Documentation sur Cloud Manager et Cloud Volumes ONTAP

Cloud Manager 3.7

NetApp
October 23, 2024

Sommaire

Documentation sur Cloud Manager et Cloud Volumes ONTAP

Avec Cloud Manager, vous pouvez déployer et gérer NetApp Cloud Volumes ONTAP, une solution de gestion des données qui assure la protection, la visibilité et le contrôle de vos charges de travail cloud.

BlueXP

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

"Consultez la documentation BlueXP"

Découvrez les nouveautés

- "Nouveautés de Cloud Manager"
- "Nouveautés de Cloud Volumes ONTAP"

Commencez

- "Commencez dans AWS"
- "Commencez à Azure"
- "Lancez-vous dans Google Cloud Platform"
- "Recherchez les configurations prises en charge pour Cloud Volumes ONTAP"
- "Examinez les exigences de mise en réseau pour Cloud Manager"
- "Analyse des exigences réseau pour Cloud Volumes ONTAP pour AWS"
- "Étude des exigences réseau pour Cloud Volumes ONTAP pour Azure"
- "Étude des exigences de mise en réseau pour Cloud Volumes ONTAP pour GCP"
- "Planifiez votre configuration Cloud Volumes ONTAP"

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 3.7

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 3.6"
"Nouveautés de la version 3.5"
"Nouveautés de la version 3.4"

Mise à jour de Cloud Manager 3.7.5 (16 décembre 2019)

Cette mise à jour comprend les améliorations suivantes :

- Cloud Volumes ONTAP 9.7
- Cloud Compliance pour Cloud Volumes ONTAP

Cloud Volumes ONTAP 9.7

Cloud Volumes ONTAP 9.7 est désormais disponible dans AWS, Azure et Google Cloud Platform.

"Découvrez les nouveautés d'Cloud Volumes ONTAP 9.7".

Cloud Compliance pour Cloud Volumes ONTAP

Cloud Compliance est un service de confidentialité et de conformité des données pour Cloud Volumes ONTAP dans AWS et Azure. Avec la technologie d'intelligence artificielle (IA), Cloud Compliance aide les entreprises à comprendre le contexte des données et à identifier les données sensibles dans les systèmes Cloud Volumes ONTAP.

Cloud Compliance est actuellement disponible sous forme de version contrôlée.

"En savoir plus sur Cloud Compliance".

Cloud Manager 3.7.5 (3 décembre 2019)

Cloud Manager 3.7.5 comprend plusieurs améliorations :

- Vitesse d'écriture élevée pour Cloud Volumes ONTAP dans GCP
- Clusters ONTAP sur site comme stockage persistant pour Kubernetes
- Dernière version de Trident pour Kubernetes
- Prise en charge des comptes de stockage v2 génériques Azure
- Préfixes dans les noms de compte de stockage Azure à l'aide d'API

Vitesse d'écriture élevée pour Cloud Volumes ONTAP dans GCP

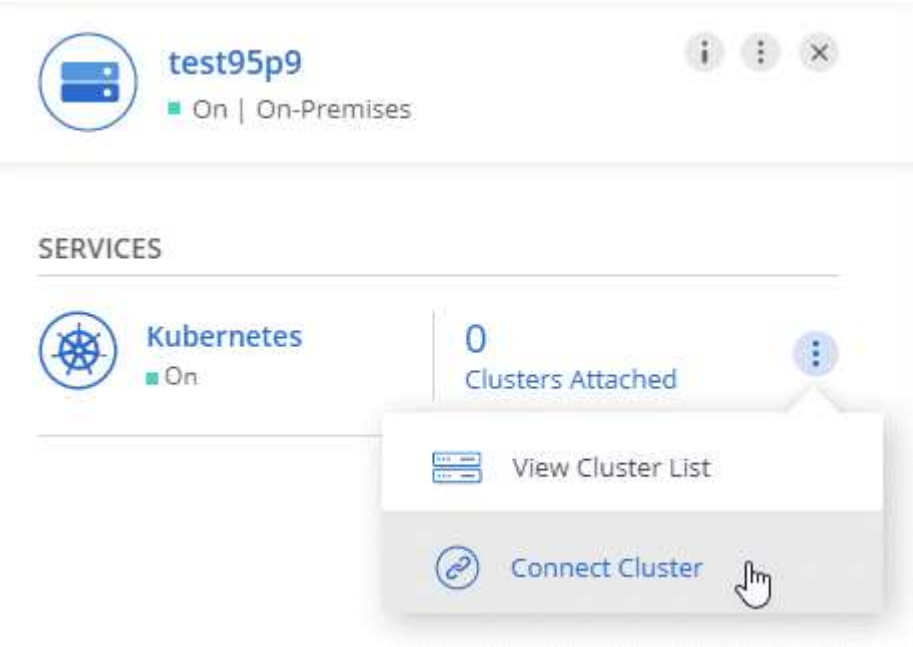
Vous pouvez désormais activer la vitesse d'écriture élevée sur les systèmes Cloud Volumes ONTAP nouveaux et existants dans Google Cloud Platform. La vitesse d'écriture élevée est un choix judicieux si vos workloads nécessitent des performances d'écriture rapides.

- "Découvrez comment choisir une vitesse d'écriture"
- "Découvrez comment modifier la vitesse d'écriture sur les systèmes existants"

Clusters ONTAP sur site comme stockage persistant pour Kubernetes

Cloud Manager vous permet désormais d'utiliser des clusters ONTAP sur site en tant que stockage persistant pour les conteneurs. À l'instar d'Cloud Volumes ONTAP, Cloud Manager automatise le déploiement de NetApp Trident et connecte ONTAP aux clusters Kubernetes.

Une fois que vous avez ajouté un cluster Kubernetes à Cloud Manager, vous pouvez le connecter à vos clusters ONTAP sur site à partir de la page Working Environments :



"Découvrez comment démarrer".

Dernière version de Trident pour Kubernetes

Cloud Manager installe désormais une version plus récente de Trident (version 19.07.1) lorsque vous connectez un environnement de travail à un cluster Kubernetes.

Prise en charge des comptes de stockage v2 génériques Azure

Lorsque vous déployez de nouveaux systèmes Cloud Volumes ONTAP dans Azure, les comptes de stockage créés par Cloud Manager pour les diagnostics et le Tiering des données sont désormais des comptes de stockage v2 à usage générique.

Préfixes dans les noms de compte de stockage Azure à l'aide d'API

Vous pouvez désormais ajouter un préfixe aux noms des comptes de stockage Azure créés par Cloud Manager pour Cloud Volumes ONTAP. Il vous suffit d'utiliser le paramètre *storageAccountPrefix* lorsque vous

déployez un nouveau système Cloud Volumes ONTAP dans Azure.

"Pour plus d'informations sur l'utilisation des API, reportez-vous au Guide du développeur d'API".

Cloud Manager 3.7.4 (6 octobre 2019)

Cloud Manager 3.7.4 comprend plusieurs améliorations :

- Prise en charge de Azure NetApp Files
- Améliorations de Cloud Volumes ONTAP pour GCP
- Sauvegardez vers l'amélioration S3
- Cryptage des disques racines et de démarrage dans AWS
- Prise en charge de la région d'AWS Bahreïn
- Soutien à la région du Nord des Émirats arabes Unis

Prise en charge de Azure NetApp Files

Vous pouvez désormais afficher et créer des volumes NFS pour Azure NetApp Files directement depuis Cloud Manager. Cette amélioration poursuit notre objectif : vous aider à gérer votre stockage cloud à partir d'une interface unique.

"Découvrez comment démarrer".

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

```
"Microsoft.NetApp/netAppAccounts/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete"
```

Améliorations de Cloud Volumes ONTAP pour GCP

Cloud Manager 3.7.4 apporte plusieurs améliorations à Cloud Volumes ONTAP pour Google Cloud Platform :

Abonnements avec paiement à l'utilisation sur GCP Marketplace
: Vous pouvez payer Cloud Volumes ONTAP selon votre utilisation en vous abonnant à Cloud Volumes ONTAP sur le marché Google Cloud Platform.

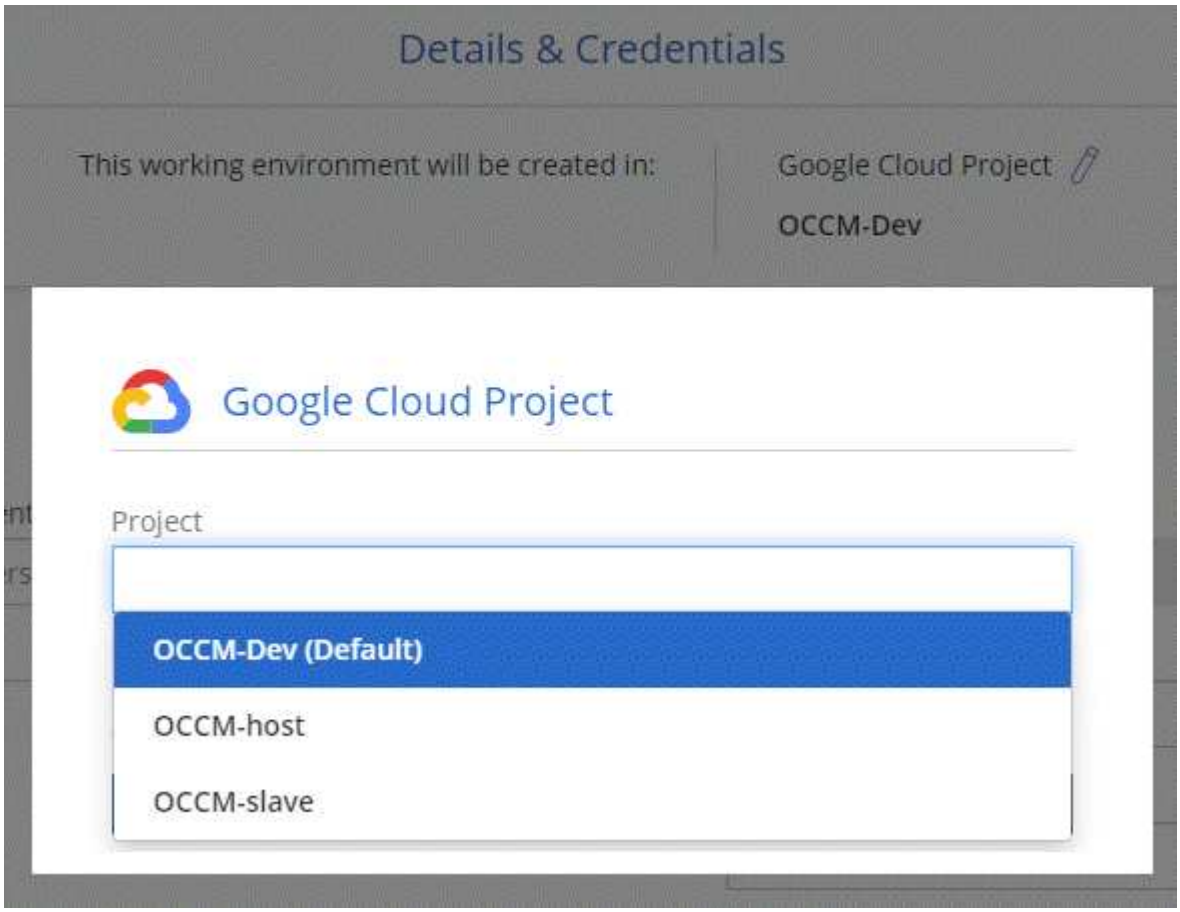
  "Google Cloud Platform Marketplace : Cloud Manager pour Cloud Volumes ONTAP"

VPC partagé
: Cloud Manager et Cloud Volumes ONTAP sont désormais pris en charge par un VPC partagé de Google Cloud Platform.

  Le VPC partagé vous permet de configurer et de gérer de manière centralisée les réseaux virtuels sur plusieurs projets. Vous pouvez configurer des réseaux VPC partagés dans le projet *host* et déployer les instances de machine virtuelle Cloud Manager et Cloud Volumes ONTAP dans un projet *service*. "Documentation Google Cloud : présentation du VPC partagé".

Plusieurs projets Google Cloud

Cloud Volumes ONTAP n'a plus besoin d'être dans le même projet que Cloud Manager. Ajoutez le compte de service Cloud Manager et le rôle aux projets supplémentaires, puis choisissez parmi ceux que vous déployez Cloud Volumes ONTAP.



Pour plus d'informations sur la configuration du compte de service Cloud Manager, "reportez-vous à l'étape 4b de cette page".

Clés de chiffrement gérées par le client lors de l'utilisation d'API Cloud Manager

Google Cloud Storage chiffre toujours vos données avant leur écriture sur le disque, mais vous pouvez utiliser les API Cloud Manager pour créer un nouveau 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.

Reportez-vous à la "Guide du développeur API" Pour plus d'informations sur l'utilisation des paramètres « GcpEncryption ».

Cette fonctionnalité requiert de nouvelles autorisations, comme indiqué dans la dernière "Règle Cloud Manager pour GCP":

```
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
```

Sauvegardez vers l'amélioration S3

Vous pouvez maintenant supprimer les sauvegardes des volumes existants. Auparavant, vous pouviez uniquement supprimer les sauvegardes des volumes qui ont été supprimés.

"En savoir plus sur Backup vers S3".

Cryptage des disques racines et de démarrage dans AWS

Lorsque vous activez le chiffrement des données à l'aide du service de gestion des clés AWS (KMS), les disques racine et de démarrage pour Cloud Volumes ONTAP sont désormais 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.

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.

Prise en charge de la région d'AWS Bahreïn

Cloud Manager et Cloud Volumes ONTAP sont désormais pris en charge dans la région AWS Moyen-Orient (Bahreïn).

Soutien à la région du Nord des Émirats arabes Unis

Cloud Manager et Cloud Volumes ONTAP sont désormais pris en charge dans la région du Nord d'Azure Émirats arabes Unis.

"Afficher toutes les régions prises en charge".

Mise à jour de Cloud Manager 3.7.3 (15 septembre 2019)

Avec Cloud Manager, vous pouvez désormais sauvegarder les données d'Cloud Volumes ONTAP vers Amazon S3.

Sauvegarde vers S3

Il s'agit d'un service complémentaire pour Cloud Volumes ONTAP offrant des fonctionnalités de sauvegarde et de restauration entièrement gérées pour la protection, ainsi que l'archivage à long terme de vos données cloud. Les sauvegardes sont stockées dans le stockage objet S3, indépendamment des copies Snapshot des volumes utilisées pour la restauration ou le clonage à court terme.

"Découvrez comment démarrer".

Cette fonction nécessite une mise à jour vers "Politique de Cloud Manager". Les autorisations de terminal VPC suivantes sont désormais requises :

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

Cloud Manager 3.7.3 (11 septembre 2019)

Cloud Manager 3.7.3 comprend plusieurs améliorations :

- Détection et gestion de Cloud Volumes Service pour AWS
- Nouvel abonnement requis dans AWS Marketplace
- Support pour AWS GovCloud (USA-est)

Détection et gestion de Cloud Volumes Service pour AWS

Cloud Manager vous permet désormais de découvrir les volumes cloud dans votre "Cloud Volumes Service pour AWS" abonnement. Une fois la découverte terminée, vous pouvez ajouter des volumes cloud supplémentaires directement à partir de Cloud Manager. Cette amélioration offre une fenêtre unique depuis laquelle vous pouvez gérer le stockage cloud NetApp.

"Découvrez comment démarrer".

Nouvel abonnement requis dans AWS Marketplace

"Un nouvel abonnement est disponible sur AWS Marketplace". Cet abonnement unique est nécessaire pour déployer Cloud Volumes ONTAP 9.6 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 créé et chaque fonctionnalité d'extension activée.

À partir de la version 9.6, cette nouvelle méthode d'abonnement remplace les deux abonnements AWS Marketplace pour Cloud Volumes ONTAP PAYGO auxquels vous avez déjà souscrit. Vous avez toujours besoin d'abonnements par le biais de "Pages AWS Marketplace existantes lors du déploiement d'Cloud Volumes ONTAP BYOL".

"En savoir plus sur chaque page AWS Marketplace".

Support pour AWS GovCloud (USA-est)

Cloud Manager et Cloud Volumes ONTAP sont désormais pris en charge dans la région AWS GovCloud (USA-East).

Disponibilité générale de Cloud Volumes ONTAP dans GCP (3 septembre 2019)

Cloud Volumes ONTAP est désormais disponible dans Google Cloud Platform (GCP) lorsque vous utilisez votre propre licence (BYOL). Une offre de paiement à l'utilisation est également disponible. La promotion offre des licences gratuites pour un nombre illimité de systèmes et expirera à la fin de septembre 2019.

- "Découvrez comment utiliser GCP"
- "Affichez les configurations prises en charge"

Cloud Manager 3.7.2 (5 août 2019)

- Licences FlexCache
- Classes de stockage Kubernetes pour iSCSI
- Gestion des inodes
- Prise en charge de la région de Hong Kong en AWS

- Prise en charge des régions centrales d'Australie dans Azure

Licences FlexCache

Cloud Manager génère désormais 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.

Classes de stockage Kubernetes pour iSCSI

Lorsque vous connectez Cloud Volumes ONTAP à un cluster Kubernetes, Cloud Manager crée désormais deux classes de stockage Kubernetes supplémentaires que vous pouvez utiliser avec les volumes persistants iSCSI :

- **netapp-file-san** : pour les volumes persistants iSCSI sur des systèmes Cloud Volumes ONTAP à un seul nœud
- **netapp-file-redondant-san** : pour la liaison de volumes persistants iSCSI aux paires HA Cloud Volumes ONTAP

Gestion des inodes

Cloud Manager surveille à présent l'utilisation d'inode dans 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.

Cloud Manager surveille l'utilisation d'inode uniquement lorsque le mode de gestion de la capacité est défini sur automatique (il s'agit du paramètre par défaut).

Prise en charge de la région de Hong Kong en AWS

Cloud Manager et Cloud Volumes ONTAP sont désormais pris en charge dans la région Asie-Pacifique (Hong Kong) dans AWS.

Prise en charge des régions centrales d'Australie dans Azure

Cloud Manager et Cloud Volumes ONTAP sont désormais pris en charge dans les régions Azure suivantes :

- Australie centrale
- Australie Centrale 2

"Voir la liste complète des régions prises en charge".

Mise à jour relative à la sauvegarde et à la restauration (15 juillet 2019)

Depuis la version 3.7.1, Cloud Manager ne prend plus en charge le téléchargement d'une sauvegarde et son utilisation pour restaurer votre configuration Cloud Manager. "Procédez comme suit pour restaurer Cloud Manager".

Cloud Manager 3.7.1 (1er juillet 2019)

- Cette version inclut principalement des correctifs.

- Une amélioration est apportée : Cloud Manager installe désormais une licence NetApp Volume Encryption (NVE) sur chaque système Cloud Volumes ONTAP enregistré auprès du support NetApp (systèmes nouveaux et existants).
  - "Ajout de comptes du site de support NetApp à Cloud Manager"
  - "Enregistrement des systèmes de paiement à l'utilisation"
  - "Configuration de NetApp Volume Encryption"

    Cloud Manager n'installe pas la licence NVE sur les systèmes de la région Chine.

Mise à jour de Cloud Manager 3.7 (16 juin 2019)

Cloud Volumes ONTAP 9.6 est désormais disponible dans AWS, Azure et dans Google Cloud Platform en tant que préversion privée. Pour rejoindre la présentation privée, envoyez une demande à l'adresse ng-Cloud-Volume-ONTAP-preview@netapp.com.

"Découvrez les nouveautés d'Cloud Volumes ONTAP 9.6"

Cloud Manager 3.7 (5 juin 2019)

- Prise en charge de la prochaine version d'Cloud Volumes ONTAP 9.6
- Comptes NetApp Cloud Central
- Sauvegarde et restauration avec Cloud Backup Service

Prise en charge de la prochaine version d'Cloud Volumes ONTAP 9.6

Cloud Manager 3.7 inclut la prise en charge de la prochaine version d'Cloud Volumes ONTAP 9.6. La version 9.6 inclut une présentation privée de Cloud Volumes ONTAP dans Google Cloud Platform. Les notes de version seront mises à jour dès que la version 9.6 sera disponible.

Comptes NetApp Cloud Central

Nous avons amélioré votre façon de gérer vos ressources clouds. Chaque système Cloud Manager sera associé à un *compte NetApp Cloud Central*. Le compte permet une colocation, qui est prévu pour d'autres services de données cloud NetApp à l'avenir.

Dans Cloud Manager, un compte Cloud Central est un conteneur pour vos systèmes Cloud Manager et pour les *espaces de travail* dans lesquels les utilisateurs déploient Cloud Volumes ONTAP.

"Découvrez comment les comptes Cloud Central favorisent la colocation".

Cloud Manager doit accéder à *https://cloudmanager.cloud.netapp.com* pour vous connecter au service de compte Cloud Central. Ouvrez cette URL sur votre pare-feu pour vous assurer que Cloud Manager peut contacter le service.

Intégration de votre système aux comptes Cloud Central

Quelques fois que vous effectuez une mise à niveau vers Cloud Manager 3.7, NetApp choisit des systèmes Cloud Manager spécifiques pour les intégrer aux comptes Cloud Central. Lors de cette procédure, NetApp crée un compte, attribue de nouveaux rôles à chaque utilisateur, crée des espaces de travail et place les environnements de travail existants dans ces espaces de travail. Les systèmes Cloud Volumes ONTAP ne provoquent aucune perturbation.

"Pour toute question, consultez cette FAQ".

Sauvegarde et restauration avec Cloud Backup Service

NetApp Cloud Backup Service pour Cloud Volumes ONTAP offre des fonctionnalités de sauvegarde et de restauration entièrement gérées pour la protection et l'archivage à long terme de vos données cloud. Vous pouvez intégrer Cloud Backup Service avec Cloud Volumes ONTAP pour AWS. Les sauvegardes créées par le service sont stockées dans le stockage objet AWS S3.

"En savoir plus sur Cloud Backup Service".

Pour démarrer, installez et configurez l'agent de sauvegarde, puis démarrez les opérations de sauvegarde et de restauration. Si vous avez besoin d'aide, nous vous encourageons à nous contacter en utilisant l'icône de chat dans Cloud Manager.

Ce processus manuel n'est plus pris en charge. La fonctionnalité de sauvegarde sur S3 a été intégrée à Cloud Manager dans la version 3.7.3.

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.

Cloud Manager doit rester exécuté en permanence

Cloud Manager est un élément clé de l'état et de la facturation de Cloud Volumes ONTAP. Si Cloud Manager est hors tension, les systèmes Cloud Volumes ONTAP s'arrêtent après une perte de communication avec Cloud Manager pendant plus de 4 jours.

Les hôtes Linux partagés ne sont pas pris en charge

Cloud Manager 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.

Active Directory n’est pas pris en charge par défaut avec les nouvelles installations de Cloud Manager

À partir de la version 3.4, les nouvelles installations de Cloud Manager ne prennent pas en charge l’authentification Active Directory de votre entreprise pour la gestion des utilisateurs. Si nécessaire, NetApp peut vous aider à configurer Active Directory avec Cloud Manager. Cliquez sur l’icône Chat dans le coin inférieur droit de Cloud Manager pour obtenir de l’aide.

Limites de la région AWS GovCloud (US)

- Cloud Manager doit être déployé dans la région AWS GovCloud (US) si vous souhaitez lancer des instances Cloud Volumes ONTAP dans la région AWS GovCloud (US).
- Lorsqu’il est déployé dans la région AWS GovCloud (US), Cloud Manager ne peut pas détecter les clusters ONTAP dans une configuration NetApp Private Storage pour Microsoft Azure ou dans une configuration NetApp Private Storage pour SoftLayer.

Cloud Manager ne configure pas les volumes iSCSI

Lorsque vous créez un volume dans Cloud Manager à l’aide de Storage System View, vous pouvez choisir le protocole NFS ou CIFS. Vous devez utiliser OnCommand System Manager pour créer un volume pour iSCSI.

Limitation de la machine virtuelle de stockage (SVM)

Cloud Volumes ONTAP prend en charge un SVM de service de données et un ou plusieurs SVM utilisés pour la reprise après incident. Le seul SVM transmettant les données s’étend à l’ensemble du système Cloud Volumes ONTAP (paire HA ou nœud unique).

Cloud Manager ne prend pas en charge la configuration ou l’orchestration de la reprise après incident SVM. Il ne prend pas en charge les tâches liées au stockage sur des SVM supplémentaires. Vous devez utiliser System Manager ou l’interface de ligne de commande pour la reprise après incident SVM.

Concepts

Présentation de Cloud Manager et de Cloud Volumes ONTAP

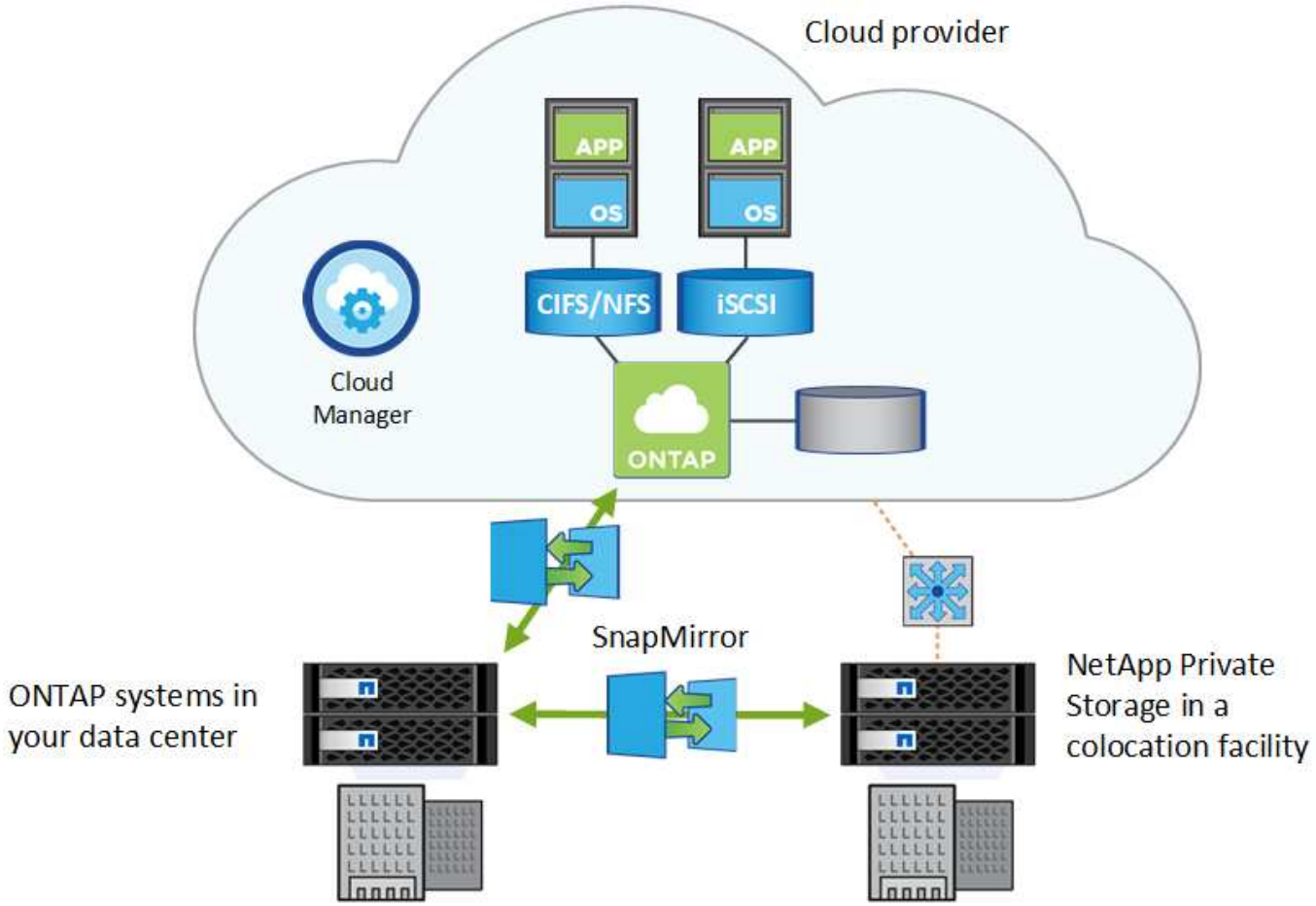
Cloud Manager vous permet de déployer Cloud Volumes ONTAP, qui fournit des fonctionnalités haute performance pour votre stockage cloud et de répliquer facilement les données dans les clouds hybrides basés sur NetApp.

Le gestionnaire Cloud

Cloud Manager a été conçu avec simplicité. Il vous guide dans la configuration de Cloud Volumes ONTAP en quelques étapes et simplifie la gestion des données en proposant un provisionnement simplifié du stockage et une gestion automatisée de la capacité, la réplication des données par glisser-déposer dans un cloud hybride, etc.

Cloud Manager est requis pour déployer et gérer Cloud Volumes ONTAP, mais il peut également découvrir et provisionner le stockage pour les clusters ONTAP sur site. Il s'agit d'un point de contrôle central pour votre infrastructure de stockage cloud et sur site.

Vous pouvez exécuter Cloud Manager dans le cloud ou dans votre réseau. Il vous suffit d'établir une connexion avec les réseaux dans lesquels vous souhaitez déployer Cloud Volumes ONTAP. L'image suivante montre Cloud Manager et Cloud Volumes ONTAP s'exécutant dans un fournisseur cloud. Il montre également la réplication des données sur un cloud hybride.



"En savoir plus sur Cloud Manager"

Cloud Volumes ONTAP

Cloud Volumes ONTAP est une appliance de stockage logicielle qui exécute le logiciel de gestion des données ONTAP dans le cloud. Vous pouvez utiliser Cloud Volumes ONTAP pour les charges de travail de production, la reprise après incident, les DevOps, les partages de fichiers et la gestion des bases de données.

Cloud Volumes ONTAP étend le stockage d'entreprise au cloud avec les fonctionnalités clés suivantes :

- Efficacité du stockage La déduplication intégrée des données, la compression des données, le provisionnement fin et le clonage sont indispensables pour réduire les coûts de stockage.
- Une haute disponibilité assure une fiabilité exceptionnelle et la continuité de l'activité en cas de défaillances dans votre environnement cloud.
- Réplication des données Cloud Volumes ONTAP exploite SnapMirror, la technologie de réplication de pointe de NetApp, pour répliquer les données sur site vers le cloud, ce qui facilite la disponibilité de copies secondaires pour plusieurs cas d'utilisation.
- Hiérarchisation des données Basculer entre les pools de stockage hautes et basses performances à la demande sans mettre les applications hors ligne.
- Cohérence des applications assurer la cohérence des copies NetApp Snapshot avec NetApp SnapCenter.

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

"Afficher les configurations Cloud Volumes ONTAP prises en charge"

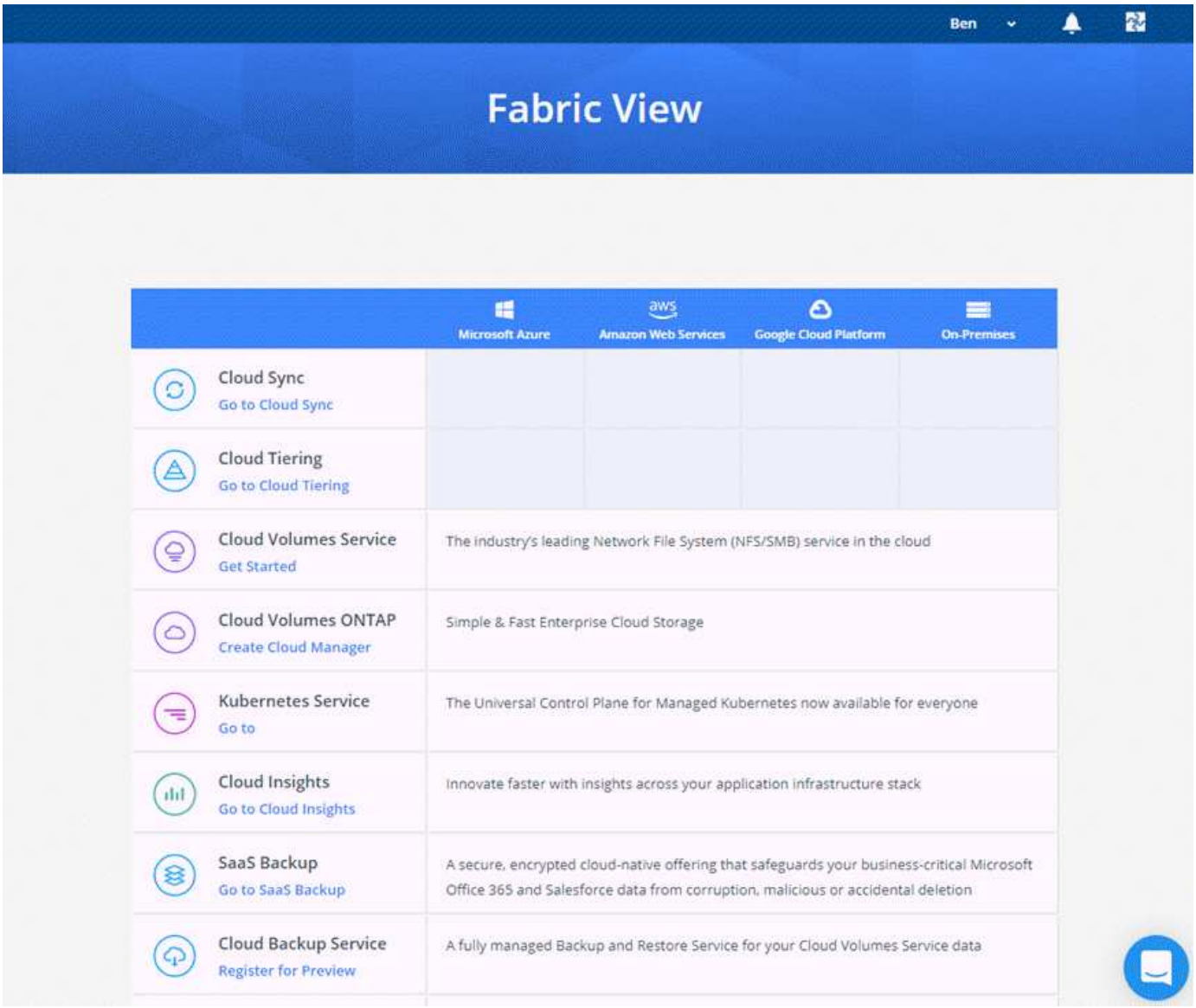
"En savoir plus sur Cloud Volumes ONTAP"

NetApp Cloud Central

"NetApp Cloud Central" Cette solution est centralisée pour accéder aux services de données cloud NetApp et les gérer. Ces services vous permettent d'exécuter des applications stratégiques dans le cloud, de créer des sites de reprise après incident automatisés, de sauvegarder vos données SaaS et de migrer et contrôler efficacement les données sur plusieurs clouds.

L'intégration de Cloud Manager avec NetApp Cloud Central offre plusieurs avantages, notamment une expérience de déploiement simplifiée, un emplacement unique pour afficher et gérer plusieurs systèmes Cloud Manager et une authentification utilisateur centralisée.

Grâce à l'authentification centralisée des utilisateurs, vous pouvez utiliser les mêmes informations d'identification sur les systèmes Cloud Manager et entre Cloud Manager et d'autres services de données, tels que Cloud Sync. Il est également facile de réinitialiser votre mot de passe si vous l'avez oublié.



Comptes Cloud Central

Chaque système Cloud Manager est associé à un *compte NetApp Cloud Central*. Un compte Cloud Central fournit une colocation qui vous permet d'organiser les utilisateurs et les ressources dans des espaces de travail isolés.

Un compte Cloud Central favorise la colocation :

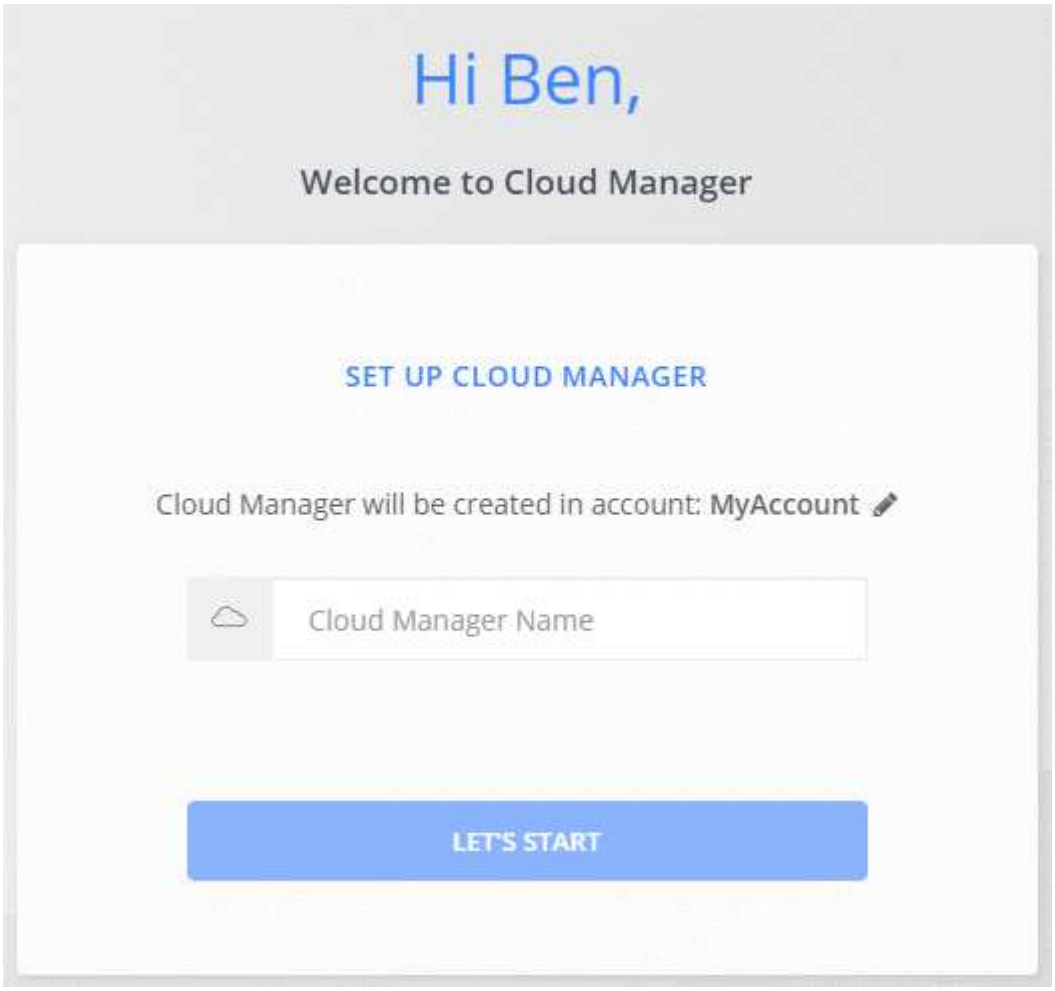
- Un seul compte Cloud Central peut inclure plusieurs systèmes Cloud Manager qui répondent à différents besoins.

  Comme les utilisateurs sont associés au compte Cloud Central, il est inutile de configurer des utilisateurs pour chaque système Cloud Manager.

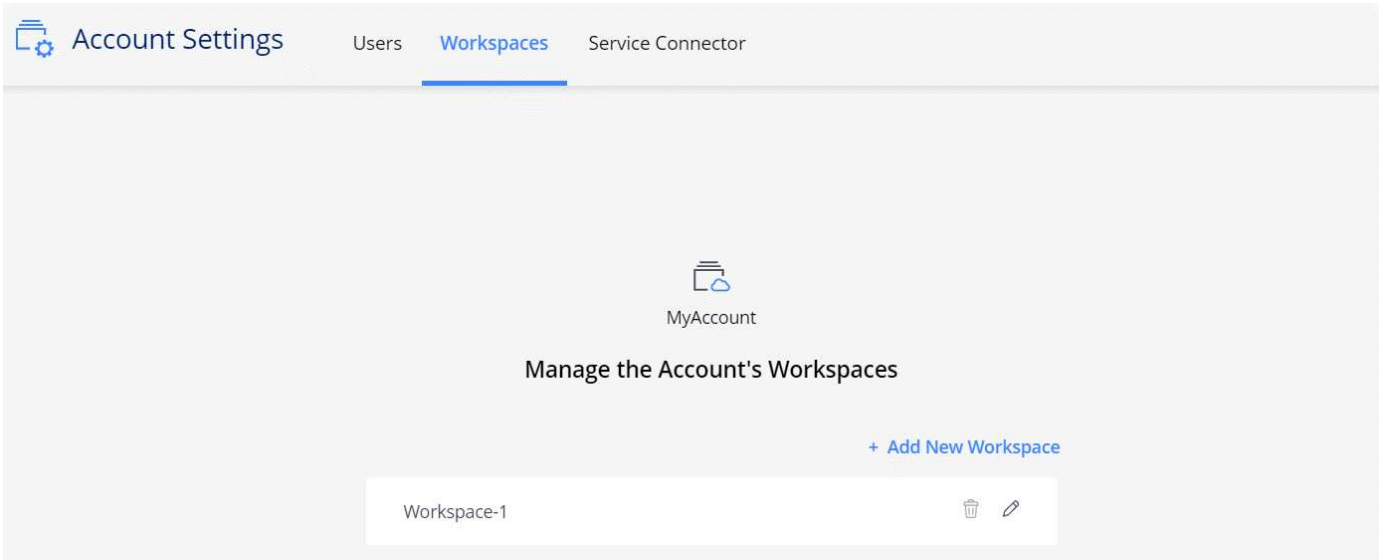
- Dans chaque système Cloud Manager, plusieurs utilisateurs peuvent déployer et gérer des systèmes Cloud Volumes ONTAP dans des environnements isolés appelés « espaces de travail ».

  Ces espaces de travail sont invisibles pour les autres utilisateurs, à moins qu'ils ne soient partagés.

Lorsque vous déployez Cloud Manager, vous sélectionnez le compte Cloud Central à associer au système :



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



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

Cloud Manager doit accéder à *https://cloudmanager.cloud.netapp.com* pour vous connecter au service de compte Cloud Central. Ouvrez cette URL sur votre pare-feu pour vous assurer que Cloud Manager peut contacter le service.

Utilisateurs, espaces de travail et connecteurs de service

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 et les connecteurs de service qui sont associés au compte.

Utilisateurs

Il s'agit des 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.

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 de service

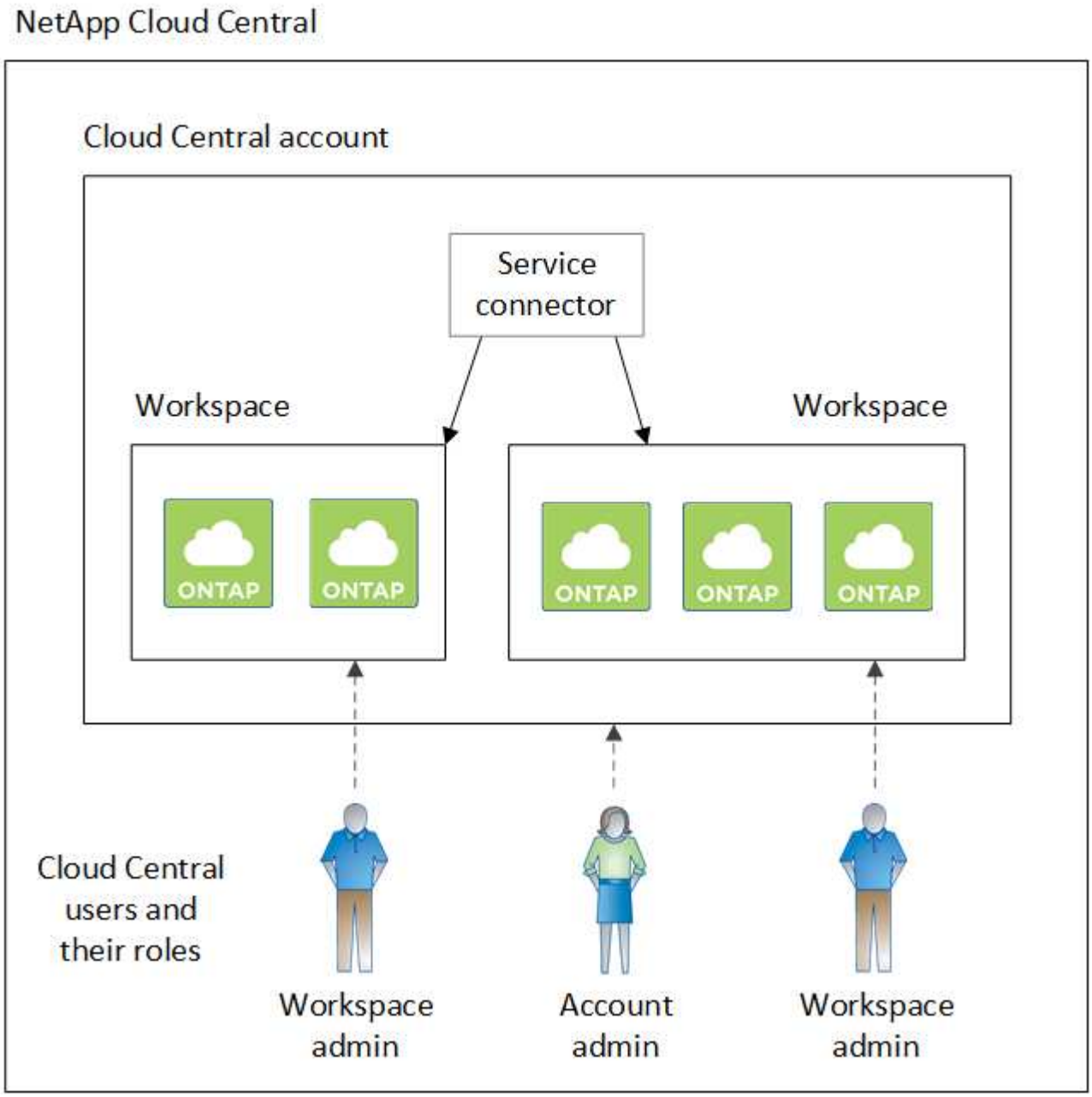
Un connecteur de service fait partie de Cloud Manager. Elle exécute la plupart du logiciel Cloud Manager (comme l'interface utilisateur), sauf quelques services Cloud Central auxquels il se connecte (authenti0 et les comptes Cloud Central). Il s'exécute sur l'instance de machine virtuelle déployée dans votre fournisseur cloud ou sur un hôte sur site que vous avez configuré.

Vous pouvez utiliser un connecteur de service avec plusieurs services de données cloud NetApp. Par exemple, si vous disposez déjà d'un connecteur de service pour Cloud Manager, vous pouvez le sélectionner une fois le service NetApp Cloud Tiering configuré.

Exemples

L'exemple suivant montre un compte qui utilise deux espaces de travail pour créer des environnements isolés pour les systèmes Cloud Volumes ONTAP. Par exemple, un espace de travail peut être pour un environnement de staging, tandis que l'autre est pour un environnement de production.

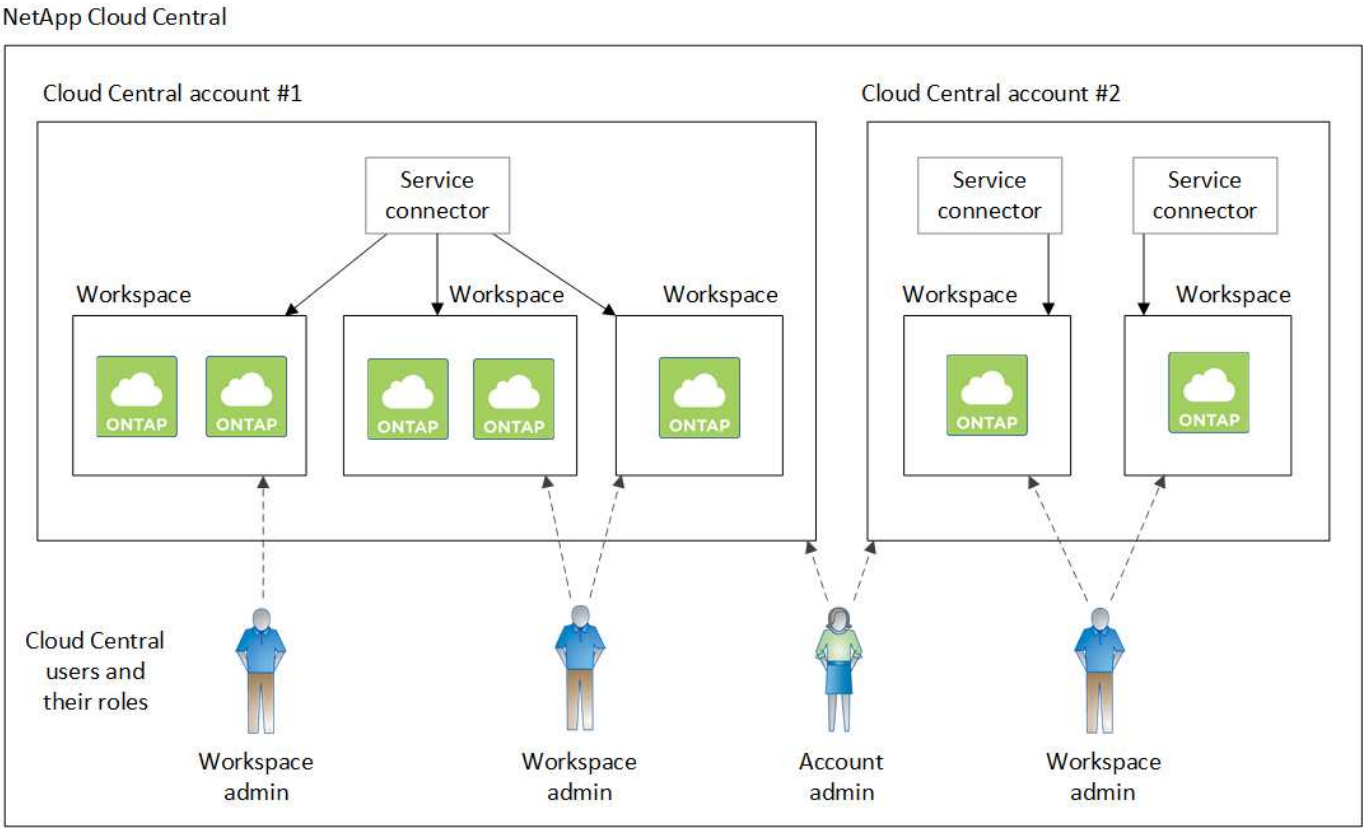
Cloud Manager et les systèmes Cloud Volumes ONTAP ne résident pas *dans* le compte NetApp Cloud Central—ils sont exécutés dans un fournisseur cloud. Il s'agit d'une représentation conceptuelle de la relation entre chaque composant.



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 Cloud Central pour fournir des services à ses clients, tout en utilisant un autre compte pour fournir la reprise après incident à l'une de ses business units.

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

Là encore, Cloud Manager et les systèmes Cloud Volumes ONTAP ne résident pas *dans* le compte NetApp Cloud Central—ils sont exécutés dans un fournisseur cloud. Il s'agit d'une représentation conceptuelle de la relation entre chaque composant.



Forum aux questions sur l'intégration avec les comptes Cloud Central

Quelques fois que vous effectuez une mise à niveau vers Cloud Manager 3.7, NetApp choisit des systèmes Cloud Manager spécifiques pour les intégrer aux comptes Cloud Central. Cette FAQ peut répondre aux questions que vous pourriez avoir sur le processus.

Quelle est la durée du processus ?

Quelques minutes à peine.

Cloud Manager sera-t-il indisponible ?

Non, vous pouvez toujours accéder au système Cloud Manager.

Qu'en est-il de Cloud Volumes ONTAP ?

Les systèmes Cloud Volumes ONTAP ne provoquent aucune perturbation.

Que se passe-t-il au cours de ce processus ?

NetApp effectue les opérations suivantes pendant le processus d'intégration :

1. Crée un compte Cloud Central et l'associe à votre système Cloud Manager.
2. Attribue de nouveaux rôles à chaque utilisateur existant :
    - Les administrateurs de Cloud Manager deviennent des administrateurs de compte
    - Les administrateurs des locataires et de l'environnement de travail deviennent des administrateurs de l'espace de travail

3. Crée des espaces de travail qui remplacent des locataires existants.
4. Place vos environnements de travail dans ces espaces de travail.
5. Associe le connecteur de service à tous les espaces de travail.

Est-ce que j'ai installé mon système Cloud Manager ?

Non NetApp intégrera les systèmes avec des comptes Cloud Central, où qu'ils résident, que ce soit dans AWS, Azure ou sur site.

Comptes de fournisseurs cloud

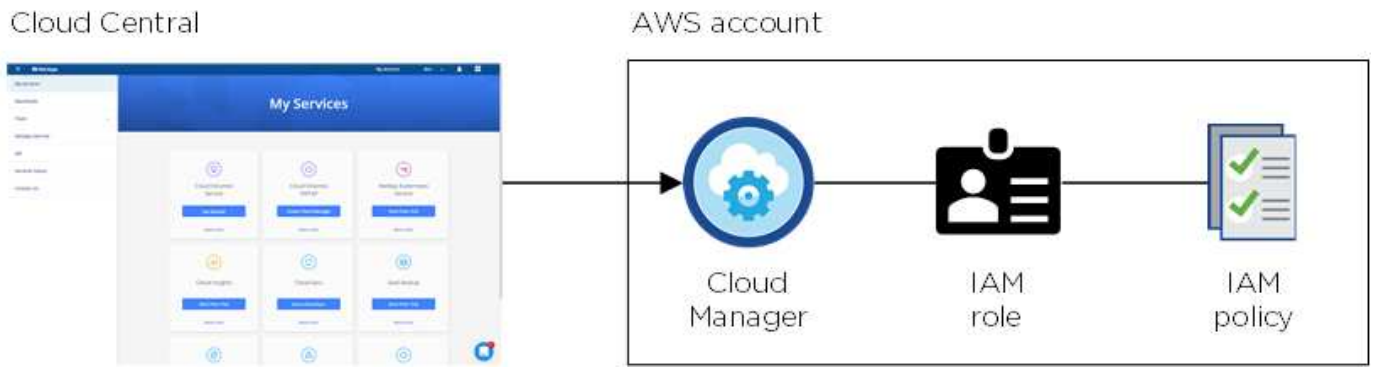
Comptes et autorisations AWS

Cloud Manager vous permet de choisir le compte AWS où vous souhaitez déployer un système Cloud Volumes ONTAP. Vous pouvez déployer tous les systèmes Cloud Volumes ONTAP sur le compte AWS initial, ou configurer d'autres comptes.

Compte AWS initial

Lorsque vous déployez Cloud Manager depuis NetApp Cloud Central, vous devez utiliser un compte AWS avec des autorisations pour lancer l'instance Cloud Manager. Les autorisations requises sont répertoriées dans le "Politique NetApp Cloud Central pour AWS".

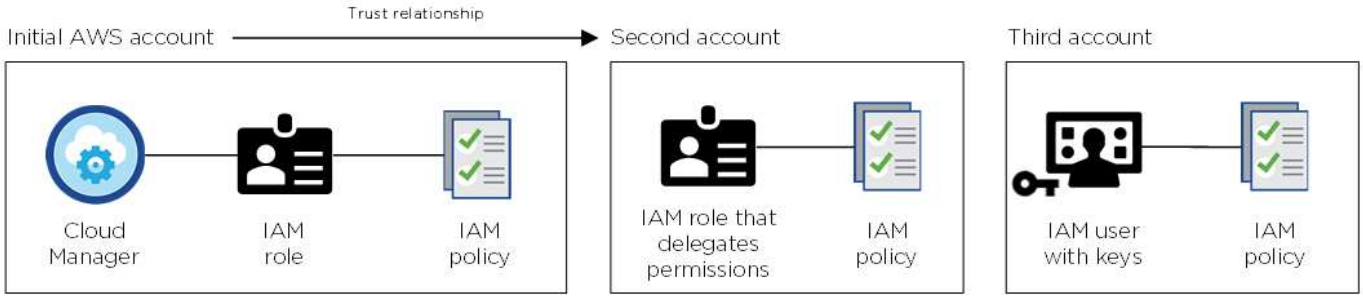
Lorsque Cloud Central lance l'instance Cloud Manager dans AWS, il crée un rôle IAM et un profil d'instance pour l'instance. Il attache également une règle qui fournit les autorisations nécessaires à cloud Manager pour déployer et gérer Cloud Volumes ONTAP dans ce compte AWS. "Examinez comment Cloud Manager utilise les autorisations".



Cloud Manager sélectionne par défaut ce compte de fournisseur cloud lors de la création d'un nouvel environnement de travail :

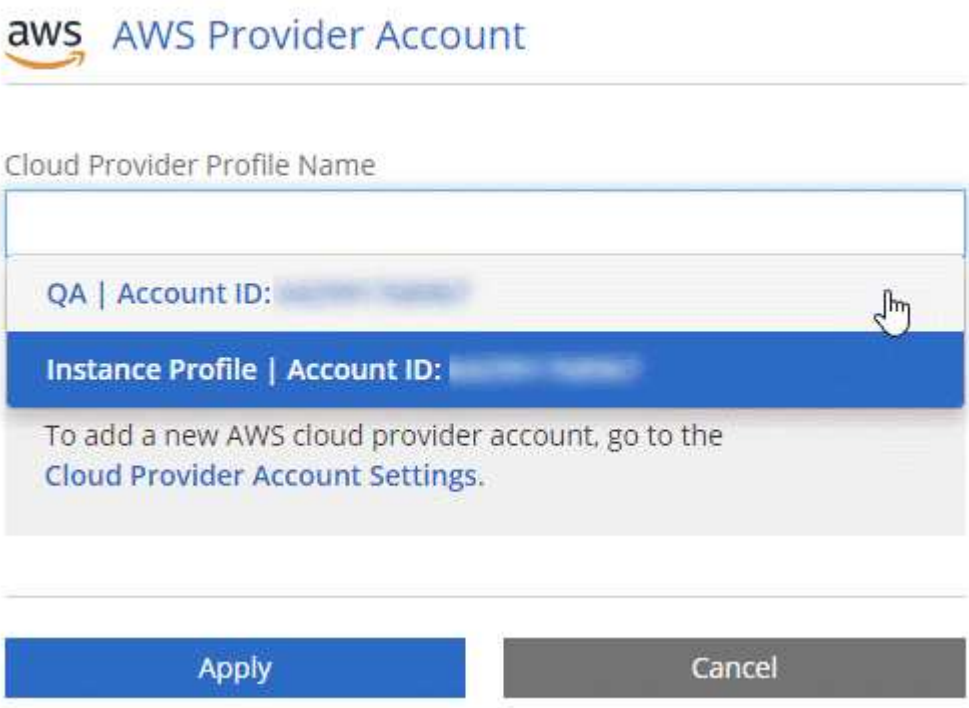
Autres comptes AWS

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 comptes des fournisseurs de services clouds 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 compte, vous pouvez le basculer 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 de NetApp Cloud Central. Vous pouvez également déployer Cloud Manager dans AWS à partir du "AWS Marketplace" et vous le pouvez "Installez Cloud Manager 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.

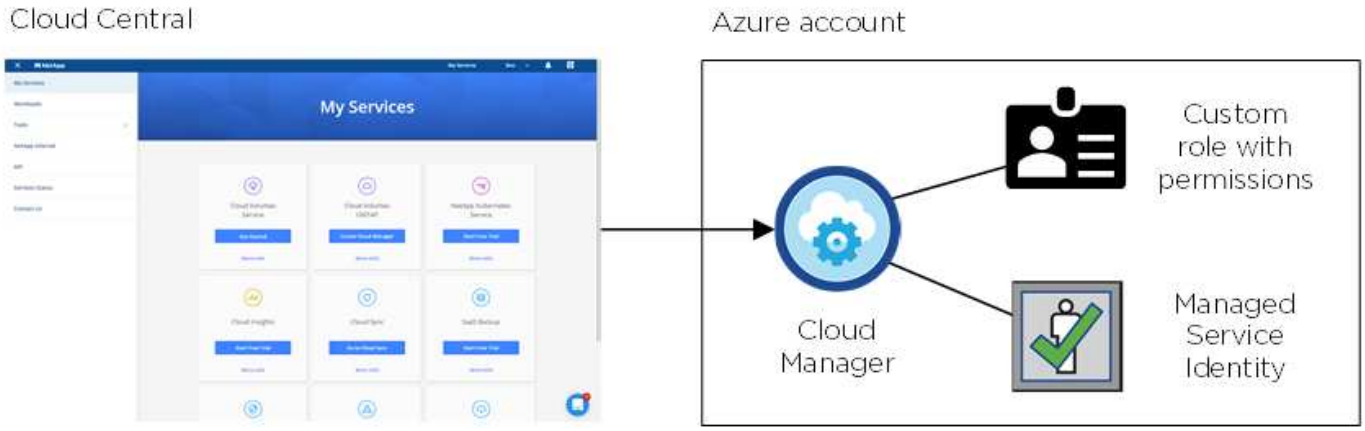
Comptes et autorisations Azure

Cloud Manager vous permet de choisir le compte Azure dans lequel vous souhaitez déployer un système Cloud Volumes ONTAP. Vous pouvez déployer tous les systèmes Cloud Volumes ONTAP sur le compte Azure initial, ou configurer d'autres comptes.

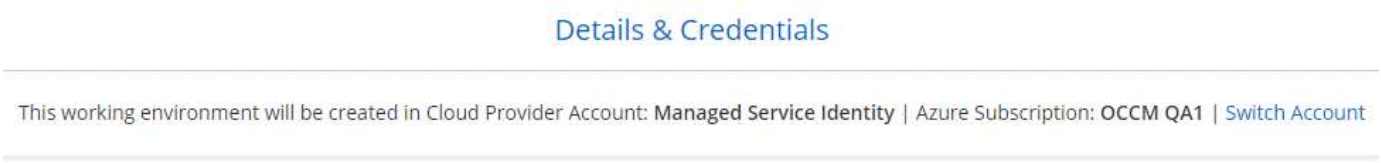
Compte Azure initial

Lorsque vous déployez Cloud Manager à partir de NetApp Cloud Central, vous devez utiliser un compte Azure disposant des autorisations nécessaires pour déployer la machine virtuelle Cloud Manager. Les autorisations requises sont répertoriées dans le "Politique NetApp Cloud Central pour Azure".

Lorsque Cloud Central déploie la machine virtuelle Cloud Manager dans Azure, il active une "identité gérée attribuée par le système" Sur la machine virtuelle Cloud Manager, crée un rôle personnalisé et le attribue à la machine virtuelle. Le rôle fournit à Cloud Manager les autorisations de déploiement et de gestion de Cloud Volumes ONTAP dans cet abonnement Azure. "Examinez comment Cloud Manager utilise les autorisations".



Cloud Manager sélectionne par défaut ce compte de fournisseur cloud lors de la création d'un nouvel environnement de travail :

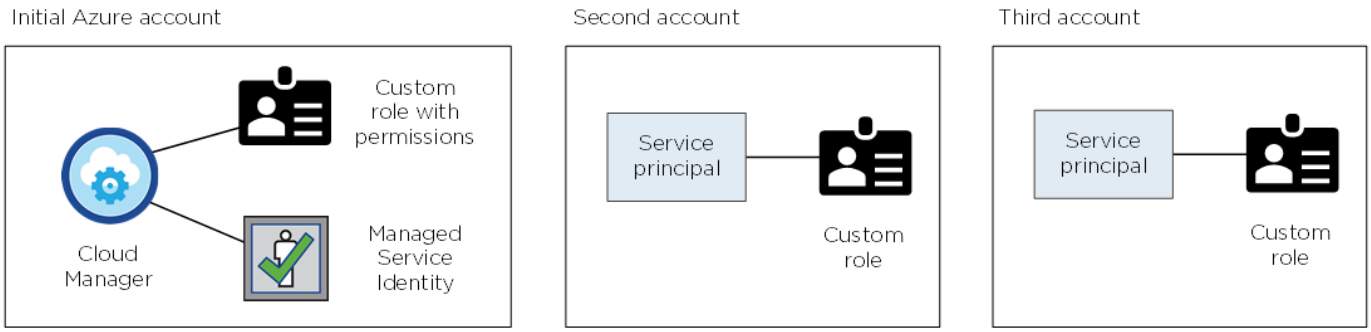


Abonnements Azure supplémentaires pour le compte initial

L'identité gérée est associée à l'abonnement dans lequel vous avez lancé Cloud Manager. Si vous souhaitez sélectionner un autre abonnement Azure, vous devez le faire "associez l'identité gérée à ces abonnements".

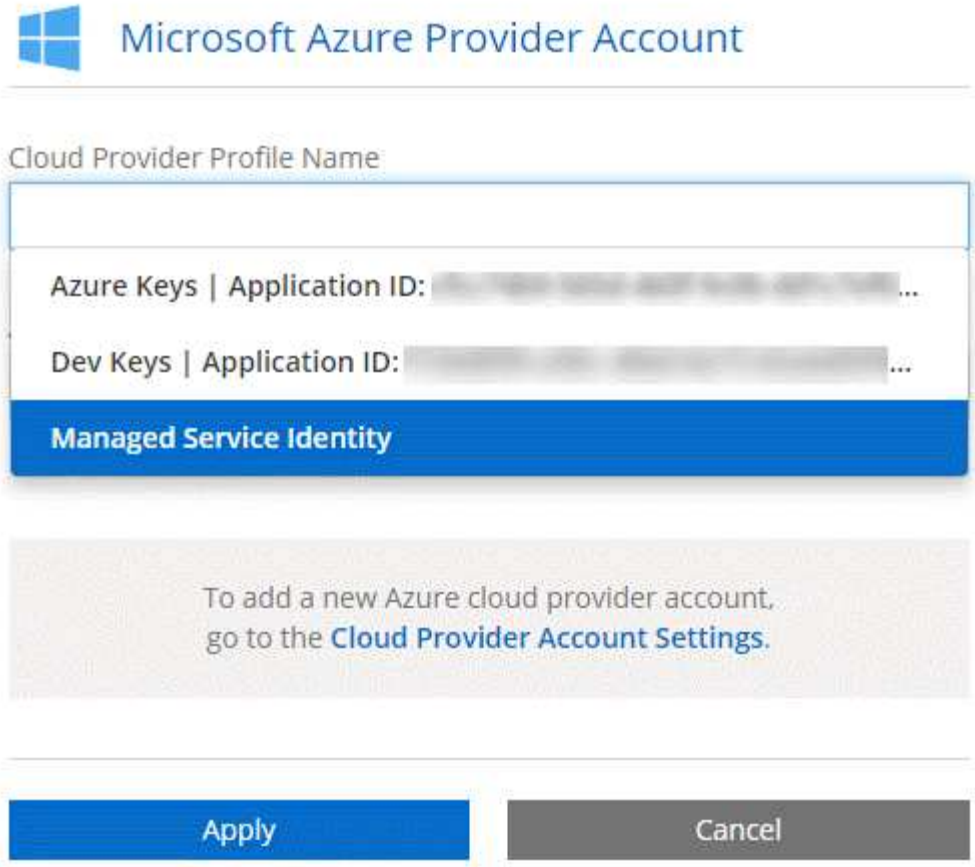
Autres comptes Azure

Si vous souhaitez déployer Cloud Volumes ONTAP sur différents comptes 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 comptes des fournisseurs de services clouds à Cloud Manager" En fournissant des détails sur le principal du service AD.

Après avoir ajouté un autre compte, vous pouvez le basculer 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 de NetApp Cloud Central. Vous pouvez également déployer Cloud Manager dans Azure à partir du "Azure Marketplace", et vous pouvez "Installez Cloud Manager 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 Cloud Manager, puis de fournir des autorisations pour tous les comptes supplémentaires.

Pour les déploiements sur site, vous ne pouvez pas configurer d'identité gérée pour le système Cloud Manager, mais vous pouvez fournir des autorisations comme vous le feriez pour des comptes supplémentaires.

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. Les comptes Google Cloud que vous ajoutez à Cloud Manager permettent le Tiering des données.

Projet et autorisations pour Cloud Manager

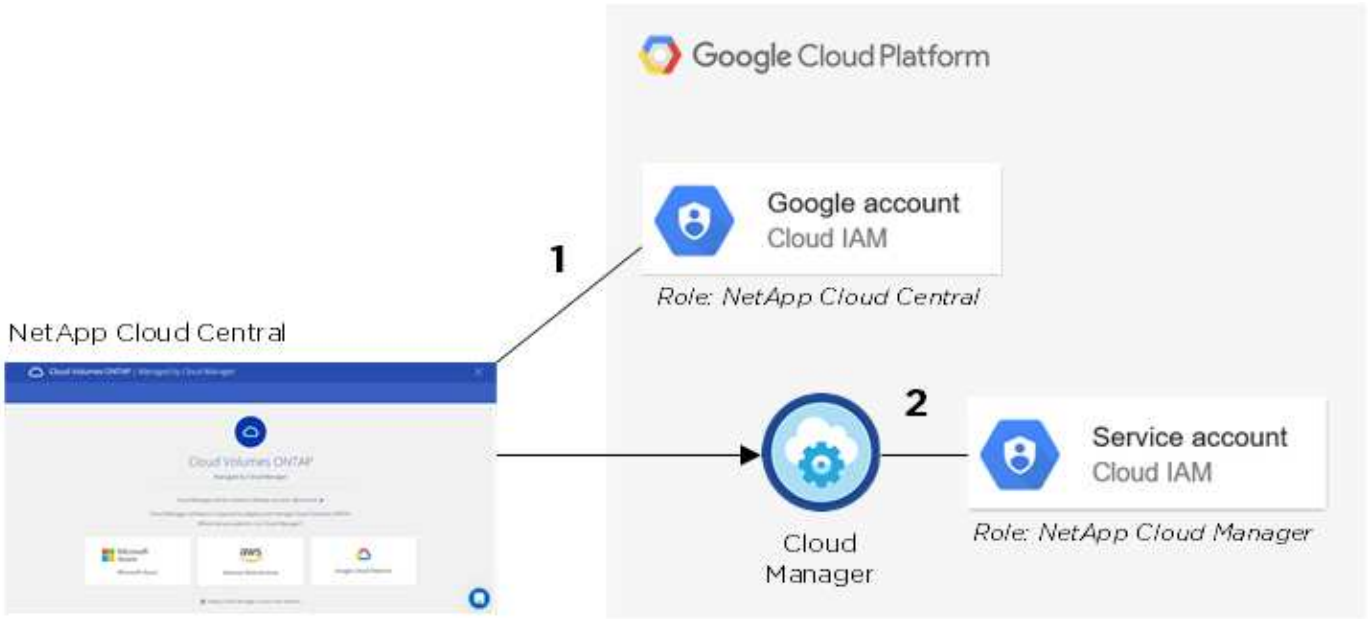
Avant de déployer Cloud Volumes ONTAP dans Google Cloud, vous devez d'abord déployer Cloud Manager dans un projet Google Cloud. Cloud Manager ne peut pas s'exécuter sur site ou dans un autre fournisseur cloud.

Deux ensembles d'autorisations doivent être en place avant de déployer Cloud Manager à partir de "NetApp Cloud Central":

1. Vous devez déployer Cloud Manager à l'aide d'un compte Google disposant d'autorisations pour lancer l'instance de machine virtuelle Cloud Manager à partir de Cloud Central.
2. Lorsque vous déployez Cloud Manager, 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 Cloud Manager ou dans un autre projet. Pour déployer Cloud Volumes ONTAP dans un autre projet, vous devez d'abord ajouter le compte de service Cloud Manager et son rôle.

- "Découvrez comment configurer un compte de service Cloud Manager (voir étape 4)".
- "Découvrez comment déployer Cloud Volumes ONTAP dans GCP et sélectionner un projet".

Compte tenu du Tiering des données

L'ajout d'un compte Google Cloud à Cloud Manager permet le Tiering des données sur un système Cloud Volumes ONTAP. 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".

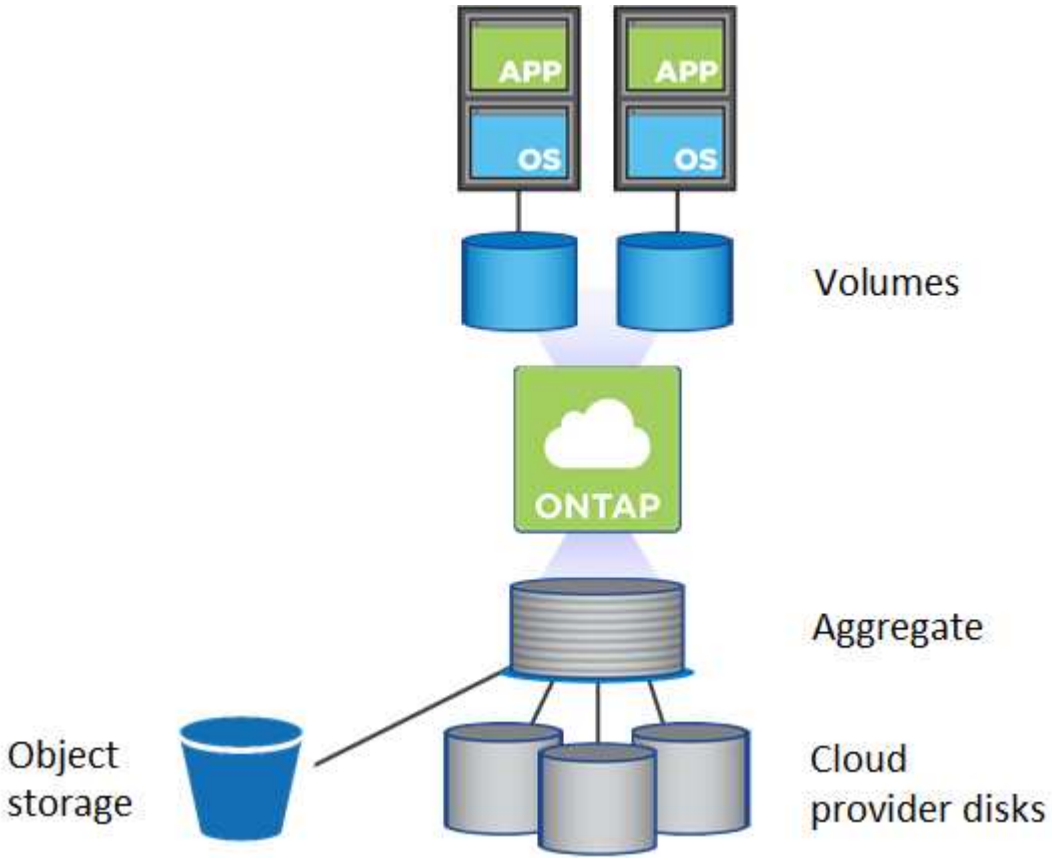
Stockage

Disques et agrégats

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

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"

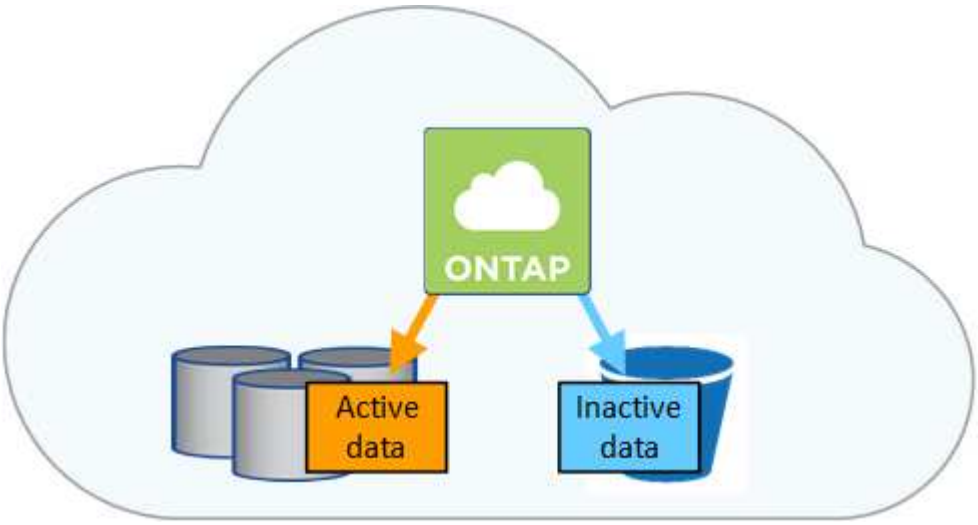
Type de RAID

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.

Vous n'avez pas besoin d'installer de 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. En cas de modification du niveau de Tiering d'un système, vous choisissez une autre classe de stockage S3.

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.

Niveaux de Tiering

Si vous ne prévoyez pas d'accéder aux données inactives, vous pouvez réduire vos coûts de stockage en changeant le niveau de hiérarchisation d'un système à l'une des options suivantes : *Intelligent Tiering*, *One-zone Infrequent Access* ou *Standard-Infrequent Access*. Lorsque vous modifiez le niveau de Tiering, les données inactives commencent dans la classe de stockage Standard et sont déplacées 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 en considération avant de changer le niveau de Tiering. "En savoir plus sur les classes de stockage Amazon S3".

La modification du niveau de hiérarchisation est possible après la création du système. Pour plus de

détails, voir "Tiering des données inactives vers un stockage objet à faible coût".

Le niveau de Tiering s'applique à l'ensemble du système --il ne s'agit pas d'un 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. En modifiant le niveau de Tiering d'un système, vous choisissez un Tier de stockage Azure différent.

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.

Niveaux de Tiering

Si vous ne prévoyez pas d'accéder aux données inactives, vous pouvez réduire vos coûts de stockage en modifiant le niveau de Tiering d'un système vers le niveau de stockage Azure *cool*. Lorsque vous modifiez le niveau de Tiering, les données inactives commencent dans le Tier de stockage à chaud et sont déplacées vers le Tier de stockage froid, si les données ne sont pas accessibles après 30 jours.

Les coûts d'accès sont plus élevés si vous accédez aux données. Prenez donc en considération avant de changer le niveau de Tiering. "En savoir plus sur les tiers d'accès au stockage Azure Blob".

La modification du niveau de hiérarchisation est possible après la création du système. Pour plus de détails, voir "Tiering des données inactives vers un stockage objet à faible coût".

Le niveau de Tiering s'applique à l'ensemble du système --il ne s'agit pas d'un 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.

Niveaux de Tiering

Aucune autre classe de stockage GCP n'est actuellement prise en charge.

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.

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 retourné à AWS ou Azure dans ce scénario.

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

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.

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.

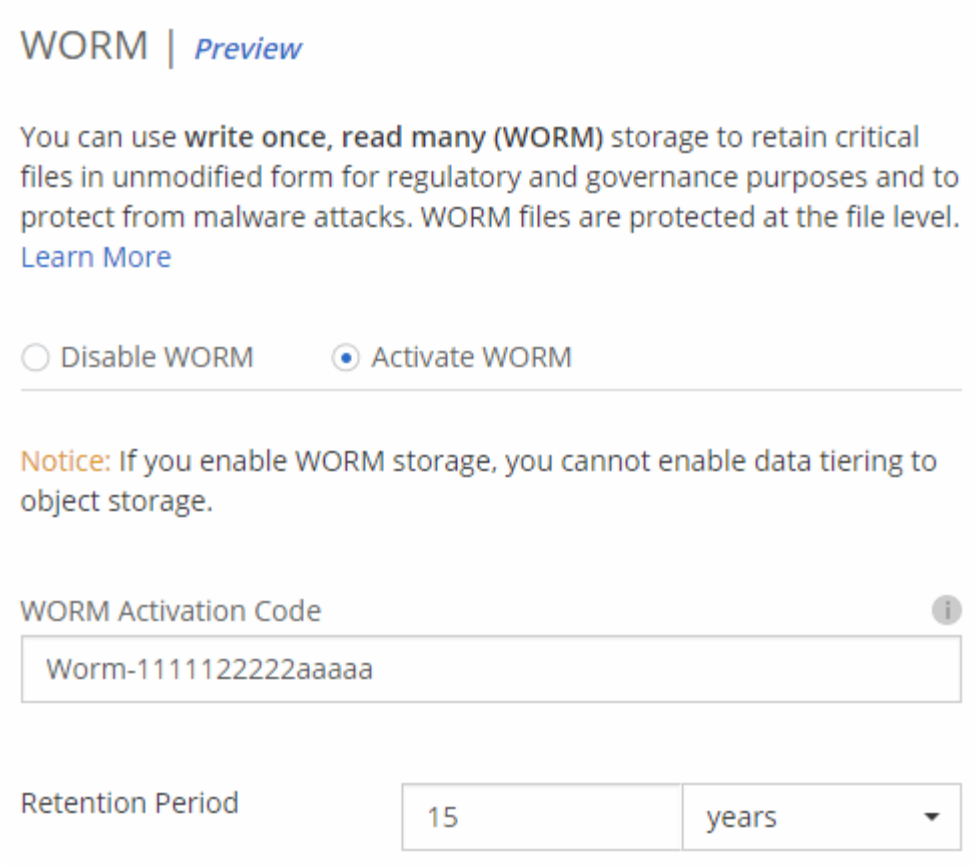
Une fois la période de conservation écoulée, vous êtes responsable de la suppression des fichiers dont vous n'avez plus besoin.

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, la hiérarchisation des données vers le stockage objet ne peut pas être activée.

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.

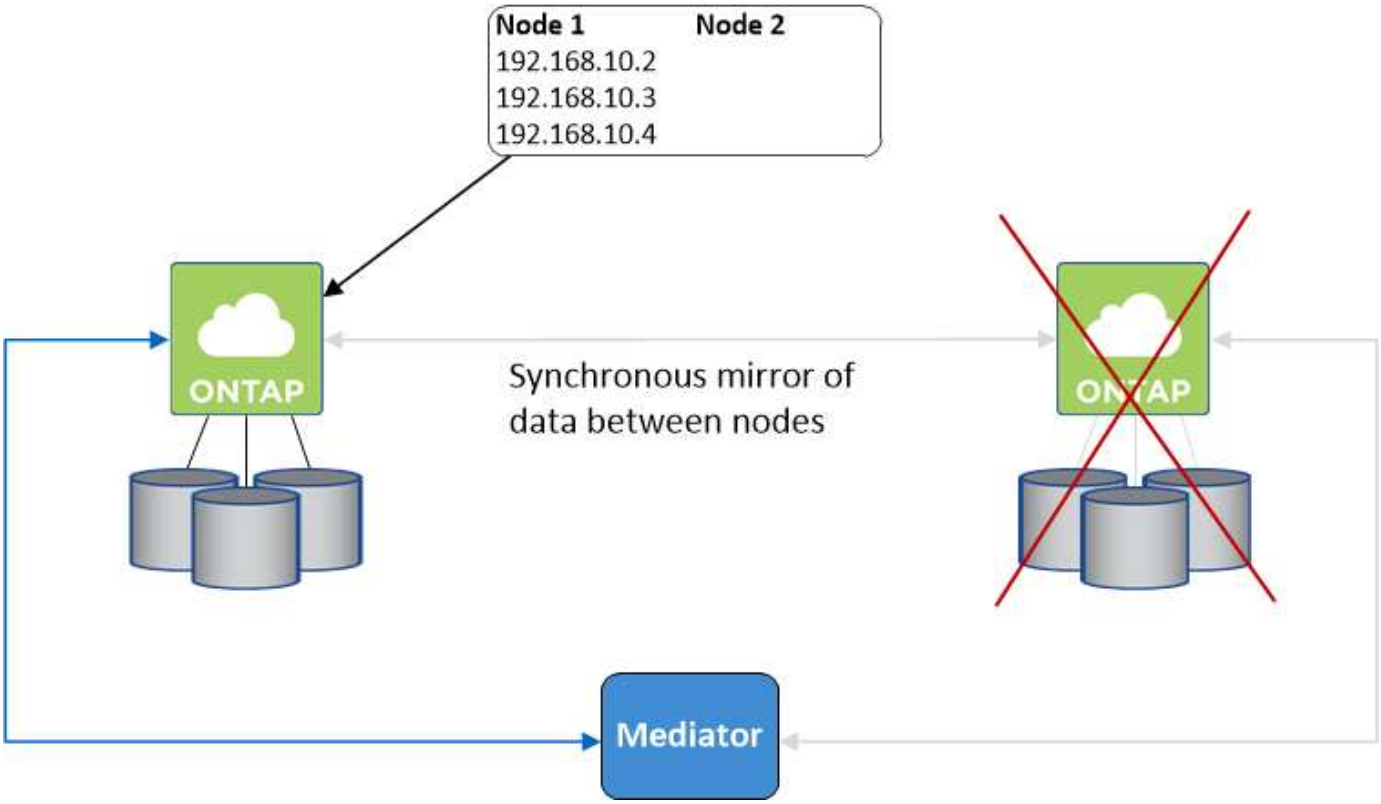
Reprise et remise du stockage pour iSCSI

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

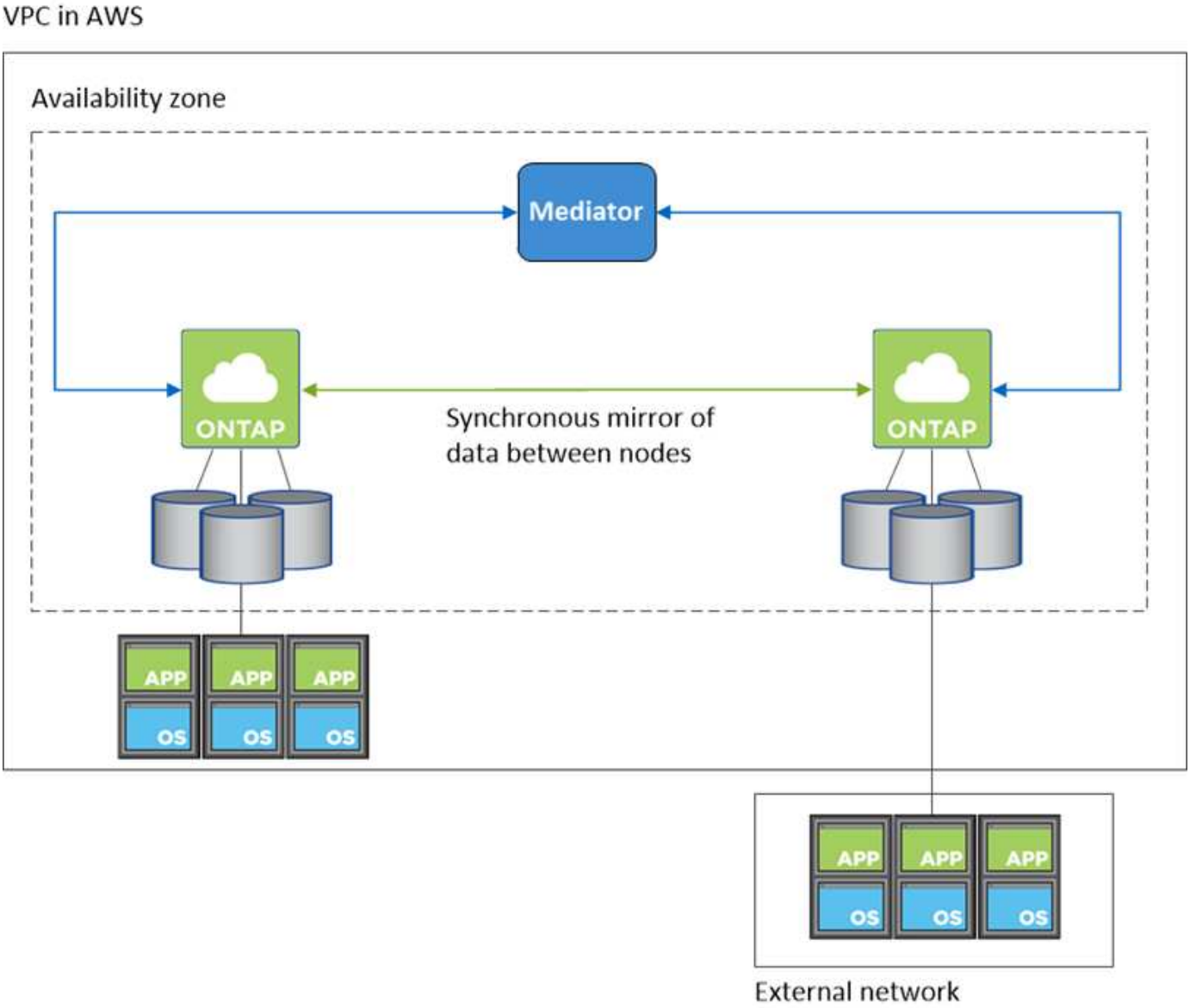
Le déploiement d'une configuration HA dans une seule zone de disponibilité (AZ) peut garantir une haute disponibilité de vos données en cas de défaillance d'une instance exécutant un nœud Cloud Volumes ONTAP. Toutes les données sont accessibles en mode natif depuis l'extérieur du VPC.

> 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.

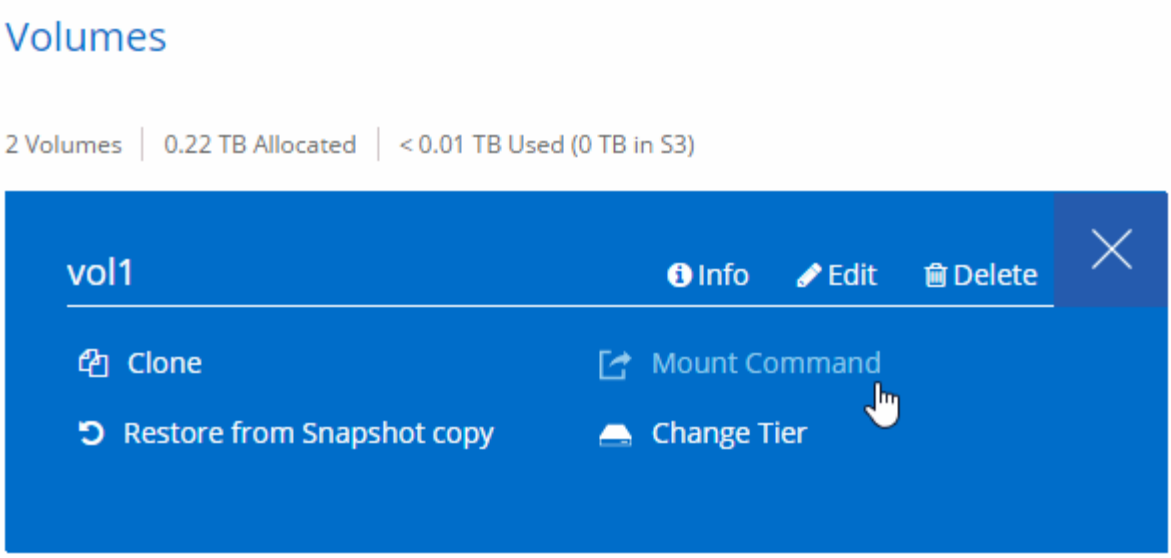
Pour plus d'informations sur les performances de Cloud Volumes ONTAP, reportez-vous à "Performance".

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 :

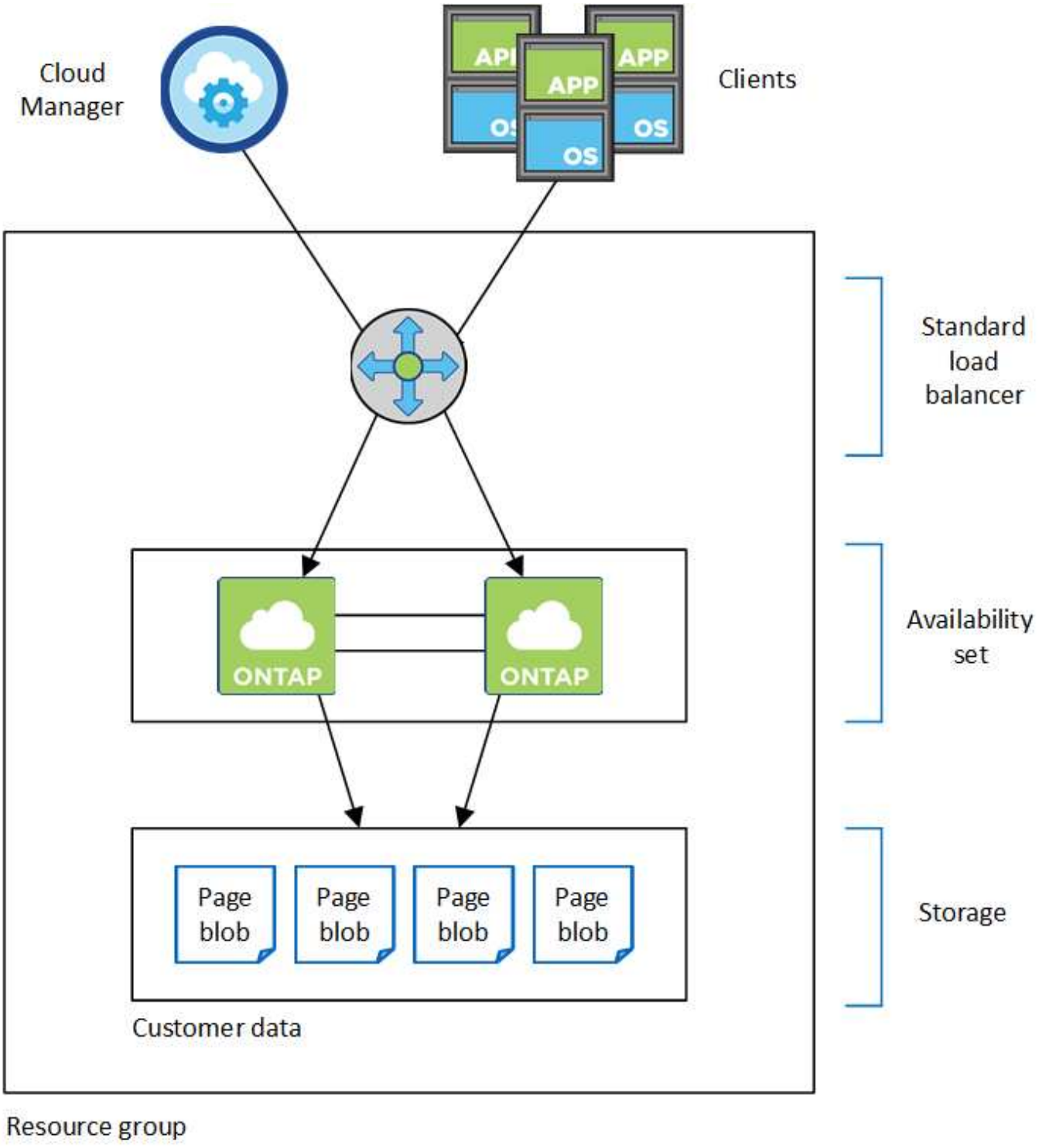


Paires haute disponibilité dans Azure

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. Un stockage supplémentaire est également nécessaire pour les données de démarrage, root et core :

- Deux disques SSD premium de 90 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 128 Go pour économiser les cœurs (un par nœud)

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.

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.

Une version d'essai gratuite de 30 jours est disponible sur un système Cloud Volumes ONTAP à un seul nœud "NetApp Cloud Central". Il n'y a pas de frais logiciels à l'heure, mais des frais d'infrastructure s'appliquent toujours. Un essai gratuit est automatiquement converti en abonnement horaire payé à la date d'expiration.

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.

Licences

Chaque système Cloud Volumes ONTAP BYOL doit disposer d'une licence installée avec un abonnement actif. Si aucune licence active n'est installée, le système Cloud Volumes ONTAP s'arrête après 30 jours. Cloud Manager simplifie le processus en gérant les licences pour vous et en vous informant avant leur expiration.

Gestion des licences pour un nouveau système

Lorsque vous créez un système BYOL, Cloud Manager vous invite à créer un 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 télécharger manuellement dans Cloud Manager. Pour obtenir des instructions, reportez-vous à la section "Installation de fichiers de licence sur les systèmes Cloud Volumes ONTAP BYOL".

Expiration de la 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 télécharger manuellement dans Cloud Manager. Pour obtenir des instructions, reportez-vous à la section "Installation de fichiers de licence sur les systèmes Cloud Volumes ONTAP BYOL".

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 :

- Chiffrement de volume NetApp (à partir de Cloud Volumes ONTAP 9.5)
- Service de gestion des clés AWS
- Chiffrement de service de stockage Azure
- Chiffrement par défaut Google Cloud Platform

Vous pouvez utiliser NetApp Volume Encryption avec le chiffrement natif AWS, Azure ou GCP, qui chiffre les données au niveau de l'hyperviseur.

NetApp Volume Encryption

NetApp Volume Encryption (NVE) est une technologie logicielle de chiffrement des données au repos d'un volume à la fois. Les données, les copies Snapshot et les métadonnées sont chiffrées. L'accès aux données est donné par une clé XTS-AES-256 unique, une par volume.

Cloud Volumes ONTAP prend en charge NetApp Volume Encryption avec un serveur de gestion externe des clés. Un gestionnaire de clés intégré n'est pas pris en charge. Vous trouverez les gestionnaires de clés pris en charge dans le "Matrice d'interopérabilité NetApp" Sous la solution **gestionnaires de clés**.

Vous pouvez activer NetApp Volume Encryption sur un volume nouveau ou existant à l'aide de l'interface de ligne de commande ou de System Manager. Cloud Manager ne prend pas en charge NetApp Volume Encryption. Pour obtenir des instructions, reportez-vous à la section "Chiffrement de volumes avec NetApp Volume Encryption".

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.

Les clés gérées par les clients ne sont pas prises en charge avec 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.

Reportez-vous à la "Guide du développeur API" Pour plus d'informations sur l'utilisation des paramètres « GcpEncryption ».

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".

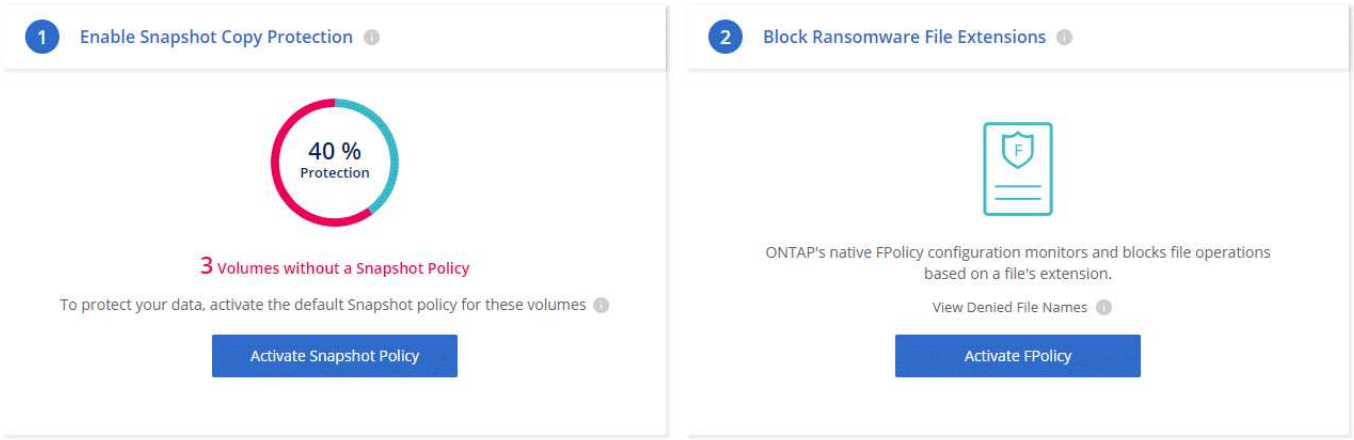
Protection par ransomware

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.

Pour plus d'informations sur Cloud Volumes ONTAP pour AWS, reportez-vous à "Rapport technique NetApp 4383 : caractérisation des performances de Cloud Volumes ONTAP dans Amazon Web Services avec des charges de travail applicatives".

Pour plus d'informations sur Cloud Volumes ONTAP pour Microsoft Azure, reportez-vous à "Rapport technique NetApp 4671 : caractérisation des performances de Cloud Volumes ONTAP dans Azure avec les charges de travail applicatives".

Commencez

Présentation du déploiement

Avant de commencer, vous voudrez peut-être mieux comprendre les options de déploiement de Cloud Manager et de Cloud Volumes ONTAP.

Installation de Cloud Manager

Le logiciel Cloud Manager est requis pour déployer et gérer Cloud Volumes ONTAP. Vous pouvez déployer Cloud Manager dans l'un des emplacements suivants :

- Services Web Amazon (AWS)
- Microsoft Azure
- Google Cloud Platform

  Cloud Manager doit être déployé dans Google Cloud Platform dans Cloud Volumes ONTAP dans GCP.

- Cloud IBM
- Dans votre propre réseau

Le mode de déploiement de Cloud Manager dépend de l'emplacement que vous choisissez :

Emplacement de Cloud Manager	Comment déployer Cloud Manager
AWS	1. "Déployez Cloud Manager à partir de NetApp Cloud Central" (recommandé) 2. "Déploiement depuis AWS Marketplace" 3. "Téléchargez et installez le logiciel sur un hôte Linux"
AWS C2S	"Déployez Cloud Manager depuis le Marketplace de la communauté AWS Intelligence"
Azure région disponible actuellement	1. "Déployez Cloud Manager à partir de NetApp Cloud Central" (recommandé) 2. "Déploiement depuis Azure Marketplace" 3. "Téléchargez et installez le logiciel sur un hôte Linux"
Gouvernement Azure	"Déployez Cloud Manager depuis Azure Government Marketplace"
Azure Allemagne	"Téléchargez et installez le logiciel sur un hôte Linux"
Google Cloud Platform	1. "Déployez Cloud Manager à partir de NetApp Cloud Central" (recommandé) 2. "Téléchargez et installez le logiciel sur un hôte Linux" Vous ne pouvez pas déployer Cloud Manager dans Google Cloud à partir de GCP Marketplace

Emplacement de Cloud Manager	Comment déployer Cloud Manager
Cloud IBM	"Téléchargez et installez le logiciel sur un hôte Linux"
Réseau sur site	"Téléchargez et installez le logiciel sur un hôte Linux"

Configuration de Cloud Manager

Une fois que vous avez installé Cloud Manager, vous pouvez effectuer des configurations supplémentaires, comme l'ajout de comptes de fournisseur de cloud supplémentaires, l'installation d'un certificat HTTPS et bien plus encore.

- "Configurez votre compte Cloud Central"
- "Ajout de comptes AWS à Cloud Manager"
- "Ajout de comptes Azure à Cloud Manager"
- "Installation d'un certificat HTTPS"
- "Configuration du système AWS KMS"

Déploiement de Cloud Volumes ONTAP

Une fois que Cloud Manager est opérationnel, vous pouvez commencer à déployer Cloud Volumes ONTAP dans votre fournisseur cloud.

"Mise en route dans AWS", "Mise en route dans Azure", et "Mise en route dans GCP" Instructions pour une mise en service rapide de Cloud Volumes ONTAP. Pour obtenir de l'aide supplémentaire, reportez-vous aux documents suivants :

- "Configurations prises en charge pour Cloud Volumes ONTAP 9.7 dans AWS"
- "Configurations prises en charge pour Cloud Volumes ONTAP 9.7 dans Azure"
- "Configurations prises en charge pour Cloud Volumes ONTAP 9.7 dans GCP"
- "Planification de votre configuration"
- "Lancement d'Cloud Volumes ONTAP dans AWS"
- "Lancement d'Cloud Volumes ONTAP dans Azure"
- "Lancement d'Cloud Volumes ONTAP dans GCP"

Mise en route de Cloud Volumes ONTAP dans AWS

Commencez avec Cloud Volumes ONTAP en configurant AWS, puis en lançant le logiciel Cloud Manager de NetApp Cloud Central. Un essai gratuit de 30 jours est disponible pour le premier système Cloud Volumes ONTAP que vous lancez dans AWS.

Configurez votre réseau

1. Activez l'accès Internet sortant à partir du VPC cible pour que Cloud Manager et Cloud Volumes ONTAP puissent contacter plusieurs terminaux.

   Cette étape est importante car Cloud Manager ne peut pas déployer Cloud Volumes ONTAP sans accès

Internet sortant. Si vous devez limiter la connectivité sortante, reportez-vous à la liste des noeuds finaux pour "Le gestionnaire Cloud" et "Cloud Volumes ONTAP".

2. 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.

Fournissez les autorisations AWS requises

Lorsque vous déployez Cloud Manager à partir de NetApp Cloud Central, vous devez utiliser un compte AWS qui dispose des autorisations nécessaires pour déployer l'instance.

1. Accédez à la console IAM AWS et créez une règle en copiant et en collant le contenu du "Politique NetApp Cloud Central pour AWS".
2. Associez la stratégie à l'utilisateur IAM.

Abonnez-vous à partir d'AWS Marketplace

"Abonnez-vous à Cloud Manager à partir d'AWS Marketplace" Pour garantir l'absence de perturbation du service après la fin de votre essai gratuit de Cloud Volumes ONTAP. Vous serez facturé à partir de cet abonnement pour chaque système Cloud Volumes ONTAP PAYGO créé et chaque fonctionnalité d'extension activée.

Si vous lancez Cloud Volumes ONTAP avec une licence (BYOL), "Vous devez ensuite vous abonner à cette offre sur AWS Marketplace".

Lancez Cloud Manager à partir de NetApp Cloud Central

Le logiciel Cloud Manager est requis pour déployer et gérer Cloud Volumes ONTAP. Quelques minutes suffisent pour lancer une instance Cloud Manager à partir de "Cloud Central".

Lancez Cloud Volumes ONTAP à l'aide de Cloud Manager

Une fois Cloud Manager prêt, cliquez simplement sur Créer, sélectionnez le type de système que vous souhaitez lancer et suivez les étapes de l'assistant. Après 25 minutes, votre premier système Cloud Volumes ONTAP doit être opérationnel.

Regardez la vidéo suivante pour une promenade à travers ces étapes :

► https://docs.netapp.com/fr-fr/occm37//media/video_getting_started_aws.mp4 *(video)*

Liens connexes

- "L'évaluation"
- "Configuration réseau requise pour Cloud Manager"
- "Configuration réseau requise pour Cloud Volumes ONTAP dans AWS"

- "Règles de groupe de sécurité pour AWS"
- "Ajout de comptes AWS à Cloud Manager"
- "Ce que fait Cloud Manager avec les autorisations AWS"
- "Lancement d'Cloud Volumes ONTAP dans AWS"
- "Lancement de Cloud Manager à partir d'AWS Marketplace"

Mise en route de Cloud Volumes ONTAP dans Azure

Lancez-vous avec Cloud Volumes ONTAP en configurant Azure, puis en déployant le logiciel Cloud Manager depuis NetApp Cloud Central. Des instructions distinctes sont disponibles pour déployer Cloud Manager dans le "Les régions du gouvernement des États-Unis Azure" et po "Les régions Azure Germany".

Configurez votre réseau

Activez l'accès Internet sortant à partir du VNet cible pour que Cloud Manager et Cloud Volumes ONTAP puissent contacter plusieurs terminaux.

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

Fournissez les autorisations Azure requises

Lorsque vous déployez Cloud Manager à partir de NetApp Cloud Central, vous devez utiliser un compte Azure disposant des autorisations nécessaires pour déployer la machine virtuelle Cloud Manager.

1. Téléchargez le "Politique NetApp Cloud Central pour Azure".
2. Modifiez le fichier JSON en ajoutant votre ID d'abonnement Azure au champ " AssignableScopes ".
3. Utilisez le fichier JSON pour créer un rôle personnalisé dans Azure nommé *Azure SetupAsService*.

   Exemple : **az role definition create --role-definition C:\Policy_for_Setup_as_Service_Azure.json**

4. À partir du portail Azure, attribuez le rôle personnalisé à l'utilisateur qui déploiera Cloud Manager à partir de Cloud Central.

Lancez Cloud Manager à partir de NetApp Cloud Central

Le logiciel Cloud Manager est requis pour déployer et gérer Cloud Volumes ONTAP. Quelques minutes suffisent pour lancer une instance Cloud Manager à partir de "Cloud Central".

Lancez Cloud Volumes ONTAP à l'aide de Cloud Manager

Une fois Cloud Manager prêt, cliquez simplement sur Créer, sélectionnez le type de système que vous

souhaitez déployer et suivez les étapes de l'assistant. Après 25 minutes, votre premier système Cloud Volumes ONTAP doit être opérationnel.

Liens connexes

- "L'évaluation"
- "Configuration réseau requise pour Cloud Manager"
- "Configuration réseau requise pour Cloud Volumes ONTAP dans Azure"
- "Règles de groupe de sécurité pour Azure"
- "Ajout de comptes Azure à Cloud Manager"
- "Ce que fait Cloud Manager avec les autorisations Azure"
- "Lancement d'Cloud Volumes ONTAP dans Azure"
- "Lancement de Cloud Manager à partir d'Azure Marketplace"

Mise en route de Cloud Volumes ONTAP dans Google Cloud Platform

Lancez-vous avec Cloud Volumes ONTAP en configurant GCP, puis en déployant le logiciel Cloud Manager de NetApp Cloud Central.

Cloud Manager doit être installé dans Google Cloud Platform afin de déployer Cloud Volumes ONTAP dans GCP.

Configurez votre réseau

Activez l'accès Internet sortant à partir du VPC cible pour que Cloud Manager et Cloud Volumes ONTAP puissent contacter plusieurs terminaux.

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

Configurez les autorisations et les projets GCP

Assurez-vous que deux ensembles d'autorisations sont en place :

1. Assurez-vous que l'utilisateur GCP qui déploie Cloud Manager à partir de NetApp Cloud Central dispose des autorisations dans le "Règle Cloud Central 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 de Cloud Manager à l'étape 6.

- "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.

- "Créez un compte de service GCP et appliquez le rôle personnalisé que vous venez de créer".
- 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 de GCP pour le Tiering des données

Deux exigences doivent être remplies pour déplacer les données inactives d'Cloud Volumes ONTAP 9.7 vers le stockage objet à faible coût (un compartiment Google Cloud Storage) :

1. "Créez un compte de service" Avec le rôle d'administrateur de stockage prédéfini et le compte de service Cloud Manager en tant qu'utilisateur.

   Vous devrez sélectionner ce compte de service ultérieurement lors de la création d'un environnement de travail Cloud Volumes ONTAP. Ce compte de service est différent du compte de service que vous avez créé à l'étape 2.

2. "Configurez le sous-réseau Cloud Volumes ONTAP pour un accès privé à Google".

Si vous souhaitez utiliser le Tiering des données avec Cloud Volumes ONTAP 9.6, "ensuite procédez comme suit".

Activez les API Google Cloud

"Activez les API Google Cloud suivantes dans votre projet". Ces API sont nécessaires pour déployer Cloud Manager et Cloud Volumes ONTAP.

- API Cloud Deployment Manager V2
- API Cloud Resource Manager
- API du moteur de calcul
- API de consignation Stackdriver

Abonnez-vous à GCP Marketplace

"Abonnez-vous à Cloud Volumes ONTAP à partir de GCP Marketplace" pour garantir l'absence de perturbation du service après la fin de votre essai gratuit. Vous serez facturé à partir de cet abonnement pour chaque système PAYGO Cloud Volumes ONTAP que vous créez.

Lancez Cloud Manager à partir de NetApp Cloud Central

Le logiciel Cloud Manager est requis pour déployer et gérer Cloud Volumes ONTAP. Quelques minutes

suffisent pour lancer une instance Cloud Manager dans GCP à partir de "Cloud Central".

Lorsque vous choisissez GCP comme fournisseur cloud, Google vous invite à vous connecter à votre compte et à accorder des autorisations. Lorsque vous cliquez sur « Autoriser », l'accès aux API de calcul requises pour déployer Cloud Manager est accordé.

Lancez Cloud Volumes ONTAP à l'aide de Cloud Manager

Une fois Cloud Manager prêt, cliquez simplement sur Créer, sélectionnez le type de système que vous souhaitez déployer et suivez les étapes de l'assistant. Après 25 minutes, votre premier système Cloud Volumes ONTAP doit être opérationnel.

Liens connexes

- "L'évaluation"
- "Configuration réseau requise pour Cloud Manager"
- "Exigences de mise en réseau pour Cloud Volumes ONTAP dans GCP"
- "Règles de pare-feu pour GCP"
- "Avantages de Cloud Manager avec les autorisations GCP"
- "Lancement d'Cloud Volumes ONTAP dans GCP"
- "Téléchargement et installation du logiciel Cloud Manager sur un hôte Linux"

Configurez Cloud Manager

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

Chaque système Cloud Manager est associé à un *compte NetApp Cloud Central*. Configurez le compte Cloud Central associé à votre système Cloud Manager pour que l'utilisateur puisse accéder à Cloud Manager et déployer des systèmes Cloud Volumes ONTAP dans ses espaces de travail. Il vous suffit d'ajouter un utilisateur ou d'ajouter plusieurs utilisateurs et espaces de travail.

Le compte est conservé dans Cloud Central. Toutes les modifications effectuées sont donc disponibles pour d'autres systèmes Cloud Manager et pour d'autres services de données cloud NetApp. "Découvrez comment fonctionnent les comptes Cloud Central".

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 aux espaces de travail.

Étapes

1. Cliquez sur **Paramètres de compte**.

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

Une fois que vous avez terminé

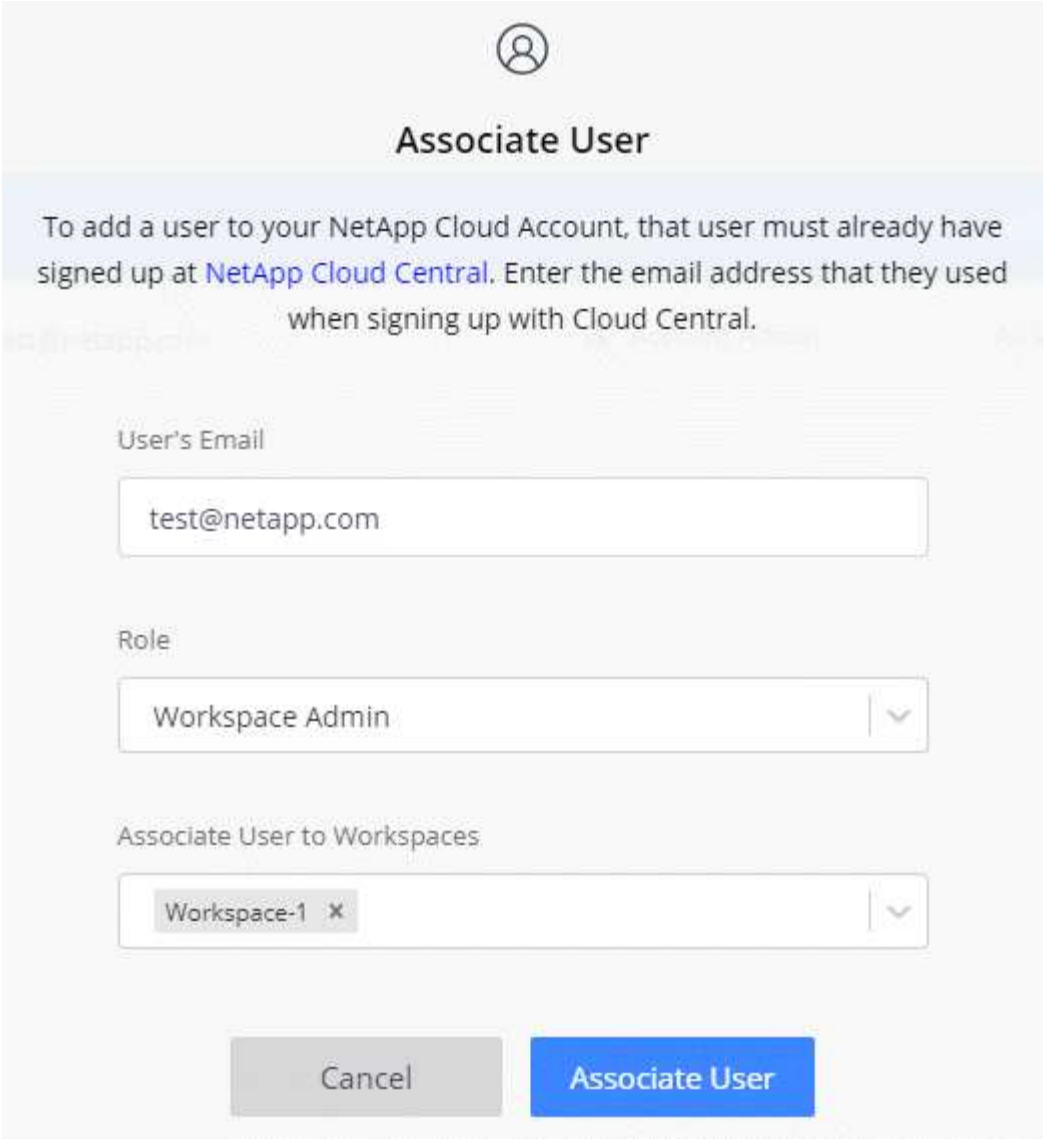
Vous pouvez désormais associer des utilisateurs et des connecteurs de service à l'espace de travail.

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 créez un compte.
2. Dans Cloud Manager, cliquez sur **Paramètres de 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.
5. Si vous avez sélectionné Workspace Admin, sélectionnez un ou plusieurs espaces de travail à associer à cet utilisateur.



6. Cliquez sur **associer utilisateur**.

Résultat

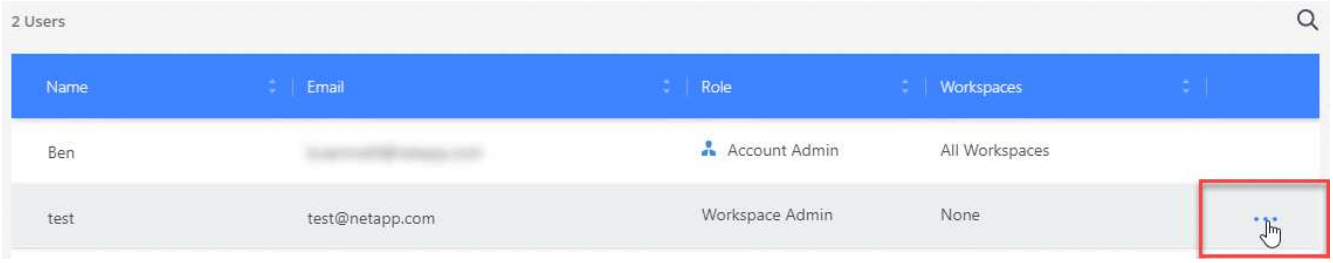
L'utilisateur doit recevoir un e-mail de la part de NetApp Cloud Central intitulé « Account Association ». Il contient les informations nécessaires pour accéder à Cloud Manager.

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. Cliquez sur **Paramètres de compte**.
2. 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

Il est désormais possible d'accéder à ces espaces de travail à partir de Cloud Manager, tant que le connecteur de service était également associé aux espaces de travail.

Association de connecteurs de service à des espaces de travail

Un connecteur de service fait partie du système Cloud Manager. Elle s'exécute sur l'instance de machine virtuelle déployée dans votre fournisseur cloud ou sur un hôte sur site que vous avez configuré. Vous devez associer ce connecteur de service 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 de service 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 de service".

Étapes

1. Cliquez sur **Paramètres de compte**.
2. Cliquez sur **Service Connector**.
3. Cliquez sur **gérer les espaces de travail** pour le connecteur de service 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 accéder aux espaces de travail associés, tant que l'utilisateur a également été associé à l'espace de travail.

Configuration et ajout de comptes AWS à Cloud Manager

Si vous souhaitez déployer Cloud Volumes ONTAP sur différents comptes AWS, vous devez fournir les autorisations requises et ajouter les informations à Cloud Manager. 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 déployez Cloud Manager depuis Cloud Central, Cloud Manager ajoute automatiquement le compte AWS dans lequel vous avez déployé Cloud Manager. Un compte initial n'est pas ajouté si vous avez installé manuellement le logiciel Cloud Manager sur un système existant. "En savoir plus sur les comptes 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

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

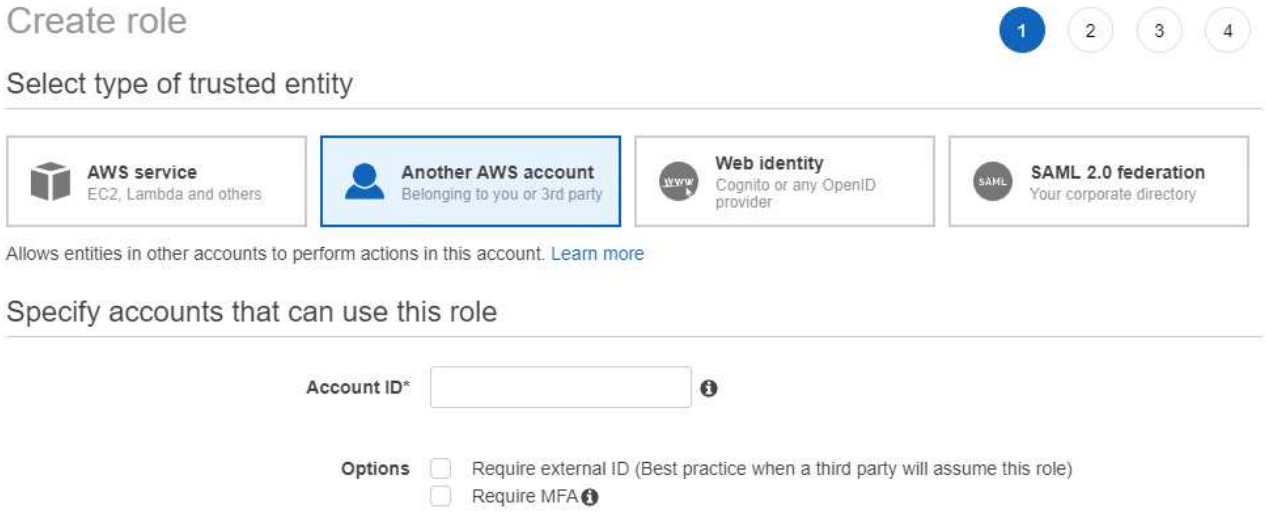
Vous pouvez définir une relation de confiance entre le compte AWS source dans lequel vous avez déployé l'instance Cloud Manager et d'autres comptes AWS en utilisant les rôles IAM. Vous pouvez ensuite fournir à Cloud Manager l'ARN des rôles IAM depuis les comptes de confiance.

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 :

   - Entrez l'ID du compte sur lequel réside l'instance Cloud Manager.
   - Joignez la politique IAM de Cloud Manager, disponible à partir du "Page Cloud Manager Policies".



2. Accédez au compte source où réside l'instance Cloud Manager et sélectionnez le rôle IAM associé à l'instance.

   a. Cliquez sur **Trust relations > Modifier la relation de confiance**.

   b. Ajoutez 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

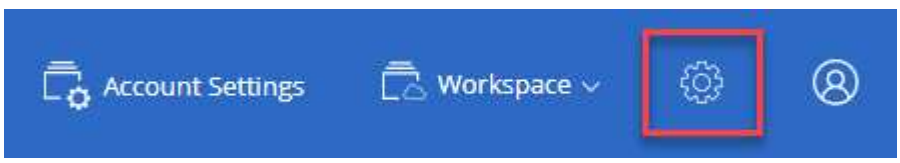
Le compte dispose désormais des autorisations requises. Vous pouvez désormais l'ajouter à Cloud Manager.

Ajout de comptes AWS à Cloud Manager

Une fois que vous avez passé un compte AWS avec les autorisations requises, vous pouvez ajouter le compte à Cloud Manager. Vous pouvez ainsi lancer les systèmes Cloud Volumes ONTAP de ce compte.

Étapes

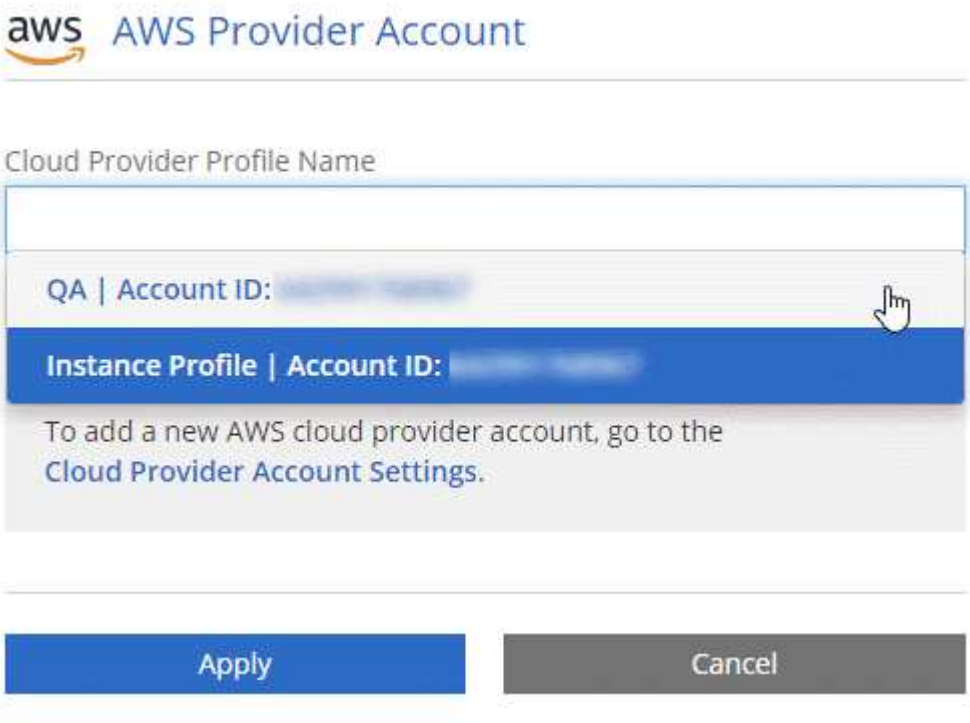
1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **Cloud Provider & support Accounts**.



2. Cliquez sur **Ajouter un nouveau compte** et sélectionnez **AWS**.
3. Indiquez si vous souhaitez fournir des clés AWS ou l'ARN d'un rôle IAM approuvé.
4. Vérifiez que les exigences de la stratégie ont été respectées, puis cliquez sur **Créer un compte**.

Résultat

Vous pouvez maintenant passer à un autre compte à partir de la page Détails et informations d'identification lors de la création d'un nouvel environnement de travail :



Configuration et ajout de comptes Azure dans Cloud Manager

Si vous souhaitez déployer Cloud Volumes ONTAP sur différents comptes Azure, vous devez fournir les autorisations requises pour ces comptes, puis ajouter des informations sur ces comptes à Cloud Manager.

Lorsque vous déployez Cloud Manager depuis Cloud Central, Cloud Manager ajoute automatiquement le compte Azure dans lequel vous avez déployé Cloud Manager. Un compte initial n'est pas ajouté si vous avez installé manuellement le logiciel Cloud Manager sur un système existant. "En savoir plus sur les comptes et les autorisations Azure".

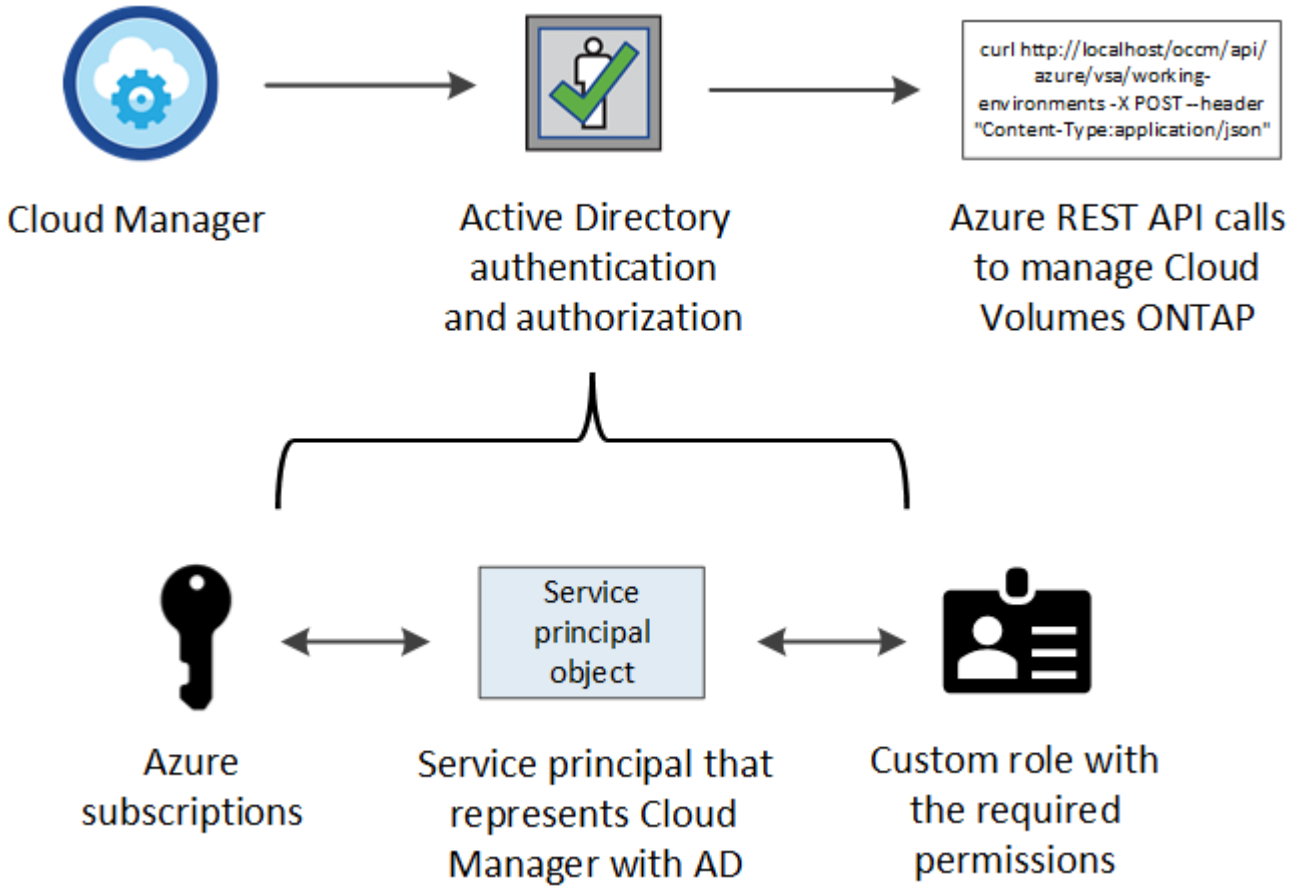
Octroi d'autorisations Azure à l'aide d'une entité de sécurité de service

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

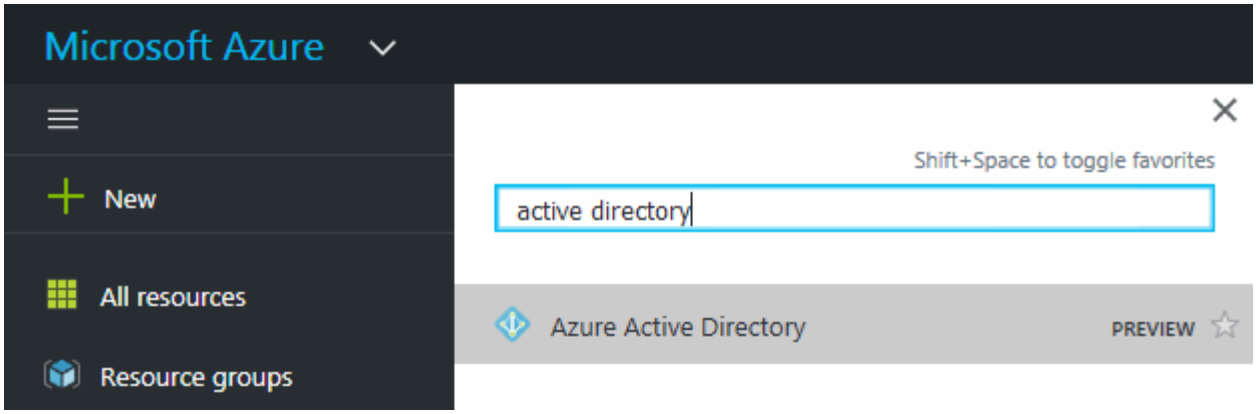
Créez une application Azure Active Directory (AD) et une entité de service que Cloud Manager peut utiliser pour le contrôle d'accès basé sur des rôles.

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 :

Définition de rôle az create --role-definition C:\Policy_for_Cloud_Manager_Azure_3.7.4.json

Vous devriez maintenant avoir un rôle personnalisé appelé *OnCommand Cloud Manager Operator*.

2. Attribuez l'application au rôle :

   a. À partir du portail Azure, ouvrez le service **abonnements**.

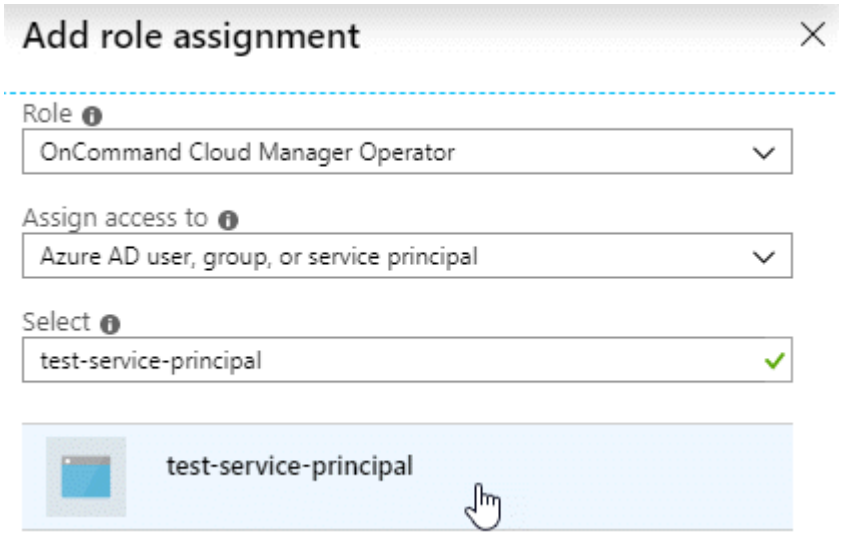
   b. Sélectionnez l'abonnement.

   c. Cliquez sur **contrôle d'accès (IAM) > Ajouter > Ajouter une affectation de rôle**.

   d. Sélectionnez le rôle **opérateur OnCommand 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.

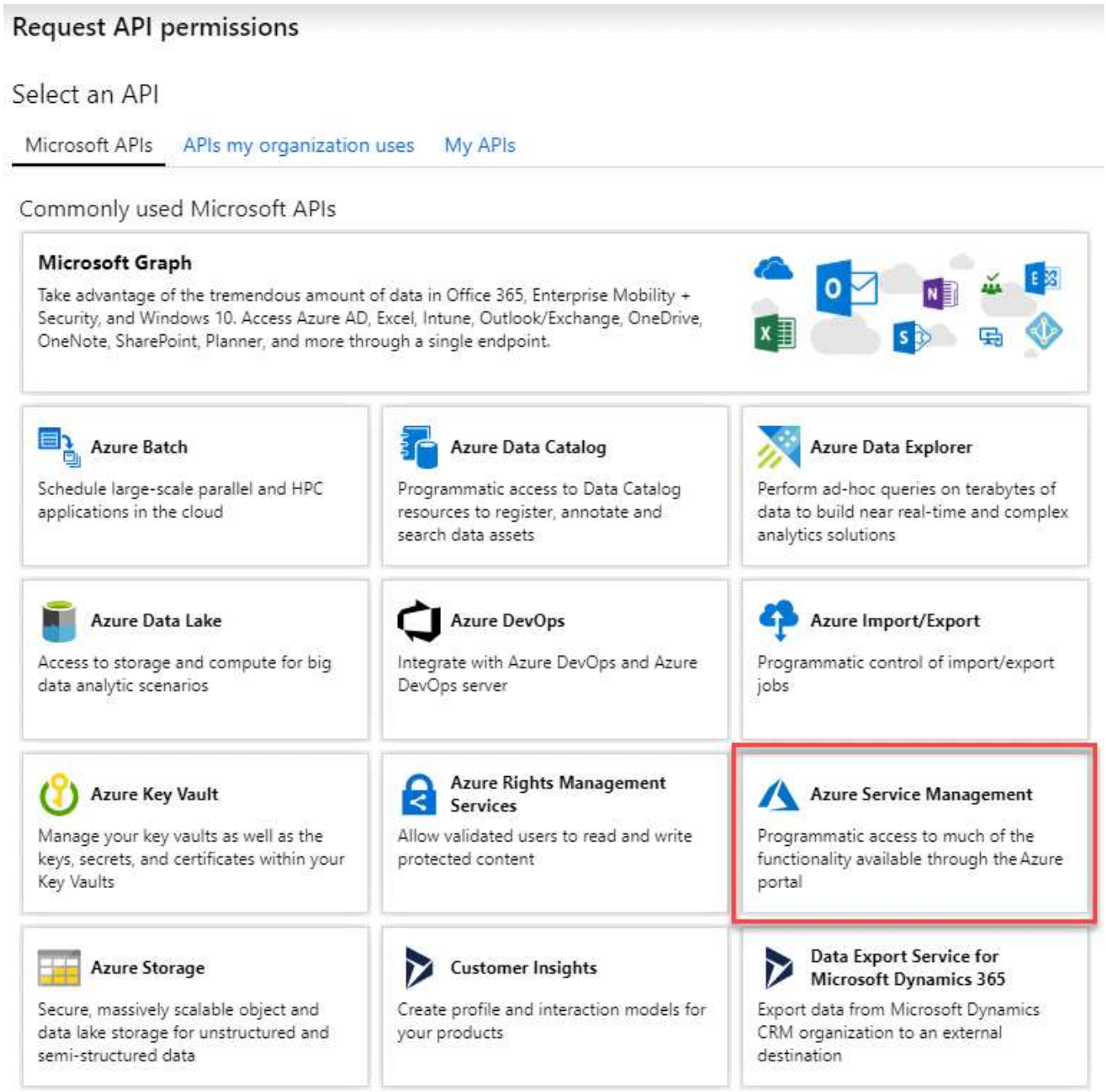
Si vous souhaitez déployer Cloud Volumes ONTAP à partir de plusieurs abonnements Azure, vous devez lier le principal de service à chacun de ces abonnements. Cloud Manager vous permet de sélectionner l'abonnement que vous souhaitez utiliser lors du déploiement de Cloud Volumes ONTAP.

Ajout d'autorisations d'API de gestion des services Windows Azure

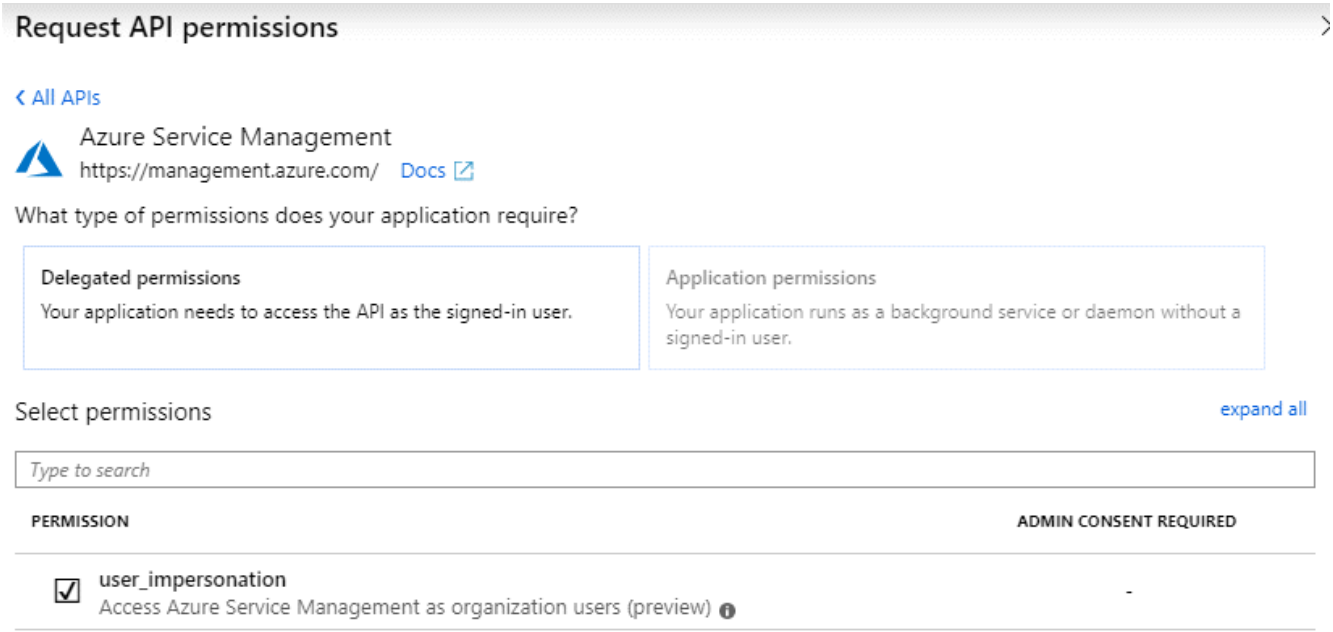
Le principal de service doit disposer d'autorisations « API de gestion des services Windows Azure ».

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**.

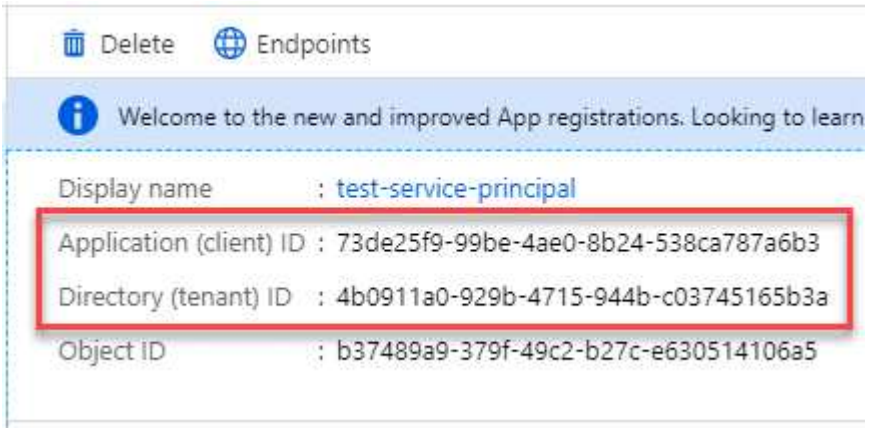


Obtention de l'ID d'application et de l'ID de répertoire

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 de comptes Azure à Cloud Manager

Une fois que vous avez autorisé à fournir un compte Azure, vous pouvez l'ajouter à Cloud Manager. Vous pouvez ainsi lancer les systèmes Cloud Volumes ONTAP de ce compte.

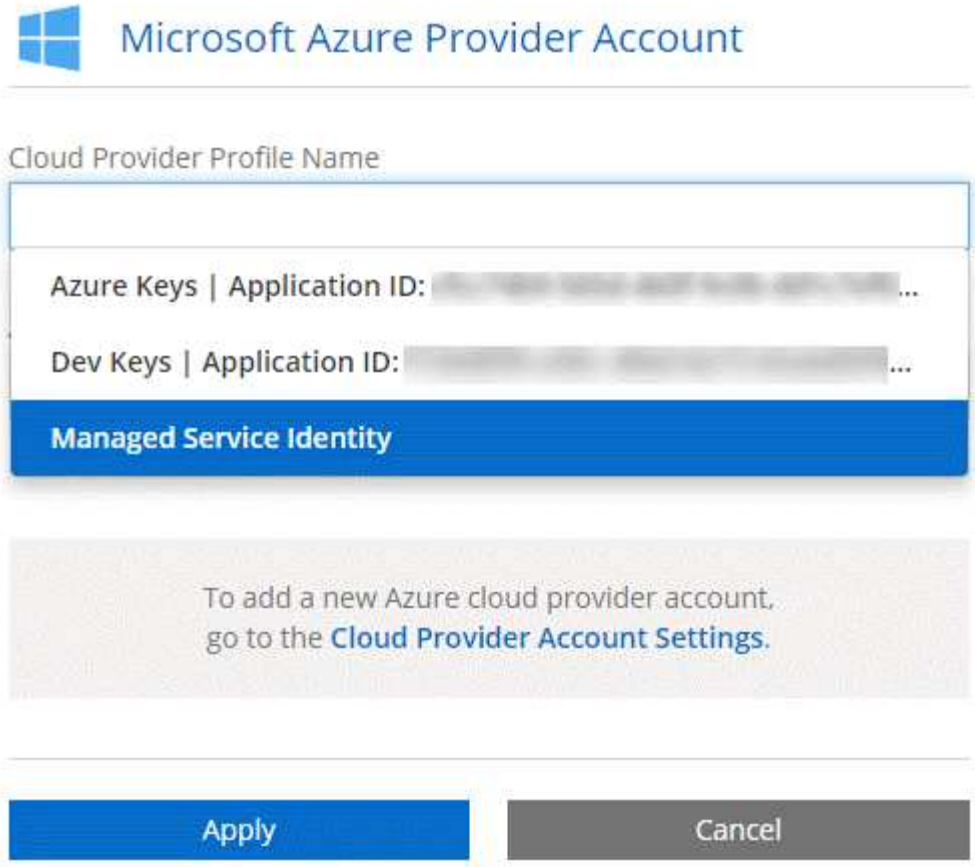
Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **Cloud Provider & support Accounts**.

2. Cliquez sur **Ajouter un nouveau compte** 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 : voir Obtention de l'ID d'application et de l'ID de répertoire.
   - ID de locataire (ou ID de répertoire) : voir Obtention de l'ID d'application et de l'ID de répertoire.
   - Clé d'application (le secret client) : voir Création d'un secret client.
4. Vérifiez que les exigences de la stratégie ont été respectées, puis cliquez sur **Créer un compte**.

Résultat

Vous pouvez maintenant passer à un autre compte à partir de la page Détails et informations d'identification lors de la création d'un nouvel environnement de travail :



Association d'abonnements Azure supplémentaires à une identité gérée

Cloud Manager vous permet de choisir le compte 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 Cloud Manager à partir de NetApp Cloud Central. Lorsque vous avez déployé Cloud Manager, Cloud Central a créé le rôle OnCommand Cloud Manager Operator et l'a affecté à la machine virtuelle Cloud Manager.

Étapes

1. Connectez-vous au portail Azure.
2. Ouvrez le service **abonnements**, puis sélectionnez l'abonnement dans lequel vous souhaitez déployer des systèmes 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 OnCommand Cloud Manager**.

        L'opérateur OnCommand 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.

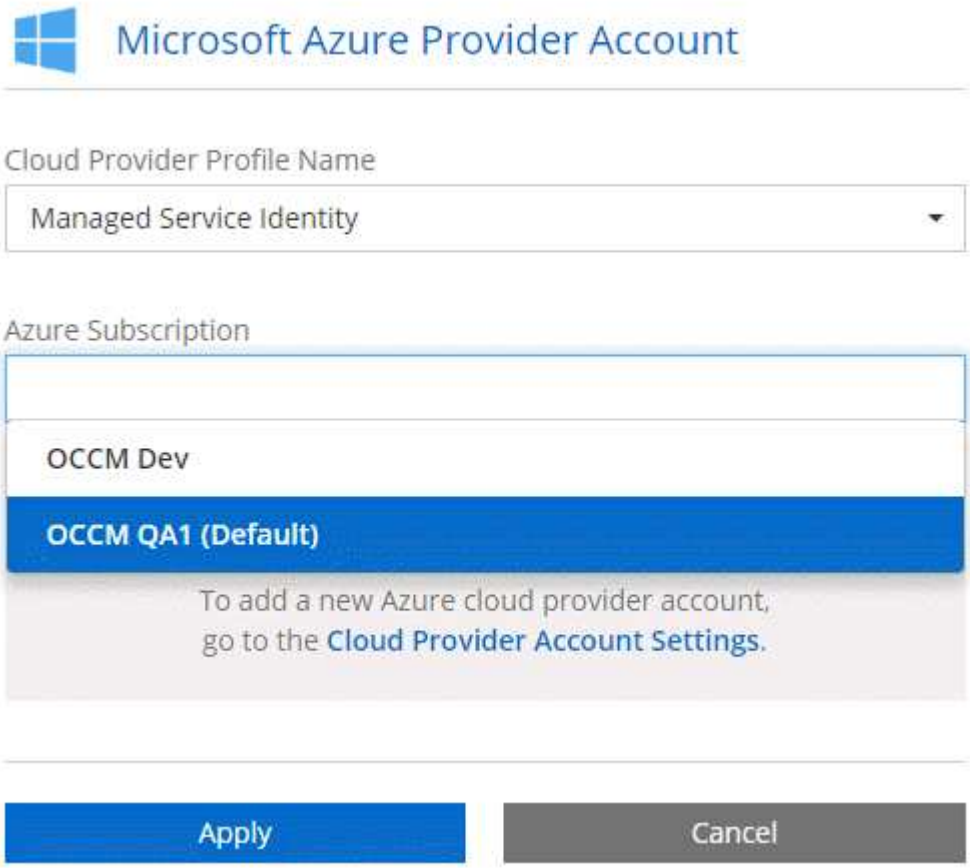
      - Attribuez l'accès à une **machine virtuelle**.

- Sélectionnez l'abonnement dans lequel la machine virtuelle Cloud Manager a été créée.
- Sélectionnez la machine virtuelle Cloud Manager.
- 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.



Configuration et ajout de comptes GCP dans Cloud Manager

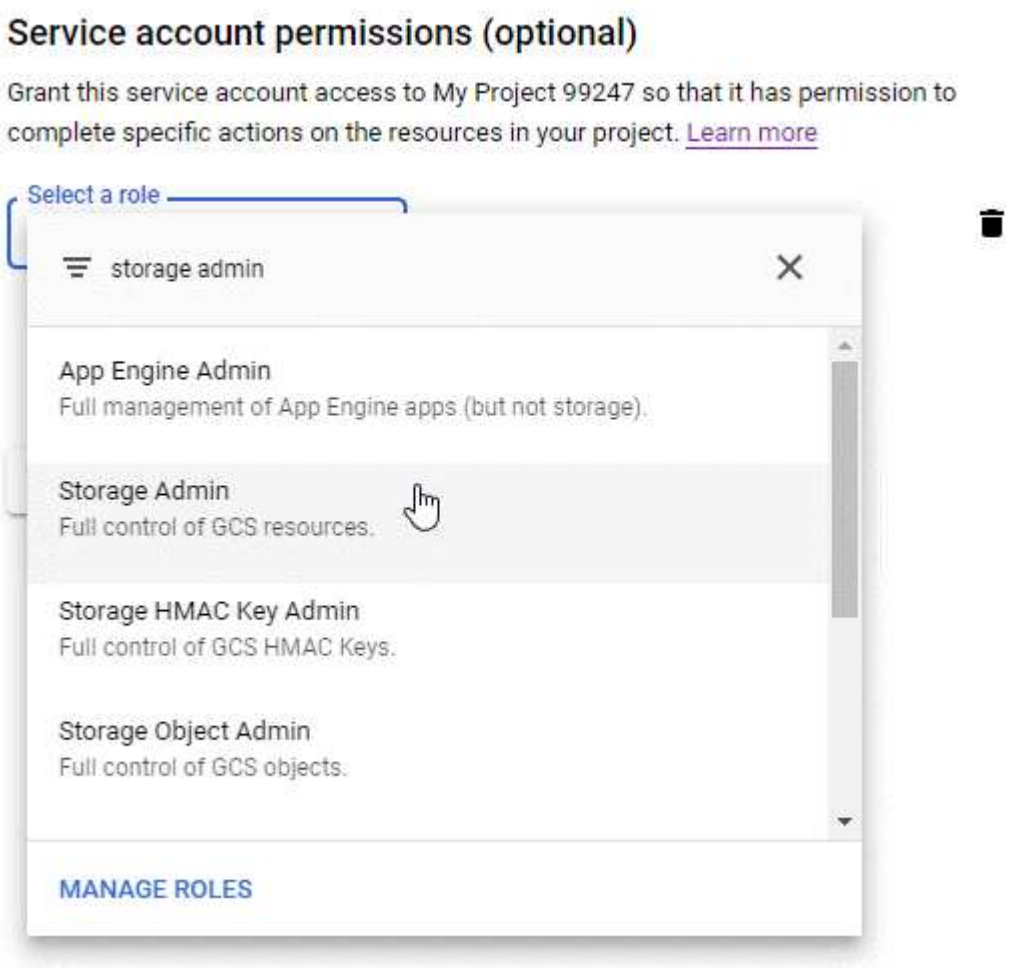
Si vous souhaitez activer "tiering des données" Sur un système Cloud Volumes ONTAP, vous devez fournir à Cloud Manager une clé d'accès de stockage pour un compte de service disposant d'autorisations d'administrateur de stockage. Cloud Manager utilise les clés d'accès pour configurer et gérer un compartiment de stockage cloud pour le Tiering des données.

Configurer un compte de service et des clés d'accès pour Google Cloud Storage

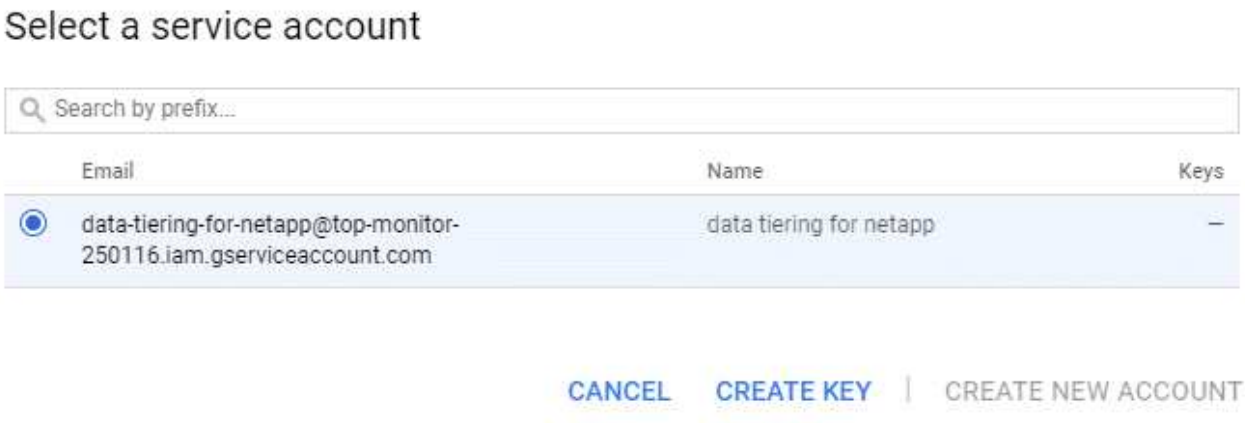
Un compte de service permet à Cloud Manager d'authentifier et d'accéder aux compartiments Cloud Storage utilisés pour le Tiering des données. Les clés sont requises pour que Google Cloud Storage sache qui effectue la demande.

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.

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **Cloud Provider & support Accounts**.

2. Cliquez sur **Ajouter un nouveau compte** et sélectionnez **GCP**.
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 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*

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

Cloud Provider & support Accounts.

3. Cliquez sur **Ajouter un compte** et sélectionnez **site de support NetApp**.
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.

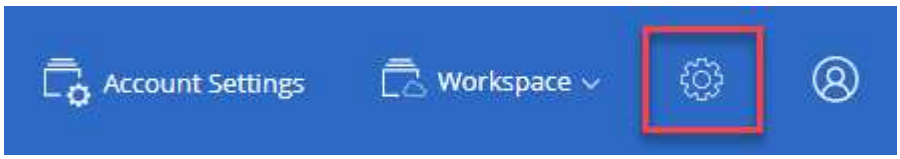
- "Lancement d'Cloud Volumes ONTAP dans AWS"
- "Lancement d'Cloud Volumes ONTAP dans Azure"
- "Enregistrement des systèmes de paiement à l'utilisation"
- "Découvrez comment Cloud Manager gère les fichiers de licences"

Installation d'un certificat HTTPS pour un 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.

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **HTTPS Setup**.

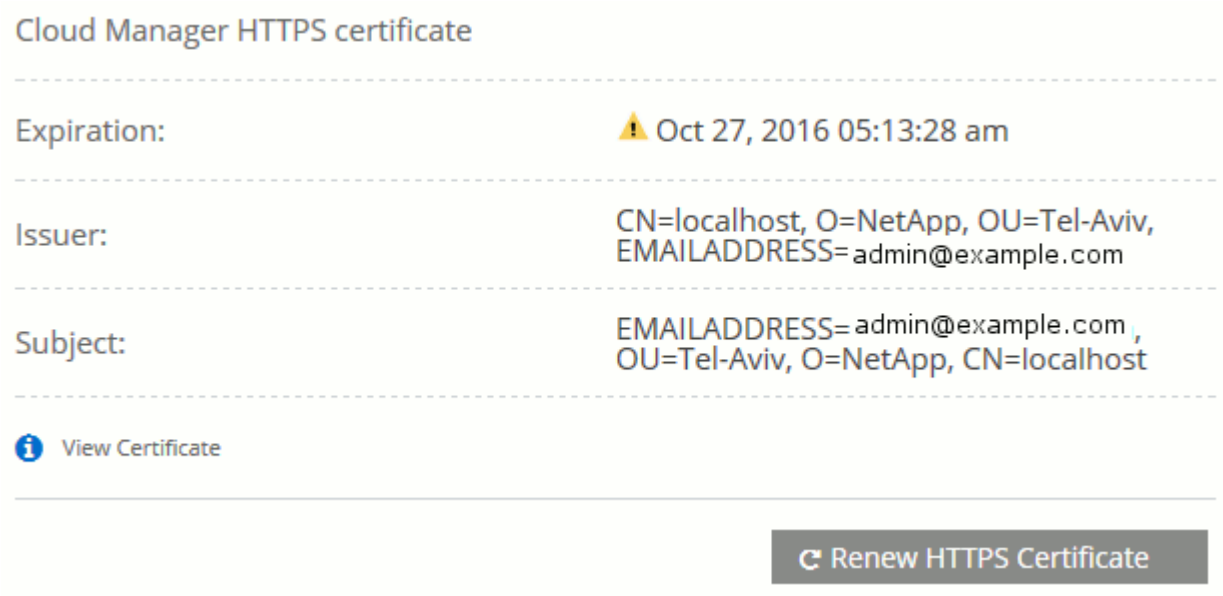


2. Dans la page Configuration HTTPS, installez un certificat en générant une requête de signature de certificat (CSR) ou en installant votre propre certificat signé par l'autorité de certification :

Option	Description
Générez une RSC	a. Entrez le nom d'hôte ou le DNS de l'hôte Cloud Manager (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 :



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 :

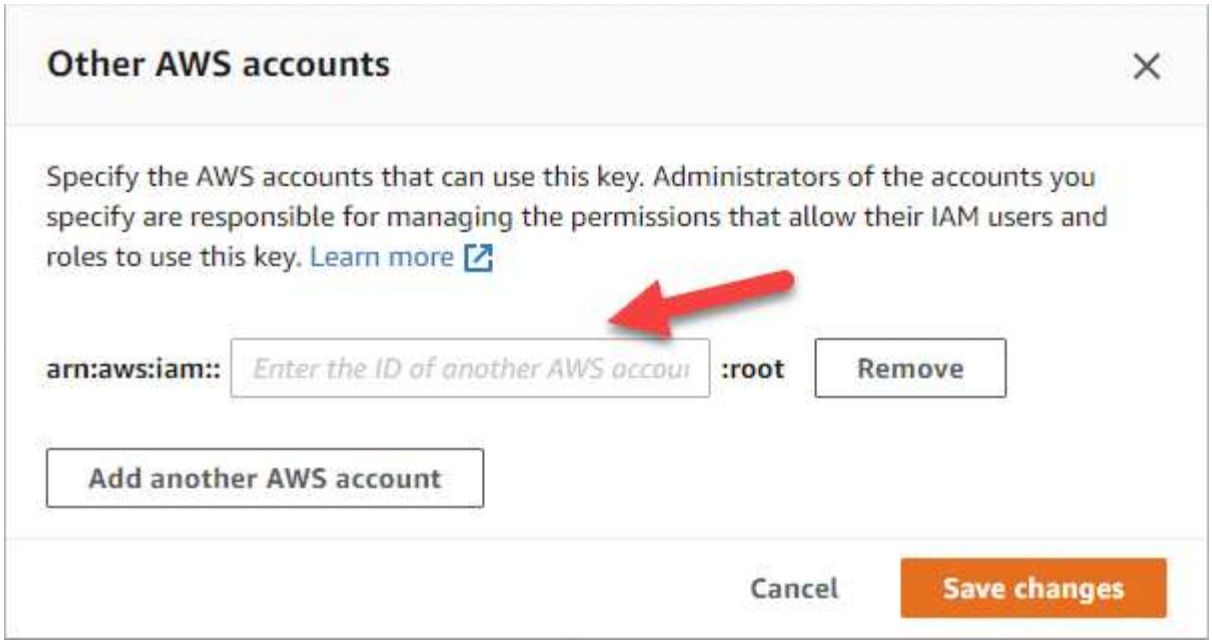
   a. Accédez à la console KMS à partir du compte où réside la CMK.
   b. Sélectionnez la touche.
   c. Dans le volet **Configuration générale**, copiez l’ARN de la clé.

      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".

Exigences liées au réseau

Configuration réseau requise pour Cloud Manager

Configurez votre réseau pour que Cloud Manager puisse déployer les systèmes Cloud Volumes ONTAP dans AWS, Microsoft Azure ou Google Cloud Platform. 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 avec Internet, Cloud Manager vous invite à spécifier le proxy lors de la configuration. Vous pouvez également spécifier le serveur proxy à partir de la page Paramètres. Reportez-vous à la section "Configuration de Cloud Manager pour utiliser un serveur proxy".

Connexion aux réseaux cibles

Cloud Manager nécessite une connexion réseau aux VPC et VNets dans lesquels vous souhaitez déployer Cloud Volumes ONTAP.

Par exemple, si vous installez Cloud Manager sur votre réseau d'entreprise, vous devez configurer une connexion VPN sur le VPC ou le Net dans lequel vous lancez Cloud Volumes ONTAP.

Accès Internet sortant

Cloud Manager nécessite un accès Internet sortant pour déployer et gérer Cloud Volumes ONTAP. Un accès Internet sortant est également requis pour accéder à Cloud Manager à partir de votre navigateur Web et pour exécuter le programme d'installation de Cloud Manager sur un hôte Linux.

Les sections suivantes identifient les terminaux spécifiques.

Des terminaux pour gérer Cloud Volumes ONTAP dans AWS

Cloud Manager nécessite un accès Internet sortant pour contacter les terminaux suivants lors du déploiement et de la gestion de Cloud Volumes ONTAP dans AWS :

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.

Terminaux	Objectif
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Permet d'accéder aux images logicielles, aux manifestes et aux modèles.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.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://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.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement	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.

Des terminaux pour gérer Cloud Volumes ONTAP dans Azure

Cloud Manager nécessite un accès Internet sortant pour contacter les terminaux suivants lors du déploiement et de la gestion de Cloud Volumes ONTAP dans Microsoft Azure :

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.

Terminaux	Objectif
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://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.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://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	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.

Des terminaux pour gérer Cloud Volumes ONTAP dans GCP

Cloud Manager requiert un accès Internet sortant pour contacter les terminaux suivants lors du déploiement et de la gestion de Cloud Volumes ONTAP dans GCP :

Terminaux	Objectif
https://www.googleapis.com	Cet outil permet à Cloud Manager d'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://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.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://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	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.

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
L'hôte Cloud Manager	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.

Terminaux pour installer Cloud Manager sur un hôte Linux

Le programme d'installation de Cloud Manager 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

Ports et groupes de sécurité

- Si vous déployez Cloud Manager à partir de Cloud Central ou des images du marché, reportez-vous aux documents suivants :
  - "Règles de groupe de sécurité pour Cloud Manager dans AWS"
  - "Règles de groupe de sécurité pour Cloud Manager in Azure"
  - "Règles de pare-feu pour Cloud Manager dans GCP"
- Si vous installez Cloud Manager sur un hôte Linux existant, reportez-vous à la section "Conditions de l'hôte Cloud Manager".

Configuration réseau requise pour Cloud Volumes ONTAP dans AWS

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

Configuration réseau AWS générale requise 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.

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".

Configuration réseau AWS requise pour Cloud Volumes ONTAP HA 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".

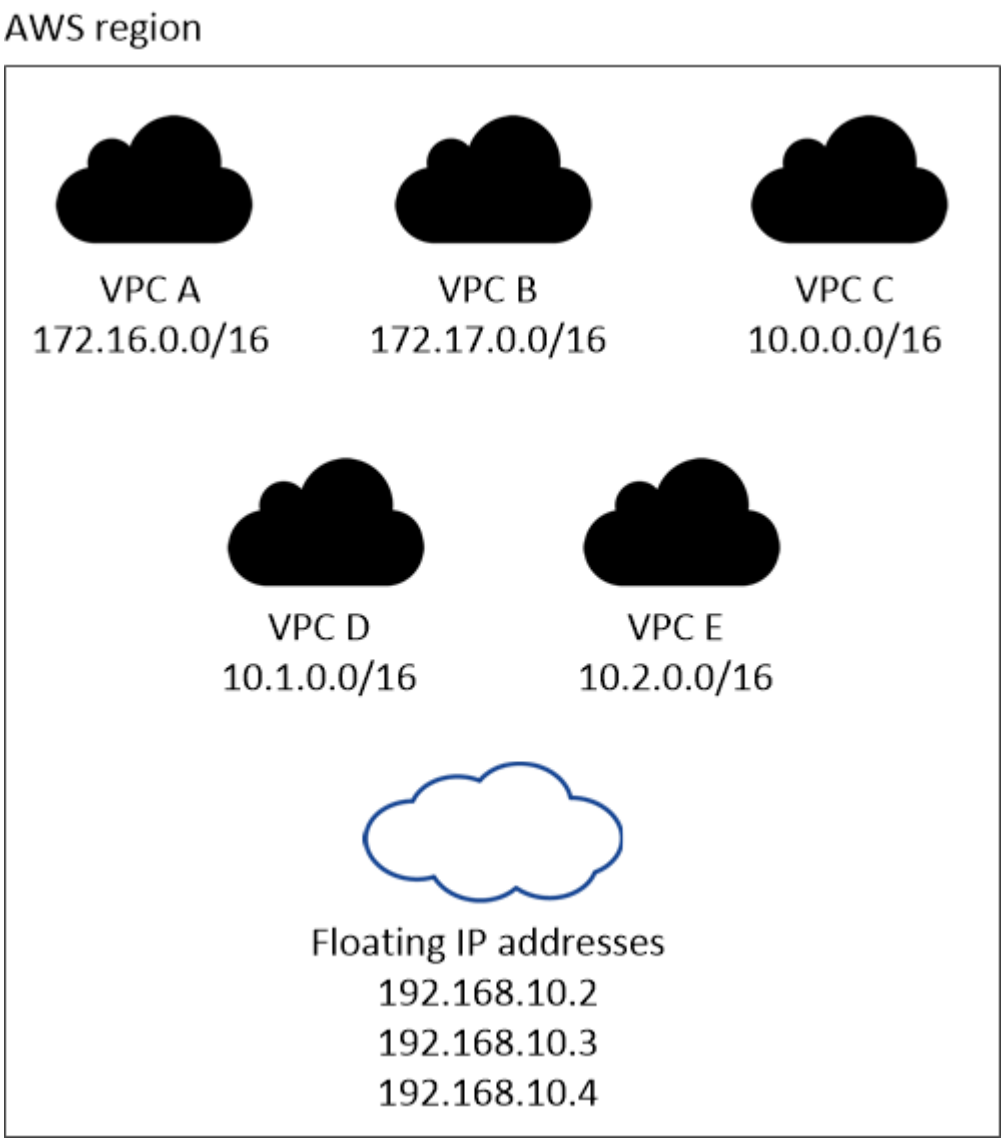
Une adresse IP flottante concerne la gestion du cluster, l'une concerne les données NFS/CIFS sur le nœud 1 et l'autre les données NFS/CIFS sur le nœud 2. Une quatrième adresse IP flottante est facultative pour la gestion des SVM.

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".

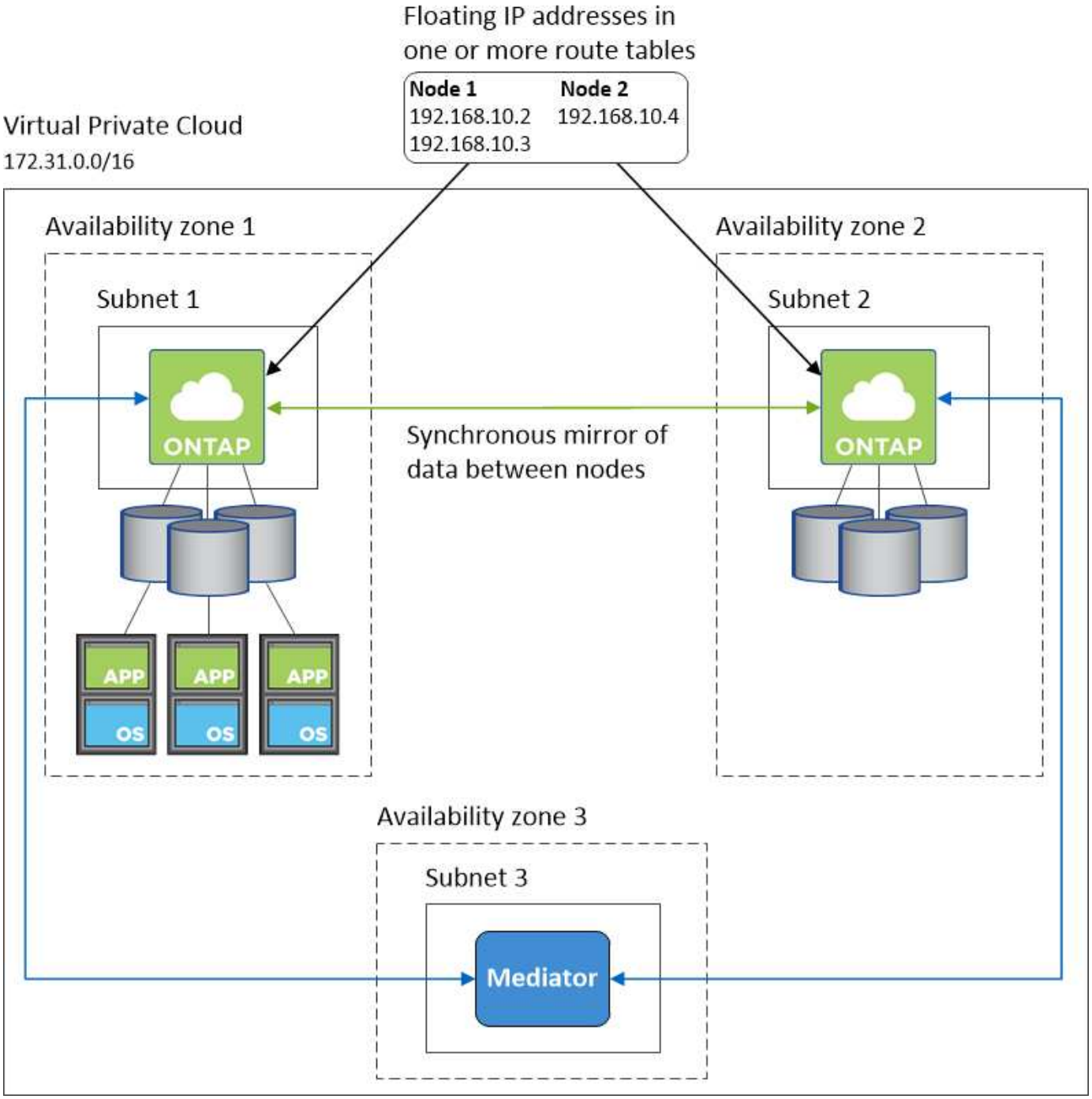
Connexion aux outils de gestion NetApp

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

L’image suivante montre une configuration HA optimale dans AWS fonctionnant comme une configuration active-passive :



Exemples de configurations VPC

Pour mieux comprendre comment déployer Cloud Manager et Cloud Volumes ONTAP dans AWS, vous devez consulter les configurations VPC les plus courantes.

- Un VPC avec des sous-réseaux publics et privés et un périphérique NAT
- Un VPC avec un sous-réseau privé et une connexion VPN avec votre réseau

Un VPC avec des sous-réseaux publics et privés et un périphérique NAT

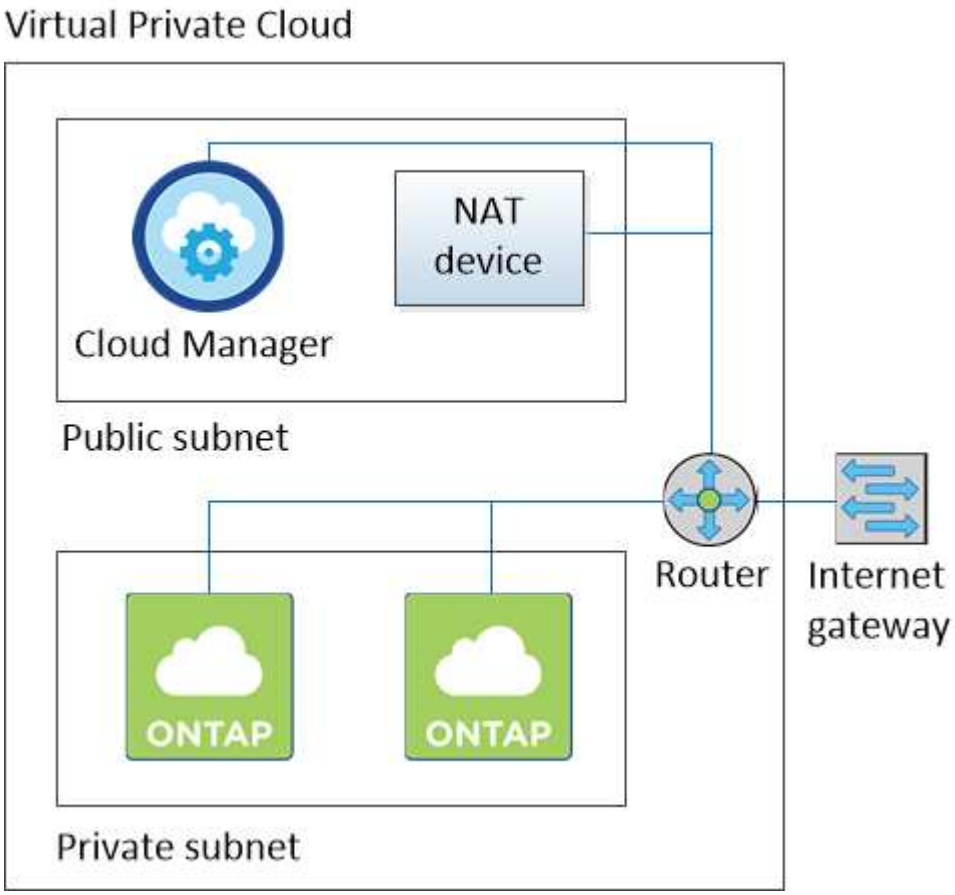
Cette configuration VPC inclut des sous-réseaux publics et privés, une passerelle Internet qui connecte le VPC à Internet et une passerelle NAT ou une instance NAT dans le sous-réseau public qui active le trafic Internet

sortant à partir du sous-réseau privé. Dans cette configuration, vous pouvez exécuter Cloud Manager dans un sous-réseau public ou privé, mais le sous-réseau public est recommandé car il permet l'accès à partir d'hôtes en dehors du VPC. Vous pouvez ensuite lancer des instances Cloud Volumes ONTAP dans le sous-réseau privé.

Au lieu d'un périphérique NAT, vous pouvez utiliser un proxy HTTP pour fournir une connectivité Internet.

Pour plus de détails sur ce scénario, voir "Documentation AWS : scénario 2 : VPC avec sous-réseaux publics et privés (NAT)".

Le graphique ci-dessous présente Cloud Manager s'exécutant dans un sous-réseau public et des systèmes à nœud unique s'exécutant dans un sous-réseau privé :



Un VPC avec un sous-réseau privé et une connexion VPN avec votre réseau

Cette configuration VPC est une configuration de cloud hybride dans laquelle Cloud Volumes ONTAP devient une extension de votre environnement privé. La configuration inclut un sous-réseau privé et une passerelle privée virtuelle avec une connexion VPN à votre réseau. Le routage à travers le tunnel VPN permet aux instances EC2 d'accéder à Internet via votre réseau et vos pare-feu. Vous pouvez exécuter Cloud Manager dans le sous-réseau privé ou dans votre data center. Vous lancez ensuite Cloud Volumes ONTAP dans le sous-réseau privé.

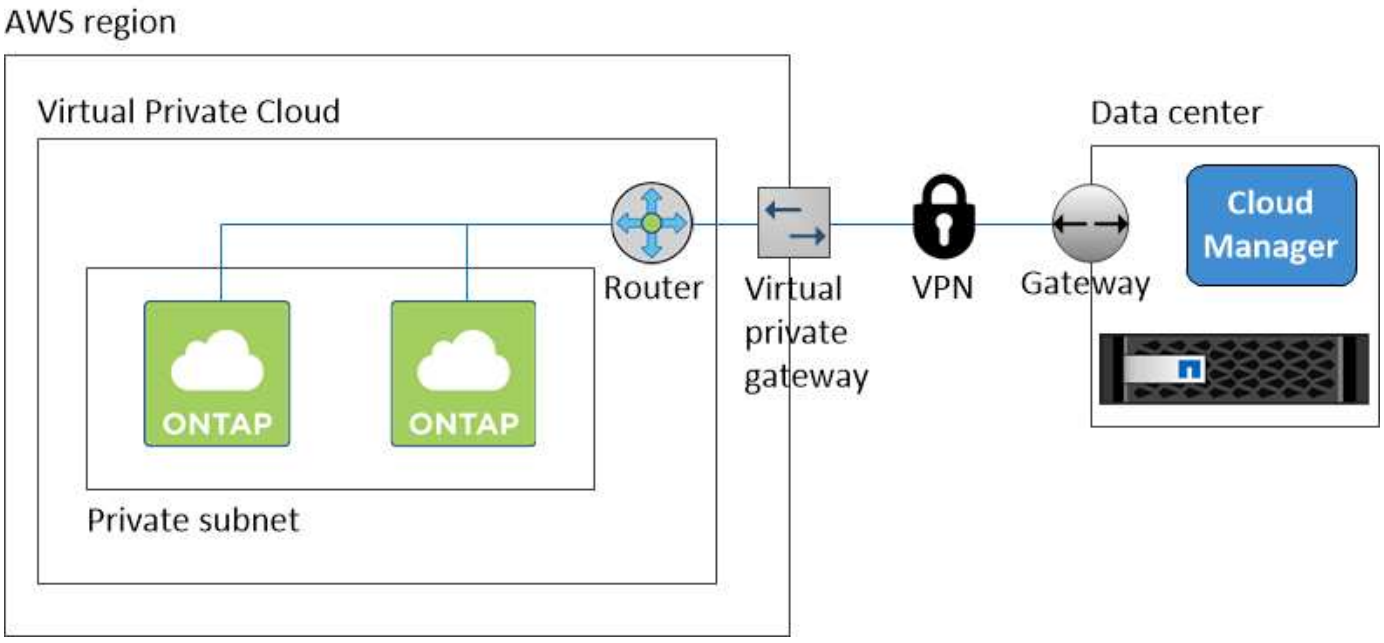
Vous pouvez également utiliser un serveur proxy dans cette configuration pour autoriser l'accès à Internet. Le serveur proxy peut se trouver dans votre data center ou dans AWS.

Si vous souhaitez répliquer des données entre les systèmes FAS de votre data center et les systèmes Cloud

Volumes ONTAP d'AWS, vous devez utiliser une connexion VPN pour sécuriser la liaison.

Pour plus de détails sur ce scénario, voir "Documentation AWS : scénario 4 : VPC avec un sous-réseau privé uniquement et accès VPN géré par AWS".

Le graphique ci-dessous présente Cloud Manager exécuté dans votre data center et les systèmes à nœud unique s'exécutant dans un sous-réseau privé :



Configuration d'une passerelle de transit AWS pour les paires HA dans plusieurs AZS

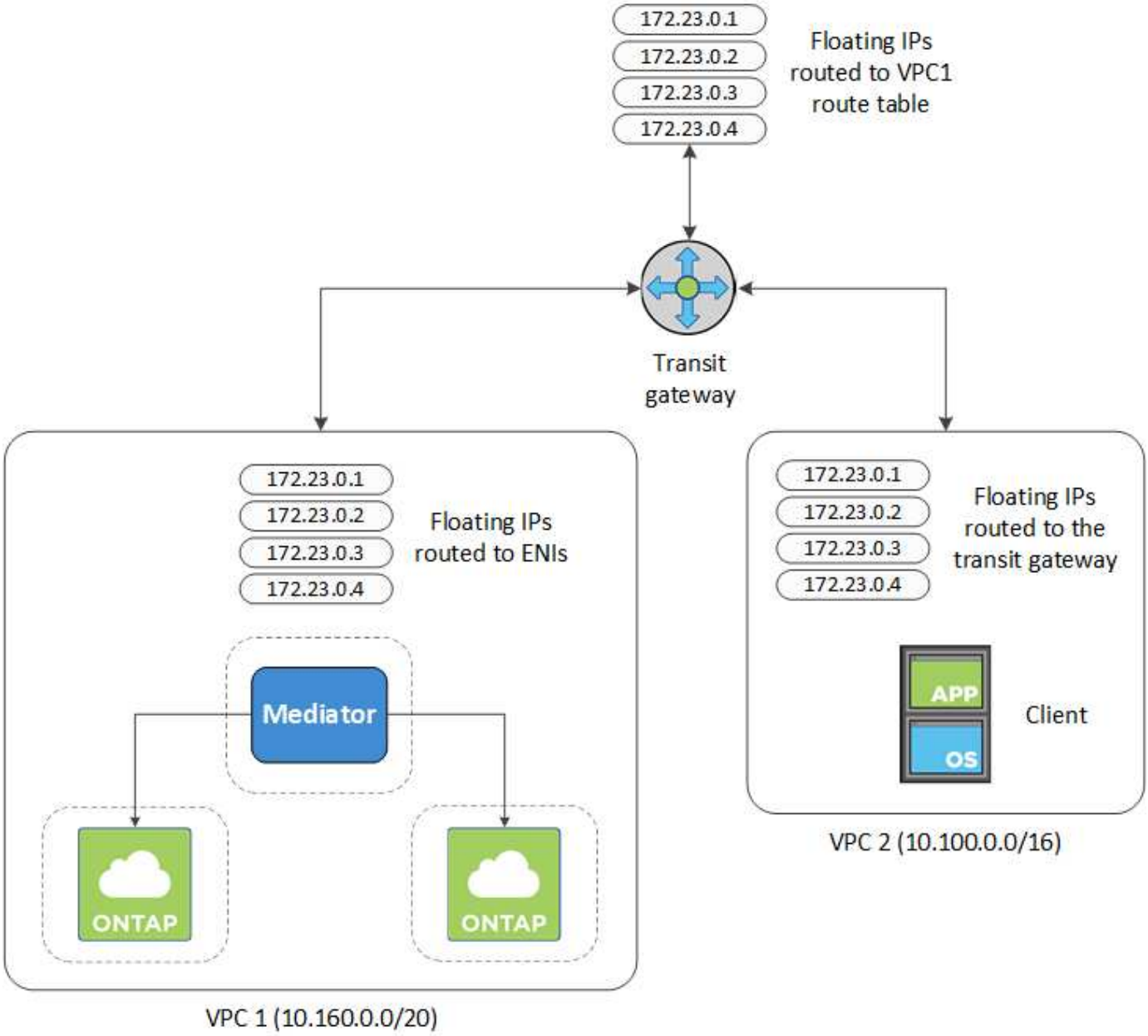
Configurez une passerelle de transit AWS pour permettre l'accès aux adresses IP flottantes d'une paire HA à l'extérieur du VPC où réside la paire HA.

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.

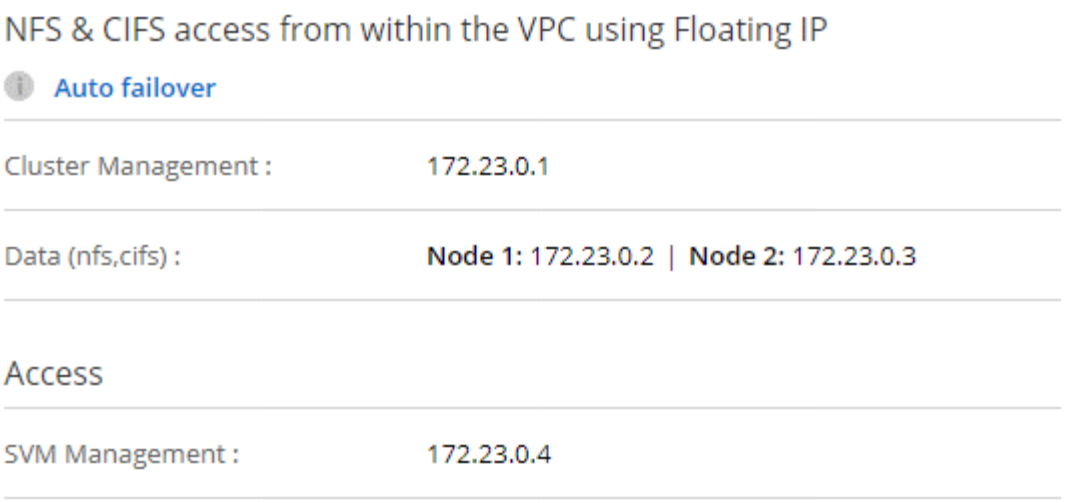


Les étapes suivantes montrent comment configurer une configuration similaire.

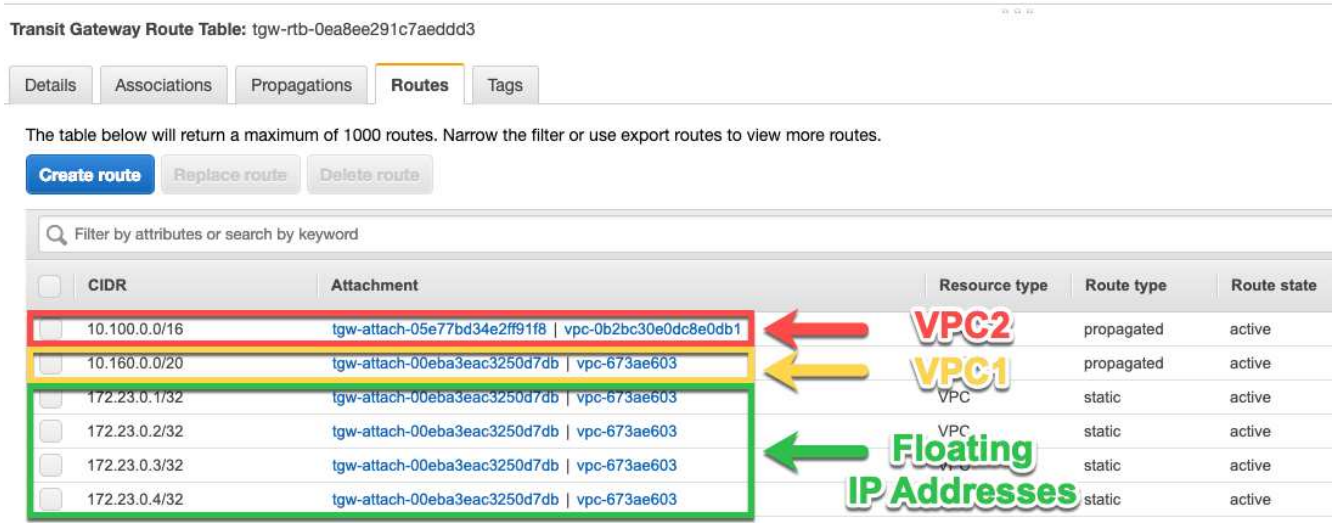
Étapes

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.

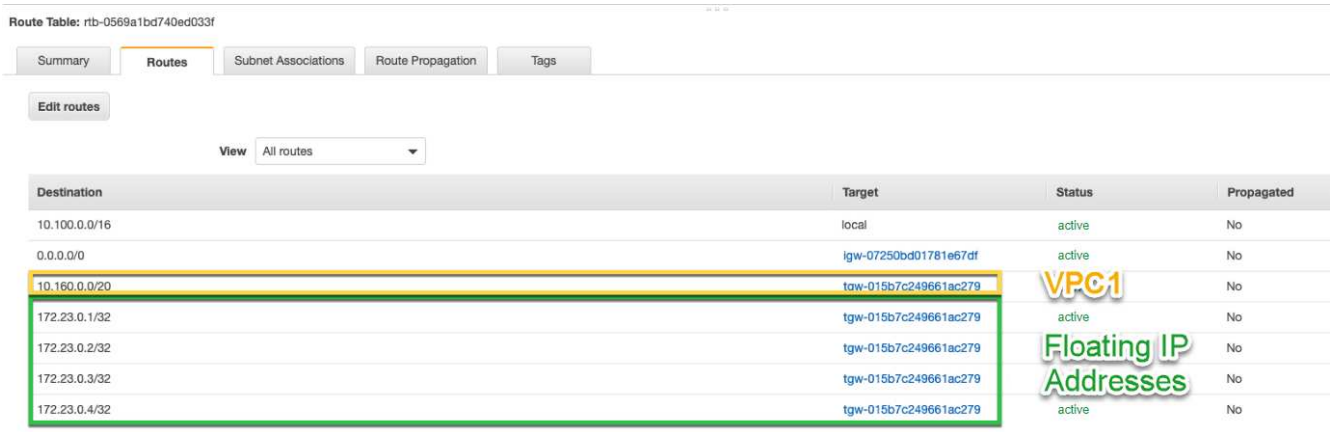


3. Modifiez la table de routage des VPC qui doivent accéder aux adresses IP flottantes.

   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.

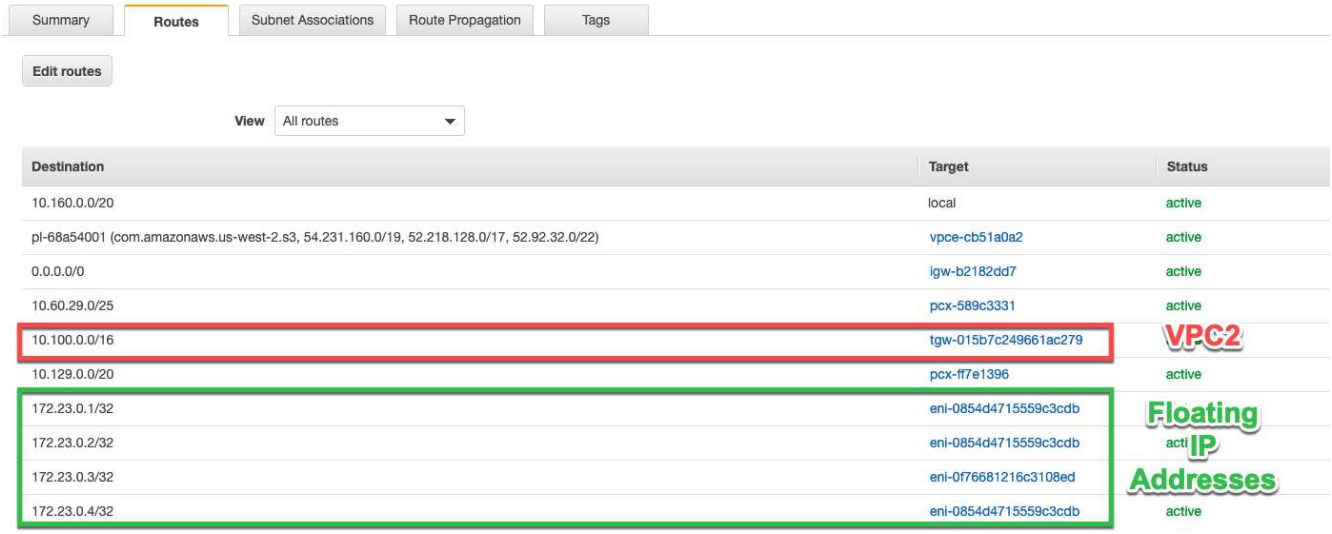
      L'exemple d'image suivant montre la table de route pour VPC 2, qui comprend les routes vers VPC 1 et les adresses IP flottantes.



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.

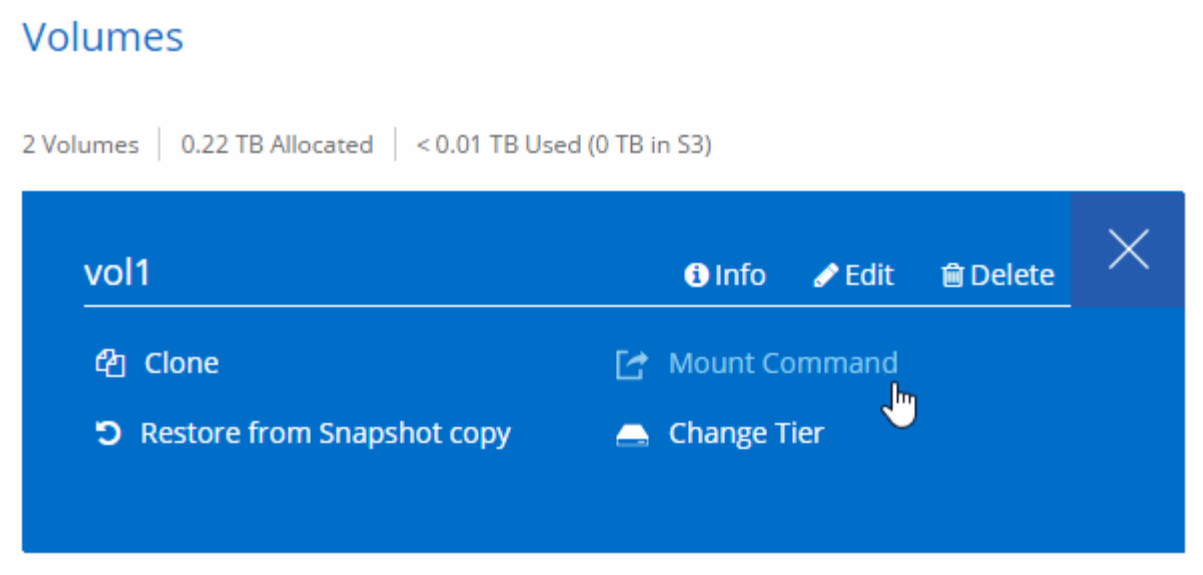
   Cette étape est importante car elle termine le routage entre les VPC.

   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"

Configuration réseau requise pour Cloud Volumes ONTAP dans Azure

Configurez votre réseau Azure de façon à ce que les systèmes Cloud Volumes ONTAP puissent fonctionner correctement.

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

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".

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".

Exigences de mise en réseau pour Cloud Volumes ONTAP dans GCP

Configurez votre réseau Google Cloud Platform de manière à ce que les systèmes Cloud Volumes ONTAP puissent fonctionner correctement.

VPC partagé

Cloud Manager et Cloud Volumes ONTAP sont pris en charge par un VPC partagé de Google Cloud Platform.

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 machine virtuelle Cloud Manager et Cloud Volumes ONTAP dans un projet *service*. "Documentation Google Cloud : présentation du VPC partagé".

La seule exigence est de fournir les autorisations suivantes au compte de service Cloud Manager dans le projet hôte VPC partagé :

compute.firewalls.* compute.networks.* compute.subnetworks.*

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

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 utiliser votre propre, reportez-vous à la section "Règles de pare-feu GCP".

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".

D'autres options de déploiement

Conditions de l'hôte Cloud Manager

Si vous installez Cloud Manager sur votre propre hôte, vous devez vérifier la prise en charge de votre configuration, notamment la configuration requise pour le système d'exploitation, la configuration requise pour le port, etc.

Vous pouvez installer Cloud Manager sur votre propre hôte dans GCP, mais pas sur votre réseau sur site. Cloud Manager doit être installé dans GCP afin de déployer Cloud Volumes ONTAP dans GCP.

Un hôte dédié est requis

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

Types d’instances AWS EC2 pris en charge

- t2.medium
- t3.medium (recommandé)
- m4.grand
- m5.xlarge
- m5.2xlarge
- m5.4xlarge
- m5.mmp2

Tailles de VM Azure prises en charge

A2, D2 v2 ou D2 v3 (selon disponibilité)

Types de machines GCP pris en charge

Type d’ordinateur avec au moins 2 CPU virtuels et 4 Go de mémoire.

Systèmes d’exploitation pris en charge

- CentOS 7.2
- CentOS 7.3
- CentOS 7.4
- CentOS 7.5
- Red Hat Enterprise Linux 7.2
- Red Hat Enterprise Linux 7.3
- Red Hat Enterprise Linux 7.4
- Red Hat Enterprise Linux 7.5

  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 lors de l’installation de Cloud Manager.

  Cloud Manager est pris en charge sur les versions anglaises 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 ?"^]

CPU

2,27 GHz ou plus avec deux cœurs

RAM

4 Go

Espace disque disponible

50 Go

Accès Internet sortant

L'accès Internet sortant est requis lors de l'installation de Cloud Manager et lors de l'utilisation de Cloud Manager pour déployer Cloud Volumes ONTAP. Pour obtenir la liste des noeuds finaux, reportez-vous à la section "Configuration réseau requise pour Cloud Manager".

Ports

Les ports suivants doivent être disponibles :

- 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

Si d'autres services utilisent ces ports, l'installation de Cloud Manager échoue.

Il existe un conflit potentiel avec le port 3306. Si une autre instance de MySQL s'exécute sur l'hôte, elle utilise le port 3306 par défaut. Vous devez modifier le port utilisé par l'instance MySQL existante.

Vous pouvez modifier les ports HTTP et HTTPS par défaut lorsque vous installez Cloud Manager. Vous ne pouvez pas modifier le port par défaut de la base de données MySQL. Si vous modifiez les ports HTTP et HTTPS, vous devez vous assurer que les utilisateurs peuvent accéder à la console Web de Cloud Manager à partir d'un hôte distant :

- Modifiez le groupe de sécurité pour autoriser les connexions entrantes via les ports.
- Indiquez le port lorsque vous entrez l'URL dans la console Web de Cloud Manager.

Installation de Cloud Manager sur un hôte Linux existant

La façon la plus courante de déployer Cloud Manager est depuis Cloud Central ou depuis le marché d'un fournisseur cloud. Mais vous avez la possibilité de télécharger et d'installer le logiciel Cloud Manager sur un hôte Linux existant de votre réseau ou dans le cloud.

Vous pouvez installer Cloud Manager sur votre propre hôte dans GCP, mais pas sur votre réseau sur site. Cloud Manager doit être installé dans GCP afin de déployer Cloud Volumes ONTAP dans GCP.

Avant de commencer

- 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 lors de l'installation de Cloud Manager.
- Le programme d'installation de Cloud Manager accède à plusieurs URL pendant le processus d'installation. Vous devez vous assurer que l'accès Internet sortant est autorisé pour ces terminaux. Reportez-vous à la section "Configuration réseau requise pour Cloud Manager".

Description de la tâche

- Les privilèges root ne sont pas requis pour installer Cloud Manager.
- Cloud Manager installe les outils de ligne de commande AWS (awscli) afin d'activer les procédures de

restauration du support NetApp.

Si vous recevez un message indiquant que l'installation de awscli a échoué, vous pouvez ignorer le message en toute sécurité. Cloud Manager peut fonctionner avec succès sans les outils.

- Le programme d'installation disponible sur le site du support NetApp peut être une version antérieure. Après l'installation, Cloud Manager se met automatiquement à jour si une nouvelle version est disponible.

Étapes

1. Examen des exigences de mise en réseau :
   - "Configuration réseau requise pour Cloud Manager"
   - "Configuration réseau requise pour Cloud Volumes ONTAP dans AWS"
   - "Configuration réseau requise pour Cloud Volumes ONTAP dans Azure"
   - "Exigences de mise en réseau pour Cloud Volumes ONTAP dans GCP"
2. Révision "Conditions de l'hôte Cloud Manager".
3. Téléchargez le logiciel à partir du "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".

4. Attribuez des autorisations pour exécuter le script.

   Exemple

   ```
    chmod +x OnCommandCloudManager-V3.7.0.sh
   . Exécutez le script d'installation :
   ```

   ```
   ./OnCommandCloudManager-V3.7.0.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 Cloud Manager se trouve 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.

5. 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.

   Si vous modifiez les ports HTTP et HTTPS, vous devez vous assurer que les utilisateurs peuvent accéder à la console Web de Cloud Manager à partir d'un hôte distant :

   - Modifiez le groupe de sécurité pour autoriser les connexions entrantes via les ports.
   - Indiquez le port lorsque vous entrez l'URL dans la console Web de Cloud Manager.

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.

6. Ouvrez un navigateur Web et entrez l'URL suivante :

   https://ipaddress:port

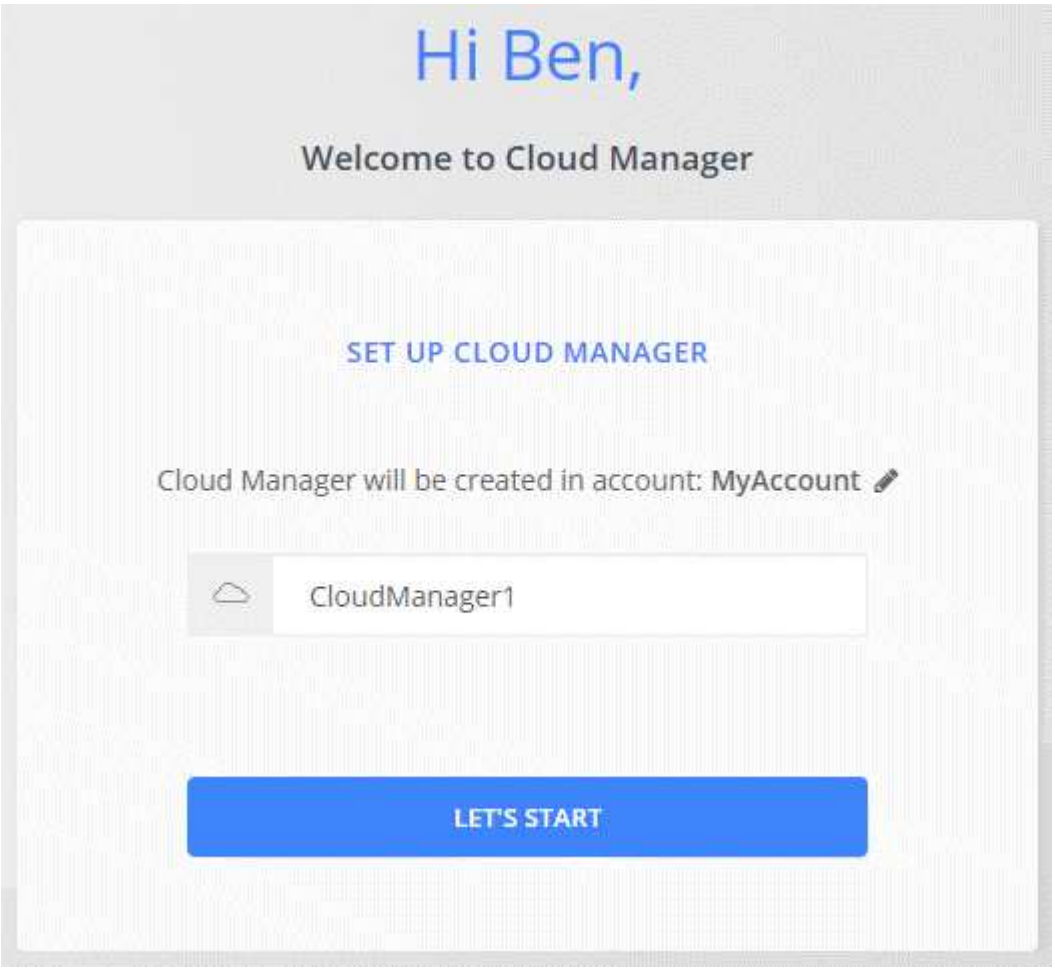
   Ipaddress peut être localhost, une adresse IP privée ou une adresse IP publique, selon la configuration de l'hôte Cloud Manager. Par exemple, si Cloud Manager se trouve dans le cloud public sans adresse IP publique, vous devez entrer une adresse IP privée à partir d'un hôte disposant d'une connexion à l'hôte Cloud Manager.

   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

7. Inscrivez-vous sur NetApp Cloud Central ou connectez-vous.
8. Une fois connecté, configurez Cloud Manager :
   a. Spécifiez le compte Cloud Central à associer à ce système Cloud Manager.

      "Découvrez les comptes Cloud Central".

   b. Entrez un nom pour le système.



Une fois que vous avez terminé

Configurez des autorisations pour que Cloud Manager puisse déployer Cloud Volumes ONTAP dans votre fournisseur cloud :

- 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. "Associez ce compte de service à la machine virtuelle Cloud Manager".
  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.

Lancement de Cloud Manager à partir d'AWS Marketplace

Il est recommandé de lancer Cloud Manager dans AWS à l'aide de "NetApp Cloud Central", Mais vous pouvez le lancer depuis AWS Marketplace, si nécessaire.

Si vous lancez Cloud Manager à partir d'AWS Marketplace, Cloud Manager est toujours intégré à NetApp Cloud Central. "En savoir plus sur l'intégration".

Description de la tâche

La procédure suivante décrit le lancement de 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**.

Étapes

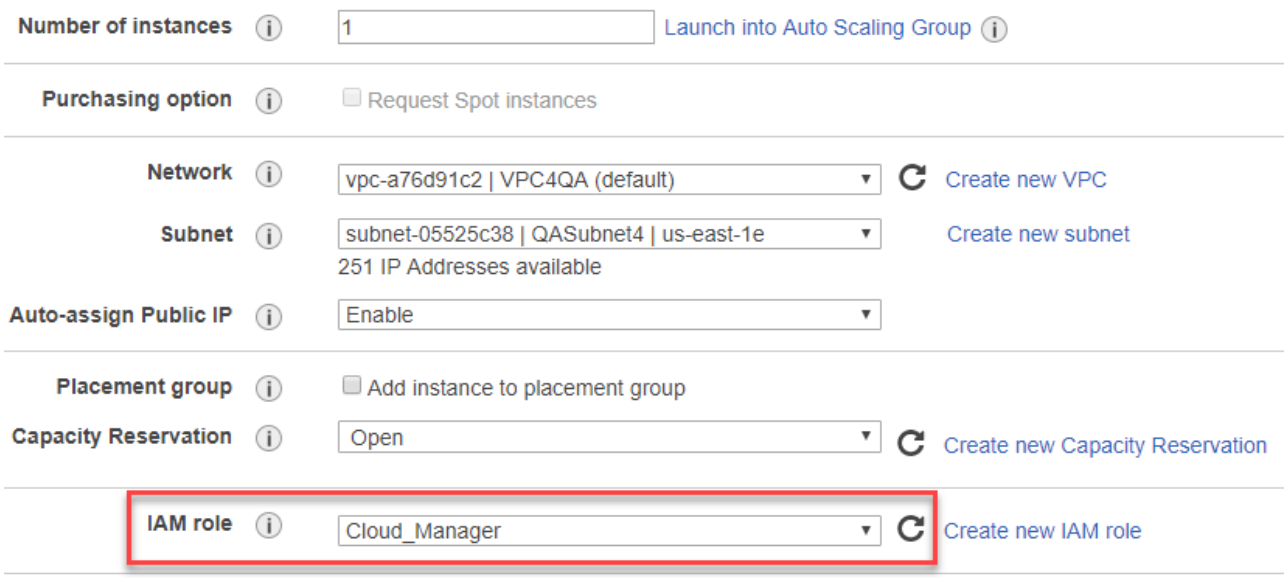
1. Créer une règle IAM et un rôle pour l'instance EC2 :
   a. Téléchargez la politique IAM de Cloud Manager à partir de l'emplacement suivant :

      "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. "Abonnez-vous à partir d'AWS Marketplace" Pour garantir l'absence de perturbation du service après la fin de votre essai gratuit de Cloud Volumes ONTAP. 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.
3. Maintenant, allez au "Page Cloud Manager sur AWS Marketplace" Pour déployer Cloud Manager à partir d'une ami.
4. Sur la page Marketplace, cliquez sur **Continuer pour s'abonner**, puis cliquez sur **Continuer la configuration**.

5. Modifiez l'une des options par défaut et cliquez sur **Continuer pour lancer**.
6. Sous **choisir action**, sélectionnez **lancer via EC2**, puis cliquez sur **lancer**.
7. Suivez les invites pour configurer et déployer l'instance :
   - **Choisir le type d'instance** : selon la disponibilité de la région, choisissez l'un des types d'instance pris en charge (t3.medium est recommandé).

     "Consultez la liste des types d'instances pris en charge".
   - **Configurer l'instance** : sélectionnez un VPC et un sous-réseau, le rôle IAM que vous avez créé à l'étape 1 et d'autres options de configuration qui répondent à vos besoins.



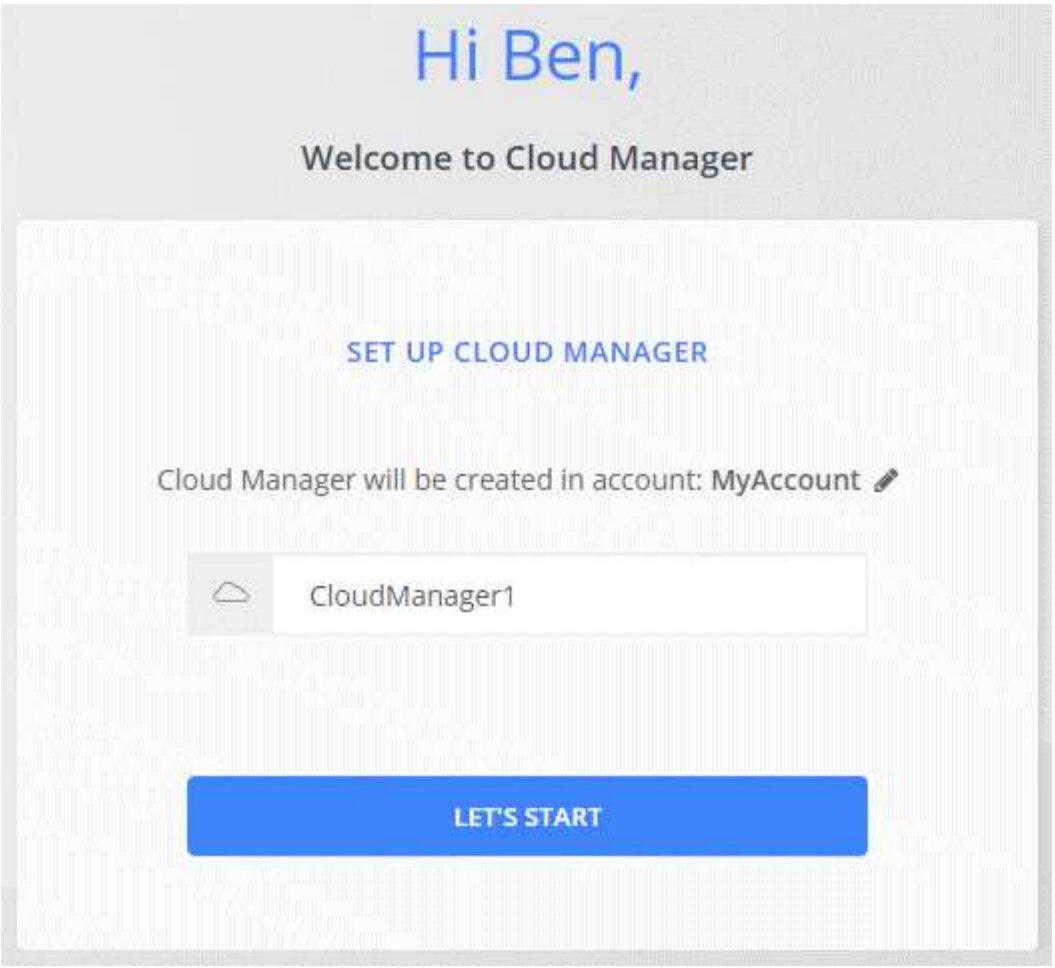
   - **Ajouter stockage** : conservez les options de stockage par défaut.
   - **Ajouter des balises** : saisissez des balises pour l'instance, si vous le souhaitez.
   - **Configurer le groupe de sécurité** : spécifiez les méthodes de connexion requises pour l'instance Cloud Manager : SSH, HTTP et HTTPS.
   - **Revue**: Passez en revue vos sélections et cliquez sur **lancer**.

     AWS lance le logiciel avec les paramètres spécifiés. L'instance et le logiciel Cloud Manager doivent être exécutés en cinq minutes environ.
8. Ouvrez un navigateur Web à partir d'un hôte qui dispose d'une connexion à la machine virtuelle Cloud Manager et entrez l'URL suivante :

   http://ipaddress:80
9. Une fois connecté, configurez Cloud Manager :
   a. Spécifiez le compte Cloud Central à associer à ce système Cloud Manager.

      "Découvrez les comptes Cloud Central".

   b. Entrez un nom pour le système.



Résultat

Cloud Manager est maintenant installé et configuré.

Déploiement de Cloud Manager à partir d'Azure Marketplace

Il est recommandé de déployer Cloud Manager dans Azure à l'aide de "NetApp Cloud Central", Mais vous pouvez le déployer à partir d'Azure Marketplace, si nécessaire.

Des instructions distinctes sont disponibles pour déployer Cloud Manager dans le "Les régions du gouvernement des États-Unis Azure" et po "Les régions Azure Germany".

Si vous déployez Cloud Manager à partir d'Azure Marketplace, Cloud Manager est toujours intégré à NetApp Cloud Central. "En savoir plus sur l'intégration".

Déploiement de Cloud Manager dans Azure

Vous devez installer et configurer Cloud Manager afin de pouvoir l'utiliser pour lancer Cloud Volumes ONTAP dans Azure.

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 l'une des tailles de machine virtuelle recommandées : A2, D2 v2 ou D2 v3 (selon disponibilité).
   - Pour le groupe de sécurité réseau, Cloud Manager nécessite des connexions entrantes via SSH, HTTP et HTTPS.

     "En savoir plus sur les règles de groupe de sécurité pour Cloud Manager".

   - Sous **Management**, activez **System Assigned Managed Identity** pour Cloud Manager en sélectionnant **On**.

     Ce paramètre est important, car une identité gérée permet à la machine virtuelle de Cloud Manager 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. La machine virtuelle et le logiciel Cloud Manager doivent être exécutés en cinq minutes environ.

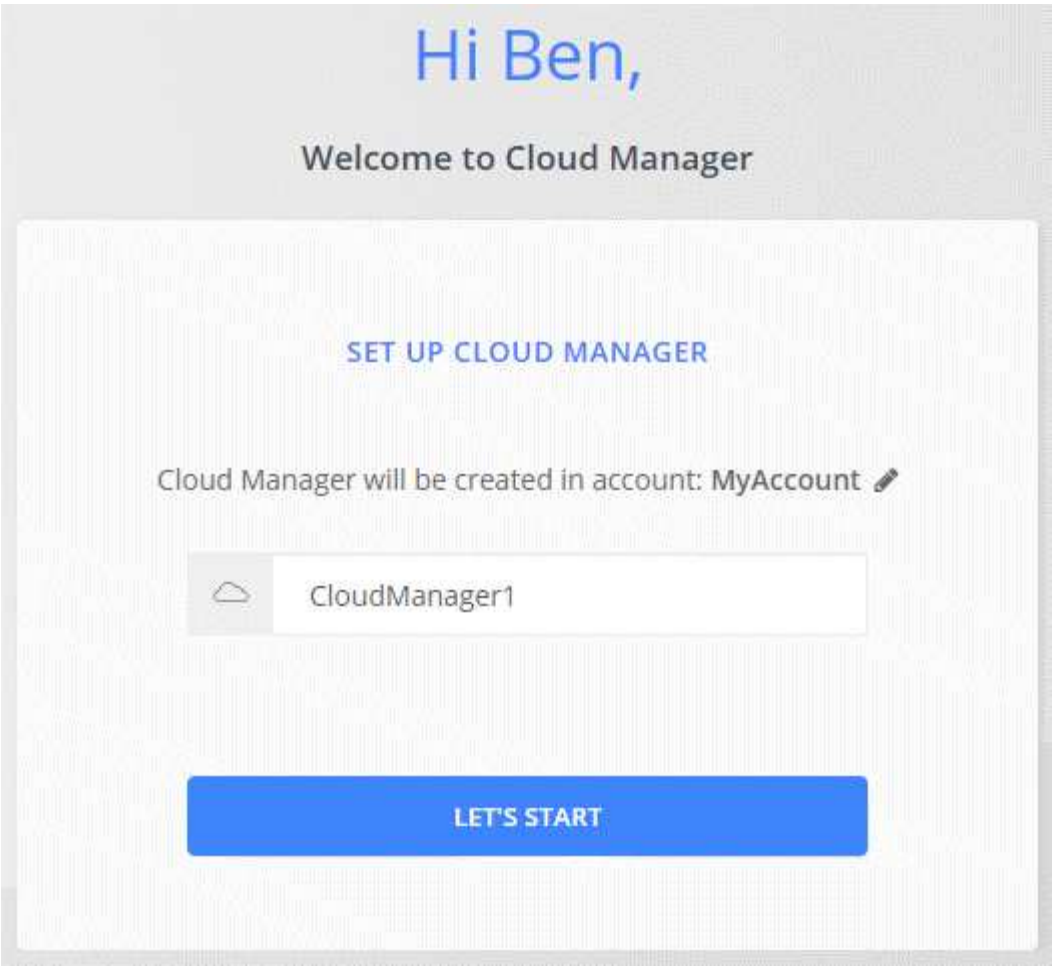
5. Ouvrez un navigateur Web à partir d'un hôte qui dispose d'une connexion à la machine virtuelle Cloud Manager et entrez l'URL suivante :

   http://ipaddress:80

6. Une fois connecté, configurez Cloud Manager :
   a. Spécifiez le compte Cloud Central à associer à ce système Cloud Manager.

      "Découvrez les comptes Cloud Central".

   b. Entrez un nom pour le système.



Résultat

Cloud Manager 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 à Cloud Manager

Lorsque vous avez déployé Cloud Manager dans Azure, vous devez avoir activé une "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 Cloud Manager 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 :

   Définition de rôle az create --role-definition C:\Policy_for_Cloud_Manager_Azure_3.7.4.json

Vous devez maintenant disposer d'un rôle personnalisé appelé OnCommand Cloud Manager Operator que vous pouvez attribuer à la machine virtuelle Cloud Manager.

2. Attribuez le rôle à la machine virtuelle Cloud Manager 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 OnCommand Cloud Manager**.

        L'opérateur OnCommand 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 Cloud Manager a été créée.
      - Sélectionnez la machine virtuelle Cloud Manager.
      - 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

Cloud Manager dispose désormais des autorisations dont il a besoin pour déployer et gérer Cloud Volumes ONTAP dans Azure.

Déploiement de Cloud Manager dans une région Azure Government

Pour que Cloud Manager soit opérationnel dans une région du gouvernement des États-Unis, commencez par déployer Cloud Manager à partir d'Azure Government Marketplace. Ensuite, fournissez les autorisations dont Cloud Manager a besoin pour déployer et gérer les systèmes Cloud Volumes ONTAP.

Pour obtenir la liste des régions du gouvernement des États-Unis d'Azure prises en charge, reportez-vous à la section "Régions Cloud volumes Global".

Déploiement de Cloud Manager à partir d'Azure US Government Marketplace

Cloud Manager est disponible en tant qu'image dans Azure Government Marketplace.

Étapes

1. Vérifiez que l'option Azure Government Marketplace est activée dans votre abonnement :
   a. Connectez-vous au portail en tant qu'administrateur d'entreprise.
   b. Accédez à **gérer**.
   c. Sous **Détails de l'inscription**, cliquez sur l'icône représentant un crayon en regard de **Azure Marketplace**.
   d. Sélectionnez **Enabled**.
   e. Cliquez sur **Enregistrer**.

      "Documentation Microsoft Azure : Azure Government Marketplace"

2. Recherchez OnCommand Cloud Manager sur le portail Azure Government.
3. Cliquez sur **Créer** et suivez les étapes pour configurer la machine virtuelle.

   Notez 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 l'une des tailles de machine virtuelle recommandées : A2, D2 v2 ou D2 v3 (selon disponibilité).
   - Pour le groupe de sécurité réseau, il est préférable de choisir **Advanced**.

     L'option **Advanced** crée un nouveau groupe de sécurité qui inclut les règles entrantes requises pour Cloud Manager. Si vous choisissez base, reportez-vous à la section "Règles de groupe de sécurité" pour la liste des règles requises.

4. Sur la page de résumé, vérifiez vos sélections et cliquez sur **Créer** pour démarrer le déploiement.

   Azure déploie la machine virtuelle avec les paramètres spécifiés. La machine virtuelle et le logiciel Cloud Manager doivent être exécutés en cinq minutes environ.

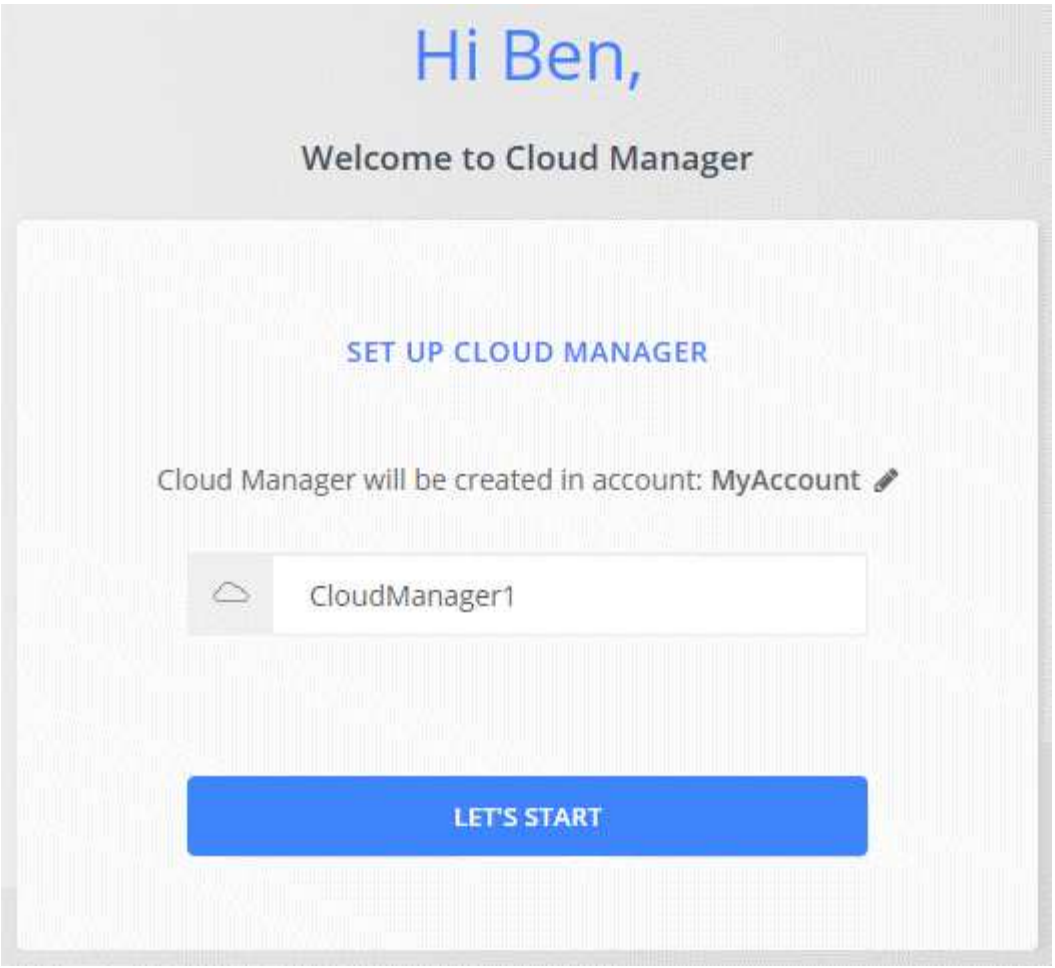
5. Ouvrez un navigateur Web à partir d'un hôte qui dispose d'une connexion à la machine virtuelle Cloud Manager et entrez l'URL suivante :

   http://ipaddress:80

6. Une fois connecté, configurez Cloud Manager :
   a. Spécifiez le compte Cloud Central à associer à ce système Cloud Manager.

      "Découvrez les comptes Cloud Central".

   b. Entrez un nom pour le système.



Résultat

Cloud Manager 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 à Cloud Manager à l'aide d'une identité gérée

Le moyen le plus simple de fournir des autorisations est d'activer un "identité gérée" Sur la machine virtuelle Cloud Manager, puis en attribuant les autorisations requises à la machine virtuelle. Si vous le souhaitez, une autre façon est de le faire "Accordez des autorisations Azure à l'aide d'une entité de service principale".

Étapes

1. Activer une identité gérée sur la machine virtuelle Cloud Manager :
   a. Accédez à la machine virtuelle Cloud Manager et sélectionnez **Identity**.
   b. Sous **System Assigned**, cliquez sur **On**, puis sur **Save**.
2. 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-c25fbzzzzzzzzzzz »,
«/abonnements/54b91999-b3e6-4599-908e-416e0zzzzzzz », «/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 :

   Définition de rôle az create --role-definition C:\Policy_for_Cloud_Manager_Azure_3.7.4.json

Vous devez maintenant disposer d'un rôle personnalisé appelé OnCommand Cloud Manager Operator que vous pouvez attribuer à la machine virtuelle Cloud Manager.

3. Attribuez le rôle à la machine virtuelle Cloud Manager 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**, cliquez sur **Ajouter une affectation de rôle**, puis ajoutez les autorisations :
      - Sélectionnez le rôle **opérateur OnCommand Cloud Manager**.

        L'opérateur OnCommand 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 Cloud Manager a été créée.
      - Saisissez le nom de la machine virtuelle, puis sélectionnez-la.
      - 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

Cloud Manager dispose désormais des autorisations dont il a besoin pour déployer et gérer Cloud Volumes ONTAP dans Azure.

Installation de Cloud Manager dans une région Azure Allemagne

Azure Marketplace n'est pas disponible dans les régions d'Azure Germany. Vous devez donc télécharger le programme d'installation de Cloud Manager à partir du site de support NetApp et l'installer sur un hôte Linux existant dans la région.

Étapes

1. "Examiner les exigences de mise en réseau pour Azure".
2. "Consultez les exigences d'hôte de Cloud Manager".
3. "Téléchargez et installez Cloud Manager".
4. "Attribuez des autorisations Azure à Cloud Manager à l'aide d'une entité principale de service".

Une fois que vous avez terminé

Cloud Manager est maintenant prêt à déployer Cloud Volumes ONTAP dans la région d'Azure Allemagne, comme dans toute autre région. Cependant, vous pouvez d'abord effectuer une configuration supplémentaire.

Assurer le fonctionnement continu de Cloud Manager

Cloud Manager doit rester exécuté en permanence.

Cloud Manager est un élément clé de l'état et de la facturation de Cloud Volumes ONTAP. Si Cloud Manager est hors tension, les systèmes Cloud Volumes ONTAP s'arrêtent après une perte de communication avec Cloud Manager pendant plus de 4 jours.

Déployez Cloud Volumes ONTAP

Avant de créer des systèmes Cloud Volumes ONTAP

Avant d'utiliser Cloud Manager pour créer et gérer des systèmes Cloud Volumes ONTAP, votre administrateur Cloud Manager doit avoir préparé la mise en réseau et installé et configuré Cloud Manager.

Les conditions suivantes doivent exister avant de commencer à déployer Cloud Volumes ONTAP :

- Les exigences de mise en réseau ont été satisfaites pour Cloud Manager et Cloud Volumes ONTAP.
- Cloud Manager dispose d'autorisations pour effectuer des opérations dans le fournisseur cloud de votre choix.
- Pour AWS, vous êtes abonné à la page AWS Marketplace appropriée :
  - Si vous souhaitez déployer un système PAYGO ou activer une fonction d'extension : "Sur la page Cloud Manager (pour Cloud Volumes ONTAP)".
  - Pour déployer un système BYOL : "Sur AWS Marketplace, le seul nœud ou la page HA".
- Cloud Manager a été installé.

Liens connexes

- "Mise en route dans AWS"
- "Mise en route dans Azure"
- "Mise en route dans GCP"
- "Configuration de Cloud Manager"

Connectez-vous à Cloud Manager

Vous pouvez vous connecter à Cloud Manager à partir de n'importe quel navigateur Web disposant d'une connexion au système Cloud Manager. Vous devez vous connecter à l'aide d'un "NetApp Cloud Central" compte utilisateur.

Étapes

1. Ouvrez un navigateur Web et connectez-vous à "NetApp Cloud Central".

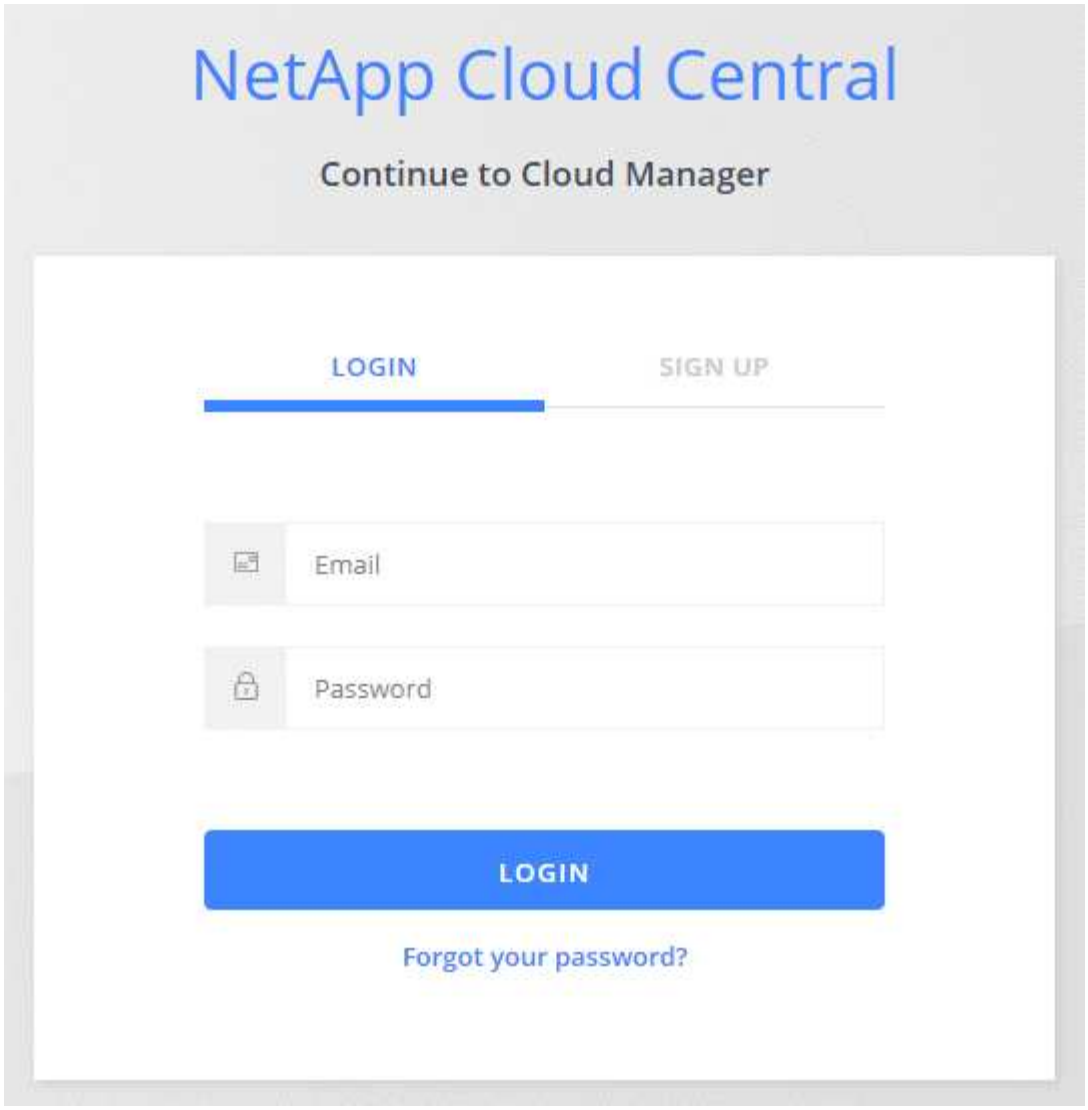
   Cette étape doit vous diriger automatiquement vers la vue de structure. Si ce n'est pas le cas, cliquez sur **vue de structure**.

2. Sélectionnez le système Cloud Manager auquel vous souhaitez accéder.

   Si vous ne voyez aucun système dans cette liste, vérifiez que l'administrateur du compte vous a ajouté au compte Cloud Central associé au système Cloud Manager.

3. Connectez-vous à Cloud Manager à l'aide de vos identifiants NetApp Cloud Central.



Planification de votre configuration Cloud Volumes ONTAP

Lorsque vous déployez Cloud Volumes ONTAP, 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"
- "Configurations prises en charge pour Cloud Volumes ONTAP 9.7 dans Azure"
- "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 AWS"
- "Limites de stockage pour Cloud Volumes ONTAP 9.7 dans Azure"
- "Limites de stockage pour Cloud Volumes ONTAP 9.7 dans GCP"

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.

Planification d'AWS

Planifiez votre déploiement d'Cloud Volumes ONTAP dans AWS en dimensionnant votre système et en examinant les informations réseau nécessaires à votre saisie.

- Dimensionnement de votre système dans AWS
- Fiche technique d'informations sur le réseau 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*

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	

Informations sur AWS	Votre valeur
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	

Planification d'Azure

Planifiez votre déploiement d'Cloud Volumes ONTAP dans Azure en dimensionnant votre système et en examinant les informations réseau nécessaires à votre saisie.

- Dimensionnement du système dans Azure
- Fiche d'informations sur le réseau 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 : présentation du stockage Microsoft 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"

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)	

Planification GCP

Planifiez votre déploiement de Cloud Volumes ONTAP dans Google Cloud Platform en dimensionnant votre système et en examinant les informations réseau à saisir.

- Dimensionnement du système dans GCP
- Fiche technique d'informations réseau 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	

Informations GCP	Votre valeur
Zone	
Réseau VPC	
Sous-réseau	
Politique de pare-feu (s'il s'agit du vôtre)	

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.

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

Activation de Flash cache sur Cloud Volumes ONTAP

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. Il 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.

Limites

- La compression doit être désactivée sur tous les volumes pour tirer parti des améliorations des performances de Flash cache.
- La réactivation du cache après un redémarrage n'est pas prise en charge avec Cloud Volumes ONTAP.

Activation de Flash cache sur Cloud Volumes ONTAP dans AWS

Flash cache est pris en charge avec Cloud Volumes ONTAP Premium et BYOL dans AWS.

Étapes

1. Sélectionnez l'un des types d'instances EC2 suivants avec un système Cloud Volumes ONTAP Premium ou BYOL existant :
   - c5d.4xlarge
   - c5d.9xlarge
   - r5d.2xlarge
2. Désactivez la compression sur tous les volumes pour bénéficier 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".

Activation de Flash cache sur Cloud Volumes ONTAP dans Azure

Flash cache est pris en charge avec Cloud Volumes ONTAP (BYOL) sur les systèmes à un nœud.

Étapes

1. Sélectionnez le type de machine virtuelle Standard_L8S_v2 avec un système Cloud Volumes ONTAP BYOL à un seul nœud dans Azure.
2. Désactivez la compression sur tous les volumes pour bénéficier 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".

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.

Abonnement sur AWS Marketplace

Vous pouvez vous abonner à AWS Marketplace pour payer le coût du stockage Cloud Volumes ONTAP à l'utilisation ou pour déployer Cloud Volumes ONTAP BYOL.

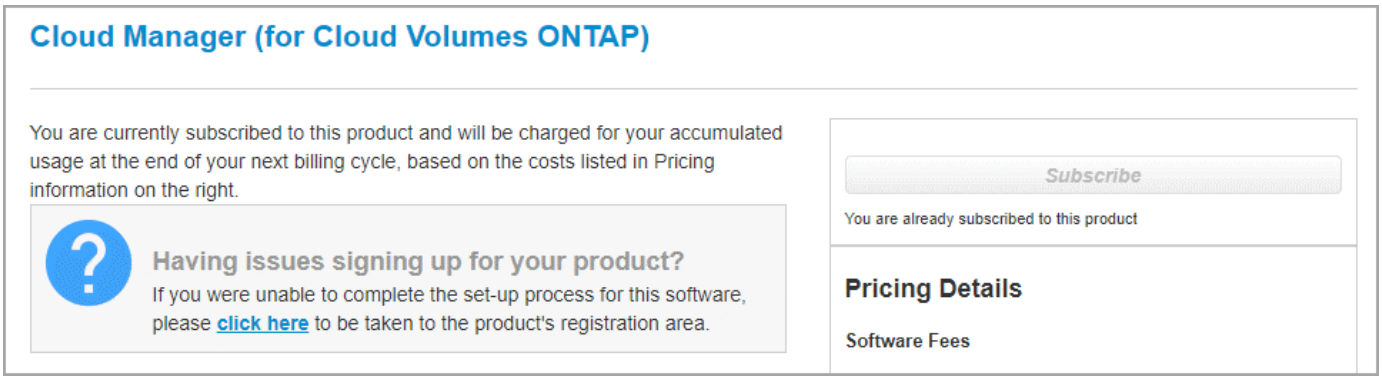
Facturation de l'abonnement à GO

"Abonnez-vous à partir d'AWS Marketplace" Pour garantir l'absence de perturbation du service après la fin de votre essai gratuit de Cloud Volumes ONTAP. 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.

La vidéo suivante montre le processus d'abonnement :

► https://docs.netapp.com/fr-fr/occm37//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 affiche les utilisateurs auxquels ils sont déjà abonnés, comme illustré dans l'image ci-dessous. Lorsqu'un abonnement est en place pour le compte AWS, chaque utilisateur IAM doit s'associer à l'abonnement. Si le message ci-dessous s'affiche, cliquez sur le lien **cliquez ici** pour accéder à Cloud Central et terminer le processus.



Abonnement BYOL

Si vous lancez Cloud Volumes ONTAP avec une licence (BYOL), "Vous devez ensuite vous abonner à cette offre sur AWS Marketplace".

"En savoir plus sur chaque page AWS Marketplace".

Lancement d'un seul système Cloud Volumes ONTAP 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 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

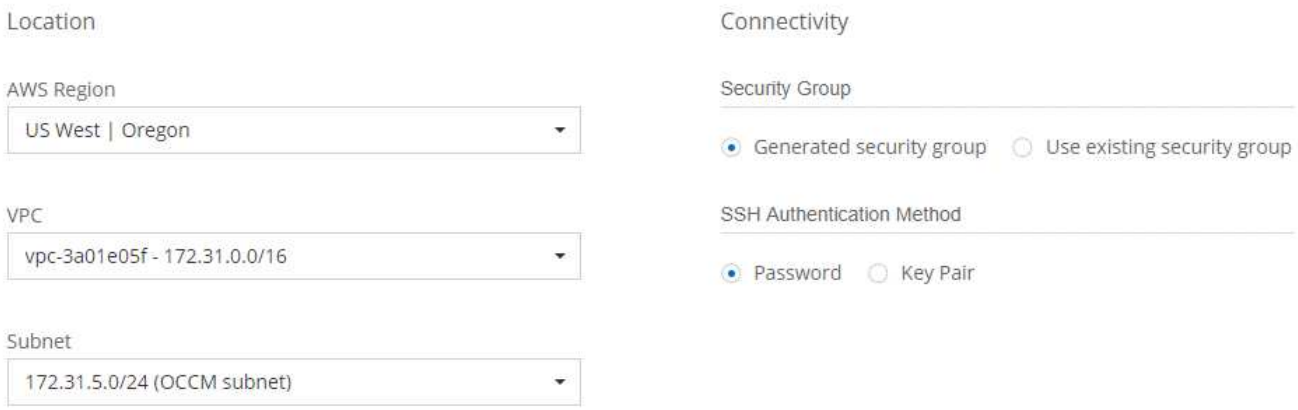
1. Sur la page environnements de travail, cliquez sur **Créer Cloud Volumes ONTAP** et suivez les invites.
2. **Définir votre environnement de travail** : sélectionnez **Amazon Web Services** et **Cloud Volumes ONTAP**.
3. **Détails et informations d'identification** : modifiez éventuellement le compte AWS et l'abonnement Marketplace, 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
Compte	Vous pouvez choisir un autre compte si vous le souhaitez "Ajout de comptes AWS supplémentaires à Cloud Manager".
Abonnement Marketplace	Sélectionnez un autre abonnement si vous souhaitez modifier le compte AWS à partir duquel vous êtes facturé. Pour ajouter un nouvel abonnement, "Rendez-vous sur AWS Marketplace".
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".
Informations d'identification	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.

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 Backup vers S3".
   - "En savoir plus sur Cloud Compliance".
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 9.4 RC1 et 9.4 GA. La mise à jour ne se produit pas d'une version à une autre, par exemple de la version 9.3 à la version 9.4.

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 S3 doit être activée ou non.

    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".

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.

    "En savoir plus sur la vitesse d'écriture".

    "En savoir plus sur le stockage WORM".

13. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

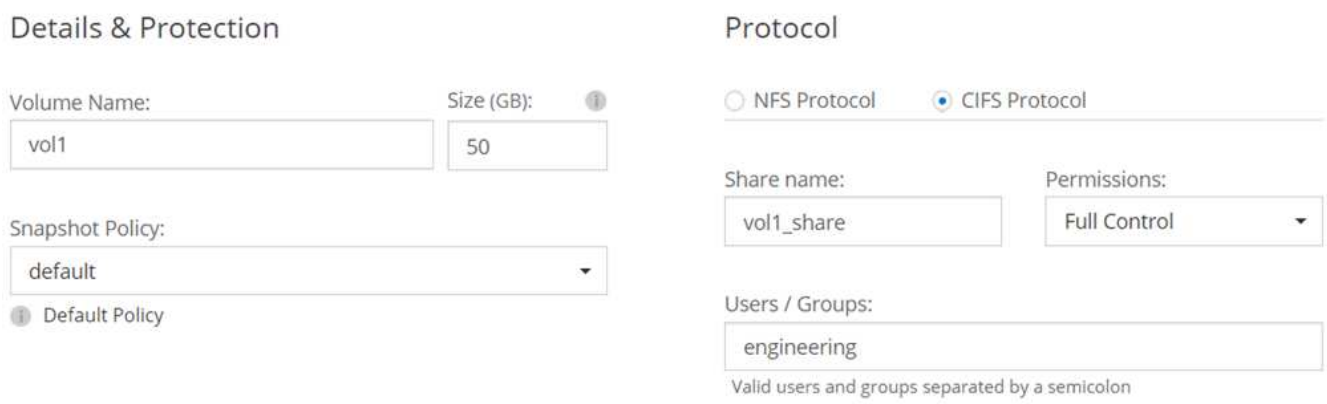
    Vous pouvez ignorer cette étape si vous souhaitez créer un volume pour iSCSI. Cloud Manager configure les volumes pour NFS et CIFS uniquement.

    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.

Champ	Description
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.

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.

Champ	Description
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 Tiering** : indiquez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifiez la règle de Tiering S3, 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 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".

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 **Créer Cloud Volumes ONTAP** et suivez les invites.
2. **Définir votre environnement de travail** : sélectionnez **Amazon Web Services** et **Cloud Volumes ONTAP HA**.
3. **Détails et informations d'identification** : modifiez éventuellement le compte AWS et l'abonnement Marketplace, 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
Compte	Vous pouvez choisir un autre compte si vous le souhaitez "Ajout de comptes AWS supplémentaires à Cloud Manager".
Abonnement Marketplace	Sélectionnez un autre abonnement si vous souhaitez modifier le compte AWS à partir duquel vous êtes facturé. Pour ajouter un nouvel abonnement, "Rendez-vous sur AWS Marketplace".
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".
Informations d'identification	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.

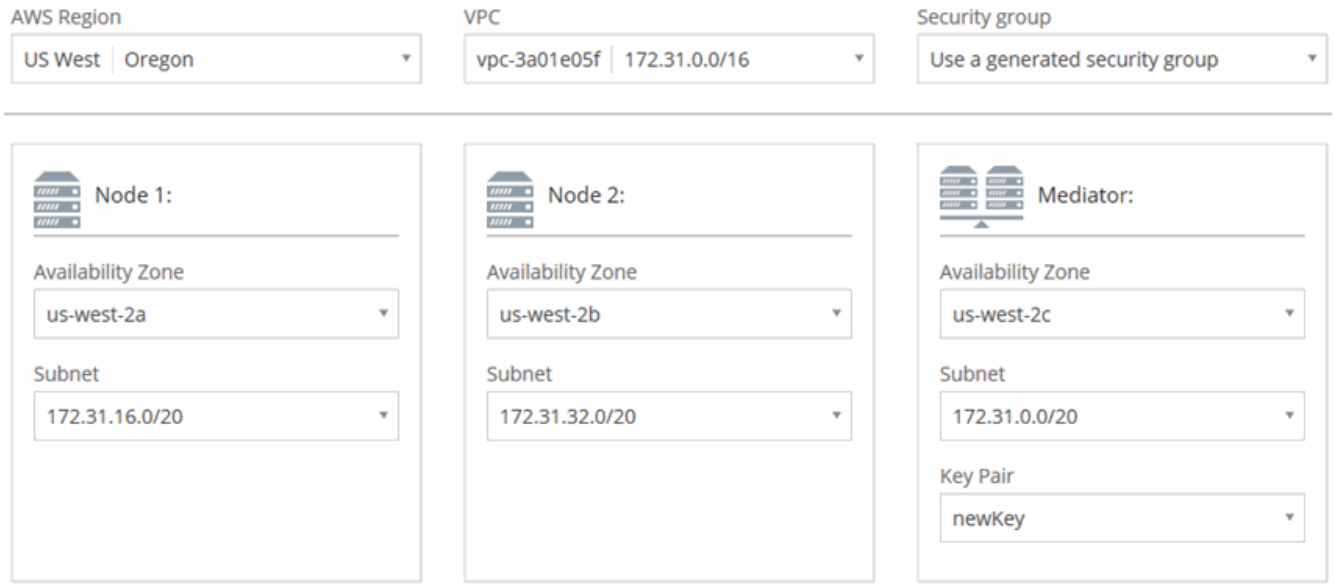
4. **Services** : conservez les services activés ou désactivez les services individuels que vous ne souhaitez pas utiliser avec ce système Cloud Volumes ONTAP.
   - "En savoir plus sur Backup vers S3".
   - "En savoir plus sur Cloud Compliance".

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 9.4 RC1 et 9.4 GA. La mise à jour ne se produit pas d'une version à une autre, par exemple de la version 9.3 à la version 9.4.

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 S3 doit être activée ou non.

    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".

16. **WORM** : activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

    "En savoir plus sur le stockage WORM".

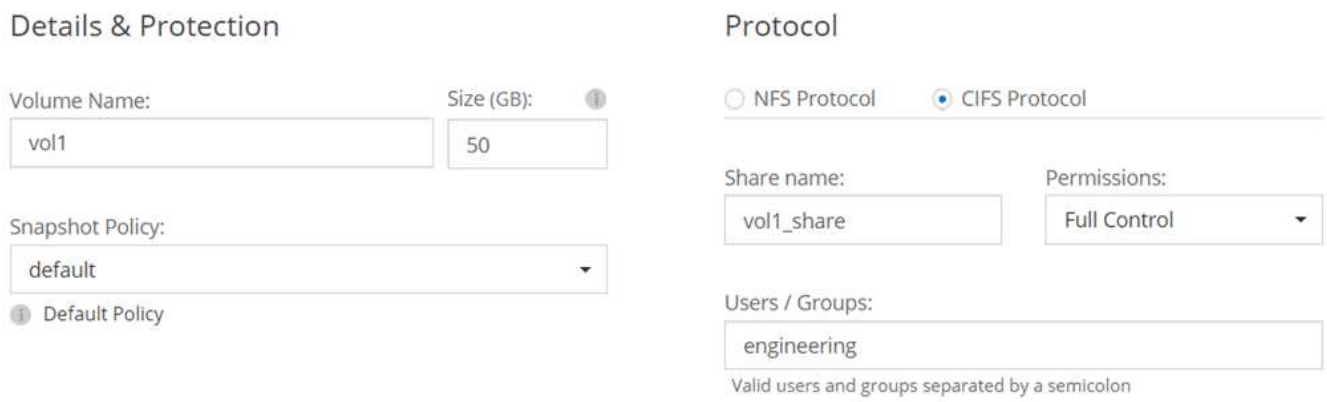
17. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

    Vous pouvez ignorer cette étape si vous souhaitez créer un volume pour iSCSI. Cloud Manager configure les volumes pour NFS et CIFS uniquement.

    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.

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.

Champ	Description
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 Tiering** : indiquez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifiez la règle de Tiering S3, 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.

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

- Assurez-vous que votre compte Azure dispose des autorisations requises, notamment si vous effectuez une mise à niveau à partir d'une version précédente et que vous déployez pour la première fois un système haute disponibilité.

  Les dernières autorisations figurent dans le "Politique NetApp Cloud Central pour Azure".

- 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.

Étapes

1. Sur la page environnements de travail, cliquez sur **Créer Cloud Volumes ONTAP** et suivez les invites.
2. **Définir votre environnement de travail** : sélectionnez **Microsoft Azure**, puis choisissez un nœud ou une paire haute disponibilité.
3. **Détails et informations d'identification** : modifiez éventuellement le compte ou l'abonnement Azure, spécifiez un nom de cluster et un nom 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
Changer de compte	Vous pouvez choisir un autre compte ou abonnement si vous le souhaitez "Configurez-les et ajoutez-les à Cloud Manager".
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.
Nom du groupe de ressources	Si vous décochez la case **utiliser par défaut**, vous pouvez entrer le nom d'un nouveau groupe de ressources. Si vous souhaitez utiliser un groupe de ressources existant, vous devez utiliser l'API.
Étiquettes	Les étiquettes sont des métadonnées pour vos ressources Azure. Cloud Manager ajoute les balises au système Cloud Volumes ONTAP et à chaque ressource Azure associée au système. 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".

Champ	Description
Informations d'identification	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.

4. **Services** : maintenir la conformité au cloud activée ou la désactiver si vous ne souhaitez pas l'utiliser avec ce système Cloud Volumes ONTAP.

   "En savoir plus sur Cloud Compliance".

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 9.5 RC1 et 9.5 GA est disponible. La mise à jour ne se produit pas d'une version à l'autre, par exemple de 9.4 à 9.5.

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.

    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".

11. **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".

    "En savoir plus sur le stockage WORM".

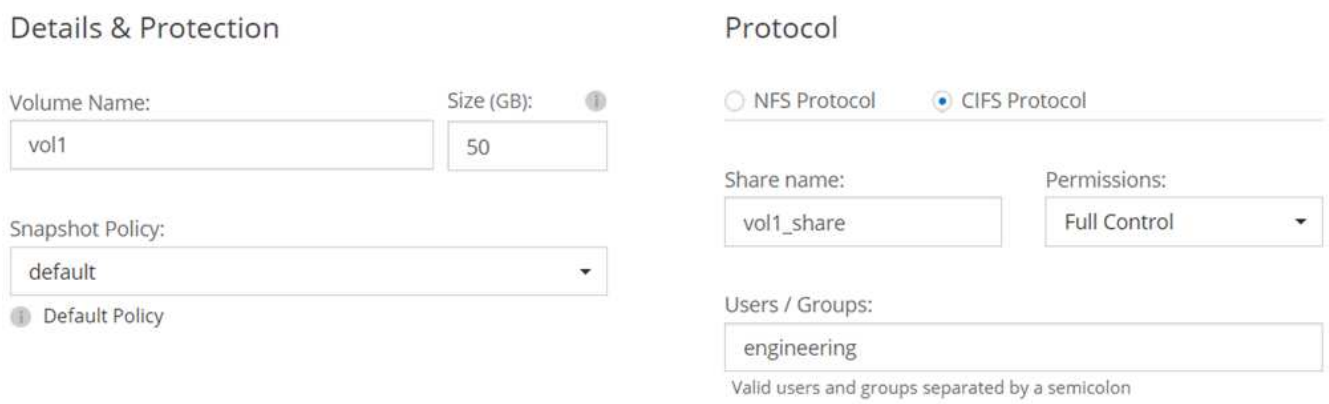
12. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

    Si vous souhaitez utiliser iSCSI, ignorez cette étape. Cloud Manager vous permet de créer des volumes pour NFS et CIFS uniquement.

    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.

    L'image suivante montre la page Volume remplie pour le protocole CIFS :



13. **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. 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.

14. **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, si nécessaire.

    Pour plus d'informations, voir "Présentation des profils d'utilisation des volumes" et "Vue d'ensemble du hiérarchisation des données".

15. **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.

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.

Avant de commencer

- 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.

Étapes

1. sur la page Working Environments, cliquez sur **Create Cloud Volumes ONTAP** et suivez les invites.
2. **Définir votre environnement de travail** : cliquez sur **Continuer**.
3. **Abonnez-vous à Cloud Volumes ONTAP**: Si vous y êtes invité, abonnez-vous à Cloud Volumes ONTAP sur le marché GCP.

   La vidéo suivante montre le processus d'abonnement :

   ► https://docs.netapp.com/fr-fr/occm37//media/video_subscribing_gcp.mp4 *(video)*

4. **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
Projet Google Cloud	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 4b de cette page".
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.
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".
Informations d'identification	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.

5. **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".

6. **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".

7. **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.

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 9.5 RC1 et 9.5 GA est disponible. La mise à jour ne se produit pas d'une version à l'autre, par exemple de 9.4 à 9.5.

9. **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.

   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".

10. **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.

    "En savoir plus sur la vitesse d'écriture".

    "En savoir plus sur le stockage WORM".

11. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

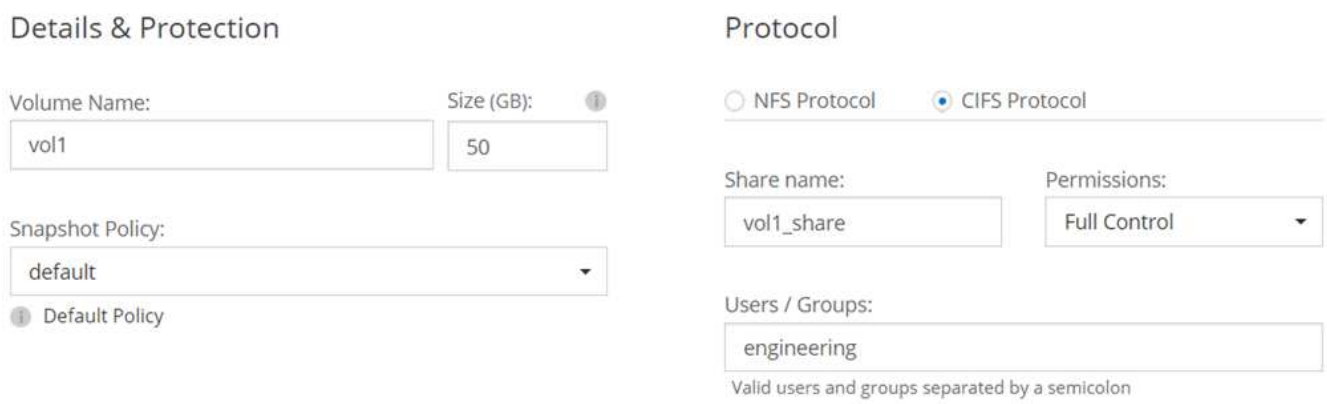
    Si vous souhaitez utiliser iSCSI, ignorez cette étape. Cloud Manager vous permet de créer des volumes pour NFS et CIFS uniquement.

    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.

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.
Unité organisationnelle	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers.

Champ	Description
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, si nécessaire.

    Pour plus d'informations, voir "Présentation des profils d'utilisation des volumes" et "Vue d'ensemble du hiérarchisation des données".

14. **Compte Google Cloud Platform pour le Tiering des données** : configurez le Tiering des données en fournissant des clés d'accès au stockage interopérables pour un compte Google Cloud Platform. Cliquez sur **Ignorer** pour désactiver la hiérarchisation des données.

    Les clés permettent à Cloud Manager de configurer un compartiment Cloud Storage pour le Tiering des données. Pour plus de détails, voir "Configuration et ajout de comptes GCP dans Cloud Manager".

15. **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.

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** :

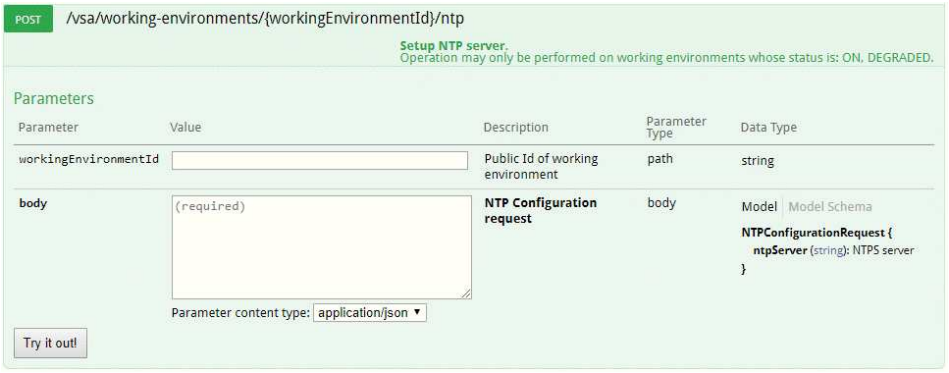
4. Sélectionnez un compte sur le site de support NetApp et cliquez sur **Register**.

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".
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".

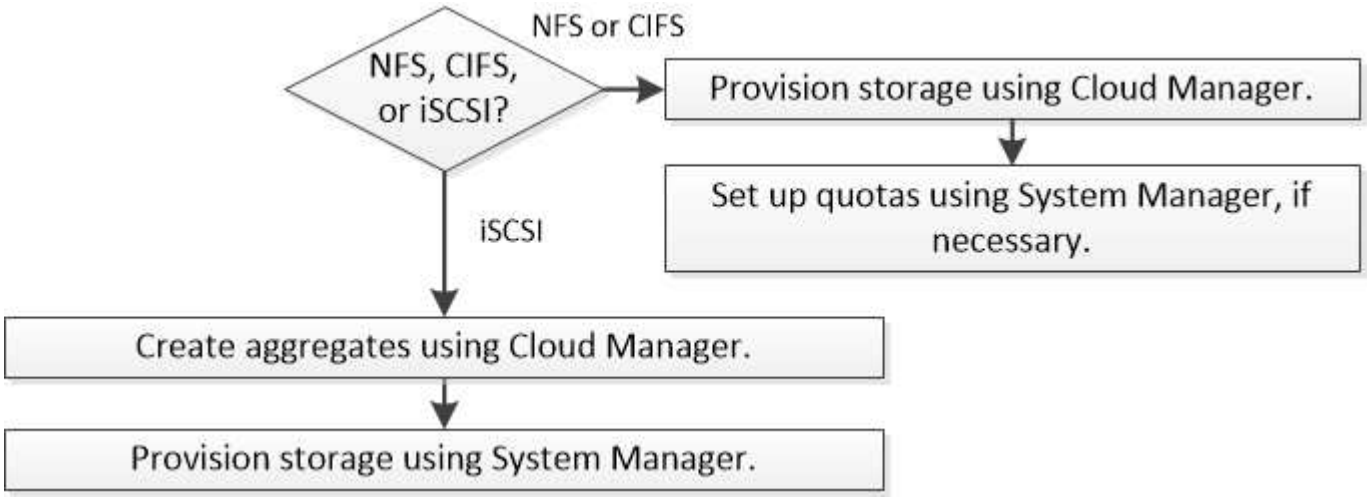
Tâche	Description
Facultatif : créez une interface réseau de gestion SVM (LIF) pour les systèmes HA dans plusieurs zones de disponibilité AWS	Une interface de réseau de gestion de machine virtuelle de stockage (LIF) est requise si vous souhaitez utiliser SnapCenter ou SnapDrive pour Windows avec une 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 Cloud Manager 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".

Provisionner le stockage

Provisionnement du stockage

Vous pouvez provisionner un stockage NFS et CIFS supplémentaire pour vos systèmes Cloud Volumes ONTAP à partir de Cloud Manager en gérant les volumes et les agrégats. Si vous devez créer du stockage iSCSI, vous devez le faire à partir de System Manager.

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 ou CIFS à partir de Cloud Manager.

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**.

Action	Étapes
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.
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.

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.

Champ	Description
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. • 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**.

Provisionnement des LUN iSCSI

Si vous souhaitez créer des LUN iSCSI, vous devez le faire à partir de System Manager.

Avant de commencer

- Les utilitaires hôte doivent être installés et configurés sur les hôtes qui se connectent à la LUN.
- Vous devez avoir enregistré le nom de l'initiateur iSCSI à partir de l'hôte. Vous devez fournir ce nom lorsque vous créez un groupe d'identifiants pour la LUN.
- Avant de créer des volumes dans System Manager, vous devez vous assurer que vous disposez d'un agrégat avec suffisamment d'espace. Vous devez créer des agrégats dans Cloud Manager. Pour plus de

détails, voir "Création d'agrégats".

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".
2. Cliquez sur **stockage > LUN**.
3. Cliquez sur **Créer** et suivez les invites pour créer la LUN.
4. Connectez-vous à la LUN à partir de vos hôtes.

   Pour obtenir des instructions, reportez-vous au "Documentation Host Utilities" pour votre système d'exploitation.

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.

Tiering des données inactives vers un stockage objet à faible coût

Vous pouvez réduire les coûts de stockage 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 ajouter un compte GCP à Cloud Manager et configurer le sous-réseau pour Private Google Access. 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

- Vous devez ajouter un compte Google Cloud Platform à Cloud Manager en saisissant des clés d'accès de stockage pour un compte de service. Les clés permettent à Cloud Manager de configurer un compartiment Cloud Storage pour le Tiering des données. Pour obtenir des instructions, reportez-vous à la section "Configuration et ajout de comptes GCP dans Cloud Manager".
- 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".

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

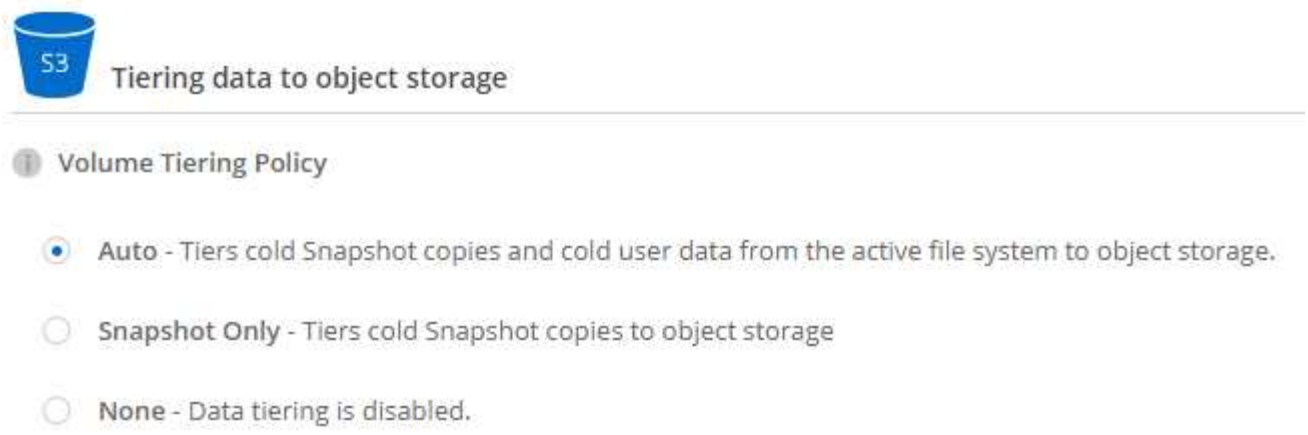
1. Dans l'environnement de travail, créez un nouveau volume ou modifiez le niveau d'un volume existant :

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 la stratégie Snapshot Only ou Auto.

   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 du niveau de Tiering dans AWS ou Azure

Lorsque vous activez le Tiering des données, Cloud Volumes ONTAP transfère les données inactives vers la classe de stockage S3 *Standard* dans AWS ou vers le Tier de stockage *hot* dans Azure. Une fois déployé Cloud Volumes ONTAP, vous pouvez réduire les coûts de stockage en modifiant le niveau de Tiering des

données inactives inutilisées depuis 30 jours. Les coûts d'accès sont plus élevés si vous accédez aux données. Vous devez donc en tenir compte avant de modifier le niveau de hiérarchisation.

> Vous ne pouvez pas modifier le niveau de hiérarchisation dans GCP, car seule la classe de stockage *régionale* est actuellement prise en charge.

Description de la tâche

Le niveau de hiérarchisation est large du système : il n'est pas par volume.

Dans AWS, vous pouvez modifier le niveau de Tiering afin que les données inactives soient déplacées vers l'une des classes de stockage suivantes après 30 jours d'inactivité :

- Hiérarchisation intelligente
- Accès autonome et peu fréquent
- Un seul accès à Zone-Infrequent

Dans Azure, vous pouvez modifier le niveau de Tiering afin que les données inactives soient déplacées vers le niveau de stockage *cool* après 30 jours d'inactivité.

Pour plus d'informations sur le fonctionnement des niveaux de hiérarchisation, voir "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 S3** ou **stockage Blob Storage Tiering**.
2. Choisissez le niveau de hiérarchisation, puis cliquez sur **Enregistrer**.

Avec ONTAP comme stockage persistant pour Kubernetes

Cloud Manager peut automatiser le déploiement de "NetApp Trident" Sur les clusters Kubernetes, vous pouvez utiliser ONTAP comme stockage persistant pour les conteneurs. Ceci fonctionne avec Cloud Volumes ONTAP et les clusters ONTAP sur site.

Avant d'effectuer ces étapes, vous devez "Créer un système Cloud Volumes ONTAP" ou "Découvrez un cluster ONTAP sur site" Depuis Cloud Manager.

Si vous déployez des clusters Kubernetes à l'aide du "NetApp Kubernetes Service", Cloud Manager peut détecter automatiquement les clusters à partir de votre compte NetApp Cloud Central. Si c'est le cas, ignorez les deux premières étapes et commencez par l'étape 3.

1 Vérifiez la connectivité réseau

1. Une connexion réseau doit être disponible entre Cloud Manager et les clusters Kubernetes, et depuis les clusters Kubernetes vers les systèmes ONTAP.
2. Lors de l'installation de Trident, Cloud Manager requiert une connexion Internet sortante pour accéder aux terminaux suivants :

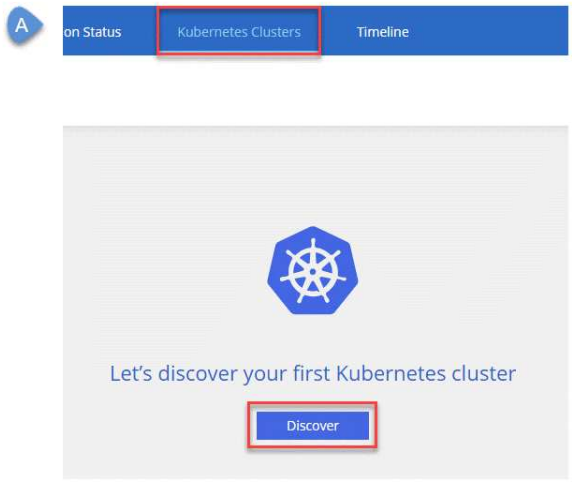
   https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/

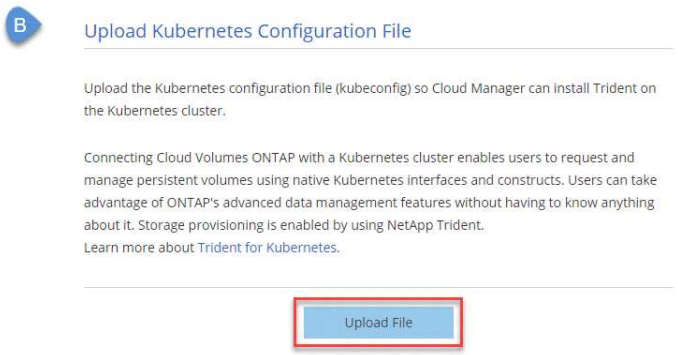
Cloud Manager installe Trident sur un cluster Kubernetes lorsque vous connectez un environnement de travail au cluster.

Téléchargez les fichiers de configuration Kubernetes dans Cloud Manager

Pour chaque cluster Kubernetes, l'administrateur du compte doit télécharger un fichier de configuration (kubeconfig) au format YAML. Une fois le fichier téléchargé, Cloud Manager vérifie la connexion au cluster et enregistre une copie chiffrée du fichier kubeconfig.

Cliquez sur **clusters Kubernetes > découvrir > Télécharger le fichier** et sélectionnez le fichier kubeconfig.

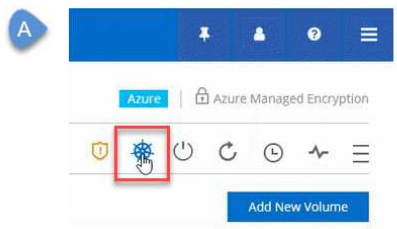


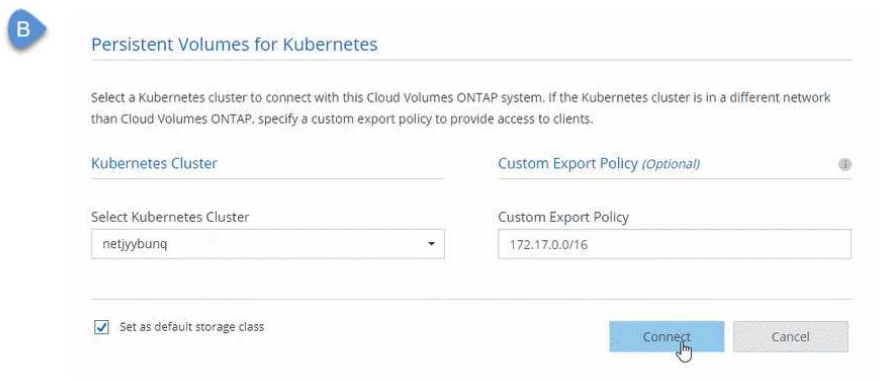


Connectez vos environnements de travail aux clusters Kubernetes

Dans l'environnement de travail, cliquez sur l'icône Kubernetes et suivez les invites. Vous pouvez connecter différents clusters à différents systèmes ONTAP et plusieurs clusters au même système ONTAP.

Vous avez la possibilité de définir la classe de stockage NetApp comme classe de stockage par défaut pour le cluster Kubernetes. Lorsqu'un utilisateur crée un volume persistant, le cluster Kubernetes peut utiliser par défaut les systèmes ONTAP connectés comme stockage back-end.





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 quatre classes de stockage Kubernetes que vous pouvez utiliser pour le provisionnement des volumes persistants :

- **netapp-fichier** : pour liaison de volumes persistants aux systèmes ONTAP à un seul nœud
- **netapp-file-san** : pour les volumes persistants iSCSI sur des systèmes ONTAP à un seul nœud
- **netapp-file-redondant** : pour la liaison de volumes persistants aux paires HA ONTAP
- **netapp-file-redondant-san** : pour la liaison de volumes persistants iSCSI aux paires HA ONTAP

Cloud Manager configure Trident pour qu'il utilise par défaut les options de provisionnement suivantes :

- Volumes fins
- La règle Snapshot par défaut
- Répertoire Snapshot accessible

"En savoir plus sur le provisionnement de votre premier volume avec Trident pour Kubernetes"

Qu'est-ce que les volumes trident_trident ?

Cloud Manager crée un volume sur le premier système ONTAP que vous connectez à un cluster Kubernetes. Le nom du volume est ajouté à «_trident_trident ». ONTAP utilise ce volume pour se connecter au cluster Kubernetes. Vous ne devez pas supprimer ces volumes.

Que se passe-t-il lorsque vous déconnectez ou supprimez un cluster Kubernetes ?

Cloud Manager vous permet de déconnecter des systèmes ONTAP individuels d'un cluster Kubernetes. Lorsque vous déconnectez un système, vous ne pouvez plus l'utiliser ONTAP comme stockage persistant pour les conteneurs. Les volumes persistants existants ne sont pas supprimés.

Une fois que vous avez déconnecté tous les systèmes d'un cluster Kubernetes, vous pouvez également supprimer l'intégralité de la configuration Kubernetes de Cloud Manager. Cloud Manager ne désinstalle pas Trident lorsque vous supprimez le cluster et ne supprime aucun volume persistant.

Ces deux actions sont disponibles via des API uniquement. Nous prévoyons d'ajouter les actions à l'interface dans une prochaine version."Cliquez ici pour plus d'informations sur les API".

Chiffrement de volumes avec NetApp Volume Encryption

NetApp Volume Encryption (NVE) est une technologie logicielle de chiffrement des données au repos d'un volume à la fois. Les données, les copies Snapshot et les métadonnées sont chiffrées. L'accès aux données est donné par une clé XTS-AES-256 unique, une par volume.

Description de la tâche

- 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.

- Pour l'instant, Cloud Volumes ONTAP prend en charge NetApp Volume Encryption avec un serveur de gestion externe des clés. Un gestionnaire de clés intégré n'est pas pris en charge.
- Vous devez configurer NetApp Volume Encryption à partir de l'interface de ligne de commande d'ONTAP.

  Vous pouvez ensuite utiliser soit l'interface de ligne de commandes, soit System Manager pour activer le chiffrement sur des volumes spécifiques. Cloud Manager ne prend pas en charge NetApp Volume Encryption à partir de son interface utilisateur et de ses API.

"En savoir plus sur les technologies de cryptage prises en charge".

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"

4. Créez un nouveau volume chiffré ou convertissez un volume non chiffré existant à l'aide de l'interface de ligne de commande ou de System Manager.
   - CLI :
     - Pour les nouveaux volumes, utilisez la commande **volume create** avec le paramètre -crypt.

       "Guide d'alimentation de ONTAP 9 NetApp Encryption : activation du chiffrement sur un nouveau volume"

     - Pour les volumes existants, utilisez la commande **Volume Encryption conversion start**.

       "Guide d'alimentation du chiffrement NetApp ONTAP 9 : activation du chiffrement sur un volume existant à l'aide de la commande de démarrage de la conversion du chiffrement de volume"

   - System Manager :
     - Pour les nouveaux volumes, cliquez sur **stockage > volumes > Créer > Créer FlexVol**, puis sélectionnez **crypté**.

       "ONTAP 9 gestion des clusters à l'aide de System Manager : création de volumes FlexVol"

     - Pour les volumes existants, sélectionnez le volume, cliquez sur **Modifier**, puis sélectionnez **crypté**.

       "ONTAP 9 gestion des clusters à l'aide de System Manager : modification des propriétés de

volume"

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 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.
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**.

Tâche	Action
Obtenez la commande NFS mount	a. Sélectionnez un volume, puis cliquez sur **Mount Command**. b. Cliquez sur **Copier**.
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.
Activer ou désactiver la synchronisation vers S3 pour un volume	Sélectionnez un volume, puis cliquez sur **Synchroniser avec S3** ou sur **Supprimer la relation de synchronisation**. La fonction de synchronisation vers S3 doit être activée avant de pouvoir utiliser ces options. Pour obtenir des instructions, reportez-vous à la section "Synchronisation des données vers AWS S3"
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.

Tâche	Action
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 pour éviter les problèmes de capacité

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.

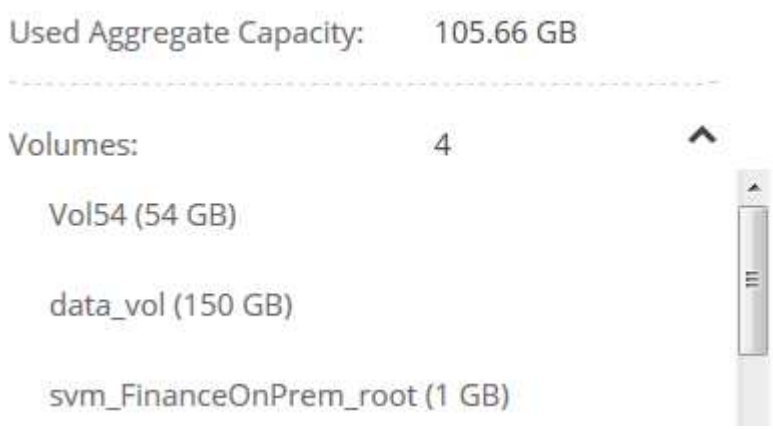
Étapes

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.

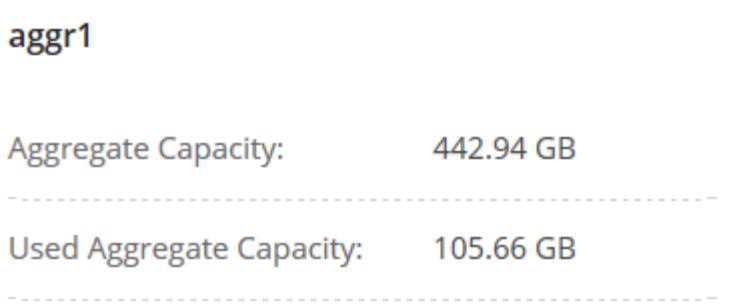
Description de la tâche

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".

Réplication et protection des données

Détection et gestion 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. La découverte de ces clusters vous permet de répliquer facilement des données dans votre environnement cloud hybride directement à partir de Cloud Manager.

Découverte des clusters ONTAP

La découverte d'un cluster ONTAP dans Cloud Manager vous permet de provisionner du stockage et de répliquer des données sur votre cloud hybride.

Avant de commencer

Pour ajouter le cluster à Cloud Manager, vous devez disposer de l'adresse IP de gestion du cluster et du mot de passe du compte utilisateur admin.

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 Cloud Manager doit autoriser l'accès HTTPS sortant via le port 443.

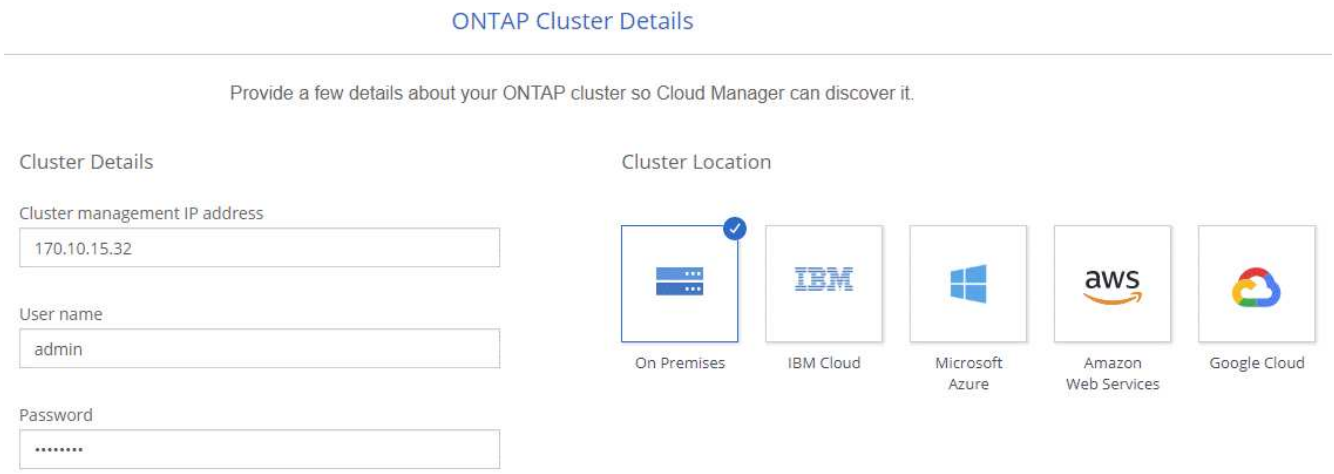
  Si Cloud Manager est dans AWS, toutes les communications sortantes sont autorisées par le groupe de sécurité prédéfini.

- 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 stratégie et activer l'accès à partir de l'hôte Cloud Manager.

Étapes

1. Sur la page environnements de travail, cliquez sur **découvrir** et sélectionnez **Cluster ONTAP**.
2. 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.



3. 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 des données vers et depuis le cluster et lancer OnCommand System Manager pour effectuer des tâches avancées.

Provisionnement des volumes sur des clusters ONTAP

Cloud Manager vous permet de provisionner des volumes NFS et CIFS sur des clusters ONTAP.

Avant de commencer

NFS ou CIFS doivent être configurés sur le cluster. Vous pouvez configurer NFS et CIFS à l'aide de System Manager ou de l'interface de ligne de commande.

Description de la tâche

Vous pouvez créer des volumes sur des agrégats existants. Vous ne pouvez pas créer de nouveaux agrégats à partir de 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.
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.
Profil d'utilisation	Les profils d'utilisation définissent les fonctionnalités d'efficacité du stockage NetApp qui sont activées pour un volume.
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.

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.

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 10000, 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

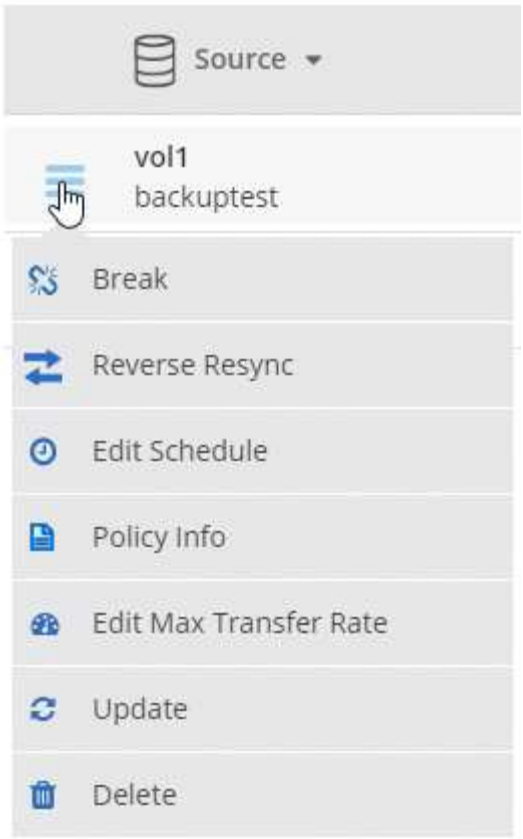
1. Sur la page environnements de travail, affichez l'état de réplication de tous les environnements de travail de l'espace de travail ou d'un environnement de travail spécifique :

Option	Action
Tous les environnements de travail de l'espace de travail	En haut de Cloud Manager, cliquez sur **Replication Status**.
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.
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.

Action	Description
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.

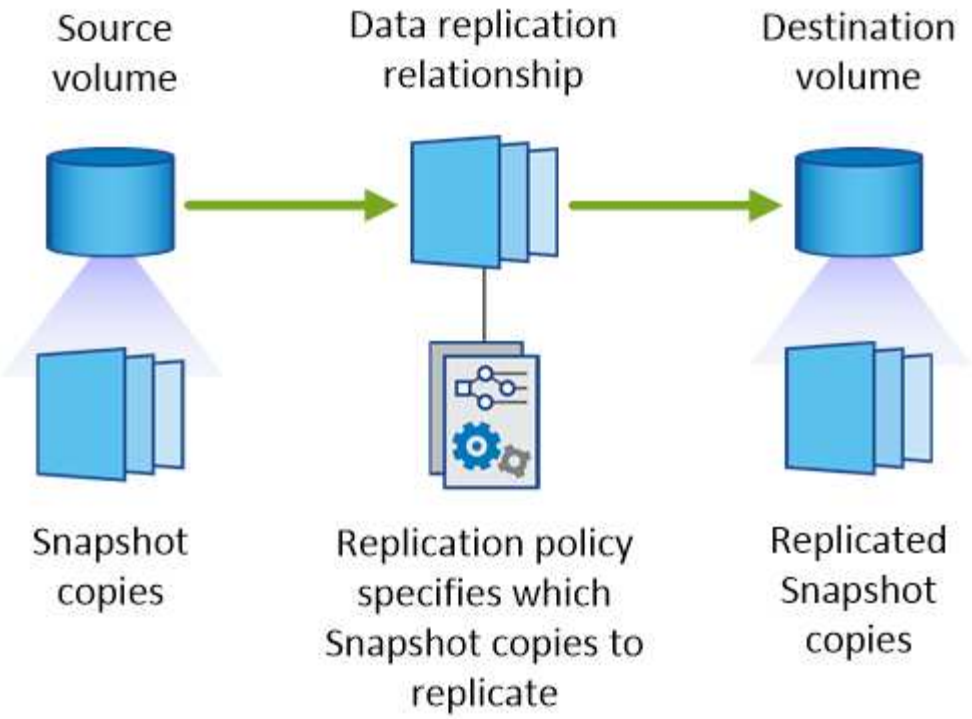
Quelles sont les règles de réplication

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.

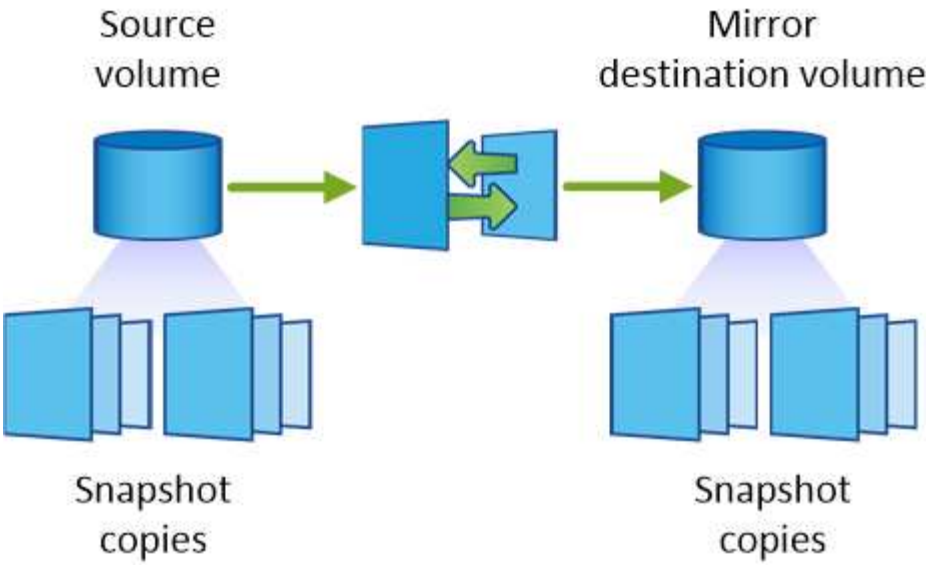
- Une règle *Backup* réplique des copies Snapshot spécifiques sur un volume de destination et les conserve généralement pendant une période plus longue que sur le volume source.

  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.

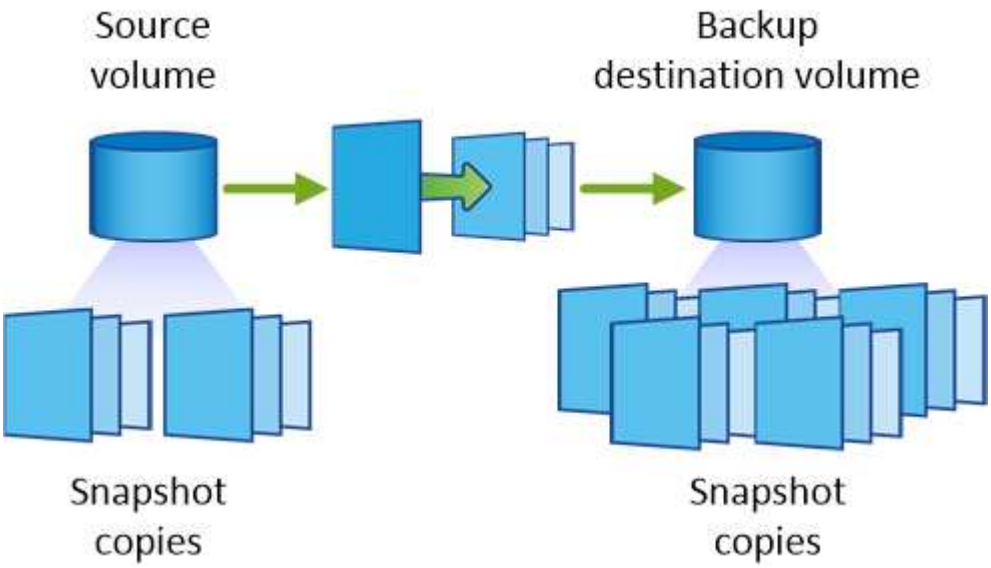
- Une politique *Mirror et Backup* permet la reprise sur incident et la conservation à long terme.

  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.

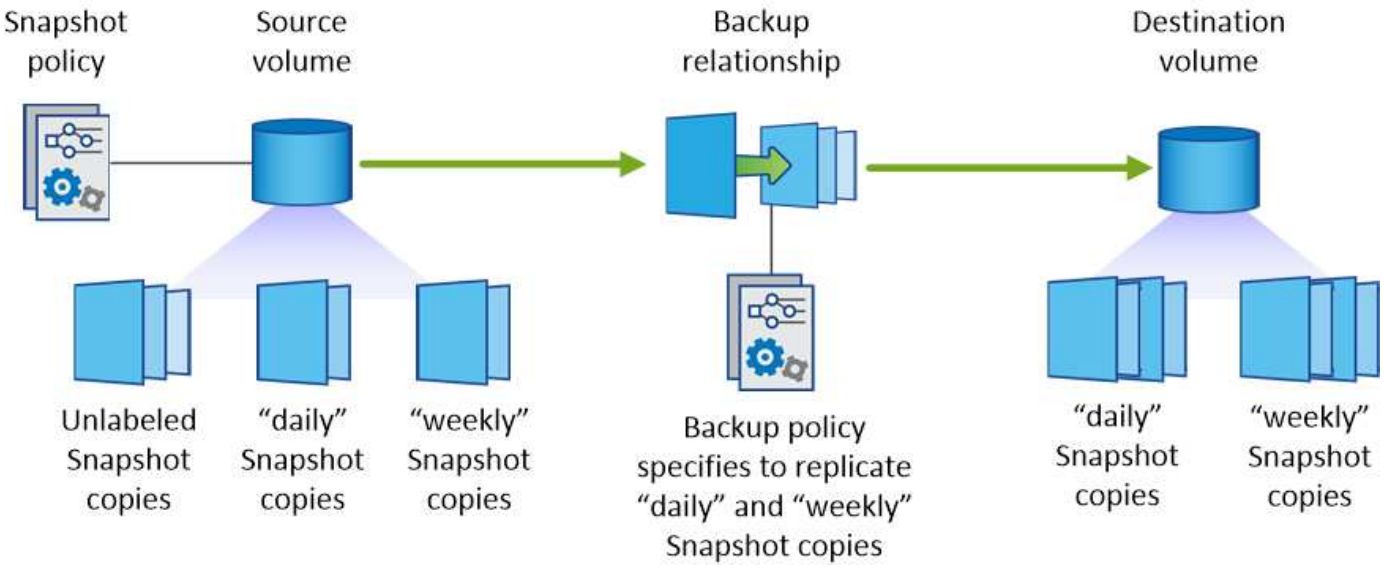
Comprendre la relation entre les étiquettes de copie Snapshot et les stratégies de sauvegarde

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.

Sauvegarde des données dans Amazon S3

Il s'agit d'une fonctionnalité complémentaire pour Cloud Volumes ONTAP offrant des fonctionnalités de sauvegarde et de restauration entièrement gérées pour la protection, ainsi que pour l'archivage à long terme de vos données cloud. Les sauvegardes sont stockées dans le stockage objet S3, indépendamment des copies Snapshot des volumes utilisées pour la restauration ou le clonage à court terme.

Lorsque vous activez Backup vers S3, le service effectue une sauvegarde complète de vos données. Toutes les sauvegardes supplémentaires sont incrémentielles, ce qui signifie que seuls les blocs modifiés et les nouveaux blocs sont sauvegardés.

"Rendez-vous sur NetApp Cloud Central pour plus d'informations sur les tarifs".

Notez que vous devez utiliser Cloud Manager pour toutes les opérations de sauvegarde et de restauration. Toute action effectuée directement depuis ONTAP ou depuis Amazon S3 entraîne une configuration non prise en charge.

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

Vérifiez les points suivants :

- Cloud Volumes ONTAP 9.4 ou version ultérieure s'exécute dans une région AWS prise en charge : N. Virginie, Oregon, Irlande, Francfort ou Sydney
- Vous êtes abonné au nouveau "Offre Cloud Manager Marketplace"
- Le port TCP 5010 est ouvert pour le trafic sortant sur le groupe de sécurité pour Cloud Volumes ONTAP (ouvert par défaut)
- Le port TCP 8088 est ouvert pour le trafic sortant sur le groupe de sécurité pour Cloud Manager (ouvert par défaut).
- Le terminal suivant est accessible depuis Cloud Manager :

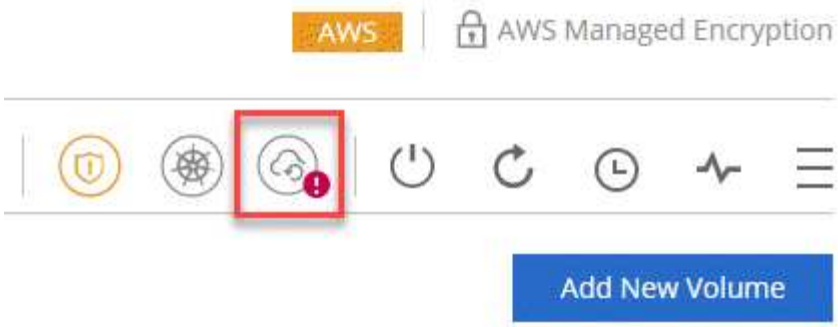
  https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist

- Cloud Manager peut allouer jusqu'à deux terminaux VPC d'interface dans le VPC (la limite AWS par VPC est de 20)
- Cloud Manager est autorisé à utiliser les autorisations du terminal VPC indiquées dans les dernières versions "Politique de Cloud Manager":

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

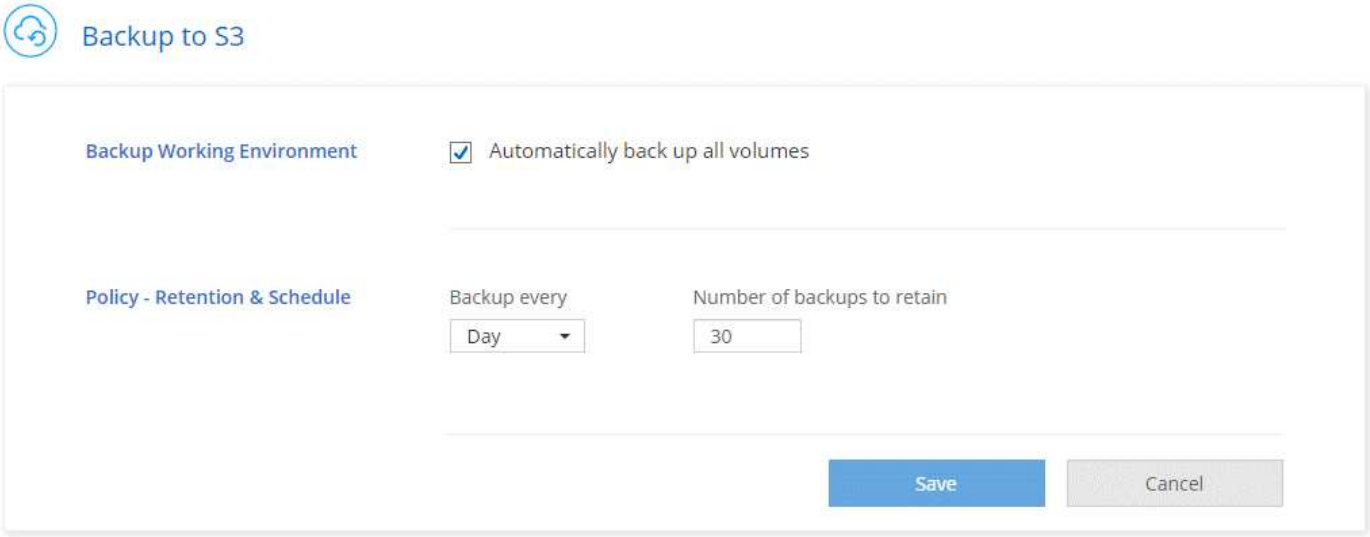
Activation de Backup vers S3 sur votre système nouveau ou existant

- Nouveaux systèmes : la fonctionnalité Backup vers S3 est activée par défaut dans l'assistant de l'environnement de travail. Assurez-vous de conserver l'option activée.
- Systèmes existants : ouvrez l'environnement de travail, cliquez sur l'icône des paramètres de sauvegarde et activez les sauvegardes.



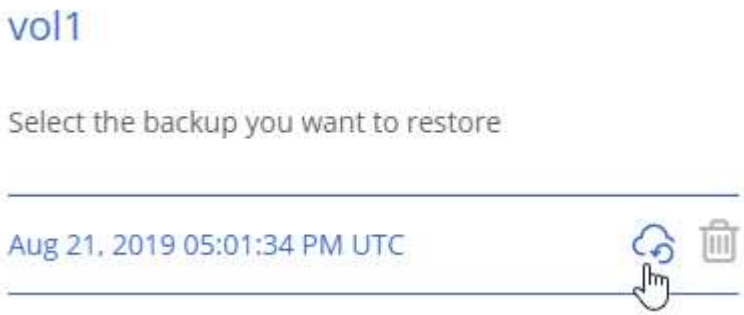
Si nécessaire, modifiez la stratégie de sauvegarde

La règle par défaut sauvegarde les volumes tous les jours et conserve 30 copies de sauvegarde de chaque volume. Si nécessaire, vous pouvez modifier le nombre de copies de sauvegarde à conserver.



Restaurez vos données à la demande

En haut de Cloud Manager, cliquez sur **Backup & Restore**, 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 Volume ONTAP 9.4 et versions ultérieures prennent en charge la sauvegarde vers S3.

Régions AWS prises en charge

La sauvegarde sur S3 est prise en charge avec Cloud Volumes ONTAP dans les régions AWS suivantes :

- US East (N. Virginie)
- US West (Oregon)
- UE (Irlande)
- UE (Francfort)
- Asie-Pacifique (Sydney)

Autorisations AWS requises

Le rôle IAM qui fournit les autorisations à Cloud Manager doit inclure les éléments suivants :

```
"ec2:DescribeVpcEndpoints",
"ec2:CreateVpcEndpoint",
"ec2:ModifyVpcEndpoint",
"ec2:DeleteVpcEndpoints"
```

Obligation d'abonnement AWS

Un nouvel abonnement Cloud Manager est disponible dans AWS Marketplace depuis la version 3.7.3. Cet abonnement permet de déployer des systèmes Cloud Volumes ONTAP 9.6 et versions ultérieures, de PAYGO et la fonctionnalité Backup vers S3. Vous devez le faire "Abonnez-vous à ce nouvel abonnement Cloud Manager" Avant d'activer Backup vers S3. La facturation de la fonctionnalité Backup to S3 se fait via cet abonnement.

Configuration requise pour les ports

- Le port TCP 5010 doit être ouvert pour le trafic sortant de Cloud Volumes ONTAP vers le service de sauvegarde.
- Le port TCP 8088 doit être ouvert pour le trafic sortant sur le groupe de sécurité pour Cloud Manager.

  Ces ports sont déjà ouverts si vous utilisez les groupes de sécurité prédéfinis. Mais si vous avez utilisé votre propre, alors vous devrez ouvrir ces ports.

Accès Internet sortant

Vérifiez que le terminal suivant est accessible depuis Cloud Manager : https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist

Cloud Manager contacte ce terminal pour ajouter votre ID de compte AWS à la liste des utilisateurs autorisés pour Backup vers S3.

Interface des terminaux VPC

Lorsque vous activez la fonctionnalité Backup vers S3, Cloud Manager crée un terminal VPC d'interface dans le VPC où Cloud Volumes ONTAP s'exécute. Ce *point de terminaison* de sauvegarde se connecte au VPC NetApp où Backup vers S3 est exécuté. Si vous restaurez un volume, Cloud Manager crée un terminal VPC d'interface supplémentaire, le *restore Endpoint*.

Les systèmes Cloud Volumes ONTAP supplémentaires du VPC utilisent ces deux terminaux VPC.

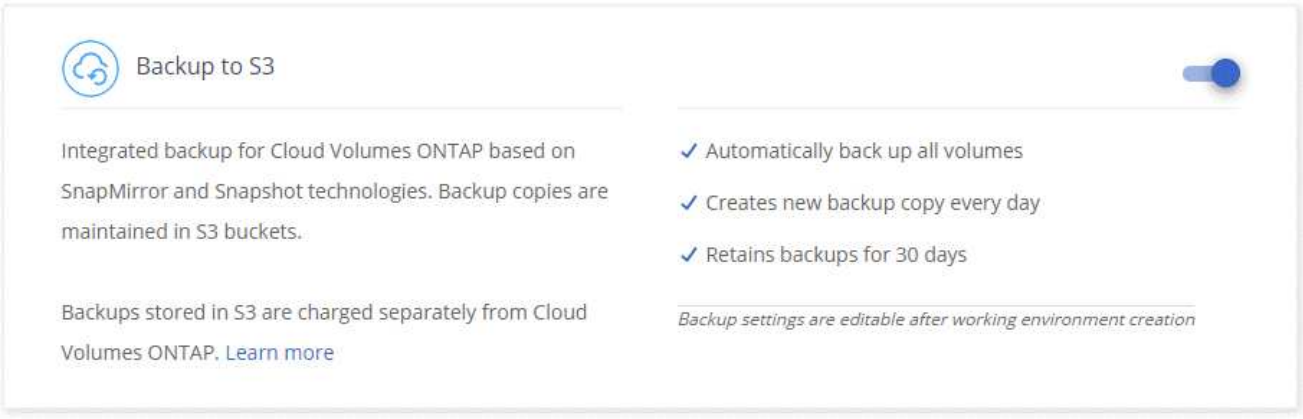
"La limite par défaut des terminaux VPC de l'interface est de 20 par VPC". Assurez-vous que votre VPC n'a pas atteint la limite avant d'activer la fonctionnalité.

Activation des sauvegardes dans S3 sur un nouveau système

La fonctionnalité Backup to S3 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 sauvegarde vers S3, laissez la fonction activée et cliquez sur **Continuer**.



5. Complétez les pages de l'assistant pour déployer le système.

Résultat

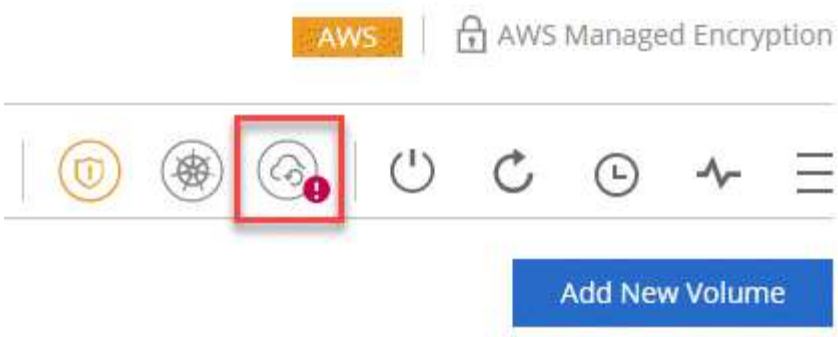
La fonctionnalité de sauvegarde sur S3 est activée sur le système. Elle sauvegarde les volumes tous les jours et conserve 30 copies de sauvegarde. Découvrez comment modifier la conservation des sauvegardes.

Activation des sauvegardes dans S3 sur un système existant

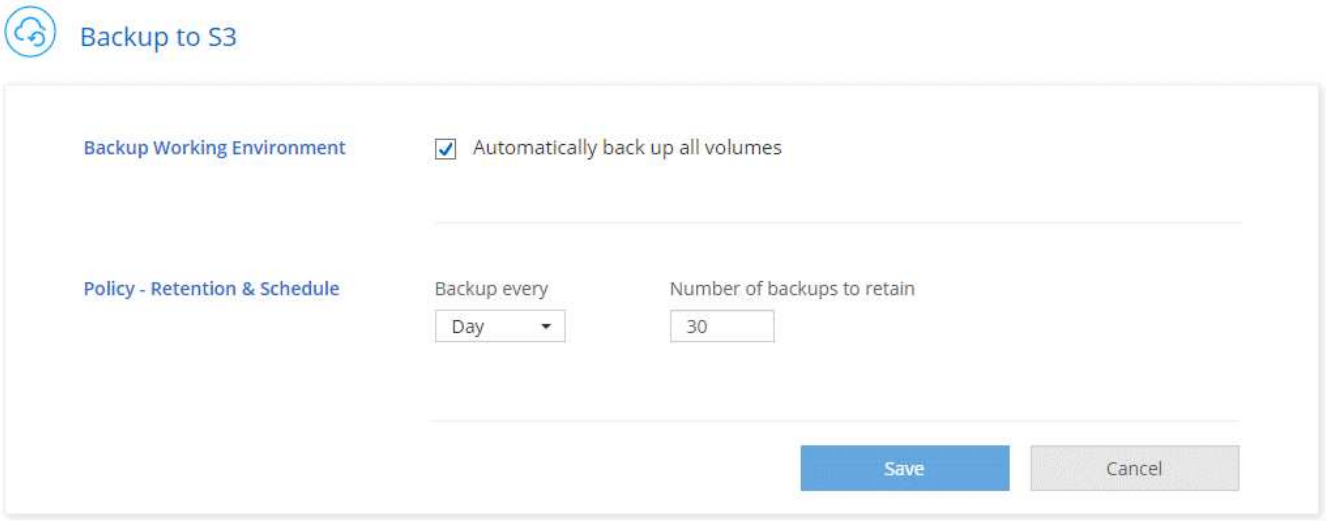
Vous pouvez activer les sauvegardes sur S3 sur un système Cloud Volumes ONTAP existant, tant que vous n'avez pas exécuté de configuration prise en charge. Pour plus de détails, voir De formation.

Étapes

1. Ouvrir l'environnement de travail.
2. Cliquez sur l'icône des paramètres de sauvegarde.



3. Sélectionnez **sauvegarder automatiquement tous les volumes**.
4. Choisissez la conservation de votre sauvegarde, puis cliquez sur **Enregistrer**.



Résultat

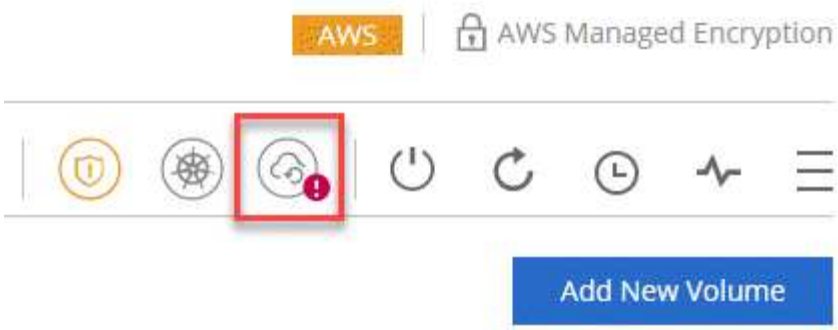
La fonctionnalité Backup vers S3 commence à effectuer les sauvegardes initiales de chaque volume.

Modification de la conservation des sauvegardes

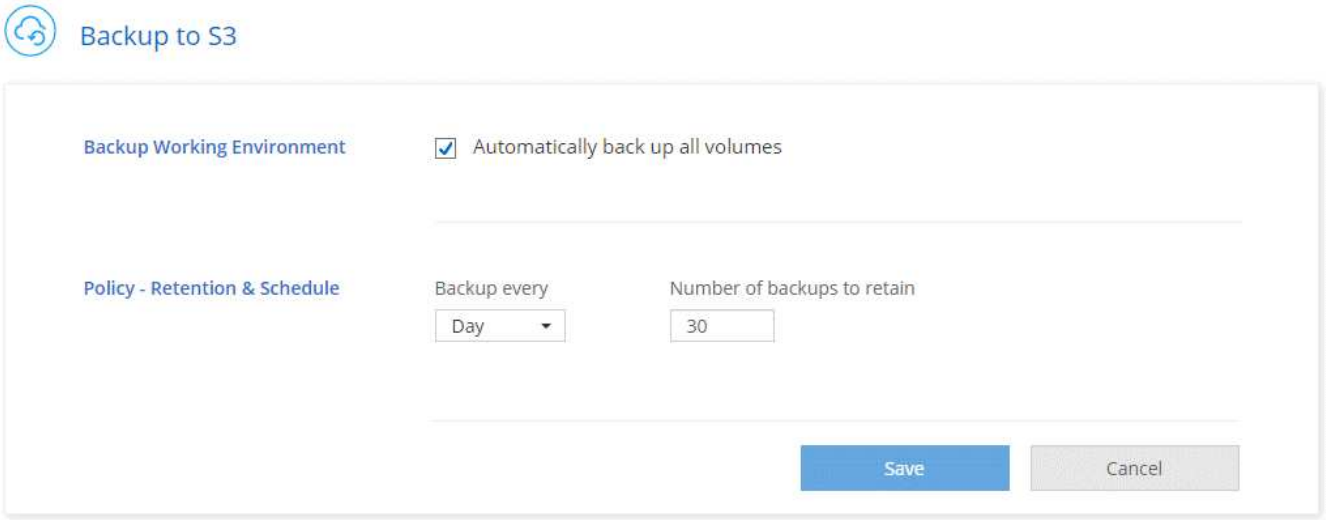
La règle par défaut sauvegarde les volumes tous les jours et conserve 30 copies de sauvegarde de chaque volume. Vous pouvez modifier le nombre de copies de sauvegarde à conserver.

Étapes

1. Ouvrir l'environnement de travail.
2. Cliquez sur l'icône des paramètres de sauvegarde.



3. Modifiez la rétention de la sauvegarde, puis cliquez sur **Enregistrer**.



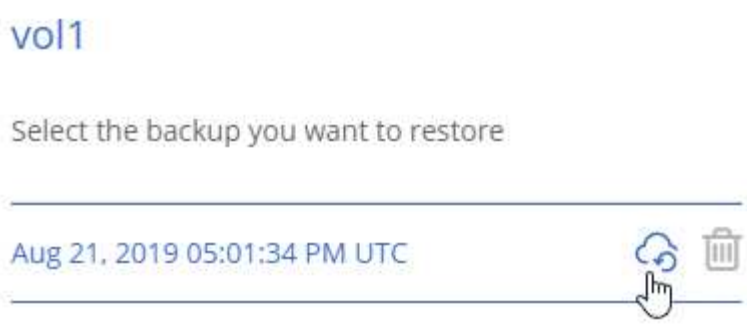
Restauration d'un volume

Lorsque vous restaurez les données à partir d'une sauvegarde, Cloud Manager effectue une restauration de volume complet vers un *nouveau* volume. Vous pouvez restaurer les données dans le même environnement de travail ou dans un autre environnement de travail.

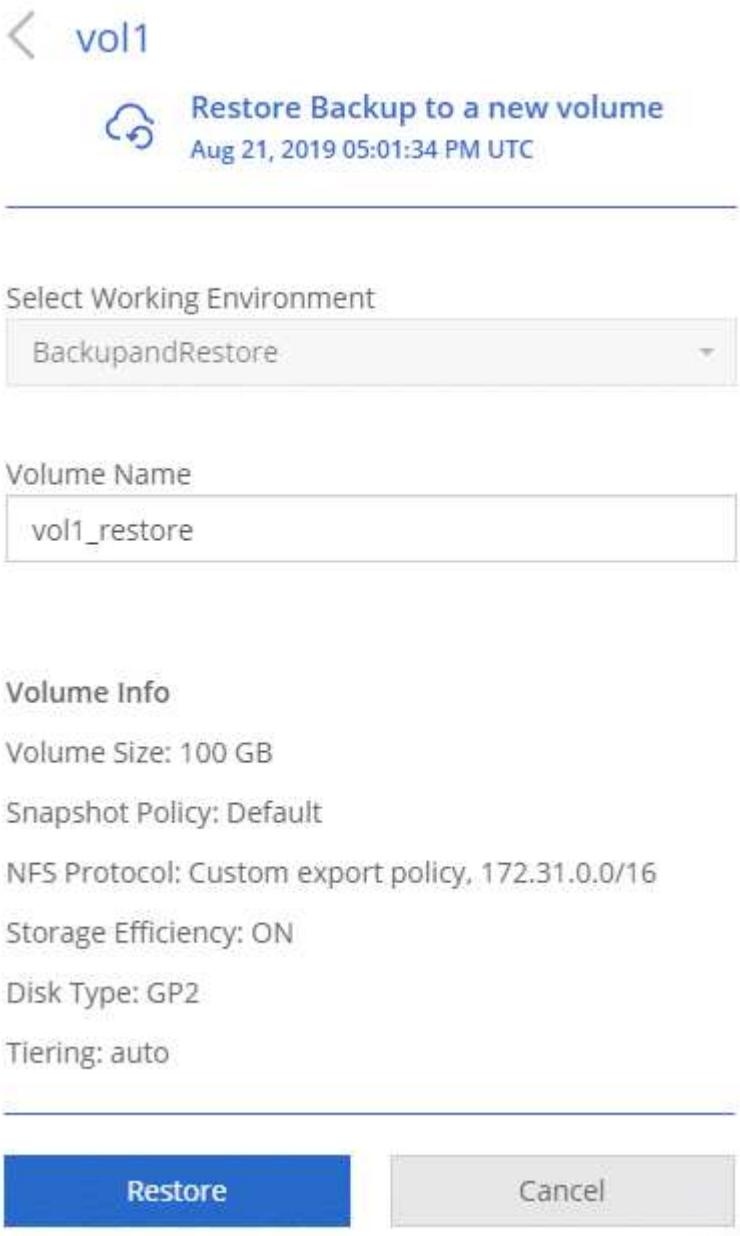
Étapes

1. En haut de Cloud Manager, cliquez sur **Backup & Restore**.
2. Sélectionnez le volume que vous souhaitez restaurer.

3. Recherchez la sauvegarde à partir de laquelle vous souhaitez restaurer et cliquez sur l'icône de restauration.



4. Sélectionnez l'environnement de travail dans lequel vous souhaitez restaurer le volume.
5. Entrez un nom pour le volume.
6. Cliquez sur **Restaurer**.

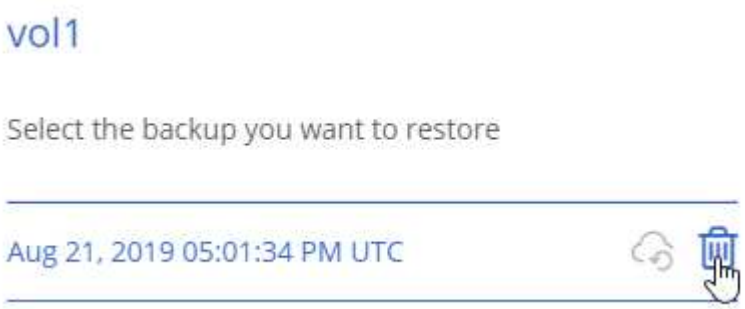


Suppression de sauvegardes

Toutes les sauvegardes sont conservées dans S3 jusqu'à leur suppression dans Cloud Manager. Les sauvegardes ne sont pas supprimées lorsque vous supprimez un volume ou lorsque vous supprimez le système Cloud Volumes ONTAP.

Étapes

1. En haut de Cloud Manager, cliquez sur **Backup & Restore**.
2. Sélectionnez un volume.
3. Recherchez la sauvegarde à supprimer et cliquez sur l'icône de suppression.



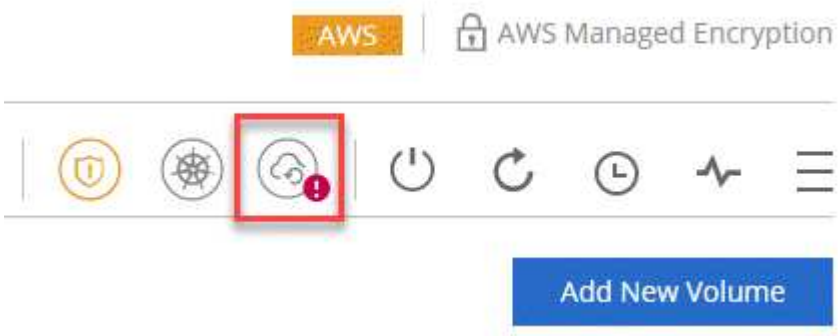
4. Confirmez la suppression de la sauvegarde.

Désactivation des sauvegardes dans S3

La désactivation des sauvegardes dans S3 désactive les sauvegardes de chaque volume sur le système. Les sauvegardes existantes ne seront pas supprimées.

Étapes

1. Ouvrir l'environnement de travail.
2. Cliquez sur l'icône des paramètres de sauvegarde.



3. Désactivez **sauvegardez automatiquement tous les volumes**, puis cliquez sur **Enregistrer**.

Fonctionnement de Backup vers S3

Les sections suivantes fournissent des informations supplémentaires sur la fonctionnalité Backup vers S3.

L’emplacement des sauvegardes

Les copies de sauvegarde sont stockées dans un compartiment S3 détenu par NetApp, dans la même région où se trouve le système Cloud Volumes ONTAP.

Les sauvegardes sont incrémentielles

Une fois la sauvegarde complète initiale de vos données effectuée, toutes les sauvegardes supplémentaires sont incrémentielles, ce qui signifie que seuls les blocs modifiés et les nouveaux blocs sont sauvegardés.

Les sauvegardes sont effectuées à minuit

Les sauvegardes quotidiennes commencent juste après minuit chaque jour. Pour l’instant, vous ne pouvez pas planifier les opérations de sauvegarde à un moment donné 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 aux instances Cloud Volumes ONTAP d’autres systèmes Cloud Manager.

La stratégie de sauvegarde est à l’échelle du système

Le nombre de sauvegardes à conserver est défini au niveau du système. Vous ne pouvez pas définir de règle différente pour chaque volume du système.

Sécurité

Les données de sauvegarde sont sécurisées par chiffrement AES 256 bits au repos et TLS 1.2 HTTPS en transit.

Les données sont transmises au service via des liaisons Direct Connect sécurisées et sont protégées au repos par le chiffrement AES 256 bits. Les données chiffrées sont ensuite écrites dans le cloud à l’aide de connexions HTTPS TLS 1.2. Les données parviennent également à Amazon S3 uniquement via des connexions de terminaux VPC sécurisées. Aucun trafic ne passe par Internet.

Chaque utilisateur se voit attribuer une clé de locataire, en plus d’une clé de chiffrement globale détenue par le service. Cette exigence est similaire au besoin d’une paire de clés pour ouvrir un coffre-fort client dans une banque. Toutes les clés, identifiants cloud, sont stockées en toute sécurité par le service et réservées à un seul personnel NetApp responsable de la maintenance du service.

Limites

- Si vous utilisez l’un des types d’instances suivants, un système Cloud Volumes ONTAP peut sauvegarder un maximum de 20 volumes dans S3 :
  - m4.xlarge
  - m5.xlarge
  - r4.xlarge
  - r5.xlarge
- Les volumes que vous créez en dehors de Cloud Manager ne sont pas automatiquement sauvegardés

dans S3.

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 Backup sur S3, puis activez-les à nouveau.

- Lorsque vous restaurez les données à partir d'une sauvegarde, Cloud Manager effectue une restauration de volume complet vers un *nouveau* volume. Ce nouveau volume n'est pas automatiquement sauvegardé sur S3.

  Si vous souhaitez sauvegarder les volumes créés à partir d'une opération de restauration, désactivez Backup sur S3, puis activez-les à nouveau.

- Vous pouvez sauvegarder des volumes dont la taille est inférieure ou égale à 50 To.
- La sauvegarde dans S3 peut conserver jusqu'à 245 sauvegardes totales d'un volume.
- Le stockage WORM n'est pas pris en charge sur un système Cloud Volumes ONTAP lorsque la sauvegarde vers S3 est activée.

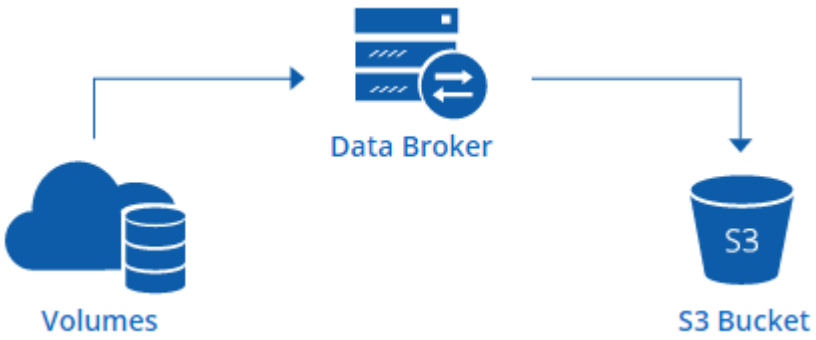
Synchronisation des données vers Amazon S3

Vous pouvez synchroniser les données des volumes ONTAP vers un compartiment Amazon S3 en intégrant un environnement de travail avec "NetApp Cloud Sync". Vous pouvez ensuite utiliser les données synchronisées comme copie secondaire ou pour le traitement des données à l'aide de services AWS tels que EMR et Redshift.

Fonctionnement de la fonction de synchronisation vers S3

Vous pouvez à tout moment intégrer un environnement de travail au service Cloud Sync. Lorsque vous intégrez un environnement de travail, le service Cloud Sync synchronise les données des volumes sélectionnés vers un seul compartiment S3. L'intégration fonctionne avec les environnements de travail Cloud Volumes ONTAP, ainsi qu'avec les clusters ONTAP qui sont sur site ou qui font partie d'une configuration NetApp Private Storage (NPS).

Pour synchroniser les données, le service lance une instance de courtier de données dans votre VPC. Cloud Sync utilise un courtier de données par environnement de travail pour synchroniser les données des volumes vers un compartiment S3. Après la synchronisation initiale, le service synchronise toutes les données modifiées une fois par jour à minuit.



Si vous souhaitez effectuer des actions Cloud Sync avancées, accédez directement au service Cloud Sync. De

là, vous pouvez effectuer des actions telles que la synchronisation de S3 vers un serveur NFS, le choix de compartiments S3 différents pour les volumes et la modification des plannings.

Essai gratuit de 14 jours

Si vous êtes un nouvel utilisateur de Cloud Sync, vos 14 premiers jours sont gratuits. Après la fin de l'essai gratuit, vous devez payer chaque relation *sync* à un tarif horaire ou en achetant des licences. Chaque volume que vous synchronisez avec un compartiment S3 est considéré comme une relation de synchronisation. Vous pouvez configurer les deux options de paiement directement à partir de Cloud Sync dans la page License Settings (Paramètres de licence).

Comment obtenir de l'aide

Utilisez les options suivantes pour toute prise en charge liée à la fonctionnalité de synchronisation de Cloud Manager vers S3 ou pour Cloud Sync en général :

- Retour d'informations générales sur le produit : ng-cloudsync-contact@netapp.com
- Options de support technique :
  - Communautés NetApp Cloud Sync
  - Chat in-product (coin inférieur droit de Cloud Manager)

Intégration d'un environnement de travail au service Cloud Sync

Si vous souhaitez synchroniser les volumes vers Amazon S3 directement depuis Cloud Manager, vous devez intégrer l'environnement de travail avec le service Cloud Sync.

[] | *https://img.youtube.com/vi/3hOtLs70_xE/maxresdefault.jpg*

Étapes

1. Ouvrez un environnement de travail et cliquez sur **Synchroniser avec S3**.
2. Cliquez sur **Sync** et suivez les invites pour synchroniser vos données avec S3.

> Vous ne pouvez pas synchroniser les volumes de protection des données vers S3. Les volumes doivent être inscriptibles.

Gestion des relations de synchronisation des volumes

Après avoir intégré un environnement de travail au service Cloud Sync, vous pouvez synchroniser des volumes supplémentaires, arrêter la synchronisation d'un volume et supprimer l'intégration avec Cloud Sync.

Étapes

1. Sur la page Environnements de travail, double-cliquez sur l'environnement de travail sur lequel vous souhaitez gérer les relations de synchronisation.
2. Si vous souhaitez activer ou désactiver la synchronisation vers S3 pour un volume, sélectionnez-le, puis cliquez sur **Synchroniser avec S3** ou sur **Supprimer la relation de synchronisation**.
3. Si vous souhaitez supprimer toutes les relations de synchronisation d'un environnement de travail, cliquez sur l'onglet **Synchroniser avec S3**, puis cliquez sur **Supprimer la synchronisation**.

   Cette action ne supprime pas les données synchronisées du compartiment S3. Si le data broker n'est pas utilisé dans d'autres relations de synchronisation, le service Cloud Sync supprime le data broker.

Améliorez la confidentialité des données

Découvrez Cloud Compliance

Cloud Compliance est un service de confidentialité et de conformité des données pour Cloud Volumes ONTAP dans AWS et Azure. Avec la technologie d'intelligence artificielle (IA), Cloud Compliance aide les entreprises à comprendre le contexte des données et à identifier les données sensibles dans les systèmes Cloud Volumes ONTAP.

Cloud Compliance est actuellement disponible sous forme de version contrôlée.

"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)

Le coût

Cloud Compliance est un service complémentaire proposé par NetApp pour Cloud Volumes ONTAP, sans frais supplémentaires. L'activation de Cloud Compliance nécessite le déploiement d'une instance cloud que votre fournisseur cloud facturera. L'entrée et la sortie des données ne sont pas facturés, car les données ne circulent pas en dehors du réseau.

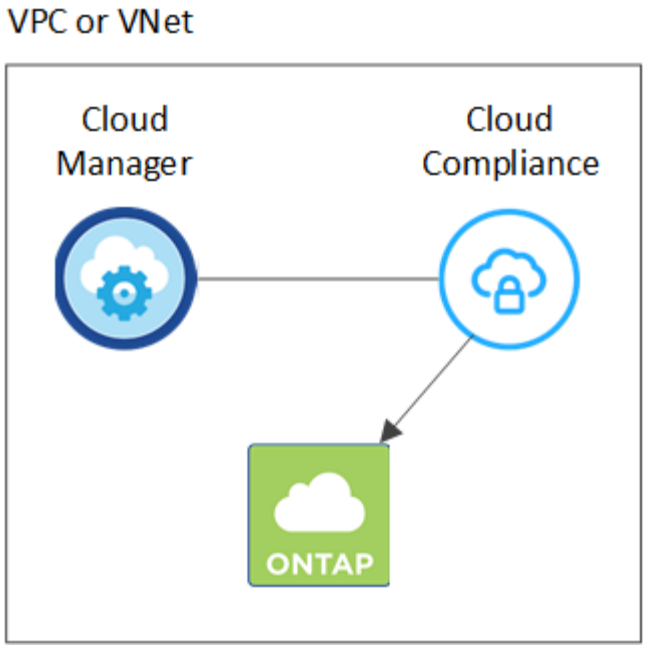
Fonctionnement de Cloud Compliance

À un niveau élevé, Cloud Compliance fonctionne comme ceci :

1. Vous activez Cloud Compliance sur un ou plusieurs systèmes Cloud Volumes ONTAP.
2. Cloud Compliance analyse les données à l'aide d'un processus de formation d'IA.
3. 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 sur un ou plusieurs systèmes Cloud Volumes ONTAP, Cloud Manager déploie une 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 io1 de 500 Go.

  Dans les régions où m5.4xlarge n'est pas disponible, Cloud Compliance s'exécute sur une instance m4.4xlarge.

- 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 système Cloud Manager.
- Les mises à niveau du logiciel Cloud Compliance sont automatisées ; vous n'avez plus à vous inquiéter.

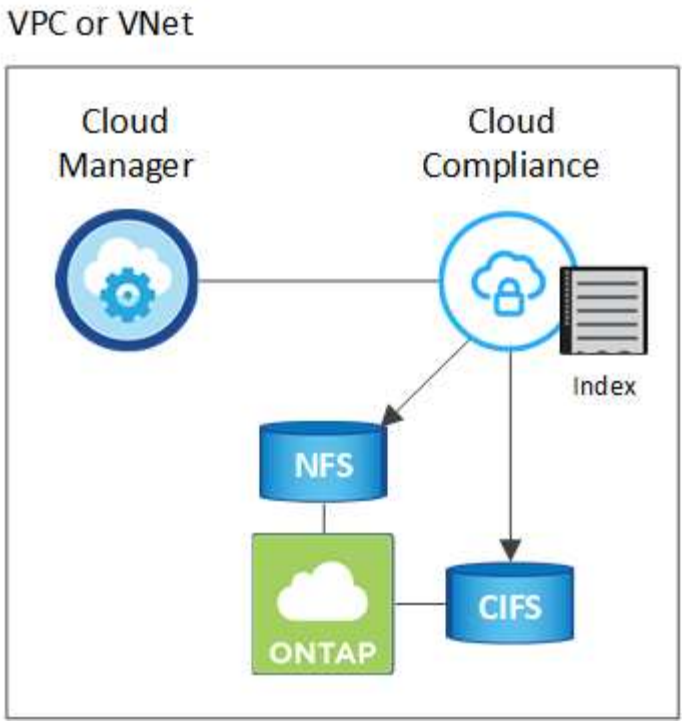
L'instance doit rester en fonctionnement permanent, car Cloud Compliance analyse en continu les données sur les systèmes Cloud Volumes ONTAP.

Fonctionnement des acquisitions

Une fois que vous avez activé Cloud Compliance, le service IT commence immédiatement à analyser vos données pour identifier les données personnelles et sensibles.

Cloud Compliance se connecte à Cloud Volumes ONTAP 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.

Cloud Compliance analyse les données non structurées sur chaque volume pour trouver une série de données personnelles. 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.



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 acquisitions au niveau de l'environnement de travail, mais pas au niveau du volume. "Découvrez comment".

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 une adresse IP privée et un groupe de sécurité qui active les connexions HTTP entrantes à partir de Cloud Manager. Cette connexion vous permet d'accéder au tableau de bord Cloud Compliance à partir de l'interface Cloud Manager.

Les règles sortantes sont complètement ouvertes. L'instance se connecte aux systèmes Cloud Volumes ONTAP et à Internet via un proxy depuis Cloud Manager. Un accès Internet est nécessaire pour mettre à niveau le logiciel Cloud Compliance et envoyer des metrics d'utilisation.

Si vous avez des exigences de mise en réseau strictes, "Découvrez les terminaux contacts par Cloud Compliance".

Les données indexées ne quittent jamais l'instance Cloud Compliance : les données ne sont pas relayées en dehors de votre réseau virtuel et ne sont pas envoyées à Cloud Manager.

Accès des utilisateurs aux informations de conformité

Les administrateurs de Cloud Manager peuvent consulter des informations de conformité pour tous les environnements de travail.

Les administrateurs de l'espace de travail peuvent afficher les informations de conformité uniquement pour les systèmes auxquels ils sont autorisés à accéder. 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.

"En savoir plus sur les rôles de Cloud Manager".

Mise en route de Cloud Compliance pour Cloud Volumes ONTAP

Découvrez comment utiliser Cloud Compliance pour Cloud Volumes ONTAP dans AWS ou Azure en quelques étapes.

Démarrage rapide

Pour commencer rapidement, suivez ces étapes ou faites défiler jusqu'aux sections restantes pour obtenir plus de détails.

Vérifiez que votre configuration répond aux exigences

- Assurez-vous que l'instance Cloud Compliance dispose d'un accès Internet sortant.

  Cloud Manager déploie l'instance dans le même VPC ou vNet que le premier système Cloud Volumes ONTAP de la demande.

- Assurez-vous que les utilisateurs peuvent accéder à l'interface Cloud Manager à partir d'un hôte avec connexion directe à AWS ou Azure, ou à partir d'un hôte sur le même réseau que l'instance Cloud Compliance (l'instance aura une adresse IP privée).
- Assurez-vous de pouvoir maintenir l'instance Cloud Compliance en cours d'exécution.

Activation de Cloud Compliance sur Cloud Volumes ONTAP

- Nouveaux environnements de travail : veillez à ce que Cloud Compliance soit activé lorsque vous créez l'environnement de travail (activé par défaut).
- Environnements de travail existants : cliquez sur **Compliance**, si vous le souhaitez, modifiez la liste des environnements de travail, puis cliquez sur **Afficher le tableau de bord de conformité**.

Vérifiez l'accès aux volumes

Lorsque Cloud Compliance est activé, assurez-vous que le service informatique peut accéder aux volumes.

- L'instance Cloud Compliance requiert une connexion réseau à chaque sous-réseau Cloud Volumes ONTAP.
- 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 **Compliance** > **Statut de lecture CIFS** > **Modifier les informations d'identification CIFS** et fournissez 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.

Assurez la connectivité entre Cloud Manager et Cloud Compliance

- Le groupe de sécurité pour Cloud Manager doit autoriser le trafic entrant et sortant via le port 80 vers et depuis l'instance Cloud Compliance.
- Si votre réseau AWS n'utilise pas de NAT ou de proxy pour l'accès Internet, le groupe de sécurité de Cloud Manager doit autoriser le trafic entrant sur le port TCP 3128 à partir de l'instance Cloud Compliance.

Vérification des prérequis

Avant d'activer Cloud Compliance, lisez les conditions préalables suivantes pour vous assurer que la configuration est prise en charge. Une fois que vous aurez activé Cloud Compliance, vous devrez assurer la connectivité entre les composants. Voici ce sujet.

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 :

Terminaux	Objectif
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://cloud-compliance-support-netapp.s3.us-west-1.amazonaws.com https://hub.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.

Vérifiez la connectivité du navigateur Web à 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.

Si vous accédez à Cloud Manager à partir d'une adresse IP publique, votre navigateur Web ne s'exécute probablement pas sur un hôte du réseau.

Assurez la conformité cloud

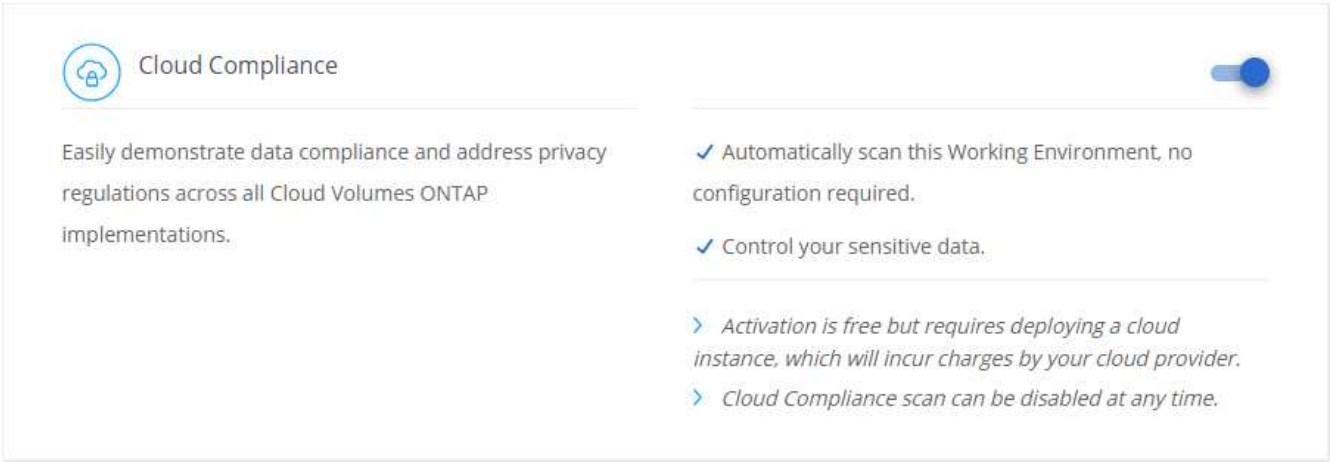
L'instance Cloud Compliance doit rester active pour analyser vos données en continu.

Activation de Cloud Compliance dans un nouvel environnement de travail

Cloud Compliance est activé par défaut dans l'assistant sur l'environnement de travail. Assurez-vous de conserver l'option activée.

Étapes

1. Cliquez sur **Créer Cloud Volumes ONTAP**.
2. Sélectionnez Amazon Web Services ou Microsoft Azure comme fournisseur cloud, puis choisissez un système haute disponibilité ou un seul nœud.
3. Remplissez la page Détails et références.
4. Sur la page Services, laissez Cloud Compliance activé et cliquez sur **Continuer**.



5. Complétez les pages de l'assistant pour déployer le système.

   Pour obtenir de l'aide, voir "Lancement d'Cloud Volumes ONTAP dans AWS" et "Lancement d'Cloud Volumes ONTAP dans Azure".

Résultat

Cloud Compliance est activé sur le système Cloud Volumes ONTAP. Si c'est la première fois que vous avez activé Cloud Compliance, Cloud Manager déploie l'instance Cloud Compliance dans votre fournisseur cloud. Dès que l'instance est disponible, il commence à analyser les données lorsqu'elles sont écrites sur chaque volume que vous créez.

Activation de Cloud Compliance dans des environnements de travail existants

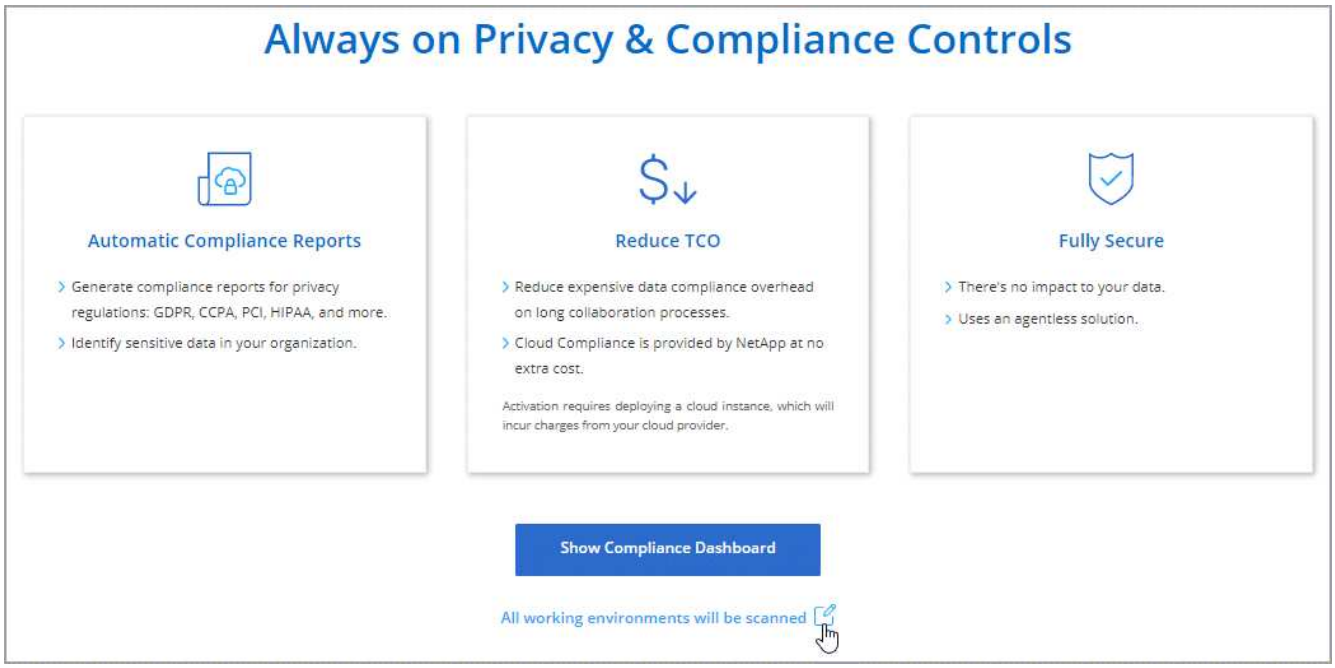
Activez Cloud Compliance sur vos systèmes Cloud Volumes ONTAP existants à partir de l'onglet **conformité** de Cloud Manager.

Une autre option consiste à activer Cloud Compliance à partir de l'onglet **environnements de travail** en sélectionnant chaque environnement de travail individuellement. Cette opération vous prendra plus de temps, sauf si vous n'avez qu'un seul système.

Étapes pour plusieurs environnements de travail

1. En haut de Cloud Manager, cliquez sur **Compliance**.
2. Si vous souhaitez activer Cloud Compliance dans des environnements de travail spécifiques, cliquez sur l'icône Modifier.

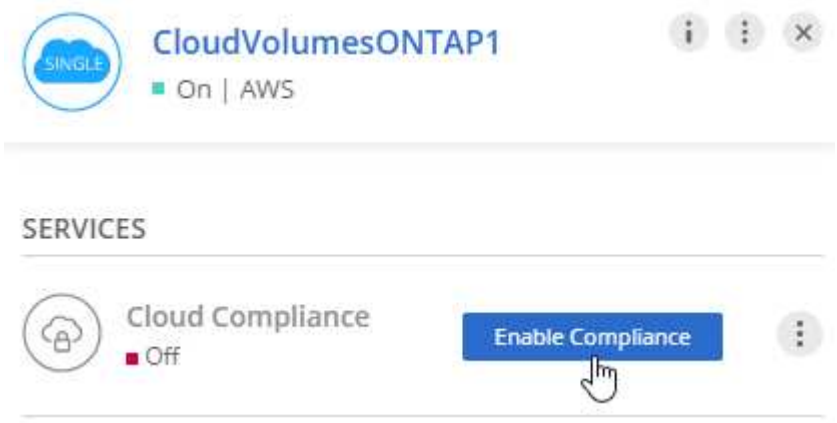
   Dans le cas contraire, Cloud Manager est défini pour activer Cloud Compliance sur tous les environnements de travail auxquels vous avez accès.



3. Cliquez sur **Afficher le tableau de bord de conformité**.

Étapes pour un environnement de travail unique

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 **Activer la conformité**.



Résultat

Si c'est la première fois que vous avez activé Cloud Compliance, Cloud Manager déploie l'instance Cloud Compliance dans votre fournisseur cloud.

Cloud Compliance commence l'analyse des données sur chaque environnement de travail. Les données 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 sur Cloud Volumes ONTAP 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 y a une connexion réseau entre l'instance Cloud Compliance et chaque sous-réseau Cloud Volumes ONTAP.

   Cloud Manager déploie l'instance Cloud Compliance dans le même VPC ou VNet que le premier système Cloud Volumes ONTAP de la demande. Cette étape est importante si certains systèmes Cloud Volumes ONTAP se trouvent dans des sous-réseaux ou des réseaux virtuels différents.

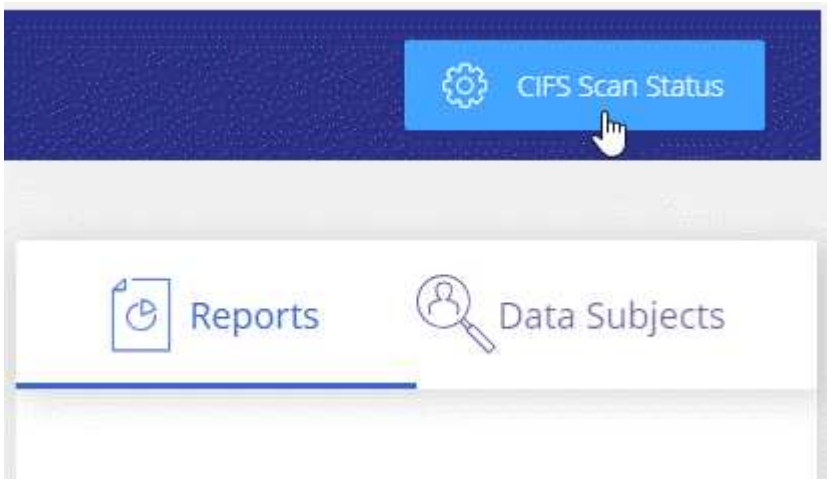
2. Assurez-vous que le groupe de sécurité pour Cloud Volumes ONTAP autorise le trafic entrant depuis l'instance Cloud Compliance.

   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 **Compliance**.

   b. Dans le coin supérieur droit, cliquez sur **Statut de numérisation CIFS**.



   c. Pour chaque système Cloud Volumes ONTAP, 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.

Vérifier que Cloud Manager peut accéder à Cloud Compliance

Assurez la connectivité entre Cloud Manager et Cloud Compliance pour pouvoir consulter les informations exploitables sur la conformité trouvées dans Cloud Compliance.

Étapes

1. Vérifiez que le groupe de sécurité de Cloud Manager permet le trafic entrant et sortant via le port 80 vers et depuis l'instance Cloud Compliance.

   Cette connexion vous permet d'afficher des informations dans l'onglet conformité.

2. Si votre réseau AWS n'utilise pas de NAT ou de proxy pour l'accès Internet, modifiez le groupe de sécurité de Cloud Manager pour autoriser le trafic entrant sur le port TCP 3128 à partir de l'instance Cloud Compliance.

   Cette étape est requise car l'instance Cloud Compliance utilise Cloud Manager comme proxy pour accéder à Internet.

   Ce port est ouvert par défaut sur toutes les nouvelles instances de Cloud Manager, à partir de la version 3.7.5. Elle n'est pas ouverte sur les instances Cloud Manager créées avant cette version.

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.

Données personnelles

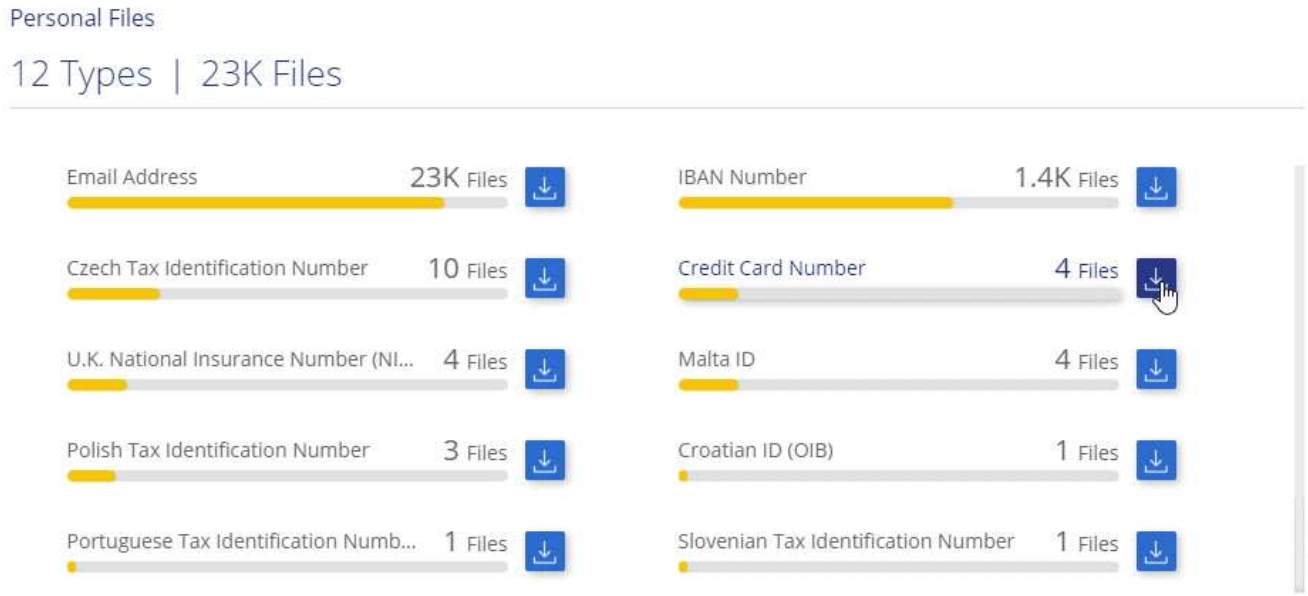
Cloud Compliance identifie automatiquement des mots, des chaînes et des motifs spécifiques (Regex) dans les données. Par exemple, les renseignements d'identification personnelle (RP), les numéros de carte de crédit, les numéros de sécurité sociale, les numéros de compte bancaire, etc. Voir la liste complète.

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 **Compliance**.
2. Téléchargez les détails de l'un des 2 principaux types de fichiers directement à partir de l'écran principal ou cliquez sur **Afficher tout** et téléchargez ensuite la liste pour l'un des types de données personnelles trouvés.



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
	Adresse IP	Oui.

Type	Identificateur	Validation de proximité ?
Identifiants nationaux	Carte d'identité belge (Numero National)	Oui.
	ID bulgare (Numéro civil unifié)	Oui.
	Chypre Numéro d'identification fiscale (TIC)	Oui.
	Numéro d'identification fiscale danois (CPR)	Oui.
	Carte d'identité estonienne (Isikukood)	Oui.
	ID finlandais (henkilötunnus)	Oui.
	Numéro d'identification fiscale (SPI)	Oui.
	Numéro d'identification fiscale allemand (identifiant Steierliche)	Oui.
	Numéro d'identification fiscale hongrois (Adóazonosító jel)	Oui.
	Irish ID (PPS)	Oui.
	ID israélien	Oui.
	ID italien (Codice Fiscale)	Oui.
	Numéro d'identification fiscale letton	Oui.
	Lituanien ID (Assens kodas)	Oui.
	Luxembourg ID	Oui.
	ID Malte	Oui.
	ID pays-Bas (BSN)	Oui.
	Numéro d'identification fiscale polonais	Oui.
	Numéro d'identification fiscale portugais (FNI)	Oui.
	Numéro d'identification fiscale roumain	Oui.
	Numéro d'identification fiscale slovaque	Oui.
	Numéro d'identification fiscale slovène	Oui.
	Carte d'identité sud-africaine	Oui.
	Numéro d'identification fiscale espagnol	Oui.
	Numéro d'identification fiscal suédois	Oui.
	ROYAUME-UNI Numéro d'assurance national (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.

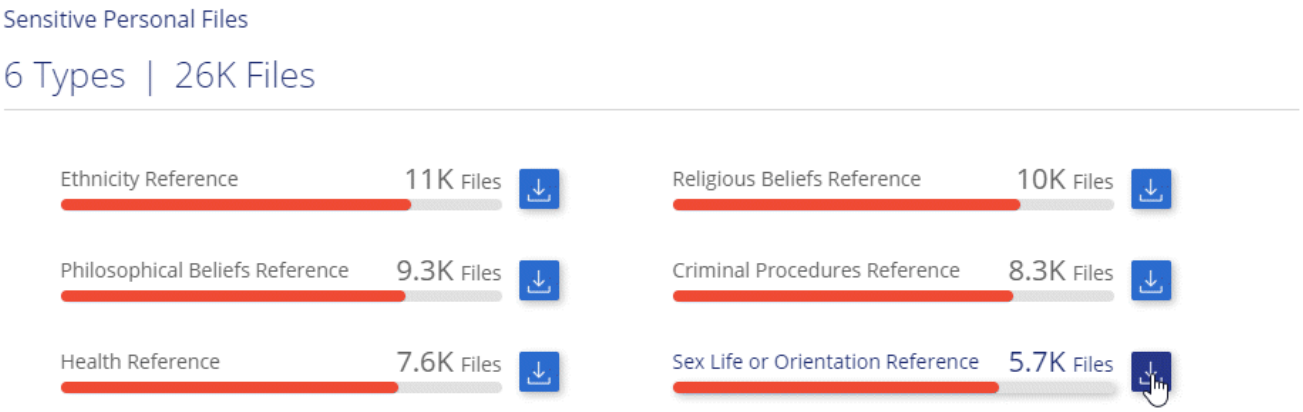
Par exemple, une catégorie de données sensibles du RGPD est l'origine ethnique. Du fait de ses capacités NLP, Cloud Compliance a la différence entre une phrase qui lit « George est mexicain » (en indiquant des données sensibles comme indiqué à l'article 9 du RGPD), et « George mange de la nourriture 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 **Compliance**.
2. Téléchargez les détails de l'un des 2 principaux types de fichiers directement à partir de l'écran principal ou cliquez sur **Afficher tout** et téléchargez ensuite la liste pour l'un des types de données personnelles sensibles trouvés.



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.

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.

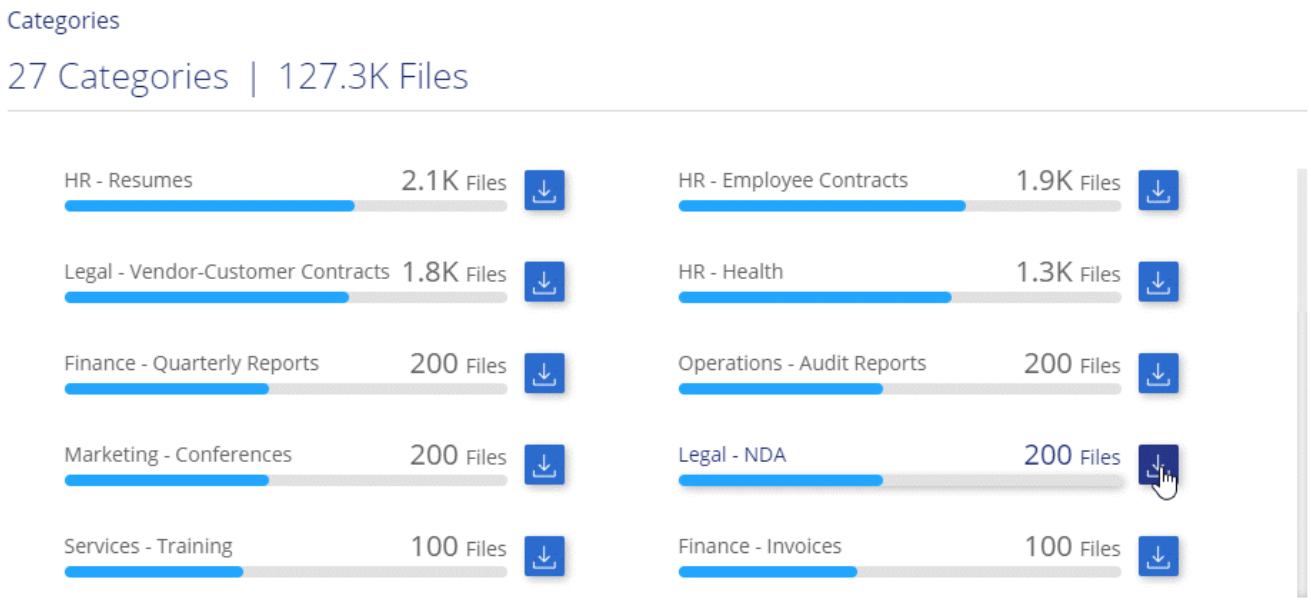
Les catégories peuvent vous aider à comprendre ce qui se passe avec vos données en vous indiquant le type d'informations dont vous disposez. Par exemple, une catégorie comme les CV ou les contrats d'employés peut inclure des données sensibles. Lorsque vous téléchargez le rapport CSV, vous pouvez constater que les contrats des 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 **Compliance**.
2. Téléchargez les détails de l'un des 4 principaux types de fichiers directement à partir de l'écran principal, ou cliquez sur **Afficher tout** et téléchargez la liste pour l'une des catégories.



Types de catégories

NetApp Cloud Compliance classe vos données comme suit :

Finances

- Bilans
- Bons de commande

- Factures
- Rapports trimestriels

RH

- Vérification des antécédents
- Plans de rémunération
- Contrats employés
- Évaluation des employés
- Santé
- Reprend

Légal

- NON DIVULGATION
- Contrats fournisseur-client

Marketing

- Campagnes
- Conférences

Exploitation

- Rapports d’audit

Ventes

- Commandes

Administratifs

- RFI
- RFP
- Formation

Assistance

- Plaintes et tickets

Autre

- Archiver les fichiers
- Audio
- Fichiers CAO
- Code
- Exécutables
- Images

Types de fichiers

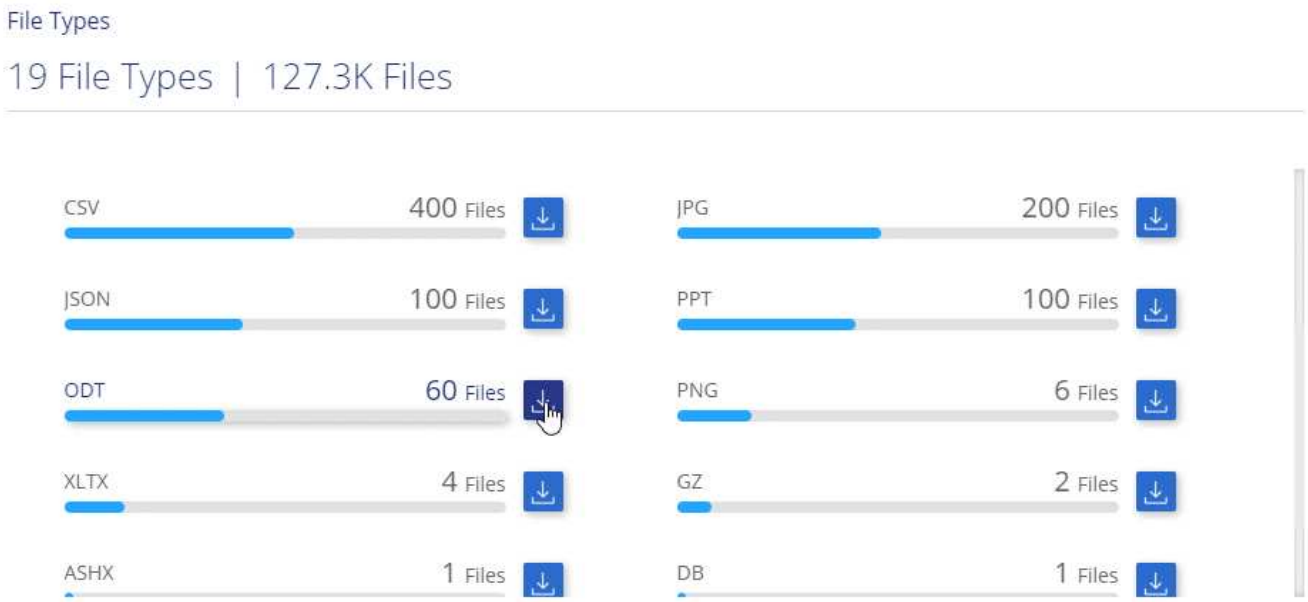
Cloud Compliance réduit les données analysées et les divise par type de fichier. Cloud Compliance peut afficher tous les types de fichiers présents dans les analyses.

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. 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 **Compliance**.
2. Téléchargez les détails de l'un des 4 principaux types de fichiers directement à partir de l'écran principal ou cliquez sur **Afficher tout** et téléchargez la liste pour n'importe quel type de fichier.



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)

Le tableau de bord vous permet de 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 premiers apparaissent dans la liste (la prise en charge de plus sera ajoutée ultérieurement).

Chaque liste de fichiers comprend les informations suivantes :

- Nom du fichier
- Type d'emplacement
- Emplacement
- 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. Les fichiers n'apparaissent que dans les rapports CSV.

Afficher le 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.

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 rapport contient les informations suivantes :

Statut de conformité

Un score de gravité (voir ci-dessous pour plus de détails) et la distribution des données, qu'elles soient personnelles, non sensibles 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

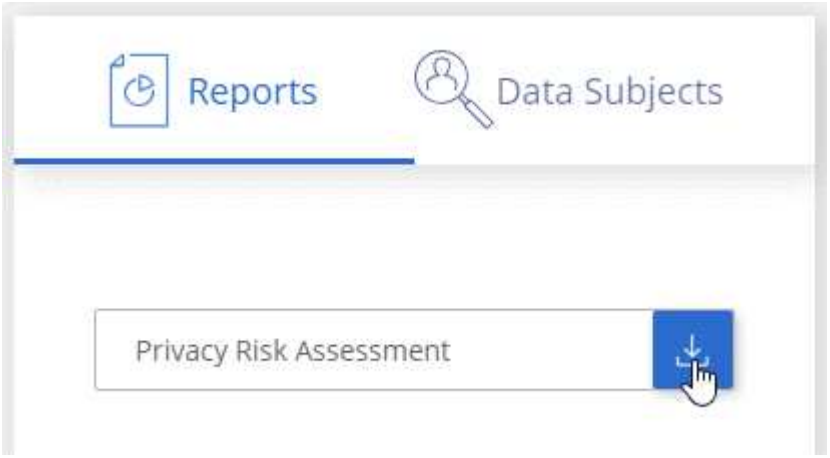
Nombre de personnes par lieu pour lesquelles des identificateurs nationaux ont été trouvés.

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 **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 plus importantes de 6 %
7	Trois des variables sont plus importantes de 6 %
8	L'une des variables est supérieure à 15 %
9	Deux des variables sont plus importantes de 15 %
10	Trois des variables sont plus importantes de 15 %

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 ou 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

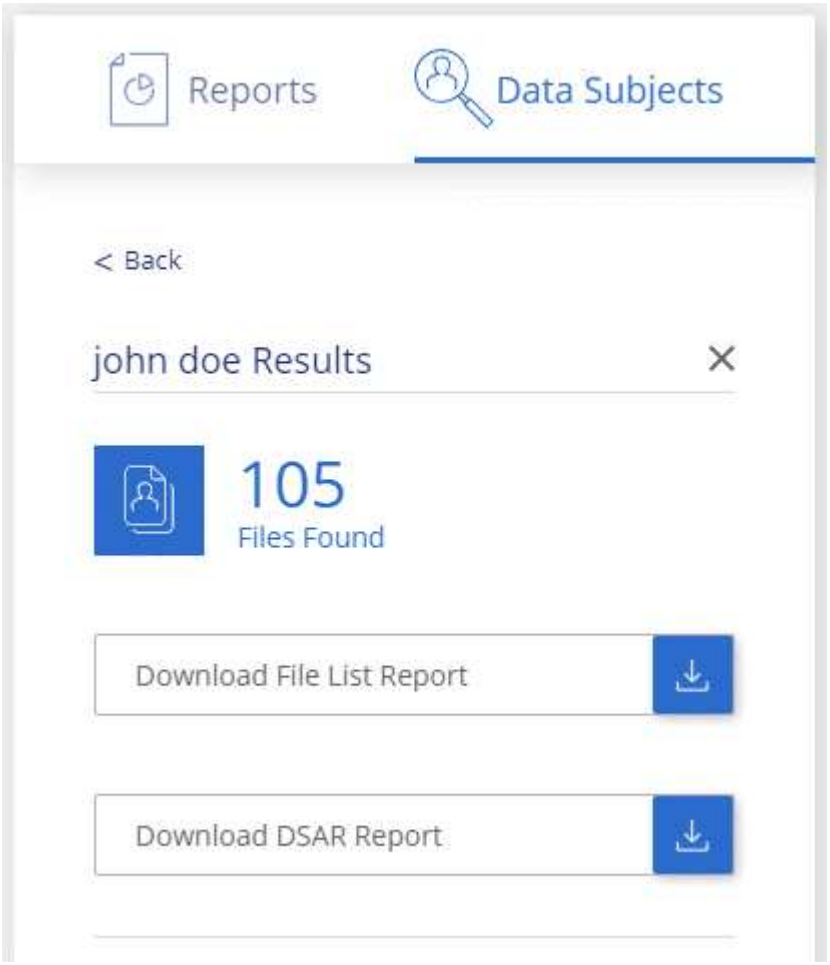
Recherchez le nom complet ou l'identifiant connu du sujet de données, puis téléchargez un rapport de liste de fichiers ou un rapport DSAR. Vous pouvez effectuer une recherche par "tout type d'informations personnelles".

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.

Étapes

1. En haut de Cloud Manager, cliquez sur **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 de liste de fichiers** : liste des fichiers qui contiennent des informations sur le sujet de données.

     S'il y a plus de 10,000 résultats, seuls les 10,000 premiers apparaissent dans le rapport (la prise en charge de plus sera ajoutée ultérieurement).

   - **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.

Désactivation de Cloud Compliance

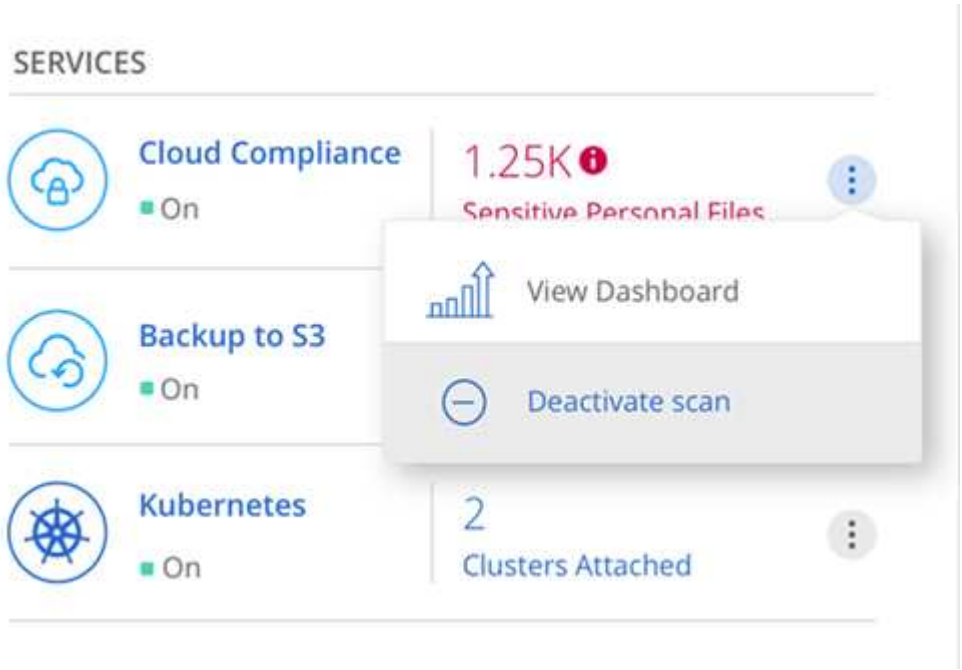
Si nécessaire, vous pouvez empêcher Cloud Compliance de scanner un ou plusieurs environnements de travail. Vous pouvez également supprimer l'instance Cloud Compliance si vous ne souhaitez plus utiliser Cloud Compliance avec vos systèmes Cloud Volumes ONTAP.

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 lui-même ne sont pas supprimées).

Étapes

1. En haut de Cloud Manager, cliquez sur **environnements de travail**.
2. Sélectionnez l'environnement de travail.
3. Dans le panneau de droite, cliquez sur l'icône d'action du service Cloud Compliance et sélectionnez **Désactiver scan**.



Suppression de l'instance Cloud Compliance

Vous pouvez supprimer l'instance Cloud Compliance si vous ne souhaitez plus utiliser Cloud Compliance avec Cloud Volumes ONTAP. 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 nouvelle offre cloud NetApp. Avec la technologie d'intelligence artificielle (IA), Cloud Compliance aide les entreprises à comprendre le contexte des données et à identifier les données sensibles dans l'ensemble de vos systèmes Cloud Volumes ONTAP hébergés sur AWS ou Azure.

Cloud Compliance fournit des paramètres prédéfinis (par exemple, des types d'informations sensibles et des catégories) pour respecter les nouvelles réglementations de conformité des données en matière de confidentialité et de sensibilité des données, notamment le RGPD et la loi CCPA.

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 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. À l'heure actuelle, Cloud Compliance analyse les données gérées par Cloud Volumes ONTAP.

"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 les instances Cloud Volumes ONTAP. Il analyse ensuite les données sur Cloud Volumes ONTAP et indexe les informations d'analyse trouvées.

"Découvrez le fonctionnement de Cloud Compliance".

Combien coûte Cloud Compliance ?

La conformité au cloud fait partie de Cloud Volumes ONTAP et ne requiert aucun coût supplémentaire. Des coûts supplémentaires peuvent être nécessaires à l'avenir pour des fonctionnalités personnalisées.

Cloud Compliance nécessite le déploiement d'une instance dans votre fournisseur cloud, pour laquelle vous serez facturé par votre fournisseur cloud.

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 >>".

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 io1 de 500 Go.

  Dans les régions où m5.4xlarge n'est pas disponible, Cloud Compliance s'exécute sur une instance m4.4xlarge.

"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.

Comment activer Cloud Compliance ?

Vous pouvez activer Cloud Compliance lorsque vous créez un nouvel environnement de travail. Vous pouvez l'activer sur les environnements de travail existants à partir de l'onglet **conformité** (lors de la première activation uniquement) 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 ?

Non Cloud Compliance est actuellement disponible dans Cloud Manager et prend en charge Cloud Volumes ONTAP. Nous prévoyons d'assurer la conformité cloud avec d'autres offres cloud telles que Cloud Volumes Service et Azure NetApp Files.

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 savoir plus >>".

Administrer Cloud Volumes ONTAP

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 OnCommand System Manager

Vous devrez peut-être effectuer certaines tâches Cloud Volumes ONTAP à partir d'OnCommand 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.

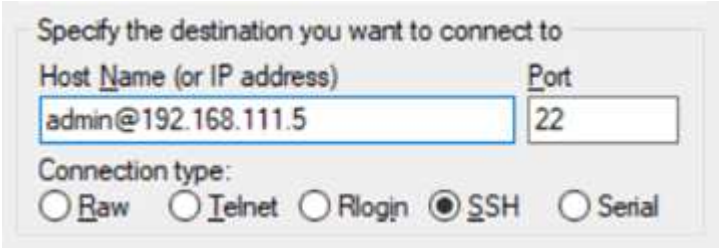
Lorsqu'elles sont déployées dans plusieurs environnements AZS, les configurations Cloud Volumes ONTAP HA utilisent une adresse IP flottante pour l'interface de gestion de cluster, ce qui signifie que le routage externe n'est pas disponible. Vous devez vous connecter à partir d'un hôte faisant partie 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::>
```

Mise à jour du logiciel Cloud Volumes ONTAP

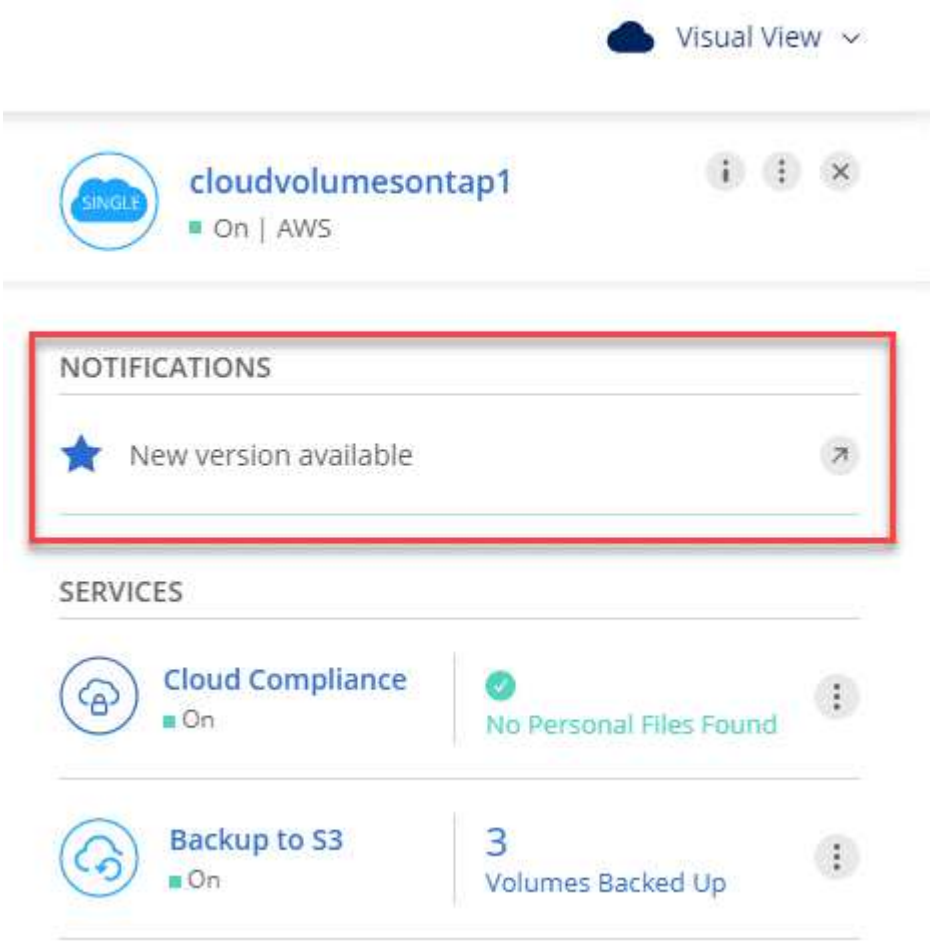
Cloud Manager inclut plusieurs options que vous pouvez utiliser pour mettre à niveau vers la version actuelle de Cloud Volumes ONTAP ou pour mettre à niveau Cloud Volumes ONTAP vers une version antérieure. Vous devez préparer les systèmes Cloud Volumes ONTAP avant de mettre à niveau ou de mettre à niveau 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

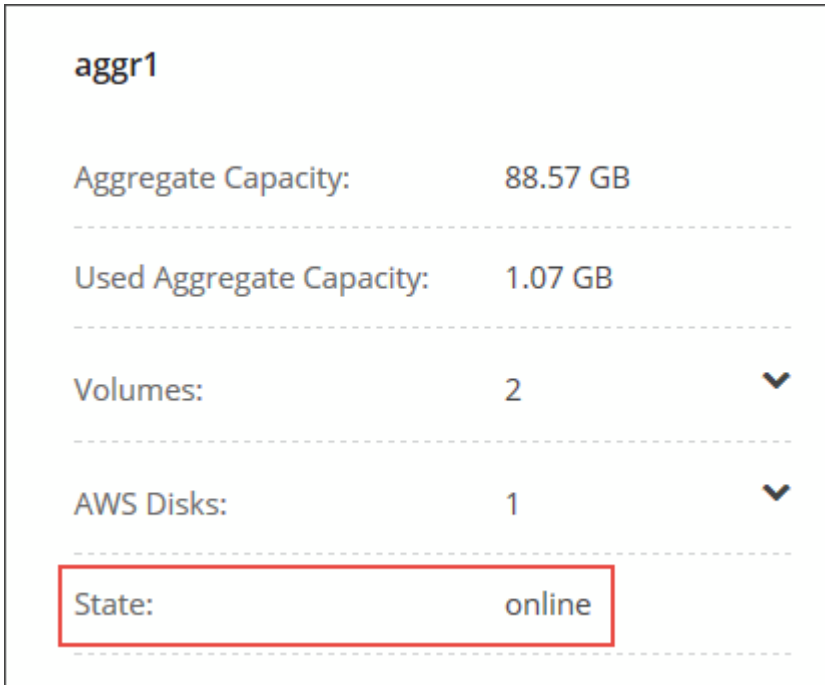
Les agrégats pour Cloud Volumes ONTAP doivent être en ligne avant de mettre à jour le logiciel. Les agrégats doivent être en ligne dans la plupart des configurations, mais si ce n'est pas le cas, vous devez les mettre en ligne.

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.

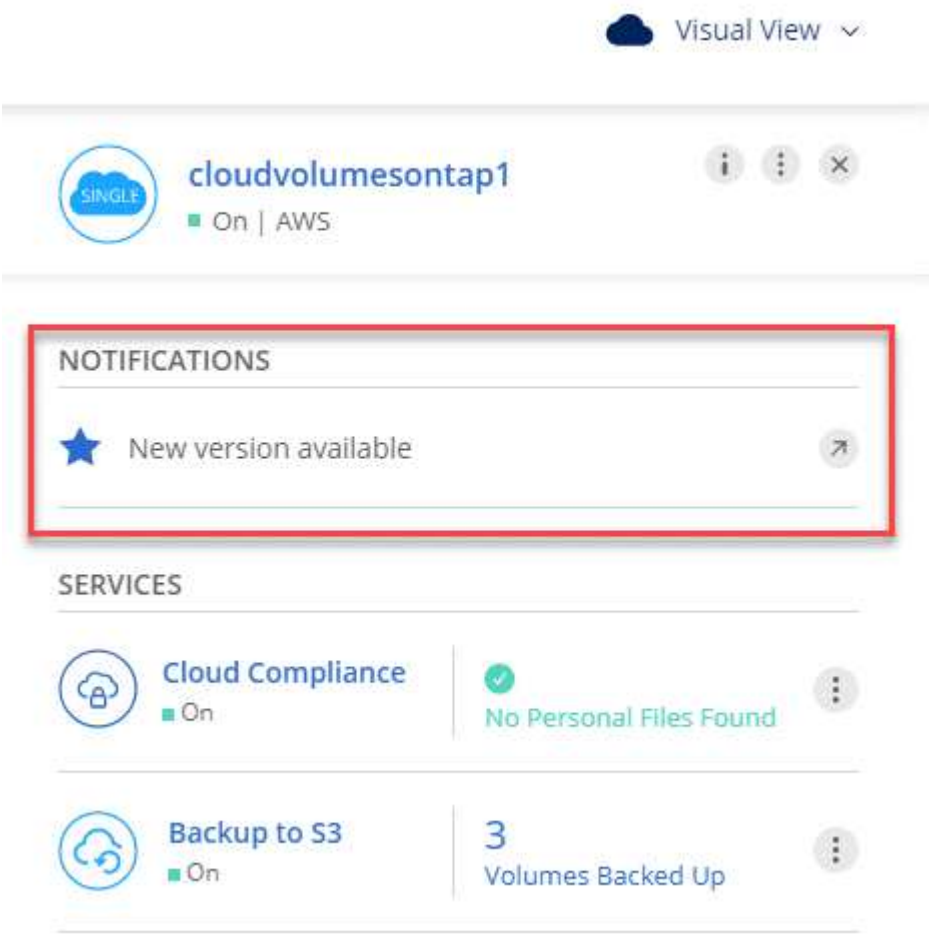
Avant de commencer

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

Vous devrez peut-être modifier la configuration des instances de Cloud Volumes ONTAP à mesure que vos besoins de stockage évoluent. Par exemple, vous pouvez modifier les configurations de paiement à la demande, modifier le type d'instance ou de VM et passer à un autre abonnement.

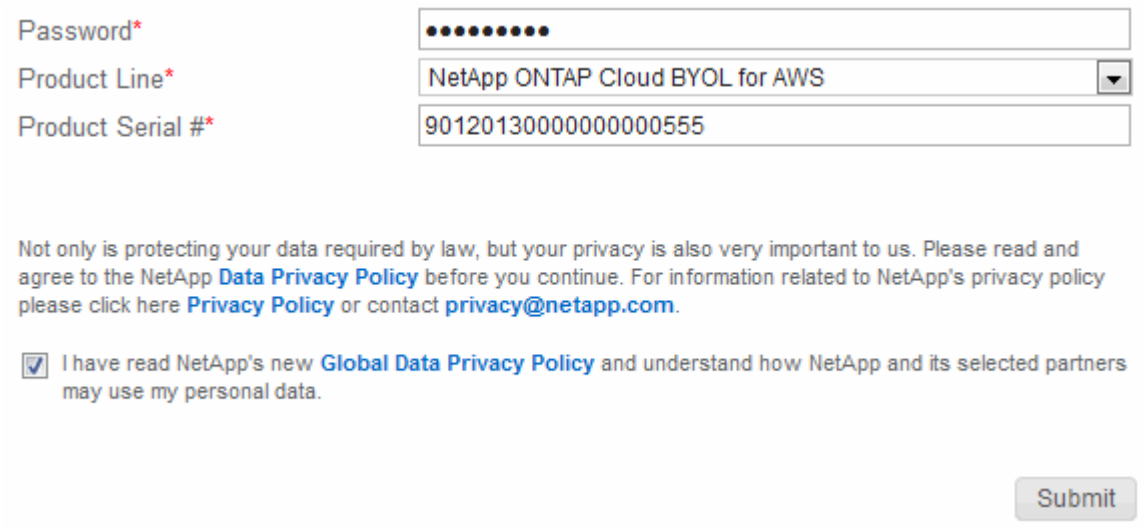
Installation de fichiers de licence sur les systèmes Cloud Volumes ONTAP BYOL

Si Cloud Manager ne parvient pas à obtenir un fichier de licence BYOL auprès de NetApp, vous pouvez obtenir le fichier vous-même, puis le télécharger manuellement dans Cloud Manager pour pouvoir installer la licence sur le système Cloud Volumes ONTAP.

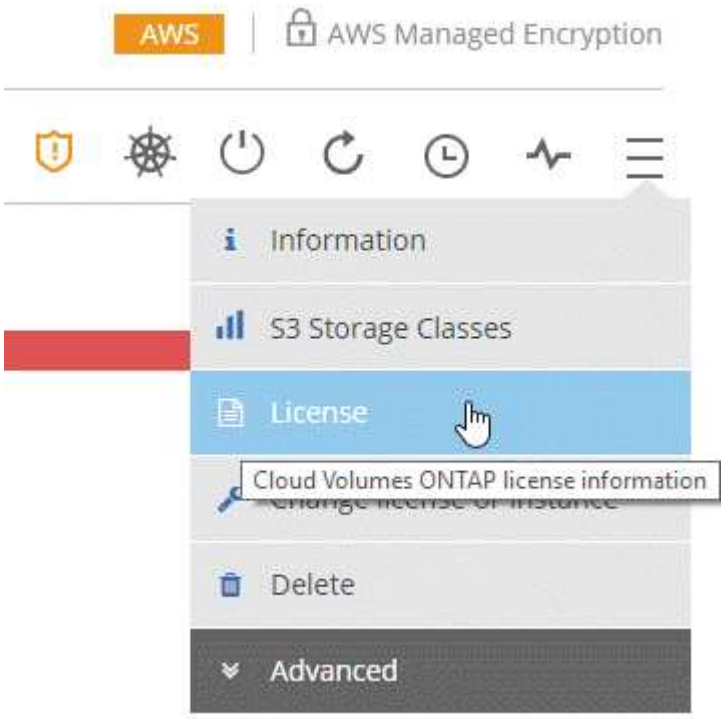
Étapes

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.
4. Dans Cloud Manager, ouvrez l'environnement de travail Cloud Volumes ONTAP BYOL.
5. Cliquez sur l'icône du menu, puis sur **Licence**.



6. Cliquez sur **Télécharger le fichier de licence**.
7. Cliquez sur **Upload**, puis sélectionnez le fichier.

Résultat

Cloud Manager installe le nouveau fichier de licence sur le système Cloud Volumes ONTAP.

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"

- 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. 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 passer d'un abonnement payant à un abonnement BYOL ou d'un système Cloud Volumes ONTAP à une paire HA, vous pouvez déployer un nouveau système, puis répliquer les données du 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 votre abonnement AWS Marketplace

Modifiez l'abonnement AWS Marketplace pour votre système Cloud Volumes ONTAP si vous souhaitez modifier le compte AWS depuis lequel vous êtes facturé.

Étapes

1. Si vous ne l'avez pas déjà fait, ajoutez un nouvel abonnement à partir de "Offre Cloud Manager dans AWS Marketplace".
2. Dans l'environnement de travail de Cloud Manager, cliquez sur l'icône de menu, puis sur **Marketplace Subscription**.
3. Sélectionnez un abonnement dans la liste déroulante.
4. Cliquez sur **Enregistrer**.

Modification de la vitesse d'écriture sur normale ou élevée

La vitesse d'écriture par défaut pour Cloud Volumes ONTAP 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.

  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.

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.

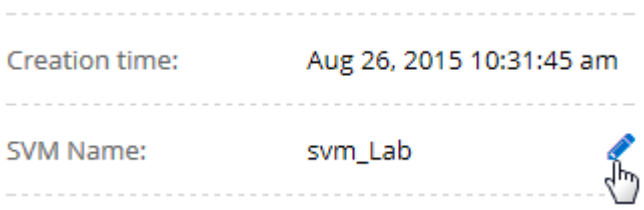
3. Cliquez sur **Enregistrer**, vérifiez le message de confirmation, puis cliquez sur **Continuer**.

Modification du nom de la machine virtuelle de stockage

Cloud Manager nomme automatiquement la machine virtuelle de stockage (SVM) 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 le faire correspondre à la façon dont vous nommez les SVM pour vos clusters 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 SVM.



3. Dans la boîte de dialogue Modifier le nom du SVM, modifier le nom du SVM, puis cliquer 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.

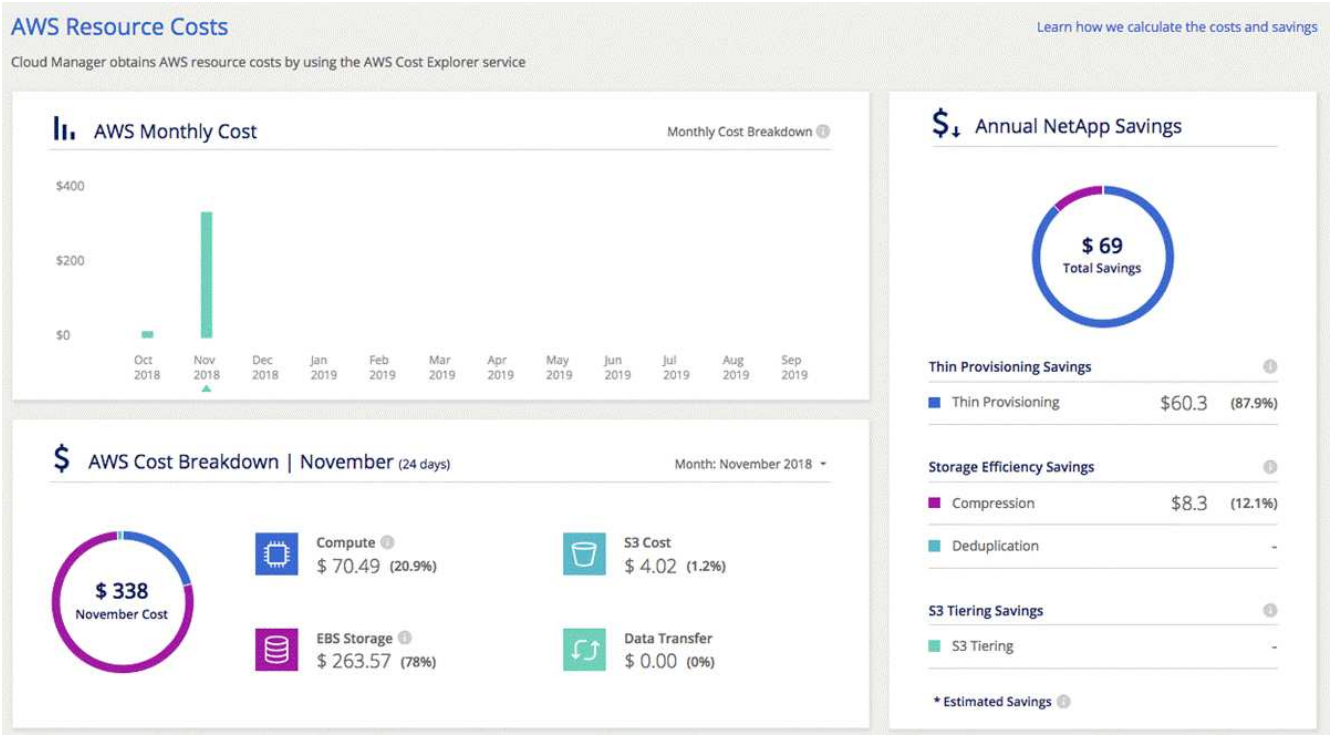
   b. "Activer la balise **WorkingEnvironnement**".

      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 :

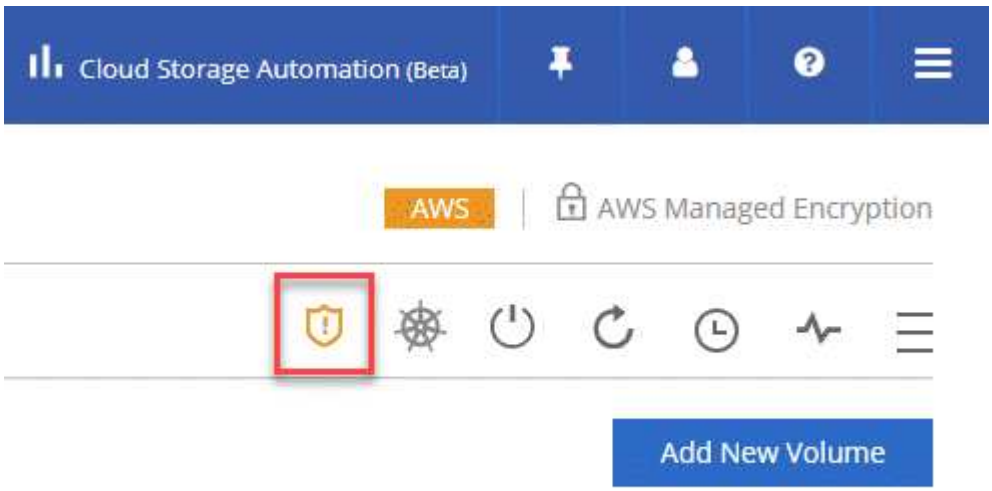


Renforcer la protection contre les attaques par ransomware

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**.

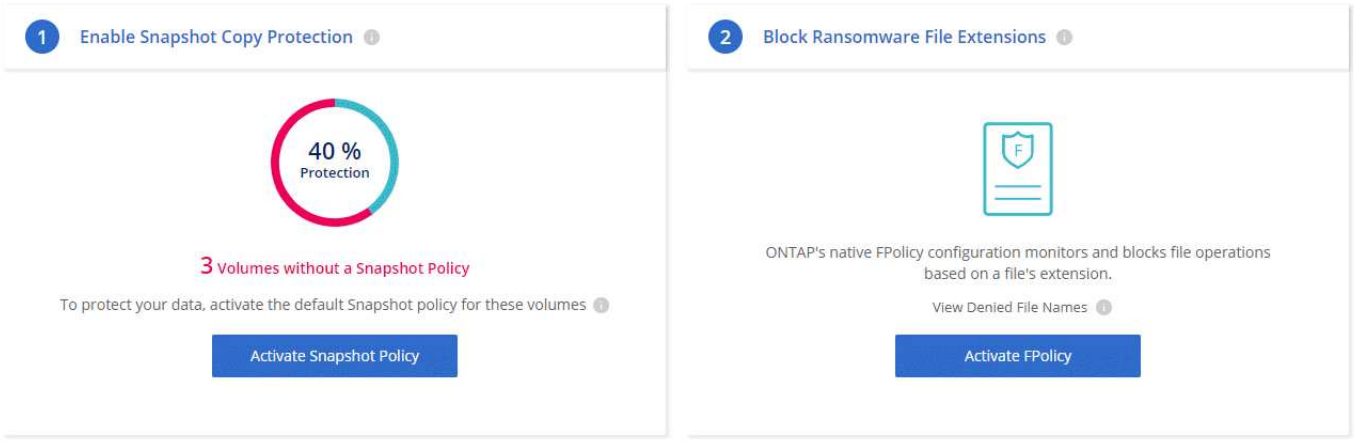


2. Implémentez la solution NetApp en cas d'attaque par ransomware :
   a. Cliquez sur **Activer la stratégie de snapshot**, si des volumes n'ont pas de règle de snapshot activée.

      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.



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 **découvrir** et sélectionnez **Cloud Volumes ONTAP**.
2. Sélectionnez le fournisseur de cloud dans lequel réside le système.
3. Sur la page Région, choisissez la région dans laquelle les instances sont exécutées, puis sélectionnez les instances.
4. 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.

Administration de Cloud Manager

Mise à jour de Cloud Manager

Vous pouvez mettre à jour Cloud Manager vers la dernière version ou avec un correctif que le personnel NetApp vous a partagé.

Activation des mises à jour automatiques

Cloud Manager peut se mettre à jour automatiquement dès qu'une nouvelle version est disponible. Cela vous permet d'exécuter la dernière version.

Description de la tâche

Cloud Manager se met automatiquement à jour à minuit si aucune opération n'est en cours d'exécution.

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **Cloud Manager Settings**.
2. Cochez la case sous mises à jour automatiques de Cloud Manager, puis cliquez sur **Enregistrer**.

Mise à jour de Cloud Manager vers la dernière version

Vous devez activer les mises à jour automatiques de Cloud Manager, mais vous pouvez toujours effectuer une mise à jour manuelle directement à partir de la console Web. Cloud Manager obtient la mise à jour logicielle d'un compartiment S3 appartenant à NetApp dans AWS.

Avant de commencer

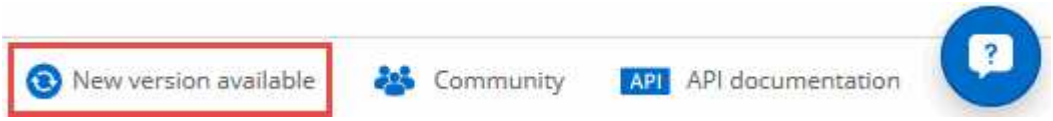
Vous devriez avoir passé en revue "nouveautés de la version" identifier les nouvelles exigences et les changements en matière de support

Description de la tâche

La mise à jour du logiciel prend quelques minutes. Cloud Manager ne sera pas disponible pendant la mise à jour.

Étapes

1. Vérifiez si une nouvelle version est disponible en consultant le coin inférieur droit de la console :



2. Si une nouvelle version est disponible, cliquez sur **Chronologie** pour déterminer si des tâches sont en cours.

   Si des tâches sont en cours, attendez qu'elles se terminent avant de passer à l'étape suivante.

3. Dans le coin inférieur droit de la console, cliquez sur **Nouvelle version disponible**.
4. Sur la page mise à jour du logiciel Cloud Manager, cliquez sur **mise à jour** en regard de la version souhaitée.

5. Complétez la boîte de dialogue de confirmation, puis cliquez sur **OK**.

Résultat

Cloud Manager démarre le processus de mise à jour. Vous pouvez vous connecter à la console après quelques minutes.

Mise à jour de Cloud Manager avec un correctif

Si NetApp a partagé un correctif avec vous, vous pouvez mettre à jour Cloud Manager avec le correctif fourni directement à partir de la console Web de Cloud Manager.

Description de la tâche

La mise à jour du correctif prend généralement quelques minutes. Cloud Manager ne sera pas disponible pendant la mise à jour.

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **mise à jour logicielle**.

2. Cliquez sur le lien pour mettre à jour Cloud Manager avec le correctif fourni.

3. Complétez la boîte de dialogue de confirmation, puis cliquez sur **OK**.
4. Sélectionnez le correctif que vous avez fourni.

Résultat

Cloud Manager applique le correctif. Vous pouvez vous connecter à la console après quelques minutes.

Gestion des espaces de travail et des utilisateurs sur le compte Cloud Central

"Après avoir effectué la configuration initiale", vous devrez peut-être gérer ultérieurement les utilisateurs, les espaces de travail et les connecteurs de service.

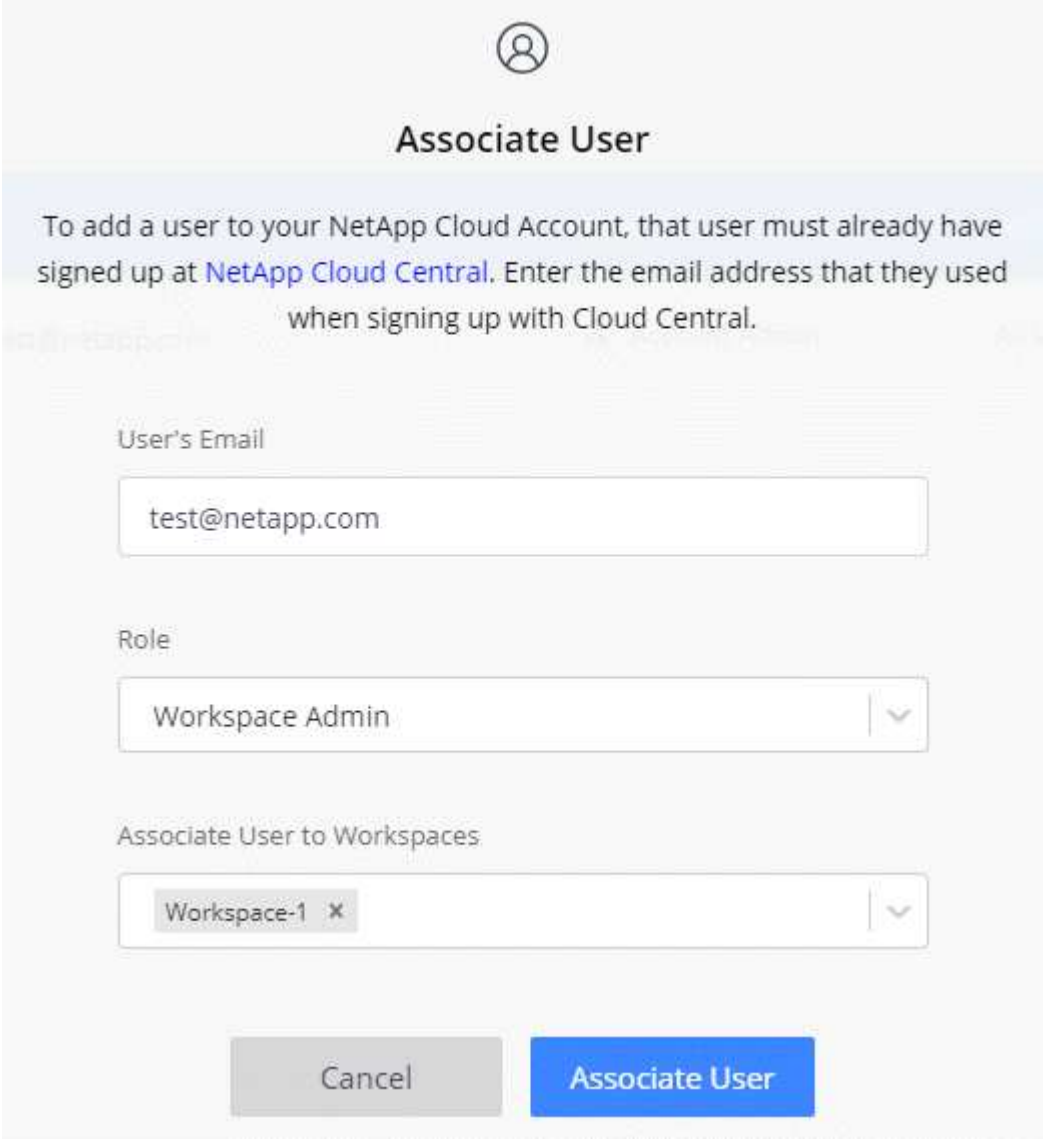
"Découvrez comment fonctionnent les comptes Cloud Central".

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 créez un compte.
2. Dans Cloud Manager, cliquez sur **Paramètres de 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.
5. Si vous avez sélectionné Workspace Admin, 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.

Résultat

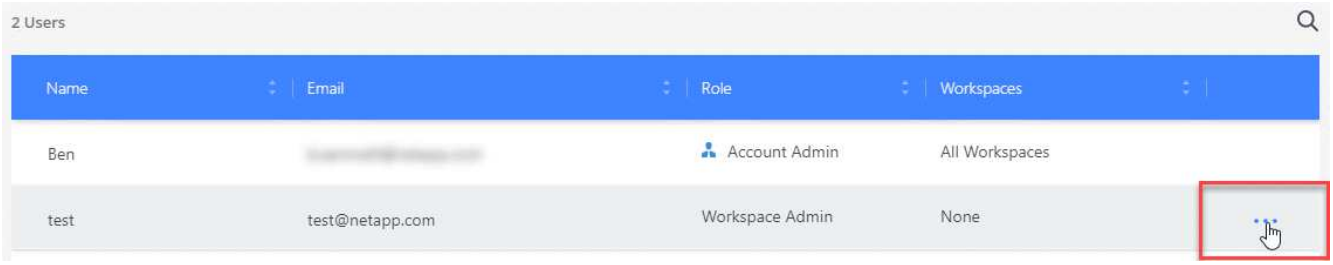
L'utilisateur doit recevoir un e-mail de la part de NetApp Cloud Central intitulé « Account Association ». Il contient les informations nécessaires pour accéder à Cloud Manager.

Suppression d'utilisateurs

La dissociation permet d'interdire l'accès aux ressources d'un compte Cloud Central.

Étapes

1. Cliquez sur **Paramètres de compte**.
2. 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

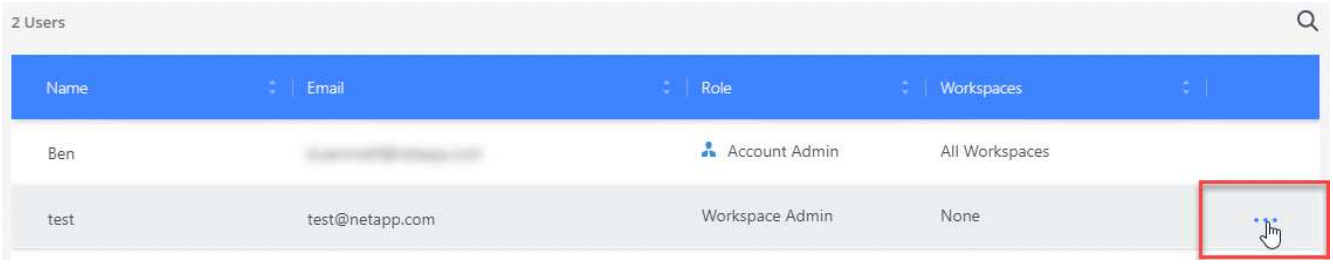
L'utilisateur ne peut plus accéder aux ressources de ce compte Cloud Central.

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. Cliquez sur **Paramètres de compte**.
2. 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

Il est désormais possible d'accéder à ces espaces de travail à partir de Cloud Manager, tant que le connecteur de service 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. Cliquez sur **Paramètres de 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 de service

Vous devez associer ce connecteur de service 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 de service 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 de service".

Étapes

1. Cliquez sur **Paramètres de compte**.
2. Cliquez sur **Service Connector**.
3. Cliquez sur **gérer les espaces de travail** pour le connecteur de service que vous souhaitez associer.
4. Sélectionnez les espaces de travail à associer au connecteur de service et cliquez sur **appliquer**.

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 de Cloud Manager pour utiliser un serveur proxy

Lorsque vous déployez Cloud Manager pour la première fois, il vous invite à entrer un serveur proxy si le système ne dispose pas d'un accès Internet. Vous pouvez également saisir et modifier manuellement le proxy à partir des paramètres de Cloud Manager.

Description de la tâche

Si vos règles d'entreprise exigent que vous utilisiez un serveur proxy pour toutes les communications HTTP sur Internet, vous devez configurer Cloud Manager pour qu'il utilise ce serveur proxy. Le serveur proxy peut se trouver dans le cloud ou dans votre réseau.

Lorsque vous configurez Cloud Manager pour qu'il utilise un serveur proxy, Cloud Manager, Cloud Volumes ONTAP et le médiateur HA utilisent tous le serveur proxy.

Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône Paramètres et sélectionnez **Cloud Manager Settings**.

2. 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 qui incluent 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 ne spécifiez pas le serveur proxy avant que les utilisateurs ne créent des systèmes Cloud Volumes ONTAP, ils doivent utiliser System Manager pour définir manuellement le serveur proxy dans les options AutoSupport pour chaque système.

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.

Restauration de Cloud Manager

Votre "Compte NetApp Cloud Central" Permet de restaurer facilement une configuration Cloud Manager. Le compte est un service exécuté dans Cloud Central. Les utilisateurs, les espaces de travail et les connecteurs de service associés sont donc toujours accessibles. Même si votre système Cloud Manager a été supprimé par erreur.

Depuis la version 3.7.1, Cloud Manager ne prend plus en charge le téléchargement d'une sauvegarde et son utilisation pour restaurer la configuration. Procédez comme suit pour restaurer Cloud Manager.

Étapes

1. Déployez un nouveau système Cloud Manager dans votre compte Cloud Central.

   "Options de déploiement"

2. Ajoutez vos comptes de fournisseurs cloud et vos comptes du site de support NetApp à Cloud Manager.

   Cette étape permet de préparer Cloud Manager pour créer d'autres systèmes Cloud Volumes ONTAP chez votre fournisseur cloud.

   Il est important d'effectuer cette étape si vous avez utilisé des clés AWS pour déployer un système Cloud Volumes ONTAP existant que vous voulez découvrir sur ce nouveau système Cloud Manager. Cloud

Manager a besoin des clés AWS pour découvrir et gérer correctement Cloud Volumes ONTAP.

- "Ajout de comptes AWS à Cloud Manager"
- "Ajout de comptes Azure à Cloud Manager"
- "Ajout de comptes du site de support NetApp à Cloud Manager"

3. Redécouvrez vos environnements de travail : systèmes Cloud Volumes ONTAP, clusters sur site et configurations NetApp Private Storage pour le cloud.
   - "Ajout de systèmes Cloud Volumes ONTAP existants à Cloud Manager"
   - "Découverte des clusters ONTAP"

Résultat

Votre configuration Cloud Manager est restaurée avec vos comptes, paramètres et environnements de travail.

Désinstallation de Cloud Manager

Cloud Manager inclut un script de désinstallation que vous pouvez utiliser pour désinstaller le logiciel pour résoudre les problèmes ou supprimer définitivement le logiciel de l'hôte.

Étapes

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.

Provisionner des volumes pour les services de fichiers

Gestion des volumes pour Azure NetApp Files

Afficher et créer des volumes NFS pour "Azure NetApp Files" Directement dans Cloud Manager.

Configuration

Votre configuration doit répondre à quelques exigences avant de gérer les volumes de Azure NetApp Files à partir de Cloud Manager.

1. Pour configurer Azure NetApp Files, procédez comme suit depuis le portail Azure :
   - "Inscrivez-vous à Azure NetApp Files"
   - "Créer un compte NetApp"
   - "Configurez un pool de capacité"
   - "Déléguer un sous-réseau à Azure NetApp Files"
2. Cloud Manager doit être configuré comme suit :
   - Cloud Manager doit être exécuté dans Azure, dans le compte où Azure NetApp Files a été configuré.
   - La machine virtuelle de Cloud Manager doit recevoir des autorisations via un "identité gérée".

     Si vous avez déployé Cloud Manager à partir de Cloud Central, vous êtes paré. Cloud Central active automatiquement une identité gérée attribuée par le système sur la machine virtuelle Cloud Manager.

   Si vous avez déployé Cloud Manager à partir d'Azure Marketplace, vous devez avoir suivi "instructions pour activer une identité gérée".

   - Le rôle Azure attribué à la machine virtuelle Cloud Manager doit inclure les autorisations répertoriées au dernier jour "Cloud Manager policy pour Azure":

     ```
     "Microsoft.NetApp/netAppAccounts/read",
     "Microsoft.NetApp/netAppAccounts/capacityPools/read",
     "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
     "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
     "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete"
     ```

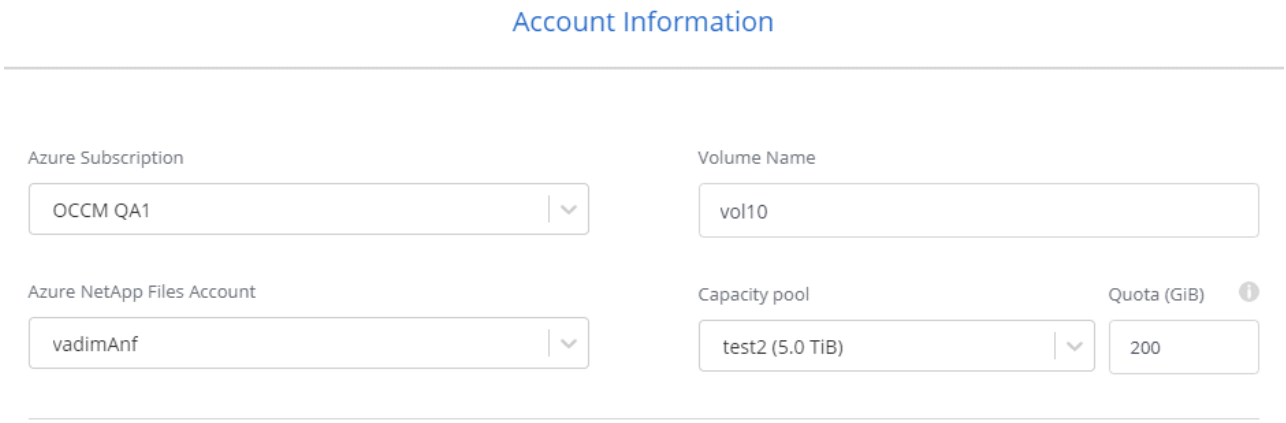
Une fois votre configuration configurée, Cloud Manager affiche automatiquement Azure NetApp Files sur la page des environnements de travail :

Création de volumes

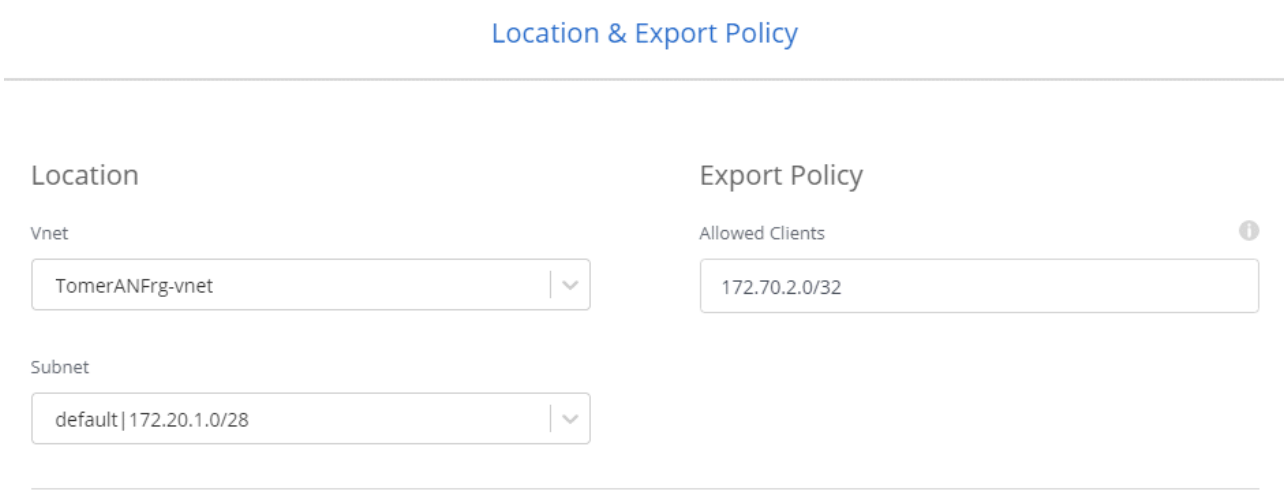
Cloud Manager vous permet de créer des volumes NFSv3 pour Azure NetApp Files.

Étapes

1. Ouvrir l'environnement de travail.
2. Cliquez sur **Ajouter nouveau volume**.
3. Entrez les détails de base sur le volume dans la page **informations de compte** :
   a. Sélectionnez un abonnement Azure et un compte Azure NetApp Files.
   b. Entrez un nom pour le volume.
   c. Sélectionnez un pool de capacités et spécifiez un quota, qui correspond à la quantité de stockage logique allouée au volume.



4. Remplissez la page **politique d'emplacement et d'exportation** :
   a. Sélectionnez un VNet et un sous-réseau.
   b. Configuration d'une export-policy pour contrôler l'accès au volume.



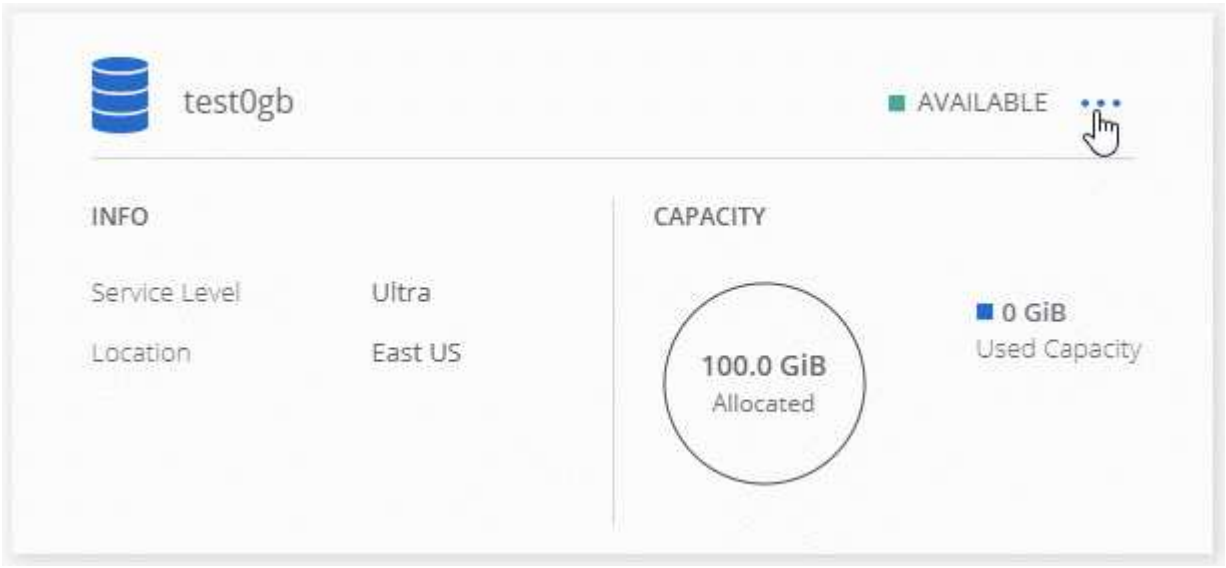
5. Cliquez sur **Go**.

Obtention du chemin de montage d'un volume

Copiez le chemin de montage d'un volume afin de pouvoir monter le volume sur une machine Linux.

Étapes

1. Ouvrir l'environnement de travail.
2. Placez le pointeur de la souris sur le volume et cliquez sur le menu.



3. Cliquez sur **Mount Command**.

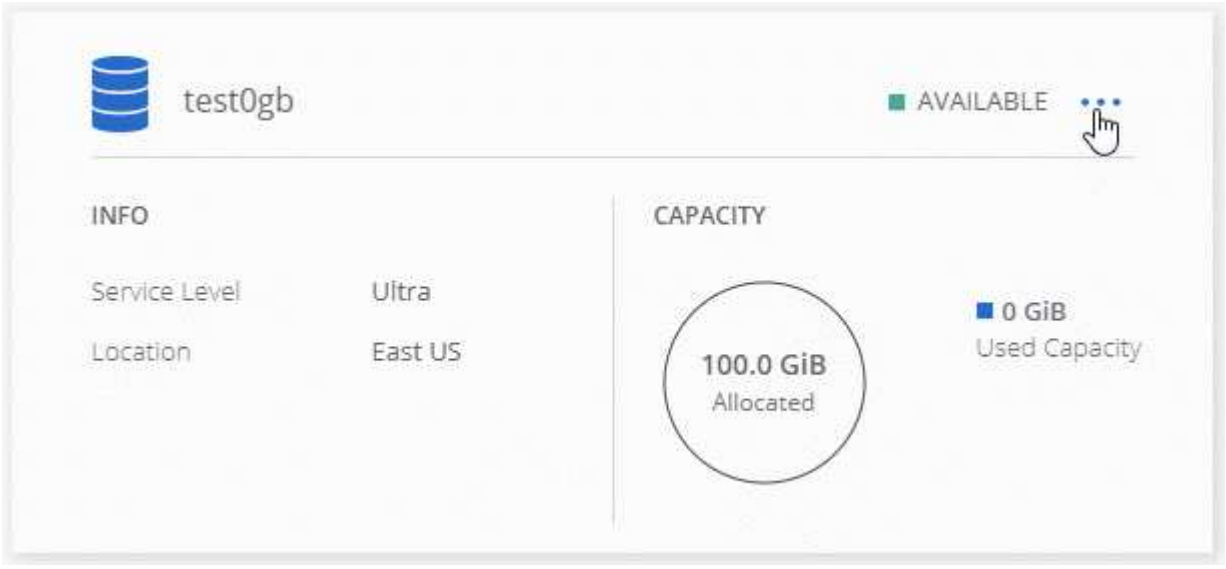
4. Copiez le chemin de montage et utilisez le texte copié pour monter le volume sur un ordinateur Linux.

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 le menu.



3. Cliquez sur **Supprimer**.
4. Confirmez la suppression du volume.

Obtenir de l'aide

Utilisez la discussion de chat Cloud Manager pour toute question générale sur les services.

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 requises pour créer votre demande de support Microsoft.

Cloud Manager permet de télécharger le AutoSupport local sous l'option de menu **support Dashboard**. Ce fichier 7z contient un fichier de débogage Azure qui affiche les communications entrantes et sortantes vers votre compte Azure NetApp Files.

Limites

- Cloud Manager ne prend pas en charge les volumes SMB.
- Cloud Manager ne vous permet pas de gérer les pools de capacité ou les copies Snapshot de volumes.
- La création de volumes peut s'effectuer selon une taille initiale et une seule export policy. La modification d'un volume doit être effectuée depuis l'interface Azure NetApp Files du portail Azure.
- Cloud Manager ne prend pas en charge la réplication des données vers ou depuis Azure NetApp Files.

Liens connexes

- "NetApp Cloud Central : Azure NetApp Files"
- "Documentation Azure NetApp Files"

Gestion d'Cloud Volumes Service pour AWS

Cloud Manager vous permet de découvrir les volumes cloud NFS dans votre "Cloud Volumes Service pour AWS" abonnement. Une fois la découverte terminée, vous pouvez ajouter des volumes cloud NFS supplémentaires directement à partir de Cloud Manager.

Cloud Manager ne prend pas en charge les volumes SMB ou double protocole avec Cloud Volumes Service pour AWS.

Avant de commencer

- Cloud Manager permet de découvrir les abonnements *existing* 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 ce processus d'installation pour chaque région et provisionner votre premier volume depuis Cloud Volumes Service avant de découvrir la région dans 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".

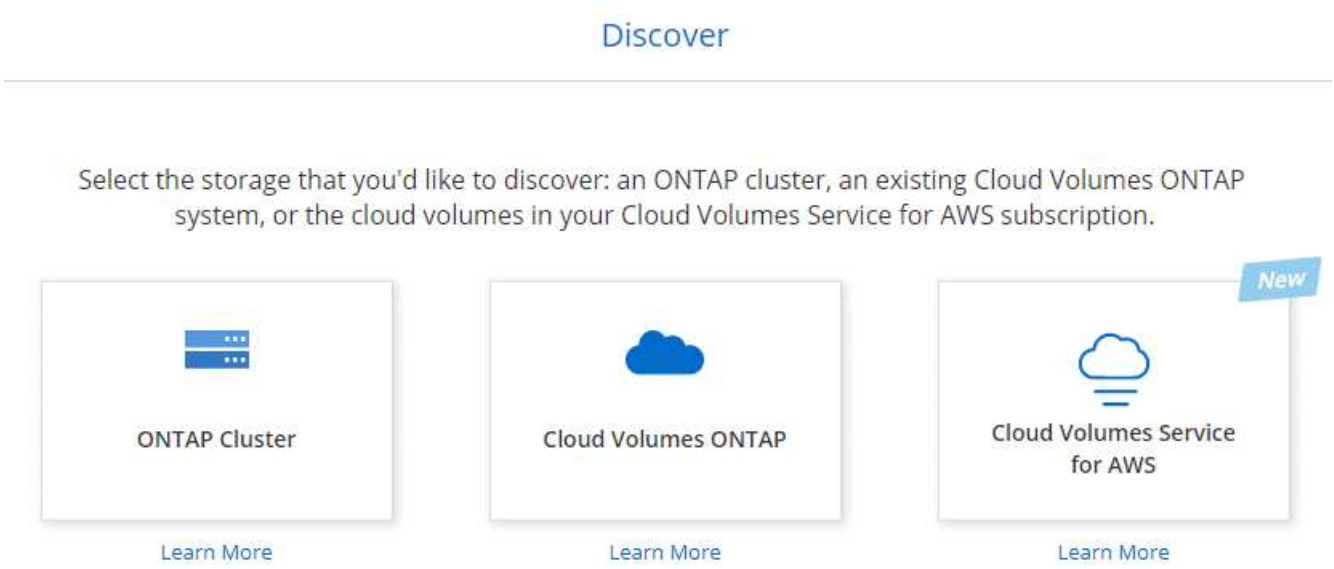
Détection de votre abonnement Cloud Volumes Service pour AWS

Pour commencer, il vous faut découvrir les volumes cloud dans une région AWS. Vous pourrez y découvrir d'autres régions ultérieurement.

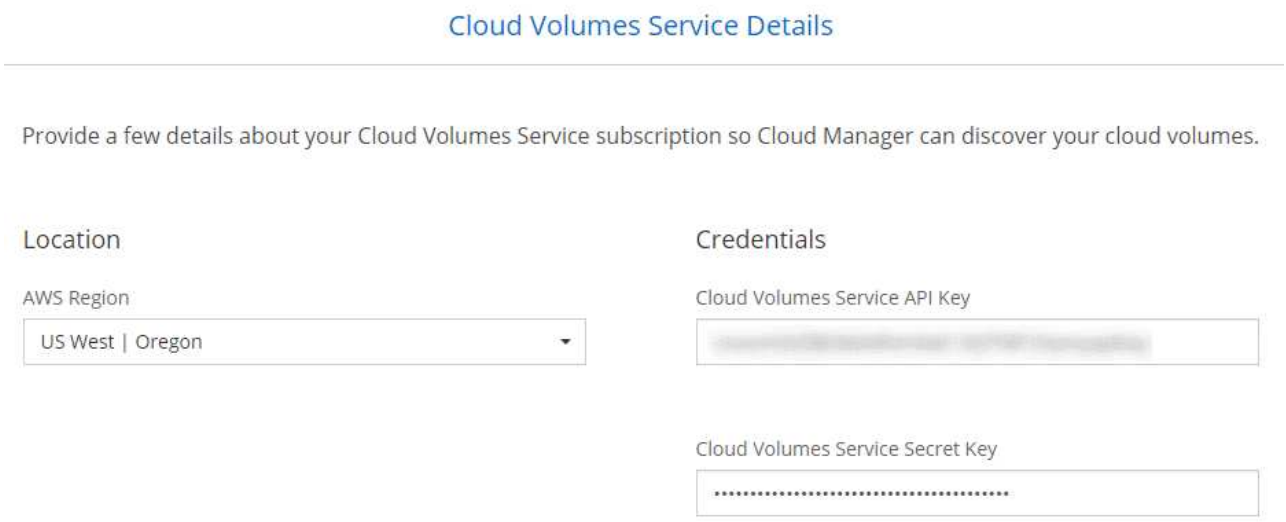
Étapes

1. Sur la page environnements de travail, cliquez sur **découvrir**.

2. Sélectionnez **Cloud Volumes Service pour AWS**.



3. Fournir des informations sur votre abonnement Cloud Volumes Service :
   a. Sélectionnez la région AWS où résident vos volumes cloud.
   b. Entrez la clé API et la clé secrète Cloud volumes. "Pour en savoir plus, consultez la documentation Cloud Volumes Service pour AWS".
   c. Cliquez sur **Go**.



Résultat

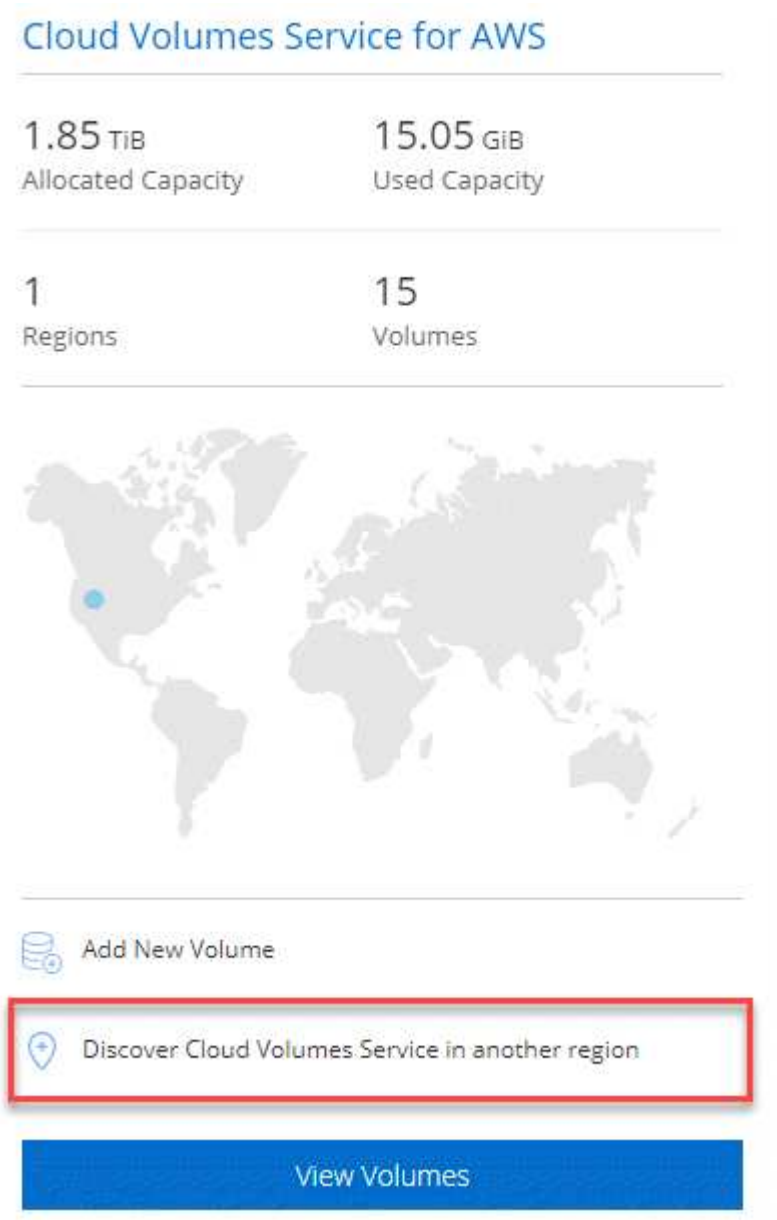
Cloud Manager doit désormais afficher votre configuration Cloud Volumes Service pour AWS sur la page Working Environments.

Découverte de régions supplémentaires

Si vous disposez de volumes cloud dans des régions supplémentaires, vous devez découvrir chaque région.

Étapes

1. Sur la page environnements de travail, sélectionnez l'environnement de travail (mais ne l'ouvrez pas en cliquant deux fois).
2. Dans le volet de droite, cliquez sur **découvrir Cloud Volumes Service dans une autre région**.



3. Fournir des informations sur votre abonnement Cloud Volumes Service :
   a. Sélectionnez la région AWS où résident vos volumes cloud.
   b. Entrez la clé API et la clé secrète Cloud volumes. "Pour en savoir plus, consultez la documentation Cloud Volumes Service pour AWS".
   c. Cliquez sur **Go**.

Résultat

Cloud Manager détecte les informations sur les volumes cloud dans la région sélectionnée.

Création de volumes cloud

Cloud Manager vous permet de créer des volumes cloud NFSv3. Les volumes cloud ne peuvent être créés qu'avec une taille initiale et des règles d'exportation uniques. La modification du volume doit être effectuée depuis l'interface utilisateur de Cloud Volume Service.

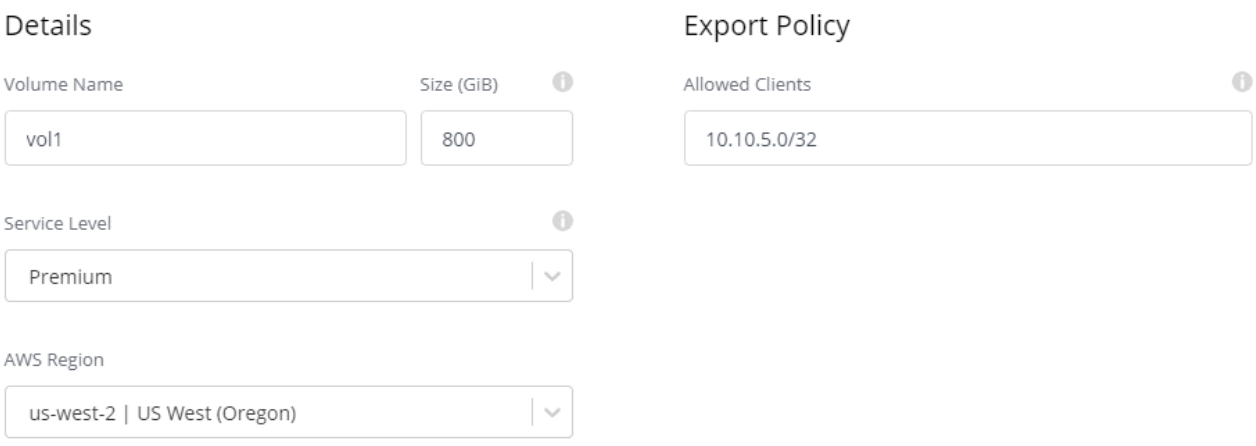
1. Ouvrir l'environnement de travail.
2. Cliquez sur **Ajouter nouveau volume**.
3. Entrez les détails du volume :
   a. Entrez un nom pour le volume.
   b. Spécifiez une taille comprise entre 100 Gio et 90,000 Gio (équivalent à 88 Tibs).

      Cloud Manager affiche les volumes de Gio, tandis que Cloud Volumes Service affiche les volumes en Go.

   c. Spécifier un niveau de service : standard, Premium ou Extreme.

      "En savoir plus sur ces niveaux de service".

   d. Choisissez une région. Vous pouvez créer le volume dans une région découverte de Cloud Manager.
   e. Limitez l'accès client en spécifiant une adresse IP ou un routage inter-domaines (CIDR) sans classe.



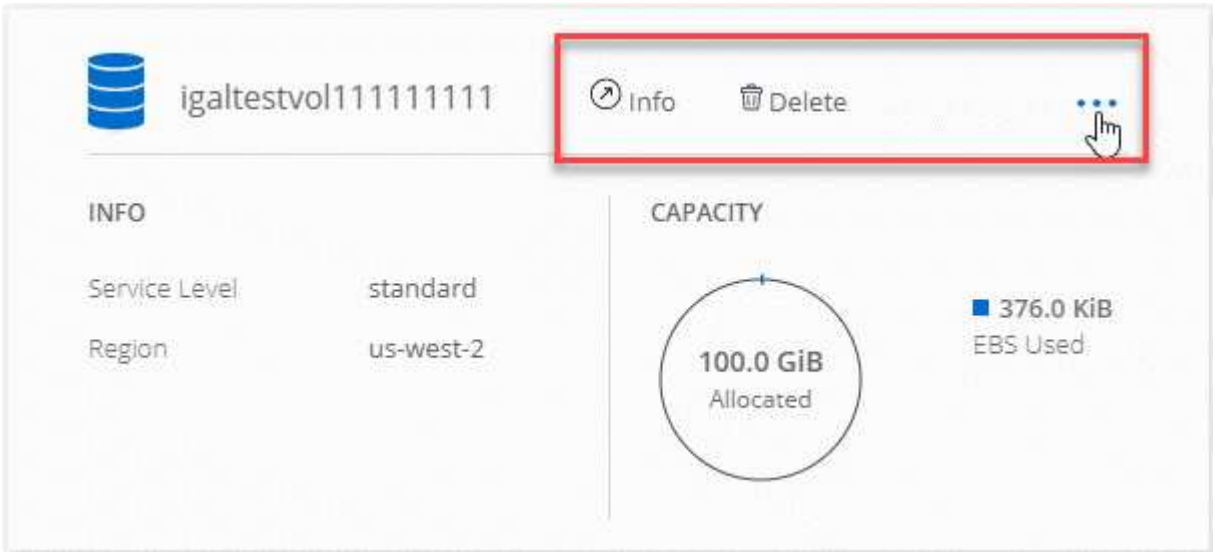
4. Cliquez sur **Go**.

Suppression de volumes Cloud

Supprimez les volumes cloud 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 le menu. Cliquez sur **Supprimer**.



3. Confirmez la suppression du volume.

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 les volumes SMB ou à double protocole.
- Les volumes cloud ne peuvent être créés qu'avec une taille initiale et des règles d'exportation uniques. La modification du volume doit être effectuée depuis l'interface utilisateur de Cloud Volume Service.
- Cloud Manager ne prend pas en charge la réplication des données vers ou depuis un abonnement Cloud Volumes Service pour AWS.
- La suppression de votre abonnement Cloud Volumes Service pour AWS de Cloud Manager n'est pas prise en charge. La découverte d'une région depuis Cloud Manager est gratuite.

Liens connexes

- "NetApp Cloud Central : Cloud Volumes Service pour AWS"
- "Documentation sur NetApp Cloud Volumes Service pour AWS"

API et automatisation

Exemples 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. Deux outils de ce type sont Ansible et Terraform. Nous avons développé des exemples Ansible et Terraform que l’équipe DevOps peut utiliser avec Cloud Manager pour automatiser et intégrer Cloud Volumes ONTAP avec l’infrastructure-as-code.

"Afficher les échantillons d’automatisation".

Par exemple, vous pouvez utiliser des exemples de playbooks Ansible pour déployer Cloud Manager et Cloud Volumes ONTAP, créer un agrégat et créer un volume. Modifiez les échantillons pour votre environnement ou créez de nouveaux manuels de vente basés sur les échantillons.

- 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"

Référence

Questions les plus fréquemment posées : intégrer Cloud Manager avec NetApp Cloud Central

Lorsque vous effectuez une mise à niveau depuis Cloud Manager 3.4 ou une version antérieure, NetApp choisit des systèmes Cloud Manager spécifiques à intégrer NetApp Cloud Central, si ces derniers ne sont pas déjà intégrés. Cette FAQ peut répondre aux questions que vous pourriez avoir sur le processus.

Qu'est-ce que NetApp Cloud Central ?

NetApp Cloud Central fournit un emplacement centralisé pour accéder aux services de données cloud NetApp et les gérer. Ces services vous permettent d'exécuter des applications stratégiques dans le cloud, de créer des sites de reprise après incident automatisés, de sauvegarder vos données SaaS et de migrer et contrôler efficacement les données sur plusieurs clouds.

Pourquoi NetApp intègre-t-il mon système Cloud Manager avec Cloud Central ?

L'intégration de Cloud Manager avec NetApp Cloud Central offre plusieurs avantages, notamment une expérience de déploiement simplifiée, un emplacement unique pour afficher et gérer plusieurs systèmes Cloud Manager et une authentification utilisateur centralisée.

Que se passe-t-il pendant le processus d'intégration ?

NetApp migre tous les comptes utilisateur locaux de votre système Cloud Manager vers l'authentification utilisateur centralisée disponible dans Cloud Central.

Comment fonctionne l'authentification centralisée des utilisateurs ?

Grâce à l'authentification centralisée des utilisateurs, vous pouvez utiliser les mêmes informations d'identification sur les systèmes Cloud Manager et entre Cloud Manager et d'autres services de données, tels que Cloud Sync. Il est également facile de réinitialiser votre mot de passe si vous l'oubliez.

Dois-je m'inscrire à un compte utilisateur Cloud Central ?

NetApp créera un compte utilisateur Cloud Central pour vous lorsque nous intégrerons votre système Cloud Manager avec Cloud Central. Il vous suffit de réinitialiser votre mot de passe pour terminer le processus d'inscription.

Et si j'ai déjà un compte utilisateur Cloud Central ?

Si l'adresse e-mail que vous utilisez pour vous connecter à Cloud Manager correspond à l'adresse e-mail d'un compte utilisateur Cloud Central, vous pouvez vous connecter directement à votre système Cloud Manager.

Que se passe-t-il si mon système Cloud Manager dispose de plusieurs comptes utilisateur ?

NetApp migre tous les comptes utilisateur locaux vers les comptes utilisateur Cloud Central. Chaque utilisateur doit réinitialiser son mot de passe.

Que se passe-t-il si j'ai un compte utilisateur qui utilise la même adresse e-mail sur plusieurs systèmes Cloud Manager ?

Vous n'avez qu'à réinitialiser votre mot de passe une fois, puis vous pouvez utiliser le même compte utilisateur Cloud Central pour vous connecter à chaque système Cloud Manager.

Que se passe-t-il si mon compte d'utilisateur local utilise une adresse e-mail non valide ?

La réinitialisation de votre mot de passe nécessite une adresse électronique valide. Contactez-nous via l'icône de chat disponible en bas à droite de l'interface de Cloud Manager.

Et si j'ai des scripts d'automatisation pour les API Cloud Manager ?

Toutes les API sont rétrocompatibles. Vous devrez mettre à jour les scripts qui utilisent des mots de passe si vous modifiez votre mot de passe lors de la réinitialisation.

Que se passe-t-il si mon système Cloud Manager utilise LDAP ?

Si votre système utilise LDAP, NetApp ne peut pas intégrer automatiquement le système à Cloud Central. Vous devez effectuer manuellement les opérations suivantes :

1. Déployez un nouveau système Cloud Manager à partir de "NetApp Cloud Central".
2. "Configuration d'LDAP avec le nouveau système".
3. "Découvrir les systèmes Cloud Volumes ONTAP existants" À partir du nouveau système Cloud Manager.
4. Supprimez l'ancien système Cloud Manager.

Est-ce que j'ai installé mon système Cloud Manager ?

Non NetApp intégrera des systèmes avec Cloud Central, quel que soit leur emplacement, qu'il s'agisse d'AWS, d'Azure ou sur votre site.

La seule exception est l'environnement AWS Commercial Cloud Services.

Règles de groupe de sécurité pour AWS

Cloud Manager crée des groupes de sécurité AWS qui incluent les règles entrantes et sortantes dont Cloud Manager et Cloud Volumes ONTAP ont besoin pour 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 Manager

Le groupe de sécurité de Cloud Manager requiert à la fois des règles entrantes et sortantes.

Règles entrantes pour Cloud Manager

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 Cloud Manager
HTTP	80	Fournit un accès HTTP depuis les navigateurs Web du client vers la console Web Cloud Manager et les connexions à partir de Cloud Compliance
HTTPS	443	Fournit un accès HTTPS depuis les navigateurs Web clients vers la console Web Cloud Manager
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 pour Cloud Manager

Le groupe de sécurité prédéfini pour Cloud Manager 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 Manager 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 Cloud Manager.

L'adresse IP source est l'hôte Cloud Manager.

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 Cloud Volumes ONTAP

Le groupe de sécurité pour Cloud Volumes ONTAP requiert des règles entrantes et sortantes.

Règles entrantes pour Cloud Volumes ONTAP

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 pour Cloud Volumes ONTAP

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	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	FRV de données (NFS, CIFS)	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	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 reposant depuis Cloud Manager

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 de Cloud Manager	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 de groupe de sécurité pour Azure

Cloud Manager crée des groupes de sécurité Azure qui incluent les règles entrantes et sortantes dont Cloud Manager et Cloud Volumes ONTAP ont besoin pour 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 Manager

Le groupe de sécurité de Cloud Manager requiert à la fois des règles entrantes et sortantes.

Règles entrantes pour Cloud Manager

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 Cloud Manager
80	HTTP	Fournit un accès HTTP depuis les navigateurs Web clients vers la console Web de Cloud Manager
443	HTTPS	Fournit un accès HTTPS depuis les navigateurs Web clients vers la console Web Cloud Manager

Règles de sortie pour Cloud Manager

Le groupe de sécurité prédéfini pour Cloud Manager 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 Manager inclut les règles de sortie suivantes.

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

Port	Protocole	Objectif
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 Manager.

L'adresse IP source est l'hôte Cloud Manager.

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

Service	Port	Protocole	Destination	Objectif
DNS	53	UDP	DNS	Utilisé pour la résolution DNS par Cloud Manager

Règles pour Cloud Volumes ONTAP

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
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

Priorité et nom	Port et protocole	Source et destination	Description
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

Priorité et nom	Port et protocole	Source et destination	Description
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 pour Cloud Volumes ONTAP

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	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	FRV de données (NFS, CIFS)	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	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
DHCPS	67	UDP	FRV de gestion des nœuds	DHCP	Serveur DHCP

Service	Port	Protocole	Source	Destination	Objectif
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 pare-feu pour GCP

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.

Règles pour Cloud Manager

Les règles de pare-feu de Cloud Manager requièrent des règles entrantes et sortantes.

Règles entrantes pour Cloud Manager

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 Cloud Manager

Protocole	Port	Objectif
HTTP	80	Fournit un accès HTTP depuis les navigateurs Web clients vers la console Web de Cloud Manager
HTTPS	443	Fournit un accès HTTPS depuis les navigateurs Web clients vers la console Web Cloud Manager

Règles de sortie pour Cloud Manager

Les règles de pare-feu prédéfinies pour Cloud Manager 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 Cloud Manager incluent 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 Cloud Manager.

L'adresse IP source est l'hôte Cloud Manager.

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

Règles pour Cloud Volumes ONTAP

Le groupe de sécurité pour Cloud Volumes ONTAP requiert des règles entrantes et sortantes.

Règles entrantes pour Cloud Volumes ONTAP

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 pour Cloud Volumes ONTAP

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	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	FRV de données (NFS, CIFS)	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	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

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 n'êtes pas sûr de la page que vous devez utiliser, lisez ci-dessous et nous vous dirigera vers la page de droite en fonction de votre objectif.

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
Déploiement de Cloud Volumes ONTAP PAYGO pour les versions 9.6 et ultérieures	"Cloud Manager (pour Cloud Volumes ONTAP)"	Cette page AWS Marketplace permet de payer la version PAYGO de Cloud Volumes ONTAP 9.6 et les versions ultérieures. Il permet également de charger les fonctions complémentaires Cloud Volumes ONTAP. 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 4 de ce tableau.
Activation des fonctionnalités d'extension pour Cloud Volumes ONTAP (PAYGO ou BYOL)		
Activer le déploiement d'Cloud Volumes ONTAP à l'aide d'une licence achetée auprès de NetApp (BYOL)	• "Cloud Volumes ONTAP pour AWS (BYOL)" • "Cloud Volumes ONTAP pour AWS - haute disponibilité (BYOL)"	Ces pages AWS Marketplace vous permettent d'abonner aux versions à un seul nœud ou haute disponibilité d'Cloud Volumes ONTAP BYOL.
Déployez Cloud Manager depuis AWS Marketplace à l'aide d'une ami	"NetApp Cloud Manager (pour NetApp Cloud Volumes ONTAP)"	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).

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.
"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.

Actions	Objectif
"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 »,	Gère le compartiment S3 qu'un système Cloud Volumes ONTAP utilise comme niveau de capacité.
« Km:liste* », « km:décrire* »	Obtenez des informations sur les clés à partir du service AWS Key Management Service.
"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.

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.
« 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.

Actions	Objectif
« Microsoft.Resources/déploiements/opérations/lecture », « Microsoft.Resources/déploiements/lecture », « Microsoft.Resources/déploiements/écriture »,	Déploie Cloud Volumes ONTAP à partir d'un modèle.
« 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.

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.
- 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.

Actions	Objectif
- 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.
- 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	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.

Configurations par défaut

Par défaut, les informations sur la configuration de Cloud Manager et de Cloud Volumes ONTAP peuvent vous aider à administrer les systèmes.

Configuration par défaut de Cloud Manager sous Linux

Si vous devez dépanner Cloud Manager ou votre hôte Linux, il peut vous aider à comprendre comment Cloud Manager est configuré.

- Si vous avez déployé Cloud Manager à partir de NetApp Cloud Central (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 Cloud Manager est Red Hat Enterprise Linux 7.4 (HVM).

Le système d'exploitation n'inclut pas d'interface graphique. Vous devez utiliser un terminal pour accéder au système.

- Le dossier d'installation de Cloud Manager 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
  - Java
  - Kubectl
  - MySQL
  - Tridentctl
  - Wget

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.

- 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 SVM de service de données lorsqu'il déploie Cloud Volumes ONTAP. Les multiples SVM n'sont pas pris en charge.
- 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 à Cloud Manager via HTTPS.

  Lorsque vous êtes connecté à Cloud Manager, les sauvegardes sont accessibles depuis https://ipaddress/occm/offboxconfig/

- 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 SSD à usage générique :
  - Un disque de 140 Go pour les données racines (un par nœud)
  - 9.6 et versions ultérieures : un disque de 86 Go pour les données de démarrage (un par nœud)
  - 9.5 et versions antérieures : un disque de 45 Go pour les données de démarrage (un par nœud)
- 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)

- Deux disques SSD Premium :
  - Un disque de 90 Go pour les données de démarrage
  - Un disque de 140 Go pour les données racines
- Un snapshot Azure pour chaque disque d'initialisation et disque racine

Azure (paires HA)

- Deux disques SSD premium de 90 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 128 Go pour économiser les cœurs (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.

Rôles

Les rôles Administrateur de compte et Administrateur d'espace de travail fournissent des autorisations spécifiques aux utilisateurs.

Tâche	Administrateur du compte	Administrateur de l'espace de travail
Gérer les environnements de travail	Oui.	Oui, pour les espaces de travail associés
Afficher l'état de la réplication des données	Oui.	Oui, pour les espaces de travail associés
Afficher la chronologie	Oui.	Oui, pour les espaces de travail associés
Supprimer les environnements de travail	Oui.	Non
Connectez les clusters Kubernetes à Cloud Volumes ONTAP	Oui.	Non
Recevoir le rapport Cloud Volumes ONTAP	Oui.	Non
Gérez les comptes Cloud Central	Oui.	Non
Gérez les comptes des fournisseurs cloud	Oui.	Non
Modifiez les paramètres de Cloud Manager	Oui.	Non
Afficher et gérer le tableau de bord du support	Oui.	Non
Supprimez les environnements de travail de Cloud Manager	Oui.	Non
Mettez à jour Cloud Manager	Oui.	Non
Installez un certificat HTTPS	Oui.	Non
Configurez Active Directory	Oui.	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"

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.

- "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"
- 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 un cluster différent que le volume d'origine pour accélérer les données access.es procédure d'activation rapide d'un SVM de destination après un incident, puis de réactiver le SVM source.

- "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.

- "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.

- "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 des versions précédentes de Cloud Manager est disponible si vous n’utilisez pas la dernière version.

"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 3.7.4"
- "Avis concernant Cloud Manager 3.7.1"
- "Avis concernant Cloud Manager 3.7"
- "Avis concernant le Cloud Backup Service"