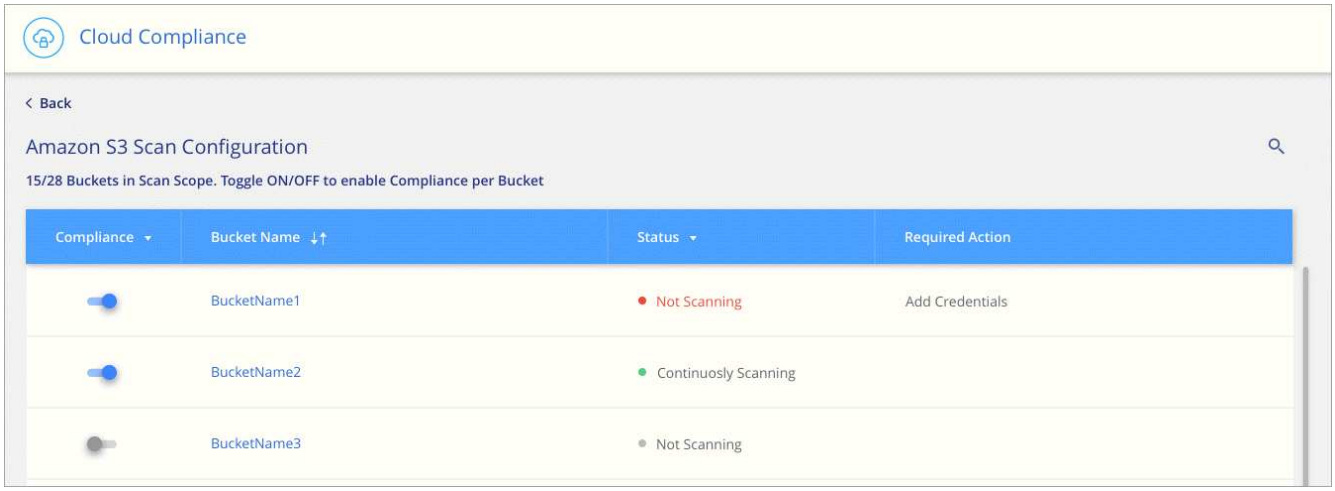
Cloud Compliance l'est également Analysez les compartiments S3 qui se trouvent dans différents comptes AWS.

Étapes

1. Sélectionnez l'environnement de travail Amazon S3.
2. Dans le volet de droite, cliquez sur **configurer les rubriques**.



3. Activez la conformité sur les compartiments à numériser.



Résultat

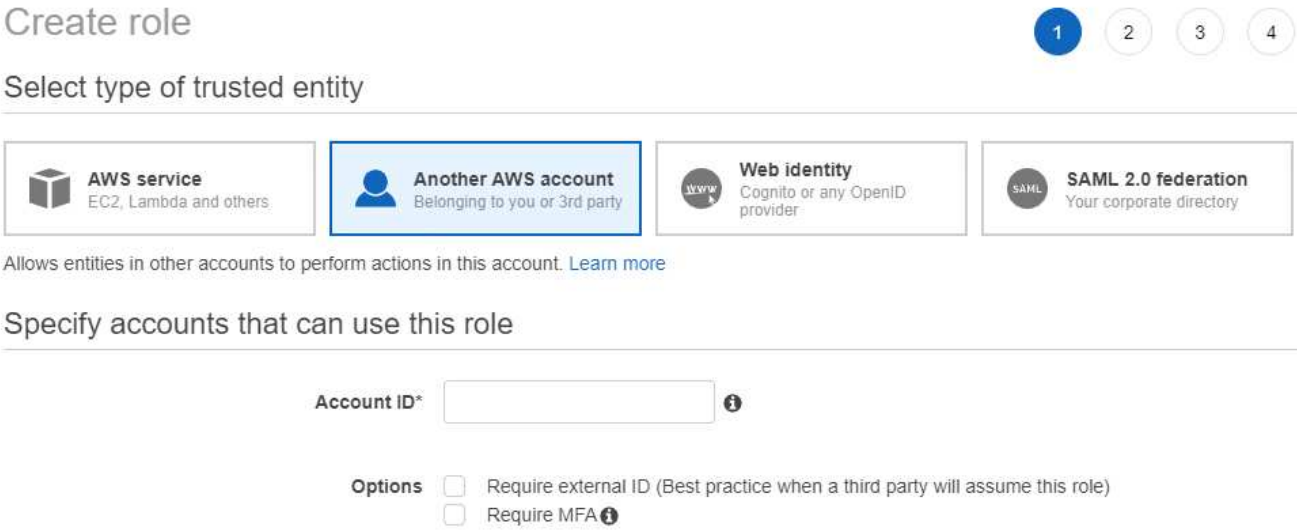
Cloud Compliance commence l'analyse des compartiments S3 activés. En cas d'erreur, elles apparaîtront dans la colonne État, ainsi que l'action requise pour corriger l'erreur.

Analyse des compartiments à partir de comptes AWS supplémentaires

Pour analyser les compartiments S3 qui se trouvent dans un autre compte AWS, vous pouvez attribuer un rôle à partir de ce compte pour accéder à l'instance Cloud Compliance existante.

Étapes

1. Accédez au compte AWS cible où vous voulez analyser les compartiments S3 et créer un rôle IAM en sélectionnant **un autre compte AWS**.



Assurez-vous de faire ce qui suit :

- Entrez l'ID du compte sur lequel réside l'instance Cloud Compliance.
- Modifiez la durée * maximale de la session CLI/API* de 1 heure à 12 heures et enregistrez cette modification.
- Joignez la politique IAM de conformité aux solutions cloud. Assurez-vous qu'il dispose des autorisations requises.

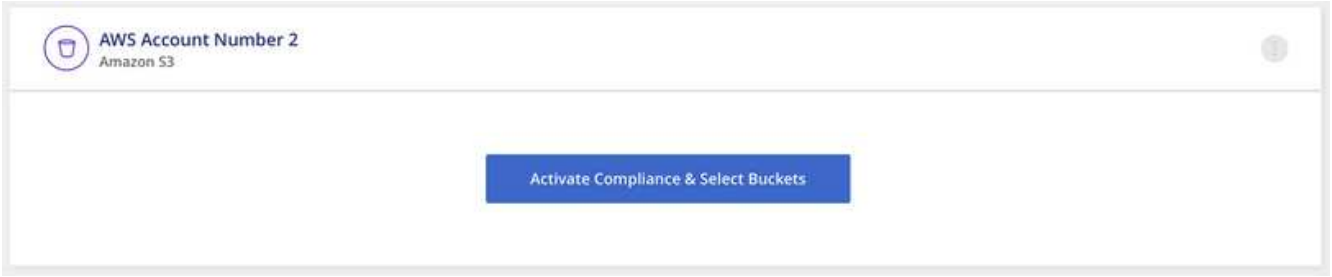
```
{
  "Version": "2012-10-17",
  "Statement": [
      {
          "Effect": "Allow",
          "Action": [
              "s3:Get*",
              "s3:List*",
              "s3:HeadBucket"
          ],
          "Resource": "*"
      },
  ]
}
```

2. Accédez au compte AWS source où réside l'instance Cloud Compliance et sélectionnez le rôle IAM associé à l'instance.
   a. Modifiez la durée * maximale de la session CLI/API* de 1 heure à 12 heures et enregistrez cette modification.
   b. Cliquez sur **attacher des stratégies**, puis sur **Créer une stratégie**.
   c. Créez une stratégie qui inclut l'action « sts:AssumeRole » et l'ARN du rôle que vous avez créé dans le compte cible.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sts:AssumeRole",
            "Resource": "arn:aws:iam::<ADDITIONAL-ACCOUNT-
ID>:role/<ADDITIONAL_ROLE_NAME>"
        },
        {
            "Effect": "Allow",
            "Action": [
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedRolePolicies"
            ],
            "Resource": [
                "arn:aws:iam::*:policy/*",
                "arn:aws:iam::*:role/*"
            ]
        }
    ]
}
```

Le compte de profil d'instance Cloud Compliance a désormais accès au compte AWS supplémentaire.

3. Accédez à la page **Amazon S3 Scan Configuration** et le nouveau compte AWS s'affiche. Notez que Cloud Compliance peut mettre quelques minutes à synchroniser l'environnement de travail du nouveau compte et afficher ces informations.



4. Cliquez sur **Activer la conformité et sélectionnez les rubriques** et sélectionnez les rubriques que vous souhaitez numériser.

Résultat

Cloud Compliance commence l'analyse des nouveaux compartiments S3 activés.

Analyse des schémas de base de données

Suivez quelques étapes pour commencer à analyser vos schémas de base de données

avec Cloud Compliance.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

Vérifiez les prérequis de la base de données

Assurez-vous que votre base de données est prise en charge et que vous disposez des informations nécessaires pour vous connecter à la base de données.

Déployez l'instance Cloud Compliance

"Déployez Cloud Compliance dans Cloud Manager" si aucune instance n'est déjà déployée.

Ajoutez le serveur de base de données

Ajoutez le serveur de base de données auquel vous souhaitez accéder.

Sélectionnez les schémas

Sélectionnez les schémas à numériser.

Vérification des prérequis

Avant d'activer Cloud Compliance, lisez les conditions préalables suivantes pour vous assurer que la configuration est prise en charge.

Bases de données prises en charge

Cloud Compliance peut scanner des schémas à partir des bases de données suivantes :

- MongoDB
- Oracle
- PostgreSQL
- SAP HANA
- Serveur SQL (MSSQL)

La fonction de collecte de statistiques **doit être activée** dans la base de données.

Configuration requise pour les bases de données

Toutes les bases de données connecté à l'instance Cloud Compliance peuvent être analysées, quel que soit l'endroit où elles sont hébergées. Pour vous connecter à la base de données, il vous suffit de disposer des informations suivantes :

- Adresse IP ou nom d'hôte
- Port
- Nom du service (uniquement pour l'accès aux bases de données Oracle)
- Références permettant l'accès en lecture aux schémas

  Lorsque vous choisissez un nom d'utilisateur et un mot de passe, il est important de choisir un nom qui dispose des autorisations de lecture complètes pour tous les schémas et tables que vous souhaitez numériser. Nous vous recommandons de créer un utilisateur dédié pour le système Cloud Compliance avec toutes les autorisations requises.

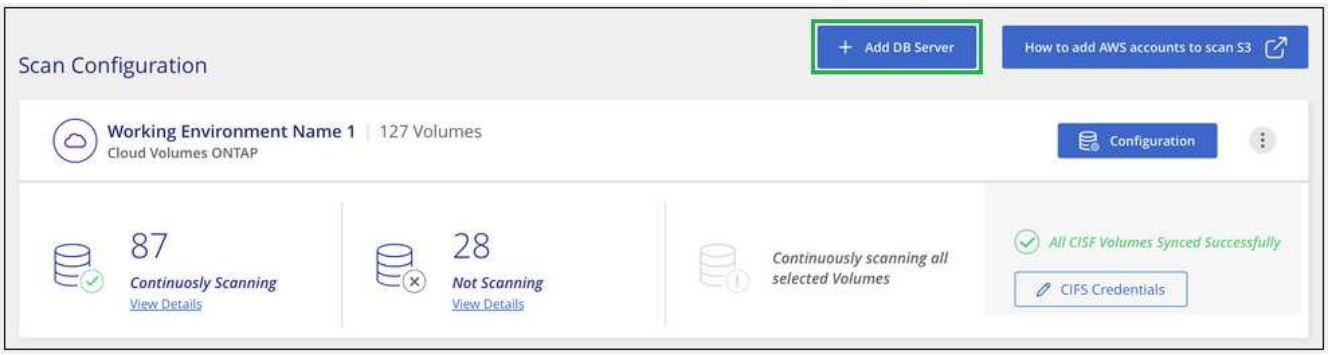
Remarque : pour MongoDB, un rôle d'administrateur en lecture seule est requis.

Ajout du serveur de base de données

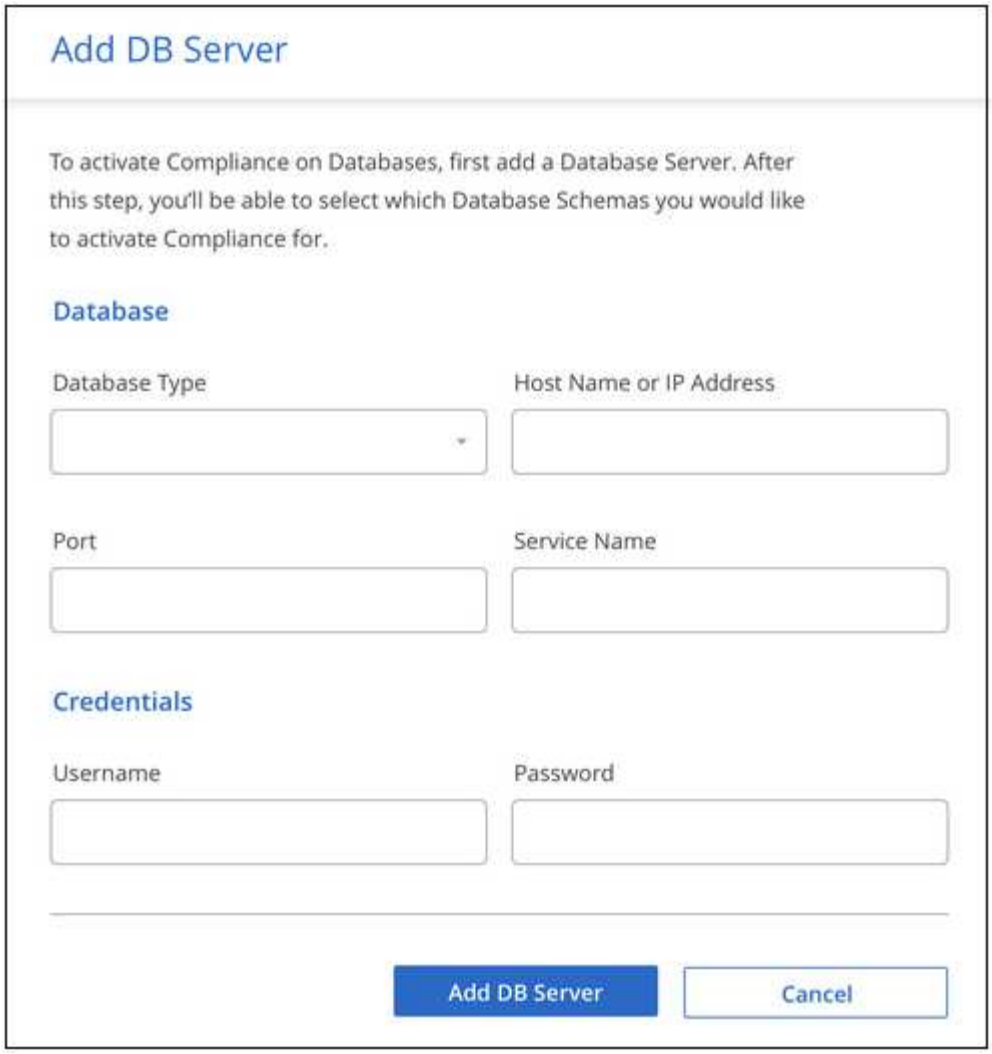
Vous devez avoir "Déploiement d'une instance de Cloud Compliance dans Cloud Manager".

Ajoutez le serveur de base de données où se trouvent les schémas.

1. Dans la page *Scan Configuration*, cliquez sur le bouton **Add DB Server**.



2. Entrez les informations requises pour identifier le serveur de base de données.
   a. Sélectionnez le type de base de données.
   b. Entrez le port et le nom d'hôte ou l'adresse IP pour vous connecter à la base de données.
   c. Pour les bases de données Oracle, entrez le nom du service.
   d. Entrez les identifiants pour que Cloud Compliance puisse accéder au serveur.
   e. Cliquez sur **Ajouter serveur DB**.



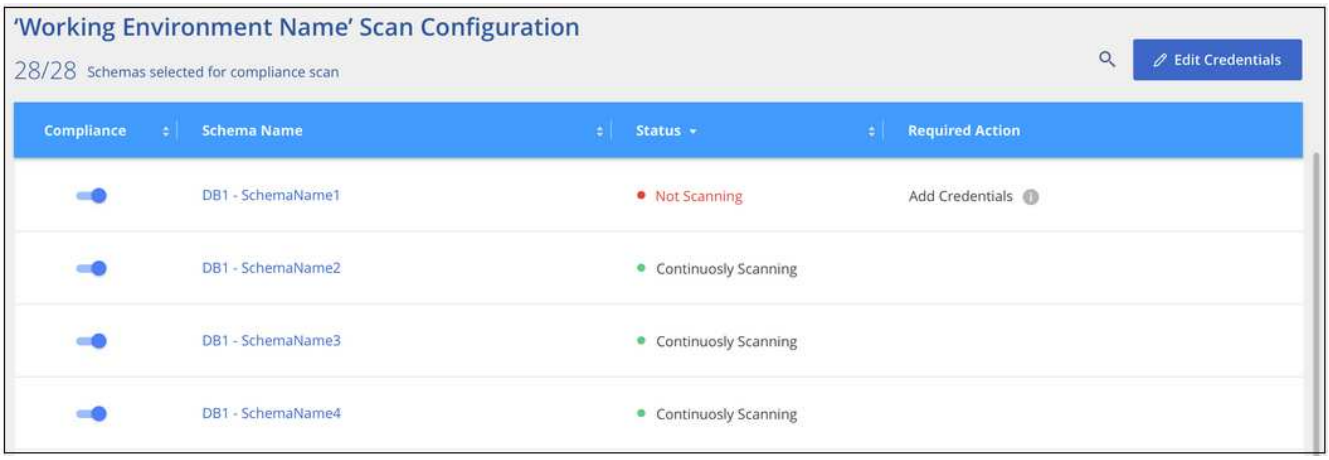
La base de données est ajoutée à la liste des répertoires de travail.

Activation et désactivation des analyses de conformité sur les schémas de base de données

Vous pouvez arrêter ou démarrer la numérisation de schémas à tout moment.

1. Dans la page *Scan Configuration*, cliquez sur le bouton **Configuration** de la base de données à configurer.

2. Sélectionnez les schémas à numériser en déplaçant le curseur vers la droite.



Résultat

Cloud Compliance commence à analyser les schémas de base de données que vous avez activés. S'il y a des erreurs, elles apparaîtront dans la colonne État, ainsi que l'action requise pour corriger l'erreur.

Suppression d'une base de données de Cloud Manager

Si vous ne souhaitez plus analyser une base de données, vous pouvez la supprimer de l'interface Cloud Manager et arrêter toutes les analyses.

Dans la page *Scan Configuration*, cliquez sur le bouton Dans la ligne de la base de données, puis cliquez sur **Supprimer serveur DB**.

Une analyse des données ONTAP sur site avec Cloud Compliance à l'aide de SnapMirror

Vous pouvez analyser les données ONTAP sur site avec Cloud Compliance en répliquant les données NFS ou CIFS sur site vers un environnement de travail Cloud Volumes ONTAP, puis en assurant la conformité. Il n'est pas possible de numériser les données directement à partir d'un environnement de travail ONTAP sur site.

Vous devez avoir "Déploiement d'une instance de Cloud Compliance dans Cloud Manager".

Étapes

1. Depuis Cloud Manager, créez une relation SnapMirror entre le cluster ONTAP sur site et Cloud Volumes ONTAP.
   a. "Découvrez le cluster sur site dans Cloud Manager".
   b. "Créez une réplication SnapMirror entre le cluster ONTAP sur site et Cloud Volumes ONTAP depuis

Cloud Manager".

2. Pour les volumes DP créés à partir de volumes SMB source, depuis l'interface de ligne de commande ONTAP, configurez les volumes de destination SMB pour l'accès aux données. (Cette opération n'est pas requise pour les volumes NFS, car l'accès aux données est activé automatiquement via Cloud Compliance.)
   a. "Créer un partage SMB sur le volume de destination".
   b. "Appliquez les ACL appropriées sur le partage SMB au volume de destination".
3. Depuis Cloud Manager, activez Cloud Compliance dans l'environnement de travail Cloud Volumes ONTAP qui contient les données SnapMirror :
   a. Cliquez sur **environnements de travail**.
   b. Sélectionnez l'environnement de travail qui contient les données SnapMirror et cliquez sur **Activer la conformité**.

      "Cliquez ici pour obtenir de l'aide sur l'activation de Cloud Compliance sur un système Cloud Volumes ONTAP".

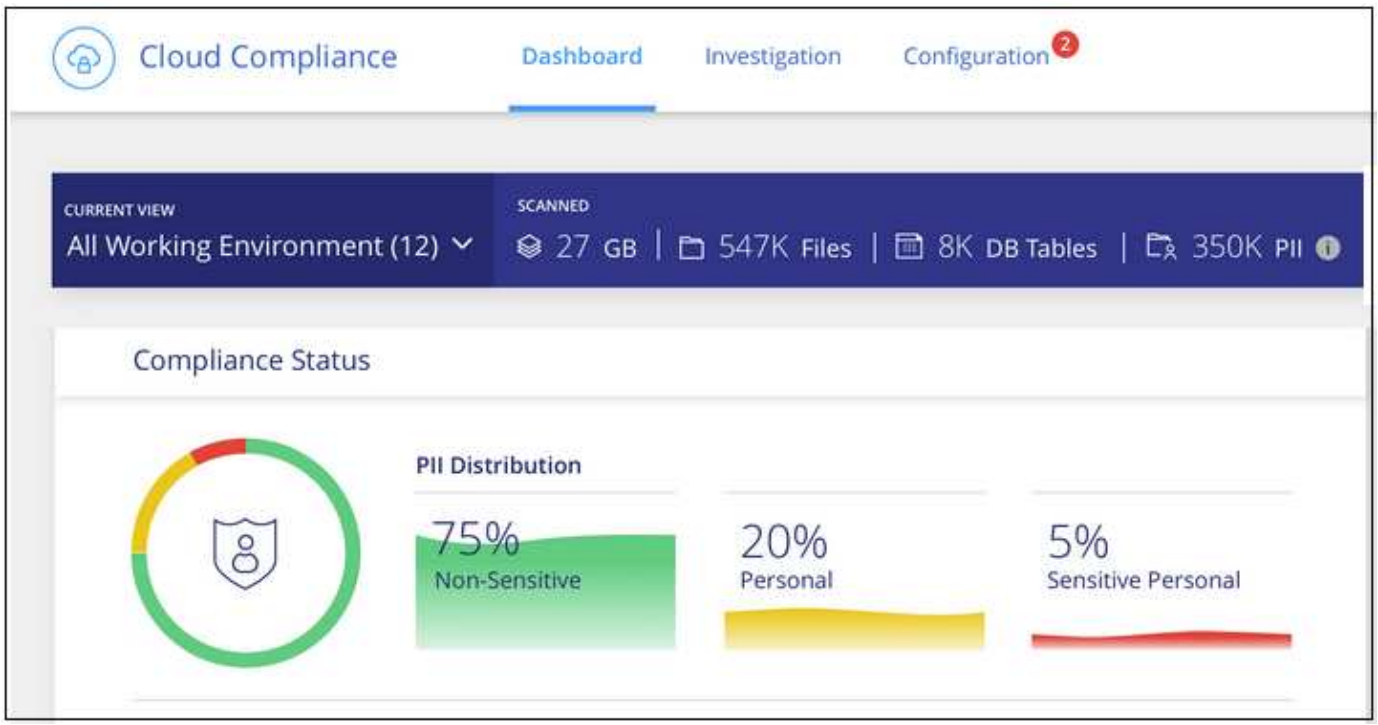
   c. Cliquez sur le bouton **Activer l'accès aux volumes DP** en haut de la page *Scan Configuration*.
   d. Activez chaque volume DP que vous souhaitez analyser ou utilisez le contrôle **Activer la conformité pour tous les volumes** pour activer tous les volumes, y compris tous les volumes DP.

Voir "Analyse des volumes de protection des données" Pour plus d'informations sur l'analyse des volumes DP.

La visibilité et le contrôle des données privées

Prenez le contrôle de vos données privées en affichant les détails sur les données personnelles et les données personnelles sensibles de votre organisation. Vous pouvez également consulter les catégories et les types de fichiers que Cloud Compliance trouve dans vos données.

Par défaut, le tableau de bord Cloud Compliance affiche les données de conformité pour tous les environnements en travail et toutes les bases de données.



Si vous ne souhaitez voir des données que pour certains environnements de travail, sélectionnez ces environnements de travail.

Données personnelles

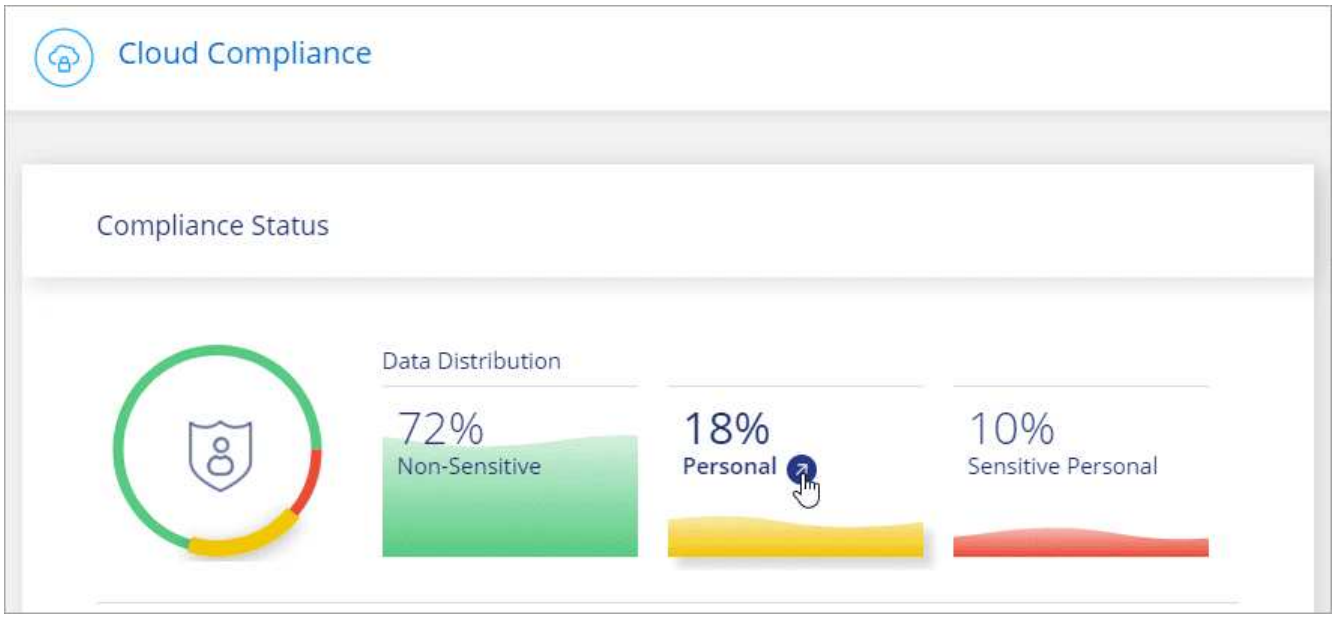
Cloud Compliance identifie automatiquement des mots, des chaînes et des motifs spécifiques (Regex) dans les données. Par exemple, les renseignements d'identification personnelle (RP), les numéros de carte de crédit, les numéros de sécurité sociale, les numéros de compte bancaire, etc. Voir la liste complète.

Pour certains types de données personnelles, Cloud Compliance utilise *proximité validation* pour valider ses résultats. La validation se produit en recherchant un ou plusieurs mots clés prédéfinis à proximité des données personnelles trouvées. Par exemple, Cloud Compliance identifie un secteur public américain Numéro de sécurité sociale (SSN) comme numéro de sécurité sociale s'il y a un mot de proximité, par exemple, *SSN* ou *social Security*. La liste ci-dessous Indique quand Cloud Compliance utilise la validation de proximité.

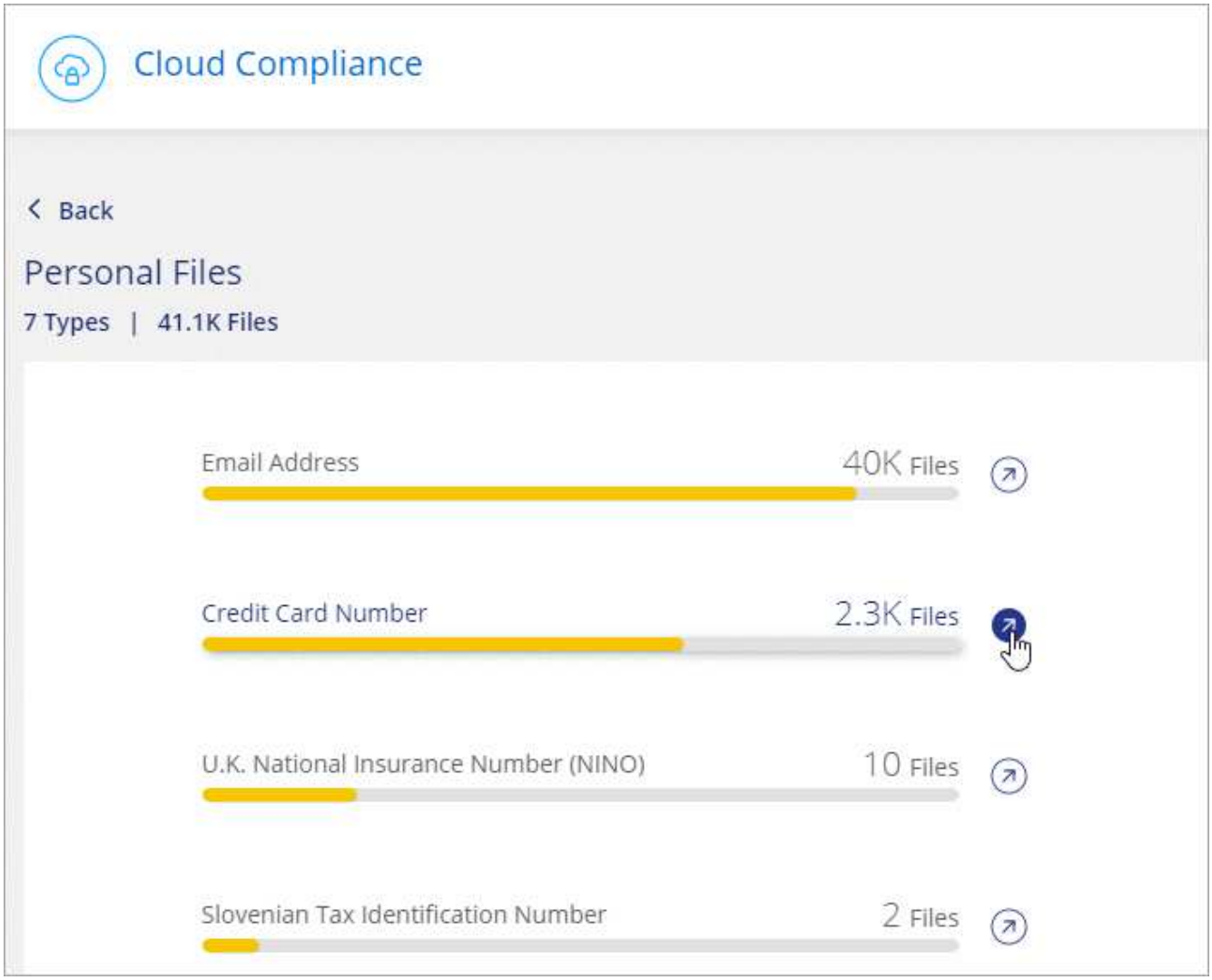
Affichage des fichiers contenant des données personnelles

Étapes

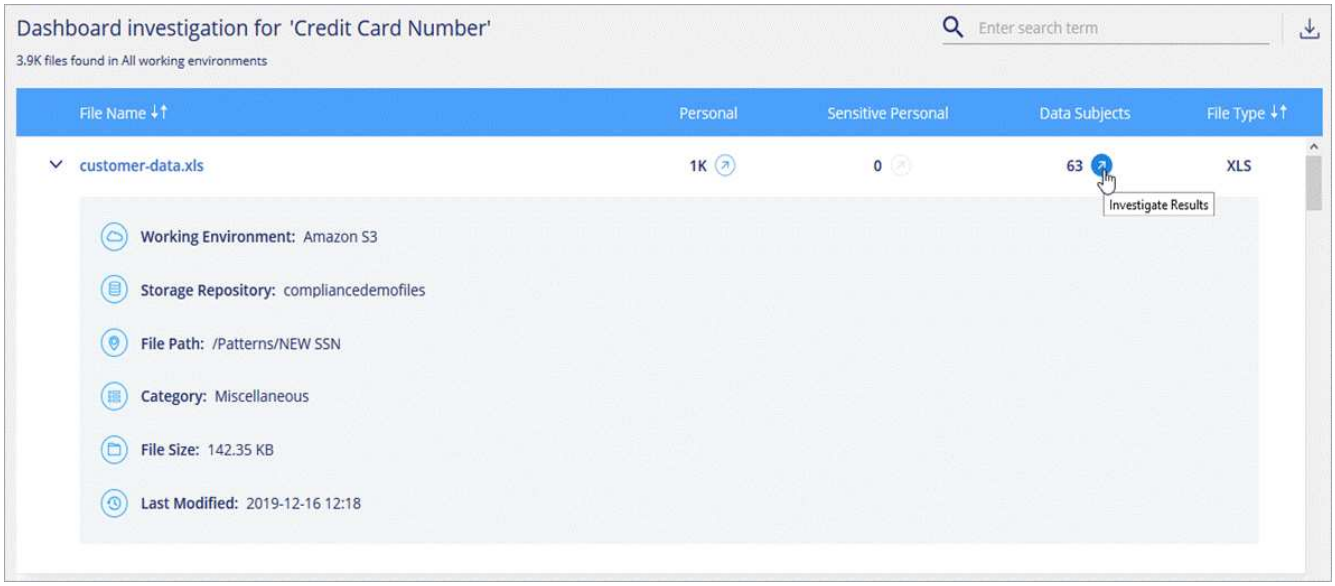
1. En haut de Cloud Manager, cliquez sur **Cloud Compliance** et cliquez sur l'onglet **Dashboard**.
2. Pour examiner les détails de toutes les données personnelles, cliquez sur l'icône en regard du pourcentage de données personnelles.



3. Pour examiner les détails d'un type spécifique de données personnelles, cliquez sur **Afficher tout**, puis cliquez sur l'icône **étudier les résultats** pour un type spécifique de données personnelles.

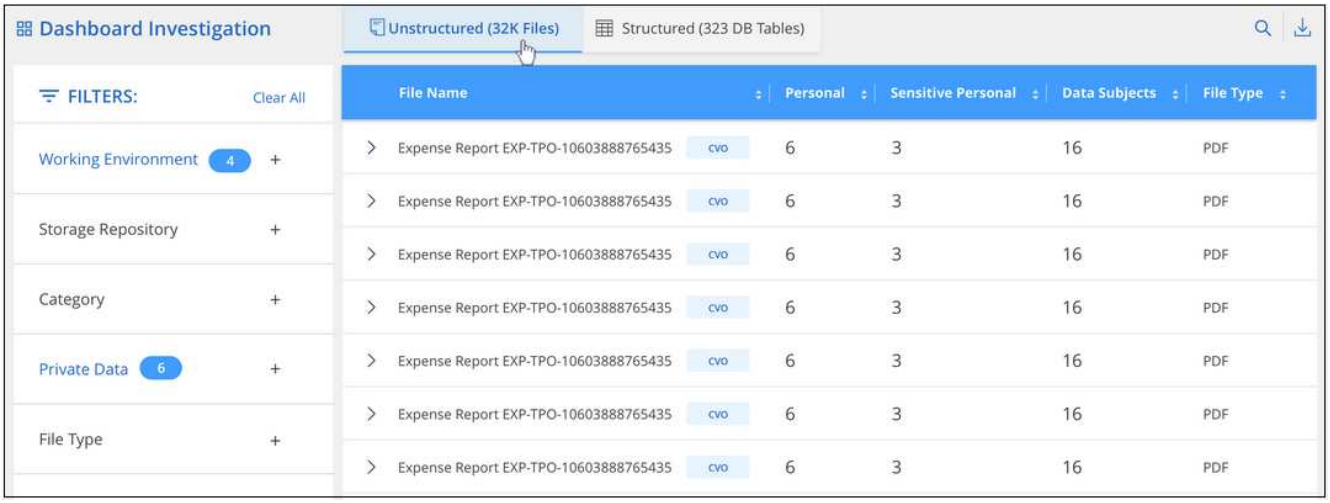


4. Examinez les données en recherchant, en triant, en développant les détails d'un fichier spécifique, en cliquant sur **Informez Results** pour afficher les informations masquées ou en téléchargeant la liste de fichiers.



5. Vous pouvez également filtrer le contenu de la page d'enquête pour n'afficher que les résultats que vous souhaitez voir. Les onglets de niveau supérieur permettent d'afficher des données à partir de fichiers (données non structurées) ou de bases de données (données structurées).

   Vous disposez ensuite de filtres pour l'environnement de travail, le référentiel de stockage, la catégorie, les données privées, le type de fichier, Dernière modification date, et si les autorisations d'accès de l'objet S3 sont ouvertes pour l'accès public.



Types de données personnelles

Les données personnelles contenues dans les dossiers peuvent être des données personnelles générales ou des identificateurs nationaux. La troisième colonne indique si Cloud Compliance utilise ou non validation de proximité pour valider ses résultats pour l'identificateur.

Type	Identificateur	Validation de proximité ?
Généralités	Adresse électronique	Non
	Numéro de carte de crédit	Non
	Numéro IBAN (Numéro de compte bancaire international)	Non

Type	Identificateur	Validation de proximité ?
Identifiants nationaux	Carte d'identité belge (Numero National)	Oui.
	ID brésilien (CPF)	Oui.
	ID bulgare (UCN)	Oui.
	Permis de conduire californien	Oui.
	ID croate (OIB)	Oui.
	Chypre Numéro d'identification fiscale (TIC)	Oui.
	Tchèque/slovaque ID	Oui.
	ID danois (RCP)	Oui.
	ID néerlandais (BSN)	Oui.
	ID estonien	Oui.
	ID finlandais (HETU)	Oui.
	Numéro d'identification fiscale (SPI)	Oui.
	Numéro d'identification fiscale allemand (identifiant Steierliche)	Oui.
	Pièce d'identité grecque	Oui.
	Numéro d'identification fiscale hongrois	Oui.
	Irish ID (PPS)	Oui.
	ID israélien	Oui.
	Numéro d'identification fiscal italien	Oui.
	Carte d'identité lettone	Oui.
	Carte d'identité lituanienne	Oui.
	Luxembourg ID	Oui.
	Identifiant maltais	Oui.
	ID polonais (PESEL)	Oui.
	Numéro d'identification fiscale portugais (FNI)	Oui.
	ID roumain (CNP)	Oui.
	ID slovène (EMSO)	Oui.
	Carte d'identité sud-africaine	Oui.
	Numéro d'identification fiscale espagnol	Oui.
	Carte d'identité suédoise	Oui.
	ROYAUME-UNI ID (NINO)	Oui.
	Numéro de sécurité sociale des États-Unis (SSN)	Oui.

Données personnelles sensibles

Cloud Compliance identifie automatiquement les types particuliers de données sensibles, conformément aux réglementations en matière de confidentialité, notamment "Les articles 9 et 10 du RGPD". Par exemple, des renseignements concernant la santé d'une personne, son origine ethnique ou son orientation sexuelle. Voir la liste complète.

Cloud Compliance exploite l'intelligence artificielle (IA), le traitement du langage naturel (NLP), le machine learning (ML) et l'informatique cognitive (CC) pour comprendre la signification du contenu balayé afin d'extraire les entités et de les catégoriser en conséquence.

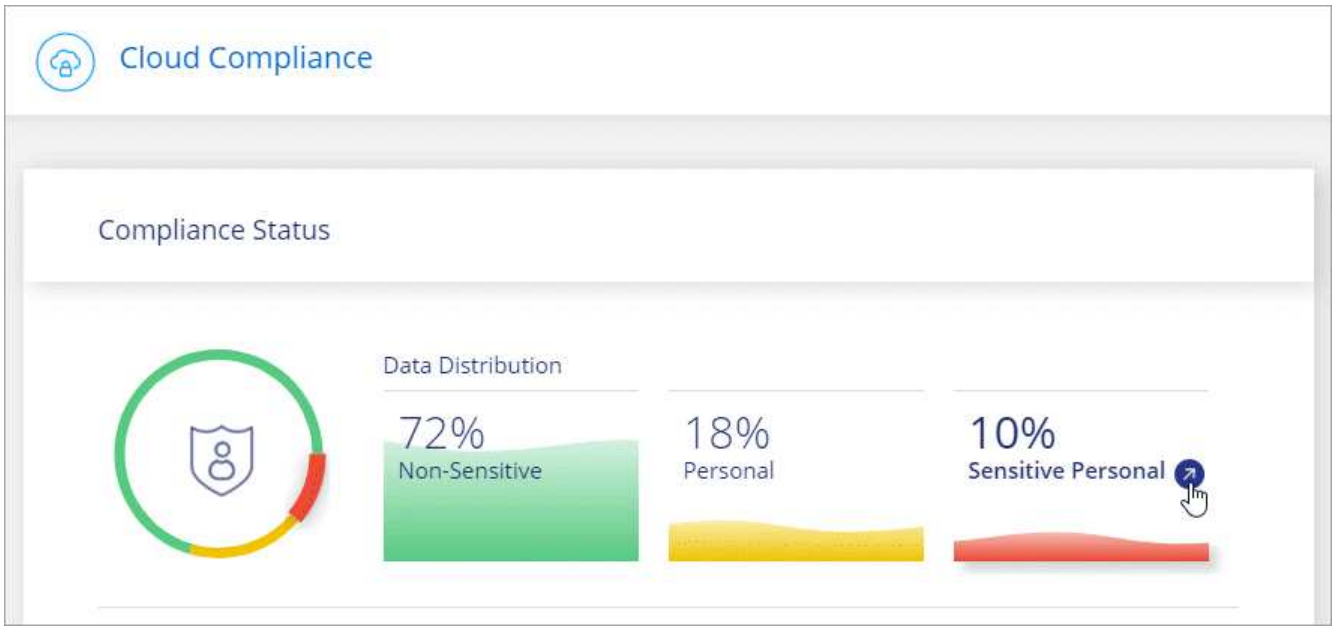
Par exemple, une catégorie de données sensibles du RGPD est l'origine ethnique. Du fait de ses capacités NLP, Cloud Compliance a la différence entre une phrase qui lit « George est mexicain » (en indiquant des données sensibles comme indiqué à l'article 9 du RGPD), et « George mange de la nourriture mexicaine ».

Seul l'anglais est pris en charge lors de la recherche de données personnelles sensibles. La prise en charge d'autres langues sera ajoutée ultérieurement.

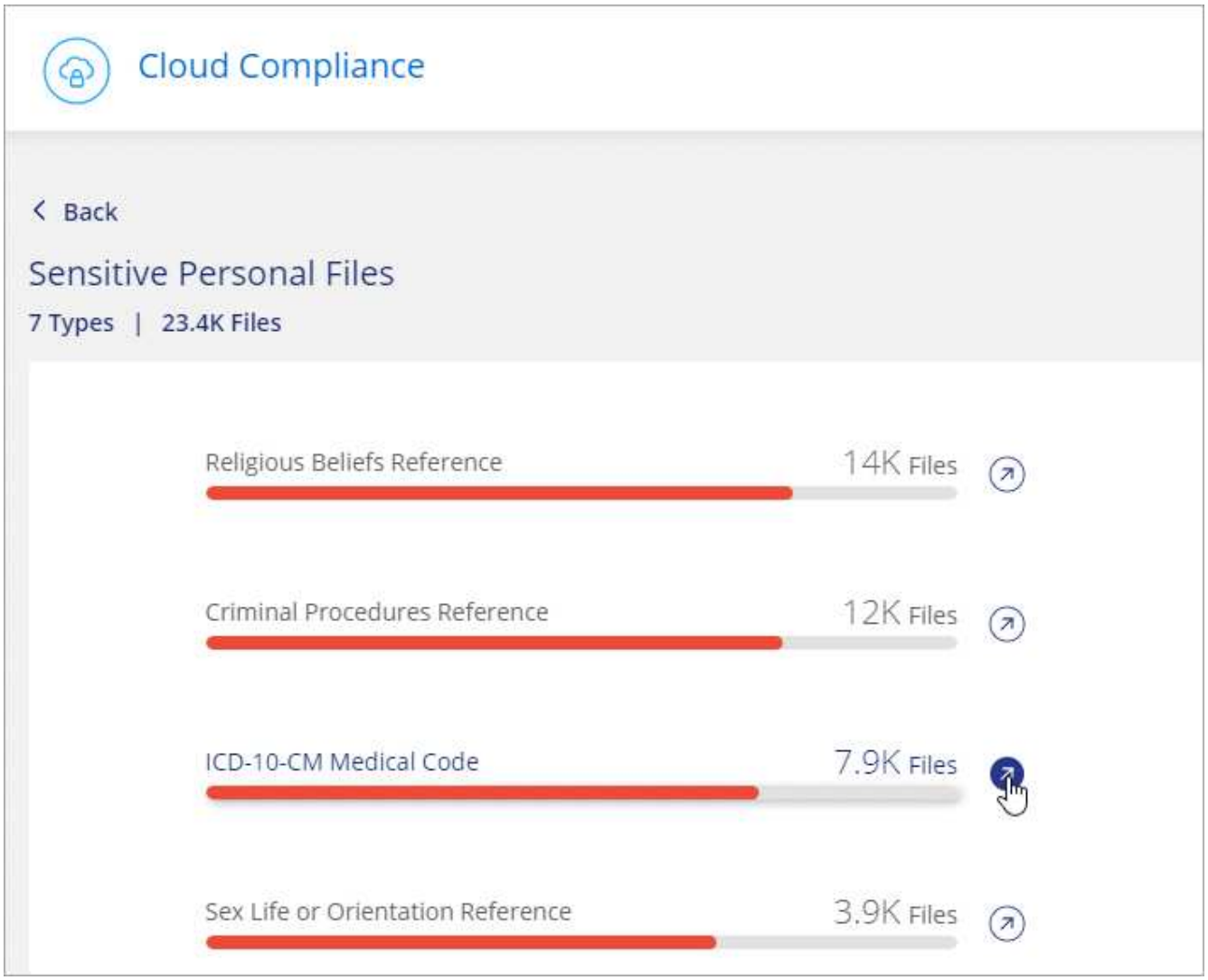
Affichage des fichiers contenant des données personnelles sensibles

Étapes

1. En haut de Cloud Manager, cliquez sur **Cloud Compliance**.
2. Pour examiner les détails de toutes les données personnelles sensibles, cliquez sur l'icône en regard du pourcentage de données personnelles sensibles.



3. Pour examiner les détails d'un type spécifique de données personnelles sensibles, cliquez sur **Afficher tout**, puis cliquez sur l'icône **enquêter sur les résultats** pour un type spécifique de données personnelles sensibles.



4. Examinez les données en recherchant, en triant, en développant les détails d'un fichier spécifique, en cliquant sur **Informez Results** pour afficher les informations masquées ou en téléchargeant la liste de fichiers.

Types de données personnelles sensibles

Les données personnelles sensibles que Cloud Compliance peut trouver dans les fichiers sont les suivantes :

Référence des procédures pénales
Données concernant les condamnations pénales et les infractions d'une personne physique.

Référence ethnique
Données concernant l'origine raciale ou ethnique d'une personne physique.

Référence santé
Données concernant la santé d'une personne physique.

Codes médicaux ICD-9-cm
Codes utilisés dans l'industrie médicale et de la santé.

Codes médicaux ICD-10-cm

Codes utilisés dans l'industrie médicale et de la santé.

Références philosophiques

Données concernant les croyances philosophiques d'une personne naturelle.

Croyances religieuses

Données concernant les croyances religieuses d'une personne naturelle.

Référence de la vie sexuelle ou de l'orientation

Données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Catégories

Cloud Compliance divise les données analysées et les divise en plusieurs types de catégories. Les catégories sont des rubriques basées sur l'analyse par IA du contenu et des métadonnées de chaque fichier. Voir la liste des catégories.

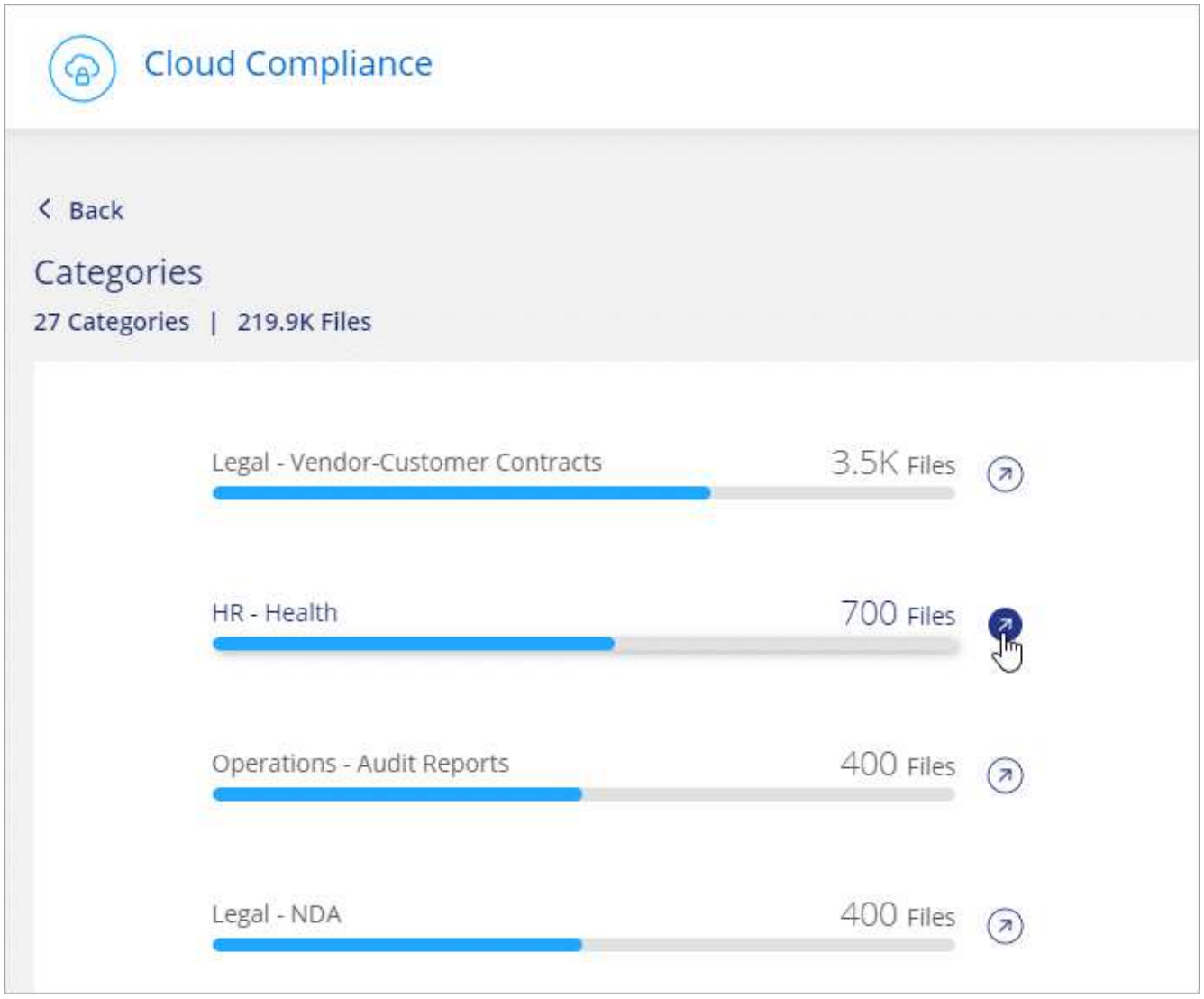
Les catégories peuvent vous aider à comprendre ce qui se passe avec vos données en vous montrant les types d'informations dont vous disposez. Par exemple, une catégorie comme les CV ou les contrats d'employés peut inclure des données sensibles. Lorsque vous étudiez les résultats, vous pouvez constater que les contrats d'employés sont stockés dans un emplacement non sécurisé. Vous pouvez ensuite corriger ce problème.

Seul l'anglais est pris en charge pour les catégories. La prise en charge d'autres langues sera ajoutée ultérieurement.

Affichage des fichiers par catégories

Étapes

1. En haut de Cloud Manager, cliquez sur **Cloud Compliance**.
2. Cliquez sur l'icône **Inquiétude Results** pour l'une des 4 catégories les plus importantes directement à partir de l'écran principal, ou cliquez sur **Afficher tout**, puis cliquez sur l'icône de l'une des catégories.



3. Examinez les données en recherchant, en triant, en développant les détails d'un fichier spécifique, en cliquant sur **Informez Results** pour afficher les informations masquées ou en téléchargeant la liste de fichiers.

Types de catégories

NetApp Cloud Compliance classe vos données comme suit :

Finances

- Bilans
- Bons de commande
- Factures
- Rapports trimestriels

RH

- Vérifications des antécédents
- Plans de rémunération
- Contrats employés

- Évaluations des employés
- Santé
- Reprend

Légal
- NDAS
- Contrats fournisseur-client

Marketing
- Campagnes
- Conférences

Exploitation
- Rapports d’audit

Ventes
- Commandes

Administratifs
- RFI
- RFP
- CAHIER DES CHARGES
- Formation

Assistance
- Plaintes et tickets

Catégories de métadonnées
- Données applicatives
- Archiver les fichiers
- Audio
- Données d’applications d’entreprise
- Fichiers CAO
- Code
- Base de données et fichiers d’index
- Fichiers de conception
- Données d’application de messagerie
- Exécutables
- Données d’applications financières
- Données d’application de santé
- Images
- Journaux
- Documents divers

- Présentations diverses
- Feuilles de calcul diverses
- Vidéos

Types de fichiers

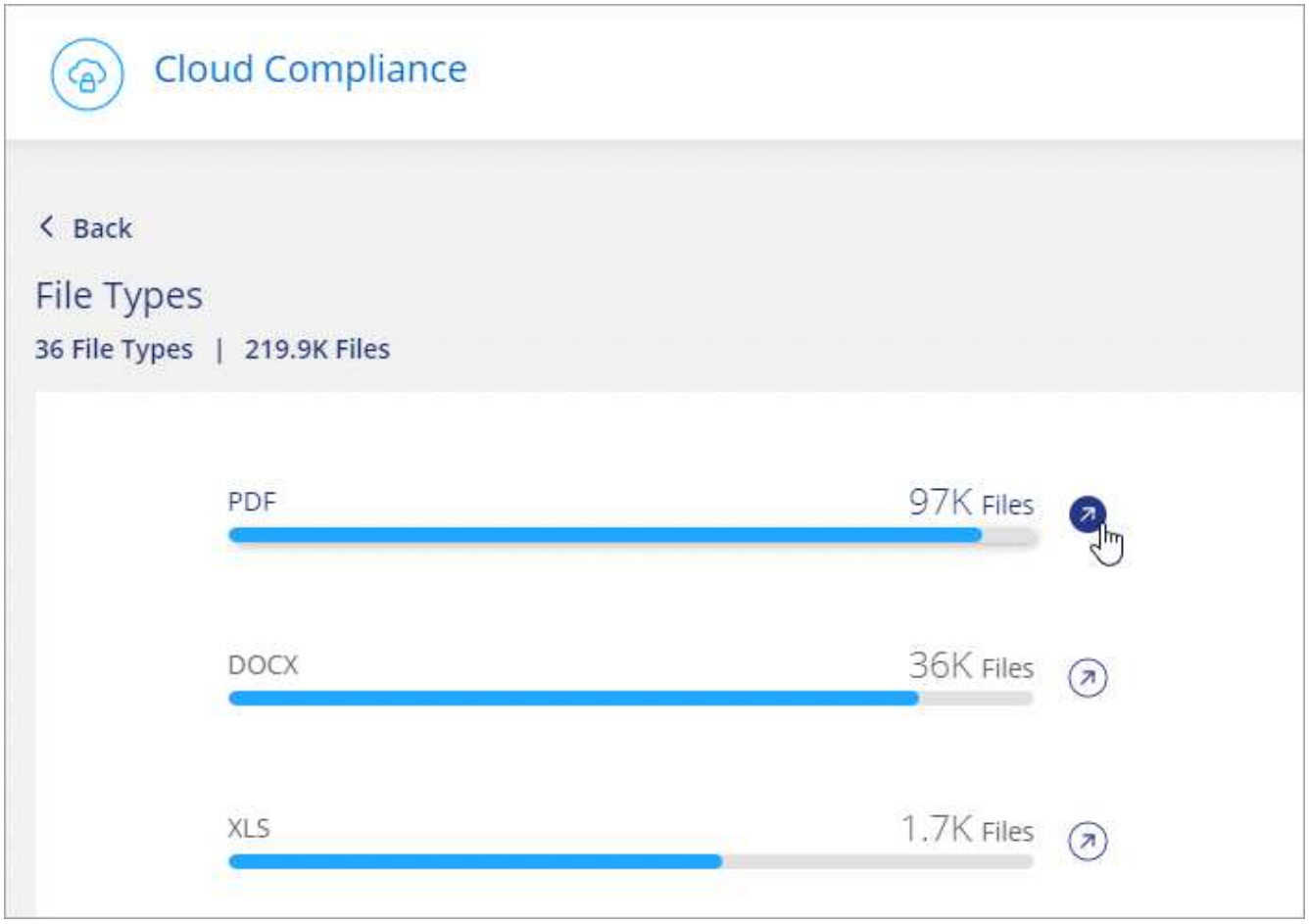
Cloud Compliance réduit les données analysées et les divise par type de fichier. La vérification de vos types de fichiers peut vous aider à contrôler vos données sensibles car il se peut que certains types de fichiers ne soient pas stockés correctement. Voir la liste des types de fichiers.

Par exemple, vous pouvez stocker des fichiers CAO qui contiennent des informations très sensibles sur votre organisation. S'ils ne sont pas sécurisés, vous pouvez prendre le contrôle des données sensibles en limitant les autorisations ou en déplaçant les fichiers vers un autre emplacement.

Affichage des types de fichiers

Étapes

1. En haut de Cloud Manager, cliquez sur **Cloud Compliance**.
2. Cliquez sur l'icône **étudier les résultats** pour l'un des 4 types de fichiers les plus importants directement à partir de l'écran principal ou cliquez sur **Afficher tout**, puis cliquez sur l'icône correspondant à l'un des types de fichiers.



3. Examinez les données en recherchant, en triant, en développant les détails d'un fichier spécifique, en cliquant sur **Informez Results** pour afficher les informations masquées ou en téléchargeant la liste de

fichiers.

Types de fichiers

Cloud Compliance analyse les informations relatives aux catégories et aux métadonnées de tous les fichiers, et affiche tous les types de fichiers dans la section types de fichiers du tableau de bord.

Mais lorsque Cloud Compliance détecte des informations à caractère personnel (PII) ou lorsqu'il effectue une recherche DSAR, seuls les formats de fichier suivants sont pris en charge : .PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF ET .JSON.

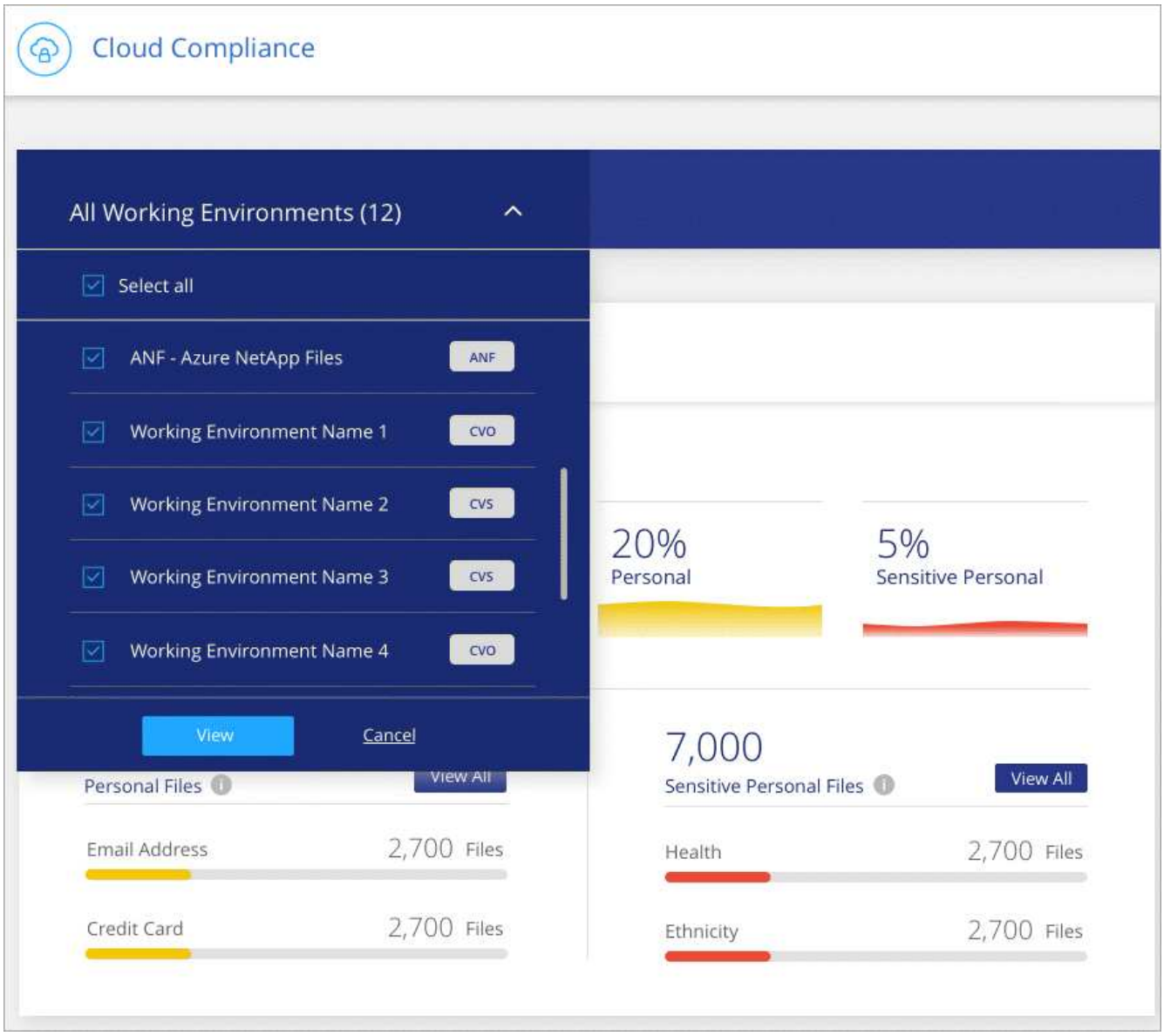
Affichage des données d'environnements de travail spécifiques

Vous pouvez filtrer le contenu du tableau de bord Cloud Compliance pour consulter les données de conformité pour tous les environnements de travail et bases de données, ou pour des environnements de travail spécifiques uniquement.

Lorsque vous filtrez le tableau de bord, Cloud Compliance évalue les données de conformité et les rapports aux environnements de travail que vous avez sélectionnés.

Étapes

1. Cliquez sur la liste déroulante du filtre, sélectionnez les environnements de travail pour lesquels vous souhaitez afficher les données, puis cliquez sur **Afficher**.



Exactitude des informations trouvées

NetApp ne peut garantir une précision de 100 % des données personnelles et des données personnelles sensibles que Cloud Compliance identifie. Vous devez toujours valider les informations en examinant les données.

Le tableau ci-dessous indique l'exactitude des informations fournies par Cloud Compliance à partir des résultats de nos tests. Nous la décomposent par *Precision* et *rappel*:

Précision

La probabilité que Cloud Compliance trouve a été identifiée correctement. Par exemple, un taux de précision de 90 % pour les données personnelles signifie que 9 fichiers sur 10 identifiés comme contenant des renseignements personnels, contiennent en fait des renseignements personnels. 1 fichier sur 10 serait un faux positif.

Rappel

La probabilité que Cloud Compliance trouve ce qu'il faut. Par exemple, un taux de rappel de 70 % pour les données personnelles signifie que Cloud Compliance peut identifier 7 fichiers sur 10 qui contiennent

réellement des données personnelles dans votre entreprise. Cloud Compliance manquerait 30 % des données et n'apparaîtra pas dans le tableau de bord.

Cloud Compliance est une version sous contrôle de disponibilité. Nous améliorons en permanence la précision de nos résultats. Ces améliorations seront automatiquement disponibles dans les prochaines versions de Cloud Compliance.

Type	Précision	Rappel
Données personnelles - général	90 à 95 %	60 à 80 %
Données personnelles - identificateurs de pays	30 à 60 %	40 à 60 %
Données personnelles sensibles	80 à 95 %	20 à 30 %
Catégories	90 à 97 %	60 à 80 %

Ce qui est inclus dans chaque rapport de liste de fichiers (fichier CSV)

À partir de chaque page Investigation, vous pouvez télécharger des listes de fichiers (au format CSV) qui incluent des détails sur les fichiers identifiés. S'il y a plus de 10,000 résultats, seuls les 10,000 meilleurs apparaissent dans la liste.

Chaque liste de fichiers comprend les informations suivantes :

- Nom du fichier
- Type d'emplacement
- Environnement de travail
- Référentiel de stockage
- Protocole
- Chemin des fichiers
- Type de fichier
- Catégorie
- Informations personnelles
- Informations personnelles sensibles
- Date de détection de suppression

  Une date de détection de suppression identifie la date à laquelle le fichier a été supprimé ou déplacé. Cela vous permet d'identifier le moment où des fichiers sensibles ont été déplacés. Les fichiers supprimés ne font pas partie du nombre de fichiers qui s'affiche dans le tableau de bord ou sur la page Investigation. Les fichiers n'apparaissent que dans les rapports CSV.

Affichage des rapports de conformité

Cloud Compliance fournit des rapports qui vous aideront à mieux comprendre l'état du programme de confidentialité des données de votre entreprise.

Par défaut, le tableau de bord Cloud Compliance affiche les données de conformité pour tous les environnements en travail et toutes les bases de données. Si vous souhaitez afficher des rapports contenant

des données pour certains environnements de travail uniquement, sélectionnez ces environnements de travail.

NetApp ne peut garantir une précision de 100 % des données personnelles et des données personnelles sensibles que Cloud Compliance identifie. Vous devez toujours valider les informations en examinant les données.

Rapport d'évaluation des risques pour la confidentialité

Le rapport d'évaluation des risques pour la protection de la vie privée fournit une vue d'ensemble de l'état des risques pour la confidentialité de votre organisation, conformément aux réglementations en matière de confidentialité, telles que le Règlement sur la protection de la vie privée et l'ACFPC. Le rapport contient les informations suivantes :

Statut de conformité

A indice de gravité et la distribution des données, qu'elles soient non sensibles, personnelles ou sensibles.

Présentation de l'évaluation

Une ventilation des types de données personnelles ainsi que des catégories de données.

Sujets de données dans cette évaluation

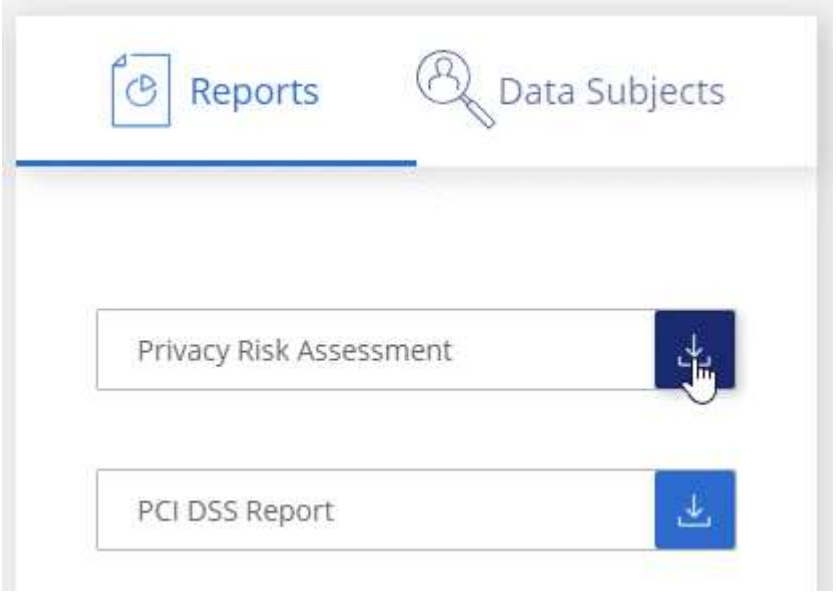
Nombre de personnes, par lieu, pour lesquelles des identificateurs nationaux ont été trouvés.

Génération du rapport d'évaluation des risques pour la confidentialité

Accédez à l'onglet conformité pour générer le rapport.

Étapes

1. En haut de Cloud Manager, cliquez sur **Cloud Compliance**.
2. Sous **Rapports**, cliquez sur l'icône de téléchargement en regard de **évaluation des risques pour la vie privée**.



Résultat

Cloud Compliance génère un rapport PDF que vous pouvez consulter et envoyer à d'autres groupes si nécessaire.

Indice de gravité

Cloud Compliance calcule le score de gravité pour le rapport d'évaluation des risques liés à la confidentialité, sur la base de trois variables :

- Pourcentage de données personnelles sur toutes les données.
- Le pourcentage de données personnelles sensibles hors de toutes les données.
- Le pourcentage de fichiers qui incluent des sujets de données, déterminé par des identificateurs nationaux tels que les ID nationaux, les numéros de sécurité sociale et les numéros d'identification fiscale.

La logique utilisée pour déterminer le score est la suivante :

Indice de gravité	Logique
0	Les trois variables sont exactement 0 %
1	L'une des variables est supérieure à 0 %
2	L'une des variables est supérieure à 3 %
3	Deux des variables sont supérieures à 3 %
4	Trois des variables sont supérieures à 3 %
5	L'une des variables est supérieure à 6 %
6	Deux des variables sont supérieures à 6 %
7	Trois des variables sont supérieures à 6 %
8	L'une des variables est supérieure à 15 %
9	Deux des variables sont supérieures à 15 %
10	Trois des variables sont supérieures à 15 %

Rapport PCI DSS

Le rapport PCI DSS (Payment Card Industry Data Security Standard) peut vous aider à identifier la distribution des informations de carte de crédit dans vos dossiers. Le rapport contient les informations suivantes :

Présentation

Combien de fichiers contiennent des informations de carte de crédit et dans quels environnements de travail.

Le cryptage

Le pourcentage de fichiers contenant des informations de carte de crédit sur des environnements de travail cryptés ou non cryptés. Ces informations sont spécifiques à Cloud Volumes ONTAP.

Protection contre les ransomwares

Le pourcentage de fichiers contenant des informations de carte de crédit sur des environnements de travail où la protection par ransomware est activée ou non. Ces informations sont spécifiques à Cloud Volumes ONTAP.

La conservation

Délai de la dernière modification des fichiers. Ceci est utile car vous ne devez pas conserver les informations de carte de crédit plus longtemps que vous n'avez besoin de les traiter.

Distribution des informations de carte de crédit

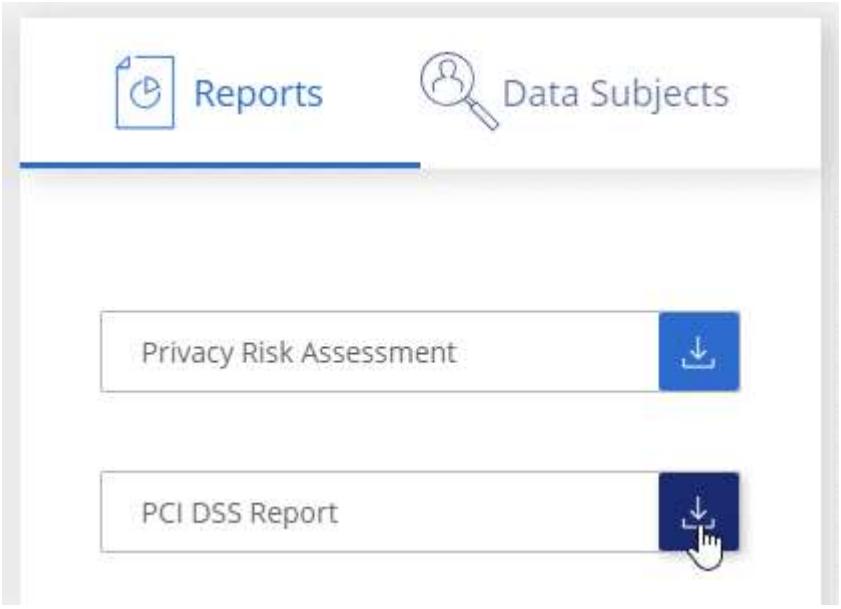
Les environnements de travail où les informations de carte de crédit ont été trouvées et où le chiffrement et la protection contre les ransomwares sont activés.

Génération du rapport PCI DSS

Accédez à l'onglet conformité pour générer le rapport.

Étapes

1. En haut de Cloud Manager, cliquez sur **Cloud Compliance**.
2. Sous **Rapports**, cliquez sur l'icône de téléchargement en regard de **PCI DSS Report**.



Résultat

Cloud Compliance génère un rapport PDF que vous pouvez consulter et envoyer à d'autres groupes si nécessaire.

Rapport HIPAA

Le rapport HIPAA (Health Insurance Portability and Accountability Act) peut vous aider à identifier les fichiers contenant des informations sur la santé. Il est conçu pour aider votre organisation à respecter les lois HIPAA sur la protection des données personnelles. Les informations fournies par Cloud Compliance sont les suivantes :

- Modèle de référence de santé
- Code médical ICD-10-cm
- Code médical ICD-9-cm
- RH – catégorie Santé
- Catégorie données d'application de santé

Le rapport contient les informations suivantes :

Présentation

Combien de fichiers contiennent des informations sur l'état de santé et dans quels environnements de travail.

Le cryptage

Le pourcentage de fichiers contenant des informations de santé sur des environnements de travail chiffrés ou non cryptés. Ces informations sont spécifiques à Cloud Volumes ONTAP.

Protection contre les ransomwares

Le pourcentage de fichiers contenant des informations d'état sur des environnements de travail qui n'ont pas ou qui sont sur lesquels une protection par ransomware est activée. Ces informations sont spécifiques à Cloud Volumes ONTAP.

La conservation

Délai de la dernière modification des fichiers. Ceci est utile parce que vous ne devez pas conserver les renseignements sur la santé plus longtemps que vous n'avez besoin de les traiter.

Distribution des renseignements sur la santé

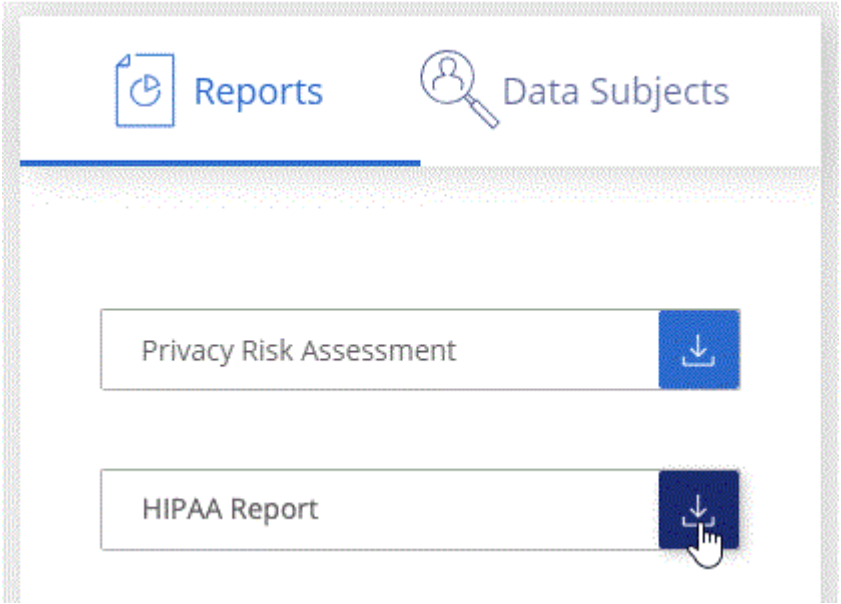
Les environnements de travail dans lesquels les informations de santé ont été trouvées et si le chiffrement et la protection par ransomware sont activés.

Génération du rapport HIPAA

Accédez à l'onglet conformité pour générer le rapport.

Étapes

1. En haut de Cloud Manager, cliquez sur **Cloud Compliance**.
2. Sous **Rapports**, cliquez sur l'icône de téléchargement en regard de **Rapport HIPAA**.



Résultat

Cloud Compliance génère un rapport PDF que vous pouvez consulter et envoyer à d'autres groupes si nécessaire.

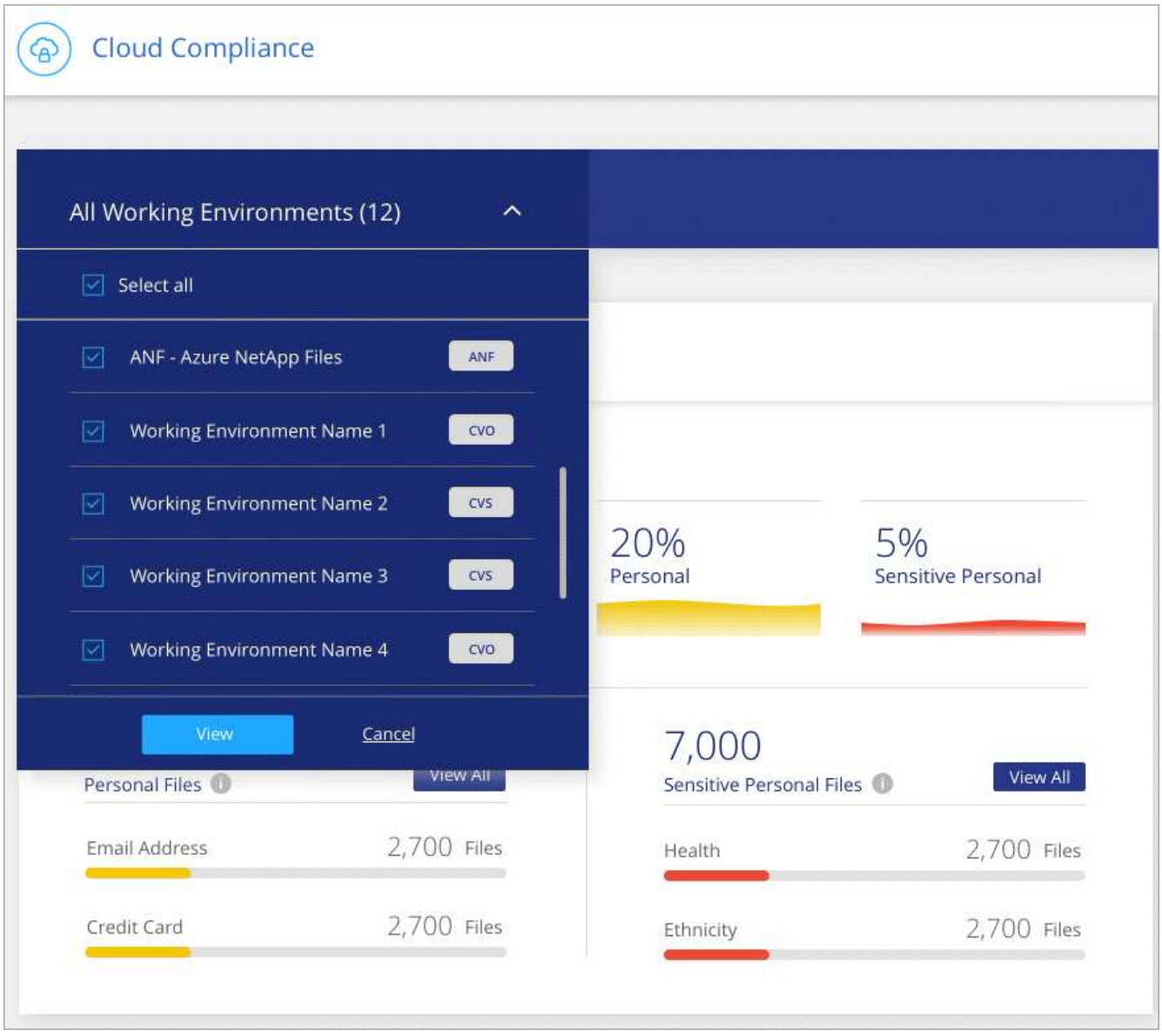
Sélection des environnements de travail pour les rapports

Vous pouvez filtrer le contenu du tableau de bord Cloud Compliance pour consulter les données de conformité pour tous les environnements de travail et bases de données, ou pour des environnements de travail spécifiques uniquement.

Lorsque vous filtrez le tableau de bord, Cloud Compliance évalue les données de conformité et les rapports aux environnements de travail que vous avez sélectionnés.

Étapes

1. Cliquez sur la liste déroulante du filtre, sélectionnez les environnements de travail pour lesquels vous souhaitez afficher les données, puis cliquez sur **Afficher**.



Réponse à une demande d'accès à un sujet de données

Répondez à une demande d'accès aux données (DSAR, Data Subject Access Request) en recherchant le nom complet ou l'identifiant connu d'un sujet (par exemple une adresse

e-mail), puis en téléchargeant un rapport. Ce rapport est conçu pour aider votre entreprise à respecter le RGPD ou les autres lois similaires sur la confidentialité des données.

NetApp ne peut garantir une précision de 100 % des données personnelles et des données personnelles sensibles que Cloud Compliance identifie. Vous devez toujours valider les informations en examinant les données.

Qu'est-ce qu'une demande d'accès aux données ?

Les réglementations en matière de confidentialité, telles que le RGPD européen, accordent à des sujets de données (clients ou employés, par exemple) le droit d'accéder à leurs données personnelles. Lorsqu'un sujet de données demande cette information, elle est appelée DSAR (Data Subject Access request). Les organisations sont tenues de répondre à ces demandes "sans délai excessif" et au plus tard dans un mois après réception.

En quoi Cloud Compliance peut-il vous aider à répondre à un SAR ?

Lorsque vous effectuez une recherche dans un sujet de données, Cloud Compliance trouve tous les fichiers dont le nom ou l'identifiant de cette personne est présent. Cloud Compliance vérifie les dernières données pré-indexées pour le nom ou l'identifiant. Il ne lance pas de nouvelle acquisition.

Une fois la recherche terminée, vous pouvez télécharger la liste des fichiers d'un rapport de demande d'accès aux données. Le rapport rassemble les informations issues des données et les place en termes juridiques que vous pouvez renvoyer à la personne.

Recherche de sujets de données et téléchargement de rapports

Recherchez le nom complet ou l'identifiant connu du sujet de données, puis téléchargez un rapport de liste de fichiers ou un rapport DSAR. Vous pouvez effectuer une recherche par "tout type d'informations personnelles".

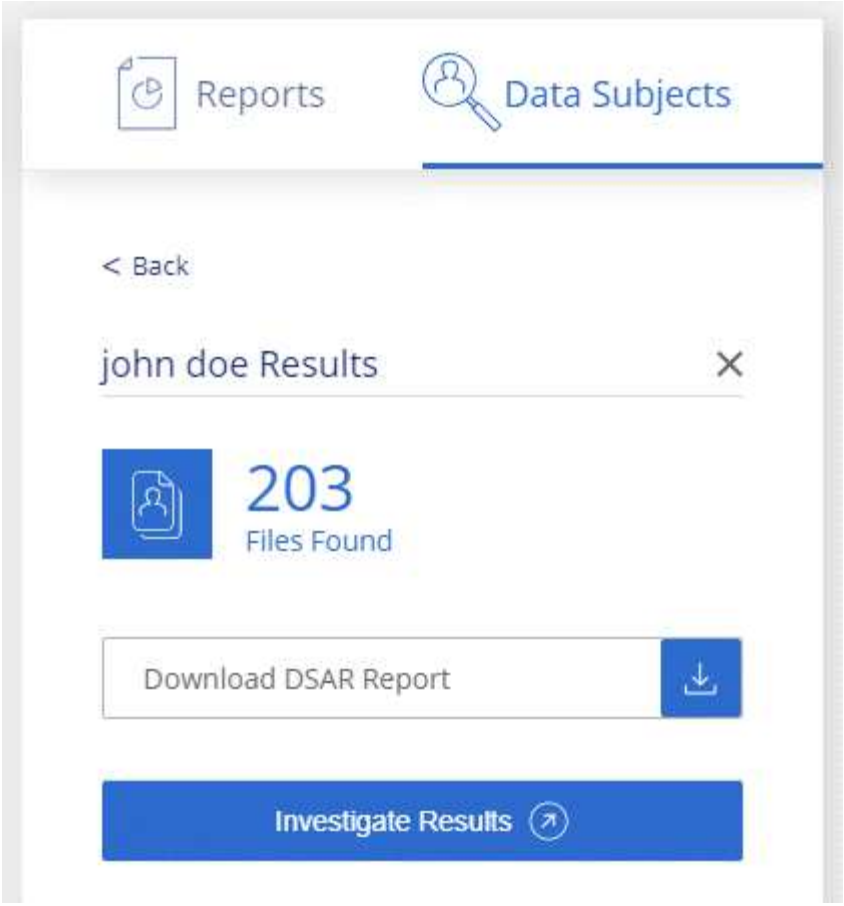
Seul l'anglais est pris en charge lors de la recherche des noms des sujets de données. La prise en charge d'autres langues sera ajoutée ultérieurement.

La recherche de sujet de données n'est pas prise en charge actuellement dans les bases de données.

Étapes

1. En haut de Cloud Manager, cliquez sur **Cloud Compliance**.
2. Cliquez sur **sujets de données**.
3. Recherchez le nom complet ou l'identifiant connu du sujet de données.

   Voici un exemple qui montre une recherche du nom *john Doe*:



4. Choisissez l'une des options disponibles :
   - **Télécharger le rapport DSAR** : réponse officielle à la demande d'accès que vous pouvez envoyer au sujet des données. Ce rapport contient des informations générées automatiquement en fonction des données que Cloud Compliance trouve sur le sujet des données et qui sont conçues pour être utilisées comme modèle. Vous devez remplir le formulaire et le revoir en interne avant de l'envoyer au sujet des données.
   - **Étudier les résultats** : une page qui vous permet d'examiner les données en recherchant, en triant, en développant les détails d'un fichier spécifique et en téléchargeant la liste de fichiers.

   S'il y a plus de 10,000 résultats, seuls les 10,000 premiers apparaissent dans la liste de fichiers.

Désactivation de Cloud Compliance

Si nécessaire, vous pouvez empêcher Cloud Compliance de scanner un ou plusieurs environnements de travail ou bases de données. Vous pouvez également supprimer l'instance Cloud Compliance si vous ne souhaitez plus utiliser Cloud Compliance avec vos environnements de travail.

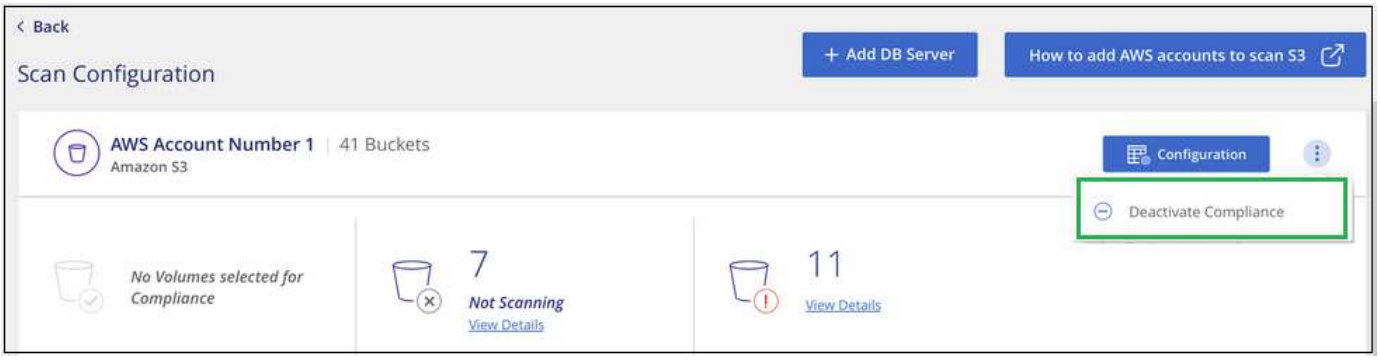
Désactivation des analyses de conformité pour un environnement de travail

Lorsque vous désactivez les analyses, Cloud Compliance ne analyse plus les données du système et supprime les informations de conformité indexées de l'instance Cloud Compliance (les données de

l'environnement de travail ou de la base de données elle-même ne sont pas supprimées).

Étapes

Dans la page *Scan Configuration*, cliquez sur le bouton Dans la ligne de l'environnement de travail, puis cliquez sur **Désactiver la conformité**.



Vous pouvez également désactiver les analyses de conformité pour un environnement de travail à partir du panneau Services lorsque vous sélectionnez l'environnement de travail.

Suppression de l'instance Cloud Compliance

Vous pouvez supprimer l'instance Cloud Compliance si vous ne souhaitez plus utiliser Cloud Compliance. La suppression de l'instance supprime également les disques associés où résident les données indexées.

Étape

1. Accédez à la console de votre fournisseur cloud et supprimez l'instance Cloud Compliance.

   L'instance s'appelle *CloudCompliance* avec un hachage (UUID) généré concaténé. Par exemple : *CloudCompliance-16bb6564-38ad-4080-9a92-36f5fd2f71c7*

Questions les plus fréquemment posées concernant Cloud Compliance

Cette FAQ peut vous aider si vous cherchez simplement une réponse rapide à une question.

En quoi consiste la conformité cloud ?

Cloud Compliance est une offre cloud qui utilise la technologie d'intelligence artificielle (IA) pour aider les entreprises à comprendre le contexte des données et à identifier les données sensibles dans l'ensemble des configurations Azure NetApp Files, les systèmes Cloud Volumes ONTAP hébergés sur AWS ou Azure, des compartiments Amazon S3 et des bases de données.

Cloud Compliance fournit des paramètres prédéfinis (par exemple, des types d'informations sensibles et des catégories) pour respecter les nouvelles réglementations en matière de conformité des données en matière de confidentialité et de sensibilité des données, notamment le RGPD, la loi CCPA, HIPAA.

Pourquoi utiliser Cloud Compliance ?

Avec Cloud Compliance, vous pouvez :

- Respectez les réglementations en matière de conformité et de confidentialité des données.
- Respectez les règles de conservation des données.
- Localiser et créer facilement des rapports sur des données spécifiques en réponse à des sujets de données, conformément aux exigences du RGPD, de la loi CCPA, de l'HIPAA et d'autres réglementations en matière de confidentialité des données.

Quelles sont les utilisations courantes de Cloud Compliance ?

- Identifier les informations à caractère personnel
- Identifier une vaste portée des informations sensibles, conformément aux réglementations du RGPD et de la loi CCPA sur la confidentialité.
- Respectez les nouvelles réglementations sur la confidentialité des données, ainsi que celles à venir.

"Pour en savoir plus sur les utilisations de Cloud Compliance".

Quels types de données peuvent être analysés avec Cloud Compliance ?

Cloud Compliance prend en charge l'analyse des données non structurées via les protocoles NFS et CIFS gérés par Cloud Volumes ONTAP et Azure NetApp Files. Cloud Compliance permet également d'analyser les données stockées dans des compartiments Amazon S3.

En outre, Cloud Compliance peut analyser les bases de données qui se trouvent n'importe où, ce qui n'est pas nécessaire de les gérer par Cloud Manager.

"Découvrez le fonctionnement des acquisitions".

Quels sont les fournisseurs de cloud pris en charge ?

Cloud Compliance fonctionne avec Cloud Manager et prend actuellement en charge AWS et Azure. Votre entreprise peut ainsi bénéficier d'une visibilité unifiée sur la confidentialité des données entre les différents fournisseurs de cloud. La prise en charge de Google Cloud Platform (GCP) sera bientôt ajoutée.

Comment accéder à Cloud Compliance ?

Cloud Compliance est exécuté et géré via Cloud Manager. Vous pouvez accéder aux fonctionnalités Cloud Compliance à partir de l'onglet **Compliance** de Cloud Manager.

Comment fonctionne Cloud Compliance ?

Cloud Compliance déploie une autre couche d'intelligence artificielle avec votre système Cloud Manager et vos systèmes de stockage. Il analyse ensuite les données sur des volumes, des compartiments, des bases de données et indexe les informations exploitables qui se trouvent.

"Découvrez le fonctionnement de Cloud Compliance".

Combien coûte Cloud Compliance ?

Le coût d'utilisation de la conformité dans le cloud dépend de la quantité de données à analyser. Les 1 premiers To de données analysés par Cloud Compliance dans un espace de travail Cloud Manager sont gratuits. Un abonnement à AWS ou Azure Marketplace est nécessaire pour poursuivre l'analyse des données après ce point. Voir "tarifs" pour plus d'informations.

À quelle fréquence Cloud Compliance analyse-t-il mes données ?

Les données évoluent fréquemment. Cloud Compliance les analyse en continu, sans affecter les données. Alors que l'analyse initiale de vos données peut prendre plus de temps, les analyses suivantes ne scannent que les modifications incrémentielles, ce qui réduit les temps d'analyse du système.

"Découvrez le fonctionnement des acquisitions".

Cloud Compliance offre-t-il des rapports ?

Oui. Les informations communiquées par Cloud Compliance peuvent s'avérer utiles pour les autres parties prenantes dans votre entreprise. Nous vous permettons de générer des rapports pour partager les informations exploitables.

Les rapports suivants sont disponibles pour Cloud Compliance :

Rapport d'évaluation des risques pour la confidentialité
: Fournit des informations sur la confidentialité à partir de vos données et un score de risque lié à la confidentialité. "En savoir plus >>".

Rapport de demande d'accès au sujet des données
: Vous permet d'extraire un rapport de tous les fichiers contenant des informations concernant le nom spécifique ou l'identifiant personnel d'un sujet de données. "En savoir plus >>".

Rapport PCI DSS
: Vous aide à identifier la distribution des informations de carte de crédit dans vos dossiers. "En savoir plus >>".

Rapport HIPAA
: Vous aide à identifier la distribution de l'information sur la santé dans vos dossiers. "En savoir plus >>".

Rapports sur un type d'information spécifique
: Des rapports sont disponibles, incluant des détails sur les fichiers identifiés qui contiennent des données personnelles et des données personnelles sensibles. Vous pouvez également voir les fichiers dérépartis par catégorie et par type de fichier. "En savoir plus >>".

Quel type d'instance ou de machine virtuelle est requis pour Cloud Compliance ?

- Dans Azure, Cloud Compliance s'exécute sur une machine virtuelle standard_D16s_v3 avec un disque de 512 Go.
- Dans AWS, Cloud Compliance s'exécute sur une instance m5.4xlarge avec un disque GP2 de 500 Go.

  Dans les régions où m5.4xlarge n'est pas disponible, Cloud Compliance s'exécute sur une instance m4.4xlarge.

La modification ou le redimensionnement du type d'instance/de VM n'est pas prise en charge. Vous devez utiliser la taille par défaut fournie.

"Découvrez le fonctionnement de Cloud Compliance".

Les performances d'acquisition varient-t-elles ?

Les performances d'analyse peuvent varier en fonction de la bande passante réseau et de la taille moyenne des fichiers dans votre environnement cloud.

Quels types de fichiers sont pris en charge ?

Cloud Compliance analyse les informations relatives aux catégories et aux métadonnées de tous les fichiers, et affiche tous les types de fichiers dans la section types de fichiers du tableau de bord.

Lorsque Cloud Compliance détecte des informations à caractère personnel (PII) ou lorsqu'il effectue une recherche DSAR, seuls les formats de fichier suivants sont pris en charge : .PDF, .DOCX, .DOC, .PPTX, .XLS, .XLSX, .CSV, .TXT, .RTF ET .JSON.

Comment activer Cloud Compliance ?

Il vous faut tout d'abord déployer une instance de Cloud Compliance dans Cloud Manager. Une fois l'instance en cours d'exécution, vous pouvez l'activer sur les environnements de travail et les bases de données existants à partir de l'onglet **Compliance** ou en sélectionnant un environnement de travail spécifique.

"Découvrez comment démarrer".

L'activation de Cloud Compliance entraîne une analyse initiale immédiate. Les résultats de conformité s'affichent peu de temps après.

Comment désactiver Cloud Compliance ?

Vous pouvez désactiver Cloud Compliance à partir de la page Working Environments après avoir sélectionné un environnement de travail individuel.

"En savoir plus >>".

Pour supprimer complètement l'instance Cloud Compliance, vous pouvez supprimer manuellement l'instance Cloud Compliance du portail de votre fournisseur cloud.

Que se passe-t-il si le Tiering des données est activé sur Cloud Volumes ONTAP ?

Vous pouvez activer Cloud Compliance sur un système Cloud Volumes ONTAP qui transfère les données inactives vers un stockage objet. Si le Tiering est activé, Cloud Compliance analyse toutes les données qui se trouvent sur des disques et les données inactives envoyées vers le stockage objet.

L'analyse de conformité ne chauffe pas les données inactives : elles restent inactives et hiérarchisées vers le stockage objet.

Puis-je utiliser Cloud Compliance pour analyser le stockage ONTAP sur site ?

La numérisation des données directement à partir d'un environnement de travail ONTAP sur site n'est pas prise en charge. Mais vous pouvez analyser vos données ONTAP sur site en répliquant les données NFS ou CIFS sur un environnement de travail Cloud Volumes ONTAP puis en activant la conformité sur ces volumes. Nous prévoyons d'assurer la conformité cloud avec d'autres offres cloud telles que Cloud Volumes Service.

"En savoir plus >>".

Cloud Compliance peut-il envoyer des notifications à mon entreprise ?

Non, mais vous pouvez télécharger des rapports de statut que vous pouvez partager en interne dans votre entreprise.

Puis-je personnaliser le service en fonction des besoins de mon entreprise ?

Cloud Compliance vous fournit des informations exploitables prêtes à l'emploi pour vos données. Ces informations peuvent être extraites et utilisées en fonction des besoins de votre entreprise.

Est-il possible de limiter les informations de conformité cloud à des utilisateurs spécifiques ?

Oui, Cloud Compliance est entièrement intégré avec Cloud Manager. Les utilisateurs de Cloud Manager ne peuvent voir que les informations relatives aux environnements de travail qu'ils peuvent afficher en fonction de leurs privilèges d'espace de travail.

En outre, si vous souhaitez autoriser certains utilisateurs à simplement afficher les résultats d'analyse de Cloud Compliance sans pouvoir gérer les paramètres Cloud Compliance, vous pouvez attribuer à ces utilisateurs le rôle *Cloud Compliance Viewer*.

"En savoir plus >>".

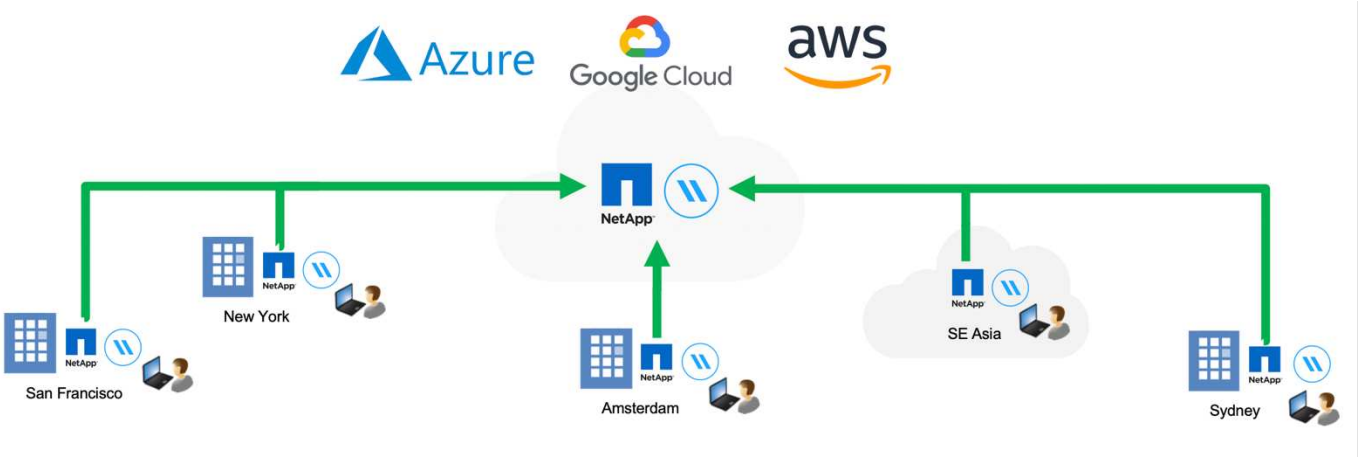
Activez le partage global des fichiers en temps réel

En savoir plus sur Global File cache

NetApp Global File cache vous permet de consolider les silos de serveurs de fichiers distribués en un seul environnement de stockage global cohérent dans le cloud public. Cela crée un système de fichiers accessible partout dans le cloud que tous les emplacements distants peuvent utiliser comme s'ils étaient locaux.

Présentation

La mise en œuvre de Global File cache engendre une empreinte du stockage unique et centralisée, par rapport à une architecture de stockage distribuée qui nécessite une gestion des données locales, des sauvegardes, une gestion de la sécurité, un stockage et une infrastructure réparties sur chaque site.



Caractéristiques

Global File cache offre les fonctionnalités suivantes :

- Consolidez et centralisez vos données dans le cloud public, et exploitez l'évolutivité et les performances de vos solutions de stockage
- Créez un seul ensemble de données pour les utilisateurs du monde entier et exploitez la mise en cache intelligente des fichiers afin d'améliorer l'accès aux données, la collaboration et les performances
- Utilisez un cache autogéré et autogéré et éliminez les copies et les sauvegardes complètes des données. Utilisation de la mise en cache locale des fichiers pour les données actives et réduction des coûts de stockage
- Accès transparent depuis les succursales via un espace de noms global avec verrouillage centralisé des fichiers en temps réel

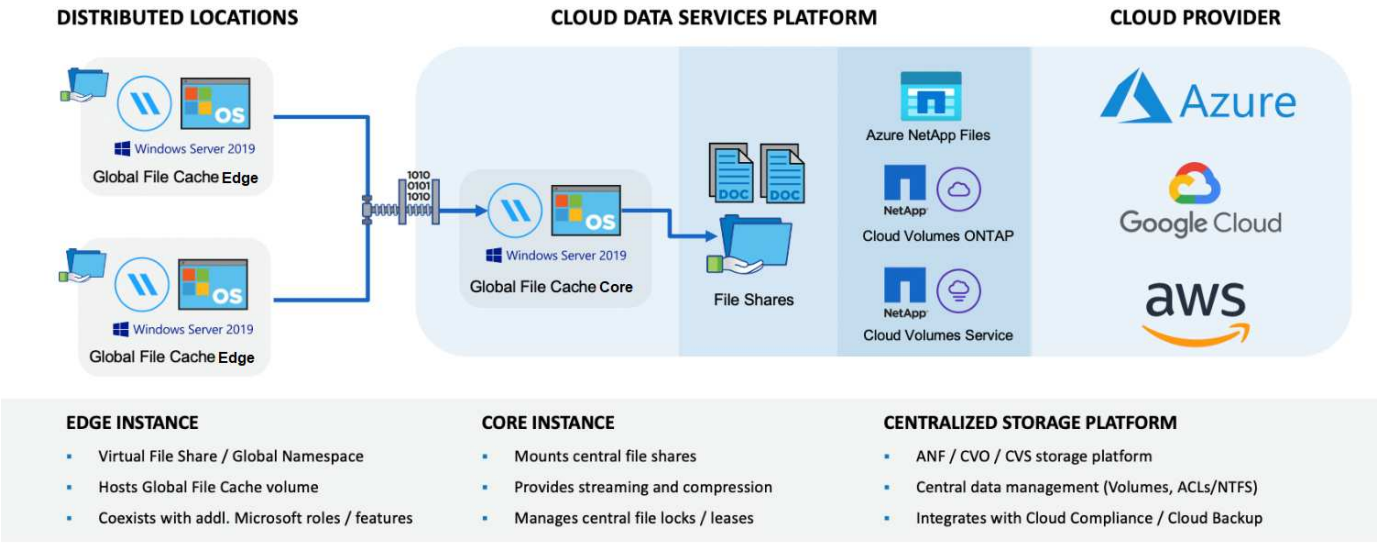
En savoir plus sur les fonctionnalités de Global File cache et ses cas d'utilisation "ici".

Composants du cache de fichiers global

Global File cache comprend les composants suivants :

- Serveur global de gestion du cache des fichiers
- Cœur de cache de fichiers global
- Cache global de fichiers Edge (déployé sur vos sites distants)

L'instance principale de NetApp Global File cache est montée sur vos partages de fichiers d'entreprise hébergés sur la plateforme de stockage interne au choix (par exemple, Cloud Volumes ONTAP, Cloud Volumes Service, Et Azure NetApp Files). Cet environnement permet de centraliser et de consolider les données non structurées dans un seul ensemble de données, qu'elles résident sur une ou plusieurs plateformes de stockage dans le cloud public.



Plateformes de stockage prises en charge

Les plates-formes de stockage prises en charge pour Global File cache diffèrent selon l'option de déploiement sélectionnée.

Options de déploiement automatisé

Le cache global de fichiers est pris en charge avec les types d'environnements de travail suivants lorsqu'il est déployé à l'aide de Cloud Manager :

- Cloud Volumes ONTAP dans Azure
- Cloud Volumes ONTAP dans AWS

Cette configuration vous permet de déployer et de gérer l'intégralité du déploiement côté serveur de Global File cache, y compris le serveur de gestion Global File cache et le cache de fichiers global, depuis Cloud Manager.

Options de déploiement manuel

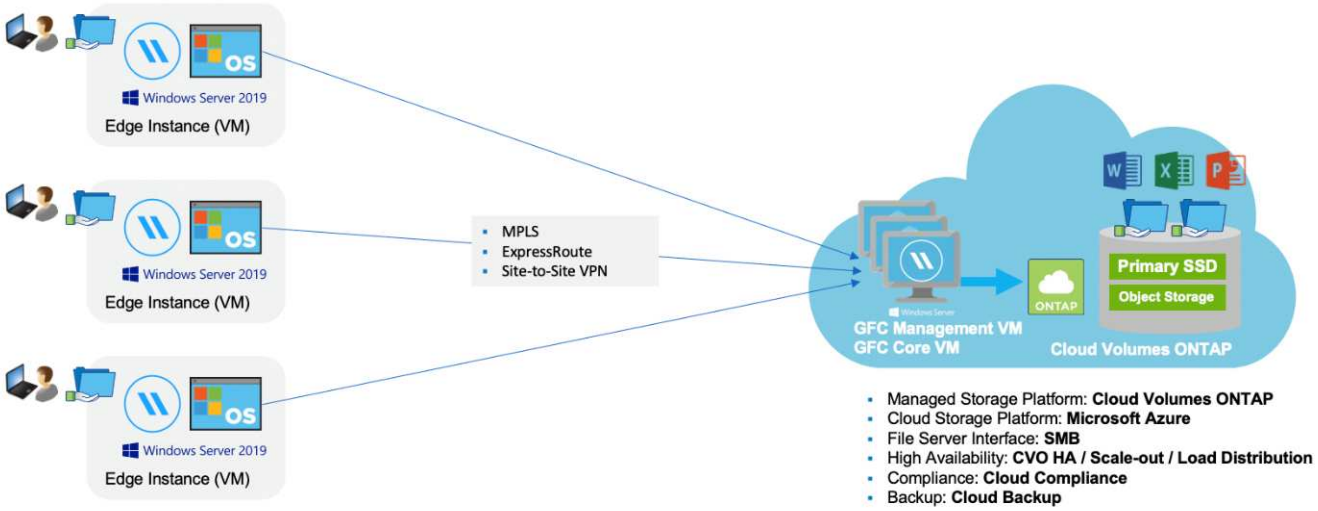
Les configurations globales de cache de fichiers sont également prises en charge avec Cloud Volumes ONTAP, Cloud Volumes Service ou Azure NetApp Files installés sur une infrastructure de stockage de cloud

public Microsoft Azure, Google Cloud Platform ou Amazon Web Services. Les solutions sur site sont également disponibles sur les plateformes NetApp AFF et FAS. Dans ces installations, les composants côté serveur Global File cache doivent être configurés et déployés manuellement, et non à l'aide de Cloud Manager.

Voir la "Guide de l'utilisateur NetApp Global File cache" pour plus d'informations.

Fonctionnement de Global File cache

Global File cache crée une structure logicielle qui met en cache les jeux de données actives dans les bureaux distants à travers le monde. Par conséquent, les utilisateurs de l'entreprise bénéficient d'un accès transparent aux données et de performances optimales à l'échelle mondiale.



La topologie référencée dans cet exemple est un modèle en étoile dans lequel le réseau de bureaux distants/emplacements accède à un ensemble commun de données dans le cloud. Les points clés de cet exemple sont les suivants :

- Magasin de données centralisé :
  - Une plateforme de stockage de cloud public d'entreprise, telle qu'Cloud Volumes ONTAP
- Structure globale de cache de fichiers :
  - Extension du magasin de données central aux sites distants
  - Instance principale du cache de fichiers global, montage sur les partages de fichiers d'entreprise (SMB).
  - Instances globales File cache Edge s'exécutant dans chaque emplacement distant.
  - Présente un partage de fichiers virtuel dans chaque emplacement distant permettant l'accès aux données centrales.
  - Héberge le cache de fichiers intelligent sur un volume NTFS personnalisé (`D:\`).
- Configuration réseau :
  - Connectivité MPLS (Multiprotocol Label Switching), ExpressRoute ou VPN
- Intégration avec les services de domaine Active Directory du client.
- Espace de noms DFS pour l'utilisation d'un espace de noms global (recommandé).

Le coût

Le coût d'utilisation de Global File cache dépend du type d'installation que vous avez choisi.

- Toutes les installations nécessitent de déployer un ou plusieurs volumes dans le cloud (Cloud Volumes ONTAP, Cloud Volumes Service ou Azure NetApp Files). Ce qui entraîne des frais pour le fournisseur cloud sélectionné.
- Toutes les installations nécessitent également de déployer au moins deux machines virtuelles dans le cloud. Ce qui entraîne des frais pour le fournisseur cloud sélectionné.
    - Serveur global de gestion du cache des fichiers :

      Dans Azure, cette opération s'exécute sur une machine virtuelle D2S_V3 ou équivalent (2 vCPU/8 Go de RAM) avec 127 Go de SSD premium

      Dans AWS, s'exécute sur une instance m4.large ou équivalente (2 vCPU/8 Go de RAM) avec des disques SSD à usage général de 127 Go
    - Cœur de cache de fichiers global :

      Dans Azure, cette opération s'exécute sur une machine virtuelle D4S_V3 ou équivalente (4 vCPU/16 Go de RAM) avec un SSD premium de 127 Go

    Dans AWS, cette instance s'exécute sur une instance m4.XLarge ou équivalent (4 vCPU/16 Go de RAM) avec un SSD générique de 127 Go
- Lorsqu'elles sont installées avec Cloud Volumes ONTAP dans Azure ou AWS (les configurations prises en charge entièrement déployées via Cloud Manager), les clients ont des frais de 3,000 $ par site (pour chaque instance Global File cache Edge), par an.
- Lorsqu'ils sont installés à l'aide des options de déploiement manuel, le prix est différent. Pour obtenir une estimation de haut niveau des coûts, voir "Calcul de votre potentiel d'économies" Vous pouvez également consulter votre ingénieur solutions Global File cache pour discuter des meilleures options de déploiement pour votre entreprise.

Licences

Global File cache inclut un serveur de gestion des licences (LMS) basé sur logiciel qui vous permet de consolider votre gestion des licences et de déployer des licences vers toutes les instances Core et Edge à l'aide d'un mécanisme automatisé.

Lorsque vous déployez votre première instance Core dans le data Center ou le cloud, vous pouvez choisir de désigner cette instance comme LMS pour votre organisation. Cette instance LMS est configurée une fois, se connecte au service d'abonnement (via HTTPS) et valide votre abonnement à l'aide de l'ID client fourni par notre service de support/opérations au moment de l'inscription. Après avoir fait cette désignation, vous associez vos instances Edge au LMS en fournissant votre ID client et l'adresse IP de l'instance LMS.

Lorsque vous achetez des licences Edge supplémentaires ou que vous renouvelez votre abonnement, notre service support/opérations met à jour les informations de licence, par exemple le nombre de sites ou la date de fin de l'abonnement. Une fois que le LMS a interrogé le service d'abonnement, les détails de la licence sont automatiquement mis à jour sur l'instance LMS et s'appliquent à vos instances de réseau de réseau central et Edge.

Voir la "Guide de l'utilisateur NetApp Global File cache" pour plus d'informations sur les licences.

Limites

- La version de Global File cache prise en charge dans Cloud Manager nécessite que la plateforme de stockage interne utilisée comme stockage central soit un environnement de travail dans lequel vous avez déployé un seul nœud Cloud Volumes ONTAP ou une paire haute disponibilité dans Azure ou AWS.

  Les autres plateformes de stockage et autres fournisseurs de cloud ne sont pas pris en charge à l'heure actuelle via Cloud Manager, mais peuvent être déployés via des procédures de déploiement héritées.

Ces autres configurations, par exemple le cache de fichiers global avec Cloud Volumes ONTAP, Cloud Volumes Service et Azure NetApp Files sur Microsoft Azure, Google Cloud et AWS, continuent à être prises en charge par les procédures existantes. Voir "Présentation et intégration de Global File cache" pour plus d'informations.

Avant de commencer à déployer Global File cache

Avant de commencer à déployer Global File cache dans le cloud et dans vos bureaux distants, vous devez connaître de nombreuses exigences.

Considérations relatives à la conception du noyau de File cache global

Selon vos besoins, vous devrez peut-être déployer une ou plusieurs instances de base Global File cache pour créer Global File cache Fabric. L'instance principale est conçue pour servir de point de défaillance du trafic entre vos instances globales de cache de fichiers Edge distribuées et les ressources du serveur de fichiers du centre de données, par exemple les partages de fichiers, les dossiers et les fichiers.

Lors de la conception de votre déploiement Global File cache, vous devez déterminer ce qui convient à votre environnement en termes d'échelle, de disponibilité des ressources et de redondance. Global File cache Core peut être déployé de plusieurs manières :

- Instance autonome Fibre Channel Core
- Conception distribuée Fibre Channel Core Load (mise en veille à froid)

Voir Instructions de dimensionnement Pour comprendre le nombre maximal d'instances Edge et le nombre total d'utilisateurs que chaque configuration peut prendre en charge :

Consultez votre ingénieur solutions Global File cache pour connaître les meilleures options de déploiement pour votre entreprise.

Instructions de dimensionnement

Il y a quelques ratios de dimensionnement que vous devez garder à l'esprit lors de la configuration du système initial. Vous devez revoir ces ratios après l'accumulation de certains historiques d'utilisation pour vous assurer que vous utilisez le système de façon optimale. À savoir :

- Rapport des arêtes/cœurs du cache de fichiers global
- Utilisateurs distribués/ratio Edge de cache de fichiers global
- Utilisateurs distribués/ratio central de cache de fichier global

Nombre d'instances Edge par instance de noyau

Nos instructions recommandent jusqu'à 10 instances Edge par instance Global File cache Core, avec un maximum de 20 arêtes par instance Global File cache Core. Cette opération dépend dans une grande mesure du type et de la taille moyenne des fichiers de la charge de travail la plus courante. Dans certains cas, avec des charges de travail plus courantes, vous pouvez ajouter d'autres instances Edge par cœur. Dans ce cas, contactez le support NetApp pour dimensionner correctement le nombre d'instances Edge et Core en fonction des types et de la taille des jeux de fichiers.

Vous pouvez exploiter plusieurs instances Global File cache Edge et Core simultanément pour faire évoluer votre infrastructure en fonction des besoins.

Nombre d'utilisateurs simultanés par instance Edge

Global File cache Edge gère l'élévation considérable en termes d'algorithmes de mise en cache et de différences au niveau des fichiers. Une seule instance Global File cache Edge peut accueillir jusqu'à 400 utilisateurs par instance physique Edge dédiée, et jusqu'à 200 utilisateurs pour les déploiements virtuels dédiés. Cette opération dépend dans une grande mesure du type et de la taille moyenne des fichiers de la charge de travail la plus courante. Pour les types de fichiers collaboratifs plus importants, guidez jusqu'à 50 % du nombre maximal d'utilisateurs par limite inférieure de cache de fichier global (selon le déploiement physique ou virtuel). Pour les éléments Office les plus courants avec une taille de fichier moyenne < 1 Mo, guide vers la limite supérieure de 100 % d'utilisateurs par Global File cache Edge (selon le déploiement physique ou virtuel).

Global File cache Edge détecte s'il s'exécute sur une instance virtuelle ou physique et limite le nombre de connexions SMB au partage de fichiers virtuel local à un maximum de 200 ou 400 connexions simultanées.

Nombre d'utilisateurs simultanés par instance Core

L'instance principale de cache de fichiers global est extrêmement évolutive, avec un nombre d'utilisateurs simultanés recommandé de 3,000 utilisateurs par cœur. Cette opération dépend dans une grande mesure du type et de la taille moyenne des fichiers de la charge de travail la plus courante.

Consultez votre ingénieur solutions Global File cache pour connaître les meilleures options de déploiement pour votre entreprise.

Prérequis

Les conditions préalables décrites dans cette section concernent les composants installés dans le cloud : Global File cache Management Server et Global File cache Core.

Les prérequis Global File cache Edge sont décrits "ici".

Instance Cloud Manager

Lorsque vous utilisez Cloud Volumes ONTAP pour Azure comme plateforme de stockage, assurez-vous que Cloud Manager dispose des autorisations nécessaires, comme indiqué au plus récent "Cloud Manager policy pour Azure".

Par défaut, toutes les autorisations requises seront attribuées aux instances nouvellement créées. Si vous avez déployé votre instance avant la version 3.8.7 (3 août 2020), vous devrez ajouter ces éléments.

```
"Microsoft.Resources/deployments/operationStatuses/read",
"Microsoft.Insights/Metrics/Read",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/virtualMachines/extensions/delete",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/delete",
"Microsoft.Resources/deployments/delete",
```

Plateforme de stockage (volumes)

La plateforme de stockage interne – dans ce cas, votre instance Cloud Volumes ONTAP déployée – doit présenter les partages de fichiers SMB. Tout partage qui sera exposé via Global File cache doit permettre au groupe Everyone de contrôler entièrement au niveau du partage, tout en limitant les autorisations par le biais des autorisations NTFS.

Si vous n'avez pas configuré au moins un partage de fichiers SMB sur l'instance Cloud Volumes ONTAP, vous devez disposer des informations suivantes pour pouvoir configurer ces informations lors de l'installation :

- Nom de domaine Active Directory, adresse IP du serveur de noms, informations d'identification d'administrateur Active Directory.
- Le nom et la taille du volume que vous souhaitez créer, le nom de l'agrégat sur lequel le volume sera créé, et le nom du partage.

Nous vous recommandons d'augmenter ce volume suffisamment pour prendre en charge le jeu de données total de l'application, ainsi que la capacité à évoluer en conséquence en fonction de la croissance du jeu de données. Si l'environnement de travail compte plusieurs agrégats, reportez-vous à "Gestion des agrégats existants" pour déterminer quel agrégat dispose de l'espace le plus disponible pour le nouveau volume.

Serveur global de gestion du cache des fichiers

Ce serveur Global File cache Management requiert un accès externe via HTTPS (port TCP 443) pour se connecter au service d'abonnement du fournisseur cloud et pour accéder aux URL suivantes :

- "https://talonazuremicroservices.azurewebsites.net"
- "https://talonlicensing.table.core.windows.net"

Ce port doit être exclu de tout périphérique d'optimisation WAN ou de toute stratégie de restriction de pare-feu pour que le logiciel Global File cache fonctionne correctement.

Le serveur de gestion du cache de fichiers global nécessite également un nom NetBIOS unique (géographique) pour l'instance (par exemple, Fibre Channel-MS1).

Un serveur de gestion peut prendre en charge plusieurs instances globales de base de cache de fichiers déployées dans différents environnements de travail. Lorsqu'il est déployé depuis Cloud Manager, chaque environnement de travail dispose de son propre système de stockage back-end et ne devrait pas contenir les mêmes données.

Cœur de cache de fichiers global

Ce noyau de cache de fichiers global écoute la plage de ports TCP 6618-6630. En fonction de votre configuration de pare-feu ou de Groupe de sécurité réseau (NSG), il se peut que vous deviez autoriser explicitement l'accès à ces ports via des règles de port entrant. Ces ports doivent également être exclus de tout périphérique d'optimisation WAN ou de toute stratégie de restriction de pare-feu pour que le logiciel Global File cache fonctionne correctement.

La configuration requise pour le module Global File cache est la suivante :

- Un nom NetBIOS unique (géographique) pour l'instance (par exemple, le réseau de stockage/réseau/réseau/réseau/réseau/réseau/réseau/réseau/réseau/réseau/réseau/
- Nom de domaine Active Directory
  - Les instances de cache de fichiers global doivent être jointes à votre domaine Active Directory.
  - Les instances de cache de fichiers global doivent être gérées dans une unité organisationnelle spécifique (ou) du cache de fichiers global et exclues des GPO de l'entreprise hérités.
- Compte de service. Les services de cette base de cache de fichiers globale fonctionnent comme un compte utilisateur de domaine spécifique. Ce compte, également appelé compte de service, doit disposer des privilèges suivants sur chacun des serveurs SMB qui seront associés à l'instance principale de cache de fichiers global :
  - Le compte de service provisionné doit être un utilisateur de domaine.

Selon le niveau des restrictions et des stratégies de groupe dans l'environnement réseau, ce compte peut nécessiter des privilèges d'administrateur de domaine.

- Le service informatique doit disposer des privilèges « Exécuter en tant que service ».
- Le mot de passe doit être défini sur « jamais expirer ».
- L'option de compte « l'utilisateur doit modifier le mot de passe lors de la prochaine connexion » doit ÊTRE DÉSACTIVÉE (décochée).
- Il doit être membre du groupe des opérateurs de sauvegarde intégré au serveur de fichiers back-end (cette option est automatiquement activée lorsqu'elle est déployée via Cloud Manager).

Serveur de gestion des licences

- Le serveur de gestion des licences de cache de fichiers global (LMS) doit être configuré sur une édition Microsoft Windows Server 2016 Standard ou Datacenter ou Windows Server 2019 Standard ou Datacenter, de préférence sur l'instance Global File cache Core du datacenter ou du Cloud.
- Si vous avez besoin d'une instance LMS Global File cache distincte, vous devez installer le dernier package d'installation du logiciel Global File cache sur une instance Microsoft Windows Server vierge.
- L'instance LMS doit pouvoir se connecter au service d'abonnement (services Azure / Internet public) via HTTPS (port TCP 443).
- Les instances Core et Edge doivent se connecter à l'instance LMS à l'aide du protocole HTTPS (port TCP 443).

Mise en réseau

- Pare-feu : les ports TCP doivent être autorisés entre les instances Global File cache Edge et Core.
- Ports TCP Global File cache : 443 (HTTPS), 6618–6630.
- Les périphériques d'optimisation réseau (tels que Riverbed Steelhead) doivent être configurés pour passer

par les ports spécifiques à Global File cache (TCP 6618-6630).

Pour commencer

Cloud Manager vous permet de déployer le serveur de gestion du cache global des fichiers et le logiciel Global File cache Core dans l'environnement de travail.

Activation du cache global de fichiers à l'aide de Cloud Manager

Dans cette configuration, vous déployez le serveur de gestion du cache de fichiers global et le noyau du cache de fichiers global dans le même environnement de travail où vous avez créé le système Cloud Volumes ONTAP à l'aide de Cloud Manager.

Regarder "vidéo" pour voir les étapes du début à la fin.

Démarrage rapide

Pour démarrer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir des informations détaillées :

Déployez Cloud Volumes ONTAP

Déployez Cloud Volumes ONTAP dans Azure ou AWS et configurez les partages de fichiers SMB. Pour plus d'informations, voir "Lancement d'Cloud Volumes ONTAP dans Azure" ou "Lancement d'Cloud Volumes ONTAP dans AWS".

Déployez le serveur Global File cache Management Server

Déployer une instance du serveur de gestion globale du cache des fichiers dans le même environnement de travail que l'instance de Cloud Volumes ONTAP.

Déployez Global File cache Core

Déployez une ou plusieurs instances de Global File cache Core dans le même environnement de travail que l'instance de Cloud Volumes ONTAP et joignez-la à votre domaine Active Directory.

Cache global des fichiers de licence

Configurez le service LMS (Global File cache License Management Server) sur une instance de base Global File cache. Pour activer votre abonnement, vous devez disposer de vos identifiants NSS ou d'un identifiant client fourni par NetApp.

Déployez les instances Global File cache Edge

Voir "Déploiement des instances Global File cache Edge" Pour déployer les instances Global File cache Edge

dans chaque emplacement distant. Cette étape n'a pas été effectuée avec Cloud Manager.

Déployez Cloud Volumes ONTAP comme plateforme de stockage

Dans la version actuelle, Global File cache prend en charge Cloud Volumes ONTAP déployé dans Azure ou AWS. Pour obtenir des informations détaillées sur les prérequis, les exigences et les instructions de déploiement, voir "Lancement d'Cloud Volumes ONTAP dans Azure" ou "Lancement d'Cloud Volumes ONTAP dans AWS".

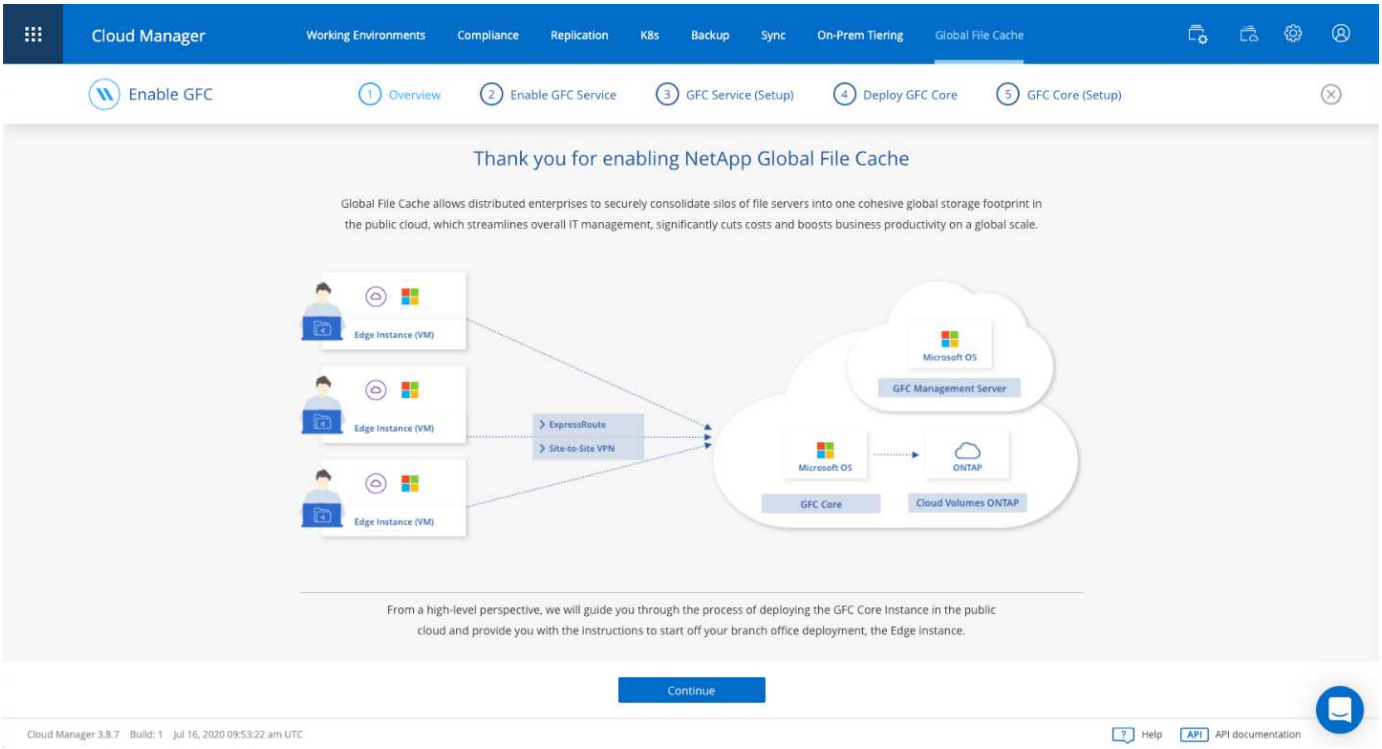
Notez la nécessité supplémentaire suivante de Global File cache :

- Vous devez configurer les partages de fichiers SMB sur l'instance de Cloud Volumes ONTAP.

  Si aucun partage de fichiers SMB n'est configuré sur l'instance, vous êtes invité à configurer les partages SMB lors de l'installation des composants Global File cache.

Activez Global File cache dans votre environnement de travail

L'assistant Global File cache vous guide dans les étapes de déploiement de l'instance Global File cache Management Server et de l'instance Global File cache Core, comme indiqué ci-dessous.



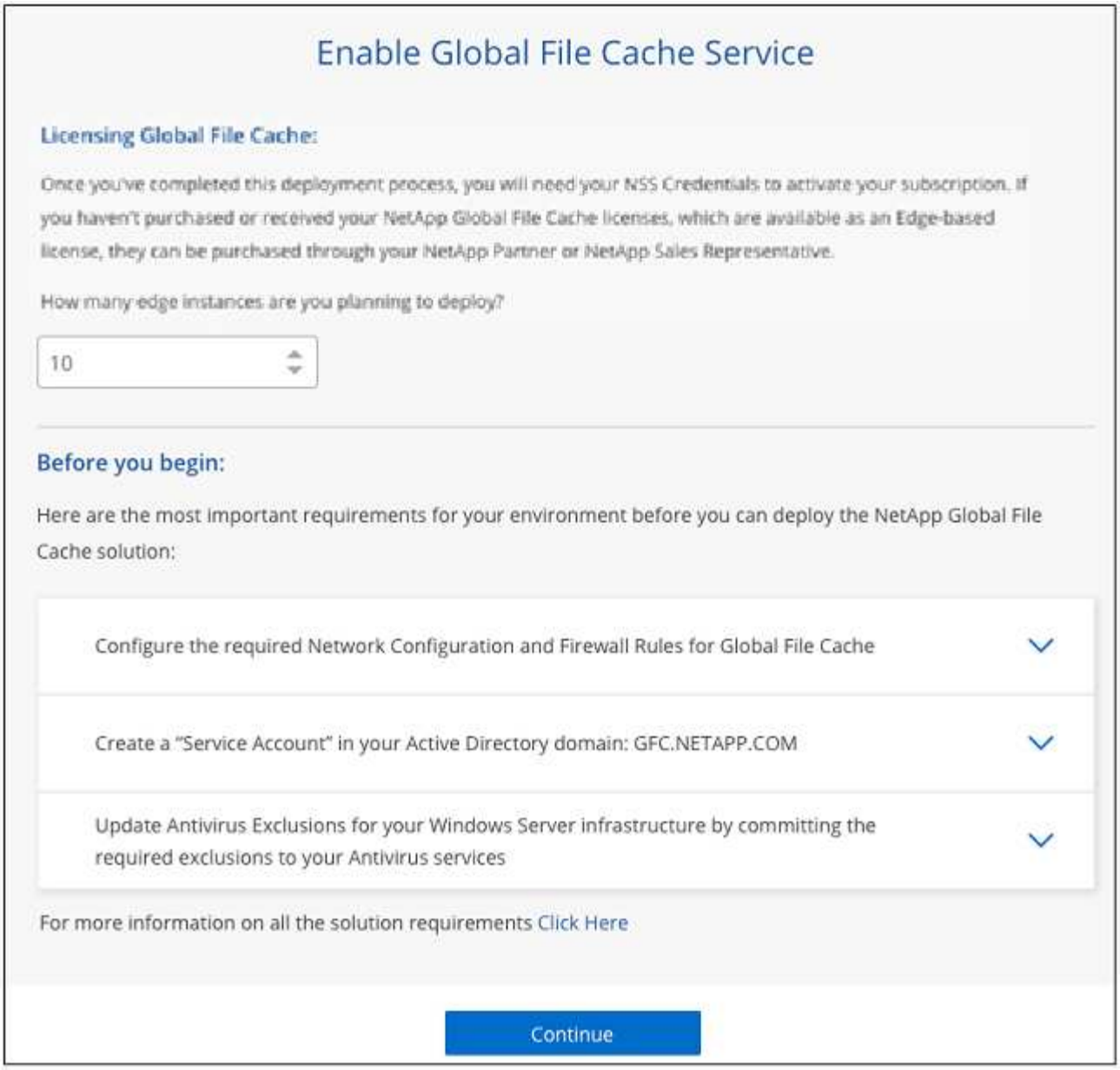
Étapes

1. Sélectionnez l'environnement de travail dans lequel vous avez déployé Cloud Volumes ONTAP.
2. Dans le panneau Services, cliquez sur *Activer le réseau de réseau sans réseau sans réseau.

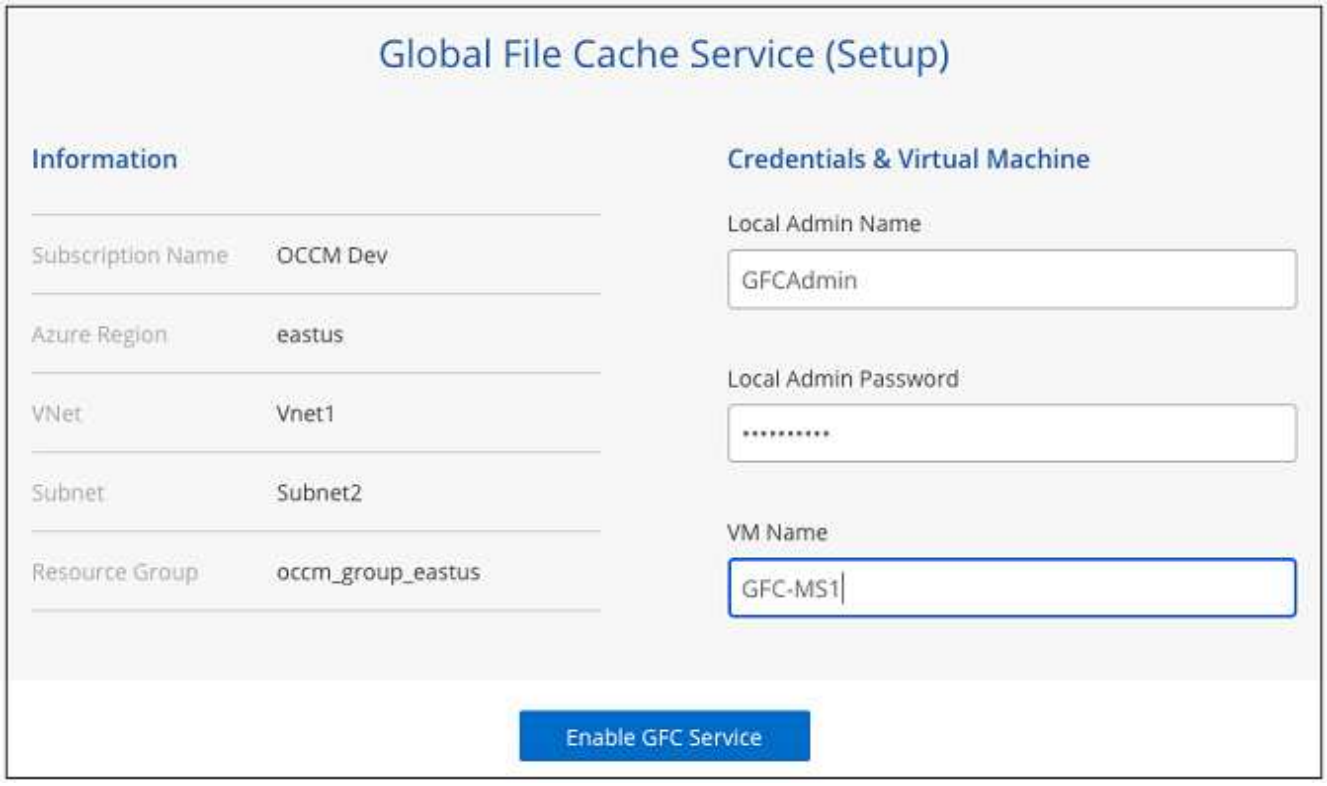
3. Lisez la page vue d'ensemble et cliquez sur **Continuer**.
4. Si aucun partage SMB n'est disponible sur l'instance Cloud Volumes ONTAP, vous êtes invité à entrer les informations du serveur SMB et du partage SMB afin de créer le partage maintenant. Pour plus de détails sur la configuration SMB, voir "Plateforme de stockage".

   Lorsque vous avez terminé, cliquez sur **Continuer** pour créer le partage SMB.

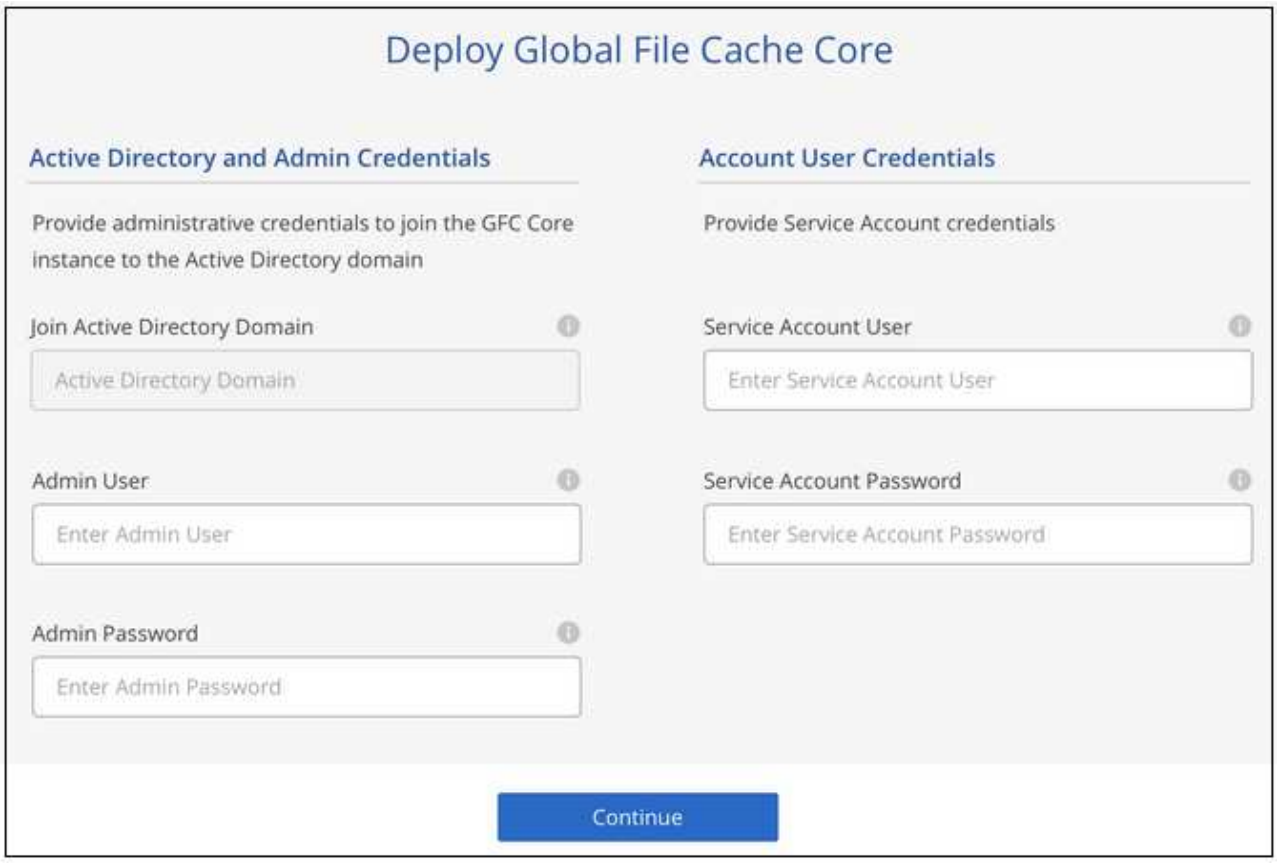
5. Sur la page Service de cache de fichiers global, entrez le nombre d'instances Global File cache Edge que vous prévoyez de déployer, puis assurez-vous que votre système répond aux exigences relatives aux règles de configuration réseau et de pare-feu, aux paramètres Active Directory et aux exclusions antivirus. Voir "Prérequis" pour en savoir plus.



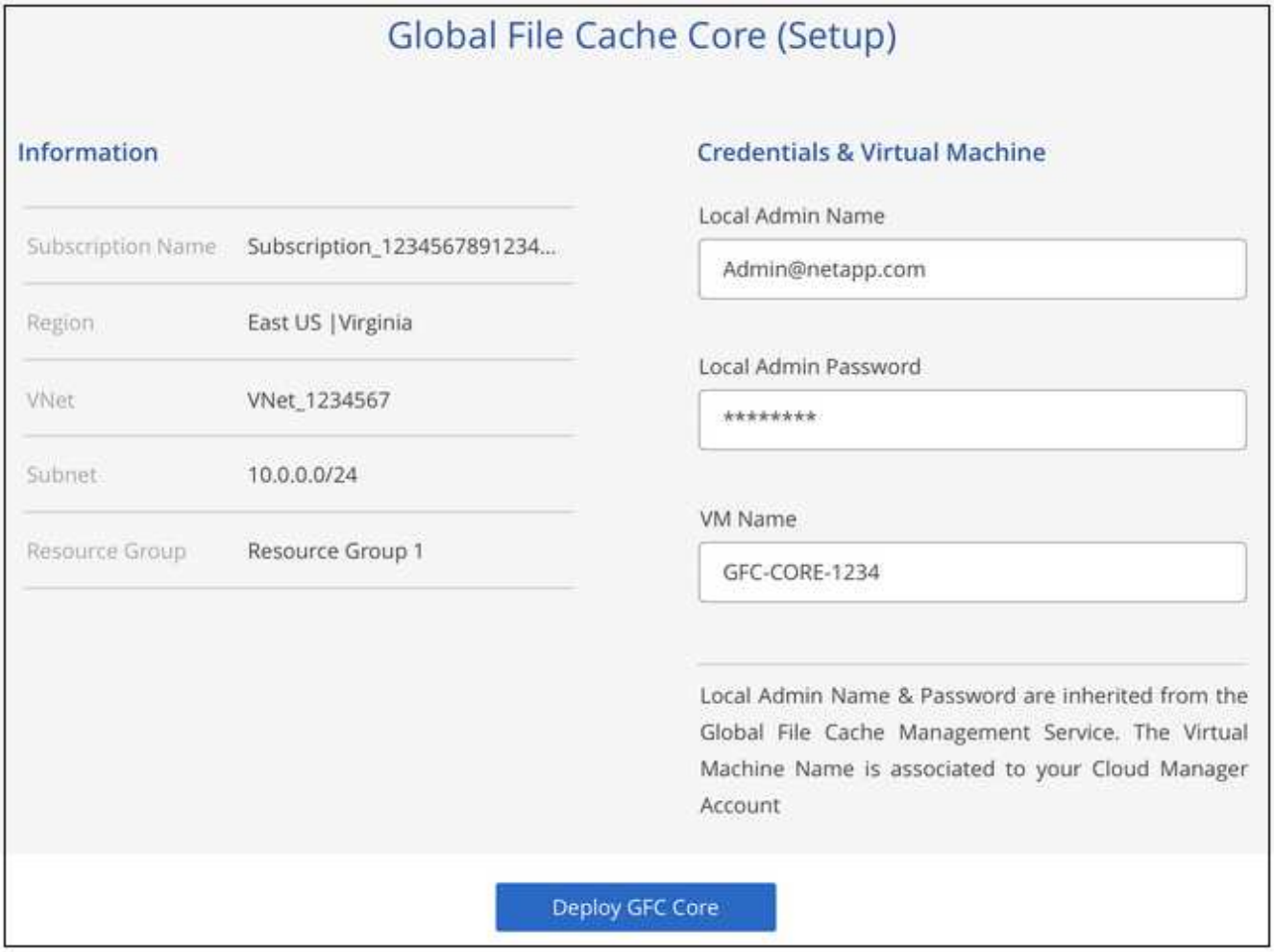
6. Après avoir vérifié que les exigences ont été respectées ou que vous disposez des informations nécessaires pour répondre à ces exigences, cliquez sur **Continuer**.
7. Entrez les informations d'identification administratives que vous utiliserez pour accéder à la VM du serveur de gestion du cache de fichiers global, puis cliquez sur **Activer le service de réseau réseau sans réseau sans réseau (GFC)**. Dans Azure, vous saisissez les identifiants sous forme de nom d'utilisateur et de mot de passe. Pour AWS, vous sélectionnez la paire de clés appropriée. Vous pouvez modifier le nom de la machine virtuelle/de l'instance si vous le souhaitez.



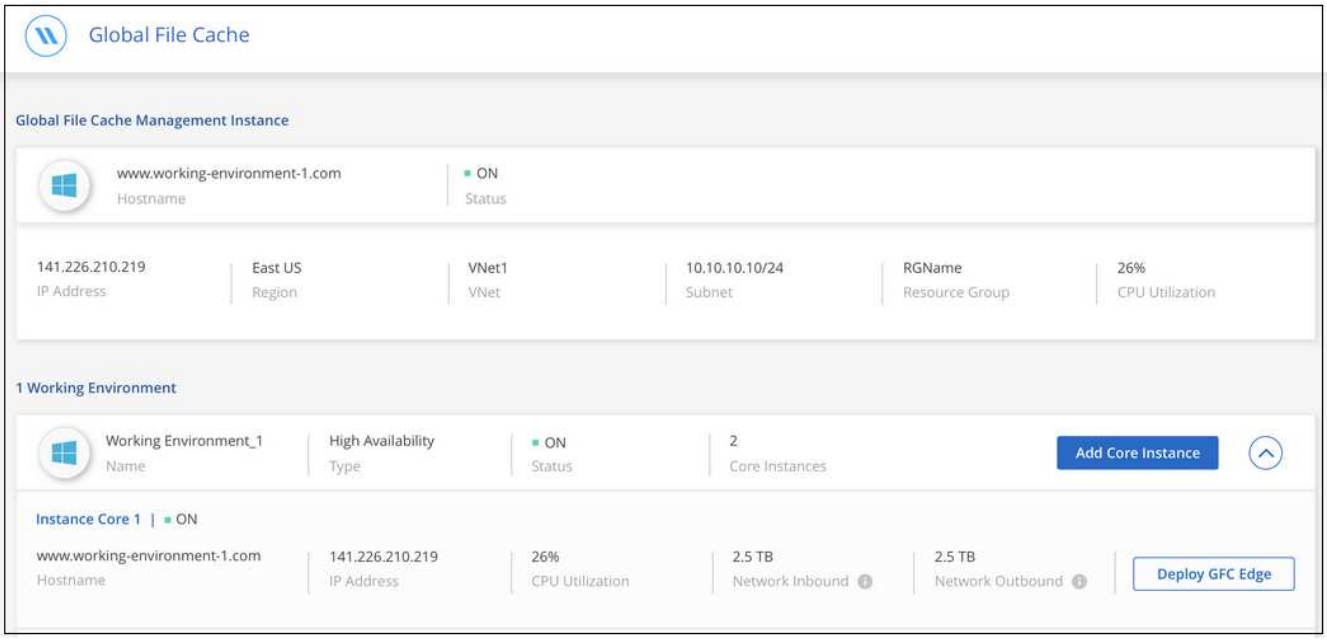
8. Une fois le service Global File cache Management déployé, cliquez sur **Continuer**.
9. Pour Global File cache Core, entrez les informations d'identification de l'utilisateur admin pour rejoindre le domaine Active Directory et les informations d'identification de l'utilisateur du compte de service. Cliquez ensuite sur **Continuer**.
   - L'instance principale du cache de fichiers global doit être déployée dans le même domaine Active Directory que l'instance Cloud Volumes ONTAP.
   - Le compte de service est un utilisateur de domaine et fait partie du groupe BULILTIN\opérateurs de sauvegarde sur l'instance Cloud Volumes ONTAP.



10. Entrez les informations d'identification administratives que vous utiliserez pour accéder à la VM de base du cache de fichiers global et cliquez sur **déployer le réseau de stockage virtuel Fibre Channel Core**. Dans Azure, vous saisissez les identifiants sous forme de nom d'utilisateur et de mot de passe. Pour AWS, vous sélectionnez la paire de clés appropriée. Vous pouvez modifier le nom de la machine virtuelle/de l'instance si vous le souhaitez.



11. Une fois que Global File cache Core a été déployé avec succès, cliquez sur **allez à Dashboard**.



Le tableau de bord indique que l'instance du serveur de gestion et l'instance Core sont à la fois * On* et fonctionnent.

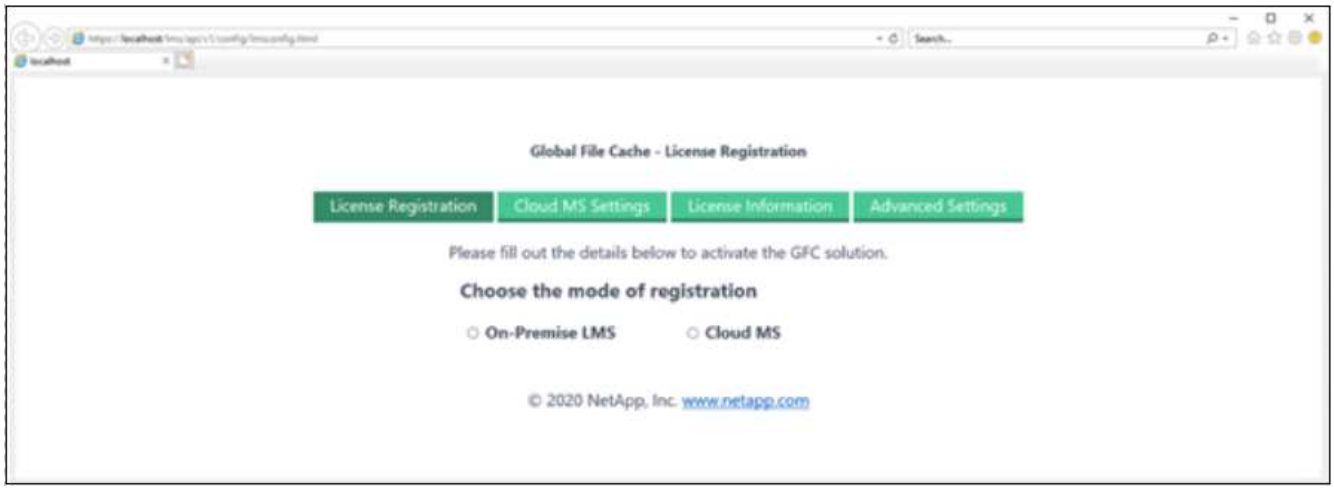
Concéder une licence à l'installation de Global File cache

Avant de pouvoir utiliser Global File cache, vous devez configurer le service LMS (Global File cache License Management Server) sur une instance Core de cache de fichiers global. Pour activer votre abonnement, vous aurez besoin de vos identifiants NSS ou d'un identifiant client fourni par NetApp.

Dans cet exemple, nous allons configurer le service LMS sur une instance Core que vous venez de déployer dans le cloud public. Il s'agit d'un processus unique qui configure votre service LMS.

Étapes

1. Ouvrez la page d'enregistrement de la licence du cache de fichiers global sur le noyau du cache de fichiers global (le noyau que vous désignant comme service LMS) à l'aide de l'URL suivante. Remplacez *<adresse_ip>* par l'adresse IP du cœur de cache de fichiers global :https://<ip_address>/lms/api/v1/config/lmsconfig.html[]
2. Cliquez sur « Continuer vers ce site Web (non recommandé) » pour continuer. Une page qui vous permet de configurer le LMS ou de vérifier les informations de licence existantes s'affiche.



3. Choisissez le mode d'enregistrement en sélectionnant "LMS sur site" ou "MS cloud".
   - « LMS sur site » est utilisé pour les clients existants ou les clients de test qui ont reçu un identifiant client via le service de support NetApp.
   - « Cloud MS » est utilisé pour les clients qui ont acheté des licences NetApp Global File cache Edge auprès de NetApp ou de ses partenaires certifiés et qui disposent de leurs identifiants NetApp.
4. Pour Cloud MS, cliquez sur **Cloud MS**, entrez vos informations d'identification NSS et cliquez sur **Submit**.

5. Pour LMS sur site, cliquez sur **LMS** sur site, saisissez votre ID client, puis cliquez sur **Enregistrer LMS**.

Et la suite ?

Si vous avez déterminé que vous devez déployer plusieurs cœurs de cache de fichiers globaux pour prendre en charge votre configuration, cliquez sur **Ajouter une instance principale** dans le tableau de bord et suivez l'assistant de déploiement.

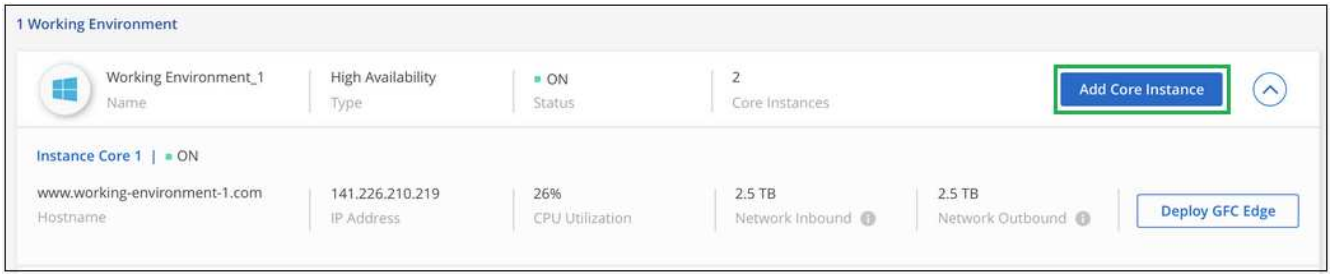
Une fois votre déploiement Core terminé, vous devez "Déployez les instances Global File cache Edge" dans chacun de vos bureaux distants.

Déployer des instances Core supplémentaires

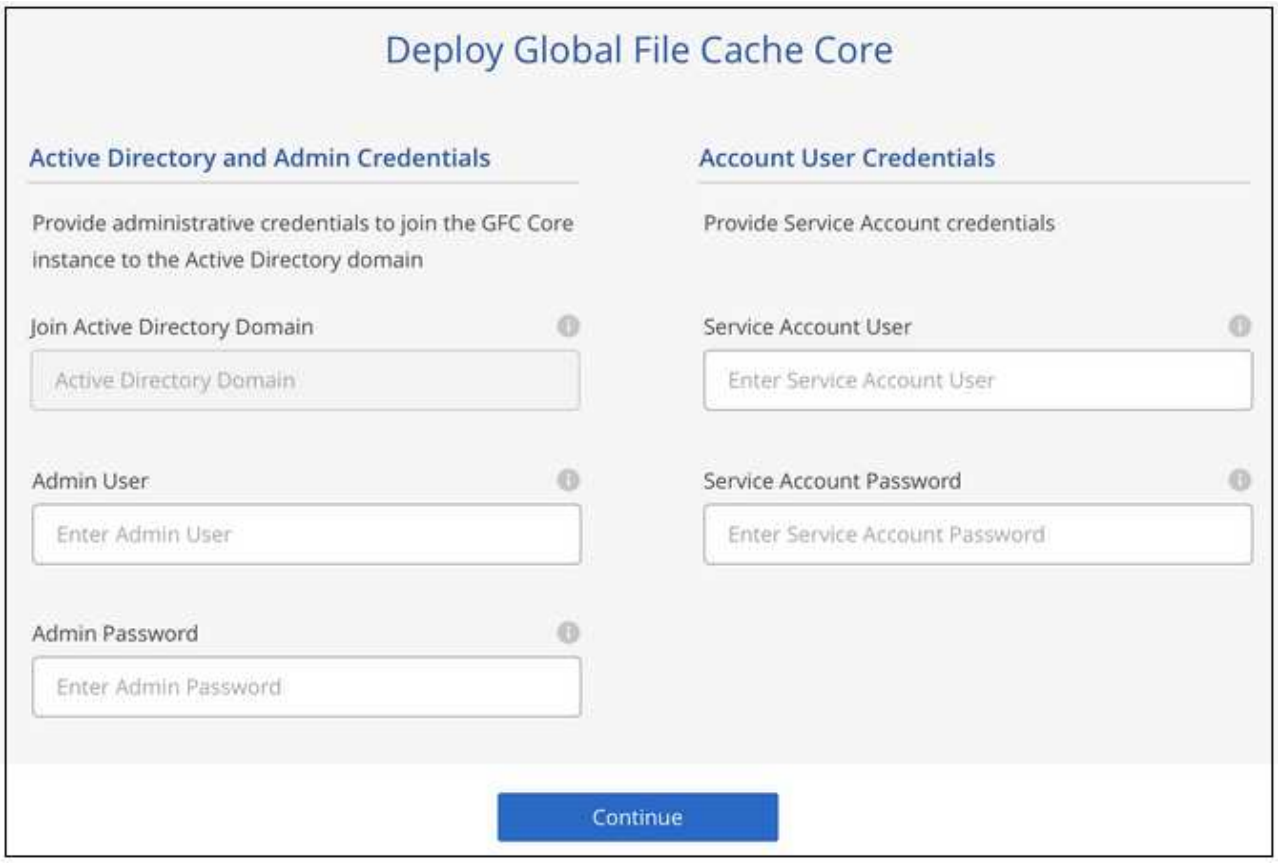
Si votre configuration nécessite l'installation de plusieurs cœurs de cache de fichiers globaux en raison d'un grand nombre d'instances Edge, vous pouvez ajouter un autre Core à l'environnement de travail.

Lors du déploiement d'instances Edge, vous configurez certains pour vous connecter au premier Core et d'autres au second Core. Les deux instances de base accèdent au même système de stockage back-end (votre instance Cloud Volumes ONTAP) dans l'environnement de travail.

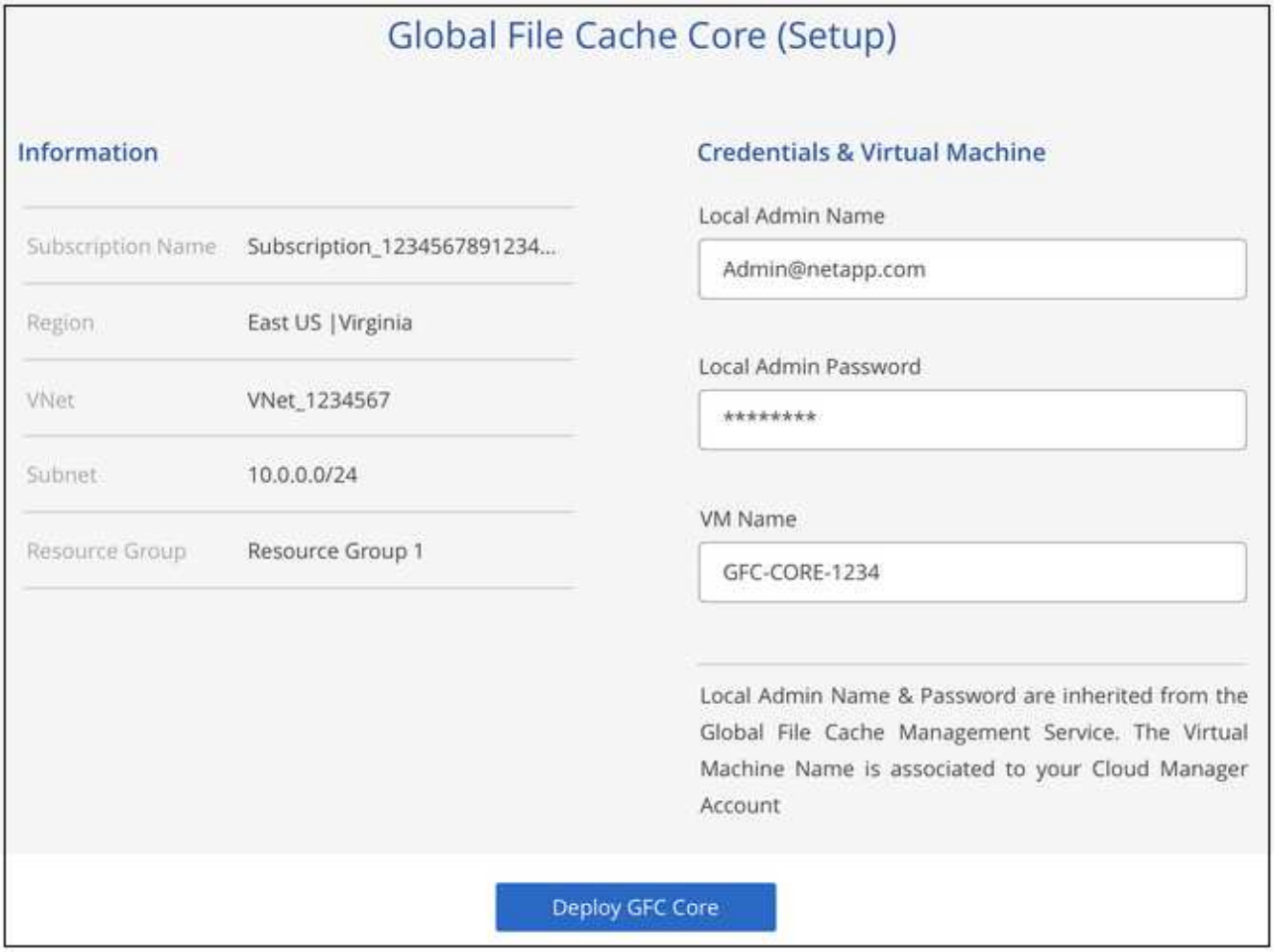
1. Dans le tableau de bord Global File cache, cliquez sur **Add Core instance**.



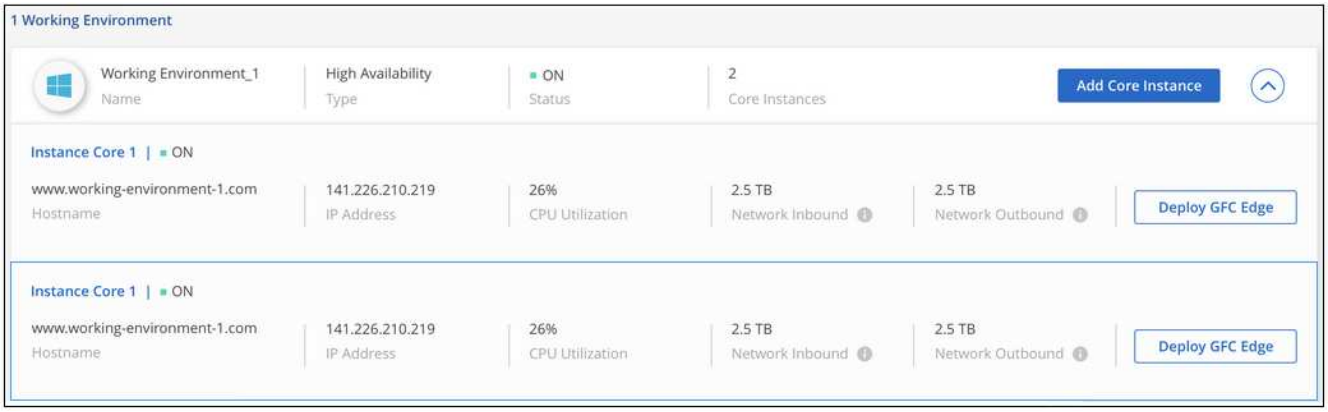
2. Entrez les informations d'identification de l'utilisateur admin pour rejoindre le domaine Active Directory et les informations d'identification de l'utilisateur du compte de service. Cliquez ensuite sur **Continuer**.
   - L'instance principale du cache de fichiers global doit se trouver dans le même domaine Active Directory que l'instance Cloud Volumes ONTAP.
   - Le compte de service est un utilisateur de domaine et fait partie du groupe BULILTIN\opérateurs de sauvegarde sur l'instance Cloud Volumes ONTAP.



3. Entrez les informations d'identification administratives que vous utiliserez pour accéder à la VM de base du cache de fichiers global et cliquez sur **déployer le réseau de stockage virtuel Fibre Channel Core**. Dans Azure, vous saisissez les identifiants sous forme de nom d'utilisateur et de mot de passe. Pour AWS, vous sélectionnez la paire de clés appropriée. Vous pouvez modifier le nom de la machine virtuelle si vous le souhaitez.



4. Une fois que Global File cache Core a été déployé avec succès, cliquez sur **allez à Dashboard**.



Le Tableau de bord reflète la deuxième instance Core pour l'environnement de travail.

Avant de commencer à déployer les instances Global File cache Edge

Vous devez connaître de nombreuses exigences avant de commencer à installer le logiciel Global File cache Edge dans vos bureaux distants.

Télécharger les ressources requises

Téléchargez les modèles virtuels du cache de fichiers global que vous envisagez d'utiliser dans vos succursales, le package d'installation du logiciel et la documentation de référence supplémentaire :

- Modèle virtuel Windows Server 2016 :

  "Windows Server 2016 .OVA avec réseau NetApp compatible avec Windows (VMware vSphere 6.5+)"
  "Windows Server 2016 .VHDX avec réseau Fibre Channel NetApp (Microsoft Hyper-v)"

- Modèle virtuel Windows Server 2019 :

  "Windows Server 2019 .OVA avec réseau NetApp compatible avec Windows (VMware vSphere 6.5+)"
  "Windows Server 2019 .VHDX avec réseau Fibre Channel NetApp (Microsoft Hyper-v)"

- Logiciel Global File cache Edge :

  "Logiciel NetApp Fibre Channel (.EXE)"

- Documentation relative au cache de fichiers global :

  "Guide de l'utilisateur NetApp Global File cache"

Conception et déploiement de Global File cache Edge

Selon vos besoins, vous devrez peut-être déployer une ou plusieurs instances Global File cache Edge en fonction des sessions utilisateur simultanées dans une succursale. L'instance Edge présente le partage de fichiers virtuels aux utilisateurs finaux au sein de la succursale, qui a été étendu de façon transparente à partir de l'instance principale de cache de fichiers global associée. L'Edge de cache de fichiers global doit contenir un `D:\` Volume NTFS, qui contient les fichiers mis en cache au sein de la succursale.

> Pour Global File cache Edge, il est important de comprendre le "instructions de dimensionnement". Cela vous aidera à concevoir correctement votre déploiement de Global File cache. Vous devrez également déterminer ce qui convient à votre environnement en termes d'échelle, de disponibilité des ressources et de redondance.

Instance globale File cache Edge

Lors du déploiement d'une instance Global File cache Edge, vous devez provisionner une seule machine virtuelle, en déployant Windows Server 2016 Standard ou Datacenter Edition, ou Windows Server 2019 Standard ou Datacenter Edition, ou en utilisant le cache de fichiers global `.OVA` ou `.VHD` Modèle comprenant le système d'exploitation Windows Server Choice et le logiciel Global File cache.

Pas de temps

1. Déployez le modèle virtuel Global File cache, la machine virtuelle Windows Server 2016 ou l'édition Standard ou Datacenter de Windows Server 2019.
2. Assurez-vous que la machine virtuelle est connectée au réseau, qu'elle est jointe au domaine et accessible via RDP.
3. Installez la dernière version du logiciel Global File cache Edge.
4. Identifier le serveur de gestion du cache de fichiers global et l'instance principale.

5. Configurez l’instance Global File cache Edge.

Configuration requise globale File cache Edge

Global File cache Edge est conçu pour fonctionner avec toutes les plateformes prenant en charge Windows Server 2016 et 2019, ce qui permet d’offrir une INFRASTRUCTURE IT simplifiée aux bureaux distants et au-delà. La fonctionnalité NetApp Global File cache peut être déployée dans presque tous les cas de figure sur votre infrastructure matérielle, la virtualisation ou les environnements de cloud hybride/public existants, s’ils répondent à quelques critères de base.

Global File cache Edge requiert les ressources matérielles et logicielles suivantes pour fonctionner de manière optimale. Pour plus d’informations sur les directives générales de dimensionnement, reportez-vous à la section "Instructions de dimensionnement".

Serveur renforcé

Le package d’installation Global File cache crée une appliance logicielle renforcée sur n’importe quelle instance de Microsoft Windows Server. *Ne pas désinstaller* le paquet de cache de fichiers global. La désinstallation de Global File cache a un impact sur les fonctionnalités de l’instance de serveur et peut nécessiter une reconstruction complète de l’instance de serveur.

Configuration matérielle physique requise

- Au moins 4 cœurs de processeurs
- 16 Go minimum de RAM
- Carte réseau 1 Gbit/s dédiée unique ou redondante
- Disque dur SAS ou SSD 10 000 tours/min (recommandé)
- Contrôleur RAID avec fonctionnalité de mise en cache de l’écriture différée activée

Besoins en matière de déploiement virtuel

Les plateformes d’hyperviseur sont réputées faire l’objet d’une dégradation des performances du point de vue du sous-système de stockage (par exemple, la latence). Pour des performances optimales à l’aide de Global File cache, il est recommandé d’utiliser une instance de serveur physique avec un disque SSD.

Pour des performances optimales dans les environnements virtuels, outre les besoins de l’hôte physique, les exigences et les réserves de ressources suivantes doivent être respectées :

Microsoft Hyper-V 2012 R2 et versions ultérieures :

- Processeur (CPU) : les processeurs doivent être définis comme **statique** : minimum : 4 cœurs CPU virtuels.
- Mémoire (RAM) : minimum : 16 Go définis comme **statique**.
- Provisionnement du disque dur : les disques durs doivent être configurés comme **disque fixe**.

VMware vSphere 6.x et versions ultérieures :

- Processeur (CPU) : la réservation des cycles CPU doit être définie. Minimum : 4 cœurs de CPU virtuels à 10000 MHz.
- Mémoire (RAM) : minimum : réservation de 16 Go.

- Provisionnement du disque dur :
  - Le provisionnement du disque doit être défini sur **thick provisioning Eager mis à zéro**.
  - Les partages de disque dur doivent être définis sur **High**.
  - Devices.hotplug doit être défini sur **Faux** à l'aide du client vSphere pour empêcher Microsoft Windows de présenter les lecteurs Global File cache comme amovibles.
- Mise en réseau : l'interface réseau doit être définie sur **VMXNET3** (nécessite VM Tools).

Le cache de fichiers global s'exécute sur Windows Server 2016 et 2019. La plateforme de virtualisation doit donc prendre en charge le système d'exploitation, ainsi que l'intégration avec des utilitaires qui améliorent les performances du système d'exploitation invité et la gestion de la machine virtuelle, tels que VM Tools.

Exigences de dimensionnement des partitions

- C:\ - 250 Go minimum (système/volume de démarrage)
- D:\ - 1 To minimum (volume de données distinct pour le cache de fichiers intelligent Global File cache*)

*La taille minimale est de deux fois le jeu de données actif. Le volume de cache (D:\) peut être étendu et n'est restreint que par les limitations du système de fichiers NTFS de Microsoft Windows.

Configuration requise pour le disque de cache de fichiers intelligent de NetApp Global File cache

La latence du disque du disque du cache de fichiers intelligent Global File cache (D:\) doit offrir une latence moyenne d'E/S < 0,5 ms et un débit de 1 IOPS par utilisateur simultané.

Pour plus d'informations, reportez-vous à la section "Guide de l'utilisateur NetApp Global File cache".

Mise en réseau

- Pare-feu : les ports TCP doivent être autorisés entre les instances Global File cache Edge et Management Server et Core.

  Ports TCP du cache global des fichiers : 443 (HTTPS - LMS), 6618 – 6630.

- Les périphériques d'optimisation réseau (tels que Riverbed Steelhead) doivent être configurés pour passer par les ports spécifiques à Global File cache (TCP 6618-6630).

Bonnes pratiques en matière d'applications et de postes de travail client

Global File cache s'intègre en toute transparence dans les environnements du client, ce qui permet aux utilisateurs d'accéder aux données centralisées à l'aide de leurs postes de travail clients, exécutant des applications d'entreprise. À l'aide du cache de fichiers global, les données sont accessibles par le biais d'un mappage direct de lecteur ou d'un espace de noms DFS. Pour plus d'informations sur Global File cache Fabric, la mise en cache intelligente des fichiers et leurs principaux aspects, consultez le "Avant de commencer à déployer Global File cache" section.

Pour garantir une expérience et des performances optimales, il est important de respecter les exigences et les meilleures pratiques du client Microsoft Windows, comme indiqué dans le Guide de l'utilisateur Global File cache. Cela s'applique à toutes les versions de Microsoft Windows.

Pour plus d'informations, reportez-vous à la section "Guide de l'utilisateur NetApp Global File cache".

Meilleures pratiques relatives aux pare-feu et à l'antivirus

Même si Global File cache fait un effort raisonnable pour vérifier que les suites d'applications antivirus les plus courantes sont compatibles avec Global File cache, NetApp ne peut garantir et n'est pas responsable des incompatibilités ou des problèmes de performances provoqués par ces programmes, de leurs mises à jour, packs de services ou de modifications associés.

Global File cache ne recommande pas l'installation ni l'application de solutions antivirus ou de surveillance sur une instance activée par Global File cache (Core ou Edge). Si une solution doit être installée, par choix ou selon des règles, les meilleures pratiques et recommandations suivantes doivent être appliquées. Pour les suites antivirus courantes, consultez l'Annexe A dans le "Guide de l'utilisateur NetApp Global File cache".

Paramètres du pare-feu

- Pare-feu Microsoft :
  - Conserver les paramètres de pare-feu par défaut.
  - Recommandation : laissez les paramètres et services de pare-feu Microsoft sur la valeur par défaut de Désactivé, et non pas démarré pour les instances standard Global File cache Edge.
  - Recommandation : laissez LES paramètres et les services de pare-feu Microsoft sur ACTIVÉ par défaut et démarré pour les instances Edge qui exécutent également le rôle Domain Controller.
- Pare-feu d'entreprise :
  - L'instance Core du cache de fichiers global écoute les ports TCP 6618-6630, assurez-vous que les instances Global File cache Edge peuvent se connecter à ces ports TCP.
  - Les instances globales de cache de fichiers requièrent des communications vers le serveur de gestion du cache de fichiers global sur le port TCP 443 (HTTPS).
- Les solutions/périphériques d'optimisation réseau doivent être configurés pour transmettre les ports spécifiques à Global File cache.

Meilleures pratiques anti-virus

Cette section vous aide à comprendre les conditions requises lors de l'exécution d'un logiciel antivirus sur une instance Windows Server exécutant Global File cache. Global File cache a testé les produits antivirus les plus utilisés, notamment Cylance, McAfee, Symantec, Sophos, Trend micro, Kaspersky et Windows Defender pour une utilisation en association avec le cache de fichiers global.

L'ajout d'antivirus à une appliance Edge peut introduire un impact de 10 à 20 % sur les performances des utilisateurs.

Pour plus d'informations, reportez-vous à la section "Guide de l'utilisateur NetApp Global File cache".

Configurez les exclusions

Les logiciels antivirus ou d'autres utilitaires d'indexation ou d'analyse tiers ne doivent jamais analyser le lecteur D:\ sur l'instance Edge. Ces analyses du lecteur de serveur Edge D:\ entraînent de nombreuses demandes ouvertes de fichiers pour l'intégralité de l'espace de noms de cache. Cela permet d'effectuer des fœtus en fichiers via le WAN vers tous les serveurs de fichiers optimisés dans le data Center. Une inondation de la connexion WAN et une charge inutile sur l'instance Edge se produisent, ce qui entraîne une dégradation des performances.

Outre le lecteur D:\, le répertoire et les processus Global File cache suivants doivent généralement être exclus de toutes les applications antivirus :

- `C:\Program Files\TalonFAST\`
- `C:\Program Files\TalonFAST\Bin\LMClientService.exe`
- `C:\Program Files\TalonFAST\Bin\LMServerService.exe`
- `C:\Program Files\TalonFAST\Bin\Optimus.exe`
- `C:\Program Files\TalonFAST\Bin\tafsexport.exe`
- `C:\Program Files\TalonFAST\Bin\tafsutils.exe`
- `C:\Program Files\TalonFAST\Bin\tapp.exe`
- `C:\Program Files\TalonFAST\Bin\tfs.exe`
- `C:\Program Files\TalonFAST\Bin\TService.exe`
- `C:\Program Files\TalonFAST\Bin\tum.exe`
- `C:\Program Files\TalonFAST\FastDebugLogs\`
- `C:\Windows\System32\drivers\tfast.sys`
- `\\?\TafsMtPt:\ or \\?\TafsMtPt*`
- `\Device\TalonCacheFS\`
- `\\?\GLOBALROOT\Device\TalonCacheFS\`
- `\\?\GLOBALROOT\Device\TalonCacheFS\*`

Politique de support NetApp

Les instances globales de cache de fichiers sont spécialement conçues pour le cache de fichiers global en tant qu'application principale s'exécutant sur une plate-forme Windows Server 2016 et 2019. Le cache de fichiers global nécessite un accès prioritaire aux ressources de plate-forme, par exemple, disque, mémoire, interfaces réseau, et peuvent allouer des exigences élevées sur ces ressources. Les déploiements virtuels requièrent des réservations pour la mémoire/CPU et des disques haute performance.

- Pour les déploiements dans les succursales de Global File cache, les services et applications pris en charge sur le serveur exécutant Global File cache sont limités à :
  - DNS/DHCP
  - Contrôleur de domaine Active Directory (le cache de fichiers global doit se trouver sur un volume distinct)
  - Services d'impression
  - Microsoft System Center Configuration Manager (SCCM)
  - Global File cache, les agents système et les applications antivirus côté client sont approuvés
- Le support et la maintenance de NetApp s'appliquent uniquement au cache de fichiers global.
- Logiciels de productivité de secteur d'activité, généralement très gourmands en ressources, par exemple serveurs de bases de données, serveurs de messagerie, etc. ne sont pas pris en charge.
- Le client est responsable de tout logiciel de cache de fichiers non global pouvant être installé sur le serveur exécutant Global File cache :
  - Si un progiciel tiers cause des conflits de logiciels ou de ressources avec Global File cache ou les performances sont compromises, l'organisation de support de Global File cache peut exiger que le client désactive ou supprime le logiciel du serveur exécutant Global File cache.

    - Il incombe au client de toute installation, intégration, assistance et mise à niveau de tout logiciel ajouté au serveur exécutant l'application Global File cache.
- Les utilitaires/agents de gestion des systèmes, tels que les outils antivirus et les agents de licences, peuvent coexister. Toutefois, à l'exception des services et applications pris en charge répertoriés ci-dessus, ces applications ne sont pas prises en charge par Global File cache et les mêmes directives doivent toujours être respectées :
    - Il incombe au client de toute installation, intégration, assistance et mise à niveau de tout logiciel ajouté.
    - Si un client installe un progiciel tiers qui cause ou est soupçonné de provoquer des conflits de logiciels ou de ressources avec Global File cache ou les performances sont compromises, l'organisation de support de Global File cache peut avoir besoin de désactiver/supprimer le logiciel.

Déploiement des instances Global File cache Edge

Après avoir vérifié que votre environnement répond à toutes les exigences, vous installez le logiciel Global File cache Edge dans chaque bureau distant.

Avant de commencer

Pour effectuer les tâches de configuration de Global File cache Edge, vous devez disposer des informations suivantes :

- Adresses IP statiques pour chaque instance Global File cache
- Masque de sous-réseau
- Adresse IP de la passerelle
- Le FQDN que vous souhaitez attribuer à chaque serveur de cache de fichiers global
- Suffixe DNS (facultatif)
- Nom d'utilisateur et mot de passe d'un utilisateur administratif dans le domaine
- Le FQDN et/ou l'adresse IP des serveurs Core associés
- Volume à utiliser comme cache de fichiers intelligent. Nous vous recommandons de doubler au moins la taille du jeu de données actif. Ce format doit être NTFS et attribué comme `D:\`.

Ports TCP couramment utilisés

Plusieurs ports TCP sont utilisés par les services Global File cache. Il est obligatoire que les périphériques puissent communiquer sur ces ports et qu'ils soient exclus de tout périphérique d'optimisation WAN ou de toute stratégie de restriction de pare-feu :

- Port TCP pour la licence du cache de fichiers global : 443
- Ports TCP du cache de fichiers global : 6618-6630

Déployez le modèle virtuel Global File cache

Le modèle virtuel `.OVA` et `.VHD`) Les images contiennent la dernière version du logiciel Global File cache. Si vous déployez Global File cache à l'aide du `.OVA` ou `.VHD` Modèle de machine virtuelle (VM), suivez les étapes décrites dans cette section. Nous partons du principe que vous comprenez comment déployer le système `.OVA` ou `.VHD` modèle sur la plateforme d'hyperviseur désignée

Assurez-vous que les préférences VM, y compris les réservations de ressources, correspondent aux

exigences décrites dans "Besoins en matière de déploiement virtuel".

Étapes

1. Extrayez le pack du modèle que vous avez téléchargé.
2. Déployez le modèle virtuel. Reportez-vous aux vidéos suivantes avant de commencer le déploiement :
   - "Déployez le modèle virtuel sur VMware"
   - "Déployez le modèle virtuel sur Hyper-V."
3. Une fois que le modèle virtuel a été déployé et que vous avez configuré les paramètres de la machine virtuelle, démarrez la machine virtuelle.
4. Lors de l'amorçage initial, lorsque le système d'exploitation Windows Server 2016 ou 2019 est en préparation à la première utilisation, complétez l'expérience prête à l'emploi en installant les pilotes appropriés et en installant les composants nécessaires pour le matériel correspondant.
5. Une fois l'installation de base de l'instance Global File cache Edge terminée, le système d'exploitation Windows Server 2016 ou 2019 vous guide à travers un assistant de configuration initiale pour configurer les spécificités du système d'exploitation, telles que la localisation et la clé de produit.
6. Une fois l'Assistant de configuration initial terminé, connectez-vous localement au système d'exploitation Windows Server 2016 ou 2019 avec les informations d'identification suivantes :
   - Nom d'utilisateur : **FASTAdmin**
   - Mot de passe : **Tal0nFAST!**
7. Configurez votre machine virtuelle Windows Server, rejoignez le domaine Active Directory de l'entreprise et passez à la section Configuration de Global File cache Edge.

Configurez l'instance Global File cache Edge

L'instance Global File cache Edge se connecte à un noyau Global File cache pour permettre aux utilisateurs de la succursale d'accéder aux ressources du serveur de fichiers du data Center.

L'instance Edge doit être sous licence dans le cadre de votre déploiement Cloud Volumes ONTAP avant de commencer la configuration. Voir "Licences" pour plus d'informations sur les licences.

Si votre configuration nécessite l'installation de plusieurs cœurs de cache de fichiers globaux en raison d'un grand nombre d'instances Edge, vous allez configurer certaines instances Edge afin qu'elles se connectent au premier Core et d'autres au second Core. Assurez-vous que vous disposez du FQDN ou de l'adresse IP, ainsi que d'autres informations requises, pour l'instance Core correcte.

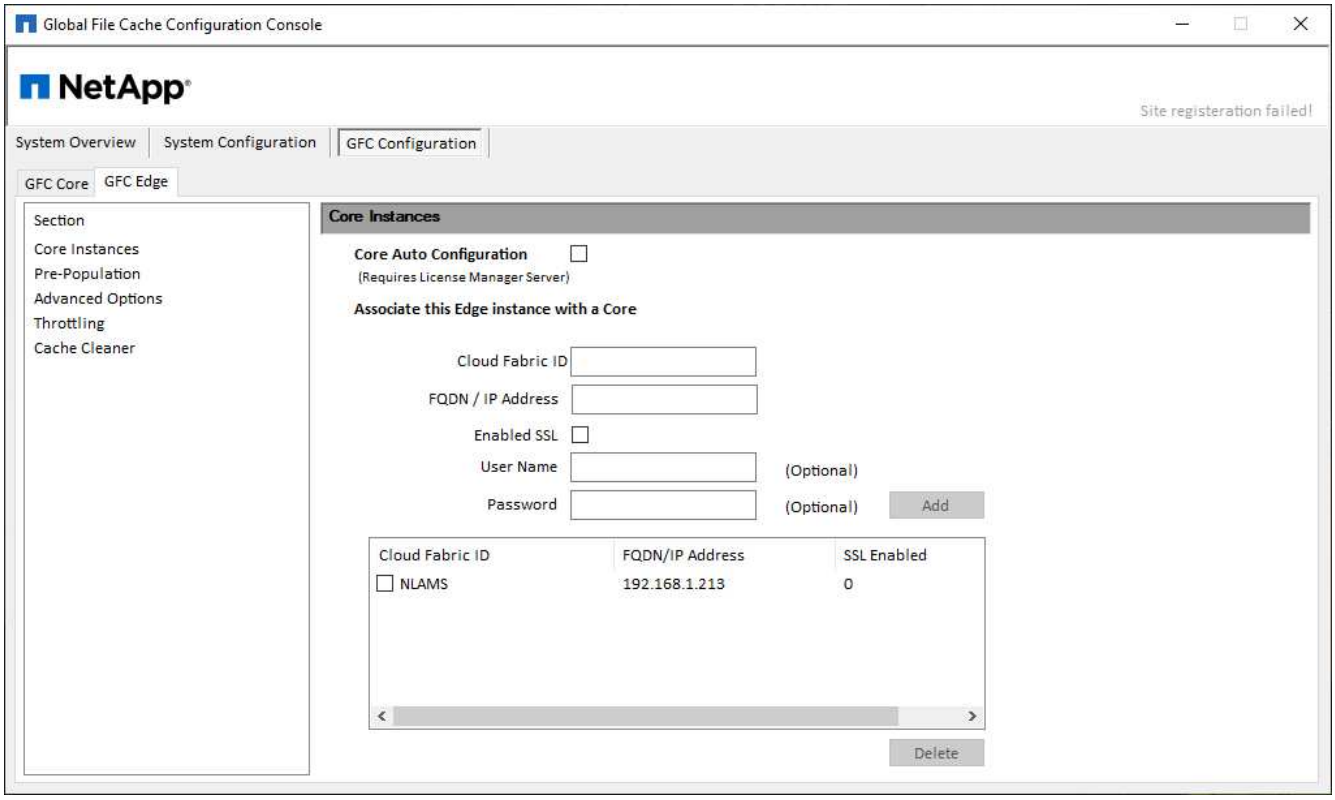
Pour configurer l'instance Edge, procédez comme suit :

Étapes

1. Cliquez sur **Perform** en regard de l'étape de configuration du noyau non cochée répertoriée dans la section « étapes de configuration du bord » de l'assistant de configuration initiale. Cela ouvre un nouvel onglet, Fibre Channel Edge, et affiche la section *instances Core*.
2. Fournissez l'ID **Cloud Fabric** du serveur de base du cache de fichiers global. L'ID Cloud Fabric est généralement le nom NetBIOS ou l'emplacement géographique du serveur de fichiers back-end.
3. Indiquez le **FQDN/adresse IP** du serveur de base du cache de fichiers global :
   a. (Facultatif) cochez la case **SSL** pour activer la prise en charge SSL pour un cryptage amélioré de la périphérie au cœur.

b. Entrez le nom d'utilisateur et le mot de passe, qui sont les informations d'identification du compte de service utilisé sur le Core.

4. Cliquez sur **Ajouter** pour confirmer l'ajout de l'appliance Global File cache Core. Une boîte de confirmation s'affiche. Cliquez sur **OK** pour le fermer.



Mettre à jour le logiciel Global File cache Edge

Global File cache publie fréquemment des mises à jour du logiciel, soit des correctifs, des améliorations, soit de nouvelles fonctions. Bien que le modèle virtuel (`.OVA` et `.VHD`) Les images contiennent la dernière version du logiciel Global File cache, il est possible qu'une version plus récente soit disponible sur le portail de téléchargement du support NetApp.

Assurez-vous que vos instances Global File cache sont à jour avec la dernière version.

Ce pack logiciel peut également être utilisé pour des installations immaculées sous Microsoft Windows Server 2016 Édition Standard ou Datacenter, Windows Server 2019 Édition Standard ou Datacenter, ou dans le cadre de votre stratégie de mise à niveau.

Vous trouverez ci-dessous les étapes nécessaires à la mise à jour du package d'installation de Global File cache :

Étapes

1. Après avoir enregistré la dernière installation dans l'instance Windows Server souhaitée, double-cliquez dessus pour exécuter l'exécutable d'installation.
2. Cliquez sur **Suivant** pour continuer le processus.
3. Cliquez sur **Suivant** pour continuer.
4. Acceptez le contrat de licence et cliquez sur **Suivant**.

5. Sélectionnez l'emplacement de destination d'installation souhaité.

   NetApp recommande d'utiliser le lieu d'installation par défaut.

6. Cliquez sur **Suivant** pour continuer.
7. Sélectionnez le dossier du menu Démarrer.
8. Cliquez sur **Suivant** pour continuer.
9. Vérifiez les paramètres d'installation souhaités et cliquez sur **Install** pour commencer l'installation.

   Le processus d'installation s'exécute.

10. Une fois l'installation terminée, redémarrez le serveur lorsque vous y êtes invité.

Et la suite ?

Pour plus d'informations sur la configuration avancée de Global File cache Edge, reportez-vous au "Guide de l'utilisateur NetApp Global File cache".

Formation des utilisateurs finaux

Vous pouvez former vos utilisateurs aux meilleures pratiques d'accès aux fichiers partagés via Global File cache.

Il s'agit de la phase finale du déploiement de Global File cache, phase d'implémentation par l'utilisateur final.

Afin de préparer et de rationaliser le processus d'intégration des utilisateurs finaux, utilisez le modèle d'e-mail ci-dessous qui vous aidera à former les utilisateurs finaux sur les moyens de travailler dans un environnement de « données centrales ». Cela aidera vos utilisateurs à tirer parti de tous les avantages de la solution Global File cache. Nous avons également publié une vidéo qui peut être partagée à "former" les utilisateurs si nécessaire.

Personnaliser et transférer les ressources suivantes aux utilisateurs finaux pour les préparer au déploiement :

- Vidéo de formation des utilisateurs"Vidéo de formation des utilisateurs finaux"
- Modèle d'e-mail"Modèle d'e-mail Mac (.emltpl)"

  "Modèle de messagerie Windows (.msg)"

- Communications d'intégration"Document Word (.docx)"

Reportez-vous au chapitre 12 du "Guide de l'utilisateur NetApp Global File cache" pour du matériel supplémentaire.

Informations supplémentaires

Utilisez les liens suivants pour en savoir plus sur Global File cache et d'autres produits NetApp :

- FAQ relative au cache global de fichiers
  - Voir une liste de questions fréquemment posées et de réponses "ici"
- "Guide de l'utilisateur NetApp Global File cache"

- Documentation produit NetApp
  - Consultez la documentation complémentaire sur les produits cloud NetApp "ici"
  - Voir la documentation complémentaire sur tous les produits NetApp "ici"
- Le support client pour les utilisateurs de Global File cache avec Cloud Volumes ONTAP est disponible via les canaux suivants :
  - Résolution assistée de problèmes, gestion des dossiers, base de connaissances, téléchargements, outils, et plus encore "ici"
  - Connectez-vous au site de support NetApp sur https://mysupport.netapp.com Avec vos identifiants NSS
  - Pour obtenir une assistance immédiate concernant les problèmes P1, appelez le +33 1 856.481.3990 00 (option 2).
- Le support client de Global File cache qui utilise NetApp Cloud volumes Services et Azure NetApp Files est proposé par votre fournisseur. Veuillez contacter le service d'assistance clientèle de Google ou le service clientèle de Microsoft respectivement.

Optimisation des coûts du cloud computing

Découvrez le service de calcul

Valorisation "Service SPOT Cloud Analyzer", Cloud Manager peut fournir une analyse des coûts généraux de vos dépenses de calcul dans le cloud et identifier les économies potentielles.

Cloud Analyzer est une solution de gestion d'infrastructure cloud qui utilise des fonctions d'analytique avancée pour vous donner une visibilité sur les coûts cloud. Il vous montre où vous pouvez optimiser ces coûts et vous permet d'implémenter cette optimisation à l'aide du portefeuille de produits d'optimisation continue de Spot en quelques clics seulement.

Caractéristiques

- Une analyse des coûts qui indique les coûts actuels du mois, les coûts mensuels prévus et les économies manquées
- Vue de l'efficacité des dépenses par compte, y compris des économies supplémentaires estimées
- Lien vers Cloud Analyzer de Spotqu'à NetApp pour des informations plus détaillées sur les dépenses de l'ensemble des comptes

Fournisseurs cloud pris en charge

Ce service est pris en charge par AWS.

Le coût

L'utilisation de ce service est gratuite grâce à Cloud Manager.

Fonctionnement de Cloud Analyzer avec Cloud Manager

À un niveau élevé, l'intégration d'Cloud Analyzer avec Cloud Manager fonctionne comme suit :

1. Vous cliquez sur **Compute** et connectez votre compte principal payeur AWS.
2. NetApp configure votre environnement comme suit :
   a. Crée une organisation dans la plateforme Spot.
   b. Envoie un e-mail de bienvenue à Spot.

      Vous pouvez vous connecter au service Spot à l'aide des mêmes identifiants de connexion unique que ceux que vous utilisez avec Cloud Central et Cloud Manager.

   c. Cloud Analyzer commence à traiter les données de votre compte AWS.
3. Dans Cloud Manager, les pages de calcul sont actualisées et vous utilisez les informations pour analyser les coûts cloud passés, actuels et futurs.
4. Vous cliquez sur **obtenir une analyse complète** à tout moment pour accéder à Cloud Analyzer de Spot, qui vous offre une analyse complète de vos dépenses en cloud et des opportunités d'économies.

Sécurité des données

Les données Cloud Analyzer sont chiffrées au repos et aucun identifiant n'est stocké pour n'importe quel compte.

Commencez à optimiser les coûts du cloud computing

Connectez votre compte AWS, puis visualisez l'analyse pour commencer à optimiser les coûts de calcul du cloud.

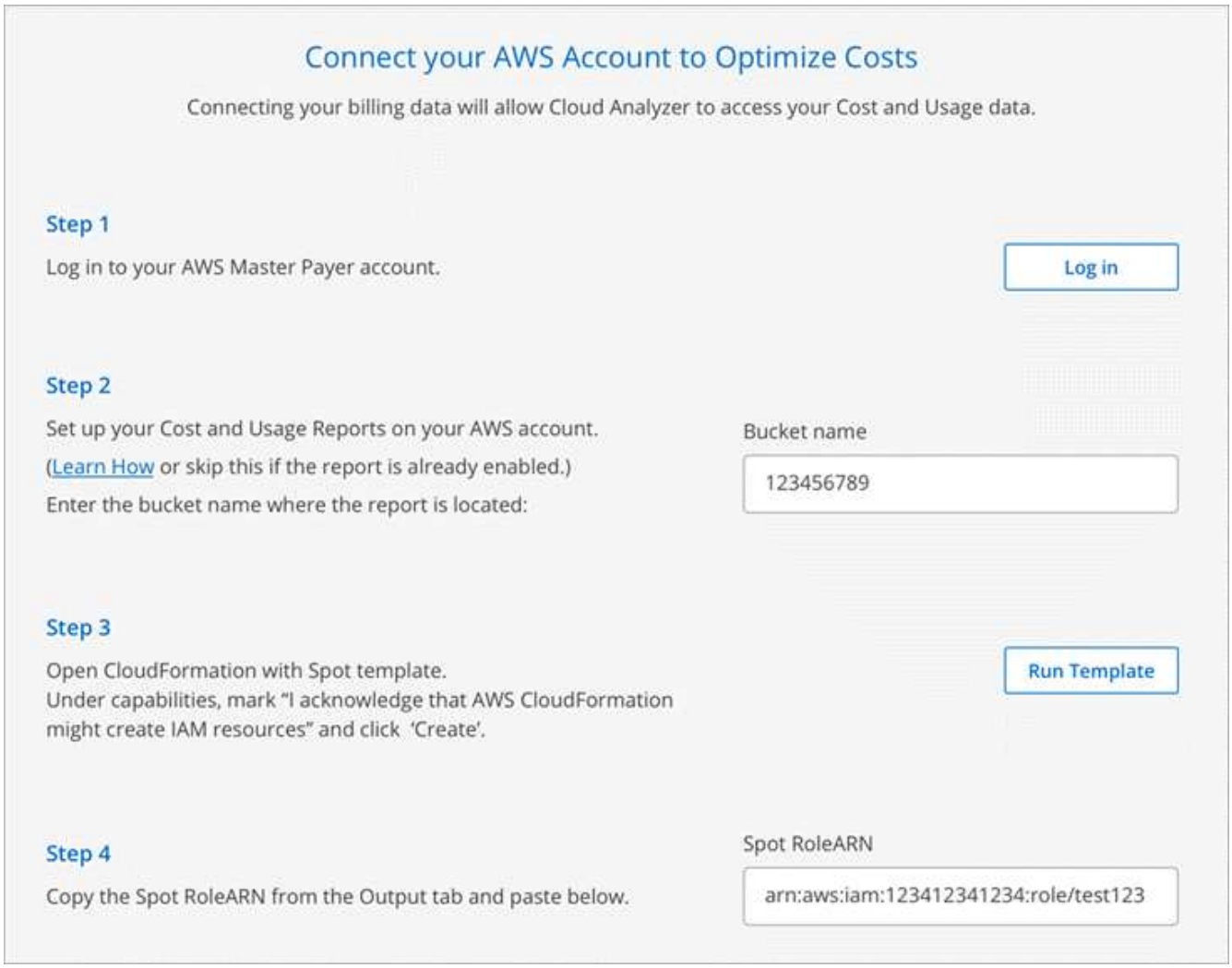
Connectez Cloud Analyzer à votre compte AWS

Cliquez sur **Compute** et connectez votre compte AWS payeur.

Étapes

1. Cliquez sur **Compute**.
2. Cliquez sur **Ajouter les informations d'identification AWS pour démarrer**.
3. Suivez les étapes indiquées sur la page pour connecter votre compte AWS :
    a. Connectez-vous à votre compte principal payeur AWS.
    b. Configurez les rapports sur les coûts et l'utilisation sur le compte AWS.
    c. Exécuter le modèle CloudFormation.
    d. Coller le point RoleARN.

    "Afficher plus de détails sur ces étapes".

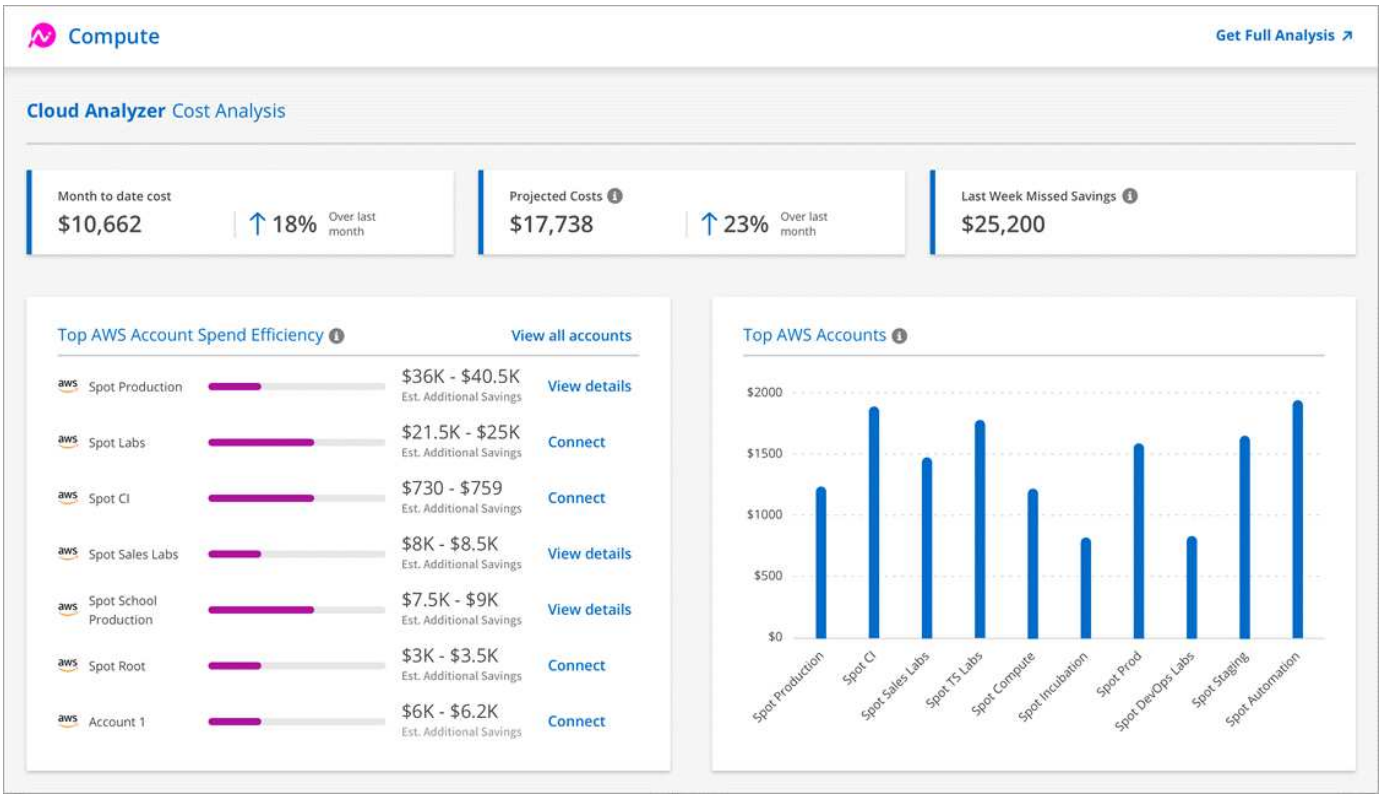


Résultat

Cloud Analyzer commence à traiter les données de votre compte AWS. Si vous avez plusieurs comptes, Cloud Analyzer commence par des capacités en lecture seule pour tous les comptes liés sous le compte payeur principal. Si vous souhaitez obtenir plus d'informations sur les économies potentielles pour ces comptes, vous devrez également les connecter. Vous trouverez plus de détails sur ce processus dans la section ci-dessous.

Analysez les coûts de calcul

Une fois que Cloud Analyzer a terminé le traitement des données de votre compte, l'onglet Compute vous donne des informations sur les coûts cloud passés, actuels et futurs.



Coût mois à ce jour

Coût total de vos charges de travail depuis le début du mois en cours.

Coûts prévus

Le coût prévu à la fin du mois, d'après l'analyse de votre modèle d'utilisation.

Économies manquées de la semaine dernière

Des économies qui auraient pu être réalisées au cours des sept derniers jours grâce à l'optimisation des instances SPOT et des réservations.

Efficacité des dépenses pour un compte AWS

Les 10 plus grands comptes selon le plus grand montant estimé d'économies supplémentaires.

Chaque compte se voit attribuer un score d'efficacité en fonction des économies actuelles et potentielles supplémentaires. Les économies supplémentaires estimées indiquent la somme qui peut être économisée en utilisant les instances ponctuelles et réservées.

Vous pouvez prendre les mesures suivantes pour optimiser davantage vos comptes :

- **Afficher les détails**: Affichez vos possibilités d'optimisation des coûts en accédant à Cloud Analyzer de Spot.
- **Connect** : permet de connecter un compte qui n'est pas encore géré. Vous serez dirigé vers l'assistant qui connecte le compte.

Principaux comptes AWS

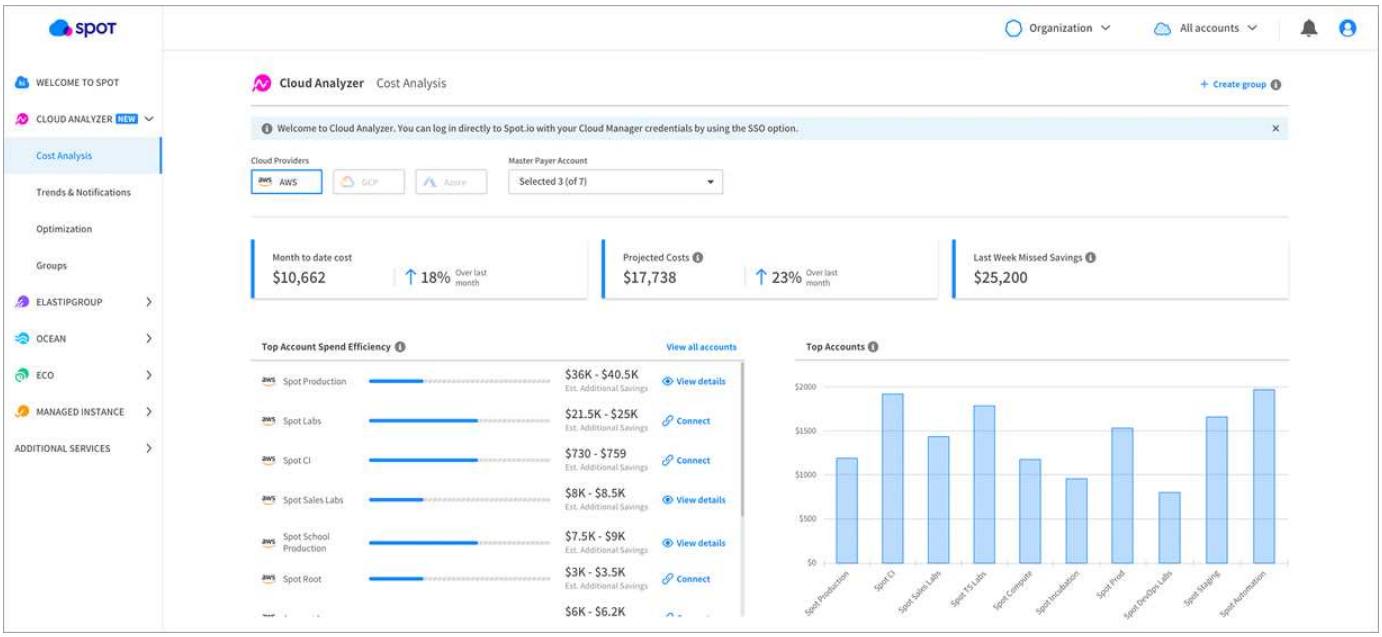
Il s'agit d'un graphique à barres indiquant les dix principaux comptes en fonction de leur coût. Le graphique est basé sur les 30 derniers jours de l'activité de dépense.

"Découvrez la page d'analyse des coûts disponible dans le Cloud Analyzer de Spot".

Accédez à Cloud Analyzer pour plus d'analyse et de recommandations

Cliquez sur **Get Full Analysis** à tout moment pour accéder à plus de graphiques et d'analyses, des recommandations détaillées, une description de l'optimisation des cas d'utilisation (conteneurs, ElasticApps, et réservations), et plus encore.

Voici un exemple de ce que vous verrez dans Cloud Analyzer :



- "Consultez la page produit de Cloud Analyzer pour en savoir plus sur ses fonctionnalités".
- "Consultez la documentation de Spot pour obtenir de l'aide sur Cloud Analyzer".

Basculez les données vers le cloud

Découvrez NetApp Cloud Tiering

Le service NetApp Cloud Tiering étend votre data Center au cloud en transférant automatiquement les données inactives des clusters ONTAP sur site au stockage objet. Cela permet de libérer de l'espace sur le cluster pour plus de charges de travail, sans apporter de modifications au niveau de la couche applicative. NetApp Cloud Tiering permet de réduire les coûts de votre data Center et de passer d'un modèle de dépenses d'investissement à un modèle de dépenses d'exploitation.

Le service de Tiering cloud exploite les fonctionnalités de *FabricPool*. FabricPool est une technologie Data Fabric qui permet le Tiering automatisé des données vers un stockage objet à faible coût. Les données actives restent sur des disques SSD haute performance, tandis que les données inactives sont envoyées vers un stockage objet à faible coût, tout en préservant les fonctions d'efficacité des données ONTAP.

Caractéristiques

NetApp Cloud Tiering propose des fonctionnalités d'automatisation, de surveillance, de rapports et une interface de gestion commune :

- Grâce à l'automatisation, vous pouvez plus facilement configurer et gérer le Tiering des données depuis les clusters ONTAP sur site vers le cloud
- Avec une fenêtre unique, vous n'avez plus besoin de gérer FabricPool de façon indépendante sur plusieurs clusters
- Des rapports indiquent la quantité de données actives et inactives sur chaque cluster
- L'état de l'état de santé par niveaux vous aide à identifier et à corriger les problèmes au fur et à mesure qu'ils se produisent
- Si vous disposez de systèmes Cloud Volumes ONTAP, vous les trouverez dans le tableau de bord des clusters pour bénéficier d'une vue complète du Tiering des données dans votre infrastructure de cloud hybride

> Les systèmes Cloud Volumes ONTAP sont en lecture seule depuis le Tiering dans le cloud. "Configuration du Tiering pour Cloud Volumes ONTAP à partir de l'environnement de travail dans Cloud Manager".

Pour en savoir plus sur les atouts de NetApp Cloud Tiering, "Consultez la page NetApp Cloud Tiering sur NetApp Cloud Central".

> Si le Tiering dans le cloud permet de réduire considérablement l'empreinte du stockage, il ne s'agit pas d'une solution de sauvegarde.

Fournisseurs de stockage objet pris en charge

Vous pouvez déplacer les données inactives d'un cluster ONTAP vers Amazon S3, Microsoft Azure Blob Storage, Google Cloud Storage ou StorageGRID (cloud privé).

Prix et licences

Payez pour le Tiering dans le cloud via un abonnement avec paiement basé sur l'utilisation, une licence de Tiering ONTAP appelée *FabricPool*, ou une combinaison des deux. Un essai gratuit de 30 jours est disponible pour votre premier cluster si vous n'avez pas de licence.

Le Tiering des données vers StorageGRID n'est pas payant. Une licence BYOL ou un enregistrement PAYGO ne sont pas nécessaires.

"Voir les détails des tarifs".

essai gratuit de 30 jours

Si vous ne disposez pas de licence FabricPool, une version d'évaluation gratuite de 30 jours de Cloud Tiering commence lorsque vous configurez le Tiering sur le premier cluster. Après la fin de l'essai gratuit de 30 jours, vous devrez payer pour NetApp Cloud Tiering par l'intermédiaire d'un abonnement avec paiement à l'utilisation, d'une licence FabricPool ou d'une combinaison des deux.

Si votre version d'évaluation gratuite est terminée et que vous n'avez pas souscrit à cette licence, ONTAP ne transfère plus les données inactives vers un stockage objet, mais les données existantes sont toujours accessibles.

Abonnement avec paiement à l'utilisation

Cloud Tiering propose un modèle de paiement à l'utilisation avec des licences basées sur la consommation. Après vous être abonné sur le marché de votre fournisseur cloud, vous payez par Go pour les données hiérarchisées - pas de paiement initial. Votre fournisseur cloud vous facturé mensuellement.

Vous devez vous abonner même si vous disposez d'une période d'essai gratuite ou si vous apportez votre propre licence (BYOL) :

- L'abonnement garantit l'absence de perturbation du service après la fin de votre essai gratuit.

  À la fin de l'essai, vous serez facturé toutes les heures en fonction de la quantité de données que vous avez réparties par niveau.

- Si vous procédez au Tiering des données plus élevé que ce qui est autorisé par votre licence FabricPool, le Tiering des données se poursuit grâce à votre abonnement au paiement à l'utilisation.

  Par exemple, si vous disposez d'une licence de 10 To, toute la capacité au-delà de 10 To est facturée par l'abonnement au paiement basé sur l'utilisation.

Vous n'aurez pas à payer votre abonnement au paiement à l'utilisation pendant votre essai gratuit ou si vous n'avez pas dépassé votre licence FabricPool.

"Découvrez comment configurer un abonnement avec paiement à l'utilisation".

Bring your own license (BYOL)

Bring your own license (BYOL) en achetant une licence ONTAP FabricPool. Vous pouvez acheter des licences basées sur des conditions ou des licences perpétuelles.

Une fois que vous achetez une licence FabricPool, vous devez l'ajouter au cluster, "Que vous pouvez faire directement depuis le Tiering dans le cloud".

Après avoir activé la licence via Cloud Tiering, si vous achetez de la capacité supplémentaire ultérieurement, la licence sur le cluster est automatiquement mise à jour avec la nouvelle capacité. Il n'est pas nécessaire d'appliquer un nouveau fichier de licence NetApp au cluster.

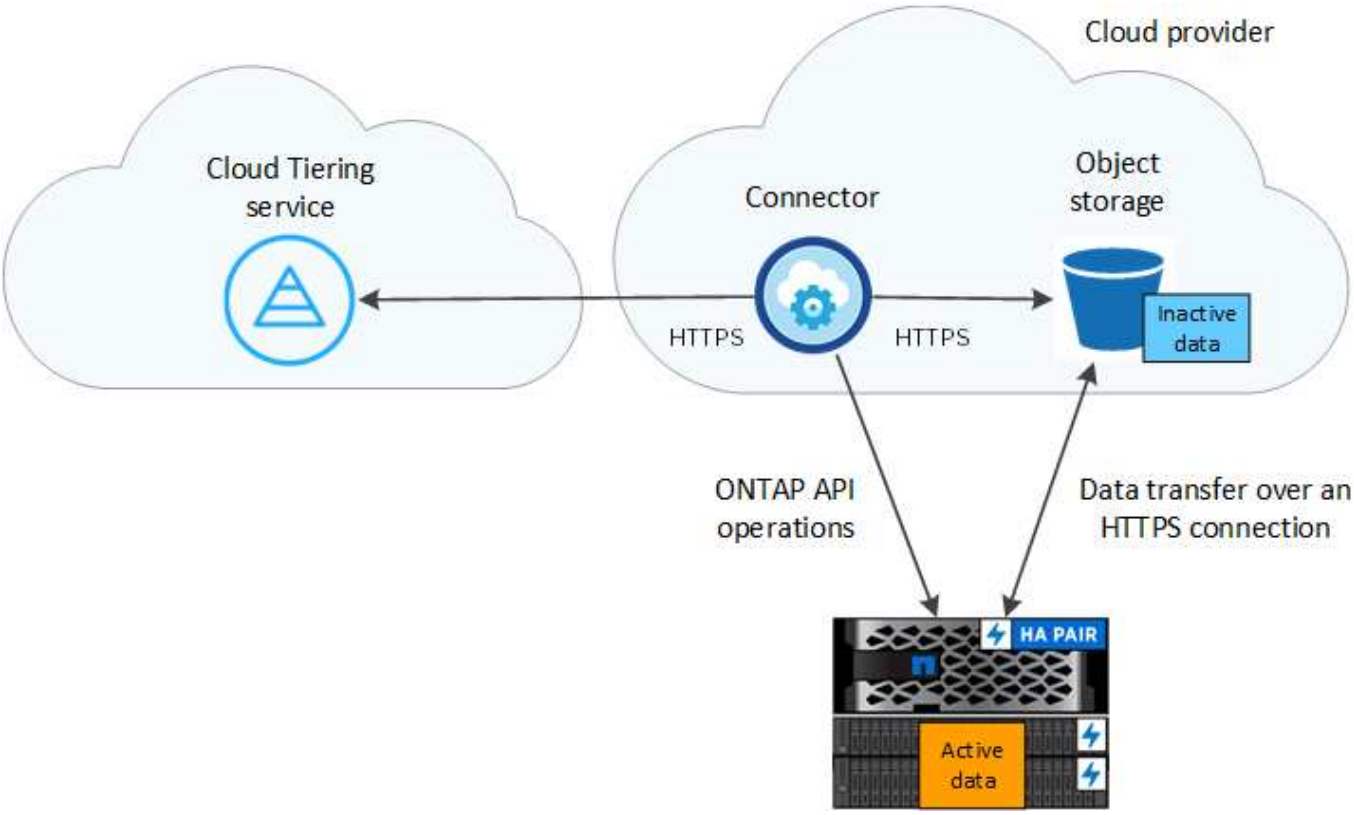
Comme indiqué ci-dessus, nous vous recommandons de configurer un abonnement avec paiement à l'utilisation, même si votre cluster possède une licence BYOL.

Mailto:ng-cloud-tiering@netapp.com?subject=Licensing[Contactez-nous pour acheter une licence].

Fonctionnement de Cloud Tiering

Cloud Tiering est un service géré par NetApp qui utilise la technologie FabricPool pour transférer automatiquement les données inactives (inactives) depuis vos clusters ONTAP sur site vers un stockage objet dans votre cloud public ou privé. Les connexions à ONTAP sont réalisées à partir d'un connecteur.

L'image suivante montre la relation entre chaque composant :



À un niveau élevé, NetApp Cloud Tiering fonctionne comme suit :

1. Vous découvrez votre cluster sur site Cloud Manager.
2. Pour configurer le Tiering, vous fournissant des informations détaillées sur le stockage objet, notamment le compartiment/conteneur et la classe de stockage ou le Tier d'accès.
3. Cloud Manager configure ONTAP pour qu'il utilise le fournisseur de stockage objet et détecte la quantité de données actives et inactives sur le cluster.
4. Vous choisissez les volumes à Tier et la règle de Tiering à appliquer à ces volumes.
5. ONTAP commence le Tiering des données inactives dans le magasin d'objets, dès que les données ont atteint les seuils à considérer comme inactives (voir la Stratégies de hiérarchisation des volumes).

Stockage objet

Chaque cluster ONTAP transfère les données inactives vers un seul magasin d'objets. Une fois le Tiering des données configuré, vous avez la possibilité d'ajouter un nouveau compartiment/conteneur, ou de sélectionner un compartiment/conteneur existant avec une classe de stockage ou un niveau d'accès.

- "En savoir plus sur les classes de stockage S3 prises en charge"
- "Découvrez les tiers d'accès Azure Blob pris en charge"
- "Découvrez les classes de stockage Google Cloud prises en charge"

Stratégies de hiérarchisation des volumes

Lorsque vous sélectionnez les volumes à placer, vous choisissez une *stratégie de Tiering des volumes* à appliquer à chaque volume. Une règle de Tiering détermine quand ou si les blocs de données utilisateur d'un volume sont déplacés vers le cloud.

Pas de règle de hiérarchisation
: Conserve les données sur un volume situé dans le Tier de performance, ce qui empêche leur déplacement vers le cloud.

Snapshots inactives (Snapshot uniquement)
: ONTAP transfère les blocs Snapshot inactives dans le volume qui ne sont pas partagés avec le système de fichiers actif vers le stockage objet. Si les blocs de données inactives du Tier cloud sont lus et déplacés vers le Tier de performance.

  Les données ne sont hiérarchisées qu'après avoir atteint leur capacité de 50 % et quand elles ont atteint la période de refroidissement. Le nombre de jours de refroidissement par défaut est 2, mais vous pouvez régler le nombre de jours.

  > Les écritures depuis le Tier cloud vers le Tier de performance sont désactivées si la capacité du Tier de performance est supérieure à 70 %. Dans ce cas, les blocs sont accessibles directement depuis le Tier cloud.

Données utilisateur inactives (auto)
: ONTAP transfère tous les blocs inactives du volume (sans inclure les métadonnées) vers le stockage objet. Les données à froid comprennent non seulement des copies Snapshot, mais aussi des données utilisateur à froid provenant du système de fichiers actif.

  Pour une lecture aléatoire, les blocs de données inactives du Tier cloud sont fortement sollicités et sont déplacés vers le Tier de performance. Lorsqu'ils sont lus par des lectures séquentielles, telles que celles associées aux analyses d'index et antivirus, les blocs de données inactives sur le Tier cloud restent inactifs et ne sont pas écrits sur le Tier de performance.

  Les données ne sont hiérarchisées qu'après avoir atteint leur capacité de 50 % et quand elles ont atteint la période de refroidissement. Pendant cette période, les données utilisateur d'un volume doivent rester inactives et déplacées vers le magasin d'objets. Le nombre de jours de refroidissement par défaut est 31, mais vous pouvez régler le nombre de jours.

  > Les écritures depuis le Tier cloud vers le Tier de performance sont désactivées si la capacité du Tier de performance est supérieure à 70 %. Dans ce cas, les blocs sont accessibles directement depuis le Tier cloud.

Toutes les données utilisateur (toutes)

Toutes les données (sans les métadonnées) sont immédiatement marquées comme inactives et hiérarchisées vers le stockage objet dès que possible. Il n'est pas nécessaire d'attendre 48 heures que les nouveaux blocs d'un volume soient inactifs. Notez que les blocs situés dans le volume avant la définition de toutes les règles exigent 48 heures pour être froids.

Si les blocs de données inactives du Tier cloud sont lus, ceux-ci restent inactives et ne sont pas réécrits sur le Tier de performance. Cette règle est disponible à partir de ONTAP 9.6.

Prenez en compte les éléments suivants avant de choisir cette règle de Tiering :

- Le Tiering des données réduit immédiatement l'efficacité du stockage (à la volée uniquement).
- Vous devez appliquer cette règle uniquement si vous êtes sûr que les données inactives du volume ne seront pas modifiées.
- En l'absence de transaction, le stockage objet peut se traduire par une fragmentation importante en cas de modification.
- Tenez compte de l'impact des transferts SnapMirror avant d'attribuer l'ensemble de la règle de Tiering aux volumes source dans les relations de protection des données.

  Dans la mesure où les données sont placées immédiatement sur le Tier de performance, SnapMirror les lit plutôt que sur le Tier de performance. Ceci ralentit les opérations SnapMirror, et peut-être ralentir les autres opérations SnapMirror plus tard dans la file d'attente, même si elles utilisent différentes règles de hiérarchisation.

Toutes les données utilisateur DP (sauvegarde)

Toutes les données d'un volume de protection des données (hors métadonnées) sont immédiatement transférées vers le Tier cloud. Si les blocs de données inactives du Tier cloud sont lus, ceux-ci restent inactives et ne sont pas réécrits sur le Tier de performance (à partir de ONTAP 9.4).

Cette règle est disponible pour ONTAP 9.5 ou version antérieure. Il a été remplacé par la stratégie de hiérarchisation **All** à partir de ONTAP 9.6.

Commencez

Tiering des données depuis des clusters ONTAP sur site vers Amazon S3

Libérez de l'espace sur vos clusters ONTAP sur site grâce au Tiering des données vers Amazon S3. Le Tiering des données est optimisé par le service NetApp Cloud Tiering.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

Préparation au Tiering des données vers Amazon S3

Il faut les éléments suivants :

- Un système AFF ou FAS doté d'agrégats 100 % SSD qui exécutent ONTAP 9.2 ou une version ultérieure

et qui bénéficie d'une connexion HTTPS vers Amazon S3.

- Un compte AWS doté d'une clé d'accès et les autorisations requises Le cluster ONTAP peut ainsi transférer les données inactives dans et depuis S3.
- Un connecteur installé sur un VPC AWS ou sur votre site.
- Mise en réseau pour le connecteur qui permet d'établir une connexion HTTPS sortante avec le cluster ONTAP, vers le stockage S3 et vers le service Cloud Tiering.

Configurer le Tiering

Dans Cloud Manager, sélectionnez un environnement de travail sur site, cliquez sur **Setup Tiering** et suivez les invites pour hiérarchiser les données vers Amazon S3.

Configuration des licences

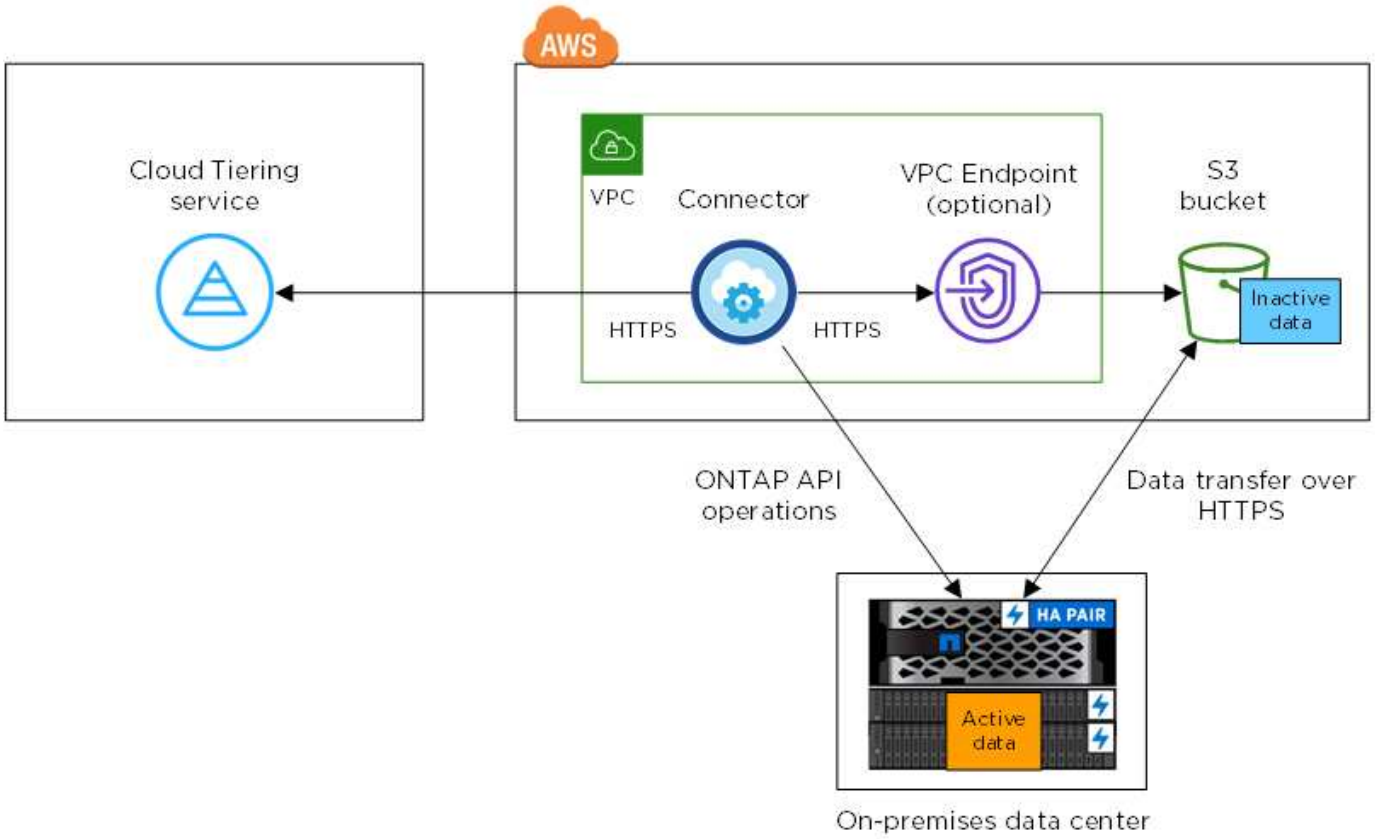
Après la fin de votre essai gratuit, payez pour Cloud Tiering par l'intermédiaire d'un abonnement avec paiement à l'utilisation, d'une licence de Tiering ONTAP ou d'une combinaison des deux :

- Pour vous abonner à AWS Marketplace, cliquez sur **Tiering > licences**, cliquez sur **Subscribe**, puis suivez les invites.
- Pour payer à l'aide d'une licence à plusieurs niveaux, contactez-nous si vous avez besoin d'en acheter une, puis "Ajoutez-le à votre cluster à partir de NetApp Cloud Tiering".

De formation

Vérifiez la prise en charge de votre cluster ONTAP, configurez votre réseau et préparez votre stockage objet.

L'image suivante montre chaque composant et les connexions que vous devez préparer entre eux :



La communication entre un connecteur et S3 est destinée uniquement à la configuration du stockage objet. Ce connecteur peut résider sur votre site au lieu de dans le cloud.

Préparation des clusters ONTAP

Lors du Tiering des données vers Amazon S3, vos clusters ONTAP doivent répondre aux exigences suivantes.

Plateformes ONTAP prises en charge

NetApp Cloud Tiering prend en charge les systèmes AFF ainsi que les agrégats 100 % SSD sur les systèmes FAS.

Version ONTAP prise en charge

ONTAP 9.2 ou version ultérieure

Configuration requise pour la mise en réseau des clusters

- Le cluster ONTAP établit une connexion HTTPS via le port 443 vers Amazon S3.

  Le ONTAP lit et écrit les données vers et à partir du stockage objet. Le stockage objet ne démarre jamais, il répond simplement.

  Bien qu'AWS Direct Connect offre de meilleures performances et des frais de transfert de données réduits, elle n'est pas requise entre le cluster ONTAP et S3. En effet, les performances sont de bien supérieures avec AWS Direct Connect, ce qui constitue la meilleure pratique recommandée.

- Une connexion entrante est requise depuis le connecteur, qui peut résider dans un VPC AWS ou sur votre site.

  Aucune connexion entre le cluster et le service Cloud Tiering n'est requise.

- Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge des volumes hiérarchisés. La LIF doit être associée au *IPspace* que ONTAP doit utiliser pour se connecter au stockage objet.

  Les IPspaces permettent la ségrégation du trafic réseau. Vous pouvez ainsi séparer le trafic client pour préserver votre confidentialité et votre sécurité. "En savoir plus sur les IPspaces".

  Lorsque vous configurez le Tiering des données, Cloud Tiering vous invite à utiliser l'IPspace. Vous devez choisir l'IPspace auquel chaque LIF est associée. Il peut s'agir de l'IPspace par défaut ou d'un IPspace personnalisé que vous avez créé.

Volumes et agrégats pris en charge

Le nombre total de volumes que vous pouvez effectuer le Tiering dans Cloud Tiering peut être inférieur au nombre de volumes sur votre système ONTAP. En effet, certains volumes ne peuvent pas être hiérarchisés à partir de certains agrégats. Par exemple, vous ne pouvez pas hiérarchiser les données depuis les volumes SnapLock ou depuis les configurations MetroCluster. Consultez la documentation ONTAP pour "Fonctionnalité ou fonctionnalités non prises en charge par FabricPool".

NetApp Cloud Tiering prend en charge les volumes FlexGroup, à partir de ONTAP 9.5. Le réglage fonctionne de la même façon que tout autre volume.

Création ou commutation de connecteurs

Un connecteur est nécessaire pour transférer les données vers le cloud. Lorsque vous effectuez le Tiering des données vers AWS S3, vous pouvez utiliser un connecteur dans un VPC AWS ou sur site. Vous devrez soit créer un nouveau connecteur, soit vérifier que le connecteur actuellement sélectionné réside dans AWS, soit sur site.

- "En savoir plus sur les connecteurs"
- "Création d'un connecteur dans AWS"
- "Exigences relatives à l'hôte de connecteur"
- "Installation du connecteur sur un hôte Linux existant"
- "Basculement entre les connecteurs"

Préparation de la mise en réseau pour le connecteur

Assurez-vous que le connecteur dispose des connexions réseau requises. Un connecteur peut être installé sur site ou dans AWS.

Étapes

1. Assurez-vous que le réseau sur lequel le connecteur est installé active les connexions suivantes :
   - Une connexion Internet sortante vers le service Cloud Tiering via le port 443 (HTTPS)
   - Une connexion HTTPS via le port 443 vers S3
   - Une connexion HTTPS via le port 443 vers vos clusters ONTAP
2. Si besoin, activez un terminal VPC sur S3.

   Un terminal VPC vers S3 est recommandé si vous disposez d'une connexion Direct Connect ou VPN entre le cluster ONTAP et le VPC, et que vous souhaitez communiquer entre le connecteur et S3 pour rester dans votre réseau AWS interne.

Préparation d'Amazon S3

Lorsque vous configurez le Tiering des données sur un nouveau cluster, vous êtes invité à créer un compartiment S3 ou à sélectionner un compartiment S3 existant dans le compte AWS où le connecteur est configuré.

Le compte AWS doit disposer d'autorisations et d'une clé d'accès que vous pouvez entrer dans Cloud Tiering. Le cluster ONTAP utilise la clé d'accès pour classer les données entrantes et sortantes de S3.

Étapes

1. Fournissez les autorisations suivantes à l'utilisateur IAM :

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetBucketLocation",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject"
```

   "Documentation AWS : création d'un rôle pour déléguer des autorisations à un utilisateur IAM"

2. Créez ou localisez une clé d'accès.

   NetApp Cloud Tiering transmet la clé d'accès au cluster ONTAP. Les identifiants ne sont pas stockés dans le service NetApp Cloud Tiering.

   "Documentation AWS : gestion des clés d'accès pour les utilisateurs IAM"

Tiering des données inactives de votre premier cluster vers Amazon S3

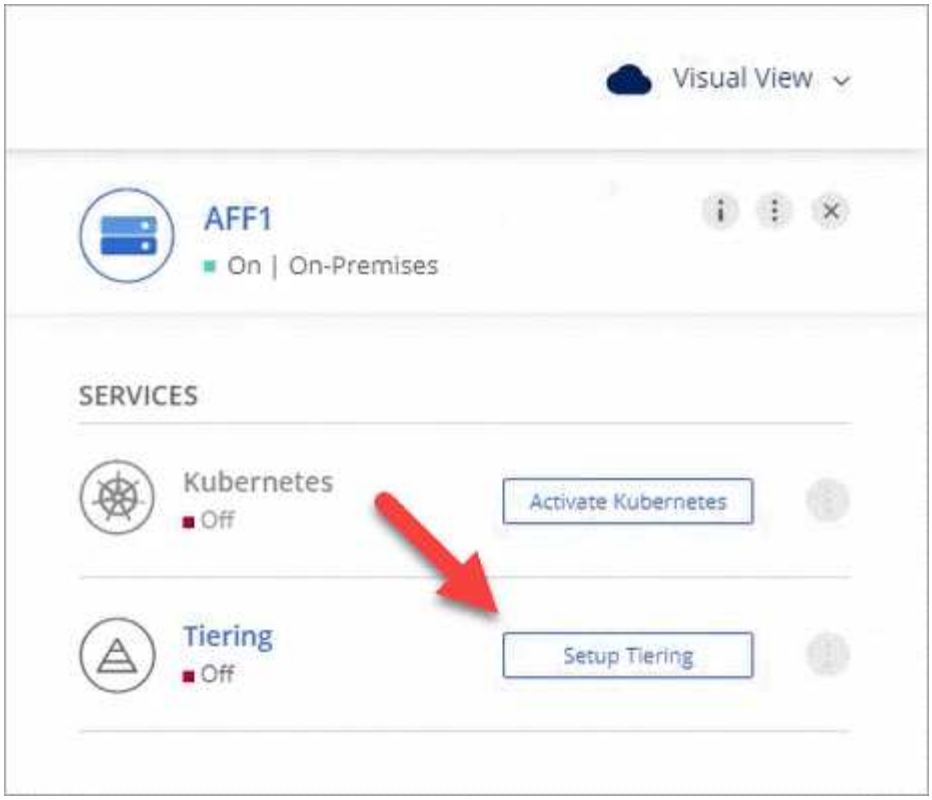
Une fois votre environnement AWS prêt, commencez le Tiering des données inactives à partir du premier cluster.

Ce dont vous avez besoin

- "Un environnement de travail sur site".
- Clé d'accès AWS pour un utilisateur IAM qui dispose des autorisations S3 requises.

Étapes

1. Sélectionnez un cluster sur site.
2. Cliquez sur **Configuration Tiering**.



Vous utilisez désormais le tableau de bord de Tiering.

3. Cliquez sur **configurer le Tiering** en regard du cluster.
4. Suivez les étapes de la page **Configuration de la hiérarchisation** :

   a. **Compartiment S3** : ajoutez un nouveau compartiment S3 ou sélectionnez un compartiment S3 existant commençant par le préfixe *fabric-pool* et cliquez sur **Continuer**.

      Le préfixe *fabric-pool* est requis car la stratégie IAM pour le connecteur permet à l'instance d'effectuer des actions S3 sur les compartiments nommés avec ce préfixe exact.

   Par exemple, vous pouvez nommer le compartiment S3 fabric-pool-AFF1, où AFF1 est le nom du cluster.

   a. **Classe de stockage** : sélectionnez la classe de stockage S3 à laquelle vous souhaitez transférer les données après 30 jours et cliquez sur **Continuer**.

      Si vous choisissez Standard, les données restent dans cette classe de stockage.

   b. **Informations d'identification** : saisissez l'ID de clé d'accès et la clé secrète pour un utilisateur IAM disposant des autorisations S3 requises.

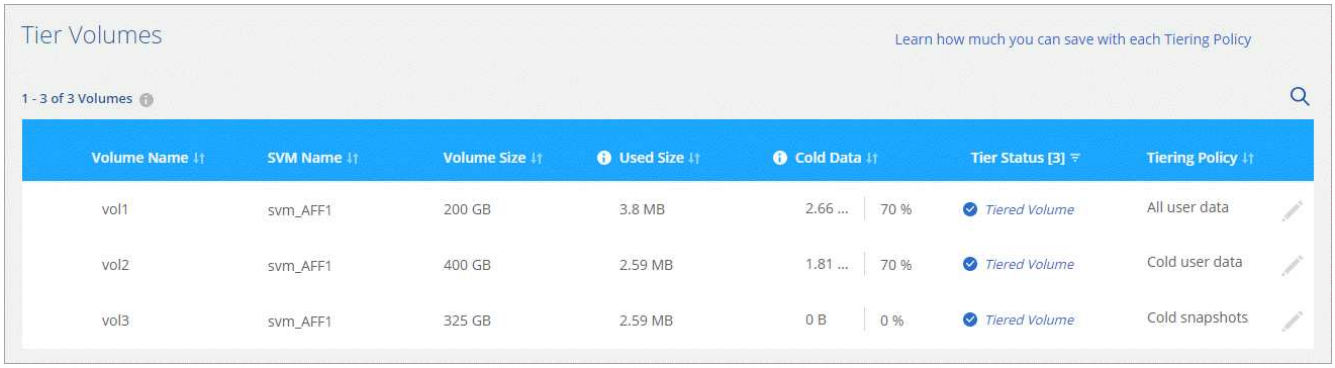
      L'utilisateur IAM doit se trouver dans le même compte AWS que le compartiment que vous avez sélectionné ou créé sur la page **compartiment S3**.

   c. **Cluster Network** : sélectionnez l'IPspace ONTAP à utiliser pour se connecter au stockage objet et cliquez sur **Continuer**.

      Le choix du bon IPspace garantit que Cloud Tiering peut établir une connexion de ONTAP au stockage objet de votre fournisseur cloud.

5. Cliquez sur **Continuer** pour sélectionner les volumes à mettre en niveau.
6. Sur la page **Tier volumes**, configurez le Tiering pour chaque volume. Cliquez sur le bouton Sélectionnez une stratégie de hiérarchisation, ajustez éventuellement les jours de refroidissement, puis cliquez sur **appliquer**.

   "En savoir plus sur les règles de Tiering des volumes".



Résultat

Vous avez configuré le Tiering des données à partir des volumes du cluster vers le stockage objet S3.

Et la suite ?

"Pensez à vous abonner au service NetApp Cloud Tiering".

Vous pouvez également ajouter des clusters ou consulter des informations sur les données actives et inactives sur le cluster. Pour plus de détails, voir "Gestion du Tiering des données à partir des clusters".

Tiering des données depuis les clusters ONTAP sur site vers le stockage Azure Blob

Libérez de l'espace sur vos clusters ONTAP sur site grâce au Tiering des données vers le stockage Azure Blob. Le Tiering des données est optimisé par le service NetApp Cloud Tiering.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

Préparez le Tiering des données vers le stockage Azure Blob

Il faut les éléments suivants :

- Un système AFF ou FAS doté d'agrégats 100 % SSD qui exécutent ONTAP 9.4 ou version ultérieure et qui dispose d'une connexion HTTPS vers le stockage Azure Blob.
- Un connecteur installé dans un Azure VNet.
- Mise en réseau d'un connecteur qui permet une connexion HTTPS sortante vers le cluster ONTAP du data Center, vers le stockage Azure Blob et vers le service NetApp Cloud Tiering.

Configurer le Tiering

Dans Cloud Manager, sélectionnez un environnement de travail sur site, cliquez sur **Setup Tiering** et suivez les invites pour hiérarchiser les données sur le stockage Azure Blob.

Configuration des licences

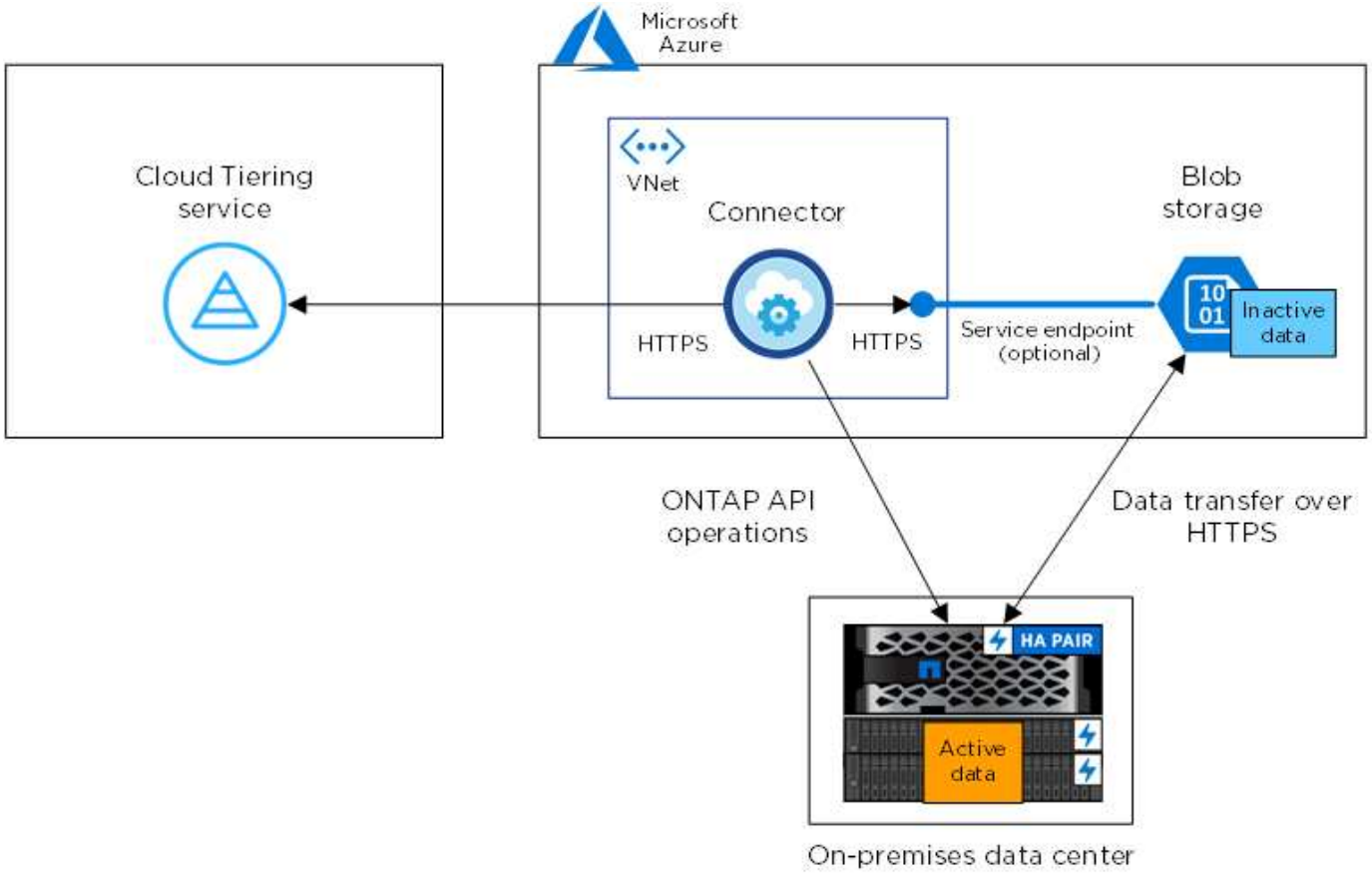
Après la fin de votre essai gratuit, payez pour Cloud Tiering par l'intermédiaire d'un abonnement avec paiement à l'utilisation, d'une licence de Tiering ONTAP ou d'une combinaison des deux :

- Pour vous abonner à Azure Marketplace, cliquez sur **Tiering > licences**, cliquez sur **Subscribe**, puis suivez les invites.
- Pour ajouter une licence de hiérarchisation, contactez-nous si vous devez en acheter une, puis "Ajoutez-le à votre cluster à partir de NetApp Cloud Tiering".

De formation

Vérifiez la prise en charge de votre cluster ONTAP, configurez votre réseau et préparez votre stockage objet.

L'image suivante montre chaque composant et les connexions que vous devez préparer entre eux :



La communication entre le connecteur et le stockage Blob est uniquement destinée à la configuration du stockage objet.

Préparation des clusters ONTAP

Lors du Tiering des données vers le stockage Azure Blob, vos clusters ONTAP doivent répondre aux exigences suivantes.

Plateformes ONTAP prises en charge

NetApp Cloud Tiering prend en charge les systèmes AFF ainsi que les agrégats 100 % SSD sur les systèmes FAS.

Version ONTAP prise en charge

ONTAP 9.4 ou version ultérieure

Configuration requise pour la mise en réseau des clusters

- Le cluster ONTAP établit une connexion HTTPS via le port 443 vers le stockage Azure Blob.

  Le ONTAP lit et écrit les données vers et à partir du stockage objet. Le stockage objet ne démarre jamais, il répond simplement.

  Bien qu'ExpressRoute offre de meilleures performances et des frais de transfert de données inférieurs, il n'est pas nécessaire d'avoir entre le cluster ONTAP et le stockage Azure Blob. Les performances étant considérablement meilleures après avoir utilisé ExpressRoute, il est conseillé de les utiliser.

- NetApp Service Connector, qui réside dans un vnet Azure, nécessite une connexion entrante.

  Aucune connexion entre le cluster et le service Cloud Tiering n'est requise.

- Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge des volumes hiérarchisés. La LIF doit être associée au *IPspace* que ONTAP doit utiliser pour se connecter au stockage objet.

  Les IPspaces permettent la ségrégation du trafic réseau. Vous pouvez ainsi séparer le trafic client pour préserver votre confidentialité et votre sécurité. "En savoir plus sur les IPspaces".

  Lorsque vous configurez le Tiering des données, Cloud Tiering vous invite à utiliser l'IPspace. Vous devez choisir l'IPspace auquel chaque LIF est associée. Il peut s'agir de l'IPspace par défaut ou d'un IPspace personnalisé que vous avez créé.

Volumes et agrégats pris en charge

Le nombre total de volumes que vous pouvez effectuer le Tiering dans Cloud Tiering peut être inférieur au nombre de volumes sur votre système ONTAP. En effet, certains volumes ne peuvent pas être hiérarchisés à partir de certains agrégats. Par exemple, vous ne pouvez pas hiérarchiser les données depuis les volumes SnapLock ou depuis les configurations MetroCluster. Consultez la documentation ONTAP pour "Fonctionnalité ou fonctionnalités non prises en charge par FabricPool".

NetApp Cloud Tiering prend en charge les volumes FlexGroup, à partir de ONTAP 9.5. Le réglage fonctionne de la même façon que tout autre volume.

Création ou commutation de connecteurs

Un connecteur est nécessaire pour transférer les données vers le cloud. Lors du Tiering des données vers le stockage Azure Blob, un connecteur doit être disponible dans un vnet Azure. Vous devrez soit créer un nouveau connecteur, soit vérifier que le connecteur actuellement sélectionné réside dans Azure.

- "En savoir plus sur les connecteurs"

- "Création d’un connecteur dans Azure"
- "Basculement entre les connecteurs"

Préparation de la mise en réseau pour le connecteur

Assurez-vous que le connecteur dispose des connexions réseau requises.

Étapes

1. S’assurer que le vnet où le connecteur est installé active les connexions suivantes :
   - Une connexion Internet sortante vers le service Cloud Tiering via le port 443 (HTTPS)
   - Une connexion HTTPS via le port 443 vers le stockage Azure Blob
   - Une connexion HTTPS via le port 443 vers vos clusters ONTAP
2. Si nécessaire, activez un terminal du service VNet sur le stockage Azure.

   Un point de terminaison du service VNet pour le stockage Azure est recommandé si vous disposez d’une connexion ExpressRoute ou VPN entre le cluster ONTAP et le vnet et que vous souhaitez que la communication entre le connecteur et le stockage Blob reste sur votre réseau privé virtuel.

Tiering des données inactives de votre premier cluster vers le stockage Azure Blob

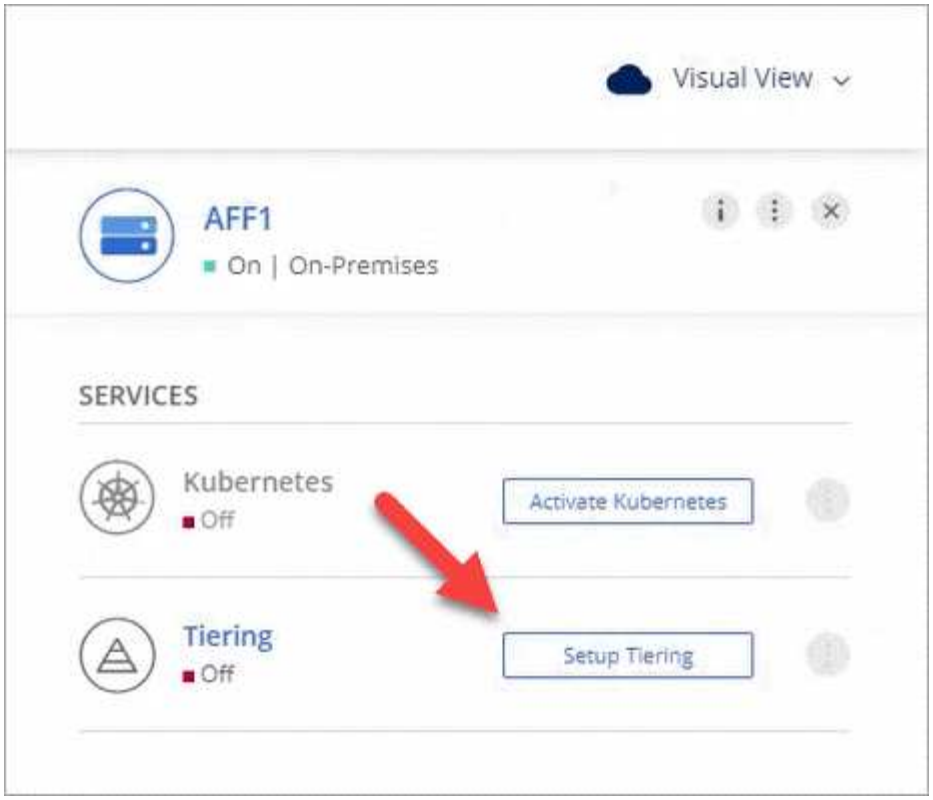
Une fois votre environnement Azure prêt, commencez le Tiering des données inactives à partir du premier cluster.

Ce dont vous avez besoin

"Un environnement de travail sur site".

Étapes

1. Sélectionnez un cluster sur site.
2. Cliquez sur **Configuration Tiering**.



Vous utilisez désormais le tableau de bord de Tiering.

3. Cliquez sur **configurer le Tiering** en regard du cluster.
4. Suivez les étapes de la page **Configuration de la hiérarchisation** :
   a. **Groupe de ressources** : sélectionnez un groupe de ressources dans lequel un conteneur existant est géré ou où vous souhaitez créer un nouveau conteneur pour les données hiérarchisées.
   b. **Conteneur Azure** : ajoutez un nouveau conteneur Blob à un compte de stockage ou sélectionnez un conteneur existant et cliquez sur **Continuer**.

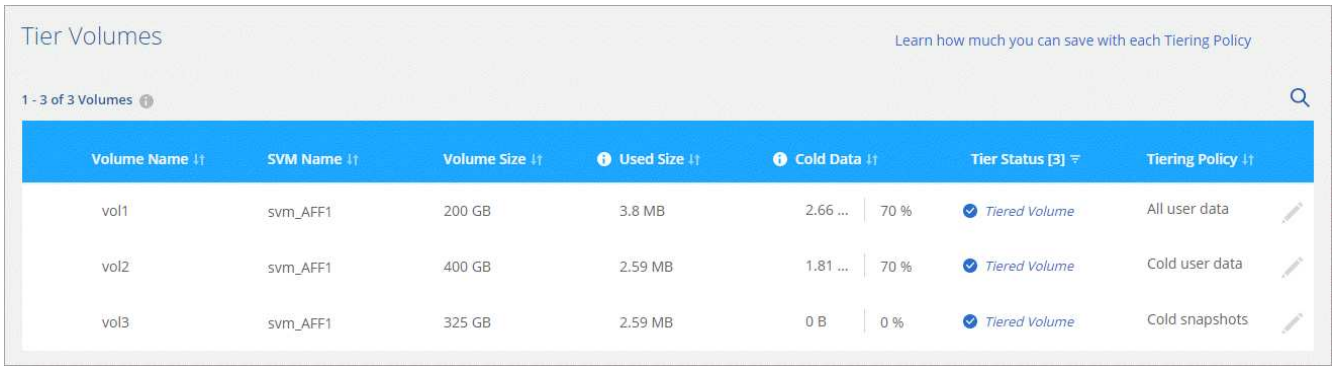
      Le compte de stockage et les conteneurs qui apparaissent à cette étape appartiennent au groupe de ressources que vous avez sélectionné à l'étape précédente.

   c. **Access Tier** : sélectionnez le niveau d'accès que vous souhaitez utiliser pour les données hiérarchisées et cliquez sur **Continuer**.
   d. **Cluster Network** : sélectionnez l'IPspace ONTAP à utiliser pour se connecter au stockage objet et cliquez sur **Continuer**.

      Le choix du bon IPspace garantit que Cloud Tiering peut établir une connexion de ONTAP au stockage objet de votre fournisseur cloud.

5. Cliquez sur **Continuer** pour sélectionner les volumes à mettre en niveau.
6. Sur la page **Tier volumes**, configurez le Tiering pour chaque volume. Cliquez sur le bouton Sélectionnez une stratégie de hiérarchisation, ajustez éventuellement les jours de refroidissement, puis cliquez sur **appliquer**.

   "En savoir plus sur les règles de Tiering des volumes".



Résultat

Vous avez configuré le Tiering des données depuis les volumes du cluster vers le stockage objet Azure Blob.

Et la suite ?

"Pensez à vous abonner au service NetApp Cloud Tiering".

Vous pouvez également ajouter des clusters ou consulter des informations sur les données actives et inactives sur le cluster. Pour plus de détails, voir "Gestion du Tiering des données à partir des clusters".

Tiering des données depuis des clusters ONTAP sur site vers Google Cloud Storage

Libérez de l'espace sur vos clusters ONTAP sur site grâce au Tiering des données vers Google Cloud Storage. Le Tiering des données est optimisé par le service NetApp Cloud Tiering.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

1 Préparez-vous au Tiering des données vers Google Cloud Storage

Il faut les éléments suivants :

- Un système AFF ou FAS doté d'agrégats 100 % SSD qui exécutent ONTAP 9.6 ou une version ultérieure et qui bénéficie d'une connexion HTTPS vers Google Cloud Storage.
- Un compte de service avec le rôle d'administrateur du stockage et les clés d'accès au stockage prédéfinis.
- Connecteur installé dans un VPC Google Cloud Platform.
- Mise en réseau pour le connecteur qui permet une connexion HTTPS sortante vers le cluster ONTAP du data Center, vers Google Cloud Storage et vers le service Cloud Tiering.

2 Configurer le Tiering

Dans Cloud Manager, sélectionnez un environnement de travail sur site, cliquez sur **Setup Tiering** et suivez les invites pour transférer les données vers Google Cloud Storage.

Configuration des licences

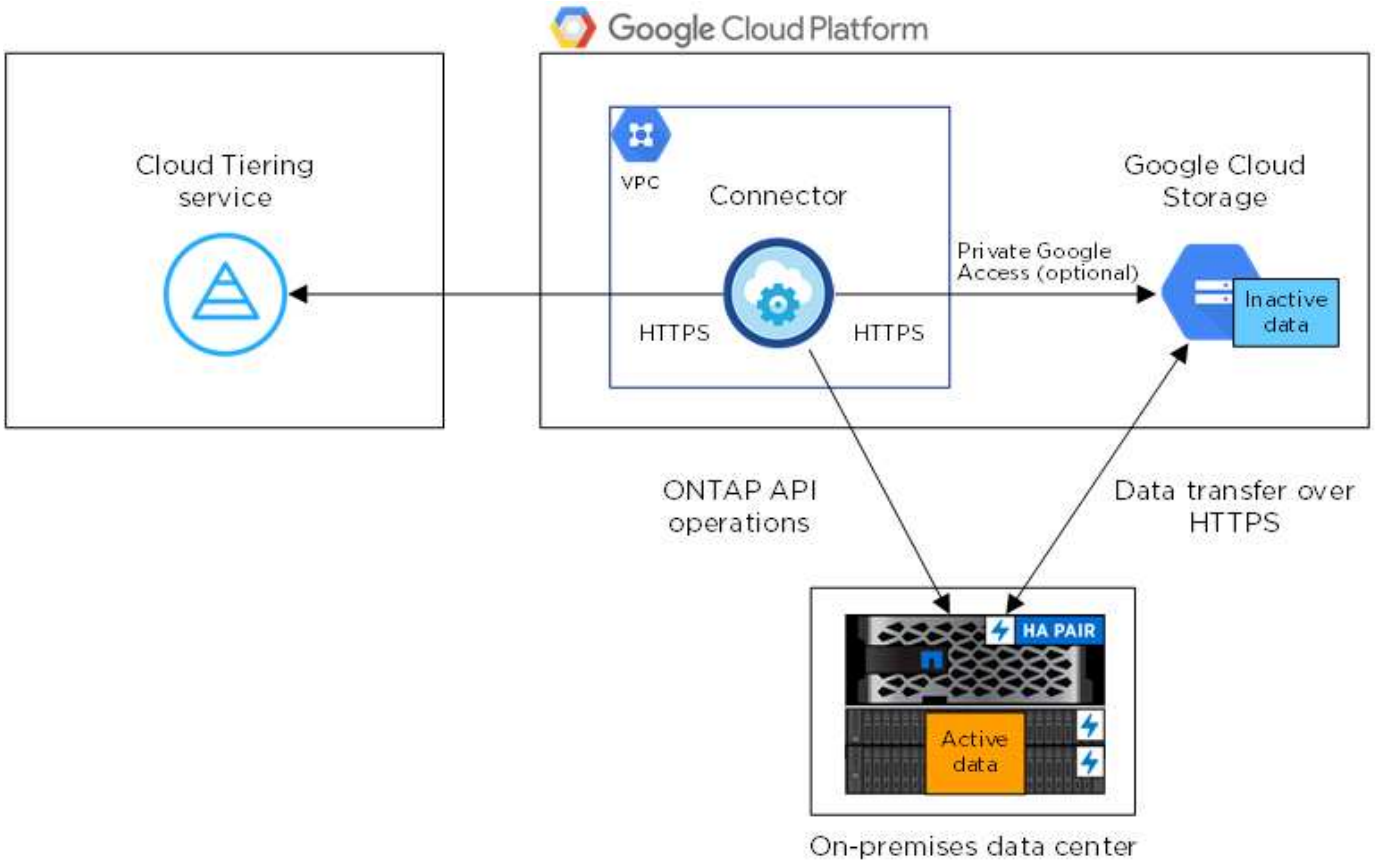
Après la fin de votre essai gratuit, payez pour Cloud Tiering par l'intermédiaire d'un abonnement avec paiement à l'utilisation, d'une licence de Tiering ONTAP ou d'une combinaison des deux :

- Pour vous abonner à GCP Marketplace, cliquez sur **Tiering > licences**, cliquez sur **Abonnez-vous**, puis suivez les invites.
- Pour ajouter une licence de hiérarchisation, contactez-nous si vous devez en acheter une, puis "Ajoutez-le à votre cluster à partir de NetApp Cloud Tiering".

De formation

Vérifiez la prise en charge de votre cluster ONTAP, configurez votre réseau et préparez votre stockage objet.

L'image suivante montre chaque composant et les connexions que vous devez préparer entre eux :



La communication entre le connecteur et Google Cloud Storage est destinée uniquement à la configuration du stockage objet.

Préparation des clusters ONTAP

Lors du Tiering des données vers Google Cloud Storage, vos clusters ONTAP doivent répondre aux exigences suivantes.

Plateformes ONTAP prises en charge

NetApp Cloud Tiering prend en charge les systèmes AFF ainsi que les agrégats 100 % SSD sur les systèmes FAS.

Versions de ONTAP prises en charge

ONTAP 9.6 ou version ultérieure

Configuration requise pour la mise en réseau des clusters

- Le cluster ONTAP établit une connexion HTTPS via le port 443 vers Google Cloud Storage.

  Le ONTAP lit et écrit les données vers et à partir du stockage objet. Le stockage objet ne démarre jamais, il répond simplement.

  Même si une interconnexion Google Cloud permet d'améliorer les performances et de réduire les frais de transfert de données, elle n'est pas requise entre le cluster ONTAP et Google Cloud Storage. Puisque les performances sont largement supérieures lorsque vous utilisez Google Cloud Interconnect, cette pratique est recommandée.

- NetApp Service Connector, qui réside dans un VPC Google Cloud Platform, nécessite une connexion entrante.

  Aucune connexion entre le cluster et le service Cloud Tiering n'est requise.

- Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge des volumes hiérarchisés. La LIF doit être associée au *IPspace* que ONTAP doit utiliser pour se connecter au stockage objet.

  Les IPspaces permettent la ségrégation du trafic réseau. Vous pouvez ainsi séparer le trafic client pour préserver votre confidentialité et votre sécurité. "En savoir plus sur les IPspaces".

  Lorsque vous configurez le Tiering des données, Cloud Tiering vous invite à utiliser l'IPspace. Vous devez choisir l'IPspace auquel chaque LIF est associée. Il peut s'agir de l'IPspace par défaut ou d'un IPspace personnalisé que vous avez créé.

Volumes et agrégats pris en charge

Le nombre total de volumes que vous pouvez effectuer le Tiering dans Cloud Tiering peut être inférieur au nombre de volumes sur votre système ONTAP. En effet, certains volumes ne peuvent pas être hiérarchisés à partir de certains agrégats. Par exemple, vous ne pouvez pas hiérarchiser les données depuis les volumes SnapLock ou depuis les configurations MetroCluster. Consultez la documentation ONTAP pour "Fonctionnalité ou fonctionnalités non prises en charge par FabricPool".

NetApp Cloud Tiering prend en charge les volumes FlexGroup. Le réglage fonctionne de la même façon que tout autre volume.

Création ou commutation de connecteurs

Un connecteur est nécessaire pour transférer les données vers le cloud. Pour le Tiering des données vers Google Cloud Storage, un connecteur doit être disponible dans un VPC Google Cloud Platform. Vous devrez soit créer un nouveau connecteur, soit vérifier que le connecteur actuellement sélectionné réside dans GCP.

- "En savoir plus sur les connecteurs"
- "Création d'un connecteur dans GCP"
- "Basculement entre les connecteurs"

Préparation de la mise en réseau pour le connecteur

Assurez-vous que le connecteur dispose des connexions réseau requises.

Étapes

1. Assurez-vous que le VPC où le connecteur est installé active les connexions suivantes :
   - Une connexion Internet sortante vers le service Cloud Tiering via le port 443 (HTTPS)
   - Une connexion HTTPS via le port 443 vers Google Cloud Storage
   - Une connexion HTTPS via le port 443 vers vos clusters ONTAP
2. Facultatif : activez l'accès privé Google sur le sous-réseau où vous prévoyez de déployer le connecteur de service.

   "Accès privé à Google" Est recommandé si vous disposez d'une connexion directe entre le cluster ONTAP et le VPC et que vous souhaitez maintenir une communication entre le connecteur et Google Cloud Storage dans votre réseau privé virtuel. Notez que Private Google Access fonctionne avec des instances de VM possédant uniquement des adresses IP internes (privées) (pas d'adresses IP externes).

Préparer le Tiering des données avec Google Cloud Storage

Lorsque vous configurez la hiérarchisation, vous devez fournir des clés d'accès au stockage pour un compte de service avec des autorisations d'administrateur du stockage. Un compte de service permet à NetApp Cloud Tiering d'authentifier et d'accéder aux compartiments de stockage cloud utilisés pour le Tiering des données. Les clés sont requises pour que Google Cloud Storage sache qui effectue la demande.

Étapes

1. "Créez un compte de service avec le rôle d'administrateur de stockage prédéfini".
2. Accédez à "Paramètres de stockage GCP" et créez des clés d'accès pour le compte de service :
   a. Sélectionnez un projet et cliquez sur **interopérabilité**. Si ce n'est déjà fait, cliquez sur **Activer l'accès à l'interopérabilité**.
   b. Sous **clés d'accès pour les comptes de service**, cliquez sur **Créer une clé pour un compte de service**, sélectionnez le compte de service que vous venez de créer, puis cliquez sur **Créer une clé**.

      Vous devez le faire "Entrez les clés dans NetApp Cloud Tiering" plus tard lorsque vous avez configuré le tiering.

Tiering des données inactives de votre premier cluster vers Google Cloud Storage

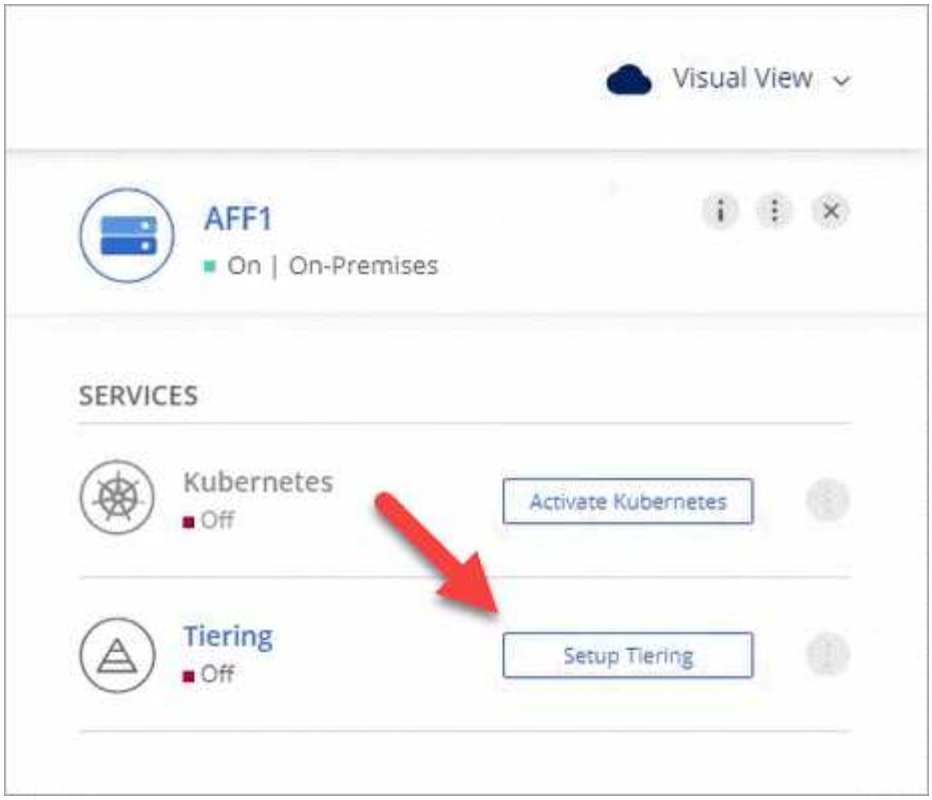
Une fois votre environnement Google Cloud prêt, commencez le Tiering des données inactives à partir du premier cluster.

Ce dont vous avez besoin

- "Un environnement de travail sur site".
- Clés d'accès au stockage pour un compte de service disposant du rôle d'administrateur du stockage.

Étapes

1. Sélectionnez un cluster sur site.
2. Cliquez sur **Configuration Tiering**.

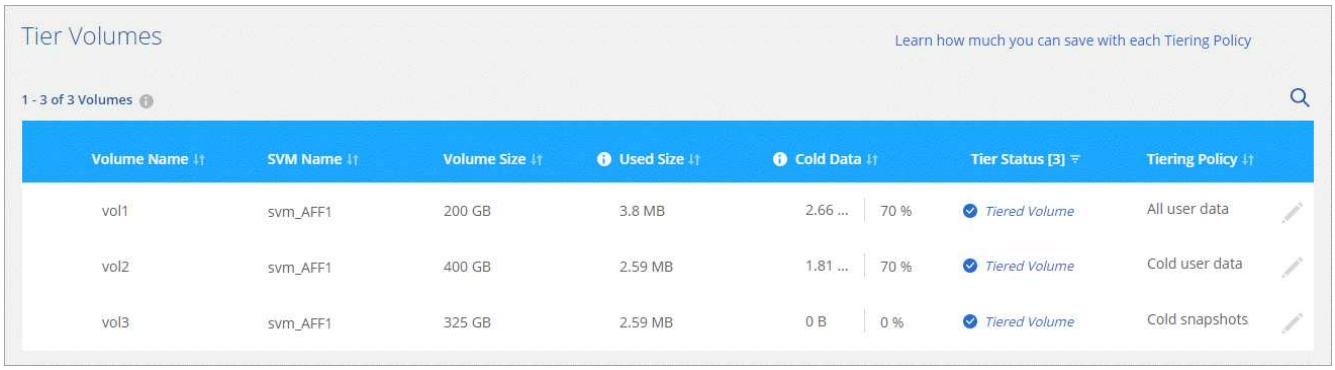


Vous utilisez désormais le tableau de bord de Tiering.

3. Cliquez sur **configurer le Tiering** en regard du cluster.
4. Suivez les étapes de la page **Configuration de la hiérarchisation** :
   a. **Compartiment** : ajoutez un nouveau compartiment Google Cloud Storage ou sélectionnez un compartiment existant et cliquez sur **Continuer**.
   b. **Classe de stockage** : sélectionnez la classe de stockage à utiliser pour les données à plusieurs niveaux et cliquez sur **Continuer**.
   c. **Informations d'identification** : saisissez la clé d'accès au stockage et la clé secrète pour un compte de service qui a le rôle d'administrateur du stockage.
   d. **Cluster Network** : sélectionnez l'IPspace ONTAP à utiliser pour se connecter au stockage objet et cliquez sur **Continuer**.

      Le choix du bon IPspace garantit que Cloud Tiering peut établir une connexion de ONTAP au stockage objet de votre fournisseur cloud.
5. Cliquez sur **Continuer** pour sélectionner les volumes à mettre en niveau.
6. Sur la page **Tier volumes**, configurez le Tiering pour chaque volume. Cliquez sur le bouton Sélectionnez une stratégie de hiérarchisation, ajustez éventuellement les jours de refroidissement, puis cliquez sur **appliquer**.

   "En savoir plus sur les règles de Tiering des volumes".



Résultat

Vous avez configuré le Tiering des données depuis les volumes du cluster vers le stockage objet Google Cloud.

Et la suite ?

"Pensez à vous abonner au service NetApp Cloud Tiering".

Vous pouvez également ajouter des clusters ou consulter des informations sur les données actives et inactives sur le cluster. Pour plus de détails, voir "Gestion du Tiering des données à partir des clusters".

Tiering des données depuis des clusters ONTAP sur site vers StorageGRID

Libérez de l'espace sur vos clusters ONTAP sur site grâce au Tiering des données vers StorageGRID. Le Tiering des données est optimisé par le service NetApp Cloud Tiering.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

1 Préparation au Tiering des données vers StorageGRID

Il faut les éléments suivants :

- Un système AFF ou FAS avec des agrégats 100 % SSD qui exécutent ONTAP 9.4 ou une version ultérieure et une connexion via un port spécifié par l'utilisateur vers StorageGRID.
- StorageGRID 10.3 ou version ultérieure avec les clés d'accès AWS qui disposent d'autorisations S3.
- Un connecteur installé sur votre site.
- Mise en réseau du connecteur qui permet d'établir une connexion HTTPS sortante avec le cluster ONTAP, vers StorageGRID et vers le service Cloud Tiering.

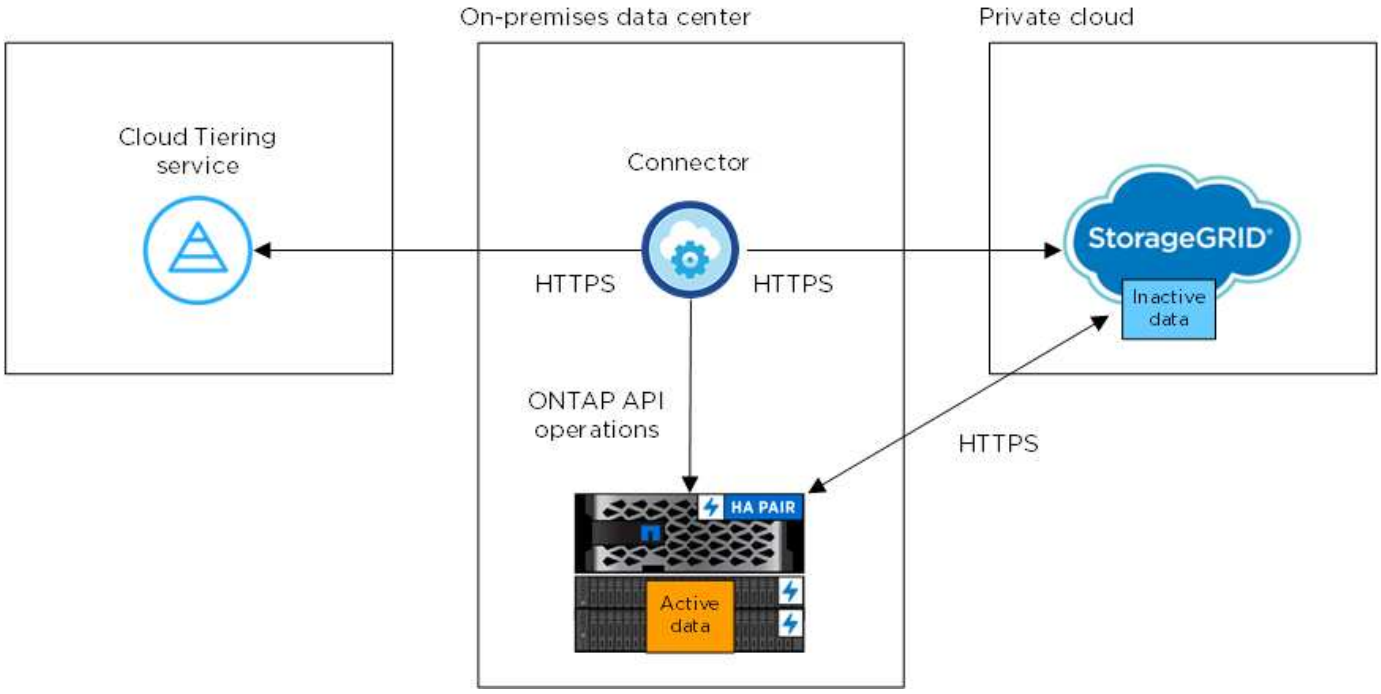
2 Configurer le Tiering

Sélectionnez un environnement de travail sur site, cliquez sur **Setup Tiering** et suivez les invites pour hiérarchiser les données dans StorageGRID.

De formation

Vérifiez la prise en charge de votre cluster ONTAP, configurez votre réseau et préparez votre stockage objet.

L'image suivante montre chaque composant et les connexions que vous devez préparer entre eux :



La communication entre le connecteur et l'StorageGRID est destinée uniquement à la configuration du stockage objet.

Préparation des clusters ONTAP

Lors du Tiering des données vers StorageGRID, vos clusters ONTAP doivent répondre aux exigences suivantes.

Plateformes ONTAP prises en charge

NetApp Cloud Tiering prend en charge les systèmes AFF ainsi que les agrégats 100 % SSD sur les systèmes FAS.

Version ONTAP prise en charge

ONTAP 9.4 ou version ultérieure

Licences

Une licence FabricPool n'est pas requise sur le cluster ONTAP lors du Tiering des données vers StorageGRID.

Configuration requise pour la mise en réseau des clusters

- Le cluster ONTAP établit une connexion HTTPS vers StorageGRID via un port spécifié par l'utilisateur (le port est configurable lors de la configuration du Tiering).

  Le ONTAP lit et écrit les données vers et à partir du stockage objet. Le stockage objet ne démarre jamais, il répond simplement.

- Une connexion entrante est requise à partir du connecteur, qui doit résider dans vos locaux.

  Aucune connexion entre le cluster et le service Cloud Tiering n'est requise.

- Un LIF intercluster est nécessaire sur chaque nœud ONTAP qui héberge des volumes hiérarchisés. La LIF doit être associée au *IPspace* que ONTAP doit utiliser pour se connecter au stockage objet.

  Les IPspaces permettent la ségrégation du trafic réseau. Vous pouvez ainsi séparer le trafic client pour préserver votre confidentialité et votre sécurité. "En savoir plus sur les IPspaces".

  Lorsque vous configurez le Tiering des données, Cloud Tiering vous invite à utiliser l'IPspace. Vous devez choisir l'IPspace auquel chaque LIF est associée. Il peut s'agir de l'IPspace par défaut ou d'un IPspace personnalisé que vous avez créé.

Volumes et agrégats pris en charge

Le nombre total de volumes que vous pouvez effectuer le Tiering dans Cloud Tiering peut être inférieur au nombre de volumes sur votre système ONTAP. En effet, certains volumes ne peuvent pas être hiérarchisés à partir de certains agrégats. Par exemple, vous ne pouvez pas hiérarchiser les données depuis les volumes SnapLock ou depuis les configurations MetroCluster. Consultez la documentation ONTAP pour "Fonctionnalité ou fonctionnalités non prises en charge par FabricPool".

NetApp Cloud Tiering prend en charge les volumes FlexGroup, à partir de ONTAP 9.5. Le réglage fonctionne de la même façon que tout autre volume.

Préparation de StorageGRID

StorageGRID doit remplir les conditions suivantes.

Versions de StorageGRID prises en charge

StorageGRID 10.3 et versions ultérieures sont prises en charge.

Identifiants S3

Lorsque vous configurez le Tiering dans StorageGRID, vous devez fournir un Tiering dans le cloud avec une clé d'accès S3 et une clé secrète. NetApp Cloud Tiering utilise les clés pour accéder à vos compartiments.

Ces clés d'accès doivent être associées à un utilisateur disposant des autorisations suivantes :

```
"s3:ListAllMyBuckets",
"s3:ListBucket",
"s3:GetObject",
"s3:PutObject",
"s3:DeleteObject",
"s3:CreateBucket"
```

Gestion des versions d'objet

Vous ne devez pas activer la gestion des versions d'objets StorageGRID sur le compartiment de magasin d'objets.

Création ou commutation de connecteurs

Un connecteur est nécessaire pour transférer les données vers le cloud. Pour le Tiering des données vers StorageGRID, un connecteur doit être disponible sur site. Vous devrez soit installer un nouveau connecteur, soit vérifier que le connecteur actuellement sélectionné réside sur site.

- "En savoir plus sur les connecteurs"
- "Exigences relatives à l'hôte de connecteur"
- "Installation du connecteur sur un hôte Linux existant"
- "Basculement entre les connecteurs"

Préparation de la mise en réseau pour le connecteur

Assurez-vous que le connecteur dispose des connexions réseau requises.

Étapes

1. Assurez-vous que le réseau sur lequel le connecteur est installé active les connexions suivantes :
    - Une connexion Internet sortante vers le service Cloud Tiering via le port 443 (HTTPS)
    - Une connexion HTTPS via le port 443 vers StorageGRID
    - Une connexion HTTPS via le port 443 vers vos clusters ONTAP

Tiering des données inactives de votre premier cluster vers StorageGRID

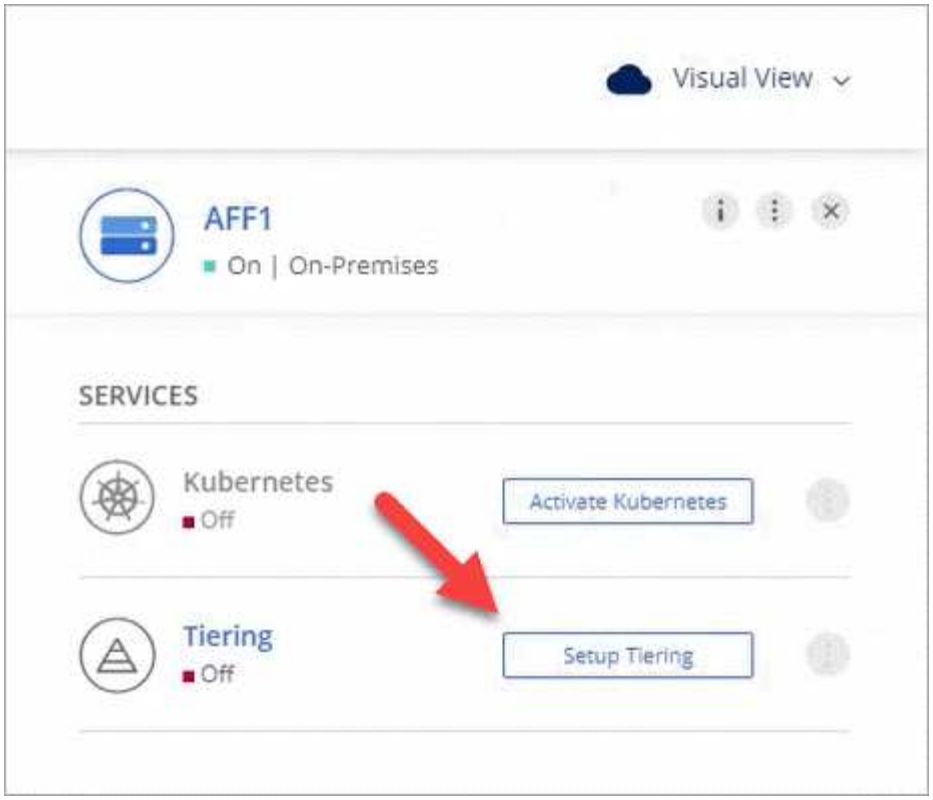
Une fois votre environnement prêt, commencez le Tiering des données inactives à partir du premier cluster.

Ce dont vous avez besoin

- "Un environnement de travail sur site".
- Clé d'accès AWS qui dispose des autorisations S3 requises.

Étapes

1. Sélectionnez un cluster sur site.
2. Cliquez sur **Configuration Tiering**.

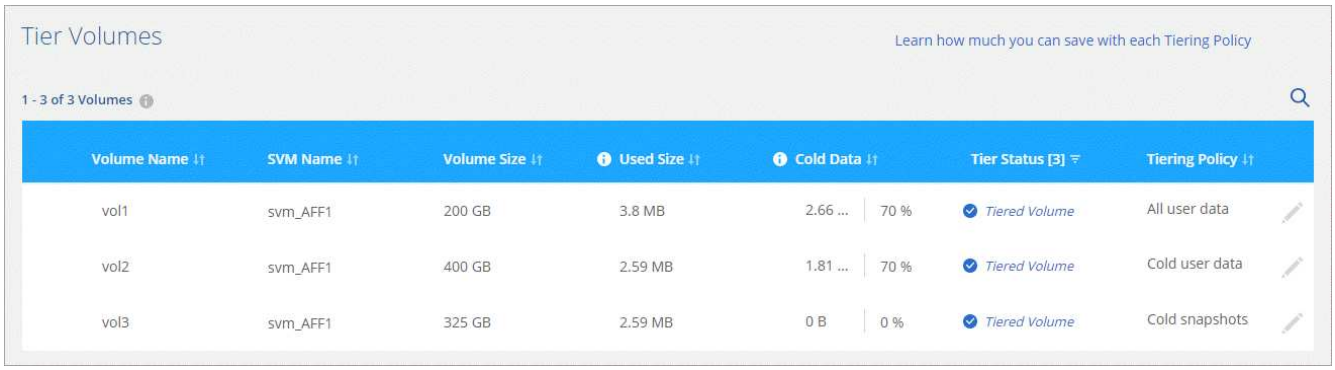


Vous utilisez désormais le tableau de bord de Tiering.

3. Cliquez sur **configurer le Tiering** en regard du cluster.
4. Suivez les étapes de la page **Configuration de la hiérarchisation** :
   a. **Choisissez votre fournisseur**: Sélectionnez StorageGRID.
   b. **Serveur** : saisissez le FQDN du serveur StorageGRID, entrez le port que ONTAP doit utiliser pour la communication HTTPS avec StorageGRID, et entrez la clé d'accès et la clé secrète pour un compte AWS disposant des autorisations S3 requises.
   c. **Godet** : ajoutez un nouveau compartiment ou sélectionnez un compartiment existant pour les données à plusieurs niveaux.
   d. **Cluster Network** : sélectionnez l'IPspace ONTAP à utiliser pour se connecter au stockage objet et cliquez sur **Continuer**.

      Le choix du bon IPspace garantit que Cloud Tiering peut établir une connexion de ONTAP au stockage objet de votre fournisseur cloud.
5. Cliquez sur **Continuer** pour sélectionner les volumes à mettre en niveau.
6. Sur la page **Tier volumes**, configurez le Tiering pour chaque volume. Cliquez sur le bouton Sélectionnez une stratégie de hiérarchisation, ajustez éventuellement les jours de refroidissement, puis cliquez sur **appliquer**.

   "En savoir plus sur les règles de Tiering des volumes".



Résultat

Vous avez configuré le Tiering des données depuis les volumes du cluster vers StorageGRID.

Et la suite ?

Vous pouvez ajouter des clusters supplémentaires ou consulter des informations sur les données actives et inactives sur le cluster. Pour plus de détails, voir "Gestion du Tiering des données à partir des clusters".

Configuration des licences pour NetApp Cloud Tiering

Payez pour le Tiering dans le cloud via un abonnement avec paiement basé sur l'utilisation, une licence de Tiering ONTAP appelée *FabricPool*, ou une combinaison des deux. Si vous optez pour un paiement basé sur l'utilisation, vous devez vous abonner au fournisseur cloud pour lequel vous voulez transférer les données inactives. Vous n'avez pas besoin d'vous abonner sur tous les marchés.

Quelques remarques avant de lire plus loin :

- Si une licence FabricPool est déjà installée sur votre cluster, alors vous êtes tous définis : rien d'autre que vous devez faire.
- Si vous êtes déjà abonné à Cloud Manager dans le Marketplace de votre fournisseur cloud, vous êtes automatiquement abonné à Cloud Tiering. Un abonnement actif s'affiche dans l'onglet Cloud Tiering **Licensing**. Vous n'aurez pas besoin de vous abonner à nouveau.
- Le Tiering des données vers StorageGRID n'est pas payant. Une licence BYOL ou un enregistrement PAYGO ne sont pas nécessaires.

"En savoir plus sur le fonctionnement des licences pour Cloud Tiering".

Abonnement sur AWS Marketplace

Abonnez-vous à Cloud Tiering depuis AWS Marketplace pour configurer un abonnement avec paiement à l'utilisation pour le Tiering des données depuis les clusters ONTAP vers AWS S3.

Étapes

1. Dans Cloud Manager, cliquez sur **Tiering > licences**.
2. Cliquez sur **Subscribe** sous AWS Marketplace, puis sur **Continuer**.
3. Abonnez-vous à partir d'AWS Marketplace, puis connectez-vous à Cloud Central pour terminer votre inscription.

La vidéo suivante montre le processus :

► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_aws_tiering.mp4 *(video)*

Abonnement depuis Azure Marketplace

Abonnez-vous à NetApp Cloud Tiering depuis Azure Marketplace pour configurer un abonnement avec paiement à l'utilisation pour le Tiering des données depuis les clusters ONTAP vers le stockage Azure Blob.

Étapes

1. Dans Cloud Manager, cliquez sur **Tiering > licences**.
2. Cliquez sur **Subscribe** sous Azure Marketplace, puis cliquez sur **Continuer**.
3. Abonnez-vous à partir d'Azure Marketplace, puis connectez-vous à Cloud Central pour terminer votre inscription.

   La vidéo suivante montre le processus :

   ► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_azure_tiering.mp4 *(video)*

Abonnement depuis GCP Marketplace

Abonnez-vous à Cloud Tiering depuis GCP Marketplace pour configurer un abonnement avec paiement à l'utilisation pour le Tiering des données depuis les clusters ONTAP vers du stockage Google Cloud.

Étapes

1. Dans Cloud Manager, cliquez sur **Tiering > licences**.
2. Cliquez sur **Subscribe** sous GCP Marketplace, puis cliquez sur **Continuer**.
3. Abonnez-vous à partir de GCP Marketplace, puis connectez-vous à Cloud Central pour terminer l'inscription.

   la vidéo suivante présente le processus :

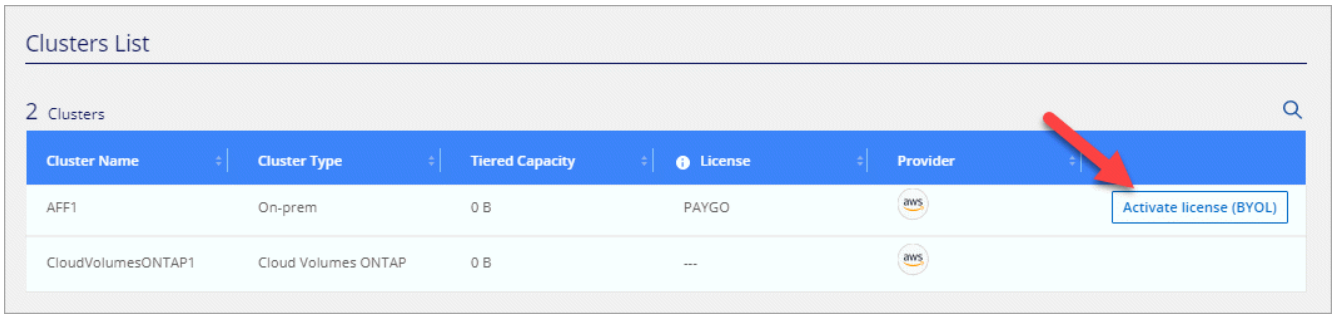
   ► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_gcp_tiering.mp4 *(video)*

Ajout d'une licence à plusieurs niveaux à ONTAP

Bring your own license (BYOL) en achetant une licence ONTAP FabricPool.

Étapes

1. Si vous n'avez pas de licence FabricPool, contactez-nous pour en acheter un.
2. Dans Cloud Manager, cliquez sur **Tiering > licences**.
3. Dans le tableau liste des clusters, cliquez sur **Activer la licence (BYOL)** pour un cluster ONTAP sur site.



4. Saisissez le numéro de série de la licence, puis saisissez le compte du site de support NetApp associé au numéro de série.
5. Cliquez sur **Activer la licence**.

Résultat

Cloud Tiering enregistre la licence et l'installe sur le cluster.

Une fois que vous avez terminé

Si vous achetez davantage de capacité d'extension ultérieurement, la licence sur le cluster est automatiquement mise à jour avec la nouvelle capacité. Il n'est pas nécessaire d'appliquer un nouveau fichier de licence NetApp au cluster.

Gestion du Tiering des données à partir des clusters

Maintenant que vous avez configuré le Tiering des données à partir de vos clusters ONTAP, vous pouvez procéder au Tiering des données à partir de volumes supplémentaires, modifier la règle de Tiering d'un volume, etc.

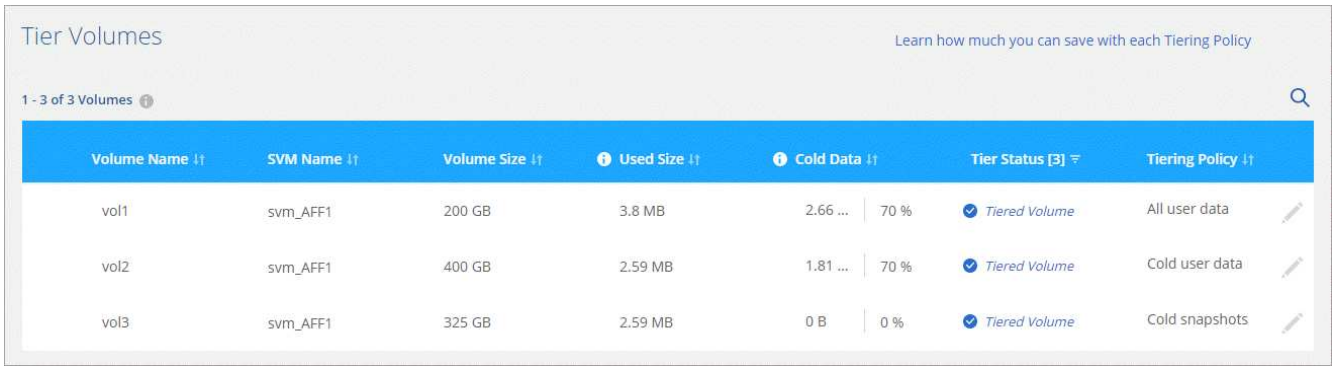
Tiering des données à partir de volumes supplémentaires

Configurez un Tiering pour des volumes supplémentaires à tout moment, par exemple après la création d'un volume.

Étapes

1. En haut de Cloud Manager, cliquez sur **Tiering**.
2. Dans **Cluster Dashboard**, cliquez sur **Tier volumes** pour le cluster.
3. Cliquez sur le bouton correspondant à chaque volume Sélectionnez une stratégie de hiérarchisation, ajustez éventuellement les jours de refroidissement, puis cliquez sur **appliquer**.

   "En savoir plus sur les règles de Tiering des volumes".



Il n'est pas nécessaire de configurer le stockage objet, car il était déjà configuré lors de la configuration initiale du Tiering pour le cluster. ONTAP effectue le Tiering des données inactives de ces volumes vers le même magasin d'objets.

4. Lorsque vous avez terminé, cliquez sur **Fermer**.

Modification de la règle de Tiering d'un volume

La modification de la règle de Tiering pour un volume modifie la façon dont ONTAP transfère les données inactives vers le stockage objet. Au moment de modifier la règle, cette modification ne modifie que le comportement de Tiering suivant pour le volume.

Étapes

1. En haut de Cloud Manager, cliquez sur **Tiering**.
2. Dans **Cluster Dashboard**, cliquez sur **Tier volumes** pour le cluster.
3. Cliquez sur le bouton Sélectionnez une stratégie de hiérarchisation, ajustez éventuellement les jours de refroidissement, puis cliquez sur **appliquer**.

   "En savoir plus sur les règles de Tiering des volumes".

Gestion des paramètres de Tiering sur les agrégats

Chaque agrégat dispose de deux paramètres que vous pouvez ajuster : le seuil de remplissage de niveaux et si le reporting des données inactives est activé.

Seuil de remplissage par niveaux

Si le seuil est inférieur, le volume de données à stocker sur le Tier de performance avant le Tiering est réduit. Ce fonctionnement peut s'avérer utile pour les agrégats volumineux qui contiennent peu de données actives.

Si la valeur du seuil est supérieure, la quantité de données à stocker sur le Tier de performance avant le Tiering est supérieure. Cela peut être utile pour les solutions conçues pour le Tiering uniquement lorsque les agrégats bénéficient d'une capacité quasi maximale.

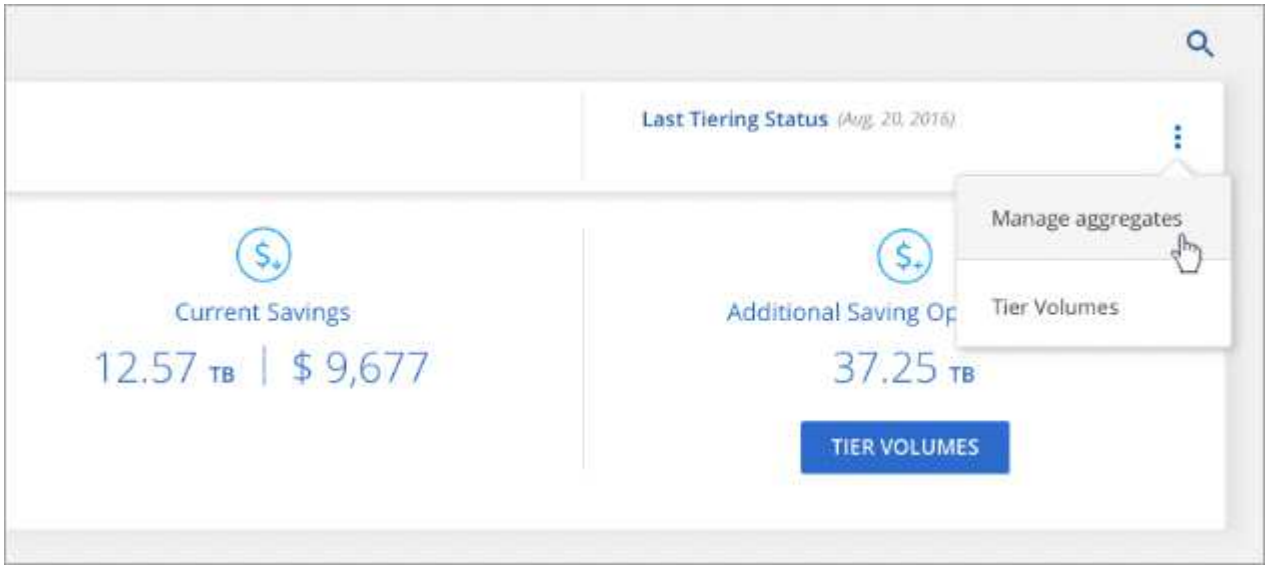
Reporting des données inactives

Le reporting des données inactives (IDR) utilise une période de refroidissement de 31 jours pour déterminer quelles données sont considérées comme inactives. La quantité de données inactives dans le Tier dépend des règles de Tiering définies sur les volumes. Cette quantité peut être différente de la quantité de données inactives détectée par l'IDR sur une période de refroidissement de 31 jours.

Il est préférable de maintenir l'option IDR activée car elle permet d'identifier vos données inactives et vos opportunités d'économies. L'IDR doit rester activé si le Tiering des données était activé sur un agrégat.

Étapes

1. En haut de Cloud Manager, cliquez sur **Tiering**.
2. Dans la page **Cloud Tiering**, cliquez sur l'icône de menu d'un cluster et sélectionnez **Manage Aggregates**.



3. Sur la page **gérer les agrégats**, cliquez sur le bouton icône d'un agrégat dans la table.
4. Modifiez le seuil de remplissage et choisissez d'activer ou de désactiver le rapport de données inactives.

5. Cliquez sur **appliquer**.

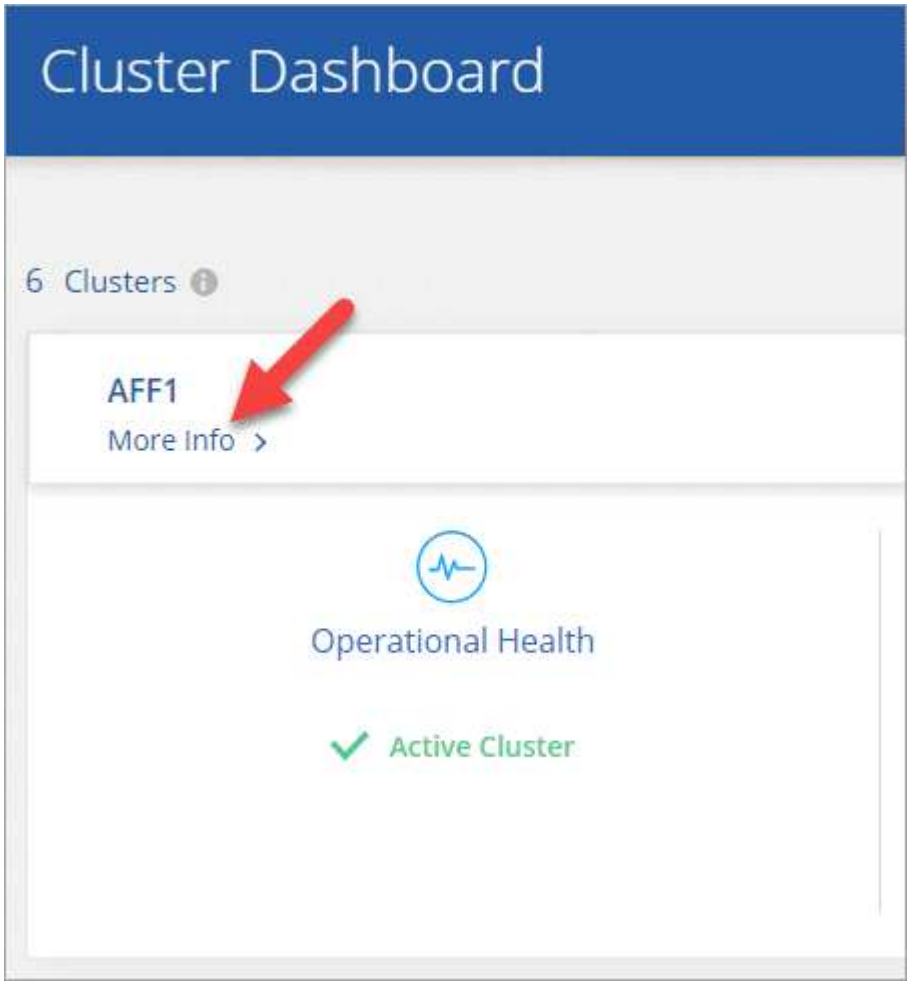
Révision des informations de hiérarchisation pour un cluster

Vous pouvez connaître la quantité de données stockées dans le Tier cloud et la quantité de données stockées sur les disques. Vous pouvez également voir la quantité de données actives et inactives sur les disques du

cluster. NetApp Cloud Tiering fournit ces informations pour chaque cluster.

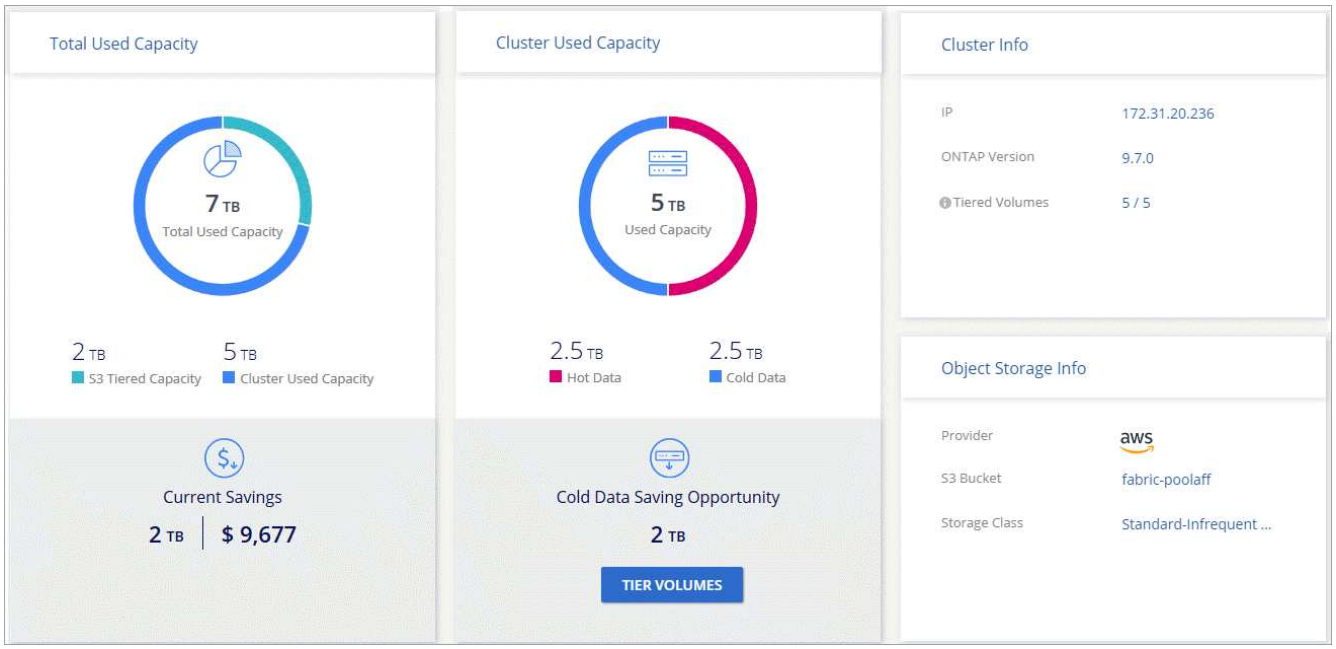
Étapes

1. En haut de Cloud Manager, cliquez sur **Tiering**.
2. Dans **Cluster Dashboard**, cliquez sur **plus d'info** pour un cluster.



3. Révision des détails du cluster.

   Voici un exemple :

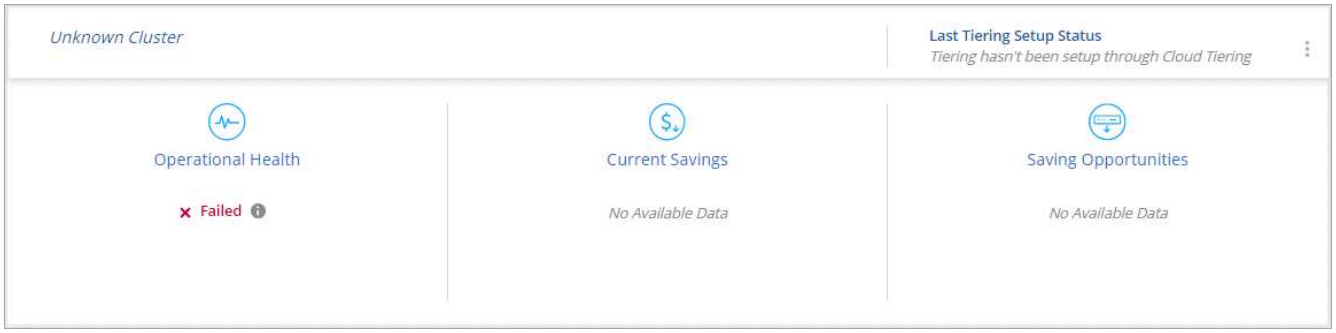


Corriger la santé opérationnelle

Les défaillances peuvent survenir. Et le cas fois, Cloud Tiering affiche l'état d'intégrité opérationnelle « défaillante » sur le tableau de bord du cluster. L'état de santé reflète l'état du système ONTAP et de Cloud Manager.

Étapes

1. Identifiez tous les clusters dont l'état opérationnel est « en panne ».



2. Placez le pointeur de la souris sur le pour voir la raison de l'échec.
3. Corriger le problème :
   a. Vérifiez que le cluster ONTAP est opérationnel et qu'il dispose d'une connexion entrante et sortante avec votre fournisseur de stockage objet.
   b. Vérifiez que Cloud Manager dispose de connexions sortantes avec le service Cloud Tiering, vers le magasin d'objets et vers les clusters ONTAP qu'il détecte.

FAQ technique sur NetApp Cloud Tiering

Cette FAQ peut vous aider si vous cherchez juste une réponse rapide à une question.

ONTAP

Les questions suivantes concernent ONTAP.

Quelles sont les exigences liées à mon cluster ONTAP ?

Cela dépend de l'endroit où vous procédez au Tiering des données inactives. Reportez-vous aux sections suivantes :

- "Tiering des données depuis des clusters ONTAP sur site vers Amazon S3"
- "Tiering des données depuis les clusters ONTAP sur site vers le stockage Azure Blob"
- "Tiering des données depuis des clusters ONTAP sur site vers Google Cloud Storage"
- "Tiering des données depuis des clusters ONTAP sur site vers StorageGRID"

Le Tiering cloud permet-il le reporting des données inactives ?

Oui, NetApp Cloud Tiering active le reporting des données inactives sur chaque agrégat. Ce paramètre nous permet d'identifier la quantité de données inactives pouvant être envoyées vers un stockage objet à faible coût.

Puis-je transférer les données à partir de volumes NAS et de volumes SAN ?

Vous pouvez utiliser NetApp Cloud Tiering pour transférer les données depuis des volumes NAS vers le cloud public et depuis des volumes SAN vers un cloud privé à l'aide de StorageGRID.

Qu'en est-il de Cloud Volumes ONTAP ?

Si vous disposez de systèmes Cloud Volumes ONTAP, vous les trouverez dans le tableau de bord des clusters pour bénéficier d'une vue complète du Tiering des données dans votre infrastructure de cloud hybride.

Depuis le tableau de bord de cluster, vous pouvez afficher des informations de hiérarchisation similaires à celles d'un cluster ONTAP sur site : état de fonctionnement, économies actuelles, économies réalisées, informations détaillées sur les volumes et les agrégats, etc.

Les systèmes Cloud Volumes ONTAP sont en lecture seule depuis le Tiering dans le cloud. Vous ne pouvez pas configurer le Tiering des données dans Cloud Volumes ONTAP à partir de NetApp Cloud Tiering. Vous allez toujours configurer le Tiering de la même manière que dans l'environnement de travail de Cloud Manager.

Stockage objet

Les questions suivantes se rapportent au stockage objet.

Quels fournisseurs de stockage objet sont pris en charge ?

Amazon S3, le stockage Azure Blob, Google Cloud Storage ou StorageGRID utilisant le protocole S3 sont pris en charge.

Est-il possible d'utiliser un compartiment/conteneur adapté à mes besoins ?

Oui, c'est possible. Une fois le Tiering configuré, vous avez la possibilité d'ajouter un nouveau compartiment/conteneur ou de sélectionner un compartiment/conteneur existant.

Quelles régions sont prises en charge ?

- "Régions AWS prises en charge"
- "Régions Azure prises en charge"
- "Régions Google Cloud prises en charge"

Quelles sont les classes de stockage S3 prises en charge ?

Cloud Tiering prend en charge le Tiering des données selon la classe de stockage *Standard*, *Standard-Infrequent Access*, *One zone-IA* ou *Intelligent*. Voir "Classes de stockage S3 prises en charge" pour en savoir plus.

Quels tiers d'accès Azure Blob sont pris en charge ?

Cloud Tiering utilise automatiquement le Tier d'accès *Hot* pour vos données inactives.

Quelles sont les classes de stockage prises en charge par Google Cloud Storage ?

La hiérarchisation du cloud utilise la classe de stockage *Standard* pour les données inactives.

NetApp Cloud Tiering utilise-t-il un magasin d'objets pour l'ensemble du cluster ou un par agrégat ?

Un magasin d'objets pour l'ensemble du cluster.

Puis-je appliquer des règles à mon magasin d'objets afin de déplacer les données sans recourir au Tiering ?

Non, NetApp Cloud Tiering ne prend pas en charge les règles de gestion du cycle de vie des objets qui déplacent ou suppriment des données des magasins d'objets.

Connecteurs

Les questions suivantes concernent les connecteurs.

Où le connecteur doit-il être installé ?

- Lorsque le Tiering des données vers S3, un connecteur peut résider dans un VPC AWS ou sur votre site.
- Lors du Tiering des données vers un stockage Blob, un connecteur doit résider dans un VNet Azure.
- Lorsque vous effectuez le Tiering des données vers Google Cloud Storage, un connecteur doit résider dans un VPC Google Cloud Platform.
- Lors du Tiering des données vers StorageGRID, un connecteur doit résider sur un hôte Linux sur site.

Mise en réseau

Les questions suivantes concernent la mise en réseau.

Quelles sont les exigences en matière de mise en réseau ?

- Le cluster ONTAP établit une connexion HTTPS via le port 443 vers votre fournisseur de stockage objet.

  Le ONTAP lit et écrit les données vers et à partir du stockage objet. Le stockage objet ne démarre jamais, il répond simplement.

- Pour StorageGRID, le cluster ONTAP établit une connexion HTTPS vers StorageGRID via un port spécifié par l'utilisateur (le port est configurable lors de la configuration du Tiering).
- Un connecteur nécessite une connexion HTTPS sortante via le port 443 vers vos clusters ONTAP, vers le magasin d'objets et vers le service Cloud Tiering.

Pour plus de détails, voir :

- "Tiering des données depuis des clusters ONTAP sur site vers Amazon S3"
- "Tiering des données depuis les clusters ONTAP sur site vers le stockage Azure Blob"
- "Tiering des données depuis des clusters ONTAP sur site vers Google Cloud Storage"
- "Tiering des données depuis des clusters ONTAP sur site vers StorageGRID"

Autorisations

Les questions suivantes concernent les autorisations.

Quelles sont les autorisations requises dans AWS ?

Des autorisations sont requises "Pour gérer le compartiment S3".

Quelles sont les autorisations requises dans Azure ?

Aucune autorisation supplémentaire n'est nécessaire en dehors des autorisations que vous devez fournir à Cloud Manager.

Quelles autorisations sont requises dans Google Cloud Platform ?

Des autorisations d'administrateur du stockage sont nécessaires pour un compte de service doté de clés d'accès au stockage.

Quelles sont les autorisations requises pour StorageGRID ?

"Des autorisations S3 sont nécessaires".

Référence

Classes et régions de stockage S3 prises en charge

NetApp Cloud Tiering prend en charge plusieurs classes de stockage S3 ainsi que la plupart des régions.

Classes de stockage S3 prises en charge

NetApp Cloud Tiering peut appliquer une règle de cycle de vie afin que les données soient transitions d'une classe de stockage *Standard* vers une autre classe de stockage après 30 jours. Vous pouvez choisir parmi les classes de stockage suivantes :

- Accès autonome et peu fréquent
- Une zone IA
- Intelligente

Si vous choisissez Standard, les données restent dans cette classe de stockage.

"Découvrez les classes de stockage S3".

Régions AWS prises en charge

NetApp Cloud Tiering prend en charge plusieurs régions AWS :

Asie Pacifique

- Mumbai
- Séoul
- Singapour
- Sydney
- Tokyo

Europe

- Francfort
- Irlande
- Londres
- Paris
- Stockholm

Amérique du Nord

- Canada Central
- GovCloud (USA-West) - disponible à partir d'ONTAP 9.3
- US East (N. Virginie)
- États-Unis Est (Ohio)
- US West (N. Californie)
- US West (Oregon)

Amérique du Sud

- São Paulo

Tiers et régions d'accès Azure Blob pris en charge

Cloud Tiering prend en charge le niveau d'accès *Hot* et la plupart des régions.

Tiers d'accès Azure Blob pris en charge

Lorsque vous configurez le Tiering des données sur Azure, Cloud Tiering utilise automatiquement le Tier d'accès *Hot* pour vos données inactives.

Régions Azure prises en charge

NetApp Cloud Tiering prend en charge les régions Azure suivantes.

Afrique

- Afrique du Sud Nord

Asie Pacifique

- Australie Est
- Australie Sud-Est
- Asie de l'Est
- Japon Est
- Japon Ouest
- Corée Centrale
- Corée du Sud
- Asie du Sud-Est

Europe

- France centrale
- Allemagne Centrale
- Allemagne Nord-Est
- Europe du Nord
- Royaume-Uni Sud
- Royaume-Uni Ouest
- Europe de l'Ouest

Amérique du Nord

- Canada Central
- Canada Est
- Centre DES ÉTATS-UNIS
- Est-É.-U.
- Est DES ÉTATS-UNIS 2
- Centre-nord des États-Unis
- Centre-sud des États-Unis
- Ouest des États-Unis
- Ouest des États-Unis 2
- Centre Ouest des États-Unis

Amérique du Sud

- Brésil Sud

Classes et régions de stockage Google Cloud prises en charge

NetApp Cloud Tiering prend en charge la classe de stockage standard et la plupart des régions Google Cloud.

Tiers d’accès pris en charge

La hiérarchisation du cloud utilise le Tier d’accès *Standard* pour vos données inactives.

Régions Google Cloud prises en charge

Cloud Tiering prend en charge les régions suivantes.

Amériques

- Iowa
- Los Angeles
- Montréal
- N. Virginie
- Oregon
- Sao Paulo
- Caroline du Sud

Asie Pacifique

- Hong Kong
- Mumbai
- Osaka
- Singapour
- Sydney
- Taïwan
- Tokyo

Europe

- Belgique
- Finlande
- Francfort
- Londres
- Pays-Bas
- Zurich

Affichage des compartiments Amazon S3

Une fois que vous avez installé un connecteur dans AWS, Cloud Manager détecte automatiquement les informations sur les compartiments Amazon S3 qui résident dans le compte AWS sur lequel il est installé.

Vous pouvez afficher des informations détaillées sur vos compartiments S3, notamment la région, le niveau d'accès et la classe de stockage, et voir si le compartiment est utilisé avec Cloud Volumes ONTAP pour les sauvegardes ou le Tiering des données. Et vous pouvez scanner les compartiments S3 avec Cloud Compliance.

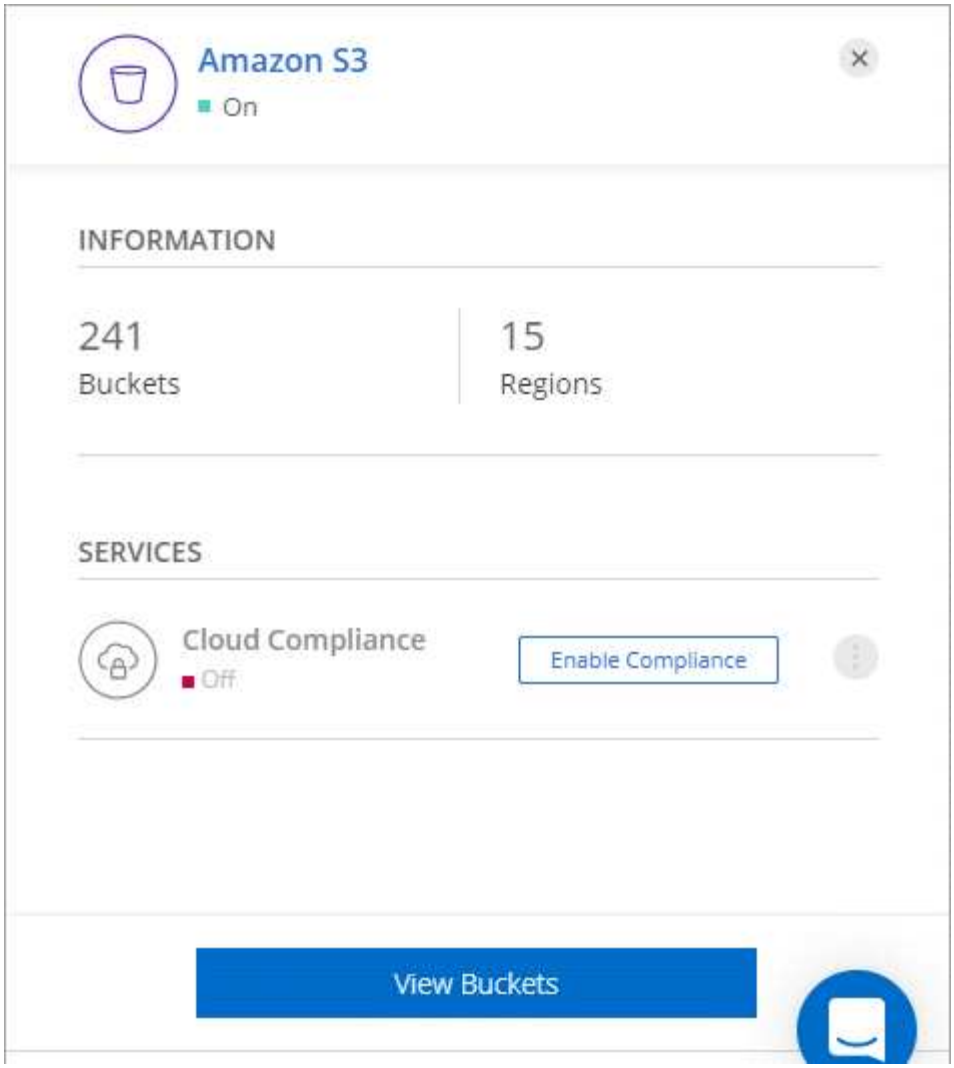
Étapes

1. "Installer un connecteur" Dans le compte AWS où vous souhaitez afficher vos compartiments Amazon S3.

   Vous devriez voir automatiquement un environnement de travail Amazon S3 peu après.

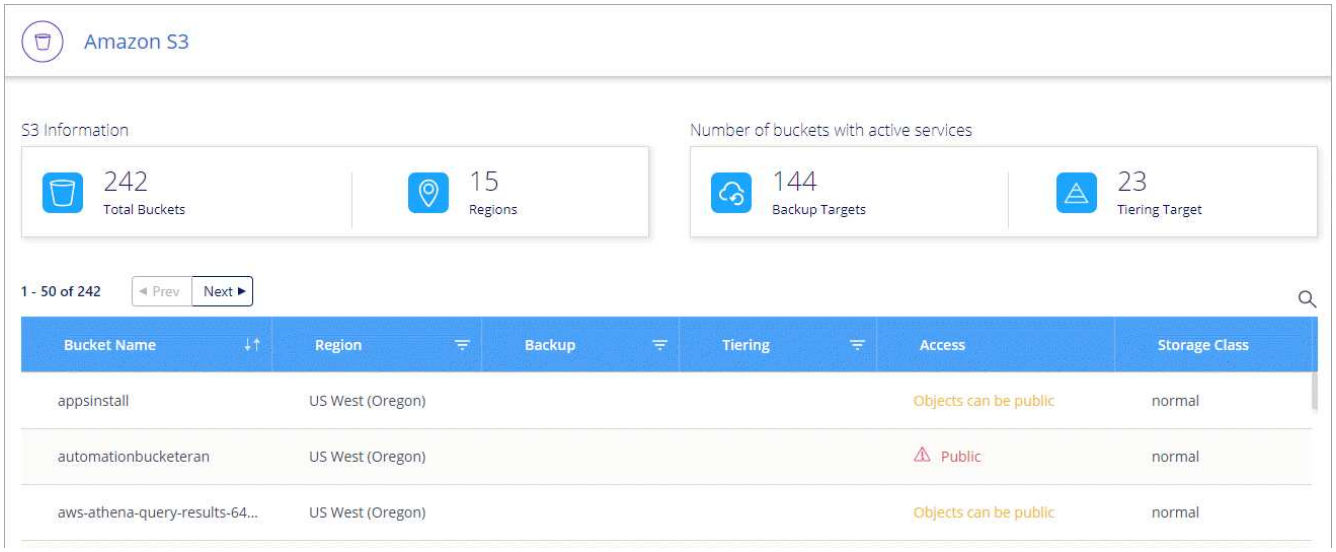
2. Cliquez sur l'environnement de travail et sélectionnez une action dans le volet droit.



3. Cliquez sur **Activer la conformité** pour rechercher les données personnelles et sensibles dans les compartiments S3.

   Pour plus de détails, voir "Mise en route de Cloud Compliance pour Amazon S3".

4. Cliquez sur **View seaux** pour afficher des détails sur les compartiments S3 de votre compte AWS.



Administration de Cloud Manager

Recherche de l'ID système Cloud Manager

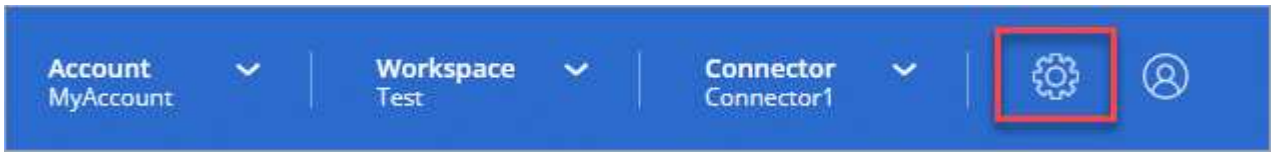
Pour vous aider à vous lancer, votre représentant NetApp peut vous demander votre identifiant de système Cloud Manager. L'ID est généralement utilisé à des fins de licence et de dépannage.

Ce dont vous avez besoin

Vous devez créer un connecteur pour modifier les paramètres de Cloud Manager. "Découvrez comment".

Étapes

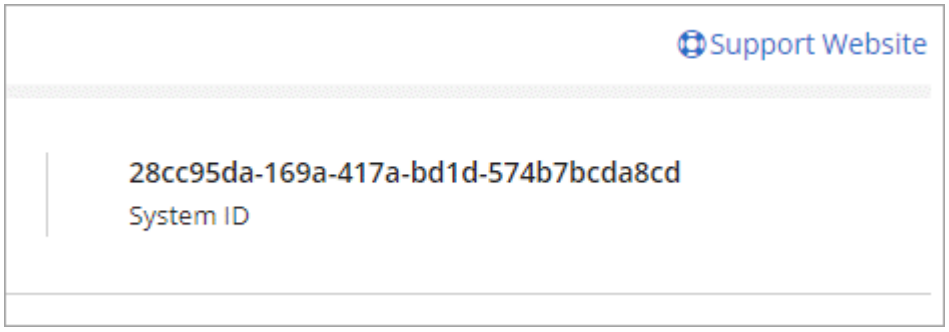
1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres.



2. Cliquez sur **support Dashboard**.

   L'ID de votre système apparaît dans le coin supérieur droit.

   Exemple



Gérer les connecteurs

Gestion des connecteurs existants

Après avoir créé un ou plusieurs connecteurs, vous pouvez les gérer en passant d'un connecteur à l'autre, en vous connectant à l'interface utilisateur locale s'exécutant sur un connecteur, et plus encore.

Basculement entre les connecteurs

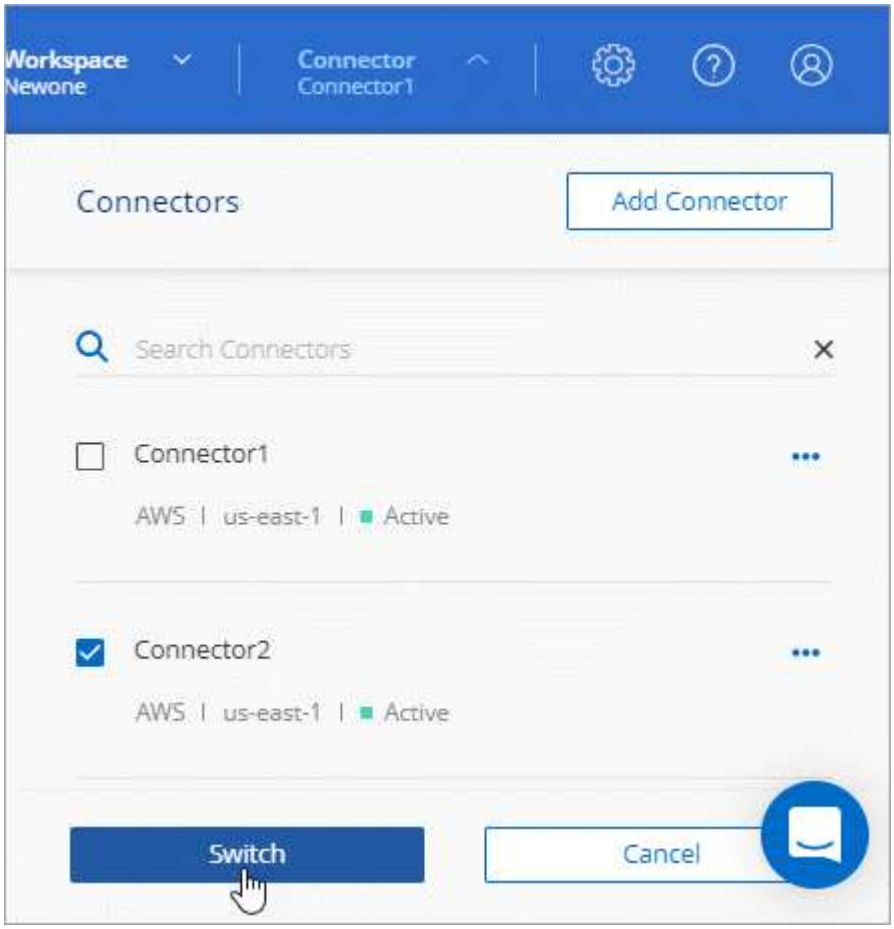
Si vous avez plusieurs connecteurs, vous pouvez passer de l'un à l'autre pour voir les environnements de travail associés à un connecteur spécifique.

Imaginons par exemple que vous travaillez dans un environnement multicloud. Vous avez peut-être un

connecteur dans AWS et un autre dans Google Cloud. Il faudrait basculer entre ces connecteurs pour gérer les systèmes Cloud Volumes ONTAP présents dans ces clouds.

Étape

1. Cliquez sur la liste déroulante **Connector**, sélectionnez un autre connecteur, puis cliquez sur **Switch**.



Cloud Manager actualise et affiche les environnements de travail associés au connecteur sélectionné.

Accès à l'interface utilisateur locale

Bien que vous devriez effectuer presque toutes les tâches à partir de l'interface utilisateur SaaS, une interface utilisateur locale est toujours disponible sur le connecteur. Cette interface est nécessaire pour quelques tâches qui doivent être effectuées à partir du connecteur lui-même :

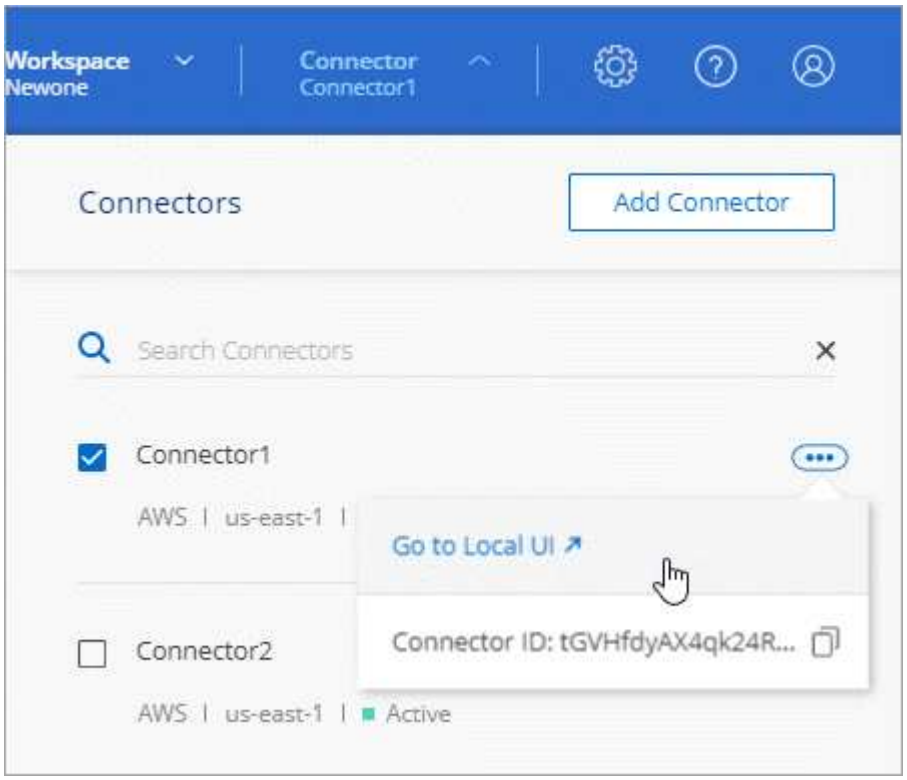
- "Configuration d'un serveur proxy"
- Installation d'un correctif (en général, vous travaillerez avec le personnel NetApp pour installer un correctif)
- Téléchargement de messages AutoSupport (généralement dirigés par le personnel NetApp en cas de problème)

Étapes

1. "Connectez-vous à l'interface SaaS Cloud Manager" À partir d'une machine dotée d'une connexion réseau à l'instance de connecteur.

   Si le connecteur n'est pas doté d'une adresse IP publique, vous aurez besoin d'une connexion VPN ou vous devrez vous connecter à partir d'un hôte de secours situé sur le même réseau que le connecteur.

2. Cliquez sur la liste déroulante **Connector**, cliquez sur le menu d'action d'un connecteur, puis cliquez sur **allez à l'interface utilisateur locale**.



L'interface Cloud Manager exécutée sur le connecteur est chargée dans un nouvel onglet du navigateur.

Retrait de connecteurs de Cloud Manager

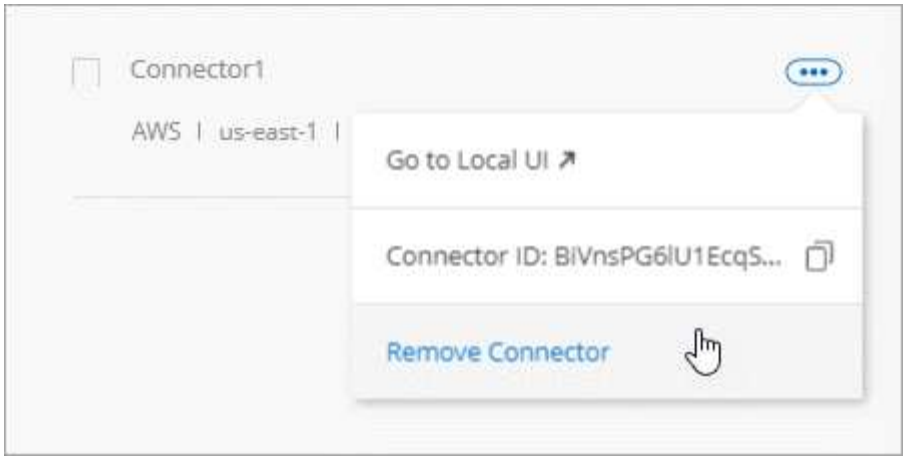
Si un connecteur est inactif, vous pouvez le supprimer de la liste des connecteurs dans Cloud Manager. Vous pouvez le faire si vous avez supprimé la machine virtuelle Connector ou si vous avez désinstallé le logiciel Connector.

Notez ce qui suit sur le retrait d'un connecteur :

- Cette action ne supprime pas la machine virtuelle.
- Cette action ne peut pas être rétablie, car une fois que vous avez supprimé un connecteur de Cloud Manager, vous ne pouvez pas le réintégrer.

Étapes

1. Dans la liste déroulante connecteur, cliquez sur l'en-tête Cloud Manager.
2. Cliquez sur le menu d'action d'un connecteur inactif et cliquez sur **Supprimer le connecteur**.



3. Entrez le nom du connecteur à confirmer, puis cliquez sur Supprimer.

Résultat

Cloud Manager élimine le connecteur de ses enregistrements.

Désinstallation du logiciel du connecteur

Le connecteur inclut un script de désinstallation que vous pouvez utiliser pour désinstaller le logiciel pour résoudre des problèmes ou pour supprimer définitivement le logiciel de l'hôte.

Étape

1. À partir de l'hôte Linux, exécutez le script de désinstallation :

   /opt/application/netapp/cloudmanager/bin/uninstall.sh [silencieux]

   silent exécute le script sans vous demander de confirmer.

Qu'en est-il des mises à niveau logicielles

Le connecteur met automatiquement à jour son logiciel à la dernière version, tant qu'il l'a fait "accès internet sortant" pour obtenir la mise à jour logicielle.

Autres façons de créer des connecteurs

Exigences relatives à l'hôte de connecteur

Le logiciel du connecteur doit être exécuté sur un hôte qui répond à des exigences spécifiques du système d'exploitation, de la RAM, des ports, etc.

Un hôte dédié est requis

Le connecteur n'est pas pris en charge sur un hôte partagé avec d'autres applications. L'hôte doit être un hôte dédié.

CPU

4 cœurs ou 4 CPU virtuels

RAM

14 GO

Type d'instance AWS EC2

Type d'instance qui répond aux exigences relatives au CPU et à la RAM indiquées ci-dessus. Nous recommandons une instance t3.XLarge d'utiliser ce type d'instance lorsque vous déployez le connecteur directement depuis Cloud Manager.

Taille des machines virtuelles Azure

Type d'instance qui répond aux exigences relatives au CPU et à la RAM indiquées ci-dessus. Nous recommandons la version DS3 v2 et d'utiliser cette taille de machine virtuelle lorsque vous déployez le connecteur directement depuis Cloud Manager.

Type de machine GCP

Type d'instance qui répond aux exigences relatives au CPU et à la RAM indiquées ci-dessus. Nous recommandons n1-standard-4 et d'utiliser ce type de machine lorsque vous déployez le connecteur directement depuis Cloud Manager.

Systèmes d'exploitation pris en charge

- CentOS 7.6
- CentOS 7.7
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7

  Le système Red Hat Enterprise Linux doit être enregistré avec Red Hat Subscription Management. S'il n'est pas enregistré, le système ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis pendant l'installation du connecteur.

  Le connecteur est pris en charge sur les versions en anglais de ces systèmes d'exploitation.

Hyperviseur

Un hyperviseur bare Metal ou hébergé certifié pour exécuter CentOS ou Red Hat Enterprise Linuxhttps://access.redhat.com/certified-hypervisors["Solution Red Hat : quels hyperviseurs sont certifiés pour l'exécution de Red Hat Enterprise Linux ?"^]

Espace disque dans /opt

100 Go d'espace doivent être disponibles

Accès Internet sortant

Un accès Internet sortant est nécessaire pour installer le connecteur et pour que le connecteur gère les ressources et les processus au sein de votre environnement de cloud public. Pour obtenir la liste des noeuds finaux, reportez-vous à la section "Exigences de mise en réseau pour le connecteur".

Création d'un connecteur à partir d'AWS Marketplace

Il est préférable de créer un connecteur directement depuis Cloud Manager, mais vous pouvez lancer un connecteur depuis AWS Marketplace, si vous ne souhaitez pas spécifier de clés d'accès AWS. Une fois que vous avez créé et configuré ce connecteur, Cloud Manager l'utilise automatiquement lors de la création de nouveaux environnements de travail.

Étapes

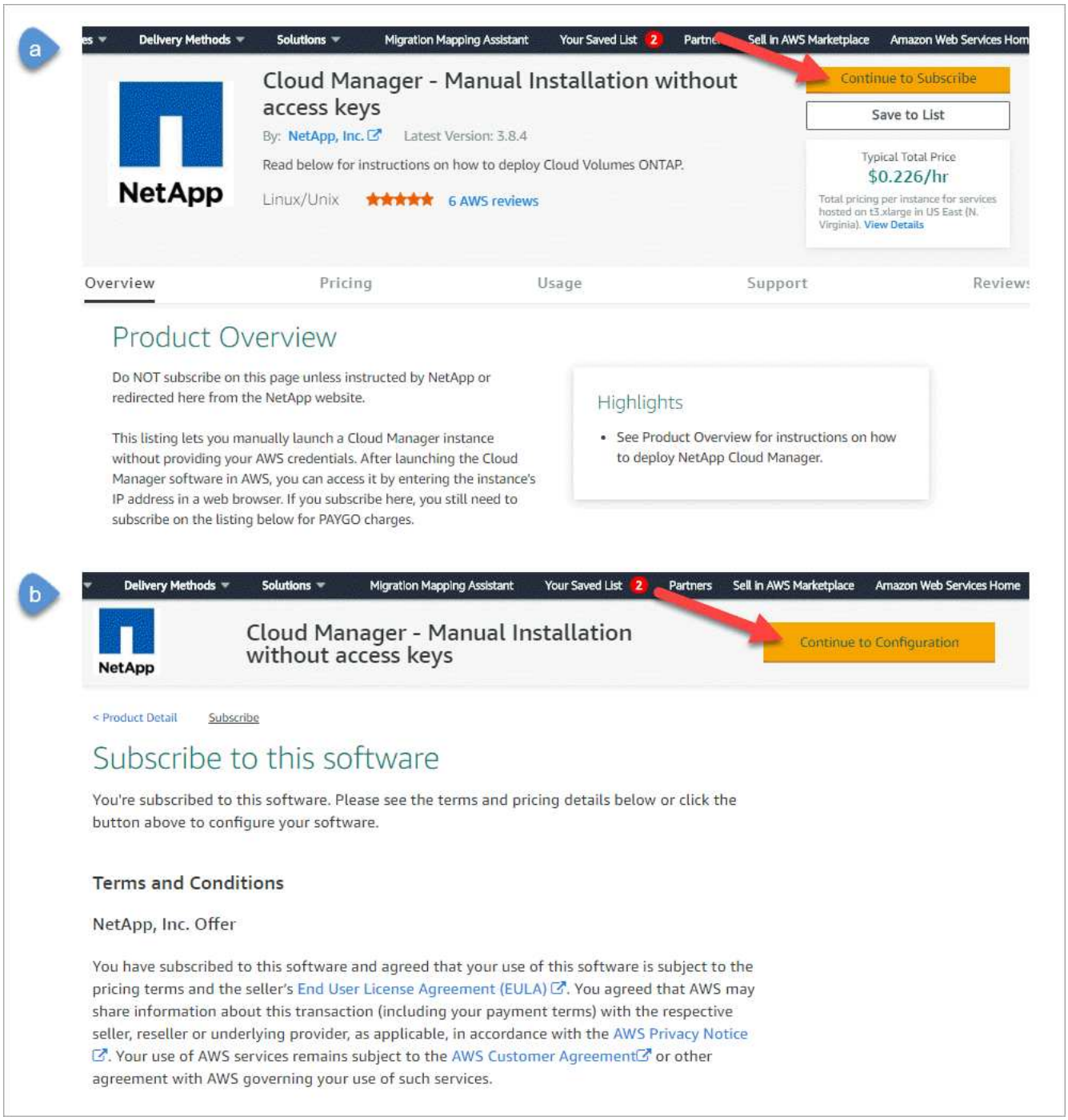
1. Créer une règle IAM et un rôle pour l'instance EC2 :
   a. Téléchargez la politique IAM de Cloud Manager à partir de l'emplacement suivant :

      "NetApp Cloud Manager : règles AWS, Azure et GCP"

   b. À partir de la console IAM, créez votre propre stratégie en copiant et en collant le texte de la stratégie IAM de Cloud Manager.
   c. Créez un rôle IAM avec le type de rôle Amazon EC2 et associez la stratégie que vous avez créée à l'étape précédente au rôle.
2. Maintenant, allez au "Page Cloud Manager sur AWS Marketplace" Pour déployer Cloud Manager à partir d'une ami.

   L'utilisateur IAM doit disposer d'autorisations AWS Marketplace pour vous abonner et se désabonner.

3. Sur la page Marketplace, cliquez sur **Continuer pour s'abonner**, puis cliquez sur **Continuer la configuration**.



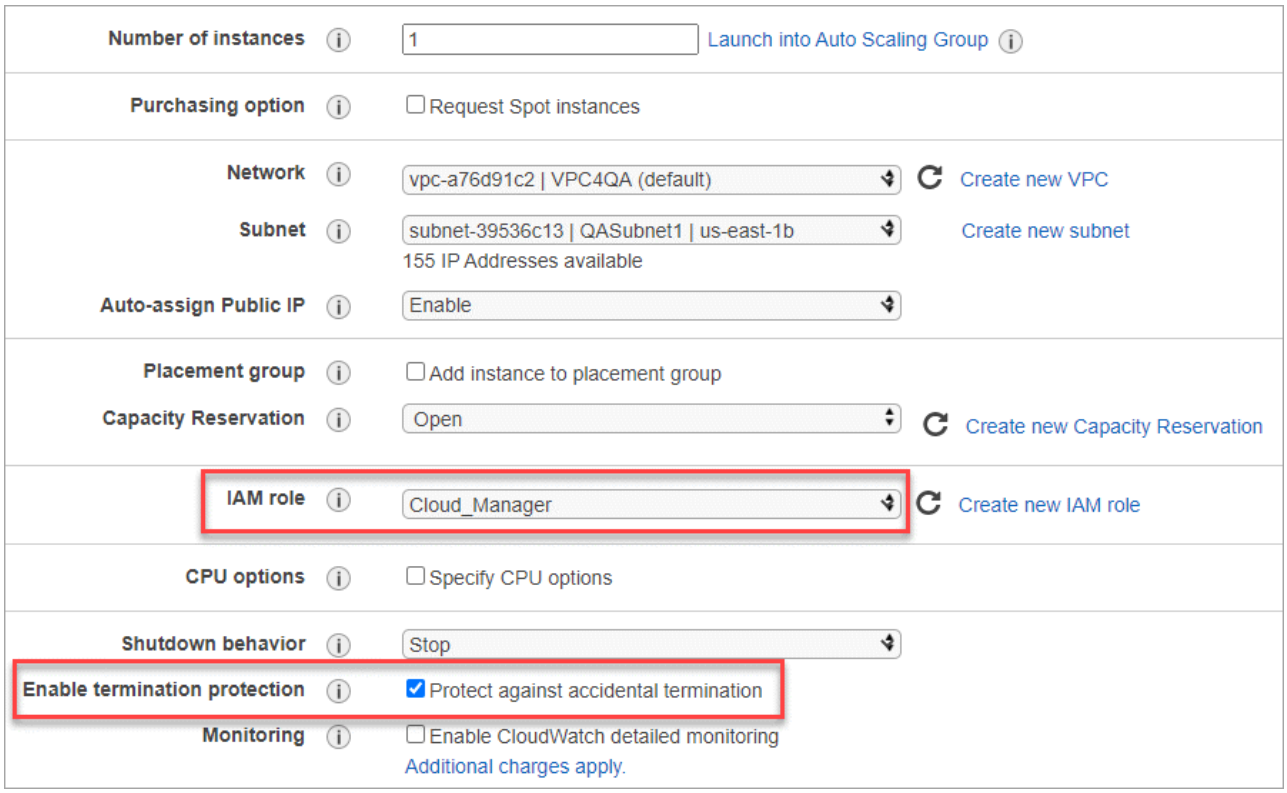
4. Modifiez l'une des options par défaut et cliquez sur **Continuer pour lancer**.
5. Sous **choisir action**, sélectionnez **lancer via EC2**, puis cliquez sur **lancer**.

   Ces étapes expliquent comment lancer l'instance à partir de la console EC2, car la console vous permet d'associer un rôle IAM à l'instance Cloud Manager. Cela n'est pas possible en utilisant l'action **lancer à partir du site Web**.

6. Suivez les invites pour configurer et déployer l'instance :
   - **Choisissez le type d'instance** : selon la disponibilité de la région, choisissez l'un des types d'instance pris en charge (t3.XLarge est recommandé).

     "Vérifiez les conditions requises pour l'instance".

- **Configurer l'instance** : sélectionnez un VPC et un sous-réseau, choisissez le rôle IAM que vous avez créé à l'étape 1, activez la protection de terminaison (recommandée) et choisissez toutes les autres options de configuration qui répondent à vos exigences.



- **Ajouter 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 connecteur : SSH, HTTP et HTTPS.
- **Revue**: Passez en revue vos sélections et cliquez sur **lancer**.

  AWS lance le logiciel avec les paramètres spécifiés. L'instance de connecteur et le logiciel doivent s'exécuter dans environ cinq minutes.

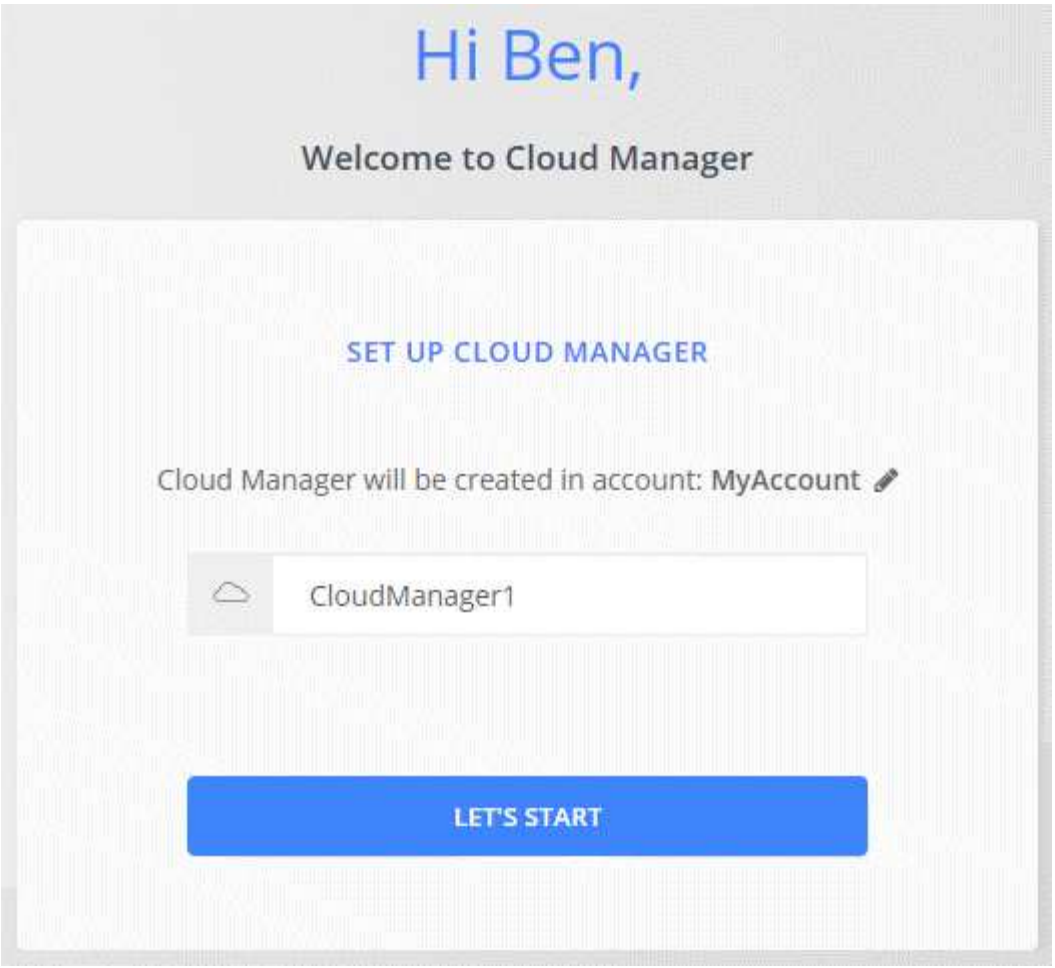
7. Ouvrez un navigateur Web à partir d'un hôte connecté à l'instance Connector et saisissez l'URL suivante :

   http://ipaddress:80

8. Une fois connecté, configurez le connecteur :
   a. Spécifiez le compte Cloud Central à associer au connecteur.

      "Découvrez les comptes Cloud Central".

   b. Entrez un nom pour le système.



Résultat

Le connecteur est maintenant installé et configuré avec votre compte Cloud Central. Cloud Manager utilisera automatiquement ce connecteur lors de la création de nouveaux environnements de travail. Mais si vous avez plus d'un connecteur, vous devrez le faire "basculer entre eux".

Création d'un connecteur à partir d'Azure Marketplace

Il est préférable de créer un connecteur directement depuis Cloud Manager, mais vous pouvez également lancer un connecteur depuis Azure Marketplace, si vous préférez. Une fois que vous avez créé et configuré ce connecteur, Cloud Manager l'utilise automatiquement lors de la création de nouveaux environnements de travail.

Création d'un connecteur dans Azure

Déployez le connecteur dans Azure en utilisant l'image dans Azure Marketplace, puis connectez-vous au connecteur pour spécifier votre compte Cloud Central.

Étapes

1. "Accédez à la page Azure Marketplace pour Cloud Manager".
2. Cliquez sur **l'obtenir maintenant**, puis sur **Continuer**.
3. Sur le portail Azure, cliquez sur **Créer** et suivez les étapes de configuration de la machine virtuelle.

   Noter les éléments suivants lors de la configuration de la machine virtuelle :

- Cloud Manager peut fonctionner de manière optimale avec des disques durs ou SSD.
- Choisissez une taille de machine virtuelle qui répond aux exigences en matière de CPU et de RAM. Nous recommandons DS3 v2.

  "Vérifier les exigences relatives aux machines virtuelles".

- Pour le groupe de sécurité réseau, le connecteur nécessite des connexions entrantes via SSH, HTTP et HTTPS.

  "En savoir plus sur les règles de groupe de sécurité pour le connecteur".

- Sous **Management**, activez **l'identité gérée attribuée par le système** pour le connecteur en sélectionnant **On**.

  Ce paramètre est important car une identité gérée permet à la machine virtuelle Connector de s'identifier à Azure Active Directory sans fournir d'informations d'identification. "En savoir plus sur les identités gérées pour les ressources Azure".

4. Dans la page **Revue + créer**, vérifiez vos sélections et cliquez sur **Créer** pour démarrer le déploiement.

   Azure déploie la machine virtuelle avec les paramètres spécifiés. Le logiciel de la machine virtuelle et du connecteur doit s'exécuter en cinq minutes environ.

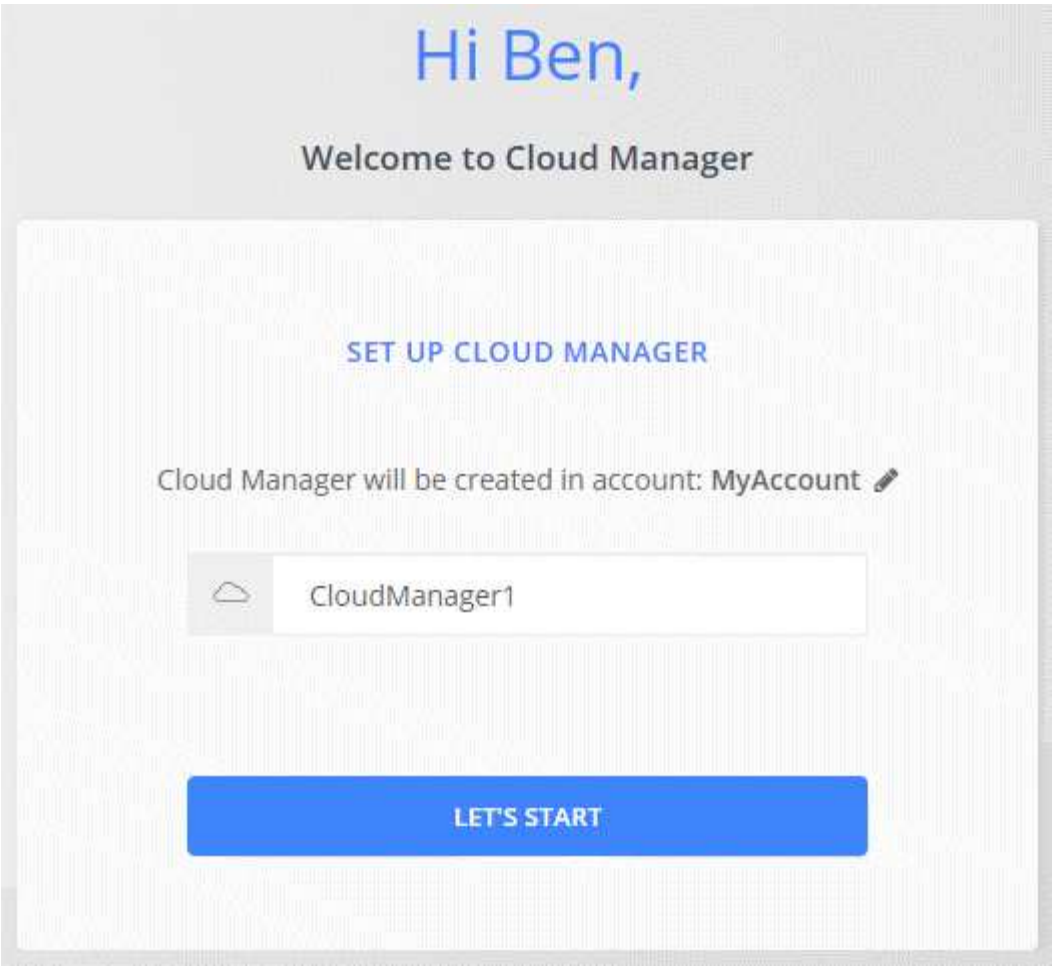
5. Ouvrez un navigateur Web à partir d'un hôte connecté à la machine virtuelle Connector et entrez l'URL suivante :

   http://ipaddress:80

6. Une fois connecté, configurez le connecteur :
   a. Spécifiez le compte Cloud Central à associer au connecteur.

      "Découvrez les comptes Cloud Central".

   b. Entrez un nom pour le système.



Résultat

Le connecteur est maintenant installé et configuré. Vous devez accorder des autorisations Azure avant que les utilisateurs puissent déployer Cloud Volumes ONTAP dans Azure.

Octroi d'autorisations Azure

Lorsque vous avez déployé le connecteur dans Azure, vous devez avoir activé un "identité gérée attribuée par le système". Vous devez maintenant accorder les autorisations Azure requises en créant un rôle personnalisé, puis en attribuant le rôle à la machine virtuelle Connector pour un ou plusieurs abonnements.

Étapes

1. Créez un rôle personnalisé à l'aide de la stratégie Cloud Manager :

   a. Téléchargez le "Politique de Cloud Manager Azure".

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

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

      Exemple

      « Assigner les Scopes » : [»/abonnements/d333af45-0d07-4154-943d-c25fbzzzzzzzzzz », «/abonnements/54b91999-b3e6-4599-908e-416e0zzzzzz », «/abonnements/8e474b-94b-4b-4b-4b-4b-4439-4b-4b-4b-4b-4b-4b-4b-4b-4b-4b-

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

   L'exemple suivant montre comment créer un rôle personnalisé à l'aide de l'interface de ligne de commande Azure CLI 2.0 :

   ```
   az role definition create --role-definition
   C:\Policy_for_cloud_Manager_Azure_3.8.7.json
   ```

Vous devez maintenant avoir un rôle personnalisé appelé opérateur Cloud Manager que vous pouvez attribuer à la machine virtuelle Connector.

2. Attribuez le rôle à la machine virtuelle Connector pour un ou plusieurs abonnements :
   a. Ouvrez le service **abonnements**, puis sélectionnez l'abonnement dans lequel vous souhaitez déployer des systèmes Cloud Volumes ONTAP.
   b. Cliquez sur **contrôle d'accès (IAM)**.
   c. Cliquez sur **Ajouter** > **Ajouter une affectation de rôle**, puis ajoutez les autorisations suivantes :
      - Sélectionnez le rôle **opérateur** de Cloud Manager.

        L'opérateur de Cloud Manager est le nom par défaut fourni dans "Politique de Cloud Manager". Si vous avez choisi un autre nom pour le rôle, sélectionnez-le à la place.

      - Attribuez l'accès à une **machine virtuelle**.
      - Sélectionnez l'abonnement dans lequel la machine virtuelle du connecteur a été créée.
      - Sélectionnez la machine virtuelle Connector.
      - Cliquez sur **Enregistrer**.
   d. Si vous souhaitez déployer Cloud Volumes ONTAP à partir d'abonnements supplémentaires, passez à cet abonnement, puis répétez ces étapes.

Résultat

Le connecteur dispose désormais des autorisations nécessaires pour gérer les ressources et les processus au sein de votre environnement de cloud public. Cloud Manager utilisera automatiquement ce connecteur lors de la création de nouveaux environnements de travail. Mais si vous avez plus d'un connecteur, vous devrez le faire "basculer entre eux".

Installation du logiciel de connecteur sur un hôte Linux existant

La méthode la plus courante pour créer un connecteur consiste à partir de Cloud Manager ou du Marketplace d'un fournisseur cloud. Mais vous avez la possibilité de télécharger et d'installer le logiciel Connector sur un hôte Linux existant de votre réseau ou dans le cloud.

Pour créer un système Cloud Volumes ONTAP dans Google Cloud, vous devez également disposer d'un connecteur exécuté dans Google Cloud. Vous ne pouvez pas utiliser un connecteur qui fonctionne à un autre emplacement.

De formation

- L'hôte doit se réunir "Configuration requise pour le connecteur".
- Un système Red Hat Enterprise Linux doit être enregistré avec Red Hat Subscription Management. S'il

n'est pas enregistré, le système ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis pendant l'installation.

- Le programme d'installation du connecteur accède à plusieurs URL pendant le processus d'installation. Vous devez vous assurer que l'accès Internet sortant est autorisé à ces noeuds finaux :
  - http://dev.mysql.com/get/mysql-community-release-el7-5.noarch.rpm
  - https://dl.fedoraproject.org/pub/epel/epel-release-latest-7.noarch.rpm
  - https://s3.amazonaws.com/aws-cli/awscli-bundle.zip

    L'hôte peut essayer de mettre à jour les packages du système d'exploitation lors de l'installation. L'hôte peut contacter différents sites de mise en miroir pour ces packages OS.

Description de la tâche

- Les privilèges root ne sont pas nécessaires pour installer le connecteur.
- L'installation installe les outils de ligne de commande AWS (awscli), afin d'activer les procédures de reprise à partir du support NetApp.

  Si vous recevez un message indiquant que l'installation de awscli a échoué, vous pouvez ignorer le message en toute sécurité. Le connecteur peut fonctionner sans outils.

- Le programme d'installation disponible sur le site du support NetApp peut être une version antérieure. Après l'installation, le connecteur se met automatiquement à jour si une nouvelle version est disponible.

Étapes

1. Téléchargez le logiciel Cloud Manager sur le "Site de support NetApp", Puis copiez-le sur l'hôte Linux.

   Pour obtenir de l'aide sur la connexion et la copie du fichier vers une instance EC2 dans AWS, reportez-vous à la section "Documentation AWS : connexion à votre instance Linux à l'aide de SSH".

2. Attribuez des autorisations pour exécuter le script.

   Exemple

   ```
    chmod +x OnCommandCloudManager-V3.8.4.sh
   . Exécutez le script d'installation :
   ```

   ```
   ./OnCommandCloudManager-V3.8.4.sh [silent] [proxy=ipaddress]
   [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   silent exécute l'installation sans vous demander des informations.

   proxy est requis si l'hôte est derrière un serveur proxy.

   proxyport est le port du serveur proxy.

   proxyuser est le nom d'utilisateur du serveur proxy, si une authentification de base est requise.

   proxypwd est le mot de passe du nom d'utilisateur que vous avez spécifié.

3. Sauf si vous avez spécifié le paramètre silencieux, tapez **y** pour continuer le script, puis entrez les ports HTTP et HTTPS lorsque vous y êtes invité.

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

4. Ouvrez un navigateur Web et entrez l'URL suivante :

   https://ipaddress:port

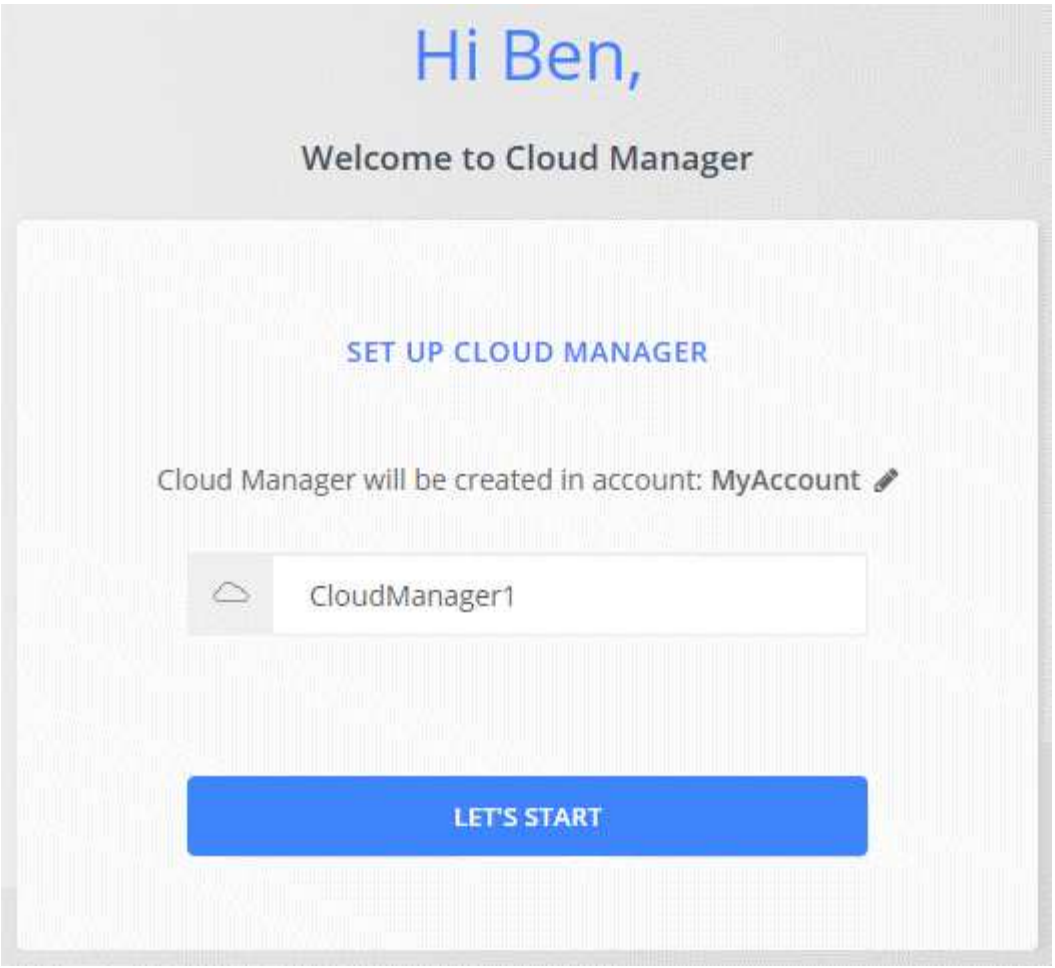
   Ipaddress peut être localhost, une adresse IP privée ou une adresse IP publique, selon la configuration de l'hôte. Par exemple, si le connecteur est dans le Cloud public sans adresse IP publique, vous devez entrer une adresse IP privée à partir d'un hôte qui a une connexion à l'hôte du connecteur.

   Port est nécessaire si vous avez modifié les ports HTTP (80) ou HTTPS (443) par défaut. Par exemple, si le port HTTPS a été modifié en 8443, vous pouvez entrer https://ipaddress:8443

5. Inscrivez-vous sur NetApp Cloud Central ou connectez-vous.
6. Une fois connecté, configurez Cloud Manager :
   a. Spécifiez le compte Cloud Central à associer au connecteur.

      "Découvrez les comptes Cloud Central".

   b. Entrez un nom pour le système.



Résultat

Le connecteur est maintenant installé et configuré avec votre compte Cloud Central. Cloud Manager utilisera automatiquement ce connecteur lors de la création de nouveaux environnements de travail.

Une fois que vous avez terminé

Configurez des autorisations pour que Cloud Manager puisse gérer les ressources et les processus dans votre environnement de cloud public :

- AWS : "Configurez un compte AWS, puis ajoutez-le à Cloud Manager".
- Azure : "Configurez un compte Azure, puis ajoutez-le à Cloud Manager".
- GCP : configurez un compte de service disposant des autorisations nécessaires à Cloud Manager pour créer et gérer des systèmes Cloud Volumes ONTAP dans des projets.
  a. "Créer un rôle dans GCP" qui inclut les autorisations définies dans le "Règle Cloud Manager pour GCP".
  b. "Créez un compte de service GCP et appliquez le rôle personnalisé que vous venez de créer".
  c. "Associer ce compte de service à la VM Connector".
  d. Si vous souhaitez déployer Cloud Volumes ONTAP dans d'autres projets, "Accordez l'accès en ajoutant le compte de service avec le rôle Cloud Manager à ce projet". Vous devrez répéter cette étape pour chaque projet.

Configuration par défaut du connecteur

Si vous devez dépanner le connecteur, il peut vous aider à comprendre sa configuration.

- Si vous avez déployé le connecteur depuis Cloud Manager (ou directement depuis le Marketplace d'un fournisseur cloud), remarque :
  - Dans AWS, le nom d'utilisateur de l'instance Linux EC2 est ec2-user.
  - Le système d'exploitation de l'image est le suivant :
    - AWS : Red Hat Enterprise Linux 7.5 (HVM)
    - Azure : Red Hat Enterprise Linux 7.6 (HVM)
    - GCP : CentOS 7.6

      Le système d'exploitation n'inclut pas d'interface graphique. Vous devez utiliser un terminal pour accéder au système.
- Le dossier d'installation du connecteur se trouve à l'emplacement suivant :

  /opt/application/netapp/cloudmanager
- Les fichiers journaux se trouvent dans le dossier suivant :

  /opt/application/netapp/cloudmanager/log
- Le service Cloud Manager s'appelle occm.
- Le service occm dépend du service MySQL.

  Si le service MySQL est en panne, le service occm est également en panne.
- Cloud Manager installe les packages suivants sur l'hôte Linux, s'ils ne sont pas déjà installés :
  - 7Zip
  - AWSCLI
  - Docker
  - Java
  - Kubectl
  - MySQL
  - Tridentctl
  - Tirer
  - Wget
- Le connecteur utilise les ports suivants sur l'hôte Linux :
  - 80 pour l'accès HTTP
  - 443 pour l'accès HTTPS
  - 3306 pour la base de données Cloud Manager
  - 8080 pour le proxy API Cloud Manager
  - 8666 pour l'API du Gestionnaire de services

◦ 8777 pour l'API du service de conteneurs Health-Checker

Gérer les identifiants

AWS

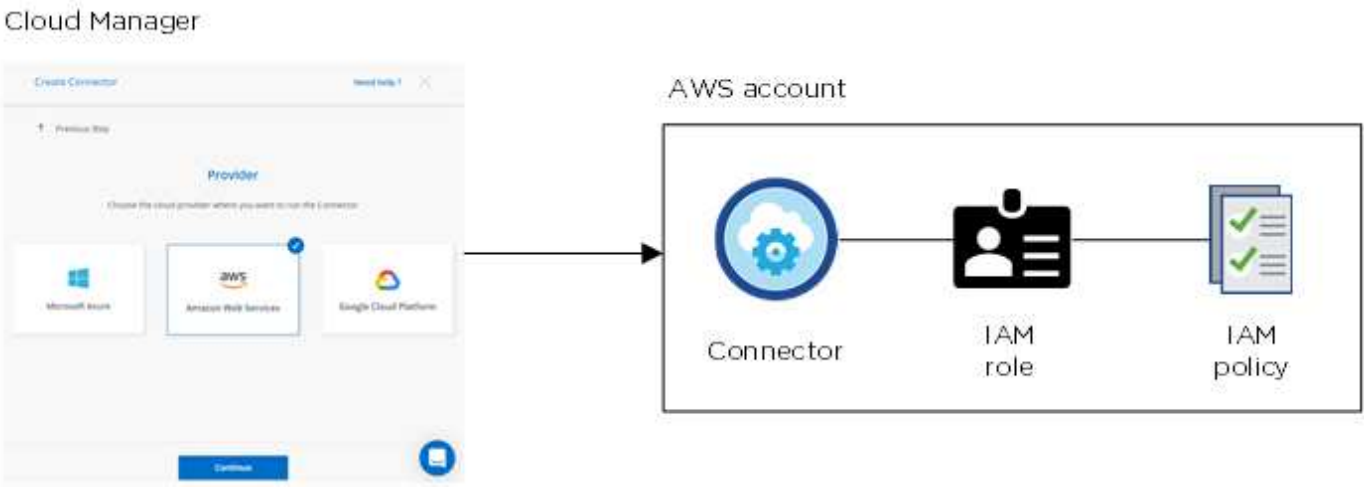
Identifiants et autorisations AWS

Cloud Manager vous permet de choisir les identifiants AWS à utiliser lors du déploiement de Cloud Volumes ONTAP. Vous pouvez déployer tous vos systèmes Cloud Volumes ONTAP à l'aide des identifiants AWS initiaux, ou ajouter des identifiants supplémentaires.

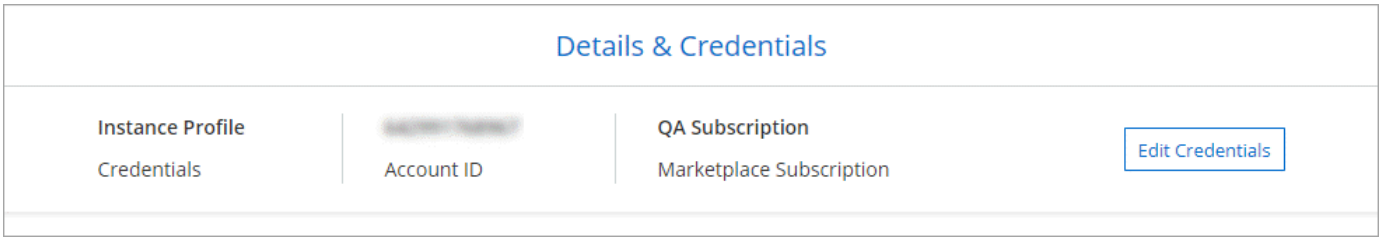
Identifiants AWS initiaux

Lorsque vous déployez un connecteur depuis Cloud Manager, vous devez utiliser un compte AWS avec des autorisations pour lancer l'instance de connecteur. Les autorisations requises sont répertoriées dans le "Règle de déploiement du connecteur pour AWS".

Lorsque Cloud Manager lance l'instance de connecteur dans AWS, il crée un rôle IAM et un profil d'instance pour l'instance. Il attache également une règle qui fournit les autorisations nécessaires à Cloud Manager pour gérer les ressources et les processus de ce compte AWS. "Examinez comment Cloud Manager utilise les autorisations".



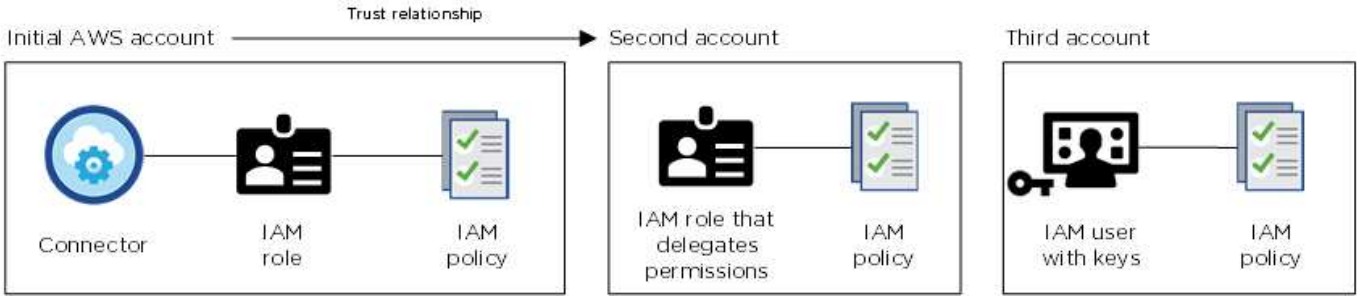
Cloud Manager sélectionne ces identifiants AWS par défaut lorsque vous créez un nouvel environnement de travail pour Cloud Volumes ONTAP :



Autres identifiants AWS

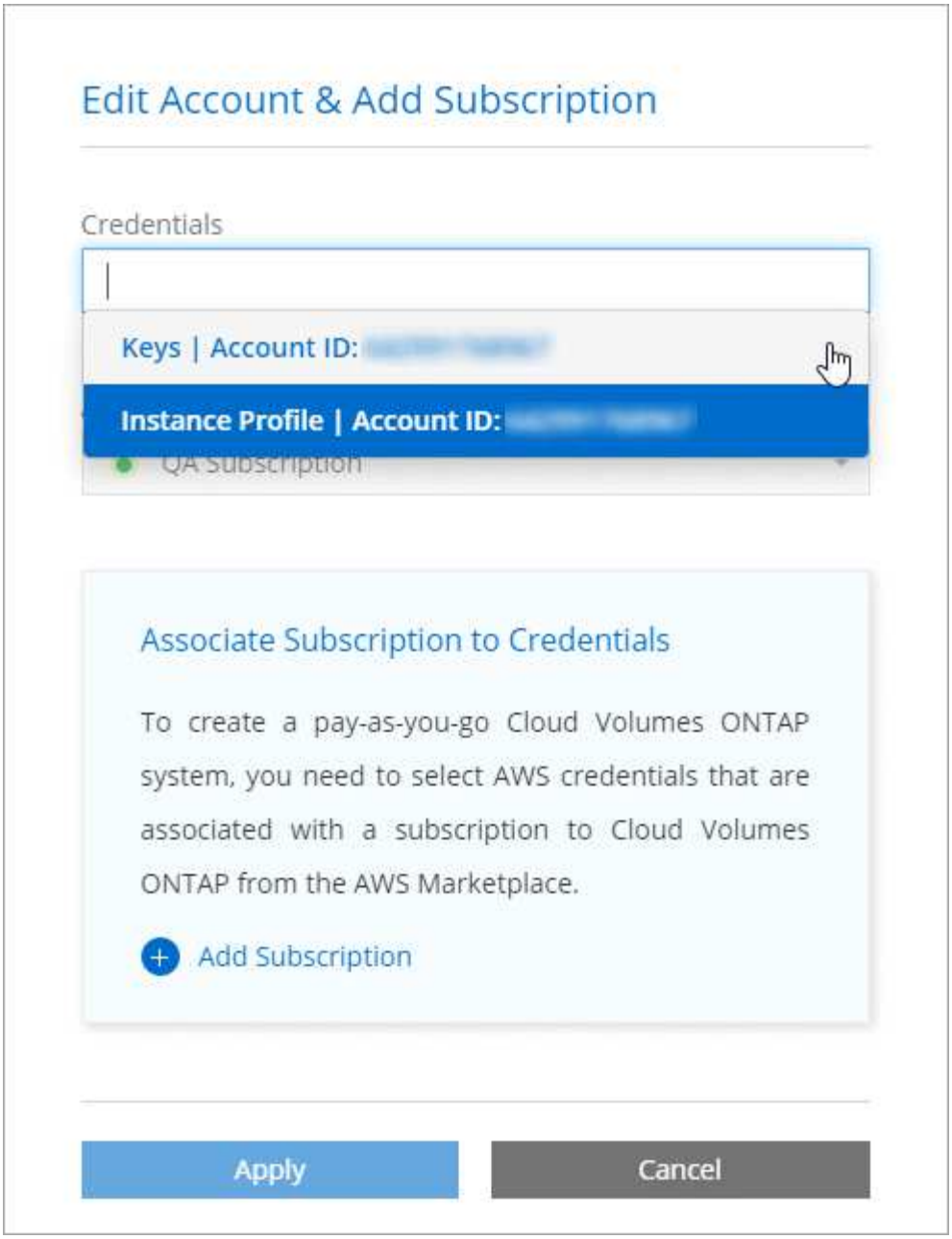
Si vous souhaitez lancer Cloud Volumes ONTAP sur différents comptes AWS, vous pouvez l'un ou l'autre "Fournir des clés AWS pour un utilisateur IAM ou le numéro ARN d'un rôle dans un compte de confiance".

L’image suivante montre deux comptes supplémentaires, l’un avec des autorisations par le biais d’un rôle IAM dans un compte de confiance et l’autre avec les clés AWS d’un utilisateur IAM :



Vous le feriez alors "Ajoutez les identifiants du compte à Cloud Manager" En spécifiant le nom de ressource Amazon (ARN) du rôle IAM ou les clés AWS pour l’utilisateur IAM.

Après avoir ajouté un autre ensemble d’informations d’identification, vous pouvez les passer lors de la création d’un nouvel environnement de travail :



Qu'en est-il des déploiements Marketplace et des déploiements sur site ?

Dans les sections ci-dessus, nous décrivons la méthode de déploiement recommandée pour le connecteur, qui provient de Cloud Manager. Vous pouvez également déployer un connecteur dans AWS à partir du "AWS Marketplace" et vous le pouvez "Installer le connecteur sur site".

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

Pour les déploiements sur site, vous ne pouvez pas configurer de rôle IAM pour le système Cloud Manager, mais vous pouvez fournir des autorisations exactement comme vous le feriez pour d'autres comptes AWS.

Comment faire tourner mes identifiants AWS en toute sécurité ?

Comme décrit ci-dessus, Cloud Manager vous permet de fournir des identifiants AWS de différentes manières : un rôle IAM associé à l'instance Connector, en assumant un rôle IAM dans un compte de confiance ou en

fournissant des clés d'accès AWS.

Avec les deux premières options, Cloud Manager utilise le service de token de sécurité AWS pour obtenir des identifiants temporaires qui pivotent en permanence. Ce processus est la meilleure pratique—il automatique et sécurisé.

Si vous fournissez les clés d'accès AWS à Cloud Manager, il est conseillé de les mettre à jour régulièrement dans Cloud Manager. Il s'agit d'un processus entièrement manuel.

Gestion des identifiants AWS et des abonnements pour Cloud Manager

Lorsque vous créez un système Cloud Volumes ONTAP, vous devez sélectionner les identifiants AWS et l'abonnement à utiliser avec ce système. Si vous gérez plusieurs abonnements AWS, vous pouvez les attribuer à différentes informations d'identification AWS à partir de la page informations d'identification.

Avant d'ajouter des identifiants AWS à Cloud Manager, vous devez fournir les autorisations requises pour ce compte. Les autorisations permettent à Cloud Manager de gérer les ressources et les processus de ce compte AWS. La manière dont vous fournissez les autorisations dépend de votre choix si vous souhaitez fournir Cloud Manager avec des clés AWS ou le NRA d'un rôle dans un compte de confiance.

Lorsque vous avez déployé un connecteur depuis Cloud Manager, Cloud Manager a automatiquement ajouté des identifiants AWS pour le compte dans lequel vous avez déployé le connecteur. Ce compte initial n'est pas ajouté si vous avez installé manuellement le logiciel Connector sur un système existant. "En savoir plus sur les identifiants et les autorisations AWS".

Choix

- Octroi d'autorisations en fournissant des clés AWS
- Octroi d'autorisations en assumant des rôles IAM dans d'autres comptes

Comment faire tourner mes identifiants AWS en toute sécurité ?

Cloud Manager vous permet de fournir des identifiants AWS de quelques façons : un rôle IAM associé à l'instance Connector, en assumant un rôle IAM dans un compte de confiance ou en fournissant des clés d'accès AWS. "En savoir plus sur les identifiants et les autorisations AWS".

Avec les deux premières options, Cloud Manager utilise le service de token de sécurité AWS pour obtenir des identifiants temporaires qui pivotent en permanence. Ce processus est la meilleure pratique, il est automatique et sécurisé.

Si vous fournissez les clés d'accès AWS à Cloud Manager, il est conseillé de les mettre à jour régulièrement dans Cloud Manager. Il s'agit d'un processus entièrement manuel.

Octroi d'autorisations en fournissant des clés AWS

Si vous souhaitez fournir Cloud Manager avec des clés AWS pour un utilisateur IAM, vous devez accorder les autorisations requises à cet utilisateur. La stratégie IAM de Cloud Manager définit les actions et les ressources AWS que Cloud Manager est autorisé à utiliser.

Étapes

1. Téléchargez la politique IAM de Cloud Manager à partir du "Page Cloud Manager Policies".
2. À partir de la console IAM, créez votre propre stratégie en copiant et en collant le texte de la stratégie IAM de Cloud Manager.

   "Documentation AWS : création de règles IAM"

3. Joignez la politique à un rôle IAM ou à un utilisateur IAM.
   - "Documentation AWS : création de rôles IAM"
   - "Documentation AWS : ajout et suppression de règles IAM"

Résultat

Le compte dispose désormais des autorisations requises. Vous pouvez désormais l'ajouter à Cloud Manager.

Octroi d'autorisations en assumant des rôles IAM dans d'autres comptes

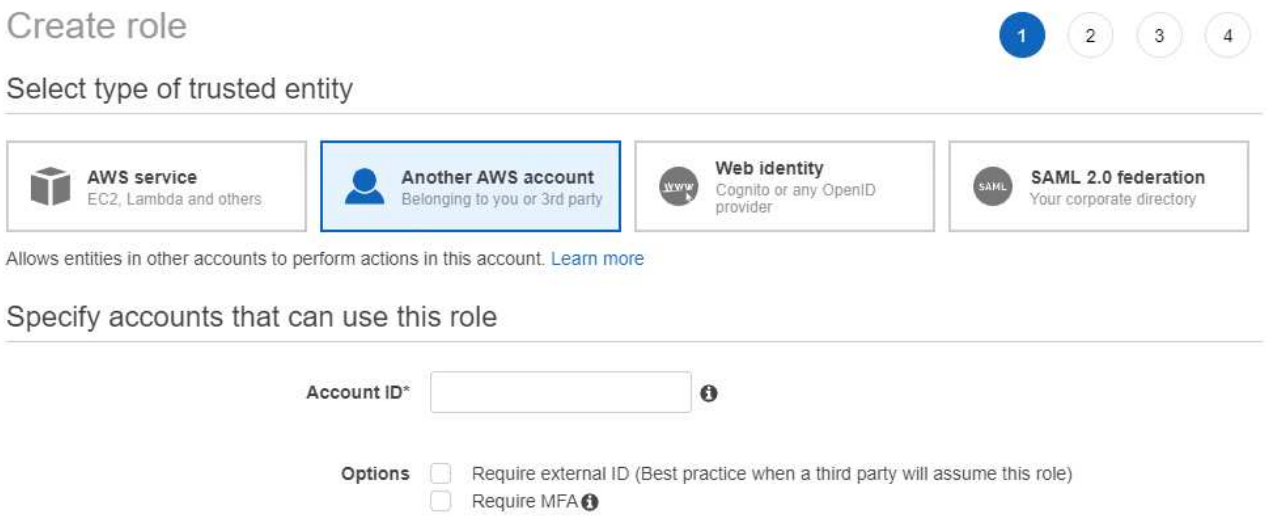
Vous pouvez définir une relation de confiance entre le compte AWS source dans lequel vous avez déployé l'instance Connector et d'autres comptes AWS en utilisant les rôles IAM. Vous pouvez ensuite fournir à Cloud Manager l'ARN des rôles IAM depuis les comptes de confiance.

Étapes

1. Accédez au compte cible sur lequel vous souhaitez déployer Cloud Volumes ONTAP et créez un rôle IAM en sélectionnant **un autre compte AWS**.

   Assurez-vous de faire ce qui suit :

   - Saisissez l'ID du compte sur lequel réside l'instance de connecteur.
   - Joignez la politique IAM de Cloud Manager, disponible à partir du "Page Cloud Manager Policies".



2. Accédez au compte source où se trouve l'instance de connecteur et sélectionnez le rôle IAM associé à l'instance.

   a. Cliquez sur **attacher des stratégies**, puis sur **Créer une stratégie**.

   b. Créez une stratégie qui inclut l'action « sts:AssumeRole » et l'ARN du rôle que vous avez créé dans le compte cible.

Exemple

```
{
 "Version": "2012-10-17",
 "Statement": {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
}
}
```

Résultat

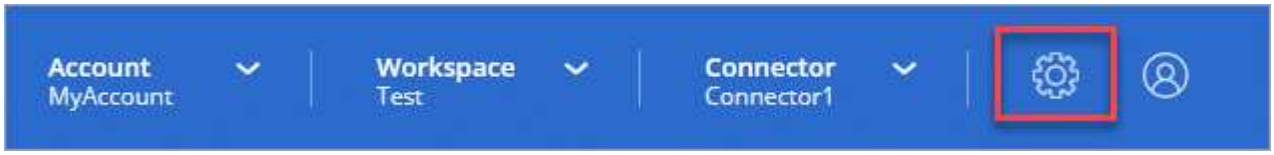
Le compte dispose désormais des autorisations requises. Vous pouvez désormais l'ajouter à Cloud Manager.

Ajout d'identifiants AWS à Cloud Manager

Une fois que vous avez passé un compte AWS avec les autorisations requises, vous pouvez ajouter les identifiants de ce compte à Cloud Manager. Vous pouvez ainsi lancer les systèmes Cloud Volumes ONTAP de ce compte.

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.



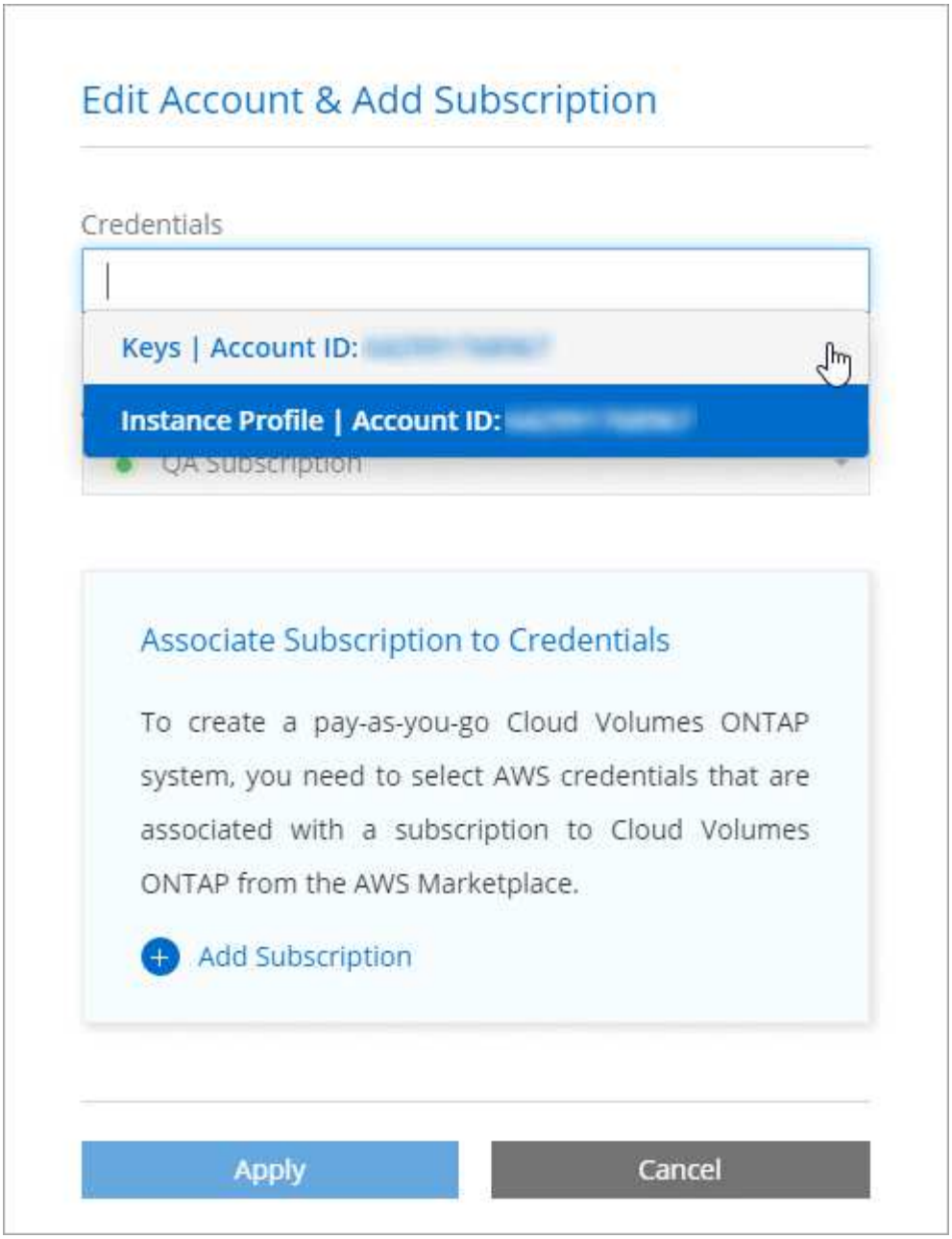
2. Cliquez sur **Ajouter des informations d'identification** et sélectionnez **AWS**.
3. Vous pouvez fournir des clés AWS ou l'ARN d'un rôle IAM approuvé.
4. Vérifiez que les exigences de la politique ont été respectées et cliquez sur **Continuer**.
5. Choisissez l'abonnement payant à l'utilisation que vous souhaitez associer aux informations d'identification ou cliquez sur **Ajouter un abonnement** si vous n'en avez pas encore.

   Pour créer un système Cloud Volumes ONTAP avec paiement à l'utilisation, vous devez associer des identifiants AWS à un abonnement à Cloud Volumes ONTAP à partir d'AWS Marketplace.

6. Cliquez sur **Ajouter**.

Résultat

Vous pouvez maintenant passer à un autre ensemble d'informations d'identification à partir de la page Détails et informations d'identification lors de la création d'un nouvel environnement de travail :



Association d'un abonnement AWS aux identifiants

Après avoir ajouté vos identifiants AWS à Cloud Manager, vous pouvez associer un abonnement AWS Marketplace à ces identifiants. Cet abonnement vous permet de créer un système Cloud Volumes ONTAP basé sur l'utilisation et d'utiliser d'autres services cloud NetApp.

Deux scénarios peuvent vous être associés à un abonnement AWS Marketplace une fois que vous avez déjà ajouté les identifiants à Cloud Manager :

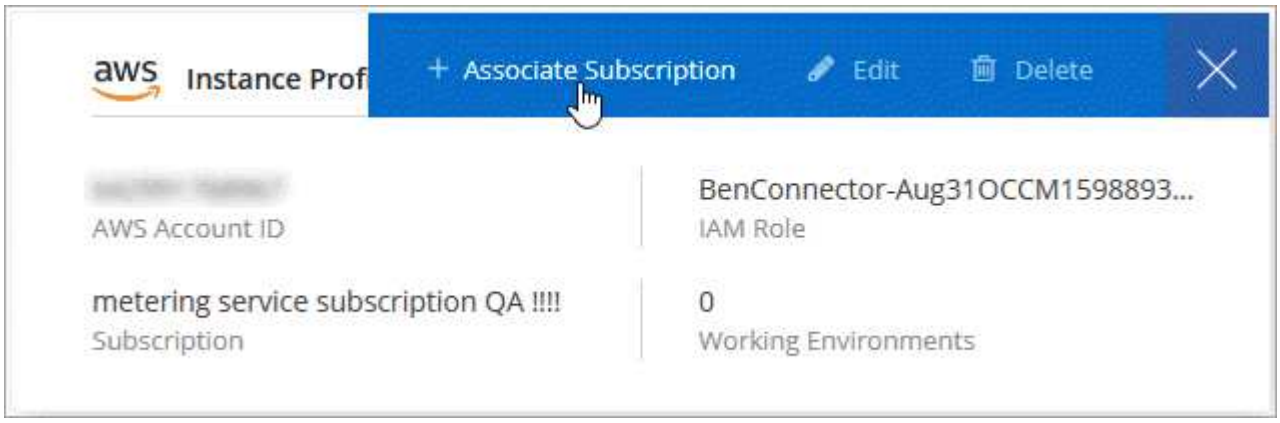
- Vous n'avez pas associé un abonnement lors de l'ajout initial des identifiants à Cloud Manager.
- Vous souhaitez remplacer un abonnement AWS Marketplace existant par un nouvel abonnement.

Ce dont vous avez besoin

Vous devez créer un connecteur pour modifier les paramètres de Cloud Manager. "Découvrez comment".

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.
2. Passez le curseur de la souris sur un ensemble d'informations d'identification et cliquez sur le menu d'action.
3. Dans le menu, cliquez sur **associer abonnement**.



4. Sélectionnez un abonnement dans la liste déroulante ou cliquez sur **Ajouter un abonnement** et suivez les étapes pour créer un nouvel abonnement.

   ► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_aws.mp4 *(video)*

Azure

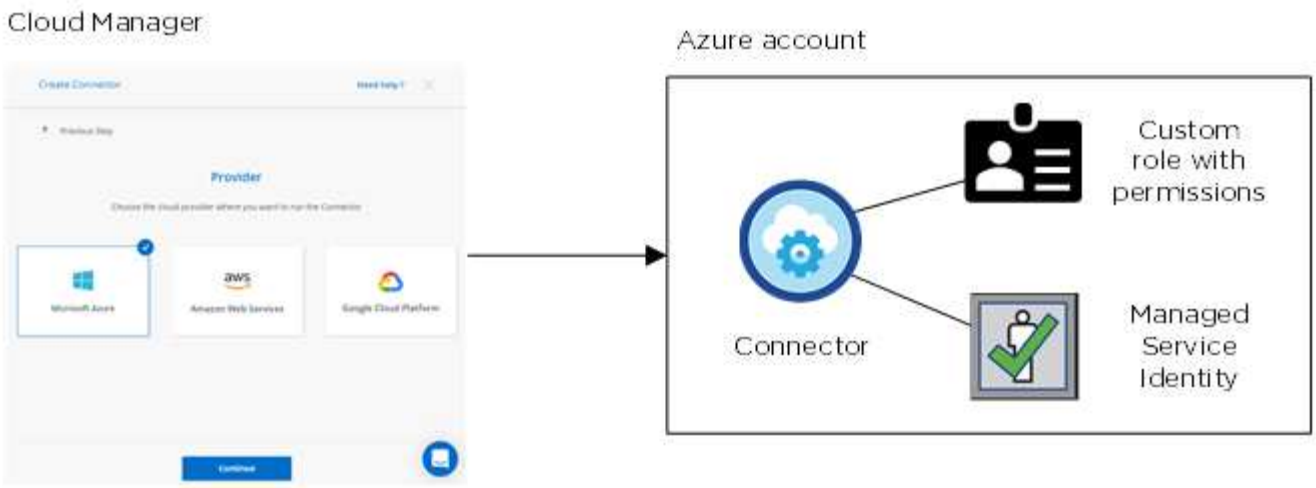
Identifiants et autorisations Azure

Cloud Manager vous permet de choisir les identifiants Azure à utiliser lors du déploiement de Cloud Volumes ONTAP. Vous pouvez déployer tous vos systèmes Cloud Volumes ONTAP à l'aide des identifiants Azure initiaux, ou ajouter des identifiants supplémentaires.

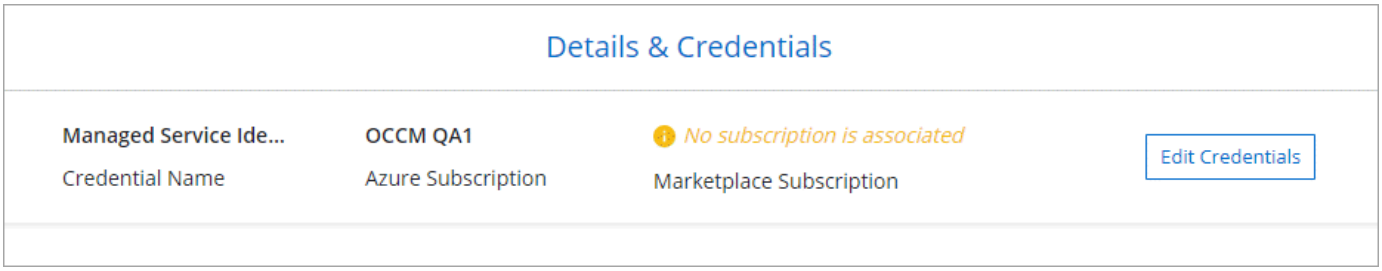
Les identifiants initiaux d'Azure

Lorsque vous déployez un connecteur depuis Cloud Manager, vous devez utiliser un compte Azure avec les autorisations de déployer la machine virtuelle Connector. Les autorisations requises sont répertoriées dans le "Stratégie de déploiement de Connector pour Azure".

Lorsque Cloud Manager déploie la machine virtuelle de connecteur dans Azure, il active une "identité gérée attribuée par le système" sur une machine virtuelle, crée un rôle personnalisé et le attribue à la machine virtuelle. Le rôle fournit à Cloud Manager des autorisations de gestion des ressources et des processus au sein de cet abonnement Azure. "Examinez comment Cloud Manager utilise les autorisations".



Cloud Manager sélectionne ces identifiants Azure par défaut lorsque vous créez un nouvel environnement de travail pour Cloud Volumes ONTAP :

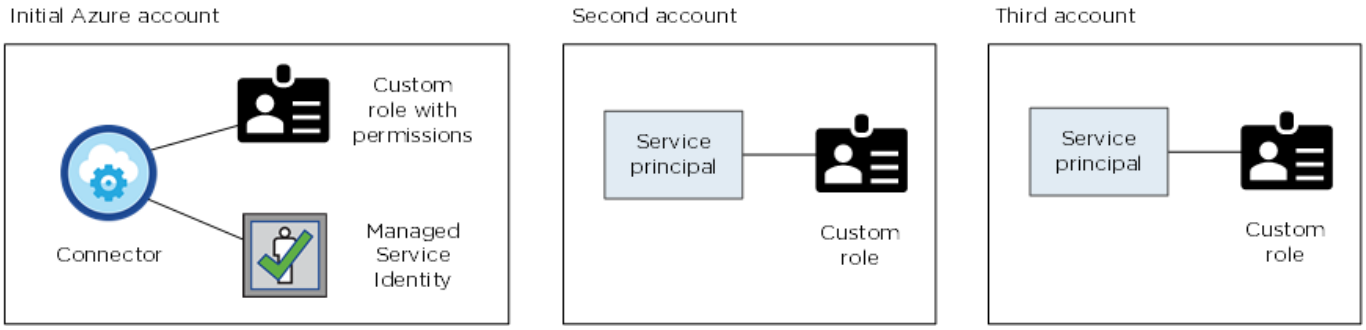


Des abonnements Azure supplémentaires pour une identité gérée

L'identité gérée est associée à l'abonnement dans lequel vous avez lancé le connecteur. Si vous souhaitez sélectionner un autre abonnement Azure, vous devez le faire "associez l'identité gérée à ces abonnements".

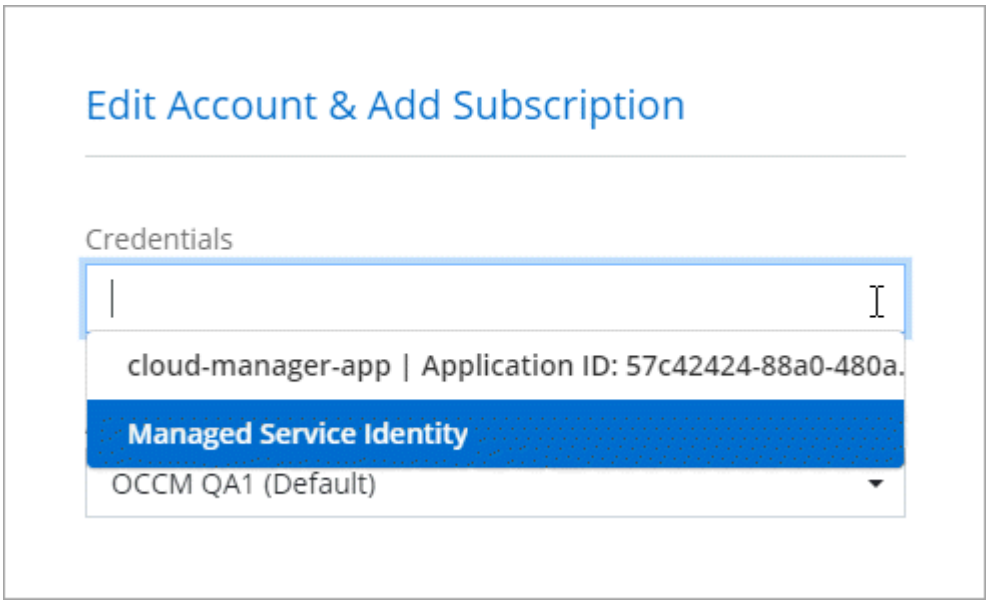
Autres identifiants Azure

Si vous souhaitez déployer Cloud Volumes ONTAP avec différents identifiants Azure, vous devez accorder les autorisations requises par "Création et configuration d'une entité de service dans Azure Active Directory" Pour chaque compte Azure. L'image suivante montre deux comptes supplémentaires, chacun étant doté d'un rôle principal de service et personnalisé qui fournit des autorisations :



Vous le feriez alors "Ajoutez les identifiants du compte à Cloud Manager" En fournissant des détails sur le principal du service AD.

Après avoir ajouté un autre ensemble d'informations d'identification, vous pouvez les passer lors de la création d'un nouvel environnement de travail :



Qu'en est-il des déploiements Marketplace et des déploiements sur site ?

Les sections ci-dessus décrivent la méthode de déploiement recommandée pour le connecteur, qui provient de NetApp Cloud Central. Vous pouvez également déployer un connecteur dans Azure à partir du "Azure Marketplace", et vous pouvez "Installer le connecteur sur site".

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

Pour les déploiements sur site, vous ne pouvez pas configurer une identité gérée pour le connecteur, mais vous pouvez fournir des autorisations comme vous le feriez pour des comptes supplémentaires en utilisant une entité de service.

Gestion des identifiants Azure et des abonnements pour Cloud Manager

Lorsque vous créez un système Cloud Volumes ONTAP, vous devez sélectionner les identifiants Azure et l'abonnement Marketplace pour les utiliser avec ce système. Si vous gérez plusieurs abonnements Azure Marketplace, vous pouvez les attribuer à différentes informations d'identification Azure à partir de la page informations d'identification.

Il existe deux façons de gérer les identifiants Azure dans Cloud Manager. Tout d'abord, si vous souhaitez déployer Cloud Volumes ONTAP sur différents comptes Azure, vous devez fournir les autorisations requises et ajouter les identifiants à Cloud Manager. La deuxième méthode consiste à associer des abonnements supplémentaires à l'identité gérée Azure.

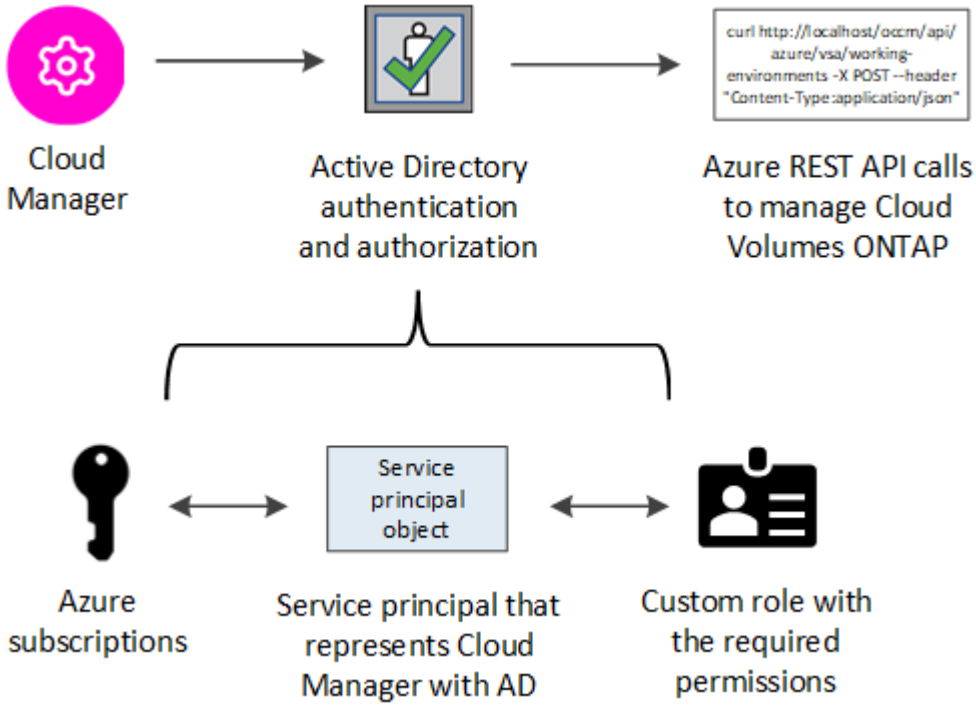
Lorsque vous déployez un connecteur depuis Cloud Manager, Cloud Manager ajoute automatiquement le compte Azure dans lequel vous avez déployé le connecteur. Un compte initial n'est pas ajouté si vous avez installé manuellement le logiciel Connector sur un système existant. "En savoir plus sur les comptes et les autorisations Azure".

Octroi d'autorisations Azure à l'aide d'une entité de sécurité de service

Cloud Manager a besoin d'autorisations pour effectuer des actions dans Azure. Vous pouvez accorder les autorisations requises à un compte Azure en créant et en configurant une entité de sécurité de service dans Azure Active Directory et en obtenant les informations d'identification Azure requises par Cloud Manager.

Description de la tâche

L'image suivante illustre comment Cloud Manager obtient les autorisations nécessaires pour effectuer des opérations dans Azure. Un objet principal de service, lié à un ou plusieurs abonnements Azure, représente Cloud Manager dans Azure Active Directory et est affecté à un rôle personnalisé qui permet les autorisations requises.



Étapes

1. Créez une application Azure Active Directory.
2. Attribuez l'application à un rôle.
3. Ajoutez des autorisations d'API de gestion de service Windows Azure.
4. Obtenir l'ID de l'application et l'ID du répertoire.
5. Créez un secret client.

Création d'une application Azure Active Directory

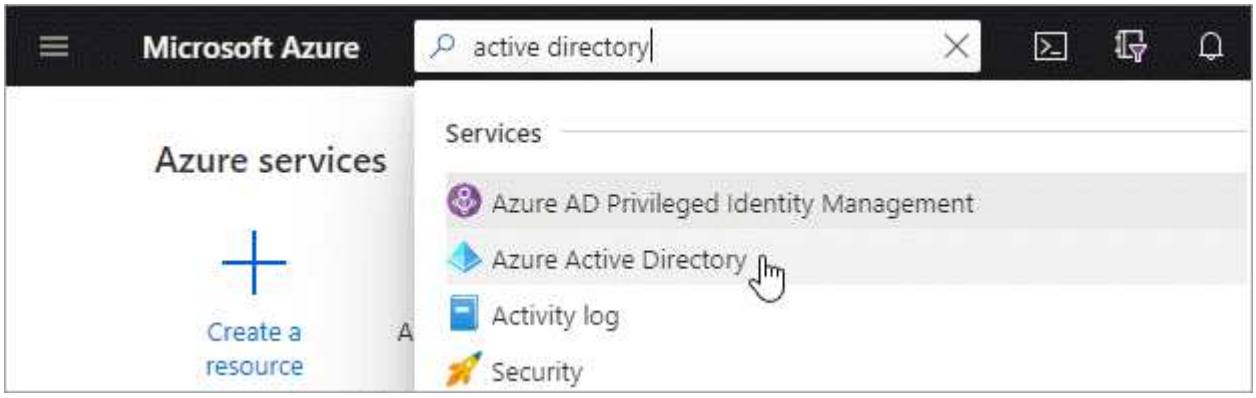
Créez une application Azure Active Directory (AD) et une entité de service que Cloud Manager peut utiliser pour le contrôle d'accès basé sur des rôles.

Avant de commencer

Vous devez disposer des droits d'accès 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".

Étapes

1. À partir du portail Azure, ouvrez le service **Azure Active Directory**.



2. Dans le menu, cliquez sur **enregistrements d'applications**.
3. Cliquez sur **Nouvelle inscription**.
4. Spécifiez les détails de l'application :
   - **Nom** : saisissez un nom pour l'application.
   - **Type de compte** : sélectionnez un type de compte (tout fonctionne avec Cloud Manager).
   - **Redirect URI** : sélectionnez **Web**, puis entrez n'importe quelle URL, par exemple, https://url
5. Cliquez sur **Enregistrer**.

Résultat

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

Affectation de l'application à un rôle

Vous devez lier la principale de service à un ou plusieurs abonnements Azure et lui attribuer le rôle « opérateur OnCommand Cloud Manager » personnalisé pour que Cloud Manager possède des autorisations dans Azure.

Étapes

1. Création d'un rôle personnalisé :

   a. Téléchargez le "Politique de Cloud Manager Azure".

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

   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.

L'exemple suivant montre comment créer un rôle personnalisé à l'aide de l'interface de ligne de commande Azure CLI 2.0 :

```
az role definition create --role-definition
C:\Policy_for_cloud_Manager_Azure_3.8.7.json
```

Vous devriez maintenant avoir un rôle personnalisé appelé *Cloud Manager Operator*.

2. Attribuez l'application au rôle :

   a. À partir du portail Azure, ouvrez le service **abonnements**.

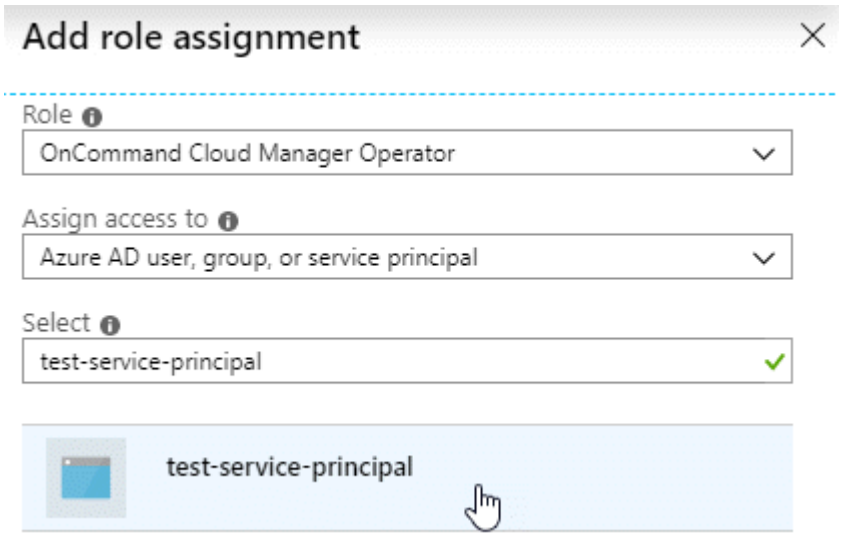
   b. Sélectionnez l'abonnement.

   c. Cliquez sur **contrôle d'accès (IAM) > Ajouter > Ajouter une affectation de rôle**.

   d. Sélectionnez le rôle **opérateur** de Cloud Manager.

   e. Conserver *l'utilisateur, le groupe ou le principal de service AD d'Azure sélectionné.

   f. Recherchez le nom de l'application (vous ne pouvez pas le trouver dans la liste en faisant défiler la liste).



   g. Sélectionnez l'application et cliquez sur **Enregistrer**.

   Le principal de service de Cloud Manager dispose désormais des autorisations Azure requises pour cet abonnement.

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. Cloud Manager vous permet de sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

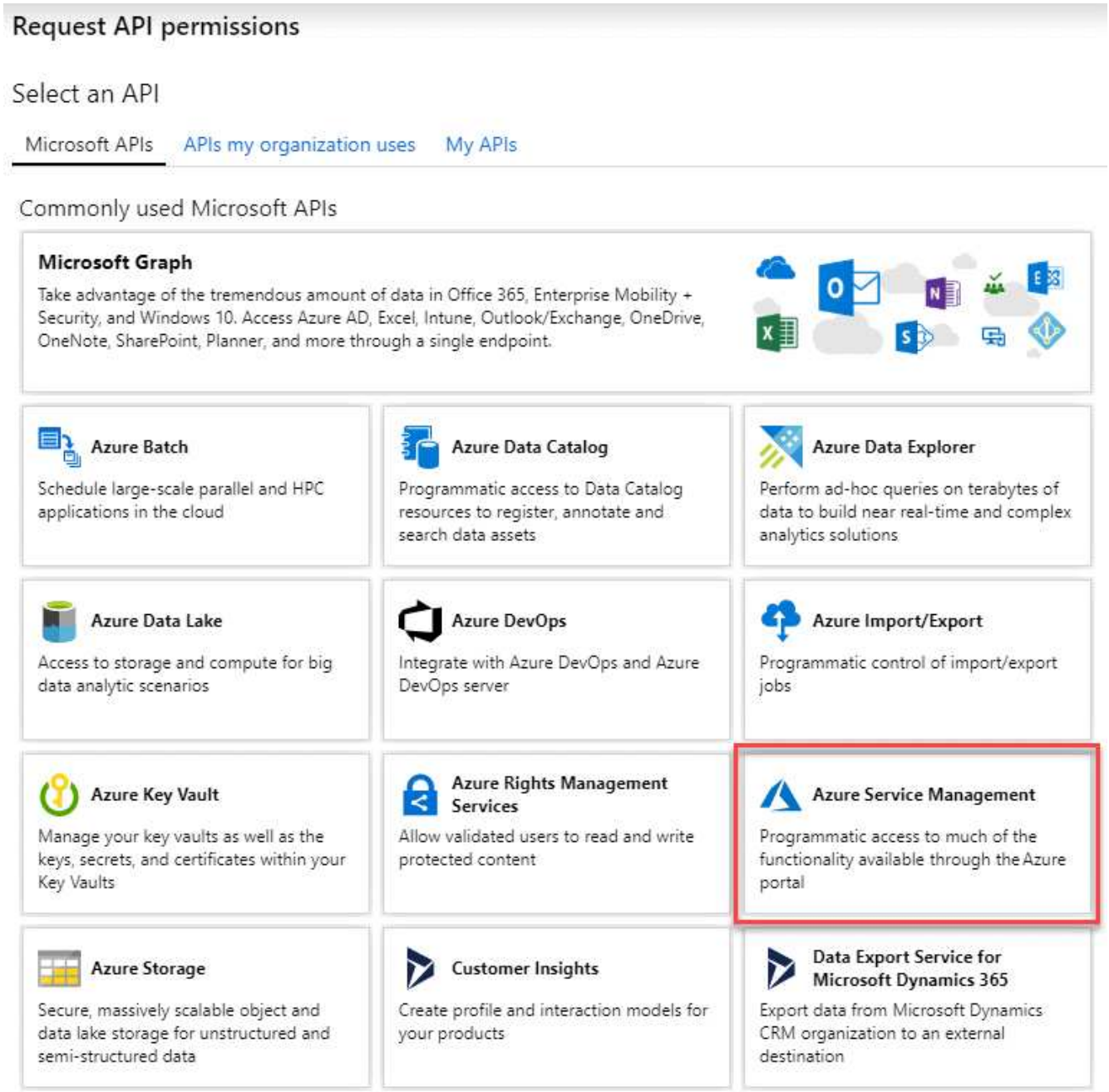
Ajout d'autorisations d'API de gestion des services Windows Azure

Le principal de service doit disposer d'autorisations « API de gestion des services Windows Azure ».

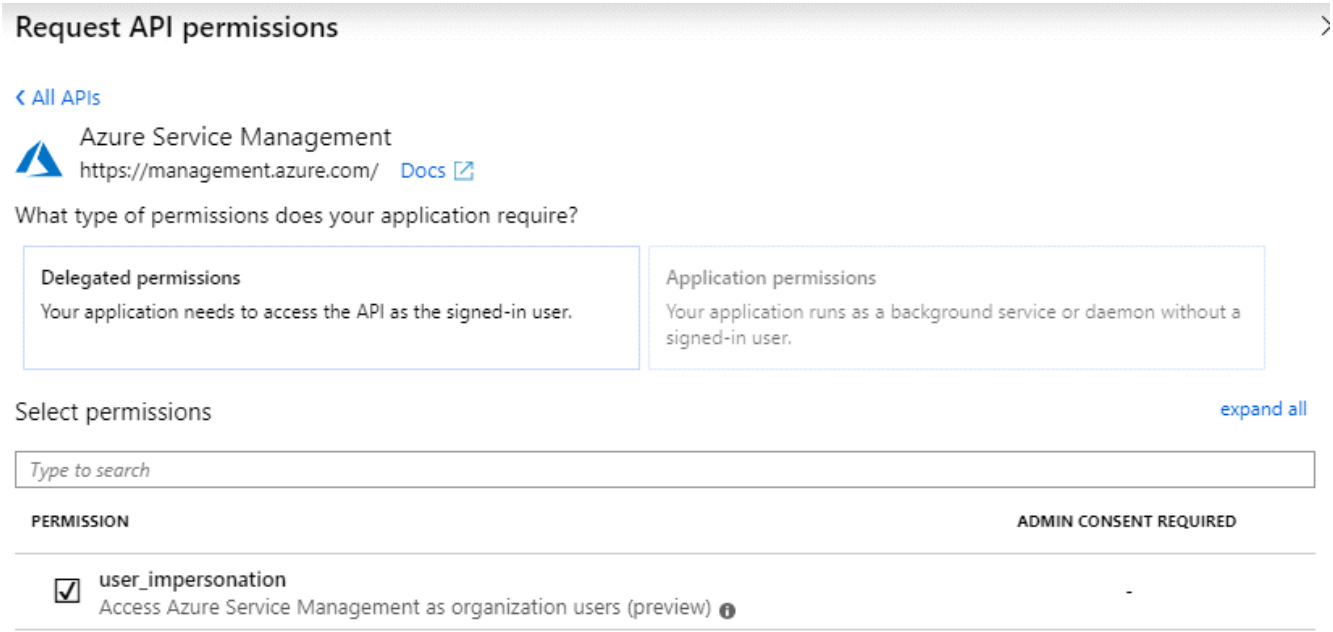
Étapes

1. Dans le service **Azure Active Directory**, cliquez sur **App inscriptions** et sélectionnez l'application.
2. Cliquez sur **autorisations API > Ajouter une autorisation**.

3. Sous **Microsoft API**, sélectionnez **Azure Service Management**.



4. Cliquez sur **Access Azure Service Management en tant qu'utilisateurs d'organisation**, puis sur **Add permissions**.

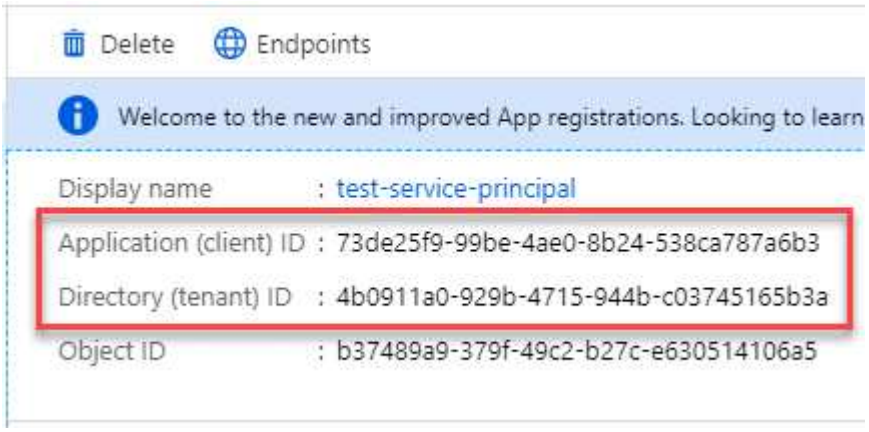


Obtention de l'ID d'application et de l'ID de répertoire

Lorsque vous ajoutez le compte Azure dans Cloud Manager, vous devez fournir l'ID d'application (client) et l'ID de répertoire (locataire) de l'application. Cloud Manager utilise ces identifiants pour vous connecter automatiquement.

Étapes

1. Dans le service **Azure Active Directory**, cliquez sur **App inscriptions** et sélectionnez l'application.
2. Copiez l'ID **application (client)** et l'ID **Directory (tenant)**.



Création d'un secret client

Vous devez créer un secret client, puis fournir à Cloud Manager la valeur du secret pour que Cloud Manager puisse l'utiliser pour vous authentifier avec Azure AD.

Lorsque vous ajoutez le compte à Cloud Manager, Cloud Manager fait référence au secret client en tant que clé d'application.

Étapes

1. Ouvrez le service **Azure Active Directory**.
2. Cliquez sur **App Inregistrations** et sélectionnez votre application.
3. Cliquez sur **certificats et secrets > Nouveau secret client**.
4. Fournissez une description du secret et une durée.
5. Cliquez sur **Ajouter**.
6. Copier 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 (tenant) et la valeur du secret client. Vous devez saisir ces informations dans Cloud Manager lorsque vous ajoutez un compte Azure.

Ajout d'identifiants Azure à Cloud Manager

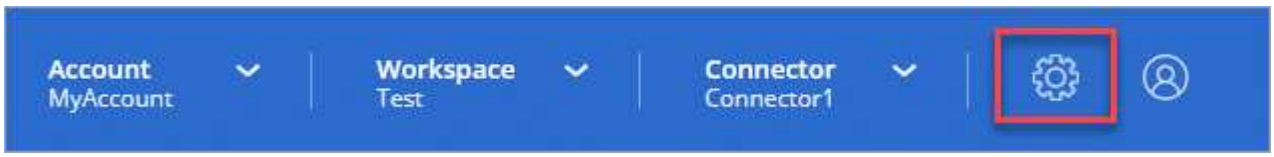
Une fois que vous avez autorisé à fournir un compte Azure, vous pouvez ajouter les identifiants de ce compte à Cloud Manager. Vous pouvez ainsi lancer les systèmes Cloud Volumes ONTAP de ce compte.

Ce dont vous avez besoin

Vous devez créer un connecteur pour modifier les paramètres de Cloud Manager. "Découvrez comment".

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.



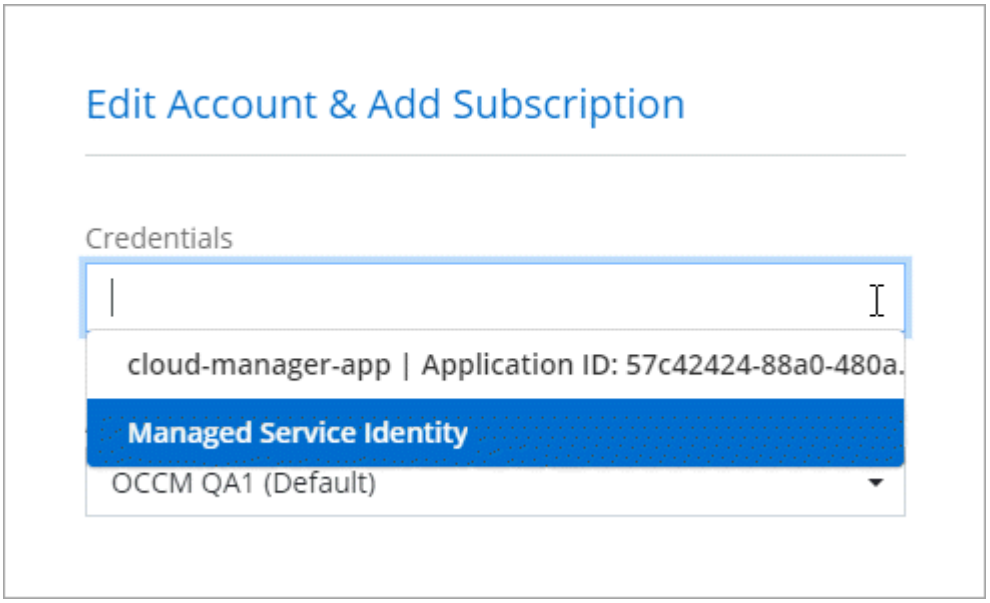
2. Cliquez sur **Ajouter des informations d'identification** et sélectionnez **Microsoft Azure**.
3. Entrez des informations sur l'entité de sécurité du service Azure Active Directory qui accorde les autorisations requises :
   - ID de l'application (client) : voir Obtention de l'ID d'application et de l'ID de répertoire.
   - ID de répertoire (locataire) : voir Obtention de l'ID d'application et de l'ID de répertoire.
   - Secret client : voir Création d'un secret client.
4. Vérifiez que les exigences de la stratégie ont été respectées, puis cliquez sur **Continuer**.
5. Choisissez l'abonnement payant à l'utilisation que vous souhaitez associer aux informations d'identification ou cliquez sur **Ajouter un abonnement** si vous n'en avez pas encore.

Pour créer un système Cloud Volumes ONTAP basé sur l'utilisation, vous devez associer des identifiants Azure à un abonnement à Cloud Volumes ONTAP à partir d'Azure Marketplace.

6. Cliquez sur **Ajouter**.

Résultat

Vous pouvez maintenant passer à différents ensembles d'informations d'identification à partir de la page Détails et informations d'identification "lors de la création d'un nouvel environnement de travail":



Association d'un abonnement à Azure Marketplace aux identifiants

Après avoir ajouté vos identifiants Azure à Cloud Manager, vous pouvez associer un abonnement Azure Marketplace à ces identifiants. Cet abonnement vous permet de créer un système Cloud Volumes ONTAP basé sur l'utilisation et d'utiliser d'autres services cloud NetApp.

Deux scénarios peuvent s'avérer nécessaires pour associer un abonnement Azure Marketplace une fois que vous avez déjà ajouté les identifiants à Cloud Manager :

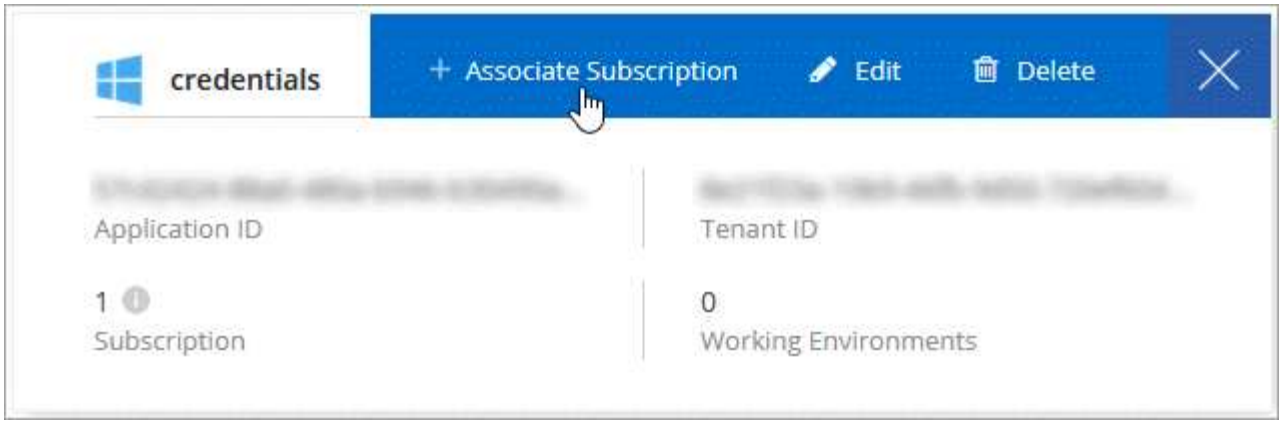
- Vous n'avez pas associé un abonnement lors de l'ajout initial des identifiants à Cloud Manager.
- Vous souhaitez remplacer un abonnement Azure Marketplace existant par un nouvel abonnement.

Ce dont vous avez besoin

Vous devez créer un connecteur pour modifier les paramètres de Cloud Manager. "Découvrez comment".

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.
2. Passez le curseur de la souris sur un ensemble d'informations d'identification et cliquez sur le menu d'action.
3. Dans le menu, cliquez sur **associer abonnement**.



4. Sélectionnez un abonnement dans la liste déroulante ou cliquez sur **Ajouter un abonnement** et suivez les étapes pour créer un nouvel abonnement.

   La vidéo suivante démarre à partir du contexte de l'assistant de l'environnement de travail, mais vous montre le même flux de travail après avoir cliqué sur **Ajouter un abonnement** :

   ► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_azure.mp4 *(video)*

Association d'abonnements Azure supplémentaires à une identité gérée

Cloud Manager vous permet de choisir les identifiants Azure et l'abonnement Azure dans lesquels vous souhaitez déployer Cloud Volumes ONTAP. Vous ne pouvez pas sélectionner un autre abonnement Azure pour le profil d'identité gérée à moins d'associer le "identité gérée" avec ces abonnements.

Description de la tâche

Une identité gérée est "Compte Azure initial" Lorsque vous déployez un connecteur depuis Cloud Manager. Une fois que vous avez déployé Connector, Cloud Manager a créé le rôle de l'opérateur Cloud Manager et l'a attribué à la machine virtuelle du connecteur.

Étapes

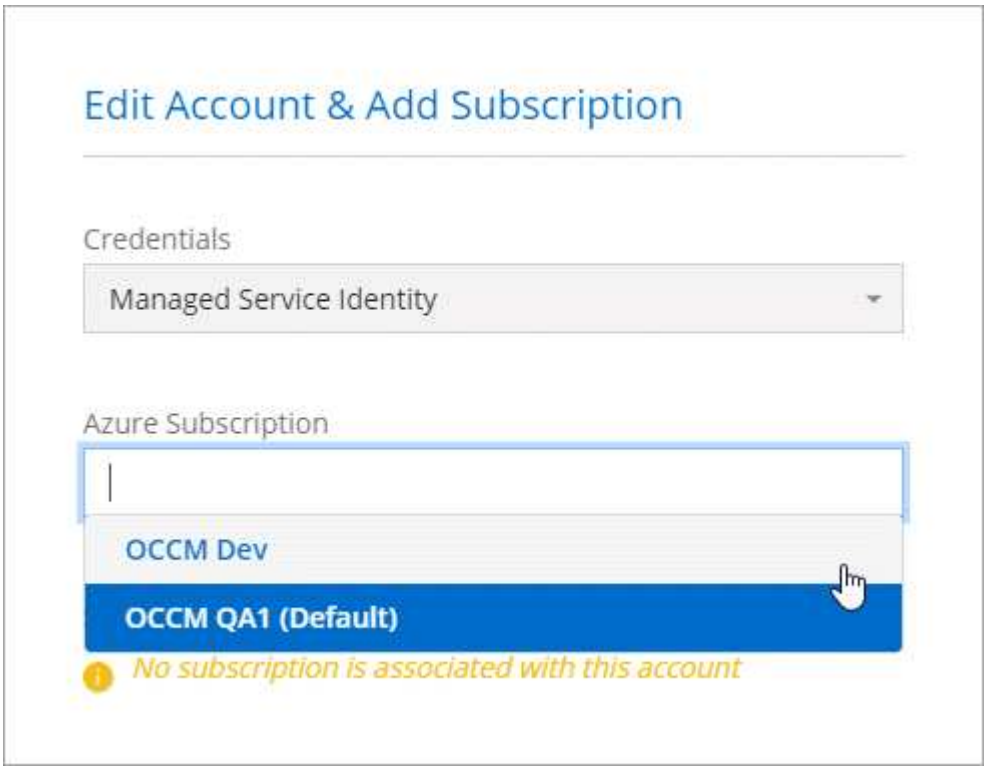
1. Connectez-vous au portail Azure.
2. Ouvrez le service **abonnements**, puis sélectionnez l'abonnement dans lequel vous souhaitez déployer Cloud Volumes ONTAP.
3. Cliquez sur **contrôle d'accès (IAM)**.
   a. Cliquez sur **Ajouter** > **Ajouter une affectation de rôle**, puis ajoutez les autorisations suivantes :
      - Sélectionnez le rôle **opérateur** de Cloud Manager.

        L'opérateur de Cloud Manager est le nom par défaut fourni dans "Politique de Cloud Manager". Si vous avez choisi un autre nom pour le rôle, sélectionnez-le à la place.

      - Attribuez l'accès à une **machine virtuelle**.
      - Sélectionnez l'abonnement dans lequel la machine virtuelle du connecteur a été créée.
      - Sélectionnez la machine virtuelle Connector.
      - Cliquez sur **Enregistrer**.
4. Répétez ces étapes pour les abonnements supplémentaires.

Résultat

Lorsque vous créez un nouvel environnement de travail, vous devriez désormais pouvoir sélectionner plusieurs abonnements Azure pour le profil d'identité géré.



GCP

Projets, autorisations et comptes Google Cloud

Un compte de service fournit à Cloud Manager les autorisations de déploiement et de gestion des systèmes Cloud Volumes ONTAP dans le même projet que Cloud Manager, ou dans des projets différents.

Projet et autorisations pour Cloud Manager

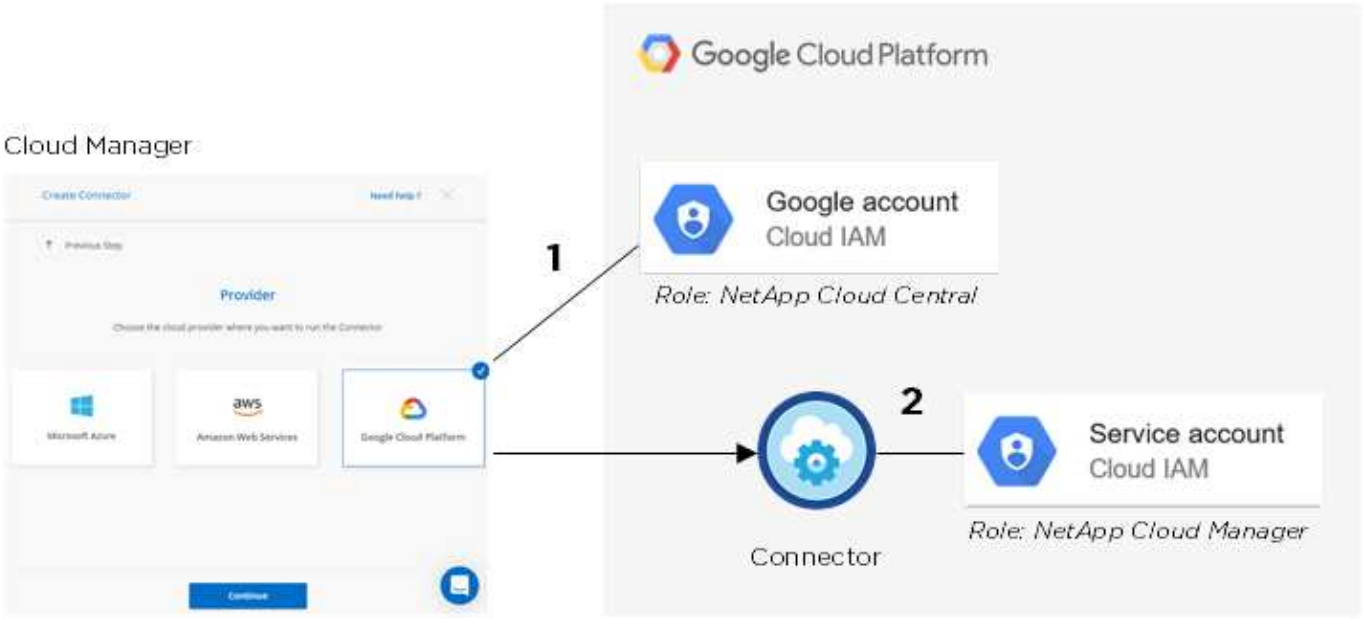
Avant de déployer Cloud Volumes ONTAP dans Google Cloud, vous devez d'abord déployer un connecteur dans un projet Google Cloud. Il ne peut pas s'exécuter sur site ou dans un autre fournisseur cloud.

Deux ensembles d'autorisations doivent être en place avant de déployer un connecteur directement depuis Cloud Manager :

1. Vous devez déployer un connecteur à l'aide d'un compte Google disposant des autorisations nécessaires pour lancer l'instance de VM Connector à partir de Cloud Manager.
2. Lorsque vous déployez le connecteur, vous êtes invité à sélectionner un "compte de service" Pour l'instance de VM. Cloud Manager obtient les autorisations du compte de service pour créer et gérer les systèmes Cloud Volumes ONTAP en votre nom. Les autorisations sont fournies en ajoutant un rôle personnalisé au compte de service.

Nous avons configuré deux fichiers YAML qui incluent les autorisations requises pour l'utilisateur et le compte de service. "Découvrez comment utiliser les fichiers YAML pour configurer les autorisations".

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



Projet pour Cloud Volumes ONTAP

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

- "Découvrez comment configurer un compte de service (voir étape 2)".
- "Découvrez comment déployer Cloud Volumes ONTAP dans GCP et sélectionner un projet".

Compte tenu du Tiering des données

Cloud Manager requiert un compte GCP pour Cloud Volumes ONTAP 9.6, mais pas pour la version 9.7 et ultérieure. Si vous souhaitez utiliser le Tiering des données avec Cloud Volumes ONTAP 9.7, suivez les étapes 4 à "Mise en route de Cloud Volumes ONTAP dans Google Cloud Platform".

L'ajout d'un compte Google Cloud à Cloud Manager permet le Tiering des données sur un système Cloud Volumes ONTAP 9.6. Le Tiering des données transfère automatiquement les données inactives vers un stockage objet plus économique, ce qui vous permet de récupérer de l'espace dans votre stockage primaire et de réduire le stockage secondaire.

Lorsque vous ajoutez ce compte, vous devez fournir à Cloud Manager une clé d'accès de stockage pour un compte de service disposant des autorisations d'administrateur de stockage. Cloud Manager utilise les clés d'accès pour configurer et gérer un compartiment de stockage cloud pour le Tiering des données.

Une fois que vous avez ajouté un compte Google Cloud, vous pouvez activer le Tiering des données sur les volumes individuels lorsque vous les créez, les modifiez ou les répliquez.

- "Découvrez comment configurer et ajouter des comptes GCP à Cloud Manager".
- "Découvrez comment transférer des données inactives vers un stockage objet à faible coût".

Gestion des identifiants GCP et des abonnements pour Cloud Manager

Vous pouvez gérer deux types d'identifiants Google Cloud Platform dans Cloud Manager

: les identifiants qui sont associés à l'instance de machine virtuelle de connecteur et les clés d'accès de stockage utilisées avec un système Cloud Volumes ONTAP 9.6 pour "tiering des données".

Association d'un abonnement Marketplace aux informations d'identification GCP

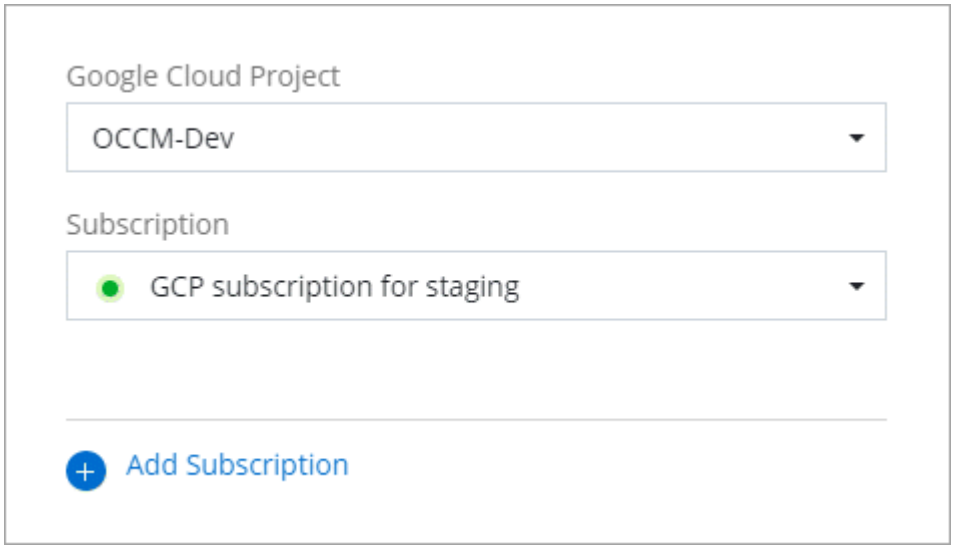
Lorsque vous déployez un connecteur dans GCP, Cloud Manager crée un ensemble d'identifiants par défaut associés à l'instance de VM de connecteur. Ce sont les identifiants utilisés par Cloud Manager pour déployer Cloud Volumes ONTAP.

Vous pouvez à tout moment modifier l'abonnement Marketplace associé à ces informations d'identification. Cet abonnement vous permet de créer un système Cloud Volumes ONTAP basé sur l'utilisation et d'utiliser d'autres services cloud NetApp.

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.
2. Passez le curseur de la souris sur un ensemble d'informations d'identification et cliquez sur le menu d'action.
3. Dans le menu, cliquez sur **associer abonnement**.

4. Sélectionnez un projet et un abonnement Google Cloud dans la liste déroulante ou cliquez sur **Ajouter un abonnement** et suivez les étapes pour créer un nouvel abonnement.



5. Cliquez sur **associé**.

Configuration et ajout de comptes GCP pour le Tiering des données avec Cloud Volumes ONTAP 9.6

Si vous souhaitez activer un système Cloud Volumes ONTAP 9.6 pour "tiering des données", Vous devez fournir à Cloud Manager une clé d'accès au stockage pour un compte de service disposant des autorisations d'administrateur de stockage. Cloud Manager utilise les clés d'accès pour configurer et gérer un compartiment de stockage cloud pour le Tiering des données.

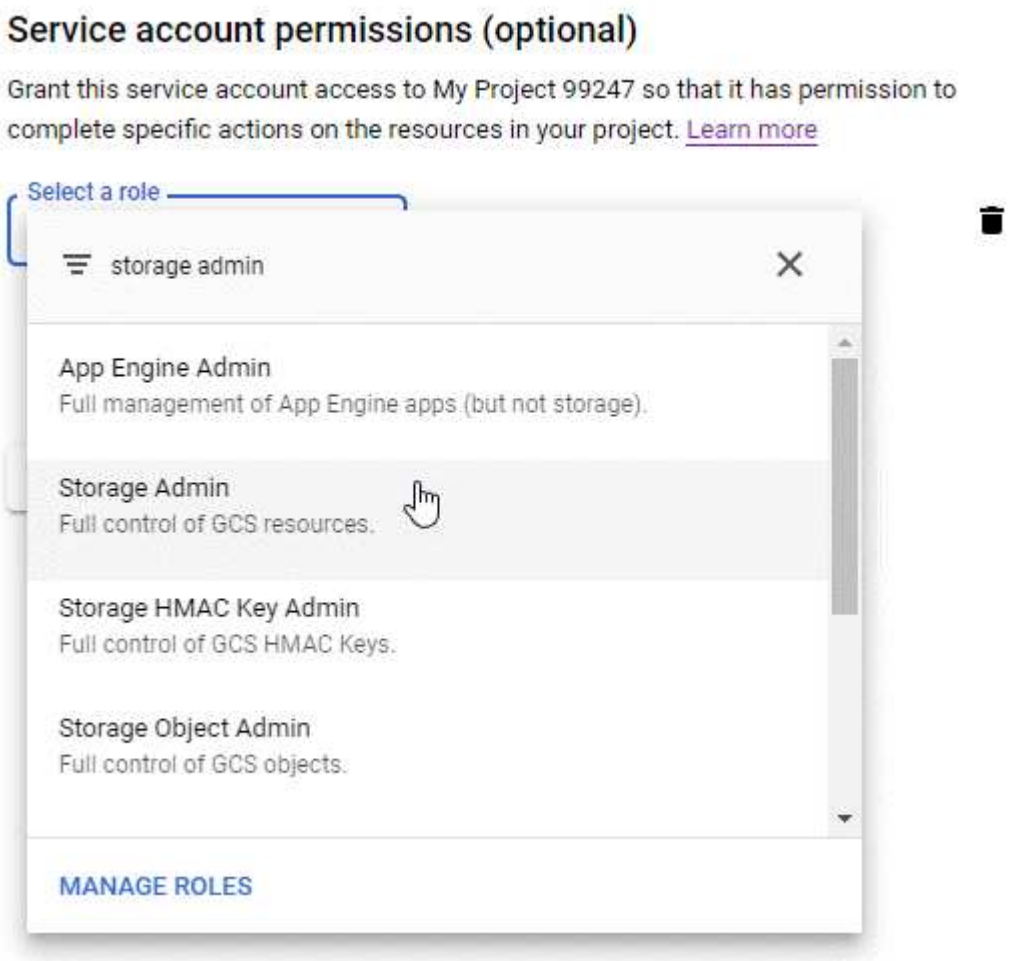
Si vous souhaitez utiliser le Tiering des données avec Cloud Volumes ONTAP 9.7, suivez les étapes 4 à "Mise en route de Cloud Volumes ONTAP dans Google Cloud Platform".

Configurer un compte de service et des clés d'accès pour Google Cloud Storage

Un compte de service permet à Cloud Manager d'authentifier et d'accéder aux compartiments Cloud Storage utilisés pour le Tiering des données. Les clés sont requises pour que Google Cloud Storage sache qui effectue la demande.

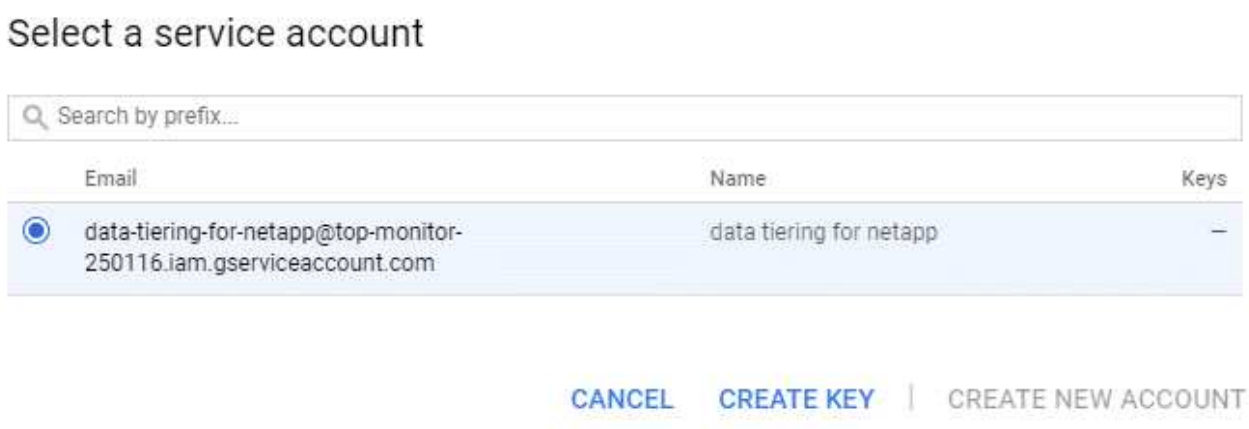
Étapes

1. Ouvrez la console IAM GCP et "Créez un compte de service avec le rôle d'administrateur du stockage".



2. Accédez à "Paramètres de stockage GCP".
3. Si vous y êtes invité, sélectionnez un projet.

4. Cliquez sur l'onglet **Interoperability**.
5. Si ce n'est déjà fait, cliquez sur **Activer l'accès à l'interopérabilité**.
6. Sous **clés d'accès pour les comptes de service**, cliquez sur **Créer une clé pour un compte de service**.
7. Sélectionnez le compte de service que vous avez créé à l'étape 1.



8. Cliquez sur **Créer clé**.
9. Copiez la clé d'accès et le secret.

   Lorsque vous ajoutez le compte GCP pour le Tiering des données, vous devez entrer ces informations dans Cloud Manager.

Ajout d'un compte GCP à Cloud Manager

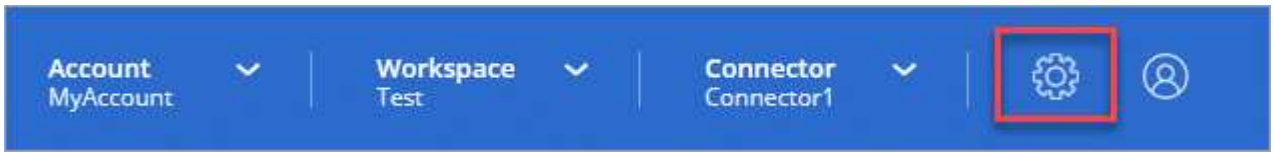
Vous pouvez désormais ajouter cette clé à Cloud Manager.

Ce dont vous avez besoin

Vous devez créer un connecteur pour modifier les paramètres de Cloud Manager. "Découvrez comment".

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.



2. Cliquez sur **Ajouter des informations d'identification** et sélectionnez **Google Cloud**.
3. Saisissez la clé d'accès et le secret du compte de service.

   Les clés permettent à Cloud Manager de configurer un compartiment Cloud Storage pour le Tiering des données.

4. Vérifiez que les exigences de la stratégie ont été respectées, puis cliquez sur **Créer un compte**.

Et la suite ?

Vous pouvez désormais activer le Tiering des données sur les volumes individuels d'un système Cloud Volumes ONTAP 9.6 lorsque vous les créez, les modifiez ou les répliquez. Pour plus de détails, voir "Tiering des données inactives vers un stockage objet à faible coût".

Mais avant cela, assurez-vous que le sous-réseau dans lequel réside Cloud Volumes ONTAP est configuré pour un accès privé à Google. Pour obtenir des instructions, reportez-vous à la section "Documentation Google Cloud : configuration de Private Google Access".

Ajout de comptes du site de support NetApp à Cloud Manager

Vous devez ajouter votre compte sur le site de support NetApp à Cloud Manager pour déployer un système BYOL. Il est également nécessaire d'enregistrer des systèmes avec paiement à l'utilisation et de mettre à niveau le logiciel ONTAP.

Découvrez dans cette vidéo comment ajouter des comptes sur le site de support NetApp à Cloud Manager. Ou faites défiler vers le bas pour lire les étapes.

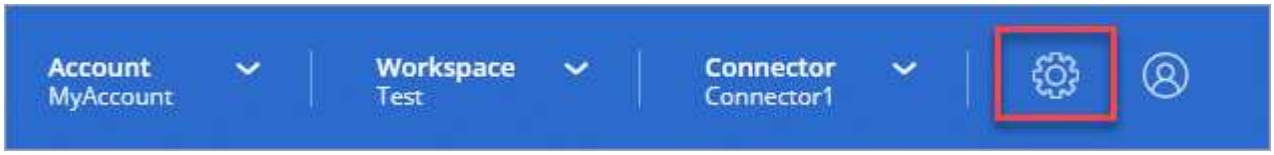
[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

Ce dont vous avez besoin

Vous devez créer un connecteur pour modifier les paramètres de Cloud Manager. "Découvrez comment".

Étapes

1. Si vous ne disposez pas encore d'un compte sur le site de support NetApp, "inscrivez-vous pour en créer un".
2. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **informations d'identification**.



3. Cliquez sur **Add Credentials** et sélectionnez **NetApp support site**.
4. Spécifiez un nom pour le compte, puis entrez le nom d'utilisateur et le mot de passe.
   - Le compte doit être un compte de niveau client (et non un compte invité ou temporaire).
   - Si vous prévoyez de déployer des systèmes BYOL :
     - Le compte doit être autorisé à accéder aux numéros de série des systèmes BYOL.
     - Si vous avez acheté un abonnement BYOL sécurisé, un compte NSS sécurisé est requis.
5. Cliquez sur **Créer un compte.**

Et la suite ?

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

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

- "Découvrez comment Cloud Manager gère les fichiers de licences"

Gestion des utilisateurs, des espaces de travail, des connecteurs et des abonnements

"Après avoir effectué la configuration initiale"Vous devrez peut-être gérer ultérieurement les paramètres de votre compte en gérant les utilisateurs, les espaces de travail, les connecteurs et les abonnements.

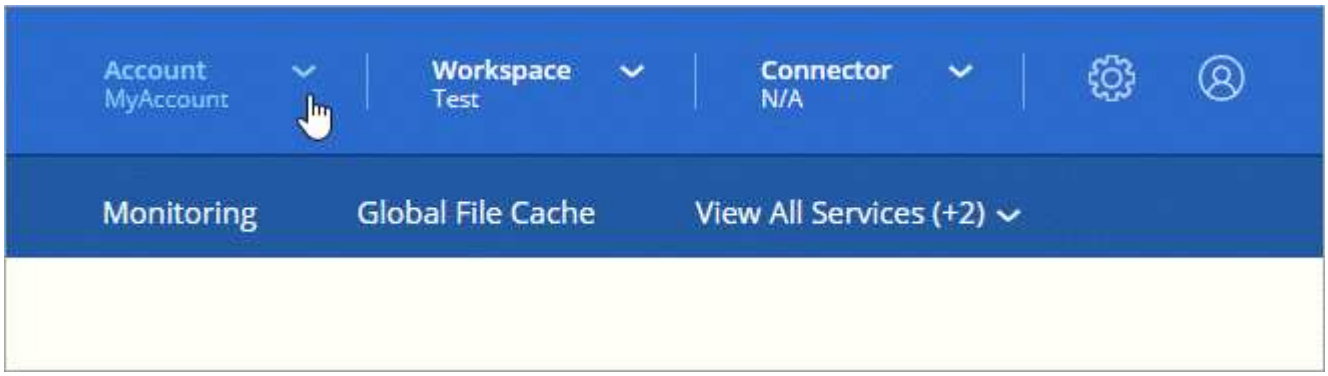
"Découvrez comment fonctionnent les comptes Cloud Central".

Ajout d'utilisateurs

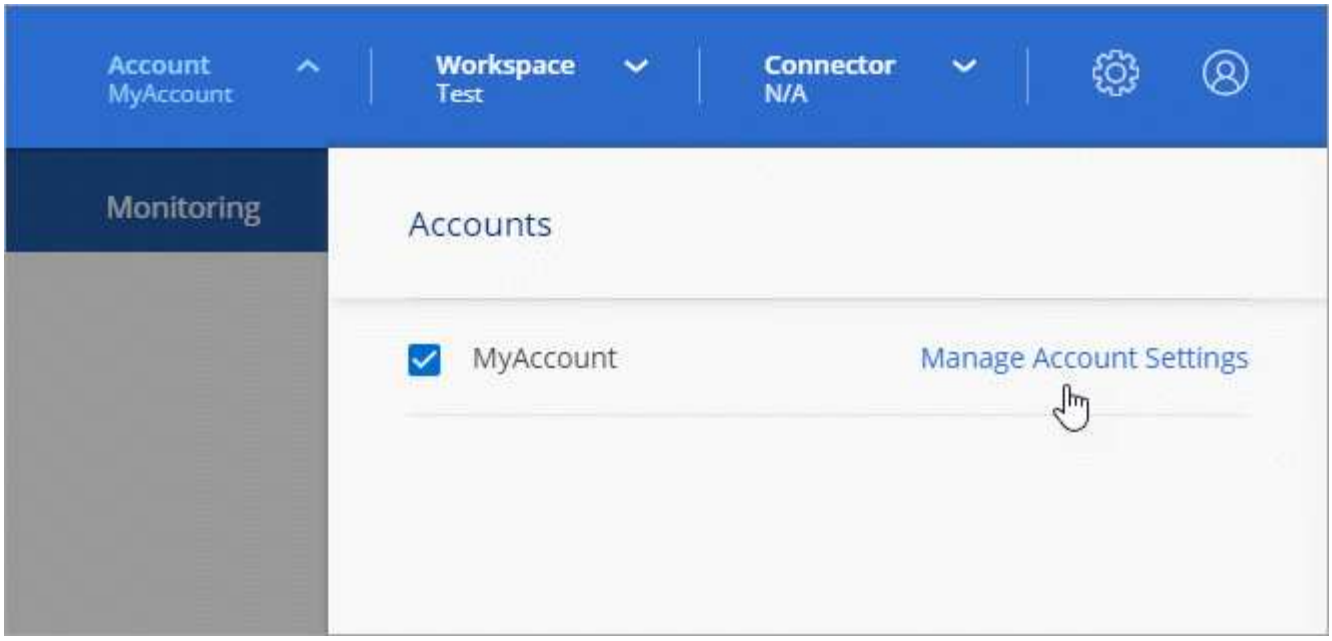
Associez les utilisateurs de Cloud Central au compte Cloud Central pour qu'ils puissent créer et gérer des environnements de travail dans Cloud Manager.

Étapes

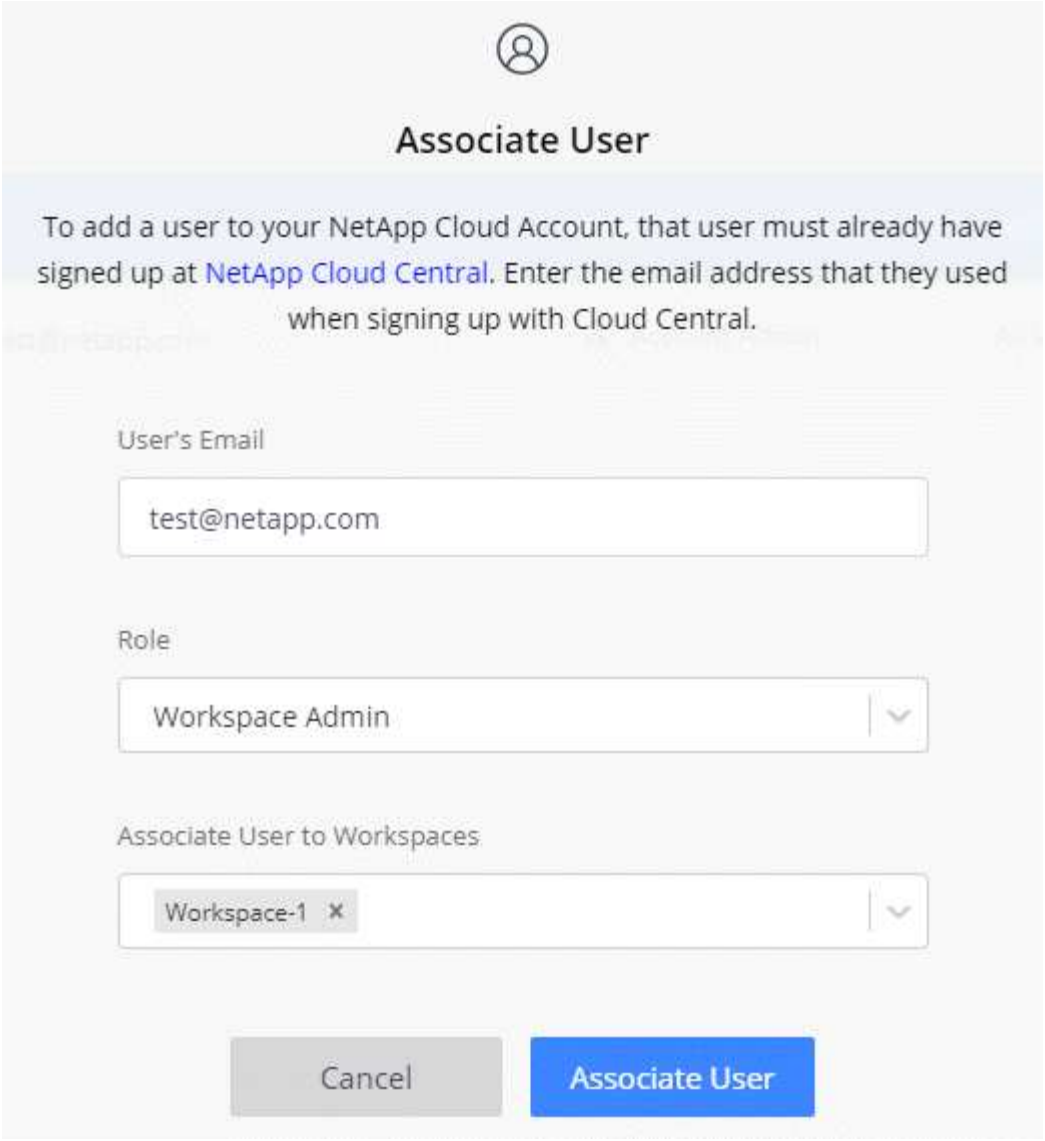
1. Si l'utilisateur ne l'a pas déjà fait, demandez-lui d'aller à "NetApp Cloud Central" et s'inscrire.
2. Dans la partie supérieure de Cloud Manager, cliquez sur la liste déroulante **Account**.



3. Cliquez sur **gérer le compte** en regard du compte actuellement sélectionné.



4. Dans l'onglet utilisateurs, cliquez sur **associer utilisateur**.
5. Entrez l'adresse e-mail de l'utilisateur et sélectionnez un rôle pour l'utilisateur :
   - **Administrateur de compte** : peut effectuer n'importe quelle action dans Cloud Manager.
   - **Workspace Admin** : permet de créer et de gérer des ressources dans des espaces de travail attribués.
   - **Compliance Viewer** : peut uniquement afficher les informations de conformité et générer des rapports pour les espaces de travail auxquels ils ont la permission d'accéder.
6. Si vous avez sélectionné Workspace Admin ou Compliance Viewer, sélectionnez un ou plusieurs espaces de travail à associer à cet utilisateur.



7. Cliquez sur **associer utilisateur**.

Résultat

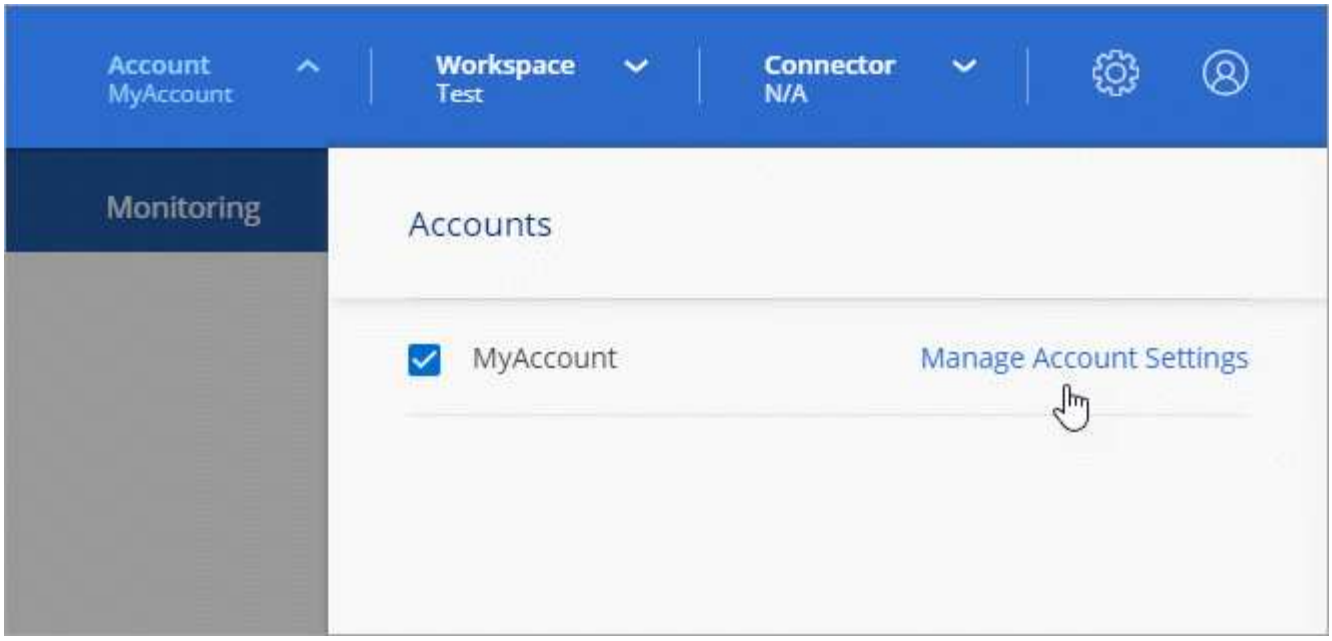
L'utilisateur doit recevoir un e-mail de la part de NetApp Cloud Central intitulé « Account Association ». Il contient les informations nécessaires pour accéder à Cloud Manager.

Suppression d'utilisateurs

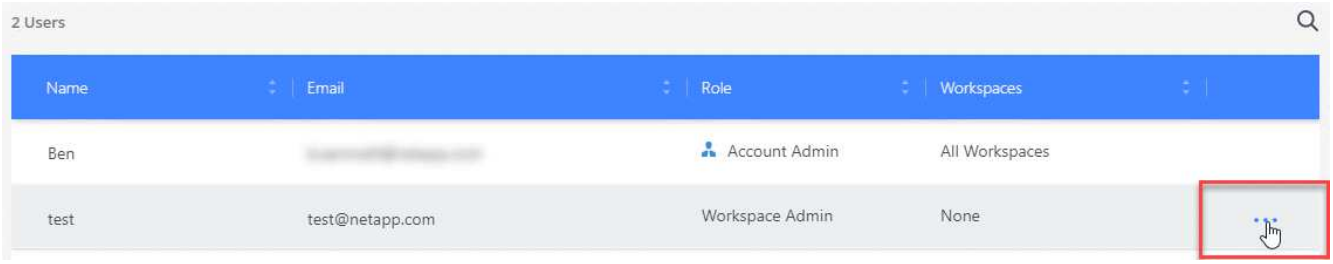
La dissociation permet d'interdire l'accès aux ressources d'un compte Cloud Central.

Étapes

1. En haut de Cloud Manager, cliquez sur la liste déroulante **compte** et cliquez sur **gérer compte**.



2. Dans l'onglet utilisateurs, cliquez sur le menu d'action de la ligne correspondant à l'utilisateur.



3. Cliquez sur **Disassocier utilisateur** et cliquez sur **Disassocier** pour confirmer.

Résultat

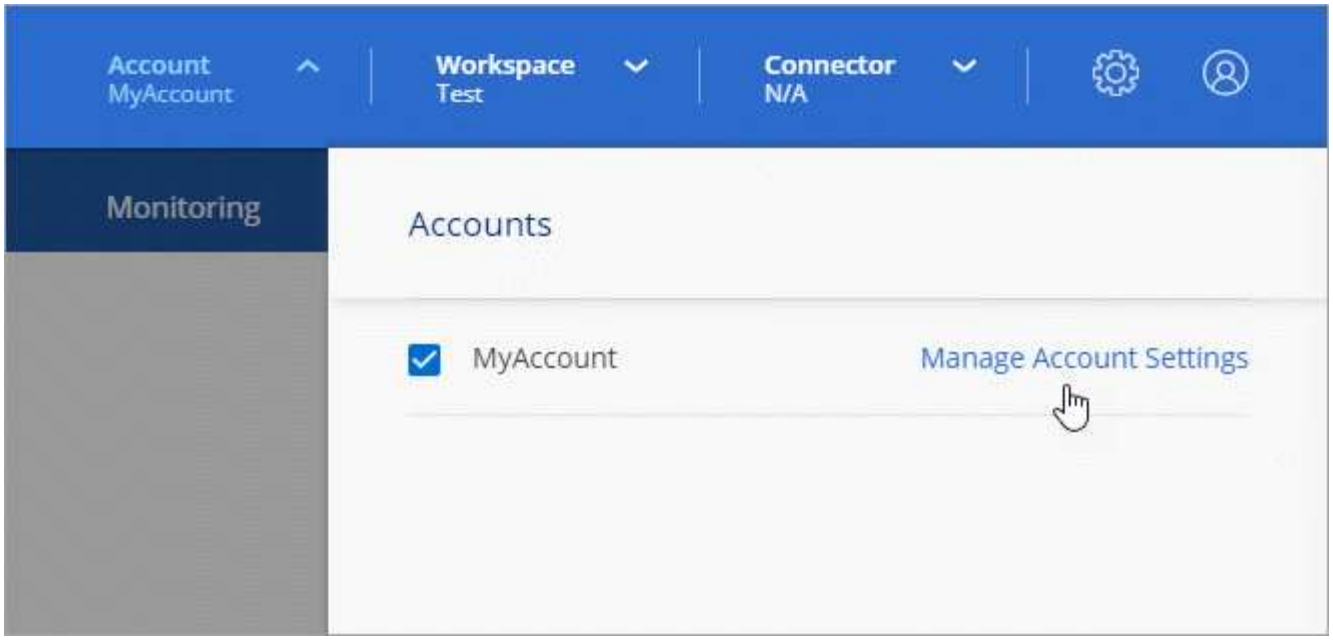
L'utilisateur ne peut plus accéder aux ressources de ce compte Cloud Central.

Gestion des espaces de travail d'un administrateur d'espace de travail

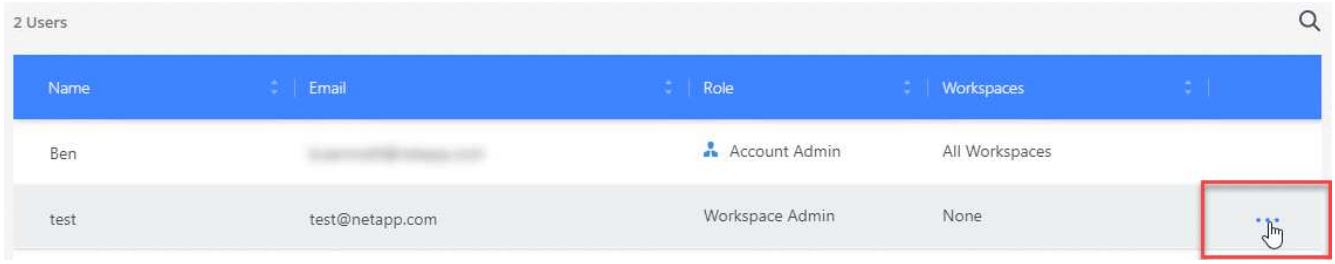
Vous pouvez associer et dissocier les administrateurs d'espace de travail avec des espaces de travail à tout moment. L'association de l'utilisateur lui permet de créer et d'afficher les environnements de travail dans cet espace de travail.

Étapes

1. En haut de Cloud Manager, cliquez sur la liste déroulante **compte** et cliquez sur **gérer compte**.



2. Dans l'onglet utilisateurs, cliquez sur le menu d'action de la ligne correspondant à l'utilisateur.



3. Cliquez sur **gérer les espaces de travail**.
4. Sélectionnez les espaces de travail à associer à l'utilisateur et cliquez sur **appliquer**.

Résultat

L'utilisateur peut désormais accéder à ces espaces de travail à partir de Cloud Manager, tant que le connecteur était également associé aux espaces de travail.

Gestion des espaces de travail

Gérez vos espaces de travail en les créant, en les renommant et en les supprimant. Notez que vous ne pouvez pas supprimer un espace de travail s'il contient des ressources. Elle doit être vide.

Étapes

1. En haut de Cloud Manager, cliquez sur la liste déroulante **compte** et cliquez sur **gérer compte**.
2. Cliquez sur **espaces de travail**.
3. Choisissez l'une des options suivantes :
   - Cliquez sur **Ajouter un nouvel espace de travail** pour créer un nouvel espace de travail.
   - Cliquez sur **Renommer** pour renommer l'espace de travail.
   - Cliquez sur **Supprimer** pour supprimer l'espace de travail.

Gestion des espaces de travail d'un connecteur

Vous devez associer le connecteur aux espaces de travail pour que les administrateurs d'espace de travail puissent accéder à ces espaces de travail à partir de Cloud Manager.

Si vous ne disposez que d'administrateurs de compte, il n'est pas nécessaire d'associer le connecteur aux espaces de travail. Ils peuvent accéder par défaut à tous les espaces de travail dans Cloud Manager.

"En savoir plus sur les utilisateurs, les espaces de travail et les connecteurs".

Étapes

1. En haut de Cloud Manager, cliquez sur la liste déroulante **compte** et cliquez sur **gérer compte**.
2. Cliquez sur **connecteur**.
3. Cliquez sur **gérer les espaces de travail** pour le connecteur que vous souhaitez associer.
4. Sélectionnez les espaces de travail à associer au connecteur et cliquez sur **appliquer**.

Gestion des abonnements

Après vous être abonné au Marketplace d'un fournisseur cloud, chaque abonnement est disponible dans le widget Account Settings. Vous avez la possibilité de renommer un abonnement et de dissocier l'abonnement d'un ou plusieurs comptes.

Par exemple, disons que vous avez deux comptes et que chacun est facturé par le biais d'abonnements distincts. Vous pouvez dissocier un abonnement de l'un des comptes afin que les utilisateurs de ce compte ne choisissent pas accidentellement l'abonnement incorrect lors de la création d'un environnement de travail Cloud Volume ONTAP.

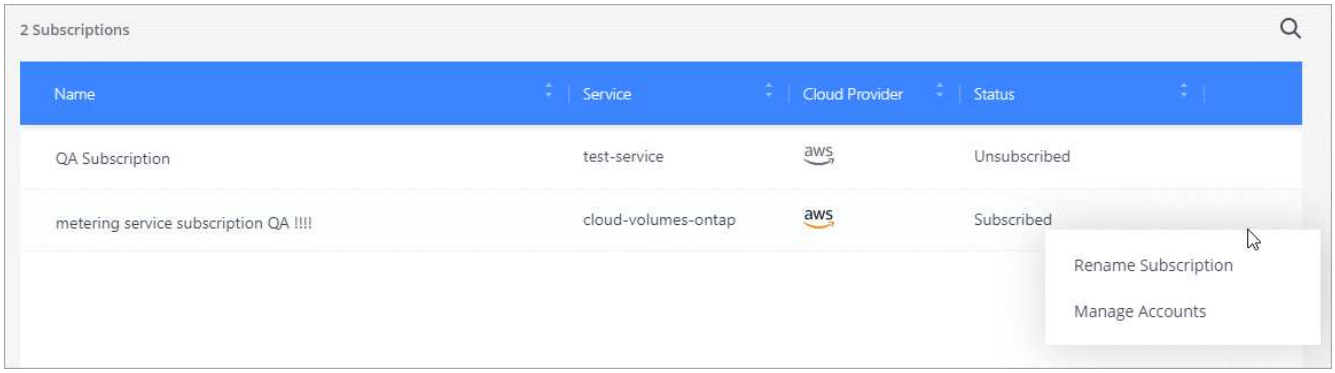
"En savoir plus sur les abonnements".

Étapes

1. En haut de Cloud Manager, cliquez sur la liste déroulante **compte** et cliquez sur **gérer compte**.
2. Cliquez sur **abonnements**.

   Vous ne verrez que les abonnements associés au compte que vous consultez actuellement.

3. Cliquez sur le menu d'action de la ligne correspondant à l'abonnement que vous souhaitez gérer.



4. Choisissez de renommer l'abonnement ou de gérer les comptes associés à l'abonnement.

Modification du nom du compte

Changez le nom de votre compte à tout moment pour le changer en quelque chose de significatif pour vous.

Étapes

1. En haut de Cloud Manager, cliquez sur la liste déroulante **compte** et cliquez sur **gérer compte**.
2. Dans l'onglet **vue d'ensemble**, cliquez sur l'icône de modification en regard du nom du compte.
3. Saisissez un nouveau nom de compte et cliquez sur **Enregistrer**.

Activation ou désactivation de la plateforme SaaS

Nous ne recommandons pas de désactiver la plate-forme SaaS sauf si vous devez vous conformer aux politiques de sécurité de votre entreprise. En désactivant la plateforme SaaS, vous vous limitent votre capacité à utiliser les services cloud intégrés de NetApp.

Si vous désactivez la plateforme SaaS, les services suivants ne sont pas disponibles depuis Cloud Manager :

- Conformité cloud
- Kubernetes
- Tiering dans le cloud
- Cache global de fichiers
- Surveillance (Cloud Insights)

Étapes

1. En haut de Cloud Manager, cliquez sur la liste déroulante **compte** et cliquez sur **gérer compte**.
2. Dans l'onglet **Présentation**, activez l'option utiliser la plateforme SaaS.

Gestion d'un certificat HTTPS pour l'accès sécurisé

Par défaut, Cloud Manager utilise un certificat auto-signé pour l'accès HTTPS à la console Web. Vous pouvez installer un certificat signé par une autorité de certification (CA), qui offre une meilleure protection de la sécurité qu'un certificat auto-signé.

Avant de commencer

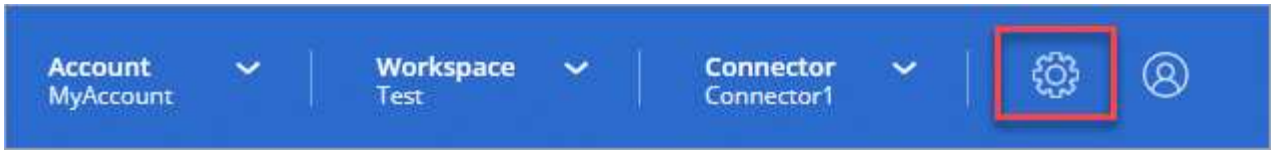
Vous devez créer un connecteur pour modifier les paramètres de Cloud Manager. "Découvrez comment".

Installation d'un certificat HTTPS

Installez un certificat signé par une autorité de certification pour un accès sécurisé.

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **HTTPS Setup**.

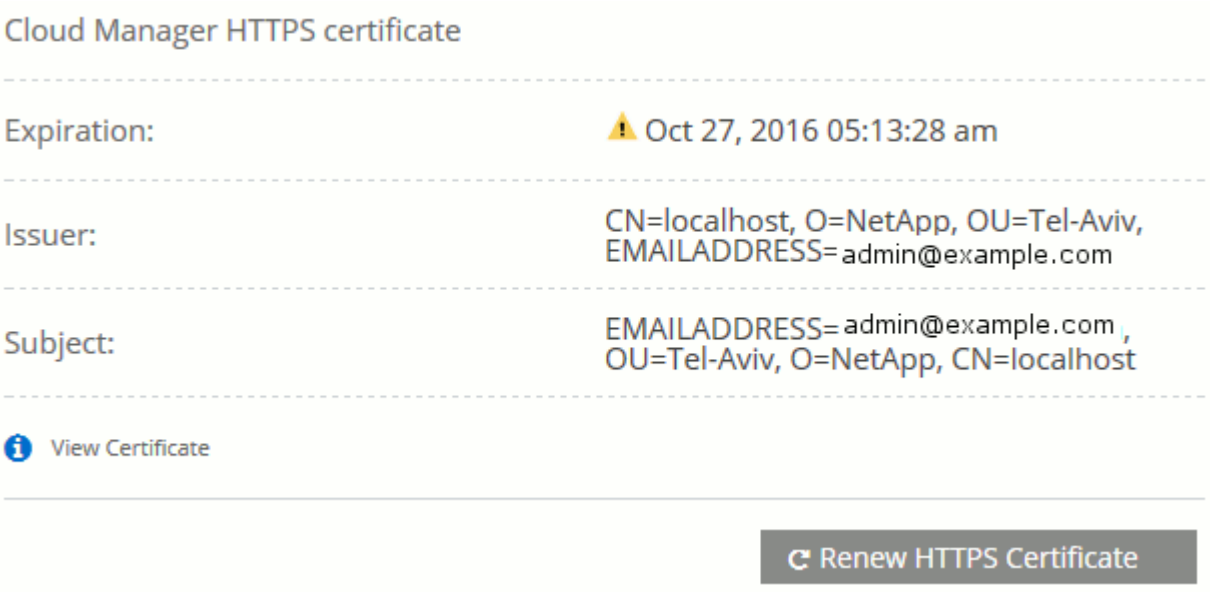


2. Dans la page Configuration HTTPS, installez un certificat en générant une requête de signature de certificat (CSR) ou en installant votre propre certificat signé par l'autorité de certification :

Option	Description
Générez une RSC	a. Entrez le nom d'hôte ou le DNS de l'hôte du connecteur (son nom commun), puis cliquez sur **generate CSR**. Cloud Manager affiche une demande de signature de certificat. b. Utilisez la RSC pour envoyer une demande de certificat SSL à une autorité de certification. Le certificat doit utiliser le format X.509 encodé au format PEM (Privacy Enhanced Mail) Base-64. c. Copiez le contenu du certificat signé, collez-le dans le champ certificat, puis cliquez sur **installer**.
Installez votre propre certificat signé par l'autorité de certification	a. Sélectionnez **installer le certificat signé CA**. b. Chargez le fichier de certificat et la clé privée, puis cliquez sur **installer**. Le certificat doit utiliser le format X.509 encodé au format PEM (Privacy Enhanced Mail) Base-64.

Résultat

Cloud Manager utilise désormais le certificat signé par l'autorité de certification pour fournir un accès HTTPS sécurisé. L'image suivante montre un système Cloud Manager configuré pour un accès sécurisé :



Renouvellement du certificat HTTPS de Cloud Manager

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

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **HTTPS Setup**.

   Des informations détaillées sur le certificat Cloud Manager s'affichent, y compris la date d'expiration.

2. Cliquez sur **renouveler le certificat HTTPS** et suivez les étapes pour générer une RSC ou installer votre propre certificat signé par une CA.

Résultat

Cloud Manager utilise le nouveau certificat signé par l'autorité de certification pour fournir un accès HTTPS sécurisé.

Suppression des environnements de travail Cloud Volumes ONTAP

L'administrateur des comptes peut supprimer un environnement de travail Cloud Volumes ONTAP pour le déplacer vers un autre système ou pour résoudre les problèmes de détection.

Description de la tâche

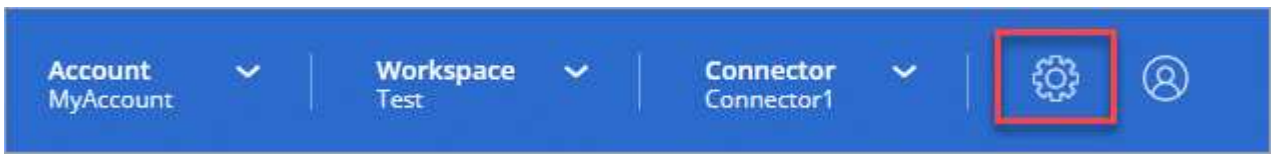
La suppression d'un environnement de travail Cloud Volumes ONTAP le supprime de Cloud Manager. Il ne supprime pas le système Cloud Volumes ONTAP. Vous pourrez par la suite redécouvrir l'environnement de travail.

La suppression d'un environnement de travail de Cloud Manager vous permet d'effectuer les opérations suivantes :

- Redécouvrez-le dans un autre espace de travail
- Redécouvrez-le à partir d'un autre système Cloud Manager
- Redécouvrez-le si vous avez rencontré des problèmes lors de la découverte initiale

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres, puis sélectionnez **Outils**.



2. Dans la page Outils, cliquez sur **lancer**.
3. Sélectionnez l'environnement de travail Cloud Volumes ONTAP que vous souhaitez supprimer.
4. Sur la page Revue et approbation, cliquez sur **Go**.

Résultat

Cloud Manager supprime l'environnement de travail. Les utilisateurs peuvent à tout moment redécouvrir cet environnement de travail à partir de la page des environnements de travail.

Configuration d'un connecteur pour utiliser un serveur proxy

Si vos stratégies d'entreprise exigent que vous utilisiez un serveur proxy pour toutes les communications HTTP vers Internet, vous devez configurer vos connecteurs pour utiliser ce serveur proxy. Le serveur proxy peut se trouver dans le cloud ou dans votre réseau.

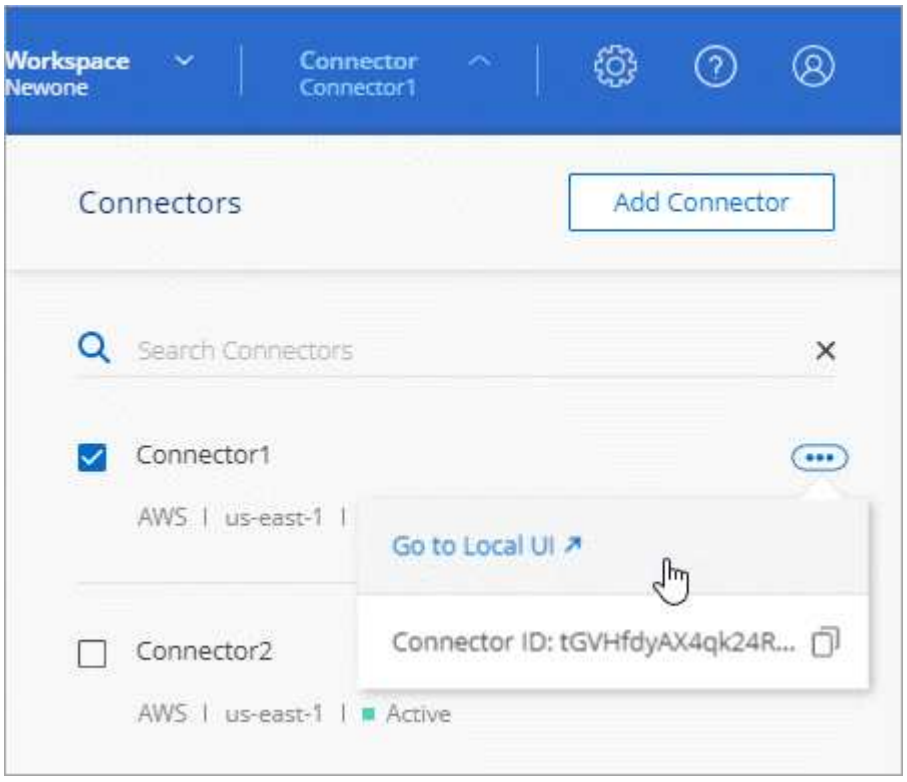
Lorsque vous configurez un connecteur pour utiliser un serveur proxy, ce connecteur et les systèmes Cloud Volumes ONTAP qu'il gère (y compris les médiateurs HA) utilisent tous le serveur proxy.

Étapes

1. "Connectez-vous à l'interface SaaS Cloud Manager" À partir d'une machine dotée d'une connexion réseau à l'instance de connecteur.

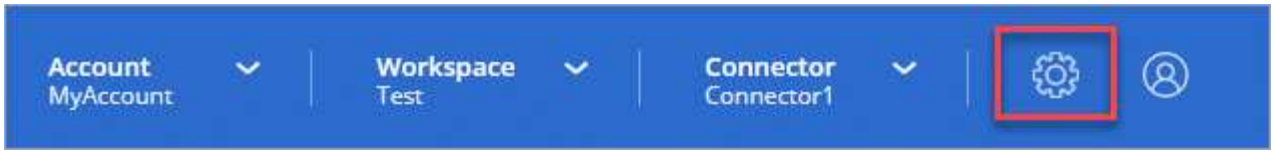
   Si le connecteur n'est pas doté d'une adresse IP publique, vous aurez besoin d'une connexion VPN ou vous devrez vous connecter à partir d'un hôte de secours situé sur le même réseau que le connecteur.

2. Cliquez sur la liste déroulante **Connector**, puis cliquez sur **allez à l'interface utilisateur locale** pour un connecteur spécifique.



   L'interface Cloud Manager exécutée sur le connecteur est chargée dans un nouvel onglet du navigateur.

3. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **Cloud Manager Settings**.



4. Sous Proxy HTTP, entrez le serveur à l’aide de la syntaxe http://address:port, Indiquez un nom d’utilisateur et un mot de passe si une authentification de base est requise pour le serveur, puis cliquez sur Enregistrer.

Cloud Manager ne prend pas en charge les mots de passe comprenant le caractère @.

Résultat

Après avoir spécifié le serveur proxy, les nouveaux systèmes Cloud Volumes ONTAP sont automatiquement configurés pour utiliser le serveur proxy lors de l'envoi de messages AutoSupport. Si vous n'avez pas spécifié le serveur proxy avant que les utilisateurs créent des systèmes Cloud Volumes ONTAP, ils doivent utiliser le Gestionnaire système pour définir manuellement le serveur proxy dans les options AutoSupport de chaque système.

Remplacement des verrouillages CIFS pour Cloud Volumes ONTAP HA dans Azure

L'administrateur du compte peut activer un paramètre dans Cloud Manager qui empêche les problèmes liés au basculement du stockage Cloud Volumes ONTAP lors des événements de maintenance Azure. Lorsque vous activez ce paramètre, Cloud Volumes ONTAP vetoes les verrous CIFS et réinitialise les sessions CIFS actives.

Description de la tâche

Microsoft Azure planifie des événements de maintenance périodiques sur ses machines virtuelles. Lorsqu'un événement de maintenance se produit sur un nœud d'une paire haute disponibilité Cloud Volumes ONTAP, la paire haute disponibilité démarre le basculement du stockage. S'il existe des sessions CIFS actives au cours de cet événement de maintenance, les verrous sur les fichiers CIFS peuvent empêcher le basculement du stockage.

Si vous activez ce paramètre, Cloud Volumes ONTAP veto aux verrous et réinitialise les sessions CIFS actives. Par conséquent, la paire haute disponibilité peut effectuer le basculement du stockage lors de ces opérations de maintenance.

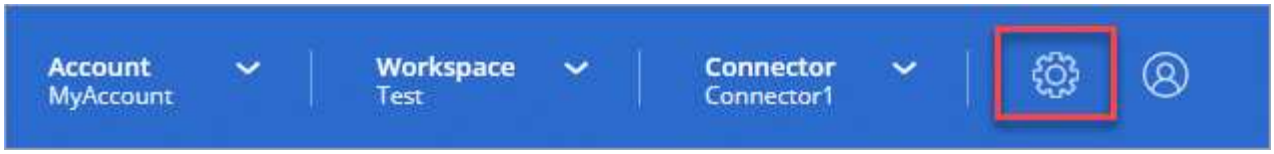
Ce processus peut entraîner des perturbations pour les clients CIFS. Les données qui ne sont pas validées auprès des clients CIFS pourraient être perdues.

Ce dont vous avez besoin

Vous devez créer un connecteur pour modifier les paramètres de Cloud Manager. "Découvrez comment".

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **Cloud Manager Settings**.



2. Sous **HA CIFS Locks**, cochez la case et cliquez sur **Save**.

Référence

Rôles

Les rôles Administrateur de compte, Administrateur d'espace de travail et Visionneuse de conformité cloud fournissent des autorisations spécifiques aux utilisateurs.

Tâche	Administrateur du compte	Administrateur de l'espace de travail	Visualiseur Cloud Compliance
Gérer les environnements de travail	Oui.	Oui.	Non
Activer les services dans les environnements de travail	Oui.	Oui.	Non
Afficher l'état de la réplication des données	Oui.	Oui.	Non
Afficher la chronologie	Oui.	Oui.	Non
Basculer entre les espaces de travail	Oui.	Oui.	Oui.
Afficher les résultats de l'analyse de conformité	Oui.	Oui.	Oui.
Supprimer les environnements de travail	Oui.	Non	Non
Connectez les clusters Kubernetes aux environnements de travail	Oui.	Non	Non
Recevoir le rapport Cloud Volumes ONTAP	Oui.	Non	Non
Créer des connecteurs	Oui.	Non	Non
Gérez les comptes Cloud Central	Oui.	Non	Non
Gérer les identifiants	Oui.	Non	Non
Modifiez les paramètres de Cloud Manager	Oui.	Non	Non
Afficher et gérer le tableau de bord du support	Oui.	Non	Non
Supprimez les environnements de travail de Cloud Manager	Oui.	Non	Non

Tâche	Administrateur du compte	Administrateur de l'espace de travail	Visualiseur Cloud Compliance
Installez un certificat HTTPS	Oui.	Non	Non

Liens connexes

- "Configuration d'espaces de travail et d'utilisateurs sur le compte Cloud Central"
- "Gestion des espaces de travail et des utilisateurs sur le compte Cloud Central"

Comment Cloud Manager utilise les autorisations du fournisseur cloud

Cloud Manager nécessite des autorisations pour effectuer des actions dans votre fournisseur cloud. Ces autorisations sont incluses dans "Règles fournies par NetApp". Vous pouvez comprendre ce que fait Cloud Manager avec ces autorisations.

Ce que fait Cloud Manager avec les autorisations AWS

Cloud Manager utilise un compte AWS pour effectuer des appels API vers plusieurs services AWS, notamment EC2, S3, CloudFormation, IAM, Security Token Service (STS) et le service de gestion des clés (KMS).

Actions	Objectif
"ec2:StartInstances", "ec2:StopInstances", "ec2:Décrivez les occurrences", "ec2:Ddescriptif InstanceStatus", "ec2:RunInstances", « ec2:TerminateInstances », « ec2:ModimodificationAttribute »,	Lance une instance Cloud Volumes ONTAP et arrête, démarre et surveille l'instance.
"EC2:DescribeInstanceAttribute",	Vérifie que la mise en réseau améliorée est activée pour les types d'instance pris en charge.
"ec2:descriptifs", "ec2:descriptifs",	Lance une configuration Cloud Volumes ONTAP HA.
"EC2:CreateTags",	Marque chaque ressource créée par Cloud Manager à l'aide des balises WorkingEnvironment et WorkingEnvironmentId. Cloud Manager utilise ces balises pour la maintenance et l'allocation des coûts.
« ec2:CreateVolume », « ec2:Describevolumes », « ec2:ModityVolumeAttribute », « ec2:AttachVolume », « ec2:DeleteVolume », « ec2:DetachVolume »,	Gère les volumes EBS utilisés par Cloud Volumes ONTAP en tant que stockage back-end.
« ec2:CreateSecurityGroup », « ec2:DeleteSecurityGroup », « ec2:descriptif SecurityGroups », « ec2:RevokeSecurityGroupEgress », « ec2:AuthoreSecurityGroupEgress », « ec2:AuthoreSecurityGroupEgress », « ec2:AuthoreSecurityGroupIngress », « ec2:RevokeSecurityGroupIngress »,	Crée des groupes de sécurité prédéfinis pour Cloud Volumes ONTAP.
« ec2:CreateNetworkinterface », « ec2:DescribeNetworkinterfaces », « ec2:DeleteNetworkinterface », « ec2:ModityNetworkInterfaceAttribute »,	Crée et gère des interfaces réseau pour Cloud Volumes ONTAP dans le sous-réseau cible.

Actions	Objectif
"ec2:DescribeSubnets", "ec2:DescribeVpcs",	Récupère la liste des sous-réseaux de destination et des groupes de sécurité nécessaires à la création d'un nouvel environnement de travail pour Cloud Volumes ONTAP.
"EC2:DescribeDhcpOptions",	Détermine les serveurs DNS et le nom de domaine par défaut lors du lancement des instances Cloud Volumes ONTAP.
« ec2:CreateSnapshot », « ec2:DeleteSnapshot », « ec2:Ddescriptif »,	Prend des snapshots des volumes EBS lors de la configuration initiale et chaque fois qu'une instance Cloud Volumes ONTAP est arrêtée.
" EC2:GetConsoleOutput ",	Capture la console Cloud Volumes ONTAP, associée aux messages AutoSupport.
"EC2:DécribeKeyPair",	Obtient la liste des paires de clés disponibles lors du lancement d'instances.
"EC2:DécribeRegions",	Récupère une liste des régions AWS disponibles.
« ec2:DeleteTags », « ec2:Ddescriptif »,	Gère les balises des ressources associées aux instances Cloud Volumes ONTAP.
"Cloudformation:CreateStack", "cloudformation:DeleteStack", "cloudformation:DescribeSacks", "cloudformation:DescribeStackEvents", "cloudformation:ValidateTemplate",	Lance les instances Cloud Volumes ONTAP.
« iam:PassRole », « iam:CreateRole », « iam:DeleteRole », « iam:PutRolePolicy », « iam:CreateInstanceProfile », "iam:DeleteRolePolicy", "iam:AddRoleToInstanceProfile", "iam:RemoveRoleFromInstanceProfile", "iam:DeleteInstanceProfile",	Lance une configuration Cloud Volumes ONTAP HA.
« iam:ListenInstanceProfiles », « sts:DecodeAuthorationmessage », « ec2:AssociationIamInstanceProfile », « ec2:DécrideIamInstanceInstanceProfileassociations », « ec2:DisassociateIamInstanceProfile »,	Gère les profils d'instance des instances Cloud Volumes ONTAP.
« s3:GetBuckeTagging », « s3:GetBuckeLocation », « s3:ListAllMyPets », « s3:ListBucket »	Obtenez des informations sur les compartiments AWS S3 pour que Cloud Manager puisse s'intégrer au service NetApp Data Fabric Cloud Sync.
« s3:CreateBucket », « s3:DeleteBucket », « s3:GetLifecyclConfiguration », « s3:PutLifecycleConfiguration », « s3:PutBuckeTagging », « s3:ListBuckeVersions », « s3:GetBuckePolicyStatus », « s3:GetBuckePublicAccessBlock », « s3:GetBuckeAcl », « s3:GetBuckePolicy », « s3:GetBuckePolicy », "s3:PutBuckePublicAccessBlock"	Gère le compartiment S3 utilisé par un système Cloud Volumes ONTAP comme Tier de capacité pour le Tiering des données.

Actions	Objectif
"Km:liste*", "km:reEncrypt*", "km:décrire*", "km:CreateGrant",	Chiffrement des données d'Cloud Volumes ONTAP à l'aide du service AWS Key Management Service (KMS).
"ce:GetReservationUtilization", "ce:GetDimensionValues", "ce:GetCostAndUsage", "ce:GetTags"	Obtient les données de coût AWS pour Cloud Volumes ONTAP.
« ec2:CreatePlaceGroup », « ec2:Deleteplacer GroupeDe »	Lorsque vous déployez une configuration HA dans une seule zone de disponibilité AWS, Cloud Manager lance les deux nœuds HA et le médiateur dans un groupe de placement AWS.
« ec2:descriptifsd'InstanciquesOfferings »	Cloud Manager utilise l'autorisation dans le cadre du déploiement de Cloud Compliance pour choisir le type d'instance à utiliser.
« s3:DeleteBucket », « s3:GetLifecyclConfiguration », « s3:PutLifecycletConfiguration », « s3:PutBuckeTagging », « s3:ListBuckeVersions », « s3:GetObject », « s3:ListBucket », « s3:ListAllMyPets », « s3:GetBuckeTagging », « s3:GetBuckeLocation » « s3:GetBuckePolicyStatus », "s3:GetBuckePublicAccessBlock", "s3:GetBuckeAcl", "s3:GetBuckePolicy", "s3:PutBuckePublicAccessBlock"	Cloud Manager utilise ces autorisations lorsque vous activez le service Backup vers S3.

Ce que fait Cloud Manager avec les autorisations Azure

La stratégie Cloud Manager Azure inclut les autorisations dont Cloud Manager a besoin pour déployer et gérer Cloud Volumes ONTAP dans Azure.

Actions	Objectif
« Microsoft.Compute/locations/operations/read", « Microsoft.Compute/locations/vmSizes/read", « Microsoft.Compute/operations/read", « Microsoft.Compute/virtualMachines/instanceView/read", « Microsoft.Compute/virtualMachines/powerOff/action", « Microsoft.Compute/virtualMachines/read", « Microsoft.Compute/virtualMachines/restart/action", « Microsoft.Compute/virtualMachines/start/action", « Microsoft.Compute/virtualMachines/deallocate/action", « Microsoft.Compute/virtualMachines/vmSizes/read", « Microsoft.Compute/virtualMachines/write",	Crée Cloud Volumes ONTAP et arrête, démarre, supprime et obtient l'état du système.
« Microsoft.Compute/images/write", « Microsoft.Compute/images/read",	Permet le déploiement de Cloud Volumes ONTAP à partir d'un disque VHD.

Actions	Objectif
« Microsoft.Compute/disks/delete", « Microsoft.Compute/disks/read", « Microsoft.Compute/disks/write", Microsoft.Storage/checkkamedisponibilité/read », « Microsoft.Storage/Operations/read », « Microsoft.Storage/storageAccounts/listkeys/action », « Microsoft.Storage/storageAccounts/read », « Microsoft.Storage/storageAccounts/redynamekey/action », « Microsoft.Storage/storageAccounts/write » « Microsoft.Storage/StorageAccounts/delete », « Microsoft.Storage/eancs/read »,	Gère les comptes et les disques de stockage Azure et les connecte à Cloud Volumes ONTAP.
« Microsoft.Network/networkInterfaces/read", « Microsoft.Network/networkInterfaces/write", « Microsoft.Network/networkInterfaces/join/action",	Crée et gère des interfaces réseau pour Cloud Volumes ONTAP dans le sous-réseau cible.
« Microsoft.Network/networkSecurityGroups/read", « Microsoft.Network/networkSecurityGroups/write", « Microsoft.Network/networkSecurityGroups/join/action",	Crée des groupes de sécurité réseau prédéfinis pour Cloud Volumes ONTAP.
« Microsoft.Resources/abonnements/emplacements/lecture », « Microsoft.Network/locations/operationResults/read", « Microsoft.Network/locations/operations/read", « Microsoft.Network/virtualNetworks/read", « Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read", » « Microsoft.Network/virtualNetworks/subnets/read", « Microsoft.Network/virtualNetworks/subnets/virtualMachines/read", « Microsoft.Network/virtualNetworks/virtualMachines/read", « Microsoft.Network/virtualNetworks/subnets/join/action",	Récupère les informations réseau sur les régions, le VNet cible et le sous-réseau, et ajoute Cloud Volumes ONTAP aux VNets.
« Microsoft.Network/virtualNetworks/subnets/write", « Microsoft.Network/routeTables/join/action",	Active les terminaux de service VNet pour le hiérarchisation des données.
« Microsoft.Resources/déploiements/opérations/lecture », « Microsoft.Resources/déploiements/lecture », « Microsoft.Resources/déploiements/écriture »,	Déploie Cloud Volumes ONTAP à partir d’un modèle.

Actions	Objectif
« Microsoft.Resources/déploiements/opérations/lecture », « Microsoft.Resources/déploiements/lecture », « Microsoft.Resources/déploiements/écriture », « Microsoft.Resources/Resources/read », « Microsoft.Resources/abonnements/résultats d'opération/lecture », « Microsoft.Resources/souscriptions/resourceGroups/delete », « Microsoft.Resources/souscriptions/resourceGroups/read », « Microsoft.Resources/souscriptions/resourcesgroupe/resources/read », « Microsoft.Resources/souscriptions/resourceGroups/write »,	Crée et gère des groupes de ressources pour Cloud Volumes ONTAP.
« Microsoft.Compute/snapshots/write", « Microsoft.Compute/snapshots/read", « Microsoft.Compute/disks/beginGetAccess/action"	Crée et gère les snapshots gérés par Azure.
« Microsoft.Compute/availabilitySets/write", « Microsoft.Compute/availabilitySets/read",	Crée et gère des ensembles de disponibilité pour Cloud Volumes ONTAP.
« Microsoft.MarketplaceOrdering/Offres/éditeurs/offres/plans/accords/lecture », « Microsoft.MarketplaceOrdering/Offres/Offres/plans/accords/write »	Permet des déploiements programmatiques depuis Azure Marketplace.
« Microsoft.Network/loadBalancers/read", « Microsoft.Network/loadBalancers/write", « Microsoft.Network/loadBalancers/delete", « Microsoft.Network/loadBalancers/backendAddressPools/read", « Microsoft.Network/loadBalancers/backendAddressPools/join/action", « Microsoft.Network/loadBalancers/frontendIPConfigurations/read", « Microsoft.Network/loadBalancers/loadBalancingRules/read", « Microsoft.Network/loadBalancers/probes/read", « Microsoft.Network/loadBalancers/probes/join/action",	Gère un équilibreur de charge Azure pour les paires HA.
" Microsoft.Authorization/locks/* "	Permet la gestion des verrous sur les disques Azure.
"Microsoft.Authorization/roleDefinitions/écrire", "Microsoft.Authorization/roleassignations/écrire", "Microsoft.Web/sites/*"	Gestion du basculement pour les paires haute disponibilité.

Actions	Objectif
« Microsoft.Network/privateEndpoints/write", « Microsoft.Storage/StorageAccounts/PrivateEndpointConnectionsApproval/action », « Microsoft.Storage/storageAccounts/EndprivatepointConnections/read », « Microsoft.Network/privateEndpoints/read", « Microsoft.Network/privateDnsZones/write", « Microsoft.Network/privateDnsZones/virtualNetworkLinks/write", « Microsoft.Network/virtualNetworks/join/action", « Microsoft.Network/privateDnsZones/A/write", « Microsoft.Network/privateDnsZones/read", « Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",	Permet la gestion des terminaux privés. Les terminaux privés sont utilisés lorsque la connectivité n'est pas fournie à l'extérieur du sous-réseau. Cloud Manager crée le compte de stockage pour la haute disponibilité avec une connectivité interne uniquement au sein du sous-réseau.
« Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",	Permet à Cloud Manager de supprimer des volumes pour Azure NetApp Files.
« Microsoft.Resources/déploiements/opérations Statelis/lectures »	Azure requiert cette autorisation pour certains déploiements de machines virtuelles (elle dépend du matériel physique sous-jacent utilisé lors du déploiement).
« Microsoft.Resources/déploiements/opérations Statelis/lire », « Microsoft.Insights/Metrics/Read », « Microsoft.Compute/virtualMachines/extensions/write", « Microsoft.Compute/virtualMachines/extensions/read", « Microsoft.Compute/virtualMachines/extensions/delete", « Microsoft.Compute/virtualMachines/delete", « Microsoft.Network/networkInterfaces/delete", « Microsoft.Network/networkSecurityGroups/delete", Microsoft.Resources/déploiements/suppression »,	Permet d'utiliser Global File cache.
« Microsoft.Compute/diskEncryptionSets/read"	Permet à Cloud Manager de chiffrer les disques gérés Azure sur des systèmes Cloud Volumes ONTAP à un seul nœud à l'aide de clés externes provenant d'un autre compte. Cette fonctionnalité est prise en charge à l'aide d'API.

Avantages de Cloud Manager avec les autorisations GCP

La règle Cloud Manager pour GCP inclut les autorisations nécessaires à Cloud Manager pour déployer et gérer Cloud Volumes ONTAP.

Actions	Objectif
- Compute.disks.create - Compute.disks.createSnapshot - compute.disks.delete - Compute.disks.get - Compute.disks.list - compute.disks.setLabels - compute.disks.use	Pour créer et gérer des disques pour Cloud Volumes ONTAP.

Actions	Objectif
- compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list	Pour créer des règles de pare-feu pour Cloud Volumes ONTAP.
- Compute.globalOperations.get	Pour obtenir l'état des opérations.
- Compute.images.get - Compute.images.getFromFamily - Compute.images.list - compute.images.useReadOnly	Pour obtenir les images des instances de VM.
- compute.instances.attachDisk - compute.instances.detachDisk	Pour attacher et détacher les disques à Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Pour créer et supprimer des instances de VM Cloud Volumes ONTAP.
- compute.instances.get	Pour afficher la liste des instances de VM.
- compute.instances.getSerialPortOutput	Pour obtenir les journaux de la console.
- compute.instances.list	Pour récupérer la liste des instances dans une zone.
- compute.instances.setDeletionProtection	Pour définir la protection de suppression sur l'instance.
- compute.instances.setLabels	Pour ajouter des étiquettes.
- compute.instances.setMachineType	Pour modifier le type de machine pour Cloud Volumes ONTAP.
- compute.instances.setMetadata	Pour ajouter des métadonnées.
- compute.instances.setTags	Pour ajouter des balises pour les règles de pare-feu.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Pour démarrer et arrêter Cloud Volumes ONTAP.
- Compute.machineTypes.get	Pour obtenir le nombre de cœurs à vérifier qoupas.
- compute.projects.get	Pour prendre en charge des projets multiples.
- Compute.snapshots.create - compute.snapshots.delete - Compute.snapshots.get - Compute.snapshots.list - compute.snapshots.setLabels	Pour créer et gérer des snapshots de disques persistants.
- compute.networks.get - compute.networks.list - Compute.rerégions.get - Compute.rerégions.list - Compute.subNetworks.get - Compute.subNetworks.list - Compute.zoneOperations.get - Compute.zones.get - Compute.zones.zones.list	Pour obtenir les informations de mise en réseau nécessaires à la création d'une nouvelle instance de machine virtuelle Cloud Volumes ONTAP.

Actions	Objectif
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifestes.get - deploymentmanager.manifestes.list - deploymentmanager.Operations.get - deploymentmanager.Operations.list - deploymentmanager.resources.get - deploymentmanager.resources.list - deploymentmanager.typeProviders.get.types.deploymentmanager.deploymentmanager.deploymentlist.types.deploymentmanager.deploymentlist.deploymentmanager.deploymentmanager.Deploymenttypes.DeploymentManager.Deploymentlist.Deploymenttypes.DeploymentManager.Deployment	Pour déployer l'instance de machine virtuelle Cloud Volumes ONTAP à l'aide de Google Cloud Deployment Manager.
- Logging.logEntries.list - logging.privateLogEntries.list	Pour obtenir les disques de consignation des piles.
- resourcemanager.projects.get	Pour prendre en charge des projets multiples.
- storage.seaux.create - storage.buckets.delete - storage.seaux.get - storage.seaux.list - storage.seaux.update	Pour créer et gérer un compartiment Google Cloud Storage pour le Tiering des données.
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.get - cloudkms.crypKeys.list - cloudkms.keyrings.list	Pour utiliser des clés de chiffrement gérées par le client à partir du service Cloud Key Management avec Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list	Pour définir un compte de service sur l'instance Cloud Volumes ONTAP. Ce compte de service fournit des autorisations de Tiering des données vers un compartiment Google Cloud Storage.

Pages AWS Marketplace pour Cloud Manager et Cloud Volumes ONTAP

Plusieurs offres sont disponibles sur AWS Marketplace pour Cloud Manager et Cloud Volumes ONTAP. Si vous avez besoin d'aide pour comprendre le but de chaque page, lisez les descriptions ci-dessous.

Dans tous les cas, n'oubliez pas que vous ne pouvez pas lancer Cloud Volumes ONTAP sur AWS à partir d'AWS Marketplace. Vous devez le lancer directement depuis Cloud Manager.

Objectif	Page AWS Marketplace à utiliser	Plus d'informations
Activez l'utilisation de Cloud Volumes ONTAP PAYGO, Cloud Tiering, Cloud Compliance et d'autres services d'extension	"Cloud Manager - déploiement et gestion des services de données cloud NetApp"	Cet abonnement permet de facturer la version PAYGO de Cloud Volumes ONTAP 9.6 et versions ultérieures. Il permet également de facturer les services de Tiering cloud, de conformité cloud et d'autres services complémentaires. Vous devez vous abonner à cette offre lorsque Cloud Manager vous invite à vous rediriger vers la page. Cloud Manager vous invite dans l'assistant Working Environment ou lorsque vous ajoutez de nouveaux identifiants dans les paramètres. Cette page ne vous permet pas de lancer Cloud Manager dans AWS. Cela devrait être fait à partir de "NetApp Cloud Central", Ou bien en utilisant l'ami répertorié à la ligne 3 de ce tableau.
Faciliter l'utilisation Cloud Volumes ONTAP de PAYGO, Cloud Tiering, Cloud Compliance et d'autres services d'extension *par le biais d'un contrat annuel*	"Cloud Manager (contrats) - déploiement et gestion des services de données cloud NetApp"	Cet abonnement est une alternative à l'abonnement sur la première ligne. Il vous permet d'obtenir un paiement annuel initial pour vos offres. Elle s'adresse principalement aux partenaires NetApp.
Déployez Cloud Manager depuis AWS Marketplace à l'aide d'une ami	"Cloud Manager : installation manuelle sans clés d'accès"	Nous vous recommandons de lancer Cloud Manager dans AWS à partir de "NetApp Cloud Central", Mais vous pouvez le lancer à partir de cette page AWS Marketplace, si vous préférez.
Déploiement de la formule de facturation Cloud Volumes ONTAP (9.5 ou antérieure)	• "Cloud Volumes ONTAP pour AWS" • "Cloud Volumes ONTAP pour AWS - haute disponibilité"	Ces pages AWS Marketplace vous permettent de vous abonner aux versions à un nœud ou haute disponibilité de Cloud Volumes ONTAP PAYGO pour les versions 9.5 et précédentes. À partir de la version 9.6, vous devez vous inscrire sur la page AWS Marketplace (première ligne de ce tableau pour les déploiements PAYGO).

API et automatisation

Les ressources d’automatisation pour l’infrastructure-as-code

Utilisez les ressources disponibles sur cette page pour obtenir de l’aide sur l’intégration de Cloud Manager et de Cloud Volumes ONTAP avec votre "infrastructure-as-code".

Les équipes DevOps utilisent plusieurs outils pour automatiser la configuration de nouveaux environnements et traiter l’infrastructure comme du code. L’un de ces outils est Terraform. Nous avons développé un fournisseur Terraform que les équipes DevOps peuvent utiliser avec Cloud Manager pour automatiser et intégrer Cloud Volumes ONTAP avec l’infrastructure-as-code.

"Découvrez le fournisseur netapp-cloudmManager".

- Liens connexes*
- "Blog sur le cloud NetApp : utilisation d’API REST de Cloud Manager avec un accès fédéré"
- "Blog sur le cloud NetApp : l’automatisation du cloud avec Cloud Volumes ONTAP et REST"
- "Blog sur le cloud NetApp : clonage automatisé des données pour le test des applications logicielles basé sur le cloud"
- "Blog NetApp : IAC (Infrastructure-as-Code) accéléré avec Ansible + NetApp"
- "NetApp thePub : gestion de la configuration et automatisation avec Ansible"
- "NetApp thePub : rôles pour l’utilisation d’Ansible ONTAP"

Où obtenir de l'aide et trouver plus d'informations

Vous pouvez obtenir de l'aide et obtenir plus d'informations sur Cloud Manager et Cloud Volumes ONTAP grâce à diverses ressources, notamment des vidéos, des forums et un support.

- "Prise en charge de NetApp Cloud Volumes ONTAP"

  Accédez aux ressources de support pour obtenir de l'aide et résoudre les problèmes liés à Cloud Volumes ONTAP.

- "Vidéos pour Cloud Manager et Cloud Volumes ONTAP"

  Visionnez des vidéos qui montrent comment déployer et gérer Cloud Volumes ONTAP, et comment répliquer des données dans l'ensemble de votre cloud hybride.

- "Stratégies pour Cloud Manager"

  Téléchargez des fichiers JSON qui incluent les autorisations requises par Cloud Manager pour effectuer des actions dans un fournisseur cloud.

- "Guide du développeur de l'API Cloud Manager"

  Consultez un aperçu des API, des exemples d'utilisation et une référence API.

- Formation pour Cloud Volumes ONTAP
  - "Notions fondamentales de Cloud Volumes ONTAP"
  - "Cloud Volumes ONTAP : déploiement et gestion pour Azure"
  - "Cloud Volumes ONTAP : déploiement et gestion pour AWS"
- Rapports techniques
  - "Rapport technique NetApp 4383 : caractérisation des performances de Cloud Volumes ONTAP dans Amazon Web Services avec des charges de travail applicatives"
  - "Rapport technique NetApp 4671 : caractérisation des performances de Cloud Volumes ONTAP dans Azure avec les charges de travail applicatives"
  - "Rapport technique NetApp 4816 : caractérisation des performances d'Cloud Volumes ONTAP pour Google Cloud"
- Reprise d'activité de SVM

  La reprise d'activité d'un SVM est la mise en miroir asynchrone des données d'un SVM et configuration depuis un SVM source vers un SVM de destination. Vous pouvez activer rapidement un SVM de destination pour accéder aux données si le SVM source n'est plus disponible.

  - "Cloud Volumes ONTAP 9 Guide Express de préparation à la reprise après incident SVM"

    Décrit comment configurer rapidement un SVM de destination en vue de la reprise après incident.

  - "Cloud Volumes ONTAP 9 SVM Disaster Recovery Express Guide"

Décrit comment activer rapidement une SVM de destination après un incident, puis réactiver la SVM source.

- "Guide de puissance des volumes FlexCache pour un accès plus rapide aux données"

  Décrit la procédure de création et de gestion de volumes FlexCache dans le même cluster ou sur un cluster différent de celui du volume d'origine pour accélérer l'accès aux données.

- "Conseils de sécurité"

  Identification des failles connues pour les produits NetApp, y compris ONTAP. Notez que vous pouvez remédier aux vulnérabilités de sécurité de Cloud Volumes ONTAP en suivant la documentation ONTAP.

- "Centre de documentation ONTAP 9"

  Accédez à la documentation produit d'ONTAP, qui peut vous aider à utiliser Cloud Volumes ONTAP.

- "Communauté NetApp : services de données cloud"

  Connectez-vous avec vos pairs, posez des questions, échangez des idées, trouvez des ressources et partagez les meilleures pratiques.

- "NetApp Cloud Central"

  Trouvez des informations sur d'autres produits et solutions NetApp pour le cloud.

- "Documentation produit NetApp"

  Recherchez des instructions, des ressources et des réponses dans la documentation produit NetApp.

Versions antérieures de la documentation de Cloud Manager

La documentation relative aux versions précédentes de Cloud Manager est disponible si vous n’utilisez pas la dernière version.

- "Cloud Manager 3.7"
- "Cloud Manager 3.6"

Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

Droits d'auteur

http://www.netapp.com/us/legal/copyright.aspx

Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

http://www.netapp.com/us/legal/netapptmlist.aspx

Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l'adresse suivante :

https://www.netapp.com/us/media/patents-page.pdf

Politique de confidentialité

https://www.netapp.com/us/legal/privacypolicy/index.aspx

Source ouverte

Les fichiers de notification fournissent des informations sur les droits d'auteur et les licences de tiers utilisés dans le logiciel NetApp.

- "Avis concernant Cloud Manager 3.8.7"
- "Avis concernant Cloud Manager 3.8.6"
- "Avis concernant Cloud Manager 3.8.5"
- "Avis concernant Cloud Manager 3.8.4"
- "Avis concernant Cloud Manager 3.8.3"
- "Avis concernant Cloud Manager 3.8.2"
- "Avis concernant Cloud Manager 3.8.1"
- "Avis concernant Cloud Manager 3.8"
- "Avis concernant le Cloud Backup Service"
- "Remarque concernant Global File cache"
- "Avis concernant Cloud Compliance"