Gérer Cloud Volumes ONTAP

Cloud Manager 3.8

NetApp
March 25, 2024

Sommaire

Gérer Cloud Volumes ONTAP

Apprendre

Découvrez Cloud Volumes ONTAP

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

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

- Fonctionnalités d'efficacité du stockage

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

- Haute disponibilité

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

- Protection des données

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

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

- Tiering des données

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

- La cohérence des applications

  Cohérence des copies NetApp Snapshot avec NetApp SnapCenter

- Sécurité des données

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

- Contrôles de conformité à la confidentialité

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

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

"Afficher les configurations Cloud Volumes ONTAP prises en charge"

"En savoir plus sur Cloud Volumes ONTAP"

Stockage

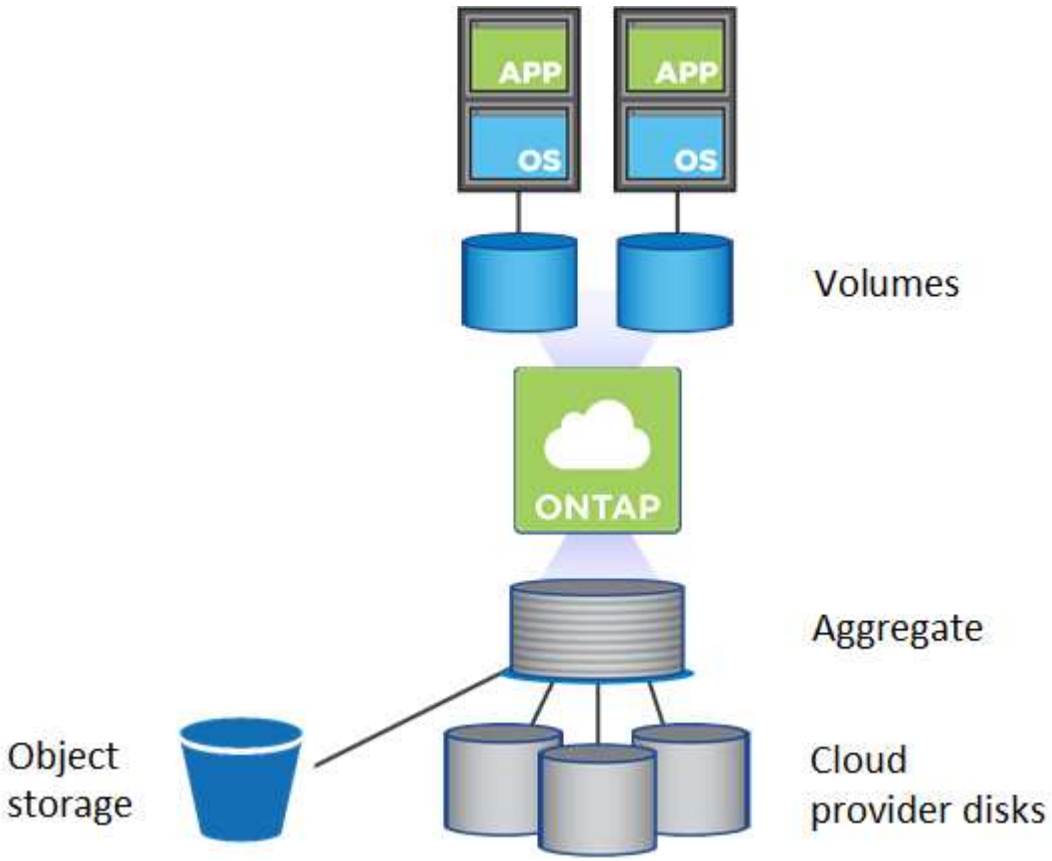
Disques et agrégats

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

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

Présentation

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



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

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

Le stockage AWS

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

Stockage EBS

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

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

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

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

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

Stockage NVMe local

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

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

Le stockage Azure

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

Systèmes à un seul nœud

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

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

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

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

Paires HA

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

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

Stockage GCP

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

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

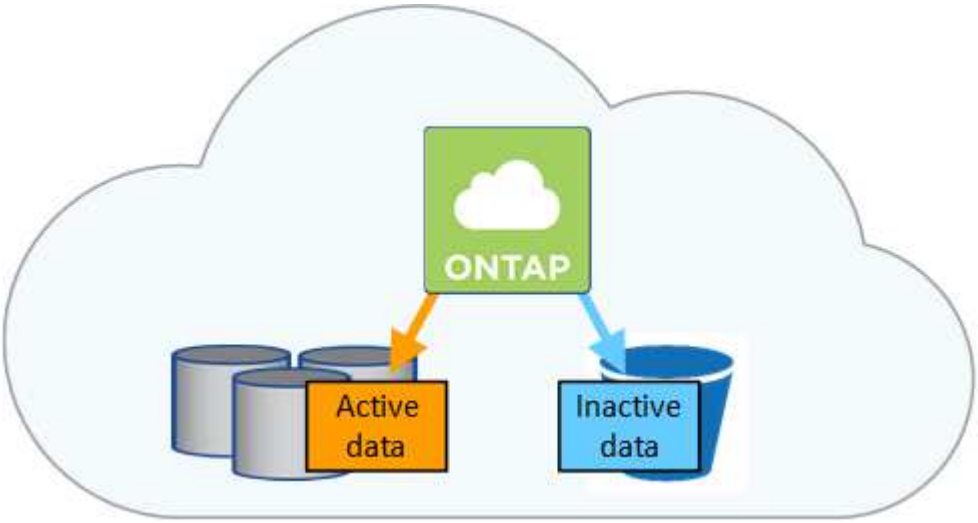
- Liens connexes*
- "Documentation sur Google Cloud Platform : options de stockage"
- "Consultez les limites de stockage des Cloud Volumes ONTAP dans GCP"

Type de RAID

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

Vue d'ensemble du hiérarchisation des données

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



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

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

Tiering des données dans AWS

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

Tier de performance

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

Des disques SSD/HDD FAS

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

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

Classes de stockage

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

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

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

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

Tiering des données dans Azure

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

Tier de performance

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

Des disques SSD/HDD FAS

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

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

Les niveaux d'accès au stockage

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

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

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

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

Tiering des données dans GCP

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

Tier de performance

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

Des disques SSD/HDD FAS

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

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

Classes de stockage

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

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

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

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

Tiering des données et limites de capacité

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

Stratégies de hiérarchisation des volumes

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

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

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

Snapshot uniquement

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

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

Tout

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

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

Auto

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

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

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

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

Aucune

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

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

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

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

- Auto : 31 jours
- Snapshot uniquement : 2 jours

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

Configuration du tiering des données

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

Gestion du stockage

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

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

Provisionnement du stockage

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

Provisionnement simplifié

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

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

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

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

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

Sélection de la taille du disque pour les agrégats dans AWS

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

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

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

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

Allocation avancée

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

Gestion de la capacité

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

Gestion automatique de la capacité

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

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

Les exemples suivants illustrent le fonctionnement de ce mode :

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

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

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

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

Gestion des LUN avec gestion automatique de la capacité

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

Gestion des inodes avec gestion automatique de la capacité

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

Gestion manuelle de la capacité

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

Flash cache

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

Qu'est-ce que Flash cache ?

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

Instances prises en charge dans AWS

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

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

Type de VM pris en charge dans Azure

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

Limites

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

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

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

Stockage WORM

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

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

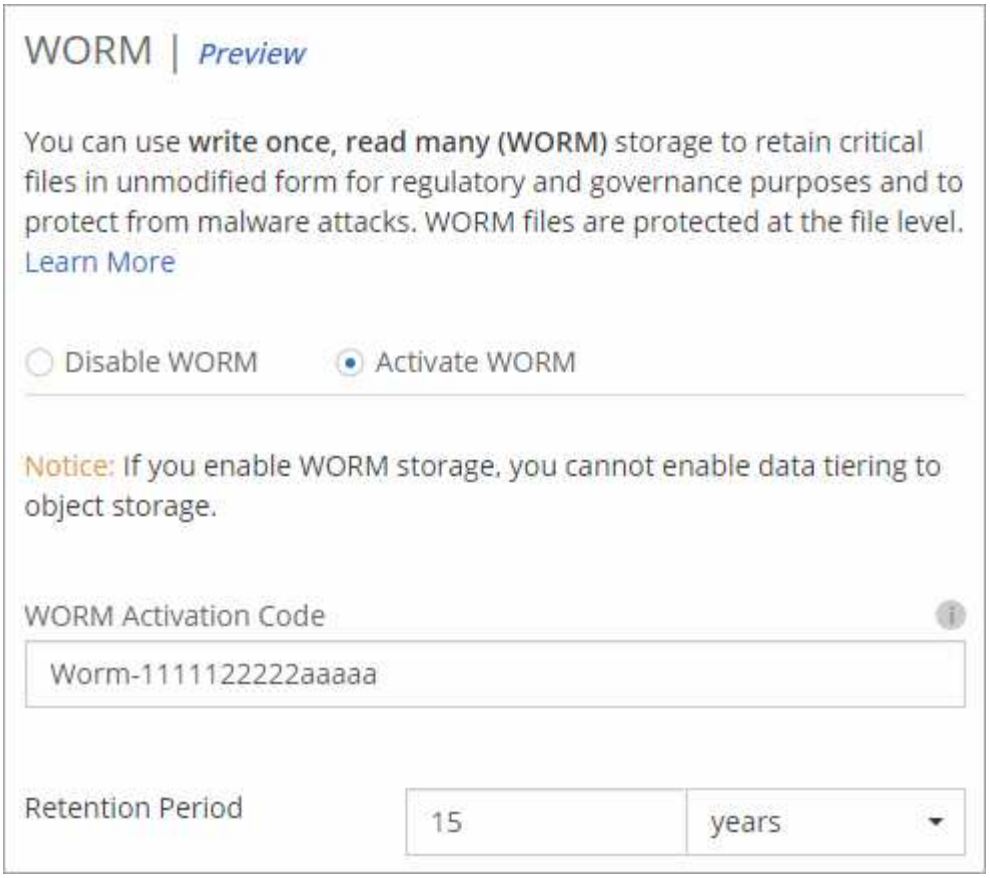
Une fois la période de conservation écoulée, vous êtes responsable de la suppression des fichiers dont vous n'avez plus besoin.

Activation du stockage WORM

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

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

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



Validation de fichiers sur WORM

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

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

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

Limites

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

Paires haute disponibilité

Paires haute disponibilité dans AWS

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

Présentation

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

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

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

Reprise et remise du stockage

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

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

RPO et RTO

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

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

Modèles de déploiement HA

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

Cloud Volumes ONTAP HA dans plusieurs zones de disponibilité

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

Accès aux données NFS et CIFS

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

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

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

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

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

Accès aux données iSCSI

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

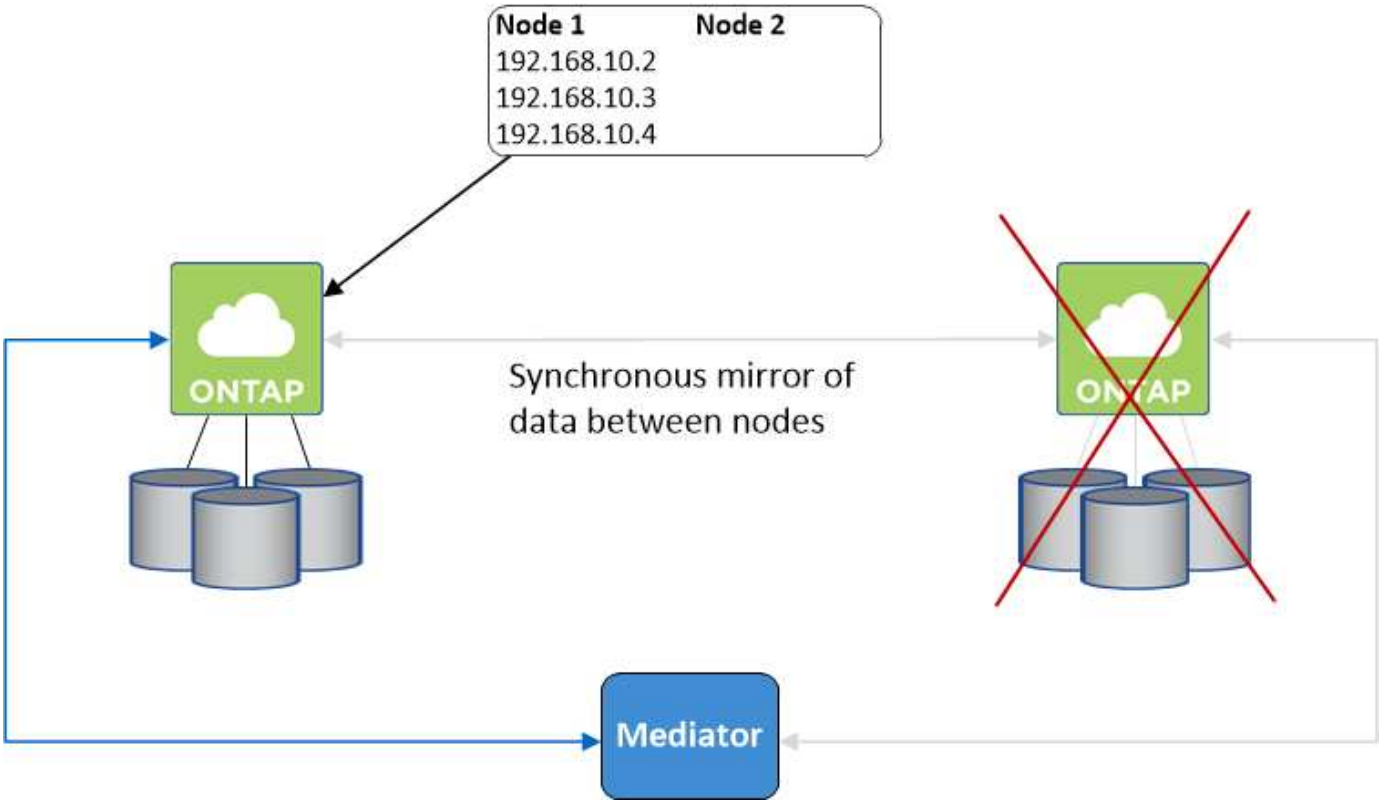
Reprise et remise du stockage pour iSCSI

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

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

Reprise et remise du stockage pour NAS

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



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

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

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

Cloud Volumes ONTAP HA dans une seule zone de disponibilité

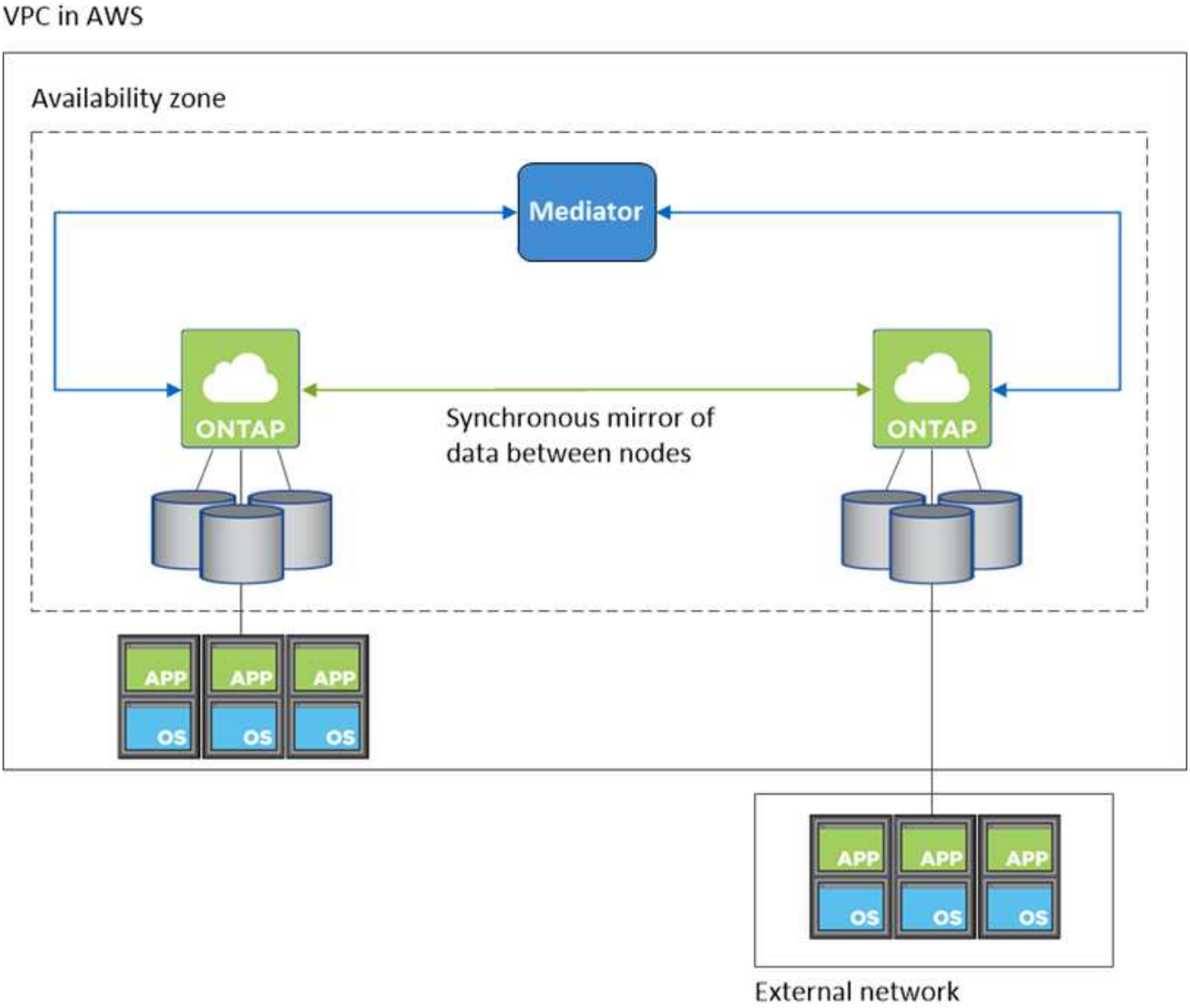
Le déploiement d'une configuration HA dans une seule zone de disponibilité (AZ) peut garantir une haute disponibilité de vos données en cas de défaillance d'une instance exécutant un nœud Cloud Volumes ONTAP. Toutes les données sont accessibles en mode natif depuis l'extérieur du VPC.

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

Accès aux données

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

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



Reprise et remise du stockage

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

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

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

Fonctionnement du stockage dans une paire haute disponibilité

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

Allocation du stockage

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

Configurations de stockage

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

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

Attentes en matière de performances pour une configuration haute disponibilité

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

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

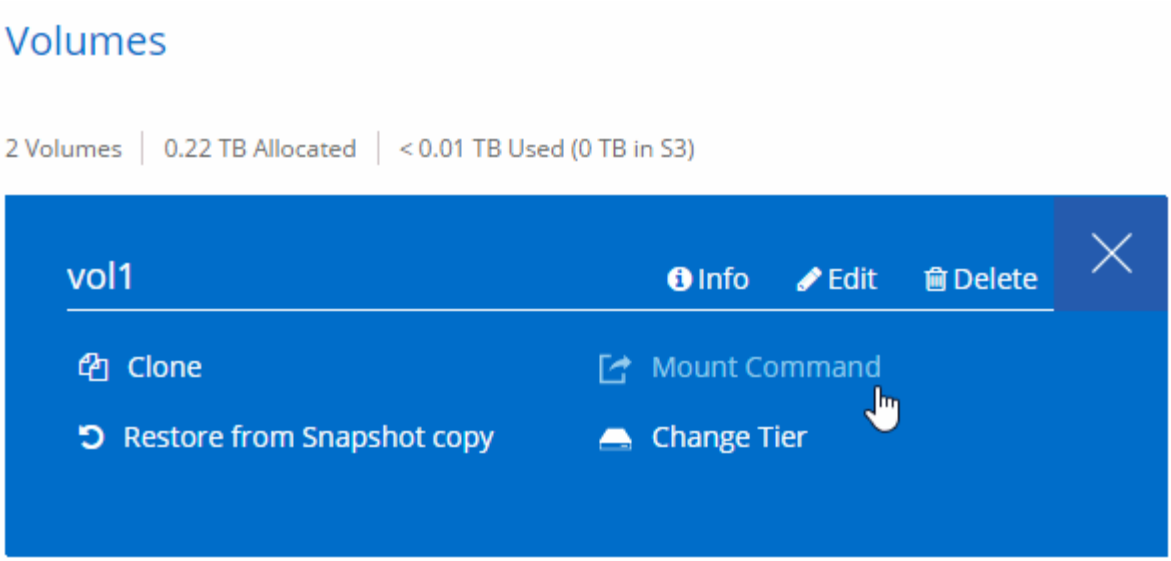
Pour plus d'informations sur les performances de Cloud Volumes ONTAP, reportez-vous à "Performance".

Accès client au stockage

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

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

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

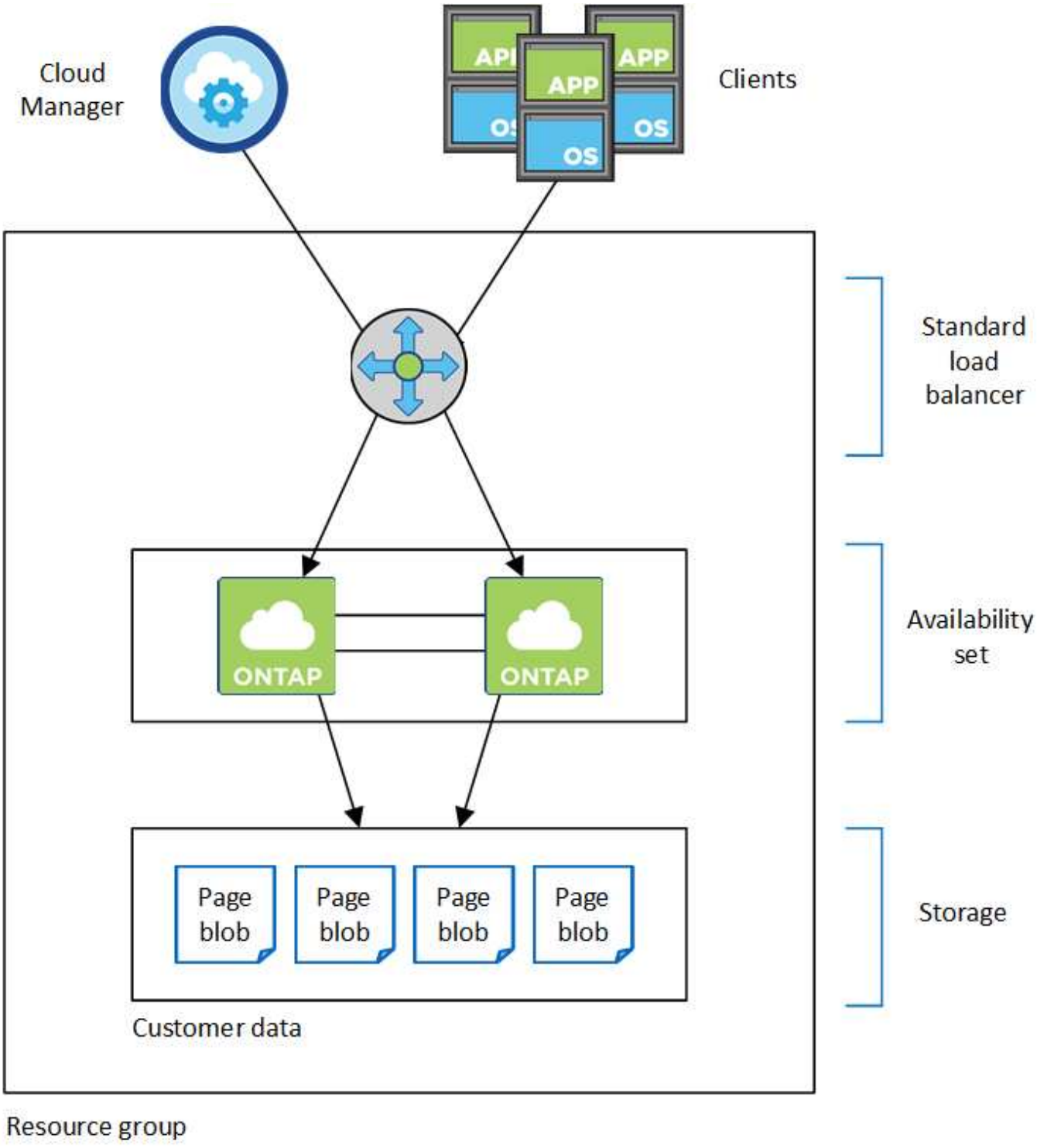


Paires haute disponibilité dans Azure

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

Composants DE HAUTE DISPONIBILITÉ

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



Les composants Azure que Cloud Manager déploie sont les suivants :

Équilibreur de la charge Azure Standard

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

Ensemble de disponibilité

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

Disques

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

Comptes de stockage

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

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

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

RPO et RTO

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

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

Reprise et remise du stockage

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

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

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

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

Configurations de stockage

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

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

Limitations de LA HAUTE DISPONIBILITÉ

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

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

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

"Découvrez comment déployer un système HA dans Azure".

L'évaluation

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

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

Essais gratuits de 30 jours pour PAYGO

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

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

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

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

Licences d'évaluation pour BYOL

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

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

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

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

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

Licences

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

Licences de système BYOL

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

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

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

Gestion des licences pour un nouveau système

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

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

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

Avertissement d'expiration de licence

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

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

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

redémarrez, il s'arrête de nouveau.

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

Renouvellement de la licence

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

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

Licences de sauvegarde BYOL

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

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

Sécurité

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

Cryptage des données au repos

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

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

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

Solutions de chiffrement NetApp (NVE et NAE)

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

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

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

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

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

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

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

Service de gestion des clés AWS

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

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

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

Chiffrement de service de stockage Azure

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

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

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

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

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

Chiffrement par défaut Google Cloud Platform

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

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

Analyse antivirus ONTAP

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

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

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

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

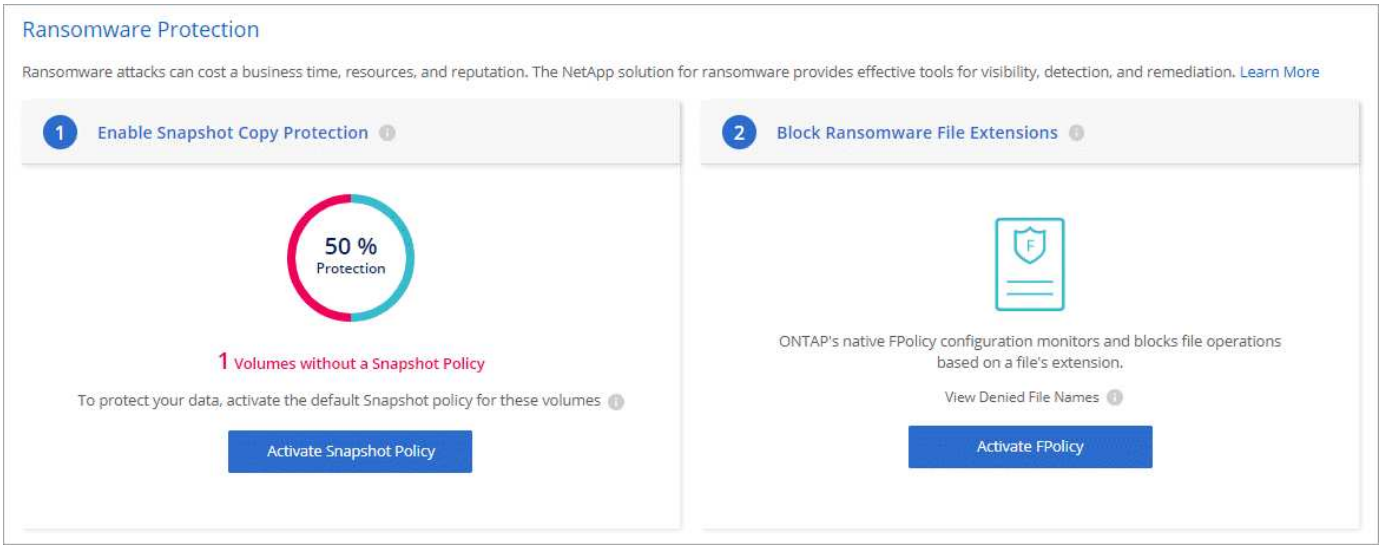
Protection par ransomware

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

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

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

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



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

Performance

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

- Cloud Volumes ONTAP pour AWS

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

- Cloud Volumes ONTAP pour Microsoft Azure

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

- Cloud Volumes ONTAP pour Google Cloud

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

Configuration par défaut pour Cloud Volumes ONTAP

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

Valeurs par défaut

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

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

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

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

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

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

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

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

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

Données de démarrage et de racine pour Cloud Volumes ONTAP

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

AWS

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

Azure (un seul nœud)

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

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

Azure (paires HA)

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

GCP

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

Où résident les disques

Cloud Manager dispose du stockage comme suit :

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

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

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

Le cryptage

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

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

Commencez dans AWS

Mise en route avec Cloud Volumes ONTAP pour AWS

Découvrez Cloud Volumes ONTAP pour AWS en quelques étapes.

Créer un connecteur

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

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

Planification de la configuration

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

Configurez votre réseau

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

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

3. Configurez un terminal VPC sur le service S3.

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

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

Configuration du KMS AWS

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

Lancez Cloud Volumes ONTAP à l'aide de Cloud Manager

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

Liens connexes

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

Planification de votre configuration Cloud Volumes ONTAP dans AWS

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

Choix d'un type de licence

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

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

Compréhension des limites de stockage

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

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

Dimensionnement de votre système dans AWS

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

Type d'instance

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

Type de disque EBS

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

Taille des disques EBS

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

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

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

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

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

Choix d'une configuration qui prend en charge Flash cache

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

Fiche technique d’informations sur le réseau AWS

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

Informations réseau pour Cloud Volumes ONTAP

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

Informations réseau pour une paire HA dans plusieurs AZS

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

Sélection d’une vitesse d’écriture

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

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

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

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

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

Quand utiliser une vitesse d’écriture élevée

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

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

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

Choix d’un profil d’utilisation du volume

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

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

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

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

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

Configurez votre réseau

Configuration réseau requise pour Cloud Volumes ONTAP dans AWS

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

Conditions générales requises pour Cloud Volumes ONTAP

Les exigences suivantes doivent être respectées dans AWS.

Accès Internet sortant pour les nœuds Cloud Volumes ONTAP

Les nœuds Cloud Volumes ONTAP nécessitent un accès Internet sortant pour envoyer des messages à NetApp AutoSupport, qui surveille de façon proactive l'état de votre stockage.

Les règles de routage et de pare-feu doivent autoriser le trafic AWS HTTP/HTTPS vers les terminaux suivants pour que Cloud Volumes ONTAP puisse envoyer les messages AutoSupport :

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

Si vous disposez d'une instance NAT, vous devez définir une règle de groupe de sécurité entrante qui autorise le trafic HTTPS du sous-réseau privé vers Internet.

"Découvrez comment configurer AutoSupport".

Accès Internet sortant pour le médiateur haute disponibilité

L'instance de médiateur haute disponibilité doit disposer d'une connexion sortante au service AWS EC2 pour qu'il puisse faciliter le basculement du stockage. Pour fournir la connexion, vous pouvez ajouter une adresse IP publique, spécifier un serveur proxy ou utiliser une option manuelle.

L'option manuelle peut être une passerelle NAT ou un terminal VPC d'interface, du sous-réseau cible au service AWS EC2. Pour plus de détails sur les terminaux VPC, reportez-vous à "Documentation AWS : terminaux VPC d'interface (AWS PrivateLink)".

Nombre d'adresses IP

Cloud Manager attribue le nombre suivant d'adresses IP à Cloud Volumes ONTAP dans AWS :

- Un seul nœud : 6 adresses IP
- Paires HA en simple AZS : 15 adresses
- Paires HAUTE DISPONIBILITÉ dans plusieurs adresses AZS : 15 ou 16 adresses IP

Notez que Cloud Manager crée une LIF de gestion des SVM sur des systèmes à un seul nœud, mais pas sur des paires haute disponibilité dans une même zone de disponibilité. Vous pouvez choisir de créer ou non une LIF de gestion SVM sur des paires HA dans plusieurs AZS.

Une LIF est une adresse IP associée à un port physique. Une LIF de gestion SVM est nécessaire pour les outils de gestion tels que SnapCenter.

Groupes de sécurité

Vous n'avez pas besoin de créer de groupes de sécurité car Cloud Manager le fait pour vous. Si vous devez utiliser votre propre, reportez-vous à la section "Règles de groupe de sécurité".

Connexion de Cloud Volumes ONTAP à AWS S3 pour le hiérarchisation des données

Si vous souhaitez utiliser EBS comme niveau de performance et AWS S3 comme niveau de capacité, vous devez vous assurer que Cloud Volumes ONTAP est connecté à S3. La meilleure façon de fournir cette connexion est de créer un terminal VPC vers le service S3. Pour obtenir des instructions, reportez-vous à la section "Documentation AWS : création d'un terminal de passerelle".

Lorsque vous créez le terminal VPC, veillez à sélectionner la région, le VPC et la table de routage correspondant à l'instance Cloud Volumes ONTAP. Vous devez également modifier le groupe de sécurité pour ajouter une règle HTTPS sortante qui active le trafic vers le terminal S3. Dans le cas contraire, Cloud Volumes ONTAP ne peut pas se connecter au service S3.

Si vous rencontrez des problèmes, reportez-vous à la section "Centre de connaissances du support AWS : pourquoi ne puis-je pas me connecter à un compartiment S3 à l'aide d'un terminal VPC de passerelle ?"

Connexions aux systèmes ONTAP dans d'autres réseaux

Pour répliquer des données entre un système Cloud Volumes ONTAP dans AWS et ONTAP sur d'autres réseaux, vous devez disposer d'une connexion VPN entre AWS VPC et l'autre réseau, par exemple Azure VNet ou votre réseau d'entreprise. Pour obtenir des instructions, reportez-vous à la section "Documentation AWS : configuration d'une connexion VPN AWS".

DNS et Active Directory pour CIFS

Si vous souhaitez provisionner le stockage CIFS, vous devez configurer DNS et Active Directory dans AWS ou étendre votre configuration sur site à AWS.

Le serveur DNS doit fournir des services de résolution de noms pour l'environnement Active Directory. Vous pouvez configurer les jeux d'options DHCP pour qu'ils utilisent le serveur DNS EC2 par défaut, qui ne doit pas être le serveur DNS utilisé par l'environnement Active Directory.

Pour obtenir des instructions, reportez-vous à la section "Documentation AWS : active Directory Domain Services sur le cloud AWS : déploiement de référence rapide".

Besoins en paires haute disponibilité dans plusieurs AZS

D'autres exigences de mise en réseau AWS s'appliquent aux configurations Cloud Volumes ONTAP HA qui utilisent plusieurs zones de disponibilité (AZS). Avant de lancer une paire haute disponibilité, vous devez consulter ces exigences car vous devez saisir les informations de mise en réseau dans Cloud Manager.

Pour comprendre le fonctionnement des paires haute disponibilité, voir "Paires haute disponibilité".

Zones de disponibilité

Ce modèle de déploiement haute disponibilité utilise plusieurs AZS pour assurer la haute disponibilité de vos données. Vous devez utiliser un système AZ dédié pour chaque instance Cloud Volumes ONTAP et l'instance médiateur, qui fournit un canal de communication entre la paire HA.

Adresses IP flottantes pour les données NAS et la gestion de cluster/SVM

Les configurations HAUTE DISPONIBILITÉ de plusieurs AZS utilisent des adresses IP flottantes qui migrent entre les nœuds en cas de défaillance. Sauf vous, ils ne sont pas accessibles de manière native depuis l'extérieur du VPC "Configuration d'une passerelle de transit AWS".

Une adresse IP flottante concerne la gestion du cluster, l'une concerne les données NFS/CIFS sur le nœud

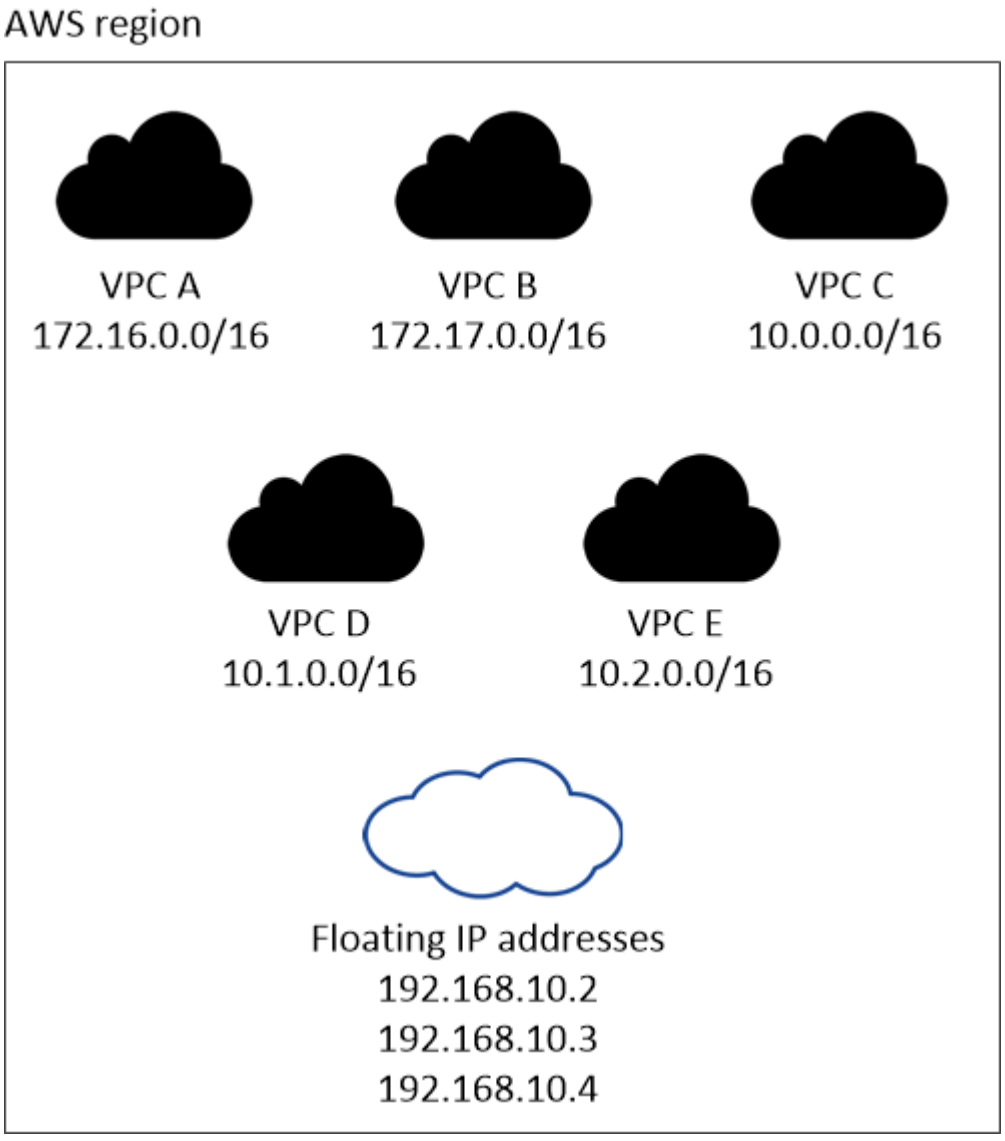
1 et l'autre les données NFS/CIFS sur le nœud 2. Une quatrième adresse IP flottante est facultative pour la gestion des SVM.

> Une adresse IP flottante est requise pour la LIF de management du SVM si vous utilisez SnapDrive pour Windows ou SnapCenter avec la paire haute disponibilité. Si vous ne spécifiez pas l'adresse IP lors du déploiement du système, vous pouvez créer la LIF plus tard. Pour plus de détails, voir "Configuration de Cloud Volumes ONTAP".

Vous devez saisir les adresses IP flottantes dans Cloud Manager lors de la création d'un environnement de travail Cloud Volumes ONTAP HA. Cloud Manager alloue les adresses IP à la paire HA lors du lancement du système.

Les adresses IP flottantes doivent être en dehors des blocs CIDR sur tous les VPC de la région AWS dans laquelle vous déployez la configuration HA. Considérez les adresses IP flottantes comme un sous-réseau logique en dehors des VPC de votre région.

L'exemple suivant illustre la relation entre les adresses IP flottantes et les VPC d'une région AWS. Alors que les adresses IP flottantes sont en dehors des blocs CIDR pour tous les VPC, elles sont routables vers les sous-réseaux via des tables de routage.



Cloud Manager crée automatiquement des adresses IP statiques pour l'accès iSCSI et pour l'accès NAS des clients en dehors du VPC. Vous n'avez pas besoin de répondre à des exigences relatives à ces types d'adresses IP.

Passerelle de transport pour activer l'accès IP flottant depuis l'extérieur du VPC

"Configuration d'une passerelle de transit AWS" Pour permettre l'accès aux adresses IP flottantes d'une paire haute disponibilité de l'extérieur du VPC où réside la paire haute disponibilité.

Tables de routage

Une fois que vous avez spécifié les adresses IP flottantes dans Cloud Manager, vous devez sélectionner les tables de route qui doivent inclure des routes vers les adresses IP flottantes. Cela permet au client d'accéder à la paire haute disponibilité.

Si vous n'avez qu'une seule table de routage pour les sous-réseaux dans votre VPC (la table de routage principale), Cloud Manager ajoute automatiquement les adresses IP flottantes à cette table de routage. Si vous avez plusieurs tables de routage, il est très important de sélectionner les tables de routage appropriées au lancement de la paire haute disponibilité. Dans le cas contraire, certains clients n'ont peut-être pas accès à Cloud Volumes ONTAP.

Par exemple, vous pouvez avoir deux sous-réseaux associés à différentes tables de routage. Si vous sélectionnez la table de routage A, mais pas la table de routage B, les clients du sous-réseau associé à la table de routage A peuvent accéder à la paire HA, mais les clients du sous-réseau associé à la table de routage B ne peuvent pas.

Pour plus d'informations sur les tables de routage, voir "Documentation AWS : tables de routage".

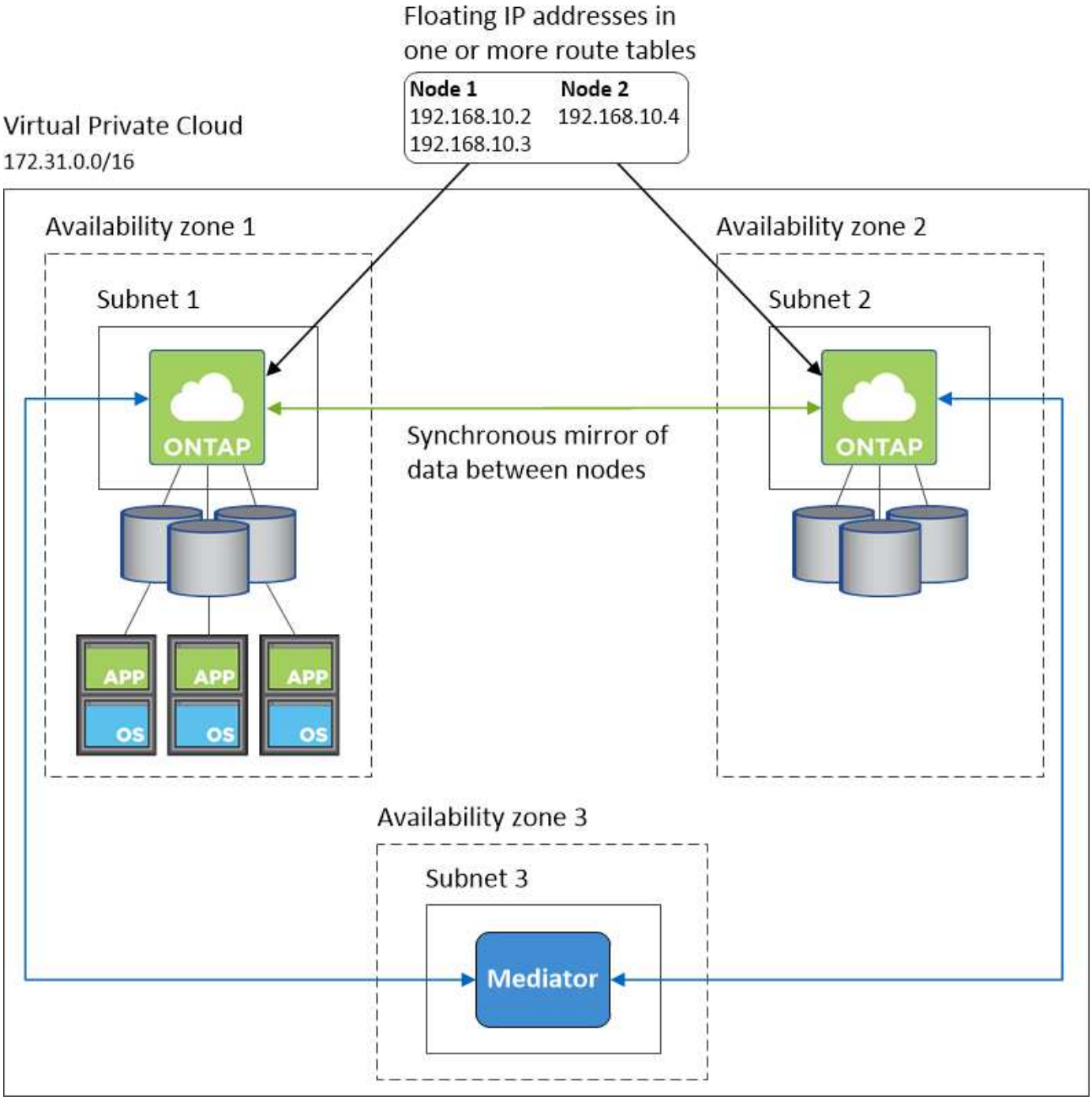
Connexion aux outils de gestion NetApp

Pour utiliser les outils de gestion NetApp avec des configurations haute disponibilité figurant dans plusieurs modèles AZS, vous disposez de deux options de connexion :

1. Déployez les outils de gestion NetApp sur un autre VPC et "Configuration d'une passerelle de transit AWS". La passerelle permet d'accéder à l'adresse IP flottante de l'interface de gestion du cluster à partir de l'extérieur du VPC.
2. Déployez les outils de gestion NetApp sur le même VPC avec une configuration de routage similaire à celle des clients NAS.

Exemple de configuration haute disponibilité

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



Configuration requise pour le connecteur

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

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

Connexion aux réseaux cibles

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

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

Accès Internet sortant

Le connecteur nécessite un accès Internet sortant pour gérer les ressources et les processus au sein de votre environnement de cloud public. Lors de la gestion des ressources dans AWS, un connecteur contacte les terminaux suivants :

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

Terminaux	Objectif
https://netapp-cloud-account.auth0.com	Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs.
https://w86yt021u5.execute-api.us-east-1.amazonaws.com/production/whitelist	Permet d'ajouter votre ID de compte AWS à la liste des utilisateurs autorisés pour Backup vers S3.
https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup	Communication avec NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Communication avec NetApp pour les licences système et l'inscription au support.
https://ipa-signer.cloudmanager.netapp.com	Génération des licences par Cloud Manager (par exemple, une licence FlexCache pour Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Nécessaire pour connecter des systèmes Cloud Volumes ONTAP avec un cluster Kubernetes. Les terminaux permettent l'installation de NetApp Trident.
Divers sites tiers, par exemple : • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Les emplacements tiers sont sujets à modification.	Lors des mises à niveau, Cloud Manager télécharge les derniers packages pour les dépendances tierces.

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

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

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

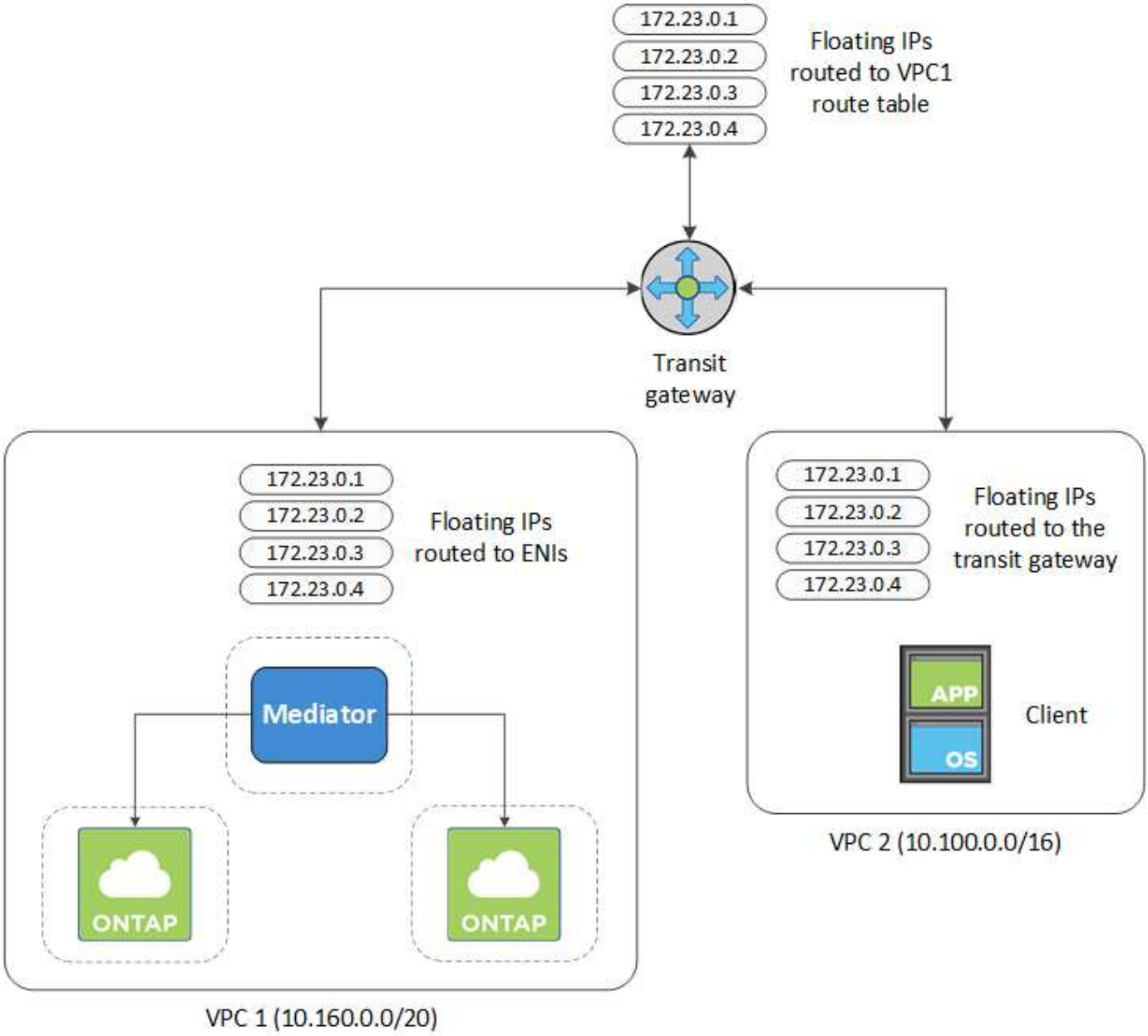
Configurez une passerelle de transit AWS pour autoriser l'accès à une paire HA "Adresses IP flottantes" Depuis l'extérieur du VPC, où réside la paire HA.

Lorsqu'une configuration Cloud Volumes ONTAP HA est répartie sur plusieurs zones de disponibilité AWS, des adresses IP flottantes sont nécessaires pour l'accès aux données NAS depuis le VPC. Ces adresses IP flottantes peuvent migrer entre les nœuds en cas de défaillance, mais elles ne sont pas accessibles de manière native en dehors du VPC. Des adresses IP privées séparées permettent un accès aux données depuis l'extérieur du VPC, mais elles ne permettent pas de procéder à un basculement automatique.

Des adresses IP flottantes sont également nécessaires pour l'interface de gestion du cluster et la LIF de gestion du SVM facultative.

Si vous configurez une passerelle de transit AWS, vous activez l'accès aux adresses IP flottantes depuis l'extérieur sur le VPC où réside la paire haute disponibilité. Les clients NAS et les outils de gestion NetApp en dehors du VPC peuvent accéder aux adresses IP flottantes.

Voici un exemple illustrant deux VPC connectés par une passerelle de transit. Un système haute disponibilité réside dans un VPC, tandis qu'un client réside dans l'autre. Vous pouvez ensuite monter un volume NAS sur le client à l'aide de l'adresse IP flottante.

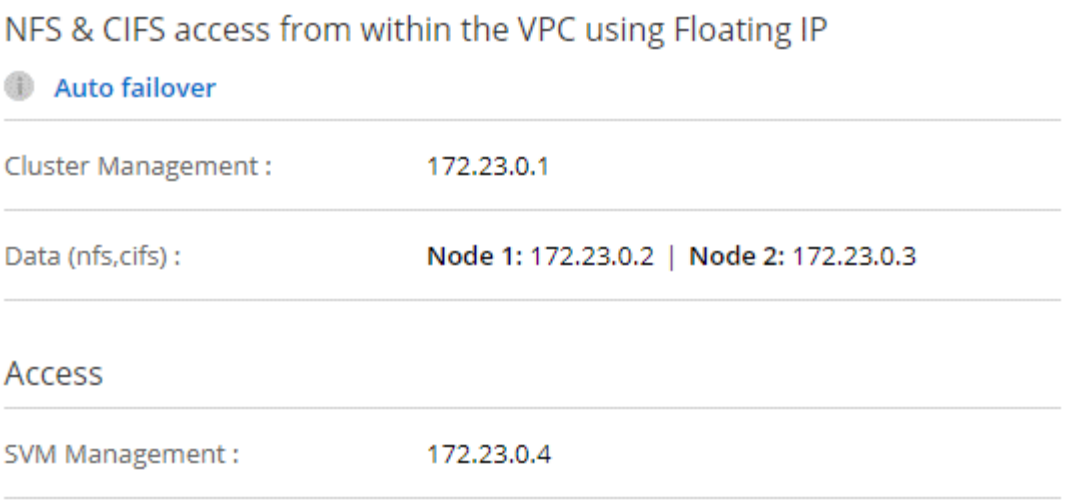


Les étapes suivantes montrent comment configurer une configuration similaire.

Étapes

1. "Créez une passerelle de transit et connectez les VPC à la passerelle".
2. Créer des routes dans la table de routage de la passerelle de transit en spécifiant les adresses IP flottantes de la paire HA.

   Les adresses IP flottantes se trouvent sur la page des informations sur l'environnement de travail dans Cloud Manager. Voici un exemple :



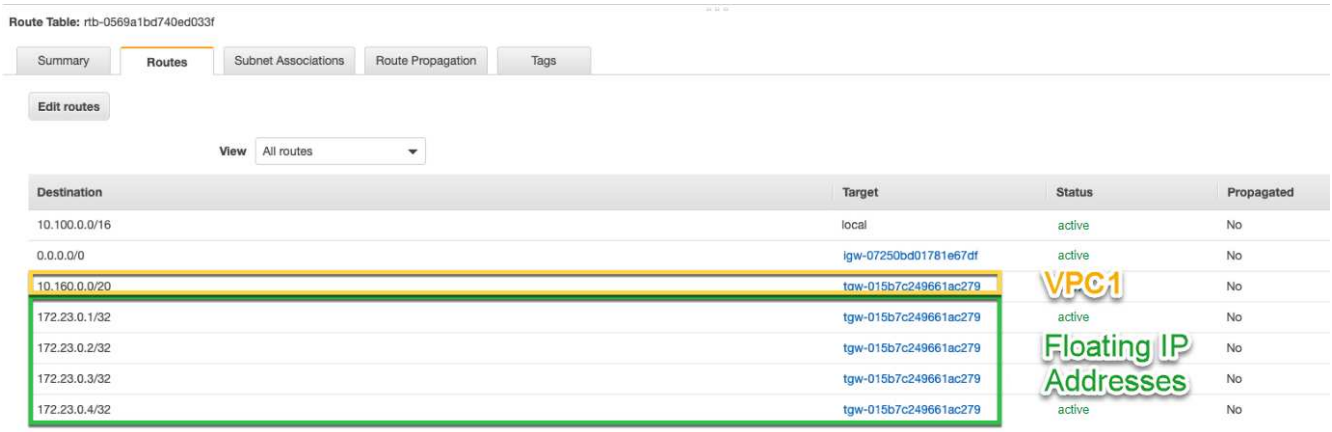
L'exemple d'image suivant montre la table de routage pour la passerelle de transit. Il comprend les routes vers les blocs CIDR des deux VPC et quatre adresses IP flottantes utilisées par Cloud Volumes ONTAP.

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

   a. Ajoutez des entrées de route aux adresses IP flottantes.

   b. Ajoutez une entrée de route au bloc CIDR du VPC où réside la paire HA.

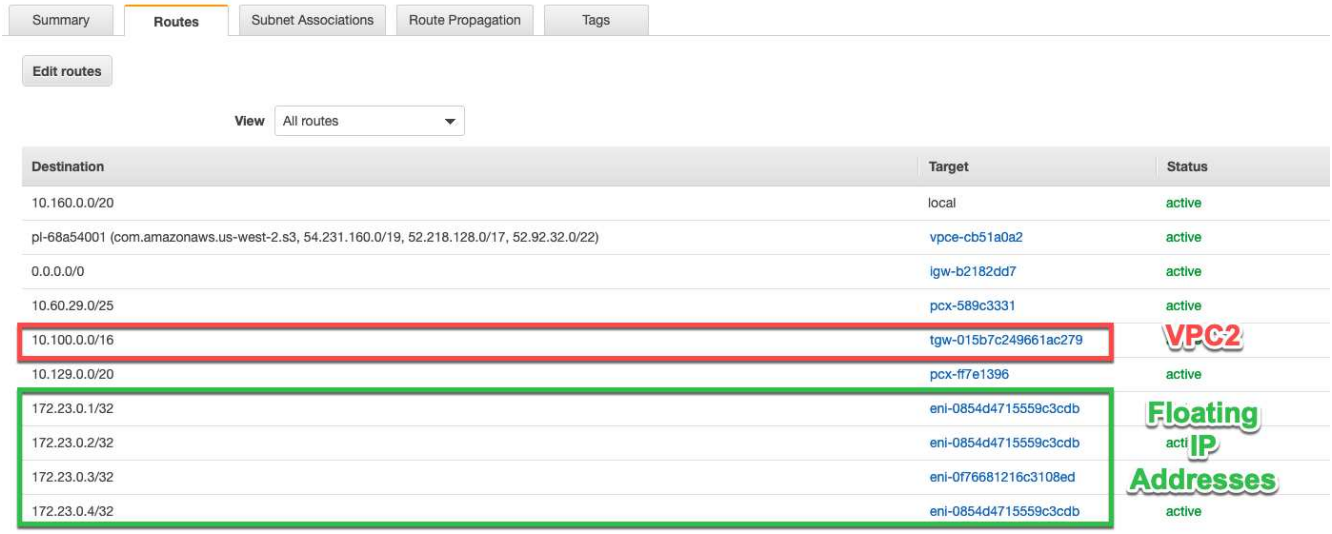
      L'exemple d'image suivant montre la table de route pour VPC 2, qui comprend les routes vers VPC 1 et les adresses IP flottantes.



4. Modifiez la table de routage du VPC de la paire HA en ajoutant une route vers le VPC qui doit accéder aux adresses IP flottantes.

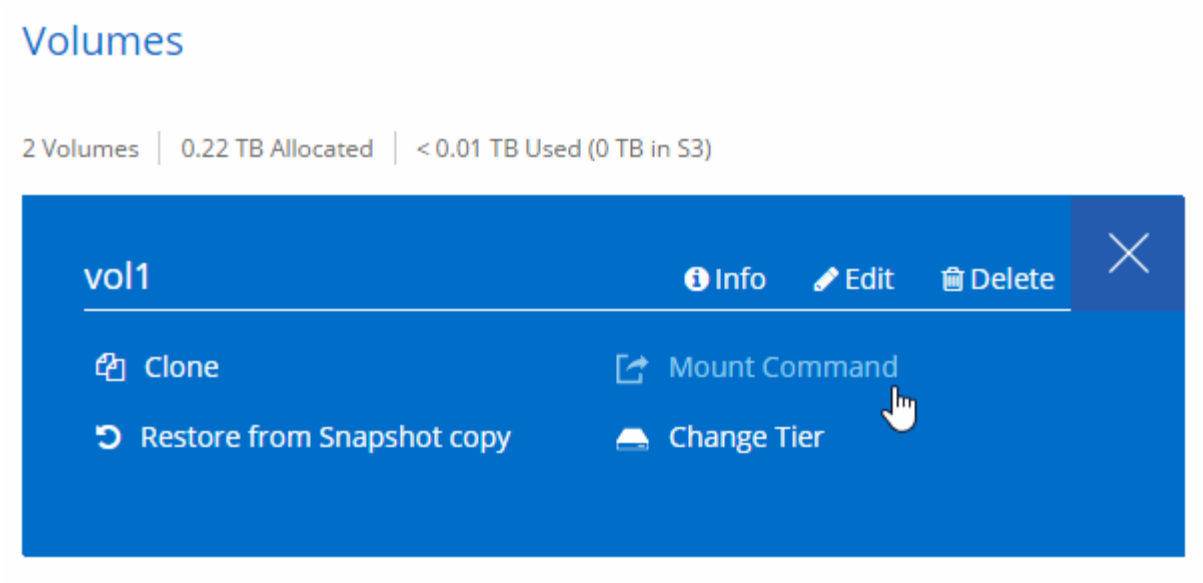
   Cette étape est importante car elle termine le routage entre les VPC.

   L'exemple d'image suivant montre la table de routage pour VPC 1. Elle inclut une route vers les adresses IP flottantes et vers VPC 2, c'est-à-dire où réside un client. Cloud Manager a automatiquement ajouté les adresses IP flottantes à la table de routage lors du déploiement de la paire haute disponibilité.



5. Montez les volumes sur des clients à l'aide de l'adresse IP flottante.

   Vous trouverez l'adresse IP correcte dans Cloud Manager en sélectionnant un volume et en cliquant sur **Mount Command**.



- Liens connexes*
- "Paires haute disponibilité dans AWS"
- "Configuration réseau requise pour Cloud Volumes ONTAP dans AWS"

Règles de groupe de sécurité pour AWS

Cloud Manager crée des groupes de sécurité AWS qui incluent les règles entrantes et sortantes que le connecteur et Cloud Volumes ONTAP doivent fonctionner correctement. Vous pouvez vous référer aux ports à des fins de test ou si vous préférez que votre utilise ses propres groupes de sécurité.

Règles pour Cloud Volumes ONTAP

Le groupe de sécurité pour Cloud Volumes ONTAP requiert des règles entrantes et sortantes.

Règles entrantes

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

Protocole	Port	Objectif
Tous les protocoles ICMP	Tout	Envoi d'une requête ping à l'instance
HTTP	80	Accès HTTP à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
HTTPS	443	Accès HTTPS à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
SSH	22	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
TCP	111	Appel de procédure à distance pour NFS
TCP	139	Session de service NetBIOS pour CIFS

Protocole	Port	Objectif
TCP	161-162	Protocole de gestion de réseau simple
TCP	445	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
TCP	658	Montage NFS
TCP	749	Kerberos
TCP	2049	Démon du serveur NFS
TCP	3260	Accès iSCSI via le LIF de données iSCSI
TCP	4045	Démon de verrouillage NFS
TCP	4046	Surveillance de l'état du réseau pour NFS
TCP	10000	Sauvegarde avec NDMP
TCP	11104	Gestion des sessions de communication intercluster pour SnapMirror
TCP	11105	Transfert de données SnapMirror à l'aide de LIF intercluster
UDP	111	Appel de procédure à distance pour NFS
UDP	161-162	Protocole de gestion de réseau simple
UDP	658	Montage NFS
UDP	2049	Démon du serveur NFS
UDP	4045	Démon de verrouillage NFS
UDP	4046	Surveillance de l'état du réseau pour NFS
UDP	4049	Protocole NFS rquotad

Règles de sortie

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

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour Cloud Volumes ONTAP inclut les règles de sortie suivantes.

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

Règles de sortie avancées

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

La source est l'interface (adresse IP) du système Cloud Volumes ONTAP.

Service	Protocole	Port	Source	Destination	Objectif
Active Directory	TCP	88	FRV de gestion des nœuds	Forêt Active Directory	Authentification Kerberos V.
	UDP	137	FRV de gestion des nœuds	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	FRV de gestion des nœuds	Forêt Active Directory	Service de datagrammes NetBIOS
	TCP	139	FRV de gestion des nœuds	Forêt Active Directory	Session de service NetBIOS
	TCP ET UDP	389	FRV de gestion des nœuds	Forêt Active Directory	LDAP
	TCP	445	FRV de gestion des nœuds	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	UDP	464	FRV de gestion des nœuds	Forêt Active Directory	Administration des clés Kerberos
	TCP	749	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)
	TCP	88	LIF de données (NFS, CIFS, iSCSI)	Forêt Active Directory	Authentification Kerberos V.
	UDP	137	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de datagrammes NetBIOS
	TCP	139	FRV de données (NFS, CIFS)	Forêt Active Directory	Session de service NetBIOS
	TCP ET UDP	389	FRV de données (NFS, CIFS)	Forêt Active Directory	LDAP
	TCP	445	FRV de données (NFS, CIFS)	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	UDP	464	FRV de données (NFS, CIFS)	Forêt Active Directory	Administration des clés Kerberos
	TCP	749	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)
Sauvegarde vers S3	TCP	5010	FRV InterCluster	Sauvegarder le terminal ou restaurer le terminal	Des opérations de sauvegarde et de restauration pour la fonctionnalité Backup vers S3

Service	Protocole	Port	Source	Destination	Objectif
Cluster	Tout le trafic	Tout le trafic	Tous les LIF sur un nœud	Tous les LIF de l'autre nœud	Communications InterCluster (Cloud Volumes ONTAP HA uniquement)
	TCP	3000	FRV de gestion des nœuds	Ha médiateur	Appels ZAPI (Cloud Volumes ONTAP HA uniquement)
	ICMP	1	FRV de gestion des nœuds	Ha médiateur	Rester en vie (Cloud Volumes ONTAP HA uniquement)
DHCP	UDP	68	FRV de gestion des nœuds	DHCP	Client DHCP pour la première configuration
DHCPS	UDP	67	FRV de gestion des nœuds	DHCP	Serveur DHCP
DNS	UDP	53	FRV de gestion des nœuds et FRV de données (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600-18699	FRV de gestion des nœuds	Serveurs de destination	Copie NDMP
SMTP	TCP	25	FRV de gestion des nœuds	Serveur de messagerie	Les alertes SMTP peuvent être utilisées pour AutoSupport
SNMP	TCP	161	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	UDP	161	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	TCP	162	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	UDP	162	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
SnapMirror	TCP	11104	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Gestion des sessions de communication intercluster pour SnapMirror
	TCP	11105	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Transfert de données SnapMirror
Syslog	UDP	514	FRV de gestion des nœuds	Serveur Syslog	Messages de transfert syslog

Règles pour le groupe de sécurité externe du médiateur de haute disponibilité

Le groupe de sécurité externe prédéfini pour le médiateur Cloud Volumes ONTAP HA inclut les règles entrantes et sortantes suivantes.

Règles entrantes

La source des règles entrantes est 0.0.0.0/0.

Protocole	Port	Objectif
SSH	22	Connexions SSH au médiateur haute disponibilité
TCP	3000	Accès à l'API RESTful depuis le connecteur

Règles de sortie

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

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini du médiateur HA inclut les règles de sortie suivantes.

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

Règles de sortie avancées

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

Protocole	Port	Destination	Objectif
HTTP	80	Adresse IP du connecteur	Télécharger les mises à niveau pour le médiateur
HTTPS	443	Services API AWS	Assistance pour le basculement du stockage
UDP	53	Services API AWS	Assistance pour le basculement du stockage

Plutôt que d'ouvrir les ports 443 et 53, vous pouvez créer un terminal VPC d'interface à partir du sous-réseau cible vers le service AWS EC2.

Règles pour le groupe de sécurité interne du médiateur de haute disponibilité

Le groupe de sécurité interne prédéfini pour le médiateur Cloud Volumes ONTAP HA inclut les règles suivantes. Cloud Manager crée toujours ce groupe de sécurité. Vous n'avez pas la possibilité d'utiliser vos propres ressources.

Règles entrantes

Le groupe de sécurité prédéfini inclut les règles entrantes suivantes.

Protocole	Port	Objectif
Tout le trafic	Tout	Communication entre le médiateur HA et les nœuds HA

Règles de sortie

Le groupe de sécurité prédéfini inclut les règles de sortie suivantes.

Protocole	Port	Objectif
Tout le trafic	Tout	Communication entre le médiateur HA et les nœuds HA

Règles pour le connecteur

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

Règles entrantes

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

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

Règles de sortie

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

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

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

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

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

Configuration du système AWS KMS

Si vous souhaitez utiliser le chiffrement Amazon avec Cloud Volumes ONTAP, vous devez configurer le service AWS Key Management Service (KMS).

Étapes

1. S'assurer qu'une clé principale client (CMK) active existe.

   La CMK peut être une CMK gérée par AWS ou une CMK gérée par le client. Il peut être hébergé sur le même compte AWS que Cloud Manager et Cloud Volumes ONTAP ou dans un autre compte AWS.

   "Documentation AWS : clés principales client (CMK)"

2. Modifiez la stratégie clé pour chaque CMK en ajoutant le rôle IAM qui fournit des autorisations à Cloud Manager en tant que *utilisateur clé*.

   L'ajout du rôle IAM en tant qu'utilisateur clé donne aux utilisateurs Cloud Manager les autorisations d'utiliser le CMK avec Cloud Volumes ONTAP.

   "Documentation AWS : modification des clés"

3. Si le CMK se trouve dans un autre compte AWS, procédez comme suit :

   a. Accédez à la console KMS à partir du compte où réside la CMK.

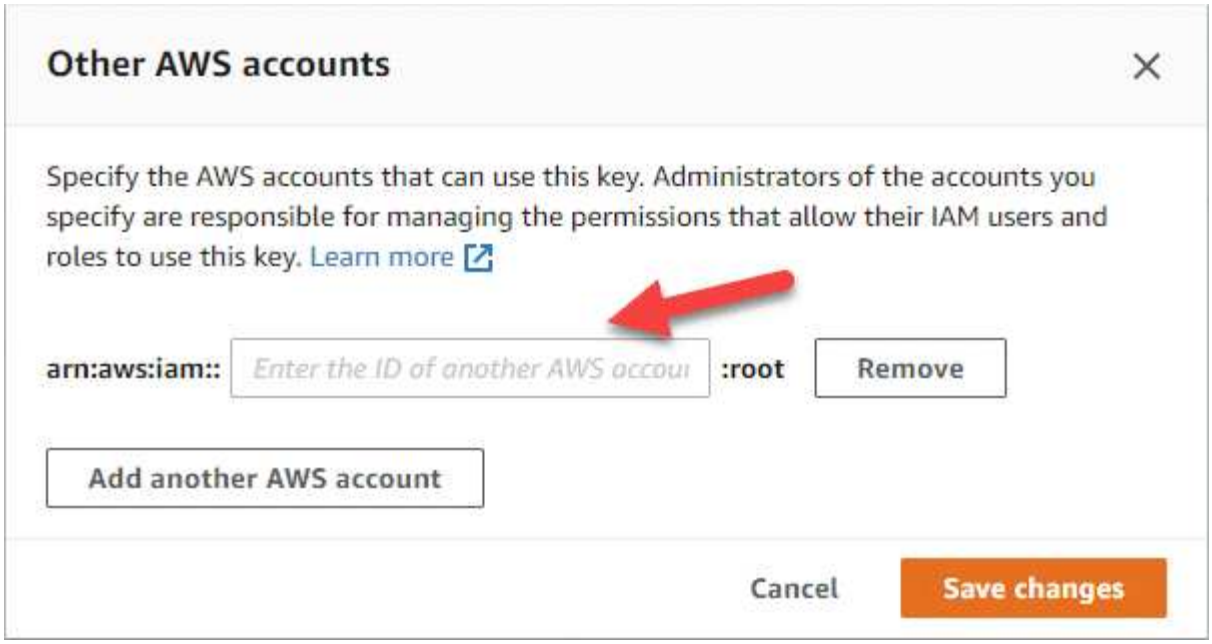
   b. Sélectionnez la touche.

   c. Dans le volet **Configuration générale**, copiez l'ARN de la clé.

      Vous devrez fournir l'ARN dans Cloud Manager lors de la création du système Cloud Volumes ONTAP.

   d. Dans le volet **autres comptes AWS**, ajoutez le compte AWS qui fournit les autorisations à Cloud Manager.

      Dans la plupart des cas, il s'agit du compte sur lequel réside Cloud Manager. Si Cloud Manager n'a pas été installé dans AWS, il s'agit du compte sur lequel vous avez fourni les clés d'accès AWS à Cloud Manager.



e. Passez maintenant au compte AWS qui fournit les autorisations nécessaires à Cloud Manager et ouvrez la console IAM.

f. Créez une stratégie IAM qui inclut les autorisations répertoriées ci-dessous.

g. Associez la règle au rôle IAM ou à l'utilisateur IAM qui donne des autorisations à Cloud Manager.

   La règle suivante fournit les autorisations requises par Cloud Manager pour utiliser le CMK à partir du compte AWS externe. Veillez à modifier la région et l'ID de compte dans les sections « ressource ».

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "AllowUseOfTheKey",
            "Effect": "Allow",
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:ReEncrypt*",
                "kms:GenerateDataKey*",
                "kms:DescribeKey"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalkeyid"
            ]
        },
        {
            "Sid": "AllowAttachmentOfPersistentResources",
            "Effect": "Allow",
            "Action": [
                "kms:CreateGrant",
                "kms:ListGrants",
                "kms:RevokeGrant"
            ],
            "Resource": [
                "arn:aws:kms:us-east-
1:externalaccountid:key/externalaccountid"
            ],
            "Condition": {
                "Bool": {
                    "kms:GrantIsForAWSResource": true
                }
            }
        }
    ]
}
```

+
Pour plus d'informations sur ce processus, reportez-vous à la section "Documentation AWS : autoriser les comptes AWS externes à accéder à un CMK".

Lancement d'Cloud Volumes ONTAP dans AWS

Vous pouvez lancer Cloud Volumes ONTAP dans une configuration à système unique ou en tant que paire haute disponibilité dans AWS.

Lancement d'un système Cloud Volumes ONTAP à un seul nœud dans AWS

Si vous souhaitez lancer Cloud Volumes ONTAP dans AWS, vous devez créer un nouvel environnement de travail dans Cloud Manager.

Avant de commencer

- Vous devez avoir un "Connecteur associé à votre espace de travail".

> Vous devez être un administrateur de compte pour créer un connecteur. Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l'avez pas encore fait.

- "Vous devez être prêt à laisser le connecteur fonctionner en permanence".
- Vous devriez avoir préparé en choisissant une configuration et en obtenant les informations de mise en réseau AWS auprès de votre administrateur. Pour plus de détails, voir "Planification de votre configuration Cloud Volumes ONTAP".
- Si vous souhaitez lancer un système BYOL, vous devez disposer du numéro de série à 20 chiffres (clé de licence).
- Si vous souhaitez utiliser CIFS, vous devez avoir configuré DNS et Active Directory. Pour plus de détails, voir "Configuration réseau requise pour Cloud Volumes ONTAP dans AWS".

Description de la tâche

Immédiatement après la création de l'environnement de travail, Cloud Manager lance une instance de test dans le VPC spécifié pour vérifier la connectivité. En cas de réussite, Cloud Manager met immédiatement fin à l'instance, puis lance le déploiement du système Cloud Volumes ONTAP. Si Cloud Manager ne parvient pas à vérifier la connectivité, la création de l'environnement de travail échoue. L'instance de test est soit t2.nano (pour la location VPC par défaut), soit m3.medium (pour la location VPC dédiée).

Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
2. **Choisissez un emplacement** : sélectionnez **Amazon Web Services** et **Cloud Volumes ONTAP Single Node**.
3. **Détails et informations d'identification** : modifiez éventuellement les informations d'identification et l'abonnement AWS, entrez un nom d'environnement de travail, ajoutez des balises si nécessaire, puis entrez un mot de passe.

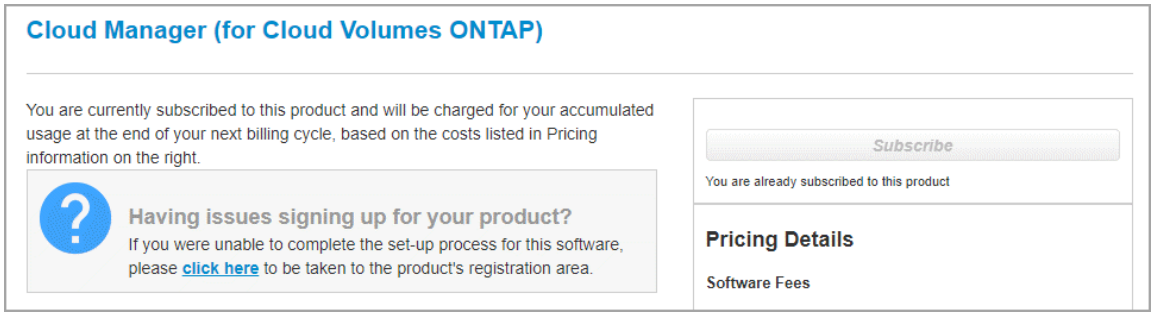
   Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Nom de l'environnement de travail	Cloud Manager utilise le nom de l'environnement de travail pour nommer à la fois le système Cloud Volumes ONTAP et l'instance Amazon EC2. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.
Ajouter des étiquettes	Les étiquettes AWS sont des métadonnées pour vos ressources AWS. Cloud Manager ajoute les balises à l'instance Cloud Volumes ONTAP et à chaque ressource AWS associée à l'instance. Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section "Documentation AWS : balisage des ressources Amazon EC2".
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte d'administration du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via OnCommand System Manager ou sa CLI.
Modifier les informations d'identification	Sélectionnez les identifiants AWS et l'abonnement Marketplace pour les utiliser avec ce système Cloud Volumes ONTAP. Cliquez sur **Ajouter un abonnement** pour associer les informations d'identification sélectionnées à un abonnement. Pour créer un système Cloud Volumes ONTAP à l'utilisation, vous devez sélectionner les identifiants AWS associés à un abonnement à Cloud Volumes ONTAP depuis AWS Marketplace. Vous serez facturé à partir de cet abonnement pour chaque système Cloud Volumes ONTAP 9.6 ou ultérieur de PAYGO que vous créez et chaque fonctionnalité d'extension activée."Découvrez comment ajouter des identifiants AWS à Cloud Manager".

Découvrez dans cette vidéo comment associer un abonnement payant basé sur l'utilisation Marketplace à vos identifiants AWS :

► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_aws.mp4 *(video)*

Si plusieurs utilisateurs IAM travaillent sur le même compte AWS, chaque utilisateur doit s'abonner. Après l'abonnement du premier utilisateur, AWS Marketplace informe les autres utilisateurs qu'ils sont déjà abonnés, comme illustré dans l'image ci-dessous. Lorsqu'un abonnement est en place pour AWS *account*, chaque utilisateur IAM doit s'associer à cet abonnement. Si le message ci-dessous s'affiche, cliquez sur le lien **cliquez ici** pour accéder à Cloud Central et terminer le processus.

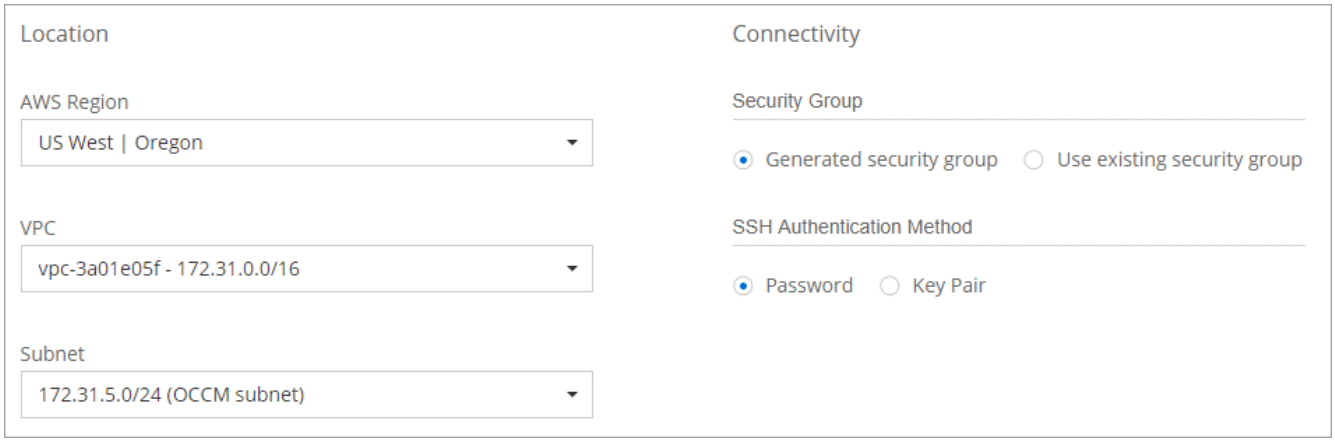


4. **Services** : conservez les services activés ou désactivez les services individuels que vous ne souhaitez pas utiliser avec Cloud Volumes ONTAP.

- "En savoir plus sur Cloud Compliance".
- "En savoir plus sur la sauvegarde dans le cloud".
- "En savoir plus sur la surveillance".

5. **Location & Connectivity** : saisissez les informations de réseau que vous avez enregistrées dans la fiche de travail AWS.

   L'image suivante montre la page remplie :



6. **Data Encryption** : choisissez pas de cryptage de données ou de cryptage géré par AWS.

   Pour le chiffrement géré par AWS, vous pouvez choisir une autre clé maître client (CMK) dans votre compte ou un autre compte AWS.

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

   "Découvrez comment configurer le KMS AWS pour Cloud Volumes ONTAP".

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

7. **Compte sur le site de licence et de support** : indiquez si vous souhaitez utiliser le paiement à l'utilisation ou BYOL, puis indiquez un compte sur le site de support NetApp.

   Pour comprendre le fonctionnement des licences, reportez-vous à la section "Licences".

   Un compte sur le site de support NetApp est facultatif afin de bénéficier d'un paiement à l'utilisation, mais requis pour les systèmes BYOL. "Découvrez comment ajouter des comptes au site de support NetApp".

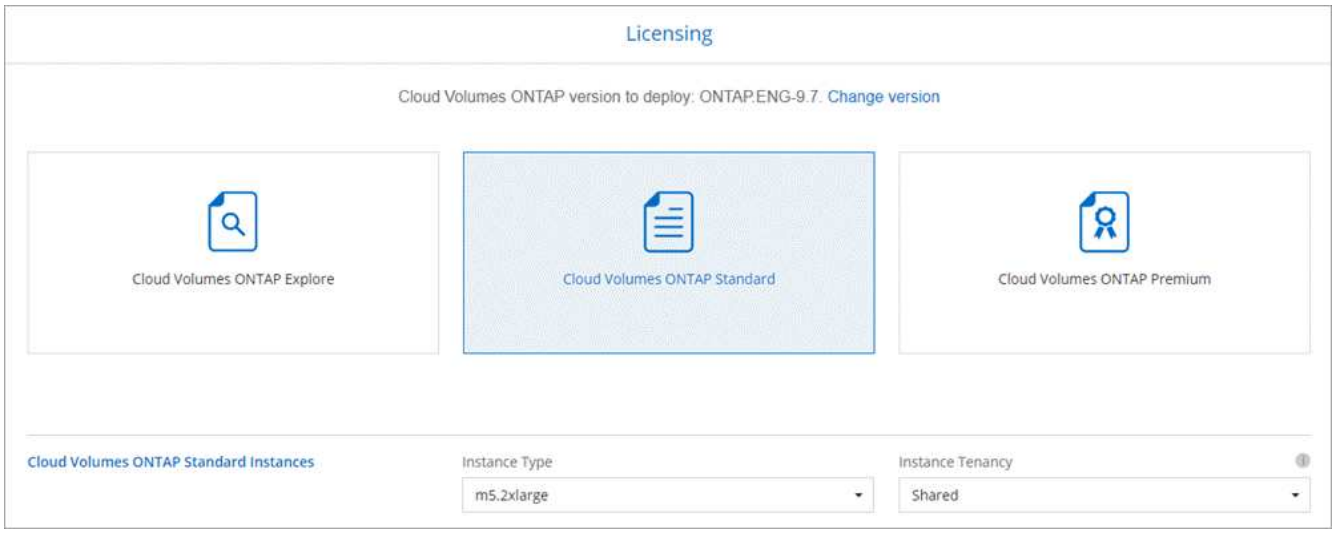
8. **Packages préconfigurés** : sélectionnez un des packages pour lancer rapidement Cloud Volumes ONTAP, ou cliquez sur **Créer ma propre configuration**.

   Si vous choisissez l'un des packages, vous n'avez qu'à spécifier un volume, puis à revoir et approuver la configuration.

9. **Rôle IAM** : vous devez conserver l'option par défaut pour permettre à Cloud Manager de créer le rôle pour vous.

   Si vous préférez utiliser votre propre police, elle doit satisfaire "Configuration requise pour les nœuds Cloud Volumes ONTAP".

10. **Licence** : modifiez la version de Cloud Volumes ONTAP selon vos besoins, sélectionnez une licence, un type d'instance et la location d'instance.



Si vos besoins changent après le lancement de l'instance, vous pouvez modifier la licence ou le type d'instance ultérieurement.

> Si une version plus récente de Release Candidate, General Availability ou patch est disponible pour la version sélectionnée, Cloud Manager met à jour le système à cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.6 RC1 et 9.6 GA est disponible. La mise à jour ne se produit pas d'une version à l'autre, par exemple de 9.6 à 9.7.

11. **Ressources de stockage sous-jacentes** : Choisissez les paramètres de l'agrégat initial : un type de disque, une taille pour chaque disque et si la hiérarchisation des données doit être activée.

    Notez ce qui suit :

    - Le type de disque correspond au volume initial. Vous pouvez choisir un autre type de disque pour les volumes suivants.
    - La taille du disque correspond à tous les disques de l'agrégat initial et à tous les agrégats supplémentaires créés par Cloud Manager lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente à l'aide de l'option d'allocation avancée.

      Pour obtenir de l'aide sur le choix du type et de la taille d'un disque, reportez-vous à la section "Dimensionnement de votre système dans AWS".

    - Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
    - Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants.

      "Découvrez le fonctionnement du Tiering des données".

12. **Vitesse d'écriture et WORM** : choisissez **Normal** ou **vitesse d'écriture élevée**, et activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

    La sélection d'une vitesse d'écriture est prise en charge avec les systèmes à un seul nœud uniquement.

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

IMPOSSIBLE D'activer WORM si le Tiering des données était activé.

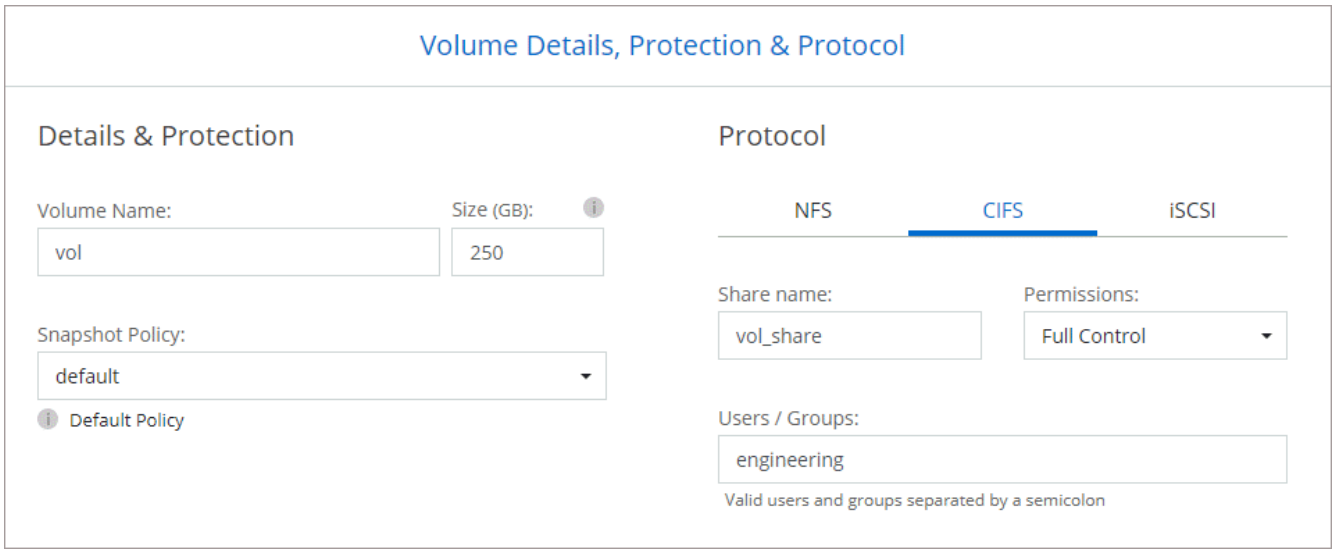
"En savoir plus sur le stockage WORM".

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

    Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, Cloud Manager entre une valeur qui donne accès à toutes les instances du sous-réseau.
Autorisations et utilisateurs/groupes (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur à l'aide du format domaine\nom d'utilisateur.
Stratégie Snapshot	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de buste hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".

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



14. **Configuration CIFS** : si vous choisissez le protocole CIFS, configurez un serveur CIFS.

Champ	Description
Adresse IP principale et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS.
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Nom de serveur CIFS unique dans le domaine AD.
Unité organisationnelle	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Si vous configurez AWS Managed Microsoft AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer **ou=ordinateurs,ou=corp** dans ce champ.
Domaine DNS	Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD.
Serveur NTP	Sélectionnez **utiliser le domaine Active Directory** pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la "Guide du développeur de l'API Cloud Manager" pour plus d'informations.

15. **Profil d'utilisation, type de disque et règle de hiérarchisation** : choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifiez la règle de hiérarchisation du volume, si nécessaire.

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

16. **Revue et approbation** : consultez et confirmez vos choix.

a. Consultez les détails de la configuration.

b. Cliquez sur **plus d'informations** pour en savoir plus sur le support et les ressources AWS que Cloud Manager achètera.

c. Cochez les cases **Je comprends…**.

d. Cliquez sur **Go**.

Résultat

Cloud Manager lance l'instance Cloud Volumes ONTAP. Vous pouvez suivre la progression dans la chronologie.

Si vous rencontrez des problèmes lors du lancement de l'instance Cloud Volumes ONTAP, consultez le message d'échec. Vous pouvez également sélectionner l'environnement de travail et cliquer sur Re-create environment.

Pour obtenir de l'aide supplémentaire, consultez la page "Prise en charge de NetApp Cloud Volumes ONTAP".

Une fois que vous avez terminé

- Si vous avez provisionné un partage CIFS, donnez aux utilisateurs ou aux groupes des autorisations sur les fichiers et les dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier.
- Si vous souhaitez appliquer des quotas aux volumes, utilisez System Manager ou l'interface de ligne de commande.

  Les quotas vous permettent de restreindre ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree.

Lancement d'une paire Cloud Volumes ONTAP HA dans AWS

Si vous souhaitez lancer une paire Cloud Volumes ONTAP HA dans AWS, vous devez créer un environnement de travail HA dans Cloud Manager.

Avant de commencer

- Vous devez avoir un "Connecteur associé à votre espace de travail".

  Vous devez être un administrateur de compte pour créer un connecteur. Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l'avez pas encore fait.

- "Vous devez être prêt à laisser le connecteur fonctionner en permanence".
- Vous devriez avoir préparé en choisissant une configuration et en obtenant les informations de mise en réseau AWS auprès de votre administrateur. Pour plus de détails, voir "Planification de votre configuration Cloud Volumes ONTAP".
- Si vous avez acheté des licences BYOL, vous devez disposer d'un numéro de série à 20 chiffres (clé de licence) pour chaque nœud.
- Si vous souhaitez utiliser CIFS, vous devez avoir configuré DNS et Active Directory. Pour plus de détails, voir "Configuration réseau requise pour Cloud Volumes ONTAP dans AWS".

Restriction

À l'heure actuelle, les paires haute disponibilité ne sont pas prises en charge avec les posts d'AWS.

Description de la tâche

Immédiatement après la création de l'environnement de travail, Cloud Manager lance une instance de test dans le VPC spécifié pour vérifier la connectivité. En cas de réussite, Cloud Manager met immédiatement fin à l'instance, puis lance le déploiement du système Cloud Volumes ONTAP. Si Cloud Manager ne parvient pas à vérifier la connectivité, la création de l'environnement de travail échoue. L'instance de test est soit t2.nano (pour la location VPC par défaut), soit m3.medium (pour la location VPC dédiée).

Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
2. **Choisissez un emplacement** : sélectionnez **Amazon Web Services** et **Cloud Volumes ONTAP Single Node**.
3. **Détails et informations d'identification** : modifiez éventuellement les informations d'identification et l'abonnement AWS, entrez un nom d'environnement de travail, ajoutez des balises si nécessaire, puis entrez un mot de passe.

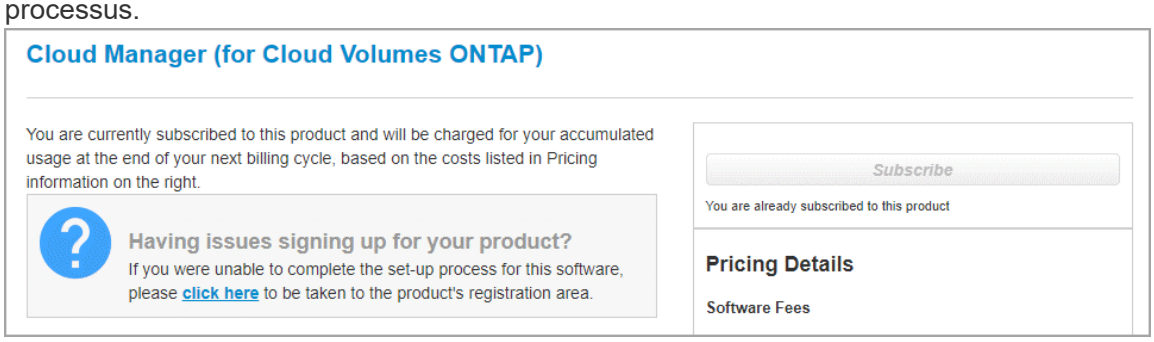
   Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Nom de l'environnement de travail	Cloud Manager utilise le nom de l'environnement de travail pour nommer à la fois le système Cloud Volumes ONTAP et l'instance Amazon EC2. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.
Ajouter des étiquettes	Les étiquettes AWS sont des métadonnées pour vos ressources AWS. Cloud Manager ajoute les balises à l'instance Cloud Volumes ONTAP et à chaque ressource AWS associée à l'instance. Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section "Documentation AWS : balisage des ressources Amazon EC2".
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte d'administration du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via OnCommand System Manager ou sa CLI.
Modifier les informations d'identification	Sélectionnez les identifiants AWS et l'abonnement Marketplace pour les utiliser avec ce système Cloud Volumes ONTAP. Cliquez sur **Ajouter un abonnement** pour associer les informations d'identification sélectionnées à un abonnement. Pour créer un système Cloud Volumes ONTAP à l'utilisation, vous devez sélectionner les identifiants AWS associés à un abonnement à Cloud Volumes ONTAP depuis AWS Marketplace. Vous serez facturé à partir de cet abonnement pour chaque système Cloud Volumes ONTAP 9.6 ou ultérieur de PAYGO que vous créez et chaque fonctionnalité d'extension activée."Découvrez comment ajouter des identifiants AWS à Cloud Manager".

Découvrez dans cette vidéo comment associer un abonnement payant basé sur l'utilisation Marketplace à vos identifiants AWS :

► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_aws.mp4 *(video)*

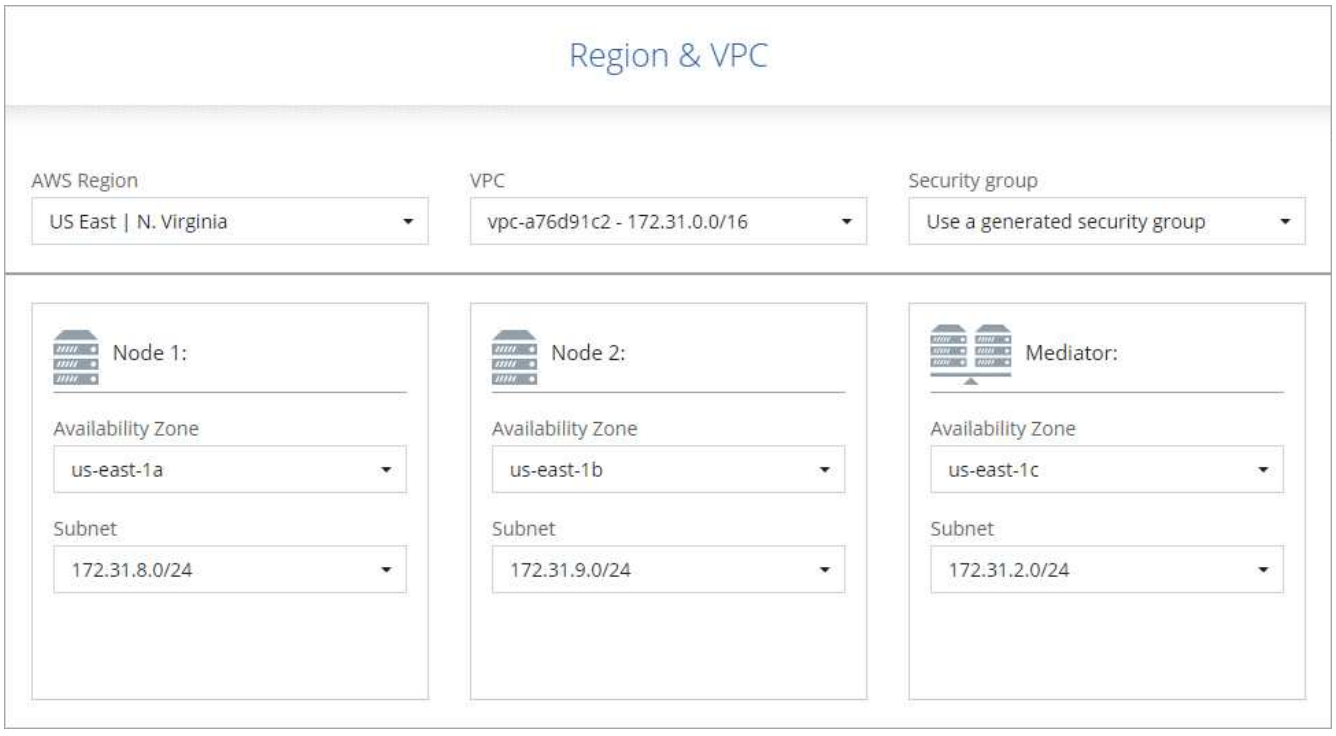
Si plusieurs utilisateurs IAM travaillent sur le même compte AWS, chaque utilisateur doit s'abonner. Après l'abonnement du premier utilisateur, AWS Marketplace informe les autres utilisateurs qu'ils sont déjà abonnés, comme illustré dans l'image ci-dessous. Lorsqu'un abonnement est en place pour AWS *account*, chaque utilisateur IAM doit s'associer à cet abonnement. Si le message ci-dessous s'affiche, cliquez sur le lien **cliquez ici** pour accéder à Cloud Central et terminer le
processus.



4. **Services** : conservez les services activés ou désactivez les services individuels que vous ne souhaitez pas utiliser avec ce système Cloud Volumes ONTAP.
   - "En savoir plus sur Cloud Compliance".
   - "En savoir plus sur la sauvegarde dans le cloud".
   - "En savoir plus sur la surveillance".
5. **Modèles de déploiement haute disponibilité** : choisir une configuration haute disponibilité.

   Pour obtenir un aperçu des modèles de déploiement, voir "Cloud Volumes ONTAP HA pour AWS".
6. **Région et VPC** : saisissez les informations de réseau que vous avez enregistrées dans la fiche AWS.

   L'image suivante montre la page remplie pour une configuration plusieurs AZ :



7. **Connectivité et authentification SSH** : choisissez des méthodes de connexion pour la paire HA et le médiateur.
8. **IP flottantes** : si vous choisissez plusieurs adresses AZS, spécifiez les adresses IP flottantes.

   Les adresses IP doivent se trouver en dehors du bloc CIDR pour tous les VPC de la région. Pour plus de détails, voir "Configuration réseau AWS requise pour Cloud Volumes ONTAP HA dans plusieurs AZS".

9. **Tables de routage** : si vous choisissez plusieurs AZS, sélectionnez les tables de routage qui doivent inclure les routes vers les adresses IP flottantes.

   Si vous disposez de plusieurs tables de routage, il est très important de sélectionner les tables de routage correctes. Dans le cas contraire, certains clients n'ont peut-être pas accès à la paire Cloud Volumes ONTAP HA. Pour plus d'informations sur les tables de routage, voir "Documentation AWS : tables de routage".

10. **Data Encryption** : choisissez pas de cryptage de données ou de cryptage géré par AWS.

    Pour le chiffrement géré par AWS, vous pouvez choisir une autre clé maître client (CMK) dans votre compte ou un autre compte AWS.

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

    "Découvrez comment configurer le KMS AWS pour Cloud Volumes ONTAP".

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

11. **Compte sur le site de licence et de support** : indiquez si vous souhaitez utiliser le paiement à l'utilisation ou BYOL, puis indiquez un compte sur le site de support NetApp.

    Pour comprendre le fonctionnement des licences, reportez-vous à la section "Licences".

    Un compte sur le site de support NetApp est facultatif afin de bénéficier d'un paiement à l'utilisation, mais requis pour les systèmes BYOL. "Découvrez comment ajouter des comptes au site de support NetApp".

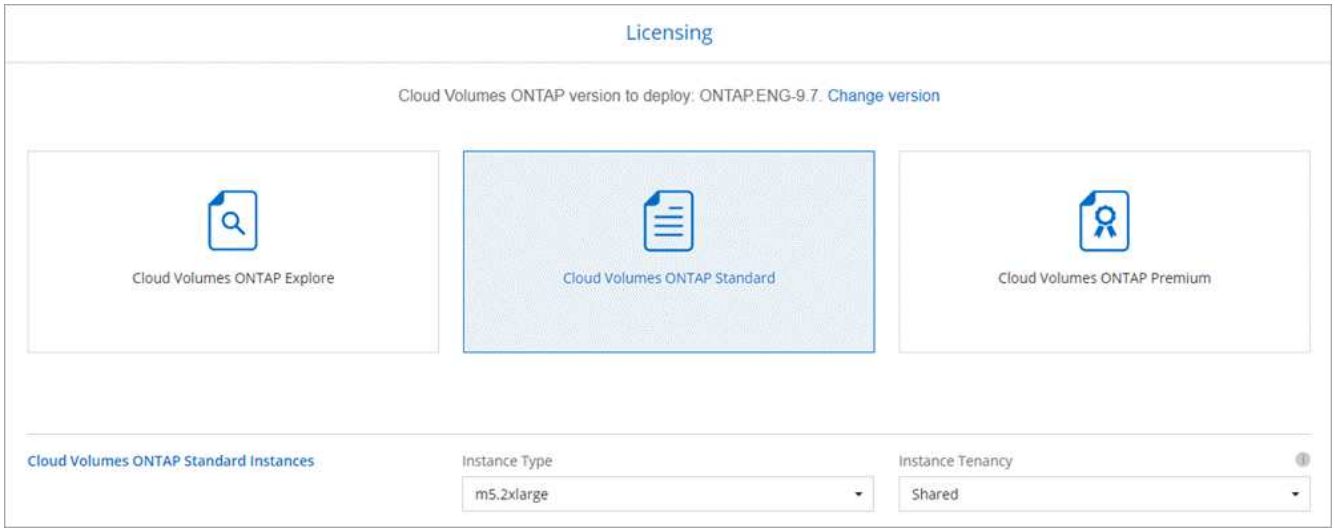
12. **Packages préconfigurés** : sélectionnez un des packages pour lancer rapidement un système Cloud Volumes ONTAP ou cliquez sur **Créer ma propre configuration**.

    Si vous choisissez l'un des packages, vous n'avez qu'à spécifier un volume, puis à revoir et approuver la configuration.

13. **Rôle IAM** : vous devez conserver l'option par défaut pour permettre à Cloud Manager de créer les rôles pour vous.

    Si vous préférez utiliser votre propre police, elle doit satisfaire "Configuration requise pour les nœuds Cloud Volumes ONTAP et le médiateur HA".

14. **Licence** : modifiez la version de Cloud Volumes ONTAP selon vos besoins, sélectionnez une licence, un type d'instance et la location d'instance.



Si vos besoins changent après le lancement des instances, vous pouvez modifier la licence ou le type d'instance ultérieurement.

> Si une version plus récente de Release Candidate, General Availability ou patch est disponible pour la version sélectionnée, Cloud Manager met à jour le système à cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.6 RC1 et 9.6 GA est disponible. La mise à jour ne se produit pas d'une version à l'autre, par exemple de 9.6 à 9.7.

15. **Ressources de stockage sous-jacentes** : Choisissez les paramètres de l'agrégat initial : un type de disque, une taille pour chaque disque et si la hiérarchisation des données doit être activée.

    Notez ce qui suit :

    - Le type de disque correspond au volume initial. Vous pouvez choisir un autre type de disque pour les volumes suivants.
    - La taille du disque correspond à tous les disques de l'agrégat initial et à tous les agrégats supplémentaires créés par Cloud Manager lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente à l'aide de l'option d'allocation avancée.

      Pour obtenir de l'aide sur le choix du type et de la taille d'un disque, reportez-vous à la section "Dimensionnement de votre système dans AWS".

    - Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
    - Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants.

      "Découvrez le fonctionnement du Tiering des données".

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

    IMPOSSIBLE D'activer WORM si le Tiering des données était activé.

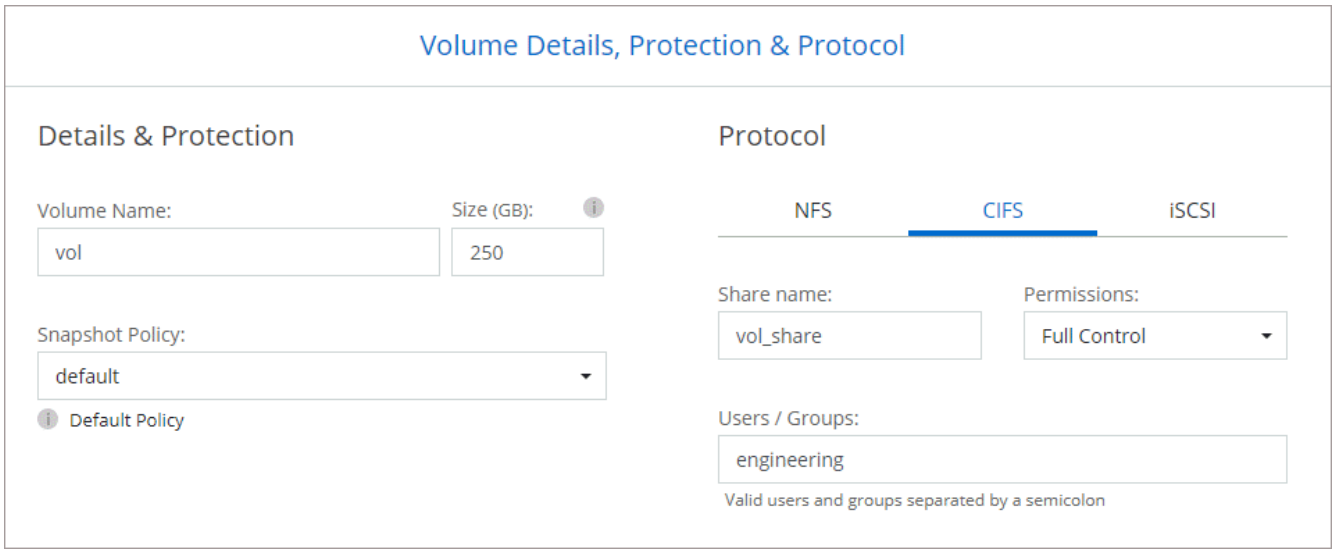
    "En savoir plus sur le stockage WORM".

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

Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, Cloud Manager entre une valeur qui donne accès à toutes les instances du sous-réseau.
Autorisations et utilisateurs/groupes (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur à l'aide du format domaine\nom d'utilisateur.
Stratégie Snapshot	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de buste hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".

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



18. **Configuration CIFS** : si vous avez sélectionné le protocole CIFS, configurez un serveur CIFS.

Champ	Description
Adresse IP principale et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS.
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Nom de serveur CIFS unique dans le domaine AD.
Unité organisationnelle	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Si vous configurez AWS Managed Microsoft AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer **ou=ordinateurs,ou=corp** dans ce champ.
Domaine DNS	Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD.
Serveur NTP	Sélectionnez **utiliser le domaine Active Directory** pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la "Guide du développeur de l'API Cloud Manager" pour plus d'informations.

19. **Profil d'utilisation, type de disque et règle de hiérarchisation** : choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifiez la règle de hiérarchisation du volume, si nécessaire.

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

20. **Revue et approbation** : consultez et confirmez vos choix.

a. Consultez les détails de la configuration.

b. Cliquez sur **plus d'informations** pour en savoir plus sur le support et les ressources AWS que Cloud Manager achètera.

c. Cochez les cases **Je comprends…**.

d. Cliquez sur **Go**.

Résultat

Cloud Manager lance la paire Cloud Volumes ONTAP HA. Vous pouvez suivre la progression dans la chronologie.

Si vous rencontrez des problèmes lors du lancement de la paire HA, consultez le message d'échec. Vous pouvez également sélectionner l'environnement de travail et cliquer sur Re-create environment.

Pour obtenir de l'aide supplémentaire, consultez la page "Prise en charge de NetApp Cloud Volumes ONTAP".

Une fois que vous avez terminé

- Si vous avez provisionné un partage CIFS, donnez aux utilisateurs ou aux groupes des autorisations sur les fichiers et les dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier.
- Si vous souhaitez appliquer des quotas aux volumes, utilisez System Manager ou l'interface de ligne de commande.

  Les quotas vous permettent de restreindre ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree.

Commencez à Azure

Mise en route de Cloud Volumes ONTAP pour Azure

Découvrez Cloud Volumes ONTAP pour Azure en quelques étapes.

Créer un connecteur

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

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

Planification de la configuration

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

Configurez votre réseau

1. Assurez-vous que votre VNet et vos sous-réseaux prennent en charge la connectivité entre le connecteur et Cloud Volumes ONTAP.
2. Activez l'accès Internet sortant à partir du réseau vnet cible de sorte que le connecteur et Cloud Volumes ONTAP puissent contacter plusieurs noeuds finaux.

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

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

Lancez Cloud Volumes ONTAP à l'aide de Cloud Manager

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

Liens connexes

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

Planification de votre configuration Cloud Volumes ONTAP dans Azure

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

Choix d'un type de licence

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

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

Compréhension des limites de stockage

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

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

Dimensionnement du système dans Azure

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

Type de machine virtuelle

Examinez les types de machines virtuelles prises en charge dans le "Notes de version de Cloud Volumes ONTAP" Examinez ensuite toutes les informations sur chaque type de machine virtuelle pris en charge. Notez que chaque type de VM prend en charge un nombre spécifique de disques de données.

- "Documentation Azure : tailles de machine virtuelle à usage général"
- "Documentation Azure : tailles de machines virtuelles optimisées pour la mémoire"

Type de disque Azure

Lorsque vous créez des volumes pour Cloud Volumes ONTAP, vous devez choisir le stockage cloud sous-jacent utilisé par Cloud Volumes ONTAP comme disque.

Les systèmes HAUTE DISPONIBILITÉ utilisent des objets blob de pages Premium. En parallèle, les systèmes à un seul nœud peuvent utiliser deux types de disques gérés Azure :

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

  Pour plus d'informations sur les cas d'utilisation de ces disques, reportez-vous à la section "Documentation Microsoft Azure : quels types de disques sont disponibles dans Azure ?".

Taille des disques Azure

Lorsque vous lancez des instances Cloud Volumes ONTAP, vous devez choisir la taille de disque par défaut des agrégats. Cloud Manager utilise cette taille de disque pour l'agrégat initial, et pour tous les agrégats supplémentaires que vous créez lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente de la taille par défaut "utilisation de l'option d'allocation avancée".

Tous les disques qui composent un agrégat doivent être de la même taille.

Lorsque vous choisissez une taille de disque, vous devez prendre en compte plusieurs facteurs. La taille des disques a une incidence sur le montant de vos frais de stockage, la taille des volumes que vous pouvez créer au sein d'un agrégat, la capacité totale disponible pour Cloud Volumes ONTAP et les performances de stockage.

Les performances du stockage Azure Premium sont liées à la taille des disques. Les disques de grande taille offrent des IOPS et un débit plus élevés. Par exemple, le choix de disques de 1 To peut fournir des performances supérieures à celles des disques de 500 Go, pour un coût plus élevé.

Avec un stockage standard, les performances sont les mêmes pour toutes les tailles de disques.

Choisissez la taille de disque en fonction de la capacité dont vous avez besoin.

Pour les IOPS et le débit par taille de disque, consultez Azure :

- "Microsoft Azure : tarification des disques gérés"
- "Microsoft Azure : tarification Blobs de page"

Choix d'une configuration qui prend en charge Flash cache

Une configuration Cloud Volumes ONTAP dans Azure inclut un stockage NVMe local, que Cloud Volumes ONTAP utilise comme *Flash cache* pour de meilleures performances. "En savoir plus sur Flash cache".

Fiche d'informations sur le réseau Azure

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

Informations sur Azure	Votre valeur
Région	
Réseau virtuel (vnet)	
Sous-réseau	
Groupe de sécurité réseau (s'il s'agit du vôtre)	

Sélection d'une vitesse d'écriture

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

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

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

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

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

Quand utiliser une vitesse d'écriture élevée

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

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

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

Choix d'un profil d'utilisation du volume

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

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

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

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

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

Exigences réseau pour déployer et gérer Cloud Volumes ONTAP dans Azure

Configurez votre réseau Azure de façon à ce que les systèmes Cloud Volumes ONTAP puissent fonctionner correctement. Cela inclut la mise en réseau pour le connecteur et le Cloud Volumes ONTAP.

Conditions requises pour Cloud Volumes ONTAP

Les exigences réseau suivantes doivent être satisfaites dans Azure.

Accès Internet sortant pour Cloud Volumes ONTAP
: Cloud Volumes ONTAP requiert un accès Internet sortant pour envoyer des messages à NetApp AutoSupport, qui surveille de façon proactive l'état de votre stockage.

  Les règles de routage et de pare-feu doivent autoriser le trafic HTTP/HTTPS vers les terminaux suivants pour que Cloud Volumes ONTAP puisse envoyer les messages AutoSupport :

  - https://support.netapp.com/aods/asupmessage
  - https://support.netapp.com/asupprod/post/1.0/postAsup

  "Découvrez comment configurer AutoSupport".

Groupes de sécurité

Vous n'avez pas besoin de créer de groupes de sécurité car Cloud Manager le fait pour vous. Si vous devez utiliser votre propre système, reportez-vous aux règles du groupe de sécurité répertoriées ci-dessous.

Nombre d'adresses IP

Cloud Manager attribue le nombre suivant d'adresses IP à Cloud Volumes ONTAP dans Azure :

- Un seul nœud : 5 adresses IP
- Paire HA : 16 adresses IP

Notez que Cloud Manager crée une LIF de gestion des SVM sur des paires haute disponibilité, mais pas sur des systèmes à un seul nœud dans Azure.

Une LIF est une adresse IP associée à un port physique. Une LIF de gestion SVM est nécessaire pour les outils de gestion tels que SnapCenter.

Connexion de Cloud Volumes ONTAP au stockage Azure Blob pour le hiérarchisation des données

Si vous souhaitez transférer les données inactives vers un stockage Azure Blob, vous n'avez pas besoin de configurer de connexion entre le Tier de performance et le Tier de capacité tant que Cloud Manager dispose des autorisations nécessaires. Cloud Manager active un terminal de service VNet pour vous si la règle Cloud Manager dispose des autorisations suivantes :

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

Ces autorisations sont incluses dans la dernière version "Politique de Cloud Manager".

Pour plus d'informations sur la configuration du Tiering des données, voir "Tiering des données inactives vers un stockage objet à faible coût".

Connexions aux systèmes ONTAP dans d'autres réseaux

Pour répliquer des données entre un système Cloud Volumes ONTAP sur les systèmes Azure et ONTAP sur d'autres réseaux, vous devez disposer d'une connexion VPN entre Azure VNet et l'autre réseau, par exemple un VPC AWS ou votre réseau d'entreprise.

Pour obtenir des instructions, reportez-vous à la section "Documentation Microsoft Azure : créez une connexion de site à site dans le portail Azure".

Configuration requise pour le connecteur

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

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

Connexions aux réseaux cibles

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

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

Accès Internet sortant

Le connecteur nécessite un accès Internet sortant pour gérer les ressources et les processus au sein de votre environnement de cloud public. Lors de la gestion des ressources dans Azure, un connecteur contacte les terminaux suivants :

Terminaux	Objectif
https://management.azure.com https://login.microsoftonline.com	Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans la plupart des régions d'Azure.
https://management.microsoftazure.de https://login.microsoftonline.de	Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans les régions d'Azure Allemagne.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans les régions d'Azure US Gov.
https://api.services.cloud.netapp.com:443	Demandes d'API à NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Permet d'accéder aux images logicielles, aux manifestes et aux modèles.
https://repo.cloud.support.netapp.com	Permet de télécharger les dépendances de Cloud Manager.
http://repo.mysql.com/	Utilisé pour télécharger MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Permet à Cloud Manager d'accéder aux manifestes, aux modèles et aux images de mise à niveau Cloud Volumes ONTAP et de les télécharger.
https://cloudmanagerinfraprod.azurecr.io	Accédez aux images logicielles des composants de conteneur pour une infrastructure exécutant Docker et fournie une solution pour les intégrations des services avec Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.
https://cloudmanager.cloud.netapp.com	Communication avec le service Cloud Manager, notamment les comptes Cloud Central.
https://netapp-cloud-account.auth0.com	Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs.
https://mysupport.netapp.com	Communication avec NetApp AutoSupport.

Terminaux	Objectif
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Communication avec NetApp pour les licences système et l'inscription au support.
https://ipa-signer.cloudmanager.netapp.com	Génération des licences par Cloud Manager (par exemple, une licence FlexCache pour Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Nécessaire pour connecter des systèmes Cloud Volumes ONTAP avec un cluster Kubernetes. Les terminaux permettent l'installation de NetApp Trident.
*.blob.core.windows.net	Requis pour les paires haute disponibilité lors de l'utilisation d'un proxy.
Divers sites tiers, par exemple : • https://repo1.maven.org/maven2 • https://oss.sonatype.org/content/repositories • https://repo.typesafe.org Les emplacements tiers sont sujets à modification.	Lors des mises à niveau, Cloud Manager télécharge les derniers packages pour les dépendances tierces.

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

Terminaux	Objectif
L'hôte du connecteur	Vous devez entrer l'adresse IP de l'hôte depuis un navigateur Web pour charger la console Cloud Manager. En fonction de votre connectivité avec votre fournisseur de cloud, vous pouvez utiliser l'IP privée ou une adresse IP publique attribuée à l'hôte : • Une adresse IP privée fonctionne si vous disposez d'un VPN et d'un accès direct à votre réseau virtuel • Un IP public fonctionne dans tous les scénarios de mise en réseau Dans tous les cas, vous devez sécuriser l'accès au réseau en vous assurant que les règles du groupe de sécurité autorisent l'accès à partir des adresses IP ou des sous-réseaux autorisés uniquement.

Terminaux	Objectif
https://auth0.com https://cdn.auth0.com https://netapp-cloud-account.auth0.com https://services.cloud.netapp.com	Votre navigateur Web se connecte à ces terminaux pour une authentification centralisée des utilisateurs via NetApp Cloud Central.
https://widget.intercom.io	Vous bénéficiez d'un chat en ligne pour discuter avec des experts du cloud NetApp.

Règles de groupe de sécurité pour Cloud Volumes ONTAP

Cloud Manager crée des groupes de sécurité Azure qui incluent les règles entrantes et sortantes nécessaires au fonctionnement de Cloud Volumes ONTAP. Vous pouvez vous référer aux ports à des fins de test ou si vous préférez que votre utilise ses propres groupes de sécurité.

Le groupe de sécurité pour Cloud Volumes ONTAP requiert des règles entrantes et sortantes.

Règles entrantes pour les systèmes à nœud unique

Les règles énumérées ci-dessous autorisent le trafic, sauf si la description indique qu'il bloque un trafic entrant spécifique.

Priorité et nom	Port et protocole	Source et destination	Description
1000 inbound_ssh	22 TCP	De tous les types à tous	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
1001 inbound_http	80 TCP	De tous les types à tous	Accès HTTP à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
1002 inbound_111_tcp	111 TCP	De tous les types à tous	Appel de procédure à distance pour NFS
1003 inbound_111_udp	111 UDP	De tous les types à tous	Appel de procédure à distance pour NFS
1004 entrant_139	139 TCP	De tous les types à tous	Session de service NetBIOS pour CIFS
1005 inbound_161-162 _tcp	161-162 TCP	De tous les types à tous	Protocole de gestion de réseau simple
1006 inbound_161-162 _udp	161-162 UDP	De tous les types à tous	Protocole de gestion de réseau simple
1007 entrant_443	443 TCP	De tous les types à tous	Accès HTTPS à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
1008 entrant_445	445 TCP	De tous les types à tous	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS

Priorité et nom	Port et protocole	Source et destination	Description
1009 inbound_635_tcp	635 TCP	De tous les types à tous	Montage NFS
1010 inbound_635_udp	635 UDP	De tous les types à tous	Montage NFS
1011 entrant_749	749 TCP	De tous les types à tous	Kerberos
1012 inbound_2049_tcp	2049 TCP	De tous les types à tous	Démon du serveur NFS
1013 inbound_2049_udp	2049 UDP	De tous les types à tous	Démon du serveur NFS
1014 entrant_3260	3260 TCP	De tous les types à tous	Accès iSCSI via le LIF de données iSCSI
1015 inbound_4045-4046_tcp	4045-4046 TCP	De tous les types à tous	Démon de verrouillage NFS et contrôle de l'état du réseau
1016 inbound_4045-4046_udp	4045-4046 UDP	De tous les types à tous	Démon de verrouillage NFS et contrôle de l'état du réseau
1017 entrant_10000	10000 TCP	De tous les types à tous	Sauvegarde avec NDMP
1018 entrant_11104-11105	11104-11105 TCP	De tous les types à tous	Transfert de données SnapMirror
3000 inbound_deny _all_tcp	Tout port TCP	De tous les types à tous	Bloquer tout autre trafic TCP entrant
3001 inbound_deny _all_udp	Tout port UDP	De tous les types à tous	Bloquer tout autre trafic entrant UDP
65000 AllowVnetInBound	N'importe quel protocole	VirtualNetwork à VirtualNetwork	Trafic entrant depuis le réseau VNet
65001 AllowAzureLoad BalancerInBound	N'importe quel protocole	AzureLoadBalancer à tout	Le trafic de données à partir d'Azure Standard Load Balancer
65500 DenyAllInBound	N'importe quel protocole	De tous les types à tous	Bloquer tout autre trafic entrant

Règles entrantes pour les systèmes HA

Les règles énumérées ci-dessous autorisent le trafic, sauf si la description indique qu'il bloque un trafic entrant spécifique.

Les systèmes HAUTE DISPONIBILITÉ disposent de règles entrantes moins strictes que les systèmes à un seul nœud, car le trafic des données entrantes transite par Azure Standard Load Balancer. Pour cette raison, le trafic provenant du Load Balancer doit être ouvert, comme indiqué dans la règle AllowAzureLoadBalancerInBound.

Priorité et nom	Port et protocole	Source et destination	Description
100 entrant_443	443 tout protocole	De tous les types à tous	Accès HTTPS à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
101 inbound_111_tcp	111 tout protocole	De tous les types à tous	Appel de procédure à distance pour NFS
102 inbound_2049_tcp	2049 tout protocole	De tous les types à tous	Démon du serveur NFS
111 inbound_ssh	22 tout protocole	De tous les types à tous	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
121 entrant_53	53 tout protocole	De tous les types à tous	DNS et CIFS
65000 AllowVnetInBound	N'importe quel protocole	VirtualNetwork à VirtualNetwork	Trafic entrant depuis le réseau VNet
65001 AllowAzureLoad BalancerInBound	N'importe quel protocole	AzureLoadBalancer à tout	Le trafic de données à partir d'Azure Standard Load Balancer
65500 DenyAllInBound	N'importe quel protocole	De tous les types à tous	Bloquer tout autre trafic entrant

Règles de sortie

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

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour Cloud Volumes ONTAP inclut les règles de sortie suivantes.

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

Règles de sortie avancées

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

La source est l'interface (adresse IP) du système Cloud Volumes ONTAP.

Service	Port	Protocole	Source	Destination	Objectif
Active Directory	88	TCP	FRV de gestion des nœuds	Forêt Active Directory	Authentification Kerberos V.
	137	UDP	FRV de gestion des nœuds	Forêt Active Directory	Service de noms NetBIOS
	138	UDP	FRV de gestion des nœuds	Forêt Active Directory	Service de datagrammes NetBIOS
	139	TCP	FRV de gestion des nœuds	Forêt Active Directory	Session de service NetBIOS
	389	TCP ET UDP	FRV de gestion des nœuds	Forêt Active Directory	LDAP
	445	TCP	FRV de gestion des nœuds	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	464	TCP	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	464	UDP	FRV de gestion des nœuds	Forêt Active Directory	Administration des clés Kerberos
	749	TCP	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)
	88	TCP	LIF de données (NFS, CIFS, iSCSI)	Forêt Active Directory	Authentification Kerberos V.
	137	UDP	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de noms NetBIOS
	138	UDP	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de datagrammes NetBIOS
	139	TCP	FRV de données (NFS, CIFS)	Forêt Active Directory	Session de service NetBIOS
	389	TCP ET UDP	FRV de données (NFS, CIFS)	Forêt Active Directory	LDAP
	445	TCP	FRV de données (NFS, CIFS)	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	464	TCP	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	464	UDP	FRV de données (NFS, CIFS)	Forêt Active Directory	Administration des clés Kerberos
	749	TCP	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)
DHCP	68	UDP	FRV de gestion des nœuds	DHCP	Client DHCP pour la première configuration

Service	Port	Protocole	Source	Destination	Objectif
DHCPS	67	UDP	FRV de gestion des nœuds	DHCP	Serveur DHCP
DNS	53	UDP	FRV de gestion des nœuds et FRV de données (NFS, CIFS)	DNS	DNS
NDMP	18600-18699	TCP	FRV de gestion des nœuds	Serveurs de destination	Copie NDMP
SMTP	25	TCP	FRV de gestion des nœuds	Serveur de messagerie	Les alertes SMTP peuvent être utilisées pour AutoSupport
SNMP	161	TCP	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	161	UDP	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	162	TCP	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	162	UDP	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
SnapMirror	11104	TCP	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Gestion des sessions de communication intercluster pour SnapMirror
	11105	TCP	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Transfert de données SnapMirror
Syslog	514	UDP	FRV de gestion des nœuds	Serveur Syslog	Messages de transfert syslog

Règles de groupe de sécurité pour le connecteur

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

Règles entrantes

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

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

Port	Protocole	Objectif
443	HTTPS	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale

Règles de sortie

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

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

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

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

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

Lancement d'Cloud Volumes ONTAP dans Azure

Vous pouvez lancer un système à un seul nœud ou une paire HA dans Azure en créant un environnement de travail Cloud Volumes ONTAP dans Cloud Manager.

Avant de commencer

- Vous devez avoir un "Connecteur associé à votre espace de travail".

Vous devez être un administrateur de compte pour créer un connecteur. Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l'avez pas encore fait.

- "Vous devez être prêt à laisser le connecteur fonctionner en permanence".
- Vous devez avoir choisi une configuration et obtenir des informations de mise en réseau Azure auprès de votre administrateur. Pour plus de détails, voir "Planification de votre configuration Cloud Volumes ONTAP".
- Pour déployer un système BYOL, vous devez disposer du numéro de série à 20 chiffres (clé de licence) pour chaque nœud.

Description de la tâche

Lorsque Cloud Manager crée un système Cloud Volumes ONTAP dans Azure, il crée plusieurs objets Azure, comme un groupe de ressources, des interfaces réseau et des comptes de stockage. Vous pouvez consulter un résumé des ressources à la fin de l'assistant.

Risque de perte de données

Le déploiement d'Cloud Volumes ONTAP dans un groupe de ressources existant et partagées n'est pas recommandé en raison du risque de perte de données. Lorsque la restauration est actuellement désactivée par défaut lors de l'utilisation de l'API pour le déploiement dans un groupe de ressources existant, la suppression de Cloud Volumes ONTAP risque de supprimer d'autres ressources de ce groupe partagé.

Il est recommandé d'utiliser un nouveau groupe de ressources dédié pour Cloud Volumes ONTAP. Il s'agit de l'option par défaut et uniquement recommandée pour le déploiement de Cloud Volumes ONTAP dans Azure à partir de Cloud Manager.

Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
2. **Choisissez un emplacement** : sélectionnez **Microsoft Azure** et **Cloud Volumes ONTAP nœud unique** ou **Cloud Volumes ONTAP haute disponibilité**.
3. **Détails et informations d'identification** : modifiez éventuellement les informations d'identification et l'abonnement Azure, spécifiez un nom de cluster et de groupe de ressources, ajoutez des balises si nécessaire, puis spécifiez des informations d'identification.

   Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Nom de l'environnement de travail	Cloud Manager utilise le nom de l'environnement de travail pour nommer à la fois le système Cloud Volumes ONTAP et la machine virtuelle Azure. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.

Champ	Description
Nom du groupe de ressources	Conservez le nom par défaut du nouveau groupe de ressources ou décochez **utiliser par défaut** et entrez votre propre nom pour le nouveau groupe de ressources. Il est recommandé d'utiliser un nouveau groupe de ressources dédié pour Cloud Volumes ONTAP. S'il est possible de déployer Cloud Volumes ONTAP dans un groupe de ressources existant et partagé à l'aide de l'API, il n'est pas recommandé en raison du risque de perte de données. Voir l'avertissement ci-dessus pour plus de détails.
Étiquettes	Les étiquettes sont des métadonnées pour vos ressources Azure. Lorsque vous saisissez des balises dans ce champ, Cloud Manager les ajoute au groupe de ressources associé au système Cloud Volumes ONTAP. Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section "Documentation Microsoft Azure : utilisation des balises pour organiser vos ressources Azure".
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte d'administration du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via OnCommand System Manager ou sa CLI.
Modifier les informations d'identification	Vous pouvez choisir plusieurs identifiants Azure et un autre abonnement Azure à utiliser avec ce système Cloud Volumes ONTAP. Vous devez associer un abonnement Azure Marketplace à l'abonnement Azure sélectionné pour déployer un système Cloud Volumes ONTAP basé sur l'utilisation. "Apprenez à ajouter des informations d'identification".

La vidéo suivante explique comment associer un abonnement Marketplace à un abonnement Azure :

► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_azure.mp4 *(video)*

4. **Services** : conservez les services activés ou désactivez les services individuels que vous ne souhaitez pas utiliser avec Cloud Volumes ONTAP.
   - "En savoir plus sur Cloud Compliance".
   - "En savoir plus sur la sauvegarde dans le cloud".
5. **Localisation et connectivité** : sélectionnez un emplacement et un groupe de sécurité et cochez la case pour confirmer la connectivité réseau entre Cloud Manager et l'emplacement cible.
6. **Compte sur le site de licence et de support** : indiquez si vous souhaitez utiliser le paiement à l'utilisation ou BYOL, puis indiquez un compte sur le site de support NetApp.

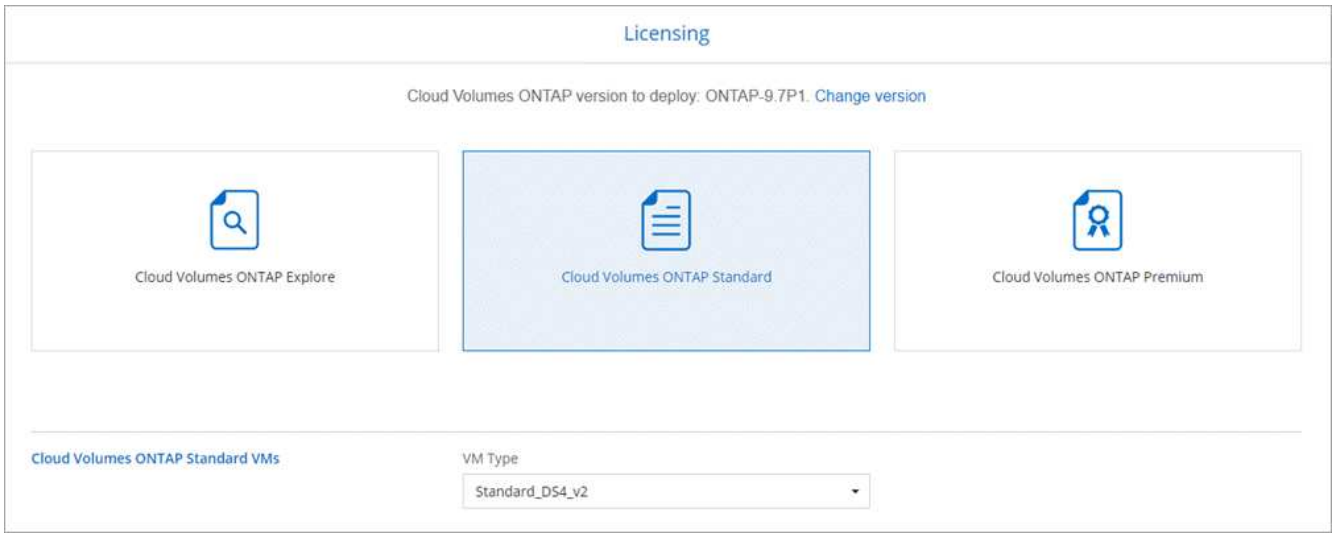
   Pour comprendre le fonctionnement des licences, reportez-vous à la section "Licences".

   Un compte sur le site de support NetApp est facultatif afin de bénéficier d'un paiement à l'utilisation, mais requis pour les systèmes BYOL. "Découvrez comment ajouter des comptes au site de support NetApp".

7. **Packages préconfigurés** : Shelect un des packages pour déployer rapidement un système Cloud Volumes ONTAP, ou cliquez sur **Créer ma propre configuration**.

   Si vous choisissez l'un des packages, vous n'avez qu'à spécifier un volume, puis à revoir et approuver la configuration.

8. **Licence** : modifiez la version de Cloud Volumes ONTAP selon vos besoins, sélectionnez une licence et sélectionnez un type de machine virtuelle.



Si vos besoins changent après le lancement du système, vous pouvez modifier la licence ou le type de machine virtuelle ultérieurement.

> Si une version plus récente de Release Candidate, General Availability ou patch est disponible pour la version sélectionnée, Cloud Manager met à jour le système à cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.6 RC1 et 9.6 GA est disponible. La mise à jour ne se produit pas d'une version à l'autre, par exemple de 9.6 à 9.7.

9. **Abonnez-vous à partir d'Azure Marketplace**: Suivez les étapes si Cloud Manager n'a pas pu activer les déploiements programmatiques de Cloud Volumes ONTAP.
10. **Ressources de stockage sous-jacentes** : Choisissez les paramètres de l'agrégat initial : un type de disque, une taille pour chaque disque et si le Tiering des données vers stockage Blob doit être activé.

    Notez ce qui suit :

    - Le type de disque correspond au volume initial. Vous pouvez choisir un autre type de disque pour les volumes suivants.
    - La taille du disque correspond à tous les disques de l'agrégat initial et à tous les agrégats supplémentaires créés par Cloud Manager lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente à l'aide de l'option d'allocation avancée.

      Pour obtenir de l'aide sur le choix du type et de la taille d'un disque, reportez-vous à la section "Dimensionnement du système dans Azure".

    - Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
    - Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants.

      "En savoir plus sur le Tiering des données".

11. **Vitesse d'écriture et WORM** (systèmes à un seul nœud uniquement) : choisissez **Normal** ou **vitesse d'écriture élevée** et activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

La sélection d'une vitesse d'écriture est prise en charge avec les systèmes à un seul nœud uniquement.

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

IMPOSSIBLE D'activer WORM si le Tiering des données était activé.

"En savoir plus sur le stockage WORM".

12. **Secure communication to Storage & WORM** (HA uniquement) : permet d'activer ou non une connexion HTTPS aux comptes de stockage Azure et d'activer le stockage WORM (Write Once, Read Many), si nécessaire.

    La connexion HTTPS est établie depuis une paire HA Cloud Volumes ONTAP 9.7 vers les comptes de stockage Azure. Notez que l'activation de cette option peut avoir un impact sur les performances d'écriture. Vous ne pouvez pas modifier le paramètre après avoir créé l'environnement de travail.

    "En savoir plus sur le stockage WORM".

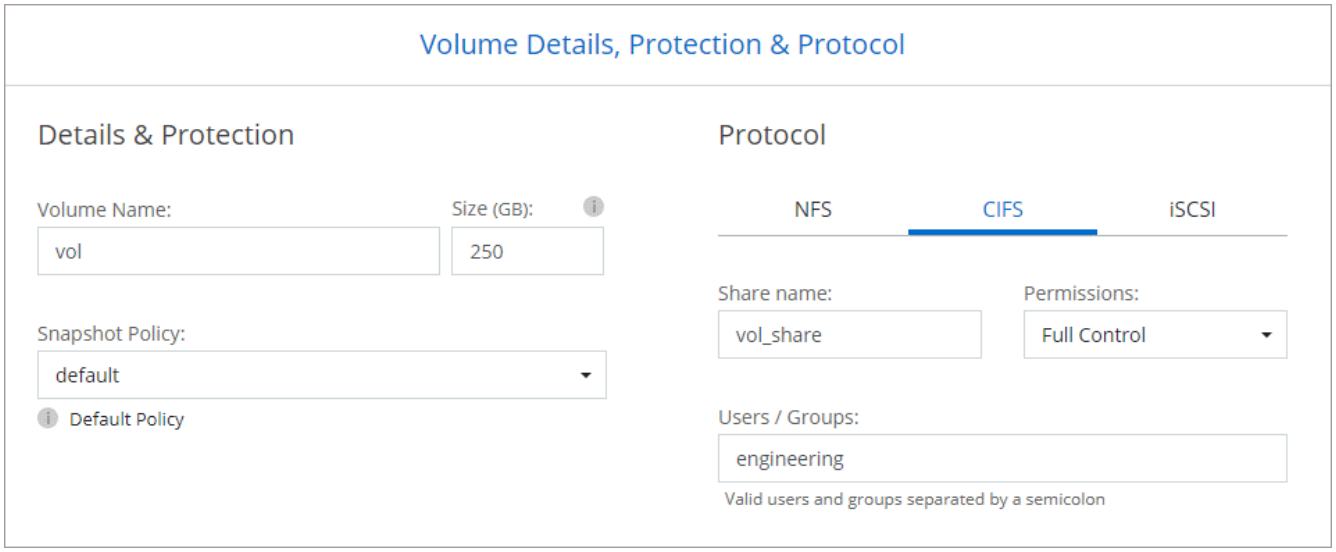
13. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

    Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, Cloud Manager entre une valeur qui donne accès à toutes les instances du sous-réseau.
Autorisations et utilisateurs/groupes (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur à l'aide du format domaine\nom d'utilisateur.
Stratégie Snapshot	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.

Champ	Description
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de buste hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".

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



14. **Configuration CIFS** : si vous choisissez le protocole CIFS, configurez un serveur CIFS.

Champ	Description
Adresse IP principale et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS.
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Nom de serveur CIFS unique dans le domaine AD.

Champ	Description
Unité organisationnelle	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Pour configurer les services de domaine Azure AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer **ou=ordinateurs ADDC** ou **ou=utilisateurs ADDC** dans ce champ.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentation Azure : créez une unité organisationnelle dans un domaine géré Azure AD Domain Services"^]
Domaine DNS	Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD.
Serveur NTP	Sélectionnez **utiliser le domaine Active Directory** pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la "Guide du développeur de l'API Cloud Manager" pour plus d'informations.

15. **Profil d'utilisation, type de disque et règle de hiérarchisation** : choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifiez la règle de hiérarchisation du volume, si nécessaire.

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

16. **Revue et approbation** : consultez et confirmez vos choix.
    a. Consultez les détails de la configuration.
    b. Cliquez sur **plus d'informations** pour en savoir plus sur le support et les ressources Azure que Cloud Manager achètera.
    c. Cochez les cases **Je comprends…**.
    d. Cliquez sur **Go**.

Résultat

Cloud Manager déploie le système Cloud Volumes ONTAP. Vous pouvez suivre la progression dans la chronologie.

Si vous rencontrez des problèmes lors du déploiement du système Cloud Volumes ONTAP, consultez le message d'échec. Vous pouvez également sélectionner l'environnement de travail et cliquer sur **recréer l'environnement**.

Pour obtenir de l'aide supplémentaire, consultez la page "Prise en charge de NetApp Cloud Volumes ONTAP".

Une fois que vous avez terminé

- Si vous avez provisionné un partage CIFS, donnez aux utilisateurs ou aux groupes des autorisations sur les fichiers et les dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier.
- Si vous souhaitez appliquer des quotas aux volumes, utilisez System Manager ou l'interface de ligne de commande.

  Les quotas vous permettent de restreindre ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree.

Lancez-vous dans GCP

Mise en route avec Cloud Volumes ONTAP pour Google Cloud

Lancez-vous avec Cloud Volumes ONTAP pour GCP en quelques étapes.

Créer un connecteur

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

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

Planification de la configuration

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

Configurez votre réseau

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

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

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

Configuration de GCP pour le Tiering des données

Deux exigences doivent être remplies pour transférer les données inactives de Cloud Volumes ONTAP vers un stockage objet à faible coût (un compartiment Google Cloud Storage) :

1. "Configurez le sous-réseau Cloud Volumes ONTAP pour un accès privé à Google".
2. "Configurez un compte de service pour le Tiering des données":
   - Attribuez le rôle *Storage Admin* prédéfini au compte de service de hiérarchisation.
   - Ajoutez le compte de service Connector en tant que *Service Account User* au compte de service Tiering.

Vous pouvez indiquer le rôle d'utilisateur "à l'étape 3 de l'assistant lorsque vous créez le compte de service de tiering", ou "attribuez le rôle après la création du compte de service".

Lorsque vous créez un environnement de travail Cloud Volumes ONTAP, vous devrez sélectionner le compte de service de Tiering.

Si vous n'activez pas le Tiering des données et sélectionnez un compte de service lorsque vous créez le système Cloud Volumes ONTAP, vous devrez désactiver le système et ajouter le compte de service à Cloud Volumes ONTAP à partir de la console GCP.

Activez les API Google Cloud

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

- API Cloud Deployment Manager V2
- API de journalisation cloud
- API Cloud Resource Manager
- API du moteur de calcul
- API de gestion des identités et des accès

Lancez Cloud Volumes ONTAP à l'aide de Cloud Manager

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

Liens connexes

- "L'évaluation"
- "Création d'un connecteur depuis Cloud Manager"
- "Installation du logiciel du connecteur sur un hôte Linux"
- "Avantages de Cloud Manager avec les autorisations GCP"

Planification de votre configuration Cloud Volumes ONTAP dans Google Cloud

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

Choix d'un type de licence

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

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

Compréhension des limites de stockage

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

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

Dimensionnement du système dans GCP

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

Type de machine

Examiner les types de machine pris en charge dans le "Notes de version de Cloud Volumes ONTAP" Puis passez en revue les détails de Google concernant chaque type de machine pris en charge. Faites correspondre les exigences de vos charges de travail au nombre de CPU virtuels et à la mémoire correspondant au type de machine. Notez que chaque cœur de processeur augmente les performances réseau.

Pour plus de détails, reportez-vous aux sections suivantes :

- "Documentation Google Cloud : types de machine standard N1"
- "Documentation Google Cloud : performances"

Type de disque GCP

Lorsque vous créez des volumes pour Cloud Volumes ONTAP, vous devez choisir le stockage cloud sous-jacent utilisé par Cloud Volumes ONTAP pour un disque. Le type de disque peut être soit *Zonal SSD persistent disks* soit *Zonal standard persistent disks*.

Les disques persistants des disques SSD sont parfaitement adaptés aux charges de travail qui exigent des taux élevés d'IOPS aléatoires, tandis que les disques persistants standard sont économiques et peuvent prendre en charge des opérations de lecture/écriture séquentielles. Pour plus de détails, voir "Documentation Google Cloud : disques persistants zonés (standard et SSD)".

Taille des disques GCP

Lorsque vous déployez un système Cloud Volumes ONTAP, vous devez choisir la taille de disque initiale. Après cela, Cloud Manager vous permet de gérer la capacité d'un système, mais si vous souhaitez créer vous-même des agrégats, sachez que :

- Tous les disques qui composent un agrégat doivent être de la même taille.
- Déterminez l'espace dont vous avez besoin tout en prenant en compte les performances.
- Les performances des disques persistants évoluent automatiquement en fonction de la taille des disques et du nombre de CPU virtuels disponibles pour le système.

  Pour plus de détails, reportez-vous aux sections suivantes :

  - "Documentation Google Cloud : disques persistants zonés (standard et SSD)"
  - "Documentation Google Cloud : optimisation des performances des disques persistants et des SSD locaux"

Fiche technique d'informations réseau GCP

Lorsque vous déployez Cloud Volumes ONTAP dans GCP, vous devez spécifier des informations relatives à votre réseau virtuel. Vous pouvez utiliser un modèle pour recueillir ces informations auprès de votre administrateur.

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

Sélection d'une vitesse d'écriture

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

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

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

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

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

Quand utiliser une vitesse d'écriture élevée

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

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

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

Choix d'un profil d'utilisation du volume

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

choisir le profil à utiliser.

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

Provisionnement fin

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

Déduplication

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

Compression

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

Exigences de mise en réseau pour le déploiement et la gestion de Cloud Volumes ONTAP dans GCP

Configurez votre réseau Google Cloud Platform de manière à ce que les systèmes Cloud Volumes ONTAP puissent fonctionner correctement. Cela inclut la mise en réseau pour le connecteur et le Cloud Volumes ONTAP.

Conditions requises pour Cloud Volumes ONTAP

Les exigences suivantes doivent être satisfaites dans GCP.

Cloud privé virtuel

Cloud Volumes ONTAP et le connecteur sont pris en charge dans un VPC partagé par Google Cloud et dans des VPC non partagés.

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

La seule exigence concernant l'utilisation d'un VPC partagé est de fournir le "Rôle utilisateur du réseau de calcul" Vers le compte de service Connector. Cloud Manager a besoin de ces autorisations pour interroger les pare-feu, le VPC et les sous-réseaux du projet hôte.

Accès Internet sortant pour Cloud Volumes ONTAP

Cloud Volumes ONTAP requiert un accès Internet sortant pour envoyer des messages à NetApp AutoSupport, qui surveille de façon proactive l'état de votre stockage.

Les règles de routage et de pare-feu doivent autoriser le trafic HTTP/HTTPS vers les terminaux suivants pour que Cloud Volumes ONTAP puisse envoyer les messages AutoSupport :

- https://support.netapp.com/aods/asupmessage
- https://support.netapp.com/asupprod/post/1.0/postAsup

"Découvrez comment configurer AutoSupport".

Nombre d'adresses IP

Cloud Manager attribue 5 adresses IP à Cloud Volumes ONTAP dans GCP.

Notez que Cloud Manager ne crée pas de LIF de gestion des SVM pour Cloud Volumes ONTAP dans GCP.

Une LIF est une adresse IP associée à un port physique. Une LIF de gestion SVM est nécessaire pour les outils de gestion tels que SnapCenter.

Règles de pare-feu

Inutile de créer des règles de pare-feu, car Cloud Manager le fait pour vous. Si vous devez vous en servir, reportez-vous aux règles de pare-feu répertoriées ci-dessous.

Connexion de Cloud Volumes ONTAP à Google Cloud Storage pour le Tiering des données

Pour transférer des données inactives vers un compartiment Google Cloud Storage, le sous-réseau dans lequel réside Cloud Volumes ONTAP doit être configuré pour un accès Google privé. Pour obtenir des instructions, reportez-vous à la section "Documentation Google Cloud : configuration de Private Google Access".

Pour connaître les étapes supplémentaires requises pour la configuration du Tiering des données dans Cloud Manager, consultez la section "Tiering des données inactives vers un stockage objet à faible coût".

Connexions aux systèmes ONTAP dans d'autres réseaux

Pour répliquer les données entre un système Cloud Volumes ONTAP dans GCP et des systèmes ONTAP d'autres réseaux, vous devez disposer d'une connexion VPN entre le VPC et l'autre réseau, par exemple votre réseau d'entreprise.

Pour obtenir des instructions, reportez-vous à la section "Documentation Google Cloud : présentation de Cloud VPN".

Configuration requise pour le connecteur

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

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

Connexion aux réseaux cibles

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

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

Accès Internet sortant

Le connecteur nécessite un accès Internet sortant pour gérer les ressources et les processus au sein de votre environnement de cloud public. Lors de la gestion des ressources dans GCP, un connecteur contacte les terminaux suivants :

Terminaux	Objectif
https://www.googleapis.com	Permet au connecteur de contacter les API Google pour le déploiement et la gestion de Cloud Volumes ONTAP dans GCP.
https://api.services.cloud.netapp.com:443	Demandes d'API à NetApp Cloud Central.
https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com	Permet d'accéder aux images logicielles, aux manifestes et aux modèles.
https://repo.cloud.support.netapp.com	Permet de télécharger les dépendances de Cloud Manager.
http://repo.mysql.com/	Utilisé pour télécharger MySQL.
https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com https://cloud-support-netapp-com-accelerated.s3.amazonaws.com	Permet au connecteur d'accéder aux manifestes, aux modèles et aux images de mise à niveau Cloud Volumes ONTAP et de les télécharger.
https://cloudmanagerinfraprod.azurecr.io	Accédez aux images logicielles des composants de conteneur pour une infrastructure exécutant Docker et fournie une solution pour les intégrations des services avec Cloud Manager.
https://kinesis.us-east-1.amazonaws.com	Permet à NetApp de diffuser des données à partir d'enregistrements d'audit.
https://cloudmanager.cloud.netapp.com	Communication avec le service Cloud Manager, notamment les comptes Cloud Central.
https://netapp-cloud-account.auth0.com	Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs.
https://mysupport.netapp.com	Communication avec NetApp AutoSupport.
https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement https://eval.lic.netapp.com.s3.us-west-1.amazonaws.com https://cloud-support-netapp-com.s3.us-west-1.amazonaws.com	Communication avec NetApp pour les licences système et l'inscription au support.
https://ipa-signer.cloudmanager.netapp.com	Génération des licences par Cloud Manager (par exemple, une licence FlexCache pour Cloud Volumes ONTAP)
https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/	Nécessaire pour connecter des systèmes Cloud Volumes ONTAP avec un cluster Kubernetes. Les terminaux permettent l'installation de NetApp Trident.

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

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

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

Règles de pare-feu pour Cloud Volumes ONTAP

Cloud Manager crée des règles de pare-feu GCP qui incluent les règles entrantes et sortantes nécessaires au bon fonctionnement de Cloud Manager et d'Cloud Volumes ONTAP. Vous pouvez vous référer aux ports à des fins de test ou si vous préférez que votre utilise ses propres groupes de sécurité.

Les règles de pare-feu de Cloud Volumes ONTAP requièrent des règles entrantes et sortantes.

Règles entrantes

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

Protocole	Port	Objectif
Tous les protocoles ICMP	Tout	Envoi d'une requête ping à l'instance
HTTP	80	Accès HTTP à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
HTTPS	443	Accès HTTPS à la console Web System Manager à l'aide de l'adresse IP du LIF de gestion de cluster
SSH	22	Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud
TCP	111	Appel de procédure à distance pour NFS
TCP	139	Session de service NetBIOS pour CIFS
TCP	161-162	Protocole de gestion de réseau simple
TCP	445	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
TCP	658	Montage NFS
TCP	749	Kerberos
TCP	2049	Démon du serveur NFS
TCP	3260	Accès iSCSI via le LIF de données iSCSI
TCP	4045	Démon de verrouillage NFS
TCP	4046	Surveillance de l'état du réseau pour NFS
TCP	10000	Sauvegarde avec NDMP
TCP	11104	Gestion des sessions de communication intercluster pour SnapMirror
TCP	11105	Transfert de données SnapMirror à l'aide de LIF intercluster
UDP	111	Appel de procédure à distance pour NFS
UDP	161-162	Protocole de gestion de réseau simple
UDP	658	Montage NFS
UDP	2049	Démon du serveur NFS
UDP	4045	Démon de verrouillage NFS
UDP	4046	Surveillance de l'état du réseau pour NFS
UDP	4049	Protocole NFS rquotad

Règles de sortie

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

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour Cloud Volumes ONTAP inclut les règles de sortie suivantes.

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

Règles de sortie avancées

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

La source est l'interface (adresse IP) du système Cloud Volumes ONTAP.

Service	Protocole	Port	Source	Destination	Objectif
Active Directory	TCP	88	FRV de gestion des nœuds	Forêt Active Directory	Authentification Kerberos V.
	UDP	137	FRV de gestion des nœuds	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	FRV de gestion des nœuds	Forêt Active Directory	Service de datagrammes NetBIOS
	TCP	139	FRV de gestion des nœuds	Forêt Active Directory	Session de service NetBIOS
	TCP ET UDP	389	FRV de gestion des nœuds	Forêt Active Directory	LDAP
	TCP	445	FRV de gestion des nœuds	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	UDP	464	FRV de gestion des nœuds	Forêt Active Directory	Administration des clés Kerberos
	TCP	749	FRV de gestion des nœuds	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)
	TCP	88	LIF de données (NFS, CIFS, iSCSI)	Forêt Active Directory	Authentification Kerberos V.
	UDP	137	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de noms NetBIOS
	UDP	138	FRV de données (NFS, CIFS)	Forêt Active Directory	Service de datagrammes NetBIOS
	TCP	139	FRV de données (NFS, CIFS)	Forêt Active Directory	Session de service NetBIOS
	TCP ET UDP	389	FRV de données (NFS, CIFS)	Forêt Active Directory	LDAP
	TCP	445	FRV de données (NFS, CIFS)	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
	TCP	464	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (SET_CHANGE)
	UDP	464	FRV de données (NFS, CIFS)	Forêt Active Directory	Administration des clés Kerberos
	TCP	749	FRV de données (NFS, CIFS)	Forêt Active Directory	Modification et définition du mot de passe Kerberos V (RPCSEC_GSS)

Service	Protocole	Port	Source	Destination	Objectif
Cluster	Tout le trafic	Tout le trafic	Tous les LIF sur un nœud	Tous les LIF de l'autre nœud	Communications InterCluster (Cloud Volumes ONTAP HA uniquement)
	TCP	3000	FRV de gestion des nœuds	Ha médiateur	Appels ZAPI (Cloud Volumes ONTAP HA uniquement)
	ICMP	1	FRV de gestion des nœuds	Ha médiateur	Rester en vie (Cloud Volumes ONTAP HA uniquement)
DHCP	UDP	68	FRV de gestion des nœuds	DHCP	Client DHCP pour la première configuration
DHCPS	UDP	67	FRV de gestion des nœuds	DHCP	Serveur DHCP
DNS	UDP	53	FRV de gestion des nœuds et FRV de données (NFS, CIFS)	DNS	DNS
NDMP	TCP	18600-18699	FRV de gestion des nœuds	Serveurs de destination	Copie NDMP
SMTP	TCP	25	FRV de gestion des nœuds	Serveur de messagerie	Les alertes SMTP peuvent être utilisées pour AutoSupport
SNMP	TCP	161	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	UDP	161	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	TCP	162	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
	UDP	162	FRV de gestion des nœuds	Serveur de surveillance	Surveillance par des interruptions SNMP
SnapMirror	TCP	11104	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Gestion des sessions de communication intercluster pour SnapMirror
	TCP	11105	FRV InterCluster	Baies de stockage inter-clusters ONTAP	Transfert de données SnapMirror
Syslog	UDP	514	FRV de gestion des nœuds	Serveur Syslog	Messages de transfert syslog

Règles de pare-feu pour le connecteur

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

Règles entrantes

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

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

Règles de sortie

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

Règles de base pour les appels sortants

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

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

Règles de sortie avancées

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

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

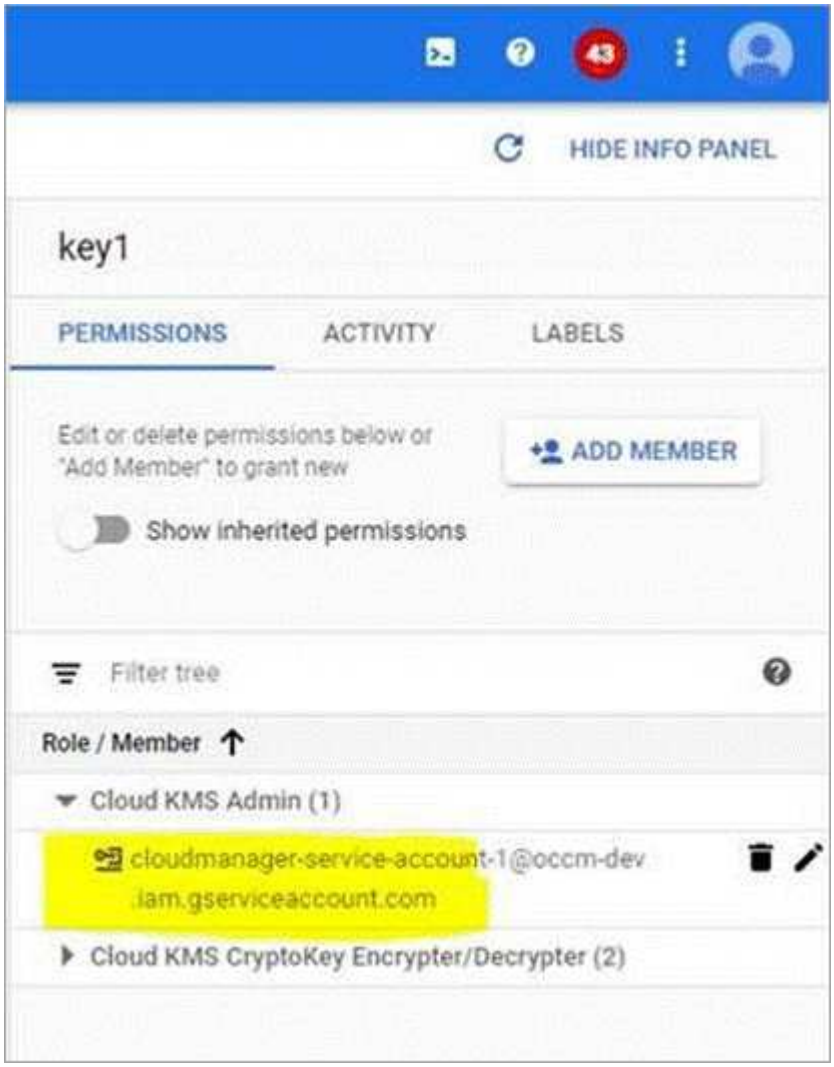
Service	Protocole	Port	Destination	Objectif
Active Directory	TCP	88	Forêt Active Directory	Authentification Kerberos V.
	TCP	139	Forêt Active Directory	Session de service NetBIOS
	TCP	389	Forêt Active Directory	LDAP
	TCP	445	Forêt Active Directory	Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS
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

Grâce à des clés de chiffrement gérées par le client avec Cloud Volumes ONTAP

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

Étapes

1. Donnez au compte de service Connector l'autorisation d'utiliser la clé de cryptage.



2. Obtenir l'ID de la clé en invoquant la commande GET pour l'API /gcp/vsa/Metadata/gcp-Encryption-keys
3. Utilisez le paramètre "GcpEncryption" avec votre requête API lors de la création d'un environnement de travail.

Exemple

```
"gcpEncryptionParameters": {
    "key": "projects/tlv-support/locations/us-
east4/keyRings/Nikiskeys/cryptoKeys/generatedkey1"
  }
```

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

Lancement d'Cloud Volumes ONTAP dans GCP

Vous pouvez lancer un système Cloud Volumes ONTAP à nœud unique dans GCP en créant un environnement de travail.

Ce dont vous avez besoin

- Vous devez avoir un "Connecteur associé à votre espace de travail".

> Vous devez être un administrateur de compte pour créer un connecteur. Lorsque vous créez votre premier environnement de travail Cloud Volumes ONTAP, Cloud Manager vous invite à créer un connecteur si vous ne l'avez pas encore fait.

- "Vous devez être prêt à laisser le connecteur fonctionner en permanence".
- Vous devez avoir choisi une configuration et obtenir des informations de mise en réseau GCP auprès de votre administrateur. Pour plus de détails, voir "Planification de votre configuration Cloud Volumes ONTAP".
- Pour déployer un système BYOL, vous devez disposer du numéro de série à 20 chiffres (clé de licence) pour chaque nœud.
- Il convient de définir les API Google Cloud suivantes "activé dans votre projet":
  - API Cloud Deployment Manager V2
  - API de journalisation cloud
  - API Cloud Resource Manager
  - API du moteur de calcul
  - API de gestion des identités et des accès

Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail** et suivez les invites.
2. **Choisissez un emplacement** : sélectionnez **Google Cloud** et **Cloud Volumes ONTAP**.
3. **Détails et informations d'identification** : sélectionnez un projet, spécifiez un nom de cluster, ajoutez éventuellement des étiquettes, puis spécifiez les informations d'identification.

   Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Nom de l'environnement de travail	Cloud Manager utilise le nom de l'environnement de travail pour nommer le système Cloud Volumes ONTAP et l'instance de machine virtuelle GCP. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option.

Champ	Description
Ajouter des étiquettes	Les étiquettes sont des métadonnées pour les ressources GCP. Cloud Manager ajoute les étiquettes au système Cloud Volumes ONTAP et aux ressources GCP associées au système. Vous pouvez ajouter jusqu'à quatre étiquettes à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis vous pouvez en ajouter d'autres une fois qu'elles ont été créées. Notez que l'API ne vous limite pas à quatre étiquettes lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section "Documentation Google Cloud : étiquetage des ressources".
Nom d'utilisateur et mot de passe	Il s'agit des informations d'identification du compte d'administration du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces identifiants pour vous connecter à Cloud Volumes ONTAP via System Manager ou son interface de ligne de commandes.
Modifier le projet	Sélectionnez le projet dans lequel vous souhaitez que Cloud Volumes ONTAP réside. Le projet par défaut est le projet sur lequel réside Cloud Manager. Si d'autres projets ne s'affichent pas dans la liste déroulante, le compte de service Cloud Manager n'est pas encore associé à d'autres projets. Accédez à la console Google Cloud, ouvrez le service IAM et sélectionnez le projet. Ajoutez le compte de service avec le rôle Cloud Manager à ce projet. Vous devrez répéter cette étape pour chaque projet. Il s'agit du compte de service que vous configurez pour Cloud Manager, "comme décrit à l'étape 2b sur cette page". Cliquez sur **Ajouter un abonnement** pour associer les informations d'identification sélectionnées à un abonnement. Pour créer un système Cloud Volumes ONTAP de paiement basé sur l'utilisation, vous devez sélectionner un projet GCP associé à un abonnement à Cloud Volumes ONTAP depuis GCP Marketplace.

Découvrez dans cette vidéo comment associer un abonnement Marketplace basé sur l'utilisation à votre projet GCP :

► https://docs.netapp.com/fr-fr/occm38//media/video_subscribing_gcp.mp4 *(video)*

4. **Localisation et connectivité** : sélectionnez un emplacement, choisissez une stratégie de pare-feu et cochez la case pour confirmer la connectivité réseau au stockage Google Cloud pour le Tiering des données.

   Pour transférer des données inactives vers un compartiment Google Cloud Storage, le sous-réseau dans lequel réside Cloud Volumes ONTAP doit être configuré pour un accès Google privé. Pour obtenir des instructions, reportez-vous à la section "Documentation Google Cloud : configuration de Private Google Access".

5. **Compte du site de licence et de support** : indiquez si vous souhaitez utiliser le paiement à l'utilisation ou BYOL, puis indiquez un compte sur le site de support NetApp.

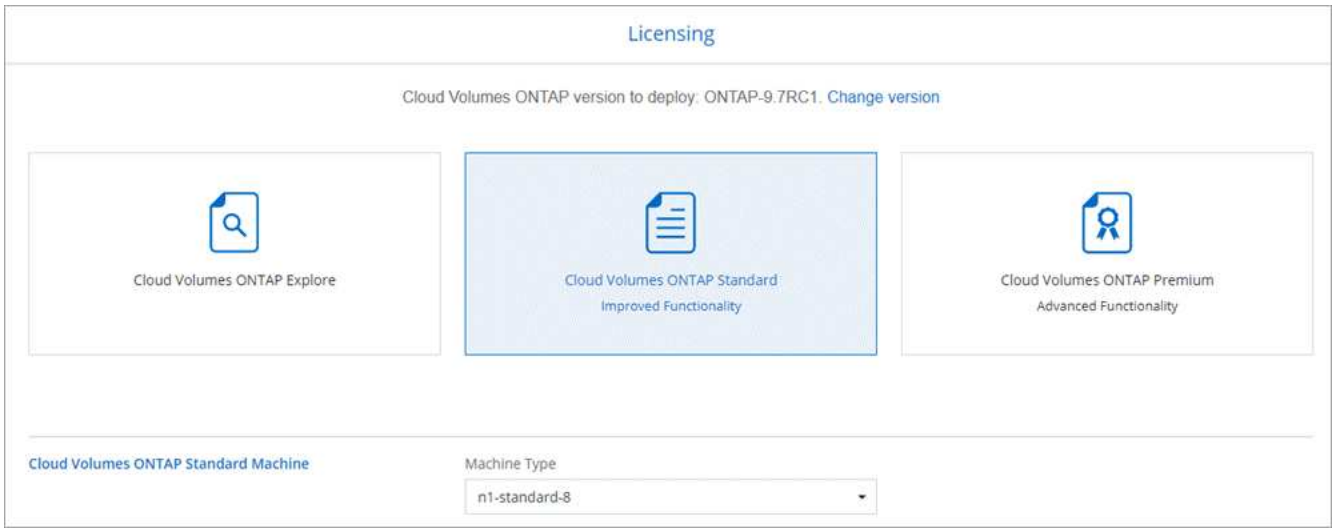
   Pour comprendre le fonctionnement des licences, reportez-vous à la section "Licences".

Un compte sur le site de support NetApp est facultatif afin de bénéficier d'un paiement à l'utilisation, mais requis pour les systèmes BYOL. "Découvrez comment ajouter des comptes au site de support NetApp".

6. **Packages préconfigurés** : sélectionnez un des packages pour déployer rapidement un système Cloud Volumes ONTAP ou cliquez sur **Créer ma propre configuration**.

   Si vous choisissez l'un des packages, vous n'avez qu'à spécifier un volume, puis à revoir et approuver la configuration.

7. **Licence** : modifiez la version de Cloud Volumes ONTAP selon vos besoins, sélectionnez une licence et sélectionnez un type de machine virtuelle.



   Si vos besoins changent après le lancement du système, vous pouvez modifier la licence ou le type de machine virtuelle ultérieurement.

   > Si une version plus récente de Release Candidate, General Availability ou patch est disponible pour la version sélectionnée, Cloud Manager met à jour le système à cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.6 RC1 et 9.6 GA est disponible. La mise à jour ne se produit pas d'une version à l'autre, par exemple de 9.6 à 9.7.

8. **Ressources de stockage sous-jacentes** : Choisissez les paramètres de l'agrégat initial : un type de disque et la taille de chaque disque.

   Le type de disque correspond au volume initial. Vous pouvez choisir un autre type de disque pour les volumes suivants.

   La taille du disque correspond à tous les disques de l'agrégat initial et à tous les agrégats supplémentaires créés par Cloud Manager lorsque vous utilisez l'option de provisionnement simple. Vous pouvez créer des agrégats qui utilisent une taille de disque différente à l'aide de l'option d'allocation avancée.

   Pour obtenir de l'aide sur le choix du type et de la taille d'un disque, reportez-vous à la section "Dimensionnement du système dans GCP".

9. **Vitesse d'écriture et WORM** : choisissez **Normal** ou **vitesse d'écriture élevée**, et activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

   La sélection d'une vitesse d'écriture est prise en charge avec les systèmes à un seul nœud uniquement.

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

IMPOSSIBLE D'activer WORM si le Tiering des données était activé.

"En savoir plus sur le stockage WORM".

10. **Tiering de données dans Google Cloud Platform**: Choisissez d'activer ou non le Tiering des données sur l'agrégat initial, de choisir une classe de stockage pour les données hiérarchisées, puis de sélectionner un compte de service disposant du rôle d'administrateur de stockage prédéfini (requis pour Cloud Volumes ONTAP 9.7) ou de sélectionner un compte GCP (requis pour Cloud Volumes ONTAP 9.6).

    Notez ce qui suit :

    - Cloud Manager définit le compte de service sur l'instance Cloud Volumes ONTAP. Ce compte de service fournit des autorisations de Tiering des données vers un compartiment Google Cloud Storage. N'oubliez pas d'ajouter le compte de service Cloud Manager en tant qu'utilisateur du compte de service de Tiering ou bien ne pouvez pas le sélectionner depuis Cloud Manager.
    - Pour obtenir de l'aide sur l'ajout d'un compte GCP, reportez-vous à "Configuration et ajout de comptes GCP pour le Tiering des données avec la version 9.6".
    - Vous pouvez choisir une règle de Tiering des volumes spécifique lorsque vous créez ou modifiez un volume.
    - Si vous désactivez le Tiering, vous pouvez l'activer sur les agrégats suivants, mais vous devrez désactiver le système et ajouter un compte de service à partir de la console GCP.

      "En savoir plus sur le Tiering des données".

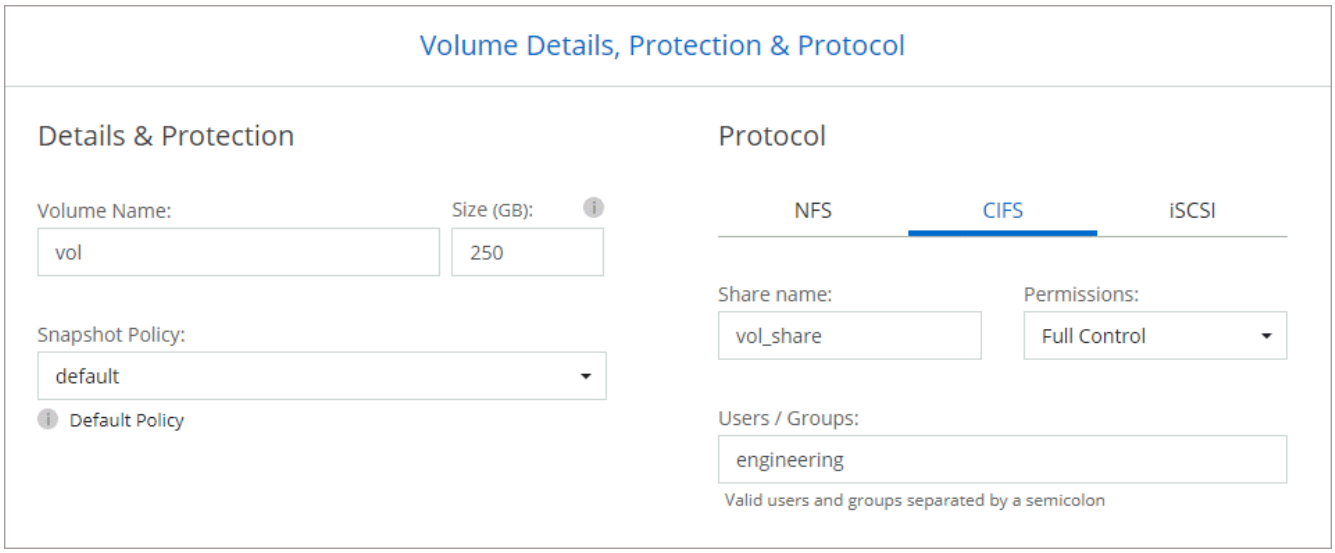
11. **Créer un volume** : saisissez les détails du nouveau volume ou cliquez sur **Ignorer**.

    Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, Cloud Manager entre une valeur qui donne accès à toutes les instances du sous-réseau.
Autorisations et utilisateurs/groupes (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur à l'aide du format domaine\nom d'utilisateur.
Stratégie Snapshot	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.

Champ	Description
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de buste hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".

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



12. **Configuration CIFS** : si vous choisissez le protocole CIFS, configurez un serveur CIFS.

Champ	Description
Adresse IP principale et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS.
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Nom de serveur CIFS unique dans le domaine AD.

Champ	Description
Unité organisationnelle	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers.
Domaine DNS	Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD.
Serveur NTP	Sélectionnez **utiliser le domaine Active Directory** pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la "Guide du développeur de l'API Cloud Manager" pour plus d'informations.

13. **Profil d'utilisation, type de disque et règle de hiérarchisation** : choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifiez la règle de hiérarchisation du volume, si nécessaire.

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

14. **Revue et approbation** : consultez et confirmez vos choix.
    a. Consultez les détails de la configuration.
    b. Cliquez sur **plus d'informations** pour en savoir plus sur le support et les ressources GCP que Cloud Manager achètera.
    c. Cochez les cases **Je comprends…**.
    d. Cliquez sur **Go**.

Résultat

Cloud Manager déploie le système Cloud Volumes ONTAP. Vous pouvez suivre la progression dans la chronologie.

Si vous rencontrez des problèmes lors du déploiement du système Cloud Volumes ONTAP, consultez le message d'échec. Vous pouvez également sélectionner l'environnement de travail et cliquer sur **recréer l'environnement**.

Pour obtenir de l'aide supplémentaire, consultez la page "Prise en charge de NetApp Cloud Volumes ONTAP".

Une fois que vous avez terminé

- Si vous avez provisionné un partage CIFS, donnez aux utilisateurs ou aux groupes des autorisations sur les fichiers et les dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier.
- Si vous souhaitez appliquer des quotas aux volumes, utilisez System Manager ou l'interface de ligne de commande.

  Les quotas vous permettent de restreindre ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree.

Provisionner et gérer le stockage

Provisionnement du stockage

Vous pouvez provisionner du stockage supplémentaire pour vos systèmes Cloud Volumes ONTAP depuis Cloud Manager en gérant les volumes et les agrégats.

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

Création de volumes FlexVol

Si vous avez besoin de plus de stockage après le lancement d'un système Cloud Volumes ONTAP, vous pouvez créer de nouveaux volumes FlexVol pour NFS, CIFS ou iSCSI à partir de Cloud Manager.

Description de la tâche

Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes.

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

Avant de commencer

Si vous souhaitez utiliser CIFS dans AWS, vous devez avoir configuré DNS et Active Directory. Pour plus de détails, voir "Configuration réseau requise pour Cloud Volumes ONTAP pour AWS".

Étapes

1. Sur la page Working Environments, double-cliquez sur le nom du système Cloud Volumes ONTAP sur lequel vous souhaitez provisionner les volumes FlexVol.
2. Créez un nouveau volume sur un agrégat ou sur un agrégat spécifique :

Action	Étapes
Créez un nouveau volume et laissez Cloud Manager choisir l'agrégat contenant	Cliquez sur **Ajouter nouveau volume**.
Créez un nouveau volume sur un agrégat spécifique	a. Cliquez sur l'icône du menu, puis sur **Avancé > attribution avancée**. b. Cliquez sur le menu correspondant à un agrégat. c. Cliquez sur **Créer un volume**.

3. Entrez les détails du nouveau volume, puis cliquez sur **Continuer**.

   Certains champs de cette page sont explicites. Le tableau suivant décrit les champs pour lesquels vous pouvez avoir besoin de conseils :

Champ	Description
Taille	La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible.
Contrôle d'accès (pour NFS uniquement)	Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, Cloud Manager entre une valeur qui donne accès à toutes les instances du sous-réseau.

Champ	Description
Autorisations et utilisateurs/groupes (pour CIFS uniquement)	Ces champs vous permettent de contrôler le niveau d'accès à un partage pour les utilisateurs et les groupes (également appelés listes de contrôle d'accès ou ACL). Vous pouvez spécifier des utilisateurs ou des groupes Windows locaux ou de domaine, ou des utilisateurs ou des groupes UNIX. Si vous spécifiez un nom d'utilisateur Windows de domaine, vous devez inclure le domaine de l'utilisateur à l'aide du format domaine\nom d'utilisateur.
Stratégie Snapshot	Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server.
Options avancées (pour NFS uniquement)	Sélectionnez une version NFS pour le volume : NFSv3 ou NFSv4.
Groupe initiateur et IQN (pour iSCSI uniquement)	Les cibles de stockage iSCSI sont appelées LUN (unités logiques) et sont présentées aux hôtes sous forme de périphériques de blocs standard. Les groupes initiateurs sont des tableaux de noms de nœud hôte iSCSI et ils contrôlent l'accès des initiateurs aux différentes LUN. Les cibles iSCSI se connectent au réseau via des cartes réseau Ethernet (NIC) standard, des cartes TOE (TCP Offload Engine) avec des initiateurs logiciels, des adaptateurs réseau convergés (CNA) ou des adaptateurs de buste hôte dédiés (HBA) et sont identifiés par des noms qualifiés iSCSI (IQN). Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".

4. Si vous avez choisi le protocole CIFS et que le serveur CIFS n'a pas été configuré, spécifiez les détails du serveur dans la boîte de dialogue Créer un serveur CIFS, puis cliquez sur **Enregistrer et continuer** :

Champ	Description
Adresse IP principale et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS.
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Nom de serveur CIFS unique dans le domaine AD.

Champ	Description
Unité organisationnelle	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. • Pour configurer Microsoft AD géré par AWS en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer **ou=ordinateurs,ou=corp** dans ce champ. • Pour configurer les services de domaine Azure AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer **ou=ordinateurs ADDC** ou **ou=utilisateurs ADDC** dans ce champ.https://docs.microsoft.com/en-us/azure/active-directory-domain-services/create-ou["Documentation Azure : créez une unité organisationnelle dans un domaine géré Azure AD Domain Services"^]
Domaine DNS	Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD.
Serveur NTP	Sélectionnez **utiliser le domaine Active Directory** pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la "Guide du développeur de l'API Cloud Manager" pour plus d'informations.

5. Sur la page profil d'utilisation, type de disque et règle de Tiering, choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage, choisissez un type de disque et modifiez la règle de Tiering, si nécessaire.

   Pour obtenir de l'aide, reportez-vous aux documents suivants :

   - "Présentation des profils d'utilisation des volumes"
   - "Dimensionnement de votre système dans AWS"
   - "Dimensionnement du système dans Azure"
   - "Vue d'ensemble du hiérarchisation des données"

6. Cliquez sur **Go**.

Résultat

Cloud Volumes ONTAP en assure la gestion.

Une fois que vous avez terminé

Si vous avez provisionné un partage CIFS, donnez aux utilisateurs ou aux groupes des autorisations sur les fichiers et les dossiers et vérifiez que ces utilisateurs peuvent accéder au partage et créer un fichier.

Si vous souhaitez appliquer des quotas aux volumes, vous devez utiliser System Manager ou l'interface de ligne de commande. Les quotas vous permettent de restreindre ou de suivre l'espace disque et le nombre de fichiers utilisés par un utilisateur, un groupe ou un qtree.

Création de volumes FlexVol sur le second nœud dans une configuration haute disponibilité

Par défaut, Cloud Manager crée des volumes sur le premier nœud d'une configuration HA. Si vous avez besoin d'une configuration active-active, dans laquelle les deux nœuds servent les données aux clients, vous devez créer des agrégats et des volumes sur le second nœud.

Étapes

1. Sur la page Working Environments, double-cliquez sur le nom de l'environnement de travail Cloud Volumes ONTAP sur lequel vous souhaitez gérer les agrégats.
2. Cliquez sur l'icône du menu, puis sur **Avancé > attribution avancée**.
3. Cliquez sur **Ajouter agrégat**, puis créez l'agrégat.
4. Pour le nœud principal, choisissez le second nœud dans la paire HA.
5. Une fois que Cloud Manager a créé l'agrégat, sélectionnez-le, puis cliquez sur **Create volume**.
6. Entrez les détails du nouveau volume, puis cliquez sur **Créer**.

Une fois que vous avez terminé

Vous pouvez créer des volumes supplémentaires sur cet agrégat si nécessaire.

Pour les paires HA déployées dans plusieurs zones de disponibilité AWS, vous devez monter le volume sur les clients en utilisant l'adresse IP flottante du nœud sur lequel réside le volume.

Création d'agrégats

Vous pouvez créer des agrégats vous-même ou laisser Cloud Manager le faire lorsque vous créez des volumes. L'avantage de créer des agrégats vous-même est de choisir la taille du disque sous-jacent, ce qui vous permet de dimensionner l'agrégat en fonction de la capacité ou des performances requises.

Étapes

1. Sur la page Working Environments, double-cliquez sur le nom de l'instance Cloud Volumes ONTAP sur laquelle vous souhaitez gérer les agrégats.
2. Cliquez sur l'icône du menu, puis sur **Avancé > attribution avancée**.
3. Cliquez sur **Ajouter agrégat**, puis spécifiez les détails de l'agrégat.

   Pour obtenir de l'aide sur le type et la taille du disque, reportez-vous à la section "Planification de votre configuration".

4. Cliquez sur **Go**, puis sur **approuver et acheter**.

Connexion d'une LUN à un hôte

Lorsque vous créez un volume iSCSI, Cloud Manager crée automatiquement une LUN pour vous. Nous avons simplifié la gestion en créant un seul LUN par volume, donc aucune gestion n'est nécessaire. Une fois le volume créé, utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes.

Notez ce qui suit :

1. La gestion automatique de la capacité de Cloud Manager ne s'applique pas aux LUN. Lorsque Cloud Manager crée un LUN, il désactive la fonctionnalité de croissance automatique.
2. Vous pouvez créer des LUN supplémentaires depuis System Manager ou l'interface de ligne de commandes.

Étapes

1. Sur la page Working Environments, double-cliquez sur l'environnement de travail Cloud Volumes ONTAP sur lequel vous souhaitez gérer les volumes.
2. Sélectionnez un volume, puis cliquez sur **IQN cible**.
3. Cliquez sur **Copy** pour copier le nom IQN.
4. Configurez une connexion iSCSI de l'hôte vers le LUN.
    - "Configuration iSCSI express ONTAP 9 pour Red Hat Enterprise Linux : démarrage des sessions iSCSI avec la cible"
    - "Configuration iSCSI express de ONTAP 9 pour Windows : démarrage des sessions iSCSI avec la cible"

Utilisation de volumes FlexCache pour accélérer l'accès aux données

Un volume FlexCache est un volume de stockage qui met en cache les données lues par NFS à partir d'un volume d'origine (ou source). Les lectures suivantes des données mises en cache permettent un accès plus rapide à ces données.

Les volumes FlexCache peuvent être utilisés pour accélérer l'accès aux données ou pour décharger le trafic des volumes fortement sollicités. Les volumes FlexCache contribuent à améliorer les performances, en particulier lorsque les clients doivent accéder de façon répétée aux mêmes données, car elles peuvent être servies directement sans avoir à accéder au volume d'origine. Les volumes FlexCache fonctionnent parfaitement pour les charges de travail système intensives en lecture.

Cloud Manager n'assure pas la gestion des volumes FlexCache pour le moment, mais vous pouvez utiliser l'interface de ligne de commande ONTAP ou ONTAP System Manager pour créer et gérer des volumes FlexCache :

- "Guide de puissance des volumes FlexCache pour un accès plus rapide aux données"
- "Création de volumes FlexCache dans System Manager"

À partir de la version 3.7.2, Cloud Manager génère une licence FlexCache pour tous les nouveaux systèmes Cloud Volumes ONTAP. La licence inclut une limite d'utilisation de 500 Go.

Pour générer la licence, Cloud Manager doit accéder au https://ipa-signer.cloudmanager.netapp.com. Assurez-vous que cette URL est accessible à partir de votre pare-feu.

Gestion du stockage existant

Cloud Manager vous permet de gérer les volumes, les agrégats et les serveurs CIFS. Il vous invite également à déplacer des volumes afin d'éviter les problèmes de capacité.

Gestion des volumes existants

Vous pouvez gérer les volumes existants à mesure que vos besoins de stockage changent. Vous pouvez afficher, modifier, cloner, restaurer et supprimer des volumes.

Étapes

1. Sur la page Working Environments, double-cliquez sur l'environnement de travail Cloud Volumes ONTAP sur lequel vous souhaitez gérer les volumes.
2. Gérez vos volumes :

Tâche	Action
Afficher des informations sur un volume	Sélectionnez un volume, puis cliquez sur **Info**.
Modifier un volume (volumes en lecture-écriture uniquement)	a. Sélectionnez un volume, puis cliquez sur **Modifier**. b. Modifiez la stratégie Snapshot du volume, la version du protocole NFS, la liste de contrôle d'accès NFS ou les autorisations de partage, puis cliquez sur **Update**. Si vous avez besoin de règles Snapshot personnalisées, vous pouvez les créer à l'aide de System Manager.

Tâche	Action
Clonez un volume	a. Sélectionnez un volume, puis cliquez sur **Clone**. b. Modifiez le nom du clone selon vos besoins, puis cliquez sur **Clone**. Ce processus crée un volume FlexClone. Un volume FlexClone est une copie inscriptible, ponctuelle et efficace dans l'espace, car il utilise une petite quantité d'espace pour les métadonnées, puis ne consomme que de l'espace supplémentaire lorsque les données sont modifiées ou ajoutées. Pour en savoir plus sur les volumes FlexClone, consultez le "Guide de gestion du stockage logique ONTAP 9".
Restaurer les données d'une copie Snapshot vers un nouveau volume	a. Sélectionnez un volume, puis cliquez sur **Restaurer à partir de la copie Snapshot**. b. Sélectionnez une copie Snapshot, indiquez le nom du nouveau volume, puis cliquez sur **Restore**.
Créez une copie Snapshot à la demande	a. Sélectionnez un volume, puis cliquez sur **Créer une copie snapshot**. b. Modifiez le nom, si nécessaire, puis cliquez sur **Créer**.
Obtenez la commande NFS mount	a. Sélectionnez un volume, puis cliquez sur **Mount Command**. b. Cliquez sur **Copier**.
Afficher l'IQN cible d'un volume iSCSI	a. Sélectionnez un volume, puis cliquez sur **IQN cible**. b. Cliquez sur **Copier**. c. "Utilisez l'IQN pour vous connecter à la LUN à partir de vos hôtes".
Modifiez le type de disque sous-jacent	a. Sélectionnez un volume, puis cliquez sur **Modifier le type de disque et la stratégie de hiérarchisation**. b. Sélectionnez le type de disque, puis cliquez sur **changer**. Cloud Manager déplace le volume vers un agrégat existant qui utilise le type de disque sélectionné ou crée un nouvel agrégat pour le volume.
Modifiez la stratégie de hiérarchisation	a. Sélectionnez un volume, puis cliquez sur **Modifier le type de disque et la stratégie de hiérarchisation**. b. Cliquez sur **Modifier la stratégie**. c. Sélectionnez une autre stratégie et cliquez sur **Modifier**. Cloud Manager déplace le volume vers un agrégat existant qui utilise le type de disque sélectionné avec hiérarchisation ou crée un nouvel agrégat pour le volume.

Tâche	Action
Supprimer un volume	a. Sélectionnez un volume, puis cliquez sur **Supprimer**. b. Cliquez à nouveau sur **Supprimer** pour confirmer.

Gestion des agrégats existants

Gérez vous-même les agrégats en ajoutant des disques, en affichant les informations sur les agrégats et en les supprimant.

Avant de commencer

Si vous souhaitez supprimer un agrégat, vous devez d'abord supprimer les volumes de l'agrégat.

Description de la tâche

Si un agrégat manque d'espace, vous pouvez déplacer des volumes vers un autre agrégat à l'aide d'OnCommand System Manager.

Étapes

1. Sur la page Working Environments, double-cliquez sur l'environnement de travail Cloud Volumes ONTAP sur lequel vous souhaitez gérer les agrégats.
2. Cliquez sur l'icône du menu, puis sur **Avancé > attribution avancée**.
3. Gérez vos agrégats :

Tâche	Action
Afficher des informations sur un agrégat	Sélectionnez un agrégat et cliquez sur **Info**.
Créez un volume sur un agrégat spécifique	Sélectionnez un agrégat et cliquez sur **Create volume**.
Ajoutez des disques à un agrégat	a. Sélectionnez un agrégat et cliquez sur **Ajouter des disques AWS** ou **Ajouter des disques Azure**. b. Sélectionnez le nombre de disques que vous souhaitez ajouter et cliquez sur **Ajouter**.  Tous les disques qui composent un agrégat doivent être de la même taille.
Supprimer un agrégat	a. Sélectionnez un agrégat qui ne contient aucun volume et cliquez sur **Supprimer**. b. Cliquez à nouveau sur **Supprimer** pour confirmer.

Modification du serveur CIFS

Si vous modifiez vos serveurs DNS ou votre domaine Active Directory, vous devez modifier le serveur CIFS dans Cloud Volumes ONTAP pour pouvoir continuer à servir le stockage aux clients.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > Configuration CIFS**.
2. Spécifiez les paramètres du serveur CIFS :

Tâche	Action
Adresse IP principale et secondaire DNS	Les adresses IP des serveurs DNS qui fournissent la résolution de noms pour le serveur CIFS. Les serveurs DNS répertoriés doivent contenir les enregistrements d'emplacement de service (SRV) nécessaires à la localisation des serveurs LDAP et des contrôleurs de domaine Active Directory pour le domaine auquel le serveur CIFS se joindra.
Domaine Active Directory à rejoindre	Le FQDN du domaine Active Directory (AD) auquel vous souhaitez joindre le serveur CIFS.
Informations d'identification autorisées à rejoindre le domaine	Nom et mot de passe d'un compte Windows disposant de privilèges suffisants pour ajouter des ordinateurs à l'unité d'organisation spécifiée dans le domaine AD.
Nom NetBIOS du serveur CIFS	Nom de serveur CIFS unique dans le domaine AD.
Unité organisationnelle	Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. Si vous configurez AWS Managed Microsoft AD en tant que serveur AD pour Cloud Volumes ONTAP, vous devez entrer **ou=ordinateurs,ou=corp** dans ce champ.
Domaine DNS	Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD.
Serveur NTP	Sélectionnez **utiliser le domaine Active Directory** pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la "Guide du développeur de l'API Cloud Manager" pour plus d'informations.

3. Cliquez sur **Enregistrer**.

Résultat

Cloud Volumes ONTAP met à jour le serveur CIFS avec les modifications.

Déplacement d'un volume

Déplacer les volumes pour optimiser l'utilisation de la capacité et les performances, et satisfaire les contrats de niveau de service.

Vous pouvez déplacer un volume dans System Manager en sélectionnant un volume et l'agrégat de destination, en commençant l'opération de déplacement de volume et, éventuellement, en surveillant la tâche de déplacement de volume. Avec System Manager, une opération de déplacement de volume se termine automatiquement.

Étapes

1. Utilisez System Manager ou l'interface de ligne de commande pour déplacer les volumes vers l'agrégat.

   Dans la plupart des cas, vous pouvez utiliser System Manager pour déplacer des volumes.

Pour obtenir des instructions, reportez-vous au "Guide de migration de volumes ONTAP 9 Express".

Déplacement d'un volume lorsque Cloud Manager affiche un message action requise

Cloud Manager peut afficher un message Action requise indiquant que le déplacement d'un volume est nécessaire pour éviter les problèmes de capacité, mais qu'il ne peut pas fournir de recommandations pour corriger le problème. Dans ce cas, vous devez identifier comment corriger le problème, puis déplacer un ou plusieurs volumes.

Étapes

1. Identifier la manière de corriger le problème.
2. En fonction de votre analyse, déplacez les volumes pour éviter les problèmes de capacité :
   - Déplacement des volumes vers un autre système.
   - Déplacement des volumes vers un autre agrégat du même système.

Identifier comment corriger les problèmes de capacité

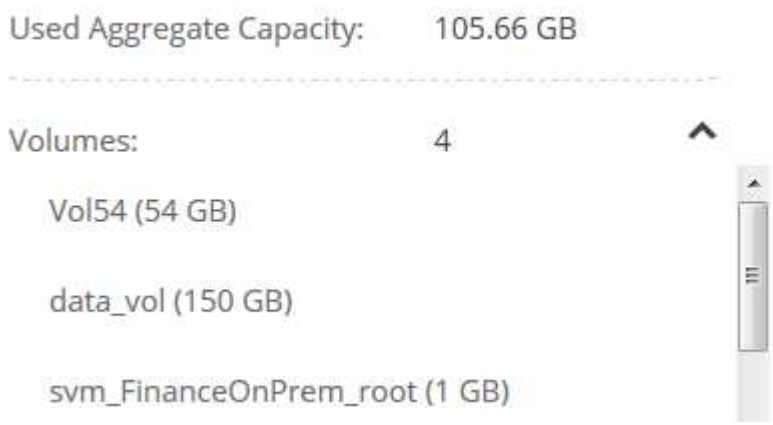
Si Cloud Manager ne peut pas fournir de recommandations pour le déplacement d'un volume afin d'éviter les problèmes de capacité, vous devez identifier les volumes que vous devez déplacer et indiquer si vous devez les déplacer vers un autre agrégat sur le même système ou vers un autre système.

Étapes

1. Consultez les informations avancées du message Action requise pour identifier l'agrégat ayant atteint sa limite de capacité.

   Par exemple, l'information avancée devrait dire quelque chose de similaire à ce qui suit : aggr1 global a atteint sa limite de capacité.

2. Identifiez un ou plusieurs volumes à sortir de l'agrégat :
   a. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > allocation avancée**.
   b. Sélectionnez l'agrégat, puis cliquez sur **Info**.
   c. Développez la liste des volumes.



   d. Passez en revue la taille de chaque volume et choisissez un ou plusieurs volumes pour sortir de l'agrégat.

      Vous devez choisir des volumes suffisamment volumineux pour libérer de l'espace dans l'agrégat afin

d'éviter d'autres problèmes de capacité à l'avenir.

3. Si le système n'a pas atteint la limite de disque, vous devez déplacer les volumes vers un agrégat existant ou vers un nouvel agrégat sur le même système.

   Pour plus de détails, voir "Déplacement des volumes vers un autre agrégat pour éviter les problèmes de capacité".

4. Si le système a atteint la limite de disque, effectuez l'une des opérations suivantes :
   a. Supprimez tous les volumes inutilisés.
   b. Réorganiser les volumes pour libérer de l'espace sur un agrégat.

      Pour plus de détails, voir "Déplacement des volumes vers un autre agrégat pour éviter les problèmes de capacité".

   c. Déplacez deux volumes ou plus vers un autre système disposant d'espace.

      Pour plus de détails, voir "Déplacement des volumes vers un autre système pour éviter les problèmes de capacité".

Déplacement des volumes vers un autre système pour éviter les problèmes de capacité

Vous pouvez déplacer un ou plusieurs volumes vers un autre système Cloud Volumes ONTAP pour éviter les problèmes de capacité. Vous devrez peut-être le faire si le système a atteint sa limite de disque.

Description de la tâche

Vous pouvez suivre les étapes de cette tâche pour corriger le message Action requise suivant :

```
 Moving a volume is necessary to avoid capacity issues; however, Cloud
Manager cannot perform this action for you because the system has reached
the disk limit.
.Étapes
. Identifiez un système Cloud Volumes ONTAP doté de la capacité disponible
ou déployez un nouveau système.
. Faites glisser et déposez l'environnement de travail source sur
l'environnement de travail cible pour effectuer une réplication unique du
volume.
```

+
Pour plus de détails, voir "Réplication des données entre les systèmes".

1. Accédez à la page Etat de la réplication, puis rompez la relation SnapMirror pour convertir le volume répliqué d'un volume de protection des données en volume en lecture/écriture.

   Pour plus de détails, voir "Gestion des planifications et des relations de réplication des données".

2. Configurez le volume pour l'accès aux données.

   Pour plus d'informations sur la configuration d'un volume de destination pour l'accès aux données, reportez-vous à la section "Guide rapide de reprise après incident de volumes ONTAP 9".

3. Supprimez le volume d'origine.

   Pour plus de détails, voir "Gestion des volumes existants".

Déplacement des volumes vers un autre agrégat pour éviter les problèmes de capacité

Vous pouvez déplacer un ou plusieurs volumes vers un autre agrégat pour éviter les problèmes de capacité.

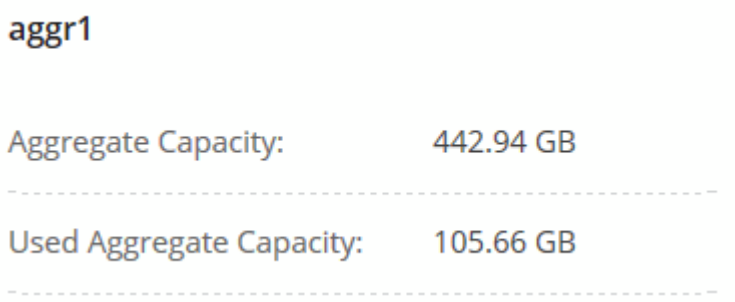
Description de la tâche

Vous pouvez suivre les étapes de cette tâche pour corriger le message Action requise suivant :

```
 Moving two or more volumes is necessary to avoid capacity issues;
however, Cloud Manager cannot perform this action for you.
.Étapes
. Vérifiez si un agrégat existant a la capacité disponible pour les
volumes que vous devez déplacer :
```

+
.. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > allocation avancée**.
.. Sélectionnez chaque agrégat, cliquez sur **Info**, puis affichez la capacité disponible (capacité d'agrégat moins la capacité d'agrégat utilisée).

+



1. Si nécessaire, ajoutez des disques à un agrégat existant :
   a. Sélectionner l'agrégat, puis cliquer sur **Add disks**.
   b. Sélectionnez le nombre de disques à ajouter, puis cliquez sur **Ajouter**.
2. Si aucun agrégat n'a de capacité disponible, créez un nouvel agrégat.

   Pour plus de détails, voir "Création d'agrégats".

3. Utilisez System Manager ou l'interface de ligne de commande pour déplacer les volumes vers l'agrégat.
4. Dans la plupart des cas, vous pouvez utiliser System Manager pour déplacer des volumes.

   Pour obtenir des instructions, reportez-vous au "Guide de migration de volumes ONTAP 9 Express".

Raisons de la lenteur d'un déplacement de volume

Le déplacement d'un volume peut prendre plus de temps que ce que vous attendez si l'une des conditions suivantes est vraie pour Cloud Volumes ONTAP :

- Le volume est un clone.
- Le volume est parent d'un clone.
- L'agrégat source ou de destination dispose d'un seul disque dur (st1) à débit optimisé.
- Le système Cloud Volumes ONTAP est dans AWS et un agrégat utilise une ancienne approche de nommage des objets. Les deux agrégats doivent utiliser le même format de nom.

  Une ancienne méthode de nommage est utilisée si le Tiering des données était activé sur un agrégat dans la version 9.4 ou antérieure.

- Les paramètres de chiffrement ne correspondent pas aux agrégats source et de destination, ou une nouvelle clé est en cours.
- L'option *-Tiering-policy* a été spécifiée sur le déplacement de volumes pour modifier la règle de Tiering.
- L'option *-generate-destination-key* a été spécifiée lors du déplacement du volume.

Tiering des données inactives vers un stockage objet à faible coût

Vous pouvez réduire les coûts de stockage pour Cloud Volumes ONTAP en combinant un Tier de performance SSD ou HDD pour les données actives avec un Tier de capacité de stockage objet pour les données inactives. Pour une vue d'ensemble de haut niveau, voir "Vue d'ensemble du hiérarchisation des données".

Pour configurer le tiering des données, il vous suffit d'effectuer les opérations suivantes :

1 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 >>".

2 Assurez la connectivité entre le Cloud Volumes ONTAP et le stockage objet

- Pour AWS, vous avez besoin d'un terminal VPC vers S3. En savoir plus >>.
- Pour Azure, vous n'aurez rien à faire tant que Cloud Manager dispose des autorisations requises. En savoir plus >>.
- Pour GCP, vous devez configurer le sous-réseau pour Private Google Access et configurer un compte de service. En savoir plus >>.

3 Choisissez une règle de Tiering lors de la création, de la modification ou de la réplication d'un volume

Cloud Manager vous invite à choisir une règle de Tiering lors de la création, de la modification ou de la réplication d'un volume.

- "Hiérarchisation des données sur les volumes en lecture-écriture"
- "Hiérarchisation des données sur les volumes de protection des données"

Quelles sont les’s non requis pour le Tiering des données

- Vous n’avez pas besoin d’installer une licence pour activer le Tiering des données.
- Inutile de créer un Tier de capacité (un compartiment S3, un conteneur Azure Blob ou un compartiment GCP). Cloud Manager le fait pour vous.

Configurations prenant en charge le tiering des données

Vous pouvez activer le tiering des données lors de l’utilisation de configurations et de fonctionnalités spécifiques :

- Le Tiering des données est pris en charge avec Cloud Volumes ONTAP Standard, Premium ou BYOL, à partir des versions suivantes :
  - Version 9.2 dans AWS
  - Version 9.4 dans Azure avec des systèmes à un seul nœud
  - Version 9.6 dans Azure avec paires HA
  - Version 9.6 dans GCP

  Le tiering des données n’est pas pris en charge dans Azure avec le type de machine virtuelle DS3_v2.

- Dans AWS, le niveau de performance peut être des disques SSD à usage général, des disques SSD IOPS provisionnés ou des disques durs optimisés pour le débit.
- Dans Azure, le Tier de performance peut être soit des disques gérés par SSD premium, soit des disques gérés par SSD standard, soit des disques gérés par des disques durs standard.
- Dans GCP, le Tier de performance peut être équipé de disques SSD ou HDD (disques standard).
- Le Tiering des données est pris en charge grâce aux technologies de chiffrement.
- Le provisionnement fin doit être activé sur les volumes.

Conditions requises pour le Tiering des données inactives vers AWS S3

Assurez-vous que Cloud Volumes ONTAP dispose d’une connexion à S3. La meilleure façon de fournir cette connexion est de créer un terminal VPC vers le service S3. Pour obtenir des instructions, reportez-vous à la section "Documentation AWS : création d’un terminal de passerelle".

Lorsque vous créez le terminal VPC, veillez à sélectionner la région, le VPC et la table de routage correspondant à l’instance Cloud Volumes ONTAP. Vous devez également modifier le groupe de sécurité pour ajouter une règle HTTPS sortante qui active le trafic vers le terminal S3. Dans le cas contraire, Cloud Volumes ONTAP ne peut pas se connecter au service S3.

Si vous rencontrez des problèmes, reportez-vous à la section "Centre de connaissances du support AWS : pourquoi ne puis-je pas me connecter à un compartiment S3 à l’aide d’un terminal VPC de passerelle ?".

Il est nécessaire de déplacer les données inactives vers le stockage Azure Blob

Vous n’avez pas besoin de configurer de connexion entre le Tier de performance et le Tier de capacité tant que Cloud Manager dispose des autorisations requises. Cloud Manager active un terminal de service VNet pour vous si la règle Cloud Manager dispose des autorisations suivantes :

```
"Microsoft.Network/virtualNetworks/subnets/write",
"Microsoft.Network/routeTables/join/action",
```

Les autorisations sont incluses dans le dernier "Politique de Cloud Manager".

Il est donc nécessaire de transférer les données inactives vers un compartiment Google Cloud Storage

- Le sous-réseau dans lequel réside Cloud Volumes ONTAP doit être configuré pour un accès privé à Google. Pour obtenir des instructions, reportez-vous à la section "Documentation Google Cloud : configuration de Private Google Access".
- Vous devez disposer d'un compte de service avec le rôle d'administrateur de stockage prédéfini. Vous devez sélectionner ce compte de service lors de la création d'un environnement de travail Cloud Volumes ONTAP.

  "Configurez ce compte de service de Tiering comme suit":

  a. Attribuez le rôle *Storage Admin* prédéfini au compte de service de hiérarchisation.
  b. Ajoutez le compte de service Connector en tant que *Service Account User* au compte de service Tiering.

     Vous pouvez indiquer le rôle d'utilisateur "à l'étape 3 de l'assistant lorsque vous créez le compte de service de tiering", ou "attribuez le rôle après la création du compte de service".

     Lorsque vous créez un environnement de travail Cloud Volumes ONTAP, vous devrez sélectionner le compte de service de Tiering.

  Si vous n'activez pas le Tiering des données et sélectionnez un compte de service lorsque vous créez le système Cloud Volumes ONTAP, vous devrez désactiver le système et ajouter le compte de service à Cloud Volumes ONTAP à partir de la console GCP.

Tiering des données à partir de volumes en lecture/écriture

Cloud Volumes ONTAP peut déplacer les données inactives sur des volumes en lecture/écriture vers un stockage objet économique, libérant ainsi le Tier de performance pour les données actives.

Étapes

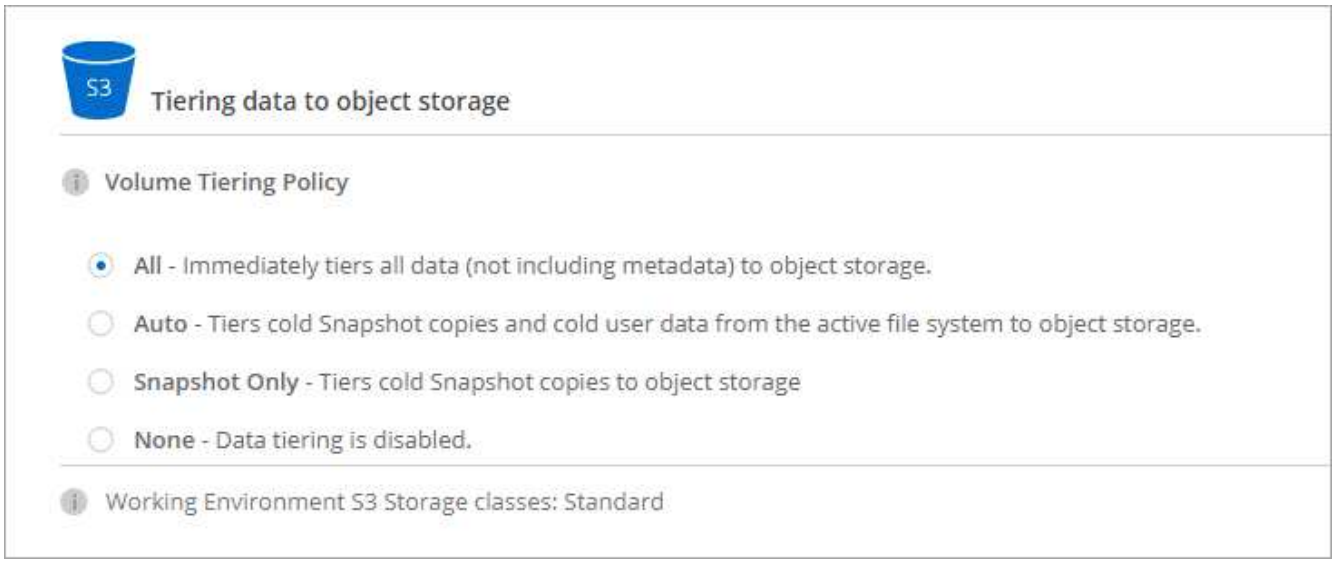
1. Dans l'environnement de travail, créez un nouveau volume ou modifiez le niveau d'un volume existant :

Tâche	Action
Créez un nouveau volume	Cliquez sur **Ajouter nouveau volume**.
Modifier un volume existant	Sélectionnez le volume et cliquez sur **Modifier le type de disque et la stratégie de hiérarchisation**.

2. Sélectionnez une règle de hiérarchisation.

   Pour obtenir une description de ces politiques, reportez-vous à la section "Vue d'ensemble du hiérarchisation des données".

   Exemple



Cloud Manager crée un nouvel agrégat pour le volume si un agrégat compatible avec le hiérarchisation des données n'existe pas déjà.

Si vous préférez créer vous-même des agrégats, vous pouvez activer le tiering des données sur les agrégats lorsque vous les créez.

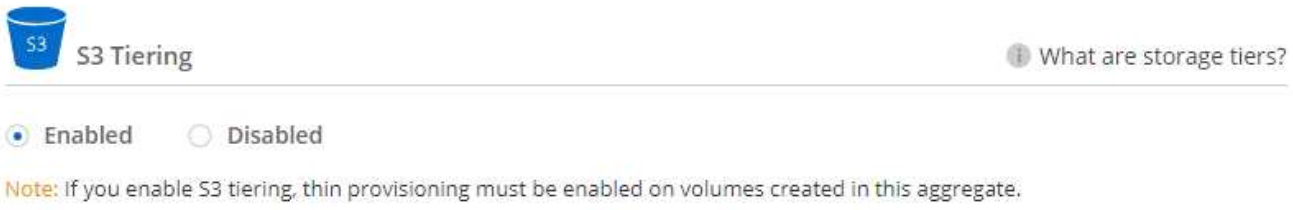
Tiering des données à partir des volumes de protection des données

Cloud Volumes ONTAP permet de hiérarchiser les données d'un volume de protection des données vers un niveau de capacité. Si vous activez le volume de destination, les données passent progressivement au niveau de performance tel qu'il est lu.

Étapes

1. Sur la page Working Environments (Environnements de travail), sélectionnez l'environnement de travail qui contient le volume source, puis faites-le glisser vers l'environnement de travail vers lequel vous souhaitez répliquer le volume.
2. Suivez les invites jusqu'à ce que vous atteigniez la page de hiérarchisation et que vous activiez le tiering des données vers le stockage d'objets.

Exemple



Pour obtenir de l'aide sur la réplication des données, voir "Réplication des données depuis et vers le cloud".

Modification de la classe de stockage pour les données hiérarchisées

Une fois déployé Cloud Volumes ONTAP, vous pouvez réduire les coûts de stockage en modifiant la classe de

stockage pour les données inactives inutilisées depuis 30 jours. Les coûts d'accès sont plus élevés si vous accédez aux données. Vous devez donc prendre en compte ces coûts avant de changer de classe de stockage.

it stockage des données hiérarchisées est disponible dans l'ensemble du système, et non dans chaque volume.

Pour plus d'informations sur les classes de stockage prises en charge, reportez-vous à la section "Vue d'ensemble du hiérarchisation des données".

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **classes de stockage** ou **stockage Blob Storage Tiering**.
2. Choisissez une classe de stockage, puis cliquez sur **Enregistrer**.

Puis-je activer le Tiering des données sur un agrégat existant ?

Non, vous ne pouvez pas activer le Tiering des données sur un agrégat existant. Vous pouvez uniquement activer le Tiering sur les nouveaux agrégats.

Vous pouvez activer le Tiering des données sur un nouvel agrégat "en créant un agrégat vous-même" ou en créant un nouveau volume sur lequel le tiering des données est activé. Cloud Manager crée ensuite un nouvel agrégat pour le volume si un agrégat compatible avec le Tiering des données n'existe pas déjà.

Gestion des machines virtuelles de stockage

Une VM de stockage est une machine virtuelle exécutée dans ONTAP, qui fournit des services de données et de stockage à vos clients. Vous pouvez le connaître comme *SVM* ou *vserver*. La solution Cloud Volumes ONTAP est configurée par défaut avec une seule machine virtuelle de stockage, mais certaines configurations prennent en charge des machines virtuelles de stockage supplémentaires.

Nombre de machines virtuelles de stockage pris en charge

Cloud Volumes ONTAP 9.7 prend en charge plusieurs machines virtuelles de stockage dans AWS avec certaines configurations et une licence d'extension. "Afficher le nombre de machines virtuelles de stockage prises en charge dans AWS". Contactez l'équipe en charge de votre compte pour obtenir une licence d'extension SVM.

Toutes les autres configurations Cloud Volumes ONTAP prennent en charge une VM de stockage servant aux données et une VM de stockage de destination utilisée pour la reprise après incident. Vous pouvez activer la machine virtuelle de stockage de destination pour l'accès aux données en cas de panne sur la machine virtuelle de stockage source.

Une machine virtuelle de stockage s'étend sur l'ensemble du système Cloud Volumes ONTAP (paire haute disponibilité ou nœud unique).

Création de machines virtuelles de stockage supplémentaires

Si votre configuration prend en charge, vous pouvez créer des VM de stockage supplémentaires à l'aide de "System Manager ou l'interface de ligne de commandes".

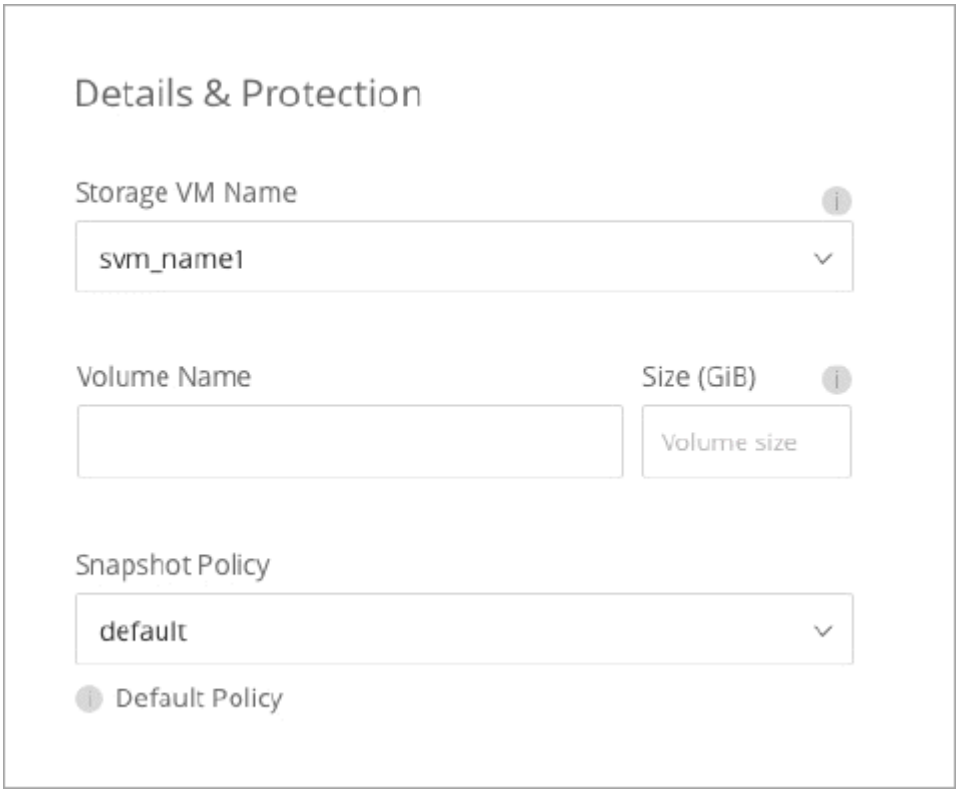
- "Création d'un SVM pour l'accès SMB"

- "Création d'un SVM pour l'accès NFS"
- "Création d'un SVM pour l'accès iSCSI"
- "Création d'un SVM de destination pour la reprise après incident"

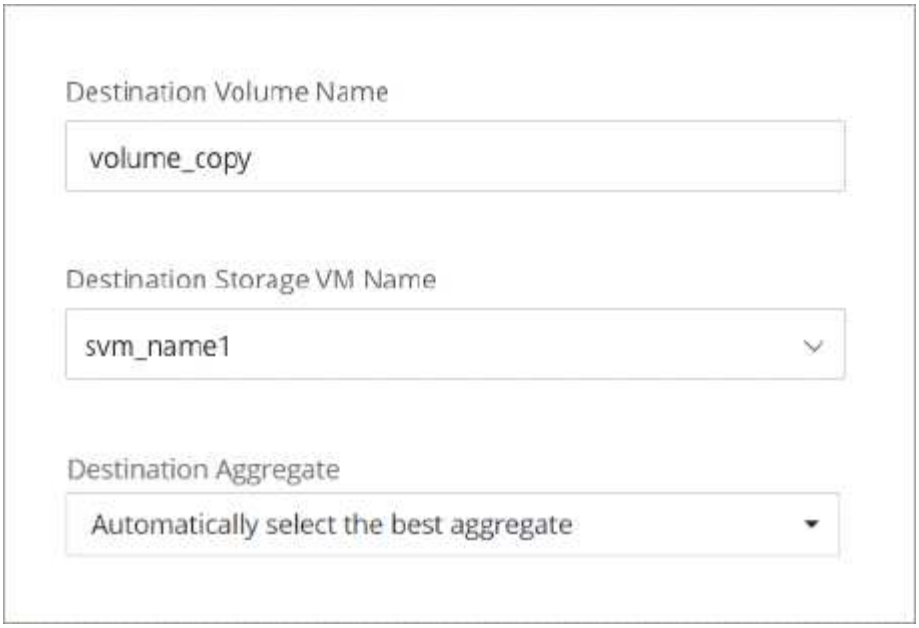
Utilisation de plusieurs VM de stockage dans Cloud Manager

Cloud Manager prend en charge toutes les machines virtuelles de stockage supplémentaires que vous créez à partir de System Manager ou de l'interface de ligne de commandes.

Par exemple, l'image suivante montre comment choisir une VM de stockage lors de la création d'un volume.



L'image suivante montre comment choisir une VM de stockage lors de la réplication d'un volume sur un autre système.



Gestion de la reprise après incident des machines virtuelles de stockage

Cloud Manager ne prend pas en charge la configuration ou l'orchestration pour la reprise d'activité des machines virtuelles de stockage. Vous devez utiliser System Manager ou l'interface de ligne de commandes.

- "Guide de préparation rapide pour la reprise après incident du SVM"
- "Guide de reprise après incident de SVM Express"

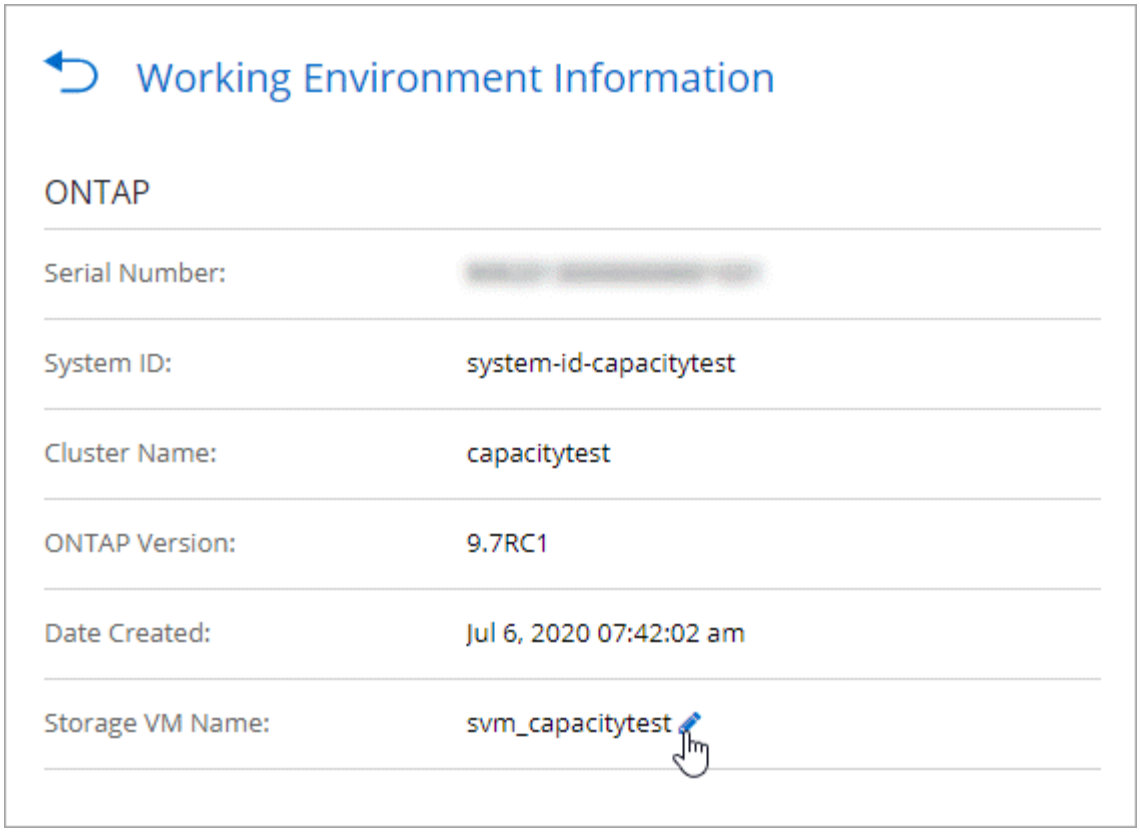
Modification du nom de la machine virtuelle de stockage

Cloud Manager attribue automatiquement la VM de stockage créée pour Cloud Volumes ONTAP. Si vous avez des normes de nommage très strictes, vous pouvez modifier le nom de la machine virtuelle de stockage. Par exemple, vous pouvez indiquer le nom des machines virtuelles de stockage dans vos clusters ONTAP.

Si vous avez créé des machines virtuelles de stockage supplémentaires pour Cloud Volumes ONTAP, vous ne pouvez pas les renommer à partir de Cloud Manager. Pour ce faire, vous devez utiliser System Manager ou l'interface de ligne de commandes directement dans Cloud Volumes ONTAP.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **informations**.
2. Cliquez sur l'icône d'édition située à droite du nom de la VM de stockage.



3. Dans la boîte de dialogue Modifier le nom du SVM, modifiez le nom, puis cliquez sur **Enregistrer**.

Avec Cloud Volumes ONTAP comme stockage persistant pour Kubernetes

Cloud Manager peut automatiser le déploiement de NetApp Trident sur les clusters Kubernetes afin d'utiliser Cloud Volumes ONTAP comme stockage persistant pour les conteneurs.

Trident est un projet open source entièrement pris en charge et géré par NetApp. Trident s'intègre de manière native avec Kubernetes et son framework de volumes persistants pour provisionner et gérer de manière transparente les volumes des systèmes qui exécutent toutes les combinaisons de plateformes de stockage NetApp. "En savoir plus sur Trident".

La fonctionnalité Kubernetes n'est pas prise en charge avec les clusters ONTAP sur site. Elle est prise en charge avec Cloud Volumes ONTAP uniquement.

Démarrage rapide

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

1 Passer en revue les prérequis

Assurez-vous que votre environnement peut répondre aux prérequis, qui inclut la connectivité entre les clusters Kubernetes et Cloud Volumes ONTAP, la connectivité entre les clusters Kubernetes et un connecteur, une version minimale de Kubernetes de 1.14, au moins un nœud worker dans un cluster et plus. Voir la liste

complète.

Ajoutez vos clusters Kubernetes à Cloud Manager

Dans Cloud Manager, cliquez sur **Kubernetes** et découvrez les clusters directement depuis le service géré de votre fournisseur cloud ou importez un cluster en fournissant un fichier kubeconfig.

Connectez vos clusters à Cloud Volumes ONTAP

Après avoir ajouté un cluster Kubernetes, cliquez sur **connexion à l'environnement de travail** pour connecter le cluster à un ou plusieurs systèmes Cloud Volumes ONTAP.

Commencez le provisionnement des volumes persistants

Demandez et gérez les volumes persistants à l'aide d'interfaces et de constructions Kubernetes natives. Cloud Manager crée des classes de stockage NFS et iSCSI que vous pouvez utiliser pour le provisionnement de volumes persistants.

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

Vérification des prérequis

Avant de commencer, assurez-vous que vos clusters Kubernetes et votre connecteur répondent à des exigences spécifiques.

Exigences relatives aux clusters Kubernetes

- La connectivité réseau est requise entre un cluster Kubernetes et le connecteur et entre un cluster Kubernetes et Cloud Volumes ONTAP.

  Le connecteur et Cloud Volumes ONTAP doivent tous deux se connecter au terminal de l'API Kubernetes :

  - Pour les clusters gérés, configurez une route entre le VPC d'un cluster et le VPC où résident le connecteur et le Cloud Volumes ONTAP.
  - Pour les autres clusters, l'adresse IP du nœud maître ou de l'équilibreur de charge (indiquée dans le fichier kubecconfig) doit être accessible par le connecteur et Cloud Volumes ONTAP, et il doit présenter un certificat TLS valide.
- Un cluster Kubernetes peut se trouver sur n'importe quel emplacement qui dispose de la connectivité réseau indiquée ci-dessus.
- Un cluster Kubernetes doit exécuter la version 1.14 au moins.

  La version maximale prise en charge est définie par Trident. "Cliquez ici pour voir la version Kubernetes maximale prise en charge".
- Un cluster Kubernetes doit disposer d'au moins un nœud worker.
- Pour les clusters exécutés dans Amazon Elastic Kubernetes Service (Amazon EKS), chaque cluster a besoin d'un rôle IAM ajouté afin de résoudre une erreur d'autorisation. Une fois le cluster ajouté, Cloud Manager vous invite à utiliser la commande eksctl exacte qui résout l'erreur.

"En savoir plus sur les limites des autorisations IAM".

- Pour les clusters exécutés dans Azure Kubernetes Service (AKS), ces clusters doivent avoir le rôle *Azure Kubernetes Service RBAC Cluster Admin*. Ceci est nécessaire afin que Cloud Manager puisse installer Trident et configurer des classes de stockage sur le cluster.
- Pour les clusters exécutés dans Google Kubernetes Engine (GKE), ces clusters ne doivent pas utiliser le système d'exploitation optimisé par défaut pour les conteneurs. Vous devez les changer pour utiliser Ubuntu.

  GKE utilise par défaut Google "image optimisée pour les conteneurs", Qui ne dispose pas des utilitaires dont Trident a besoin pour monter des volumes.

Exigences relatives au connecteur

Assurez-vous que la mise en réseau et les autorisations suivantes sont en place pour le connecteur.

Mise en réseau

- Lors de l'installation de Trident, le connecteur doit disposer d'une connexion Internet sortante pour accéder aux terminaux suivants :

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

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

Autorisations requises pour détecter et gérer les clusters EKS

Pour détecter et gérer les clusters Kubernetes exécutés dans Amazon Elastic Kubernetes Service (EKS), le connecteur a besoin d'autorisations d'administration :

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "eks:*",
            "Resource": "*"
        }
    ]
}
```

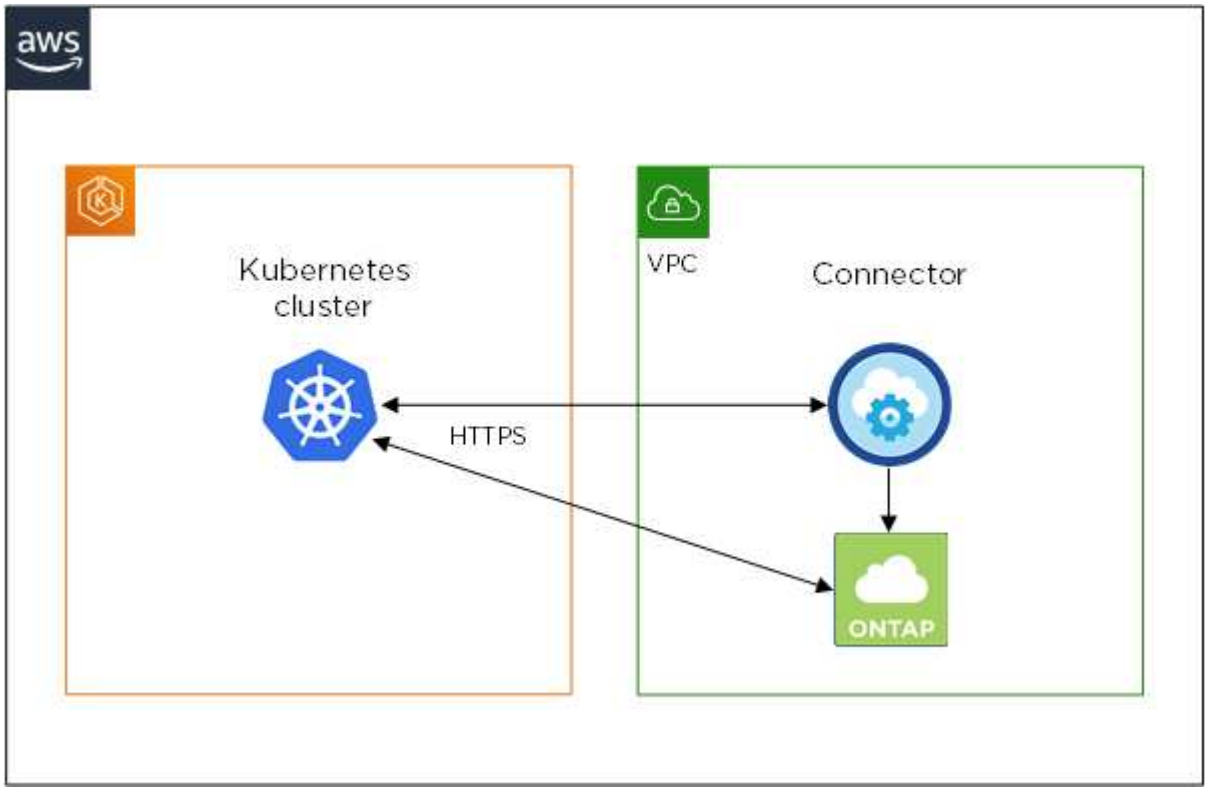
Autorisations requises pour détecter et gérer les clusters GKE

Le connecteur a besoin des autorisations suivantes pour détecter et gérer les clusters Kubernetes exécutés dans Google Kubernetes Engine (GKE) :

```
container.*
```

Exemple de configuration

L'image suivante montre un exemple de cluster Kubernetes exécuté dans Amazon Elastic Kubernetes Service (Amazon EKS) et ses connexions au connecteur et à Cloud Volumes ONTAP.



Ajout des clusters Kubernetes

Ajoutez des clusters Kubernetes à Cloud Manager en découvrant les clusters exécutés dans le service Kubernetes géré de votre fournisseur cloud ou en important le fichier kubeconfig d'un cluster.

Étapes

1. En haut de Cloud Manager, cliquez sur **Kubernetes**.
2. Cliquez sur **Ajouter un cluster**.
3. Choisissez l'une des options disponibles :
   - Cliquez sur **découvrir les clusters** pour découvrir les clusters gérés auxquels Cloud Manager a accès en fonction des autorisations que vous avez fournies au connecteur.

     Par exemple, si votre connecteur est exécuté dans Google Cloud, Cloud Manager utilise les autorisations du compte de service du connecteur pour détecter les clusters exécutés dans Google Kubernetes Engine (GKE).

   - Cliquez sur **Import Cluster** pour importer un cluster à l'aide d'un fichier kubeconfig.

     Une fois le fichier téléchargé, Cloud Manager vérifie la connexion au cluster et enregistre une copie chiffrée du fichier kubeconfig.

Résultat

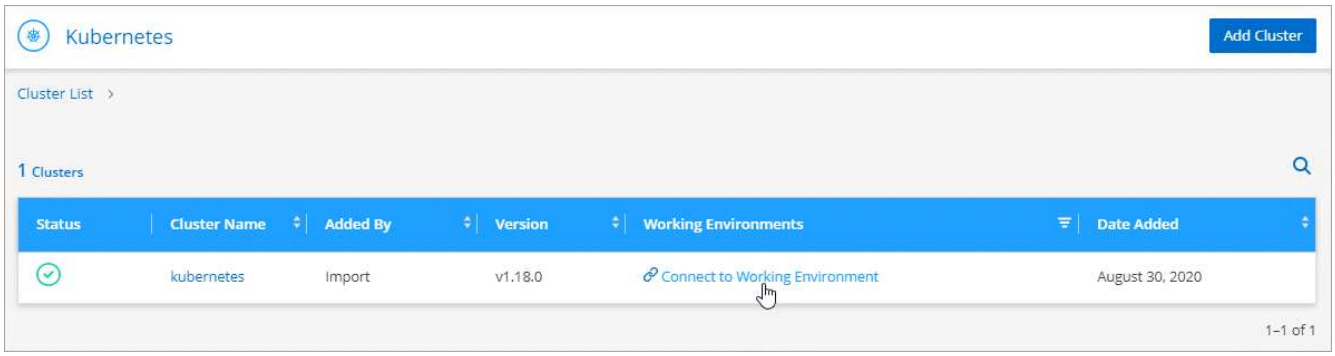
Cloud Manager ajoute le cluster Kubernetes. Vous pouvez désormais connecter le cluster à Cloud Volumes ONTAP.

Connexion d'un cluster à Cloud Volumes ONTAP

Connectez un cluster Kubernetes à Cloud Volumes ONTAP afin d'utiliser Cloud Volumes ONTAP comme stockage persistant pour les conteneurs.

Étapes

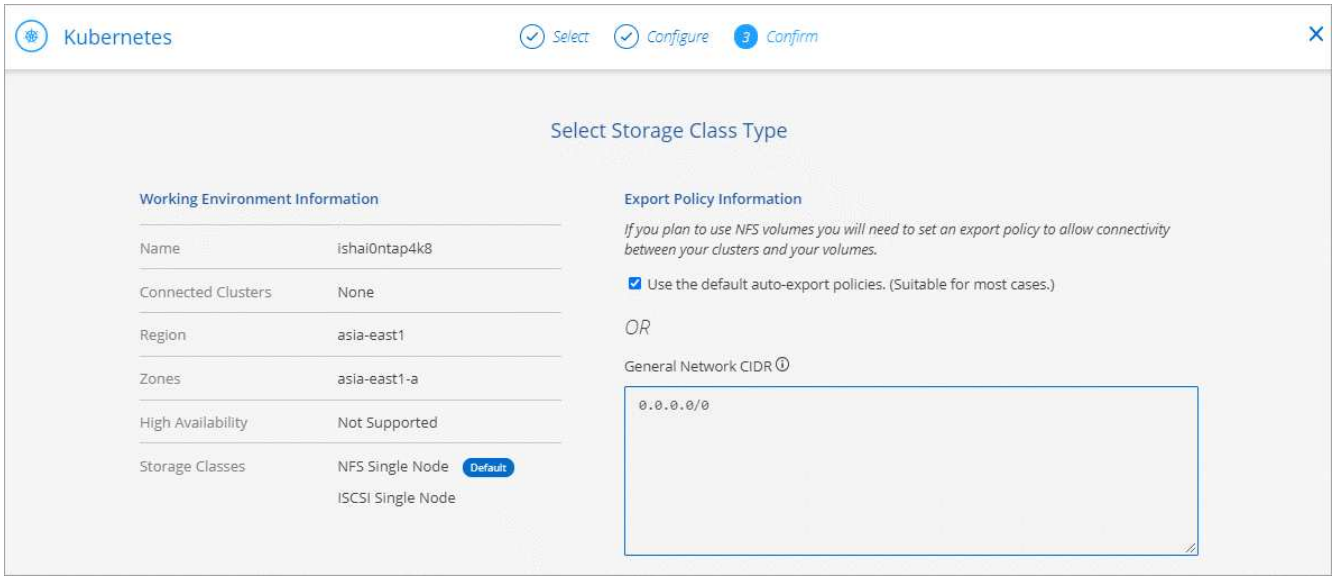
1. En haut de Cloud Manager, cliquez sur **Kubernetes**.
2. Cliquez sur **connexion à l'environnement de travail** pour le cluster que vous venez d'ajouter.



3. Sélectionnez un environnement de travail et cliquez sur **Continuer**.
4. Sélectionnez la classe de stockage NetApp à utiliser comme classe de stockage par défaut pour le cluster Kubernetes, puis cliquez sur **Continuer**.

   Lorsqu'un utilisateur crée un volume persistant, le cluster Kubernetes peut utiliser cette classe de stockage comme stockage back-end par défaut.

5. Choisissez d'utiliser les règles d'exportation automatique par défaut ou d'ajouter un bloc CIDR personnalisé.



6. Cliquez sur **Ajouter un environnement de travail**.

Résultat

Cloud Manager connecte l'environnement de travail au cluster, qui peut prendre jusqu'à 15 minutes.

Gestion des clusters

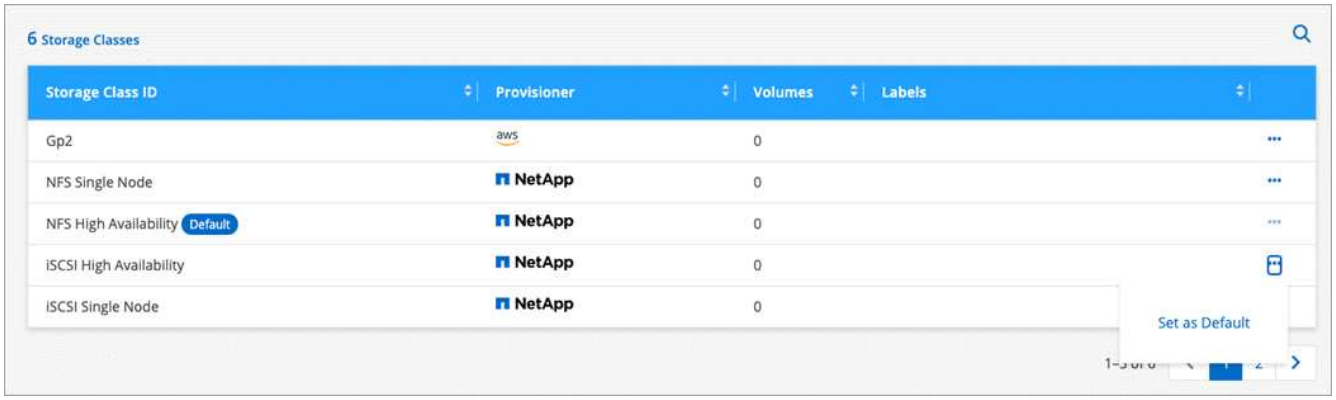
Cloud Manager vous permet de gérer vos clusters Kubernetes en modifiant la classe de stockage par défaut, en mettant à niveau Trident, etc.

Modification de la classe de stockage par défaut

Assurez-vous d'avoir défini une classe de stockage Cloud Volumes ONTAP comme classe de stockage par défaut, de sorte que les clusters utilisent Cloud Volumes ONTAP comme système de stockage back-end.

Étapes

1. En haut de Cloud Manager, cliquez sur **Kubernetes**.
2. Cliquez sur le nom du cluster Kubernetes.
3. Dans le tableau **classes de stockage**, cliquez sur le menu actions à l'extrême droite de la classe de stockage que vous souhaitez définir comme valeur par défaut.



4. Cliquez sur **définir comme valeur par défaut**.

Mise à niveau de Trident

Vous pouvez mettre à niveau Trident depuis Cloud Manager lorsqu'une nouvelle version de Trident est disponible.

Étapes

1. En haut de Cloud Manager, cliquez sur **Kubernetes**.
2. Cliquez sur le nom du cluster Kubernetes.
3. Si une nouvelle version est disponible, cliquez sur **Upgrade** en regard de la version de Trident.

Mise à jour du fichier kubeconfig

Si vous avez ajouté votre cluster à Cloud Manager en important le fichier kubeconfig, vous pouvez télécharger le dernier fichier kubeconfig vers Cloud Manager à tout moment. Vous pouvez le faire si vous avez mis à jour les identifiants, si vous avez modifié des utilisateurs ou des rôles, ou si un changement affecte le cluster, l'utilisateur, l'espace de noms ou l'authentification.

Étapes

1. En haut de Cloud Manager, cliquez sur **Kubernetes**.
2. Cliquez sur le nom du cluster Kubernetes.
3. Cliquez sur **mettre à jour Kubeconfig**.
4. Lorsque vous y êtes invité par l'intermédiaire de votre navigateur Web, sélectionnez le fichier mis à jour kubeconfig et cliquez sur **Ouvrir**.

Résultat

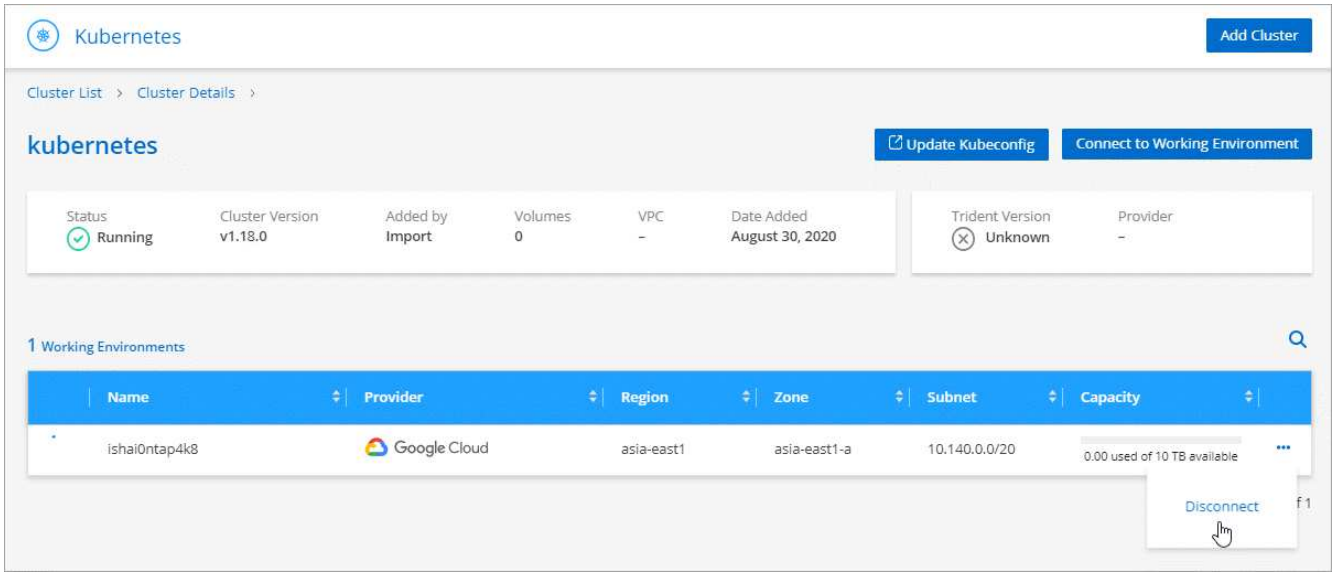
Cloud Manager met à jour des informations concernant le cluster Kubernetes d'après le dernier fichier kubeconfig.

Déconnexion d'un cluster

Lorsque vous déconnectez un cluster de Cloud Volumes ONTAP, vous ne pouvez plus utiliser ce système Cloud Volumes ONTAP comme stockage persistant pour les conteneurs. Les volumes persistants existants ne sont pas supprimés.

Étapes

1. En haut de Cloud Manager, cliquez sur **Kubernetes**.
2. Cliquez sur le nom du cluster Kubernetes.
3. Dans le tableau **environnements de travail**, cliquez sur le menu actions à l'extrême droite de l'environnement de travail que vous souhaitez déconnecter.



4. Cliquez sur **déconnecter**.

Résultat

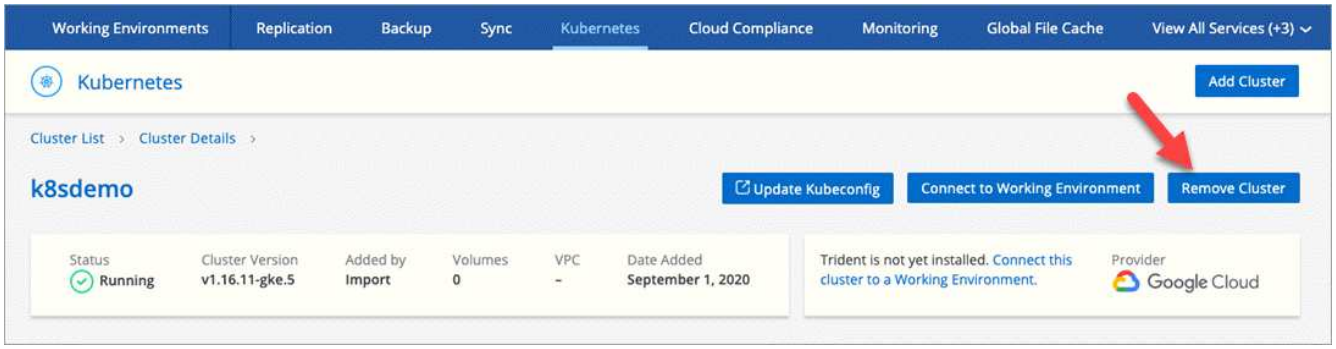
Cloud Manager déconnecte le cluster du système Cloud Volumes ONTAP.

Suppression d'un cluster

Retirez les clusters désaffectés de Cloud Manager après avoir déconnecté tous les environnements de travail du cluster.

Étapes

1. En haut de Cloud Manager, cliquez sur **Kubernetes**.
2. Cliquez sur le nom du cluster Kubernetes.
3. Cliquez sur **Supprimer le cluster**.



Cryptage de volumes grâce aux solutions de cryptage NetApp

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

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

Cloud Volumes ONTAP ne prend pas en charge la gestion intégrée des clés.

Ce dont vous avez besoin

Votre système Cloud Volumes ONTAP doit être enregistré auprès du support NetApp. Depuis la version Cloud Manager 3.7.1, une licence NetApp Volume Encryption est automatiquement installée sur chaque système Cloud Volumes ONTAP enregistré auprès du support NetApp.

- "Ajout de comptes du site de support NetApp à Cloud Manager"
- "Enregistrement des systèmes de paiement à l'utilisation"

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

Étapes

1. Consultez la liste des gestionnaires de clés pris en charge dans le "Matrice d'interopérabilité NetApp".

   Recherchez la solution **gestionnaires de clés**.

2. "Connectez-vous à l'interface de ligne de commandes de Cloud Volumes ONTAP".
3. Installez les certificats SSL et connectez-vous aux serveurs de gestion des clés externes.

   "Guide d'alimentation du cryptage ONTAP 9 NetApp : configuration de la gestion externe des clés"

Réplication des données entre les systèmes

Vous pouvez répliquer des données entre des environnements de travail en choisissant une réplication de données unique pour le transfert de données, ou un planning récurrent pour la reprise sur incident ou la conservation à long terme. Par exemple, vous pouvez configurer la réplication des données depuis un système ONTAP sur site vers Cloud Volumes ONTAP pour la reprise après incident.

Cloud Manager simplifie la réplication des données entre les volumes sur des systèmes distincts à l'aide des technologies SnapMirror et SnapVault. Il vous suffit d'identifier le volume source et le volume de destination, puis de choisir une stratégie et un planning de réplication. Cloud Manager achète les disques requis, configure les relations, applique la stratégie de réplication, puis lance le transfert de base entre les volumes.

Le transfert de base inclut une copie complète des données source. Les transferts ultérieurs contiennent des copies différentielles des données source.

Cloud Manager permet la réplication des données entre différents types d'environnements de travail :

- D'un système Cloud Volumes ONTAP à un autre système Cloud Volumes ONTAP
- Entre un système Cloud Volumes ONTAP et un cluster ONTAP sur site
- D'un cluster ONTAP sur site vers un autre cluster ONTAP sur site

Exigences de réplication des données

Avant de pouvoir répliquer des données, vous devez confirmer que des exigences spécifiques sont respectées pour les systèmes Cloud Volumes ONTAP et les clusters ONTAP.

Exigences de version

Vérifiez que les volumes source et de destination exécutent des versions ONTAP compatibles avant de répliquer les données. Pour plus d'informations, reportez-vous à la "Guide d'alimentation de la protection des données".

Exigences spécifiques à Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'ICMP et les ports 11104 et 11105.

  Ces règles sont incluses dans le groupe de sécurité prédéfini.

- Pour répliquer des données entre deux systèmes Cloud Volumes ONTAP dans différents sous-réseaux, les sous-réseaux doivent être routés ensemble (paramètre par défaut).
- Pour répliquer des données entre un système Cloud Volumes ONTAP dans AWS et un système dans Azure, vous devez disposer d'une connexion VPN entre AWS VPC et Azure VNet.

Exigences spécifiques aux clusters ONTAP

- Une licence SnapMirror active doit être installée.
- Si le cluster se trouve sur votre site, vous devez disposer d'une connexion entre votre réseau d'entreprise et AWS ou Azure, qui est généralement une connexion VPN.
- Les clusters ONTAP doivent répondre à des exigences supplémentaires en termes de sous-réseau, de port, de pare-feu et de cluster.

  Pour plus d'informations, reportez-vous au Cluster and SVM Peering Express Guide de votre version d'ONTAP.

Configuration de la réplication des données entre les systèmes

Vous pouvez répliquer des données entre les systèmes Cloud Volumes ONTAP et les clusters ONTAP en choisissant une réplication de données unique, qui peut vous aider à déplacer des données vers et depuis le cloud, ou un planning récurrent, qui peut vous aider à la reprise sur incident ou à la conservation à long terme.

Description de la tâche

Cloud Manager prend en charge des configurations de protection des données simples, en panne et en cascade :

- Dans une configuration simple, la réplication s'effectue du volume A au volume B.
- Dans une configuration en panne, la réplication se produit du volume A vers plusieurs destinations.
- Dans une configuration en cascade, la réplication s'effectue du volume A au volume B et du volume B au volume C.

Vous pouvez configurer les configurations en cascade et en panne dans Cloud Manager en configurant plusieurs réplications de données entre les systèmes. Par exemple, en répliquant un volume du système A vers le système B, puis en répliquant le même volume du système B vers le système C.

Étapes

1. Sur la page Working Environments (Environnements de travail), sélectionnez l'environnement de travail qui contient le volume source, puis faites-le glisser vers l'environnement de travail vers lequel vous souhaitez répliquer le volume :

2. Si les pages Configuration de la mise en valeur de la source et de la destination s'affichent, sélectionnez tous les LIF intercluster pour la relation d'homologues du cluster.

   Le réseau intercluster doit être configuré de sorte que les pairs de cluster disposent d'une connectivité « full-mesh » au niveau des paires, ce qui signifie que chaque paire de clusters d'une relation cluster peer-to-peer dispose d'une connectivité parmi l'ensemble de leurs LIFs intercluster.

Ces pages s'affichent si un cluster ONTAP disposant de plusieurs LIF est la source ou la destination.

3. Sur la page Sélection du volume source, sélectionnez le volume que vous souhaitez répliquer.
4. Sur la page Nom du volume de destination et Tiering, spécifiez le nom du volume de destination, choisissez un type de disque sous-jacent, modifiez l'une des options avancées, puis cliquez sur **Continuer**.

   Si la destination est un cluster ONTAP, vous devez également spécifier le SVM de destination et l'agrégat.

5. Sur la page Taux de transfert maximal, spécifiez le débit maximal (en mégaoctets par seconde) auquel les données peuvent être transférées.
6. Sur la page Stratégie de réplication, choisissez l'une des stratégies par défaut ou cliquez sur **stratégies supplémentaires**, puis sélectionnez l'une des stratégies avancées.

   Pour obtenir de l'aide, voir "Choix d'une stratégie de réplication".

   Si vous choisissez une stratégie de sauvegarde personnalisée (SnapVault), les étiquettes associées à la stratégie doivent correspondre aux étiquettes des copies Snapshot sur le volume source. Pour plus d'informations, voir "Fonctionnement des stratégies de sauvegarde".

7. Sur la page Programmation, choisissez une copie unique ou un planning récurrent.

   Plusieurs plannings par défaut sont disponibles. Si vous souhaitez un autre planning, vous devez créer une nouvelle planification sur le cluster *destination* à l'aide de System Manager.

8. Sur la page Revue, vérifiez vos sélections, puis cliquez sur **Go**.

Résultat

Cloud Manager démarre le processus de réplication des données. Vous pouvez afficher des informations détaillées sur la réplication dans la page Etat de la réplication.

Gestion des planifications et des relations de réplication des données

Après avoir configuré la réplication des données entre deux systèmes, vous pouvez gérer le planning et la relation de réplication des données à partir de Cloud Manager.

Étapes

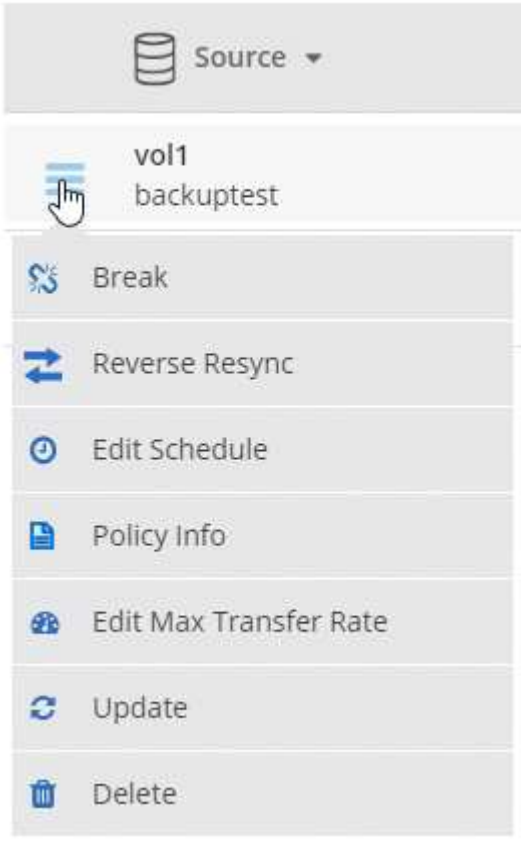
1. Sur la page environnements de travail, affichez l'état de réplication de tous les environnements de travail de l'espace de travail ou d'un environnement de travail spécifique :

Option	Action
Tous les environnements de travail de l'espace de travail	En haut de Cloud Manager, cliquez sur **Replication**.
Un environnement de travail spécifique	Ouvrez l'environnement de travail et cliquez sur **réplications**.

2. Vérifiez l'état des relations de réplication des données pour vérifier qu'elles sont en bon état.

Si l'état d'une relation est inactif et que l'état Miroir n'est pas initialisé, vous devez initialiser la relation à partir du système de destination pour que la réplication des données se produise selon le planning défini. Vous pouvez initialiser la relation à l'aide de System Manager ou de l'interface de ligne de commande (CLI). Ces états peuvent apparaître en cas de défaillance du système de destination, puis revenir en ligne.

3. Sélectionnez l'icône de menu située en regard du volume source, puis choisissez l'une des actions disponibles.



Le tableau suivant décrit les actions disponibles :

Action	Description
Pause	Rompt la relation entre les volumes source et de destination et active le volume de destination pour l'accès aux données. Cette option est généralement utilisée lorsque le volume source ne peut pas servir de données en raison d'événements tels que la corruption des données, la suppression accidentelle ou un état hors ligne. Pour plus d'informations sur la configuration d'un volume de destination pour l'accès aux données et la réactivation d'un volume source, reportez-vous au Guide ONTAP 9 Volume Disaster Recovery Express Guide.

Action	Description
Resynchroniser	Rétablit une relation interrompue entre les volumes et reprend la réplication des données selon le planning défini. Lorsque vous resynchronisez les volumes, le contenu du volume de destination est remplacé par le contenu du volume source. Pour effectuer une resynchronisation inverse, qui resynchronise les données du volume de destination vers le volume source, consultez la "Guide rapide de reprise après incident de volumes ONTAP 9".
Resynchronisation inverse	Inverse les rôles des volumes source et de destination. Le contenu du volume source d'origine est remplacé par le contenu du volume de destination. Ceci est utile lorsque vous souhaitez réactiver un volume source hors ligne. Toutes les données écrites sur le volume source d'origine entre la dernière réplication de données et l'heure à laquelle le volume source a été désactivé ne sont pas conservées.
Modifier le planning	Vous permet de choisir un planning différent pour la réplication des données.
Informations sur les règles	Affiche la stratégie de protection attribuée à la relation de réplication des données.
Modifier le taux de transfert maximal	Permet de modifier le taux maximal (en kilo-octets par seconde) auquel les données peuvent être transférées.
Mise à jour	Lance un transfert incrémentiel pour mettre à jour le volume de destination.
Supprimer	Supprime la relation de protection des données entre les volumes source et de destination, ce qui signifie que la réplication des données n'a plus lieu entre les volumes. Cette action n'active pas le volume de destination pour l'accès aux données. Cette action supprime également la relation d'homologues de cluster et la relation d'homologues de la machine virtuelle de stockage (SVM), si aucune autre relation de protection des données n'existe entre les systèmes.

Résultat

Après avoir sélectionné une action, Cloud Manager met à jour la relation ou le planning.

Choix d'une stratégie de réplication

Vous aurez peut-être besoin d'aide pour choisir une règle de réplication lorsque vous configurez la réplication des données dans Cloud Manager. Une stratégie de réplication définit la manière dont le système de stockage réplique les données d'un volume source vers un volume de destination.

Quelles sont les règles de réplication

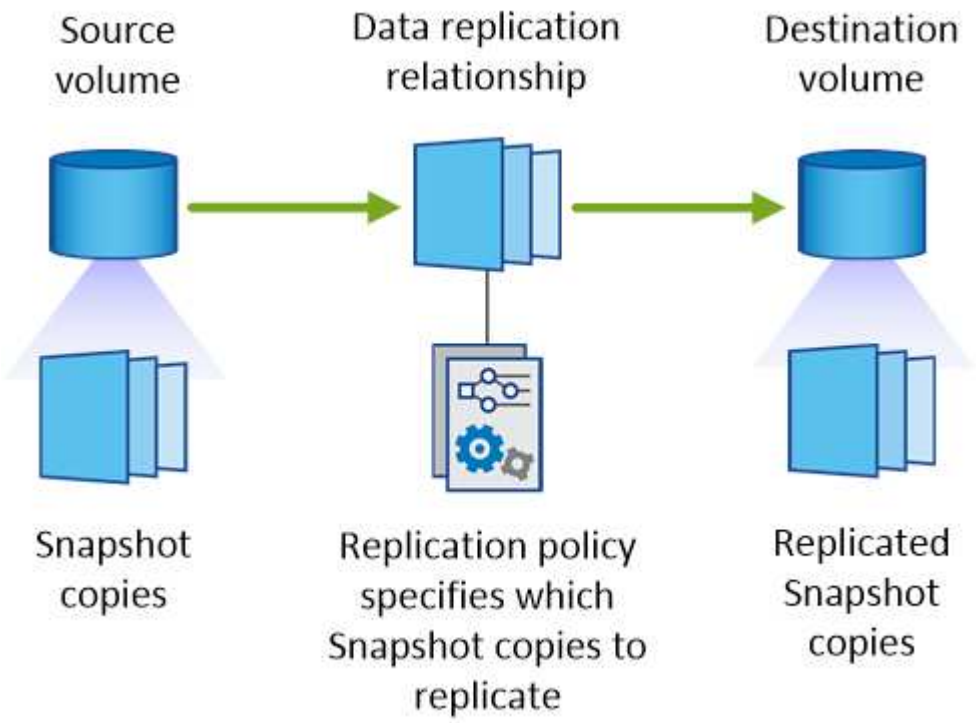
Le système d'exploitation ONTAP crée automatiquement des sauvegardes appelées copies Snapshot. Une copie Snapshot est une image en lecture seule d'un volume qui capture l'état du système de fichiers à un moment donné.

Lorsque vous répliquez des données entre des systèmes, vous répliquez des copies Snapshot d'un volume source vers un volume de destination. Une stratégie de réplication spécifie les copies Snapshot à répliquer du

volume source vers le volume de destination.

Les règles de réplication sont également appelées « stratégies de protection_ car elles sont optimisées par les technologies SnapMirror et SnapVault, qui assurent la protection de la reprise après incident ainsi que la sauvegarde et la restauration disque à disque.

L'image suivante montre la relation entre les copies Snapshot et les règles de réplication :



Types de règles de réplication

Il existe trois types de règles de réplication :

- Une règle *Mirror* réplique les copies Snapshot nouvellement créées vers un volume de destination.

  Vous pouvez utiliser ces copies Snapshot pour protéger le volume source en vue de la reprise après incident ou de la réplication de données unique. Vous pouvez activer le volume de destination pour l'accès aux données à tout moment.

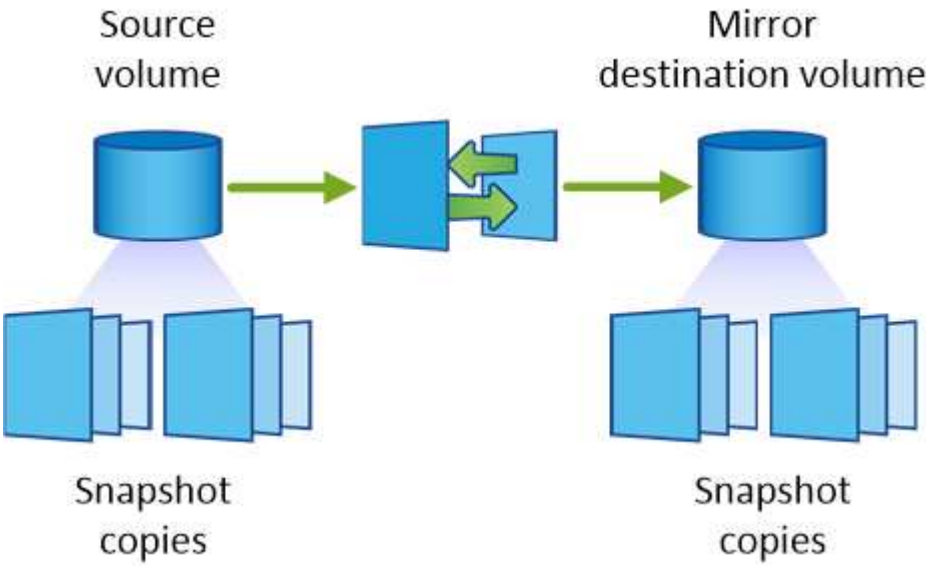
- Une règle *Backup* réplique des copies Snapshot spécifiques sur un volume de destination et les conserve généralement pendant une période plus longue que sur le volume source.

  Vous pouvez restaurer des données à partir de ces copies Snapshot lorsque les données sont corrompues ou perdues, et les conserver à des fins de conformité aux normes et à d'autres fins liées à la gouvernance.

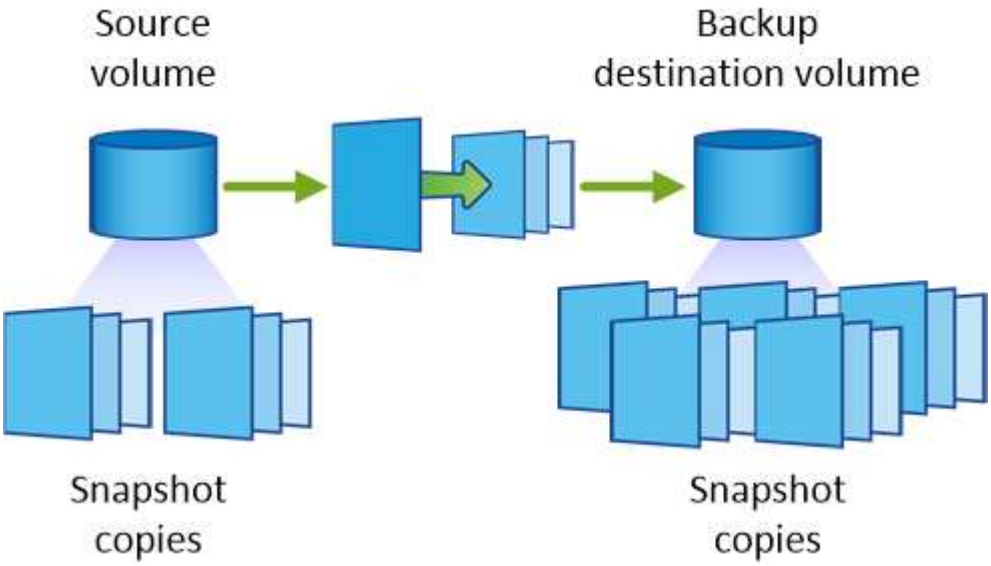
- Une politique *Mirror et Backup* permet la reprise sur incident et la conservation à long terme.

  Chaque système inclut une stratégie de mise en miroir et de sauvegarde par défaut, qui fonctionne bien dans de nombreuses situations. Si vous avez besoin de règles personnalisées, vous pouvez créer vos propres règles à l'aide de System Manager.

Les images suivantes montrent la différence entre les stratégies Miroir et Sauvegarde. Une stratégie Miroir reflète les copies Snapshot disponibles sur le volume source.



Une stratégie de sauvegarde conserve généralement les copies Snapshot plus longtemps qu'elles ne sont conservées sur le volume source :



Fonctionnement des stratégies de sauvegarde

Contrairement aux stratégies Mirror, les stratégies de sauvegarde (SnapVault) répliquent des copies Snapshot spécifiques vers un volume de destination. Il est important de comprendre le fonctionnement des stratégies de sauvegarde si vous souhaitez utiliser vos propres règles au lieu des règles par défaut.

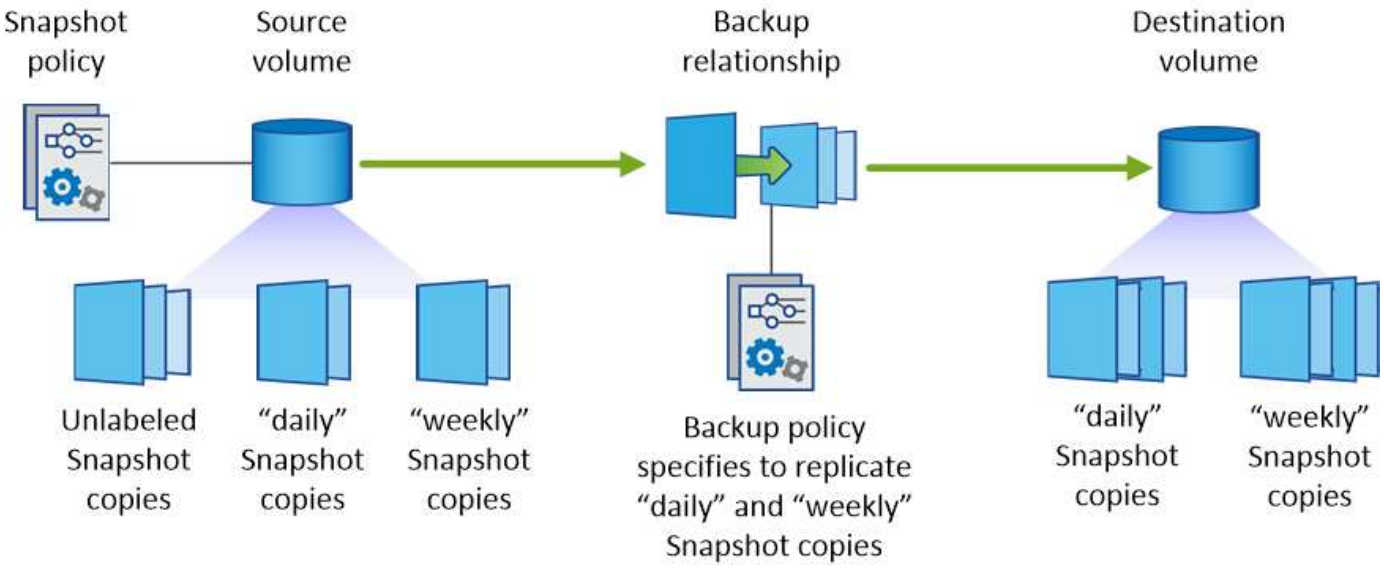
Comprendre la relation entre les étiquettes de copie Snapshot et les stratégies de sauvegarde

Une stratégie Snapshot définit la façon dont le système crée des copies Snapshot de volumes. La stratégie indique quand créer les copies Snapshot, le nombre de copies à conserver et comment les étiqueter. Par exemple, un système peut créer une copie Snapshot tous les jours à 12 h 10, conserver les deux copies les plus récentes et les étiqueter " quotidiennement ".

Une stratégie de sauvegarde inclut des règles qui spécifient les copies Snapshot à répliquer sur un volume de destination et le nombre de copies à conserver. Les étiquettes définies dans une stratégie de sauvegarde doivent correspondre à une ou plusieurs étiquettes définies dans une stratégie Snapshot. Dans le cas

contraire, le système ne peut pas répliquer de copies Snapshot.

Par exemple, une stratégie de sauvegarde qui inclut les étiquettes " quotidiennes " et " hebdomadaires " entraîne la réplication des copies Snapshot qui n'incluent que ces étiquettes. Aucune autre copie Snapshot n'est répliquée, comme illustré dans l'image suivante :



Règles par défaut et règles personnalisées

La stratégie Snapshot par défaut crée des copies Snapshot toutes les heures, quotidiennes et hebdomadaires, conservant six copies Snapshot toutes les heures, deux copies quotidiennes et deux copies Snapshot hebdomadaires.

Vous pouvez facilement utiliser une stratégie de sauvegarde par défaut avec la stratégie Snapshot par défaut. Les règles de sauvegarde par défaut répliquent les copies Snapshot quotidiennes et hebdomadaires, en conservant sept copies Snapshot quotidiennes et 52 copies Snapshot hebdomadaires.

Si vous créez des règles personnalisées, les étiquettes définies par ces règles doivent correspondre. Vous pouvez créer des règles personnalisées à l'aide de System Manager.

Réplication des données de NetApp HCI vers Cloud Volumes ONTAP

Si vous essayez de répliquer des données de NetApp HCI vers Cloud Volumes ONTAP, vous pouvez le faire sur un système NetApp HCI exécutant le logiciel NetApp Element à l'aide de SnapMirror. Vous pouvez également répliquer les données sur des volumes créés sur un système ONTAP Select, qui s'exécute en tant qu'invité virtuel dans une solution NetApp HCI vers Cloud Volumes ONTAP.

Pour plus d'informations, reportez-vous aux rapports techniques suivants :

- "Rapport technique 4641 : protection des données NetApp HCI"
- "Rapport technique 4651 : architecture et configuration de NetApp SolidFire SnapMirror"

Contrôle des performances

Découvrez le service surveillance

En exploitant la "Service NetApp Cloud Insights", Cloud Manager vous donne des informations sur l'état et les performances de vos instances Cloud Volumes ONTAP et vous aide à dépanner et à optimiser les performances de votre environnement de stockage cloud.

Caractéristiques

- Surveillance automatique de tous les volumes
- Affichez les données de performances de volumes en termes d'IOPS, de débit et de latence
- Identifiez les problèmes de performances pour minimiser l'impact sur vos utilisateurs et vos applications

Fournisseurs cloud pris en charge

Le service de contrôle est pris en charge par Cloud Volumes ONTAP pour AWS.

Le coût

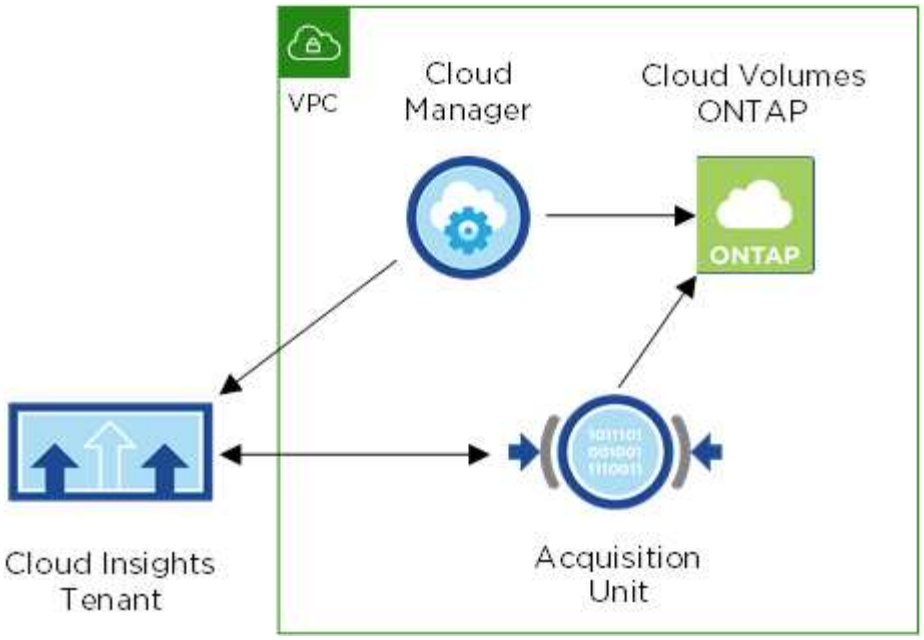
La surveillance est actuellement disponible sous forme d'aperçu. L'activation est gratuite, mais Cloud Manager lance une machine virtuelle dans votre VPC pour faciliter le contrôle. Cette machine virtuelle entraîne des frais supplémentaires de la part de votre fournisseur cloud.

Fonctionnement de Cloud Insights avec Cloud Manager

À un niveau élevé, l'intégration d'Cloud Insights avec Cloud Manager fonctionne comme suit :

1. Vous activez le service de surveillance sur Cloud Volumes ONTAP.
2. Cloud Manager configure votre environnement. Il effectue les opérations suivantes :
    a. Crée un locataire Cloud Insights (également appelé *environnement*) et associe tous les utilisateurs de votre compte Cloud Central au locataire.
    b. Offre une version d'essai gratuite de 30 jours d'Cloud Insights.
    c. Déploie une machine virtuelle dans votre VPC appelé unité d'acquisition, ce qui facilite la surveillance des volumes (il s'agit de la machine virtuelle mentionnée dans la section de coût ci-dessus).
    d. Connecte l'unité d'acquisition à Cloud Volumes ONTAP et au locataire Cloud Insights.
3. Dans Cloud Manager, vous cliquez sur surveillance et utilisez les données de performance pour résoudre les problèmes et optimiser les performances.

L'image suivante montre la relation entre ces composants :



L'unité d'acquisition

Lorsque vous activez surveillance, Cloud Manager déploie une unité d'acquisition dans le même sous-réseau que le connecteur.

Une *unité d'acquisition* collecte les données de performances de Cloud Volumes ONTAP et les envoie au locataire Cloud Insights. Cloud Manager interroge ensuite les données et les présente à votre place.

Notez ce qui suit à propos de l'instance d'unité d'acquisition :

- L'unité d'acquisition fonctionne sur une instance t3.XLarge avec un volume GP2 de 100 Go.
- L'instance s'appelle *AcquisitionUnit* avec un hachage (UUID) généré concaténé. Par exemple : *AcquisitionUnit-FAN7FqeH*
- Une seule unité d'acquisition est déployée par connecteur.
- L'instance doit être en cours d'exécution pour accéder aux informations de performances dans l'onglet surveillance.

Locataire Cloud Insights

Cloud Manager configure un *tenant* lorsque vous activez la surveillance. Un locataire Cloud Insights vous permet d'accéder aux données de performance collectées par l'unité d'acquisition. Le locataire est une partition de données sécurisée au sein du service NetApp Cloud Insights.

Interface Web de Cloud Insights

L'onglet Monitoring de Cloud Manager fournit des données de performance de base pour vos volumes. Vous pouvez accéder à l'interface Web de Cloud Insights depuis votre navigateur pour effectuer un contrôle plus approfondi et configurer des alertes pour vos systèmes Cloud Volumes ONTAP.

Essai gratuit et abonnement

Cloud Manager propose une version d'évaluation gratuite de 30 jours de Cloud Insights. Elle vous permet de fournir des données de performances dans Cloud Manager et d'explorer les fonctionnalités proposées par Cloud Insights Standard Edition.

Vous devez vous abonner d'ici la fin de la période d'essai gratuite ; sinon, votre locataire Cloud Insights finira par être supprimé. Vous pouvez vous abonner à l'édition Basic, Standard ou Premium pour continuer à utiliser la fonctionnalité Monitoring dans Cloud Manager.

"Découvrez comment vous inscrire à Cloud Insights".

Contrôle d'Cloud Volumes ONTAP dans AWS

Suivez quelques étapes pour contrôler les performances d'Cloud Volumes ONTAP.

Démarrage rapide

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

Vérifiez la prise en charge de votre configuration

Vous devez avoir installé Cloud Manager 3.8.4 ou une version ultérieure dans AWS et Cloud Volumes ONTAP dans AWS. Vous devez également être un nouveau client Cloud Insights.

Activez la surveillance sur votre système nouveau ou existant

- Nouveaux environnements de travail : assurez-vous de maintenir l'option surveillance activée lorsque vous créez l'environnement de travail (activé par défaut).
- Environnements de travail existants : sélectionnez un environnement de travail et cliquez sur **Démarrer la surveillance**.

Afficher les données de performances

Cliquez sur **Monitoring** et affichez les données de performances de vos volumes.

Abonnez-vous à Cloud Insights

Abonnez-vous avant la fin de votre essai gratuit de 30 jours pour continuer à consulter les données de performances dans Cloud Manager et Cloud Insights. "Découvrez comment vous inscrire".

De formation

Lisez les informations suivantes pour vous assurer que votre configuration est prise en charge.

Versions de Cloud Manager prises en charge

Vous devez installer Cloud Manager 3.8.4 ou une version ultérieure. Une nouvelle installation est nécessaire car une nouvelle infrastructure est requise pour activer le service de surveillance. Cette infrastructure est disponible en commençant par les nouvelles installations de Cloud Manager 3.8.4.

Versions de Cloud Volumes ONTAP prises en charge

Toute version d'Cloud Volumes ONTAP dans AWS.

Condition Cloud Insights

Vous devez être un nouveau client de Cloud Insights. La surveillance n'est pas prise en charge si vous disposez déjà d'un locataire Cloud Insights.

Adresse e-mail pour Cloud Central

L'adresse e-mail de votre compte utilisateur Cloud Central doit être l'adresse e-mail professionnelle. Les domaines de messagerie gratuits tels que gmail et hotmail ne sont pas pris en charge lors de la création d'un locataire Cloud Insights.

Mise en réseau pour l'unité d'acquisition

L'unité d'acquisition utilise une authentification bidirectionnelle/mutuelle pour se connecter au serveur Cloud Insights. Le certificat client doit être transmis au serveur Cloud Insights pour être authentifié. Pour ce faire, le proxy doit être configuré pour transférer la requête http au serveur Cloud Insights sans décrypter les données.

L'unité d'acquisition utilise les deux noeuds finaux suivants pour communiquer avec Cloud Insights. Si vous disposez d'un pare-feu entre le serveur de l'unité d'acquisition et Cloud Insights, vous avez besoin de ces noeuds finaux lors de la configuration des règles de pare-feu :

```
https://aulogin.<Cloud Insights Domain>
https://<your-tenant-ID>.<Cloud Insights Domain>
```

Par exemple :

```
https://aulogin.c01.cloudinsights.netapp.com
https://cg0c586a-ee05-45rb-a5ac-
333b5ae7718d7.c01.cloudinsights.netapp.com
```

Contactez-nous via la discussion interne si vous avez besoin d'aide pour identifier votre domaine Cloud Insights et votre identifiant de locataire.

Mise en réseau du connecteur

Comme pour l'unité d'acquisition, le connecteur doit disposer d'une connectivité sortante avec le locataire Cloud Insights. Mais le point d'extrémité que les contacts du connecteur sont légèrement différents. Il contacte l'URL de l'hôte du locataire à l'aide de l'ID de locataire raccourci :

```
 https://<your-short-tenant-ID>.<Cloud Insights Domain>
Par exemple :
```

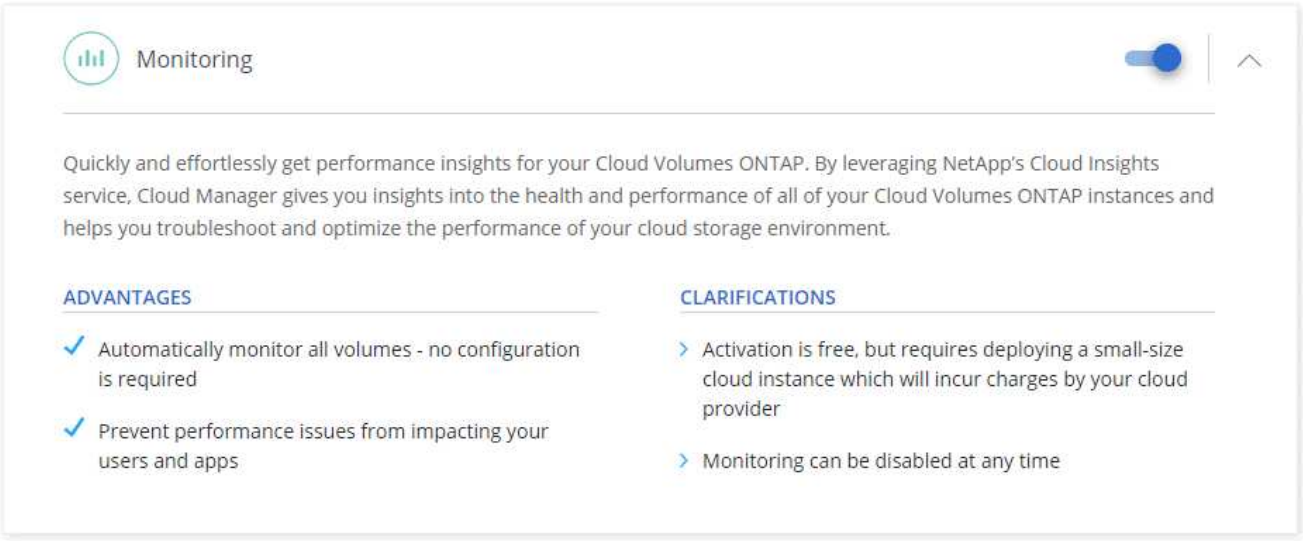
```
 https://abcd12345.c01.cloudinsights.netapp.com
Encore une fois, vous pouvez nous contacter par le biais de la
discussion sur le produit si vous avez besoin d'aide pour identifier
l'URL d'hôte du locataire.
```

Activation de la surveillance sur un nouveau système

Le service de surveillance est activé par défaut dans l'assistant de l'environnement de travail. Assurez-vous de conserver l'option activée.

Étapes

1. Cliquez sur **Créer Cloud Volumes ONTAP**.
2. Sélectionnez Amazon Web Services en tant que fournisseur cloud, puis choisissez un système à un seul nœud ou haute disponibilité.
3. Remplissez la page Détails et références.
4. Sur la page Services, laissez le service activé et cliquez sur **Continuer**.

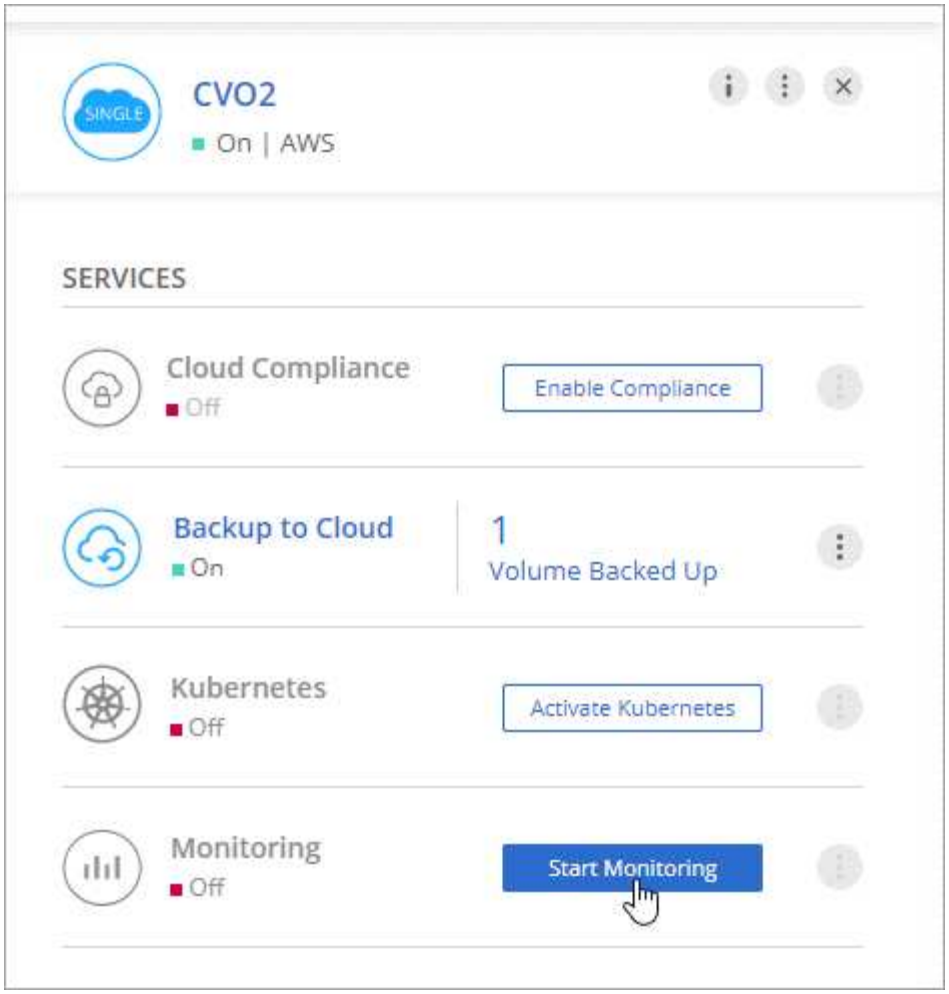


Activation de la surveillance sur un système existant

Activez la surveillance à tout moment à partir de l'environnement de travail.

Étapes

1. En haut de Cloud Manager, cliquez sur **environnements de travail**.
2. Sélectionnez un environnement de travail.
3. Dans le volet de droite, cliquez sur **Démarrer la surveillance**.



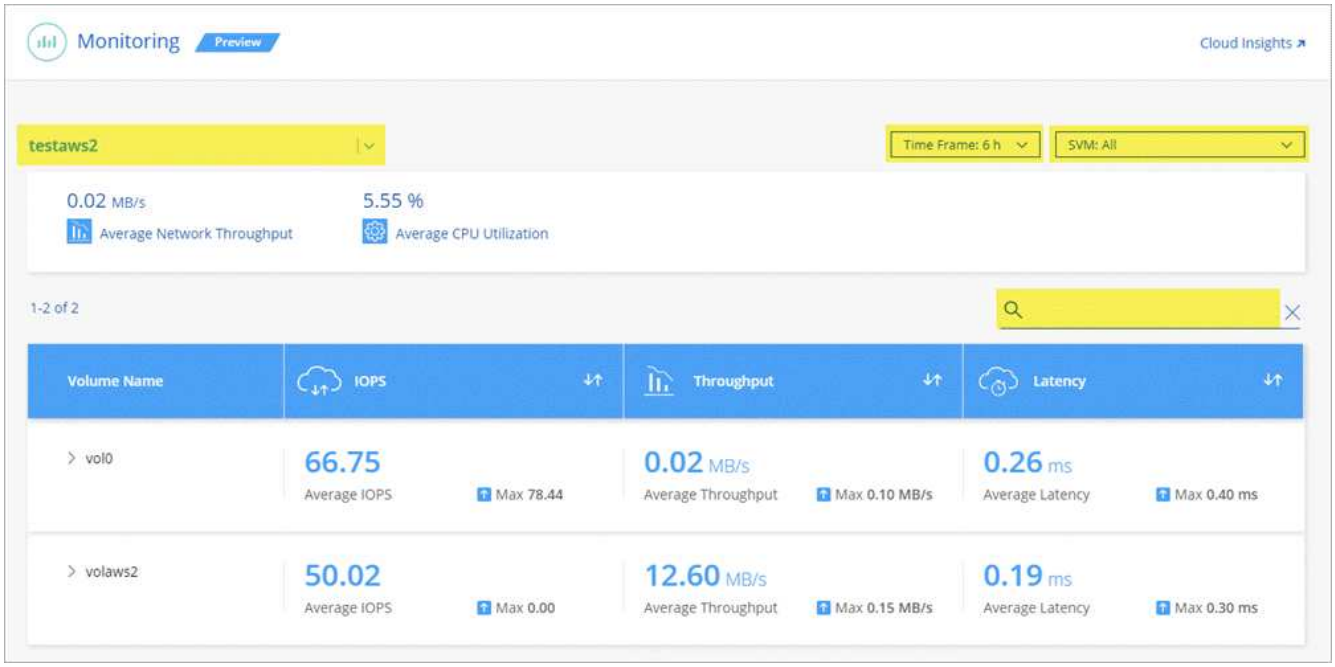
Surveillance de vos volumes

Surveillez les performances en affichant les IOPS, le débit et la latence de chacun de vos volumes.

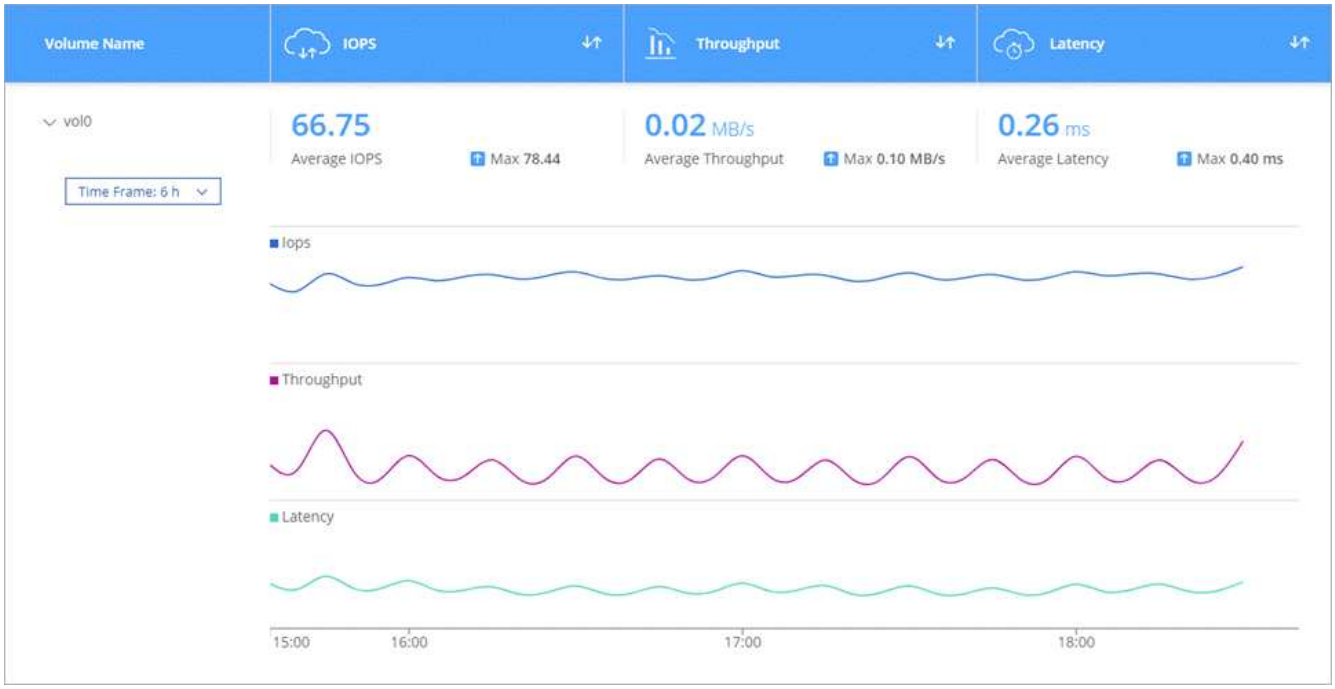
Étapes

1. En haut de Cloud Manager, cliquez sur **Monitoring**.
2. Filtrez le contenu du tableau de bord pour afficher les informations dont vous avez besoin.
    - Sélectionnez un environnement de travail spécifique.
    - Sélectionnez une autre période.
    - Sélectionnez un SVM spécifique.
    - Rechercher un volume spécifique.

    L'image suivante met en évidence chacune de ces options :



3. Cliquez sur un volume dans le tableau pour développer la ligne et afficher une chronologie pour les IOPS, le débit et la latence.



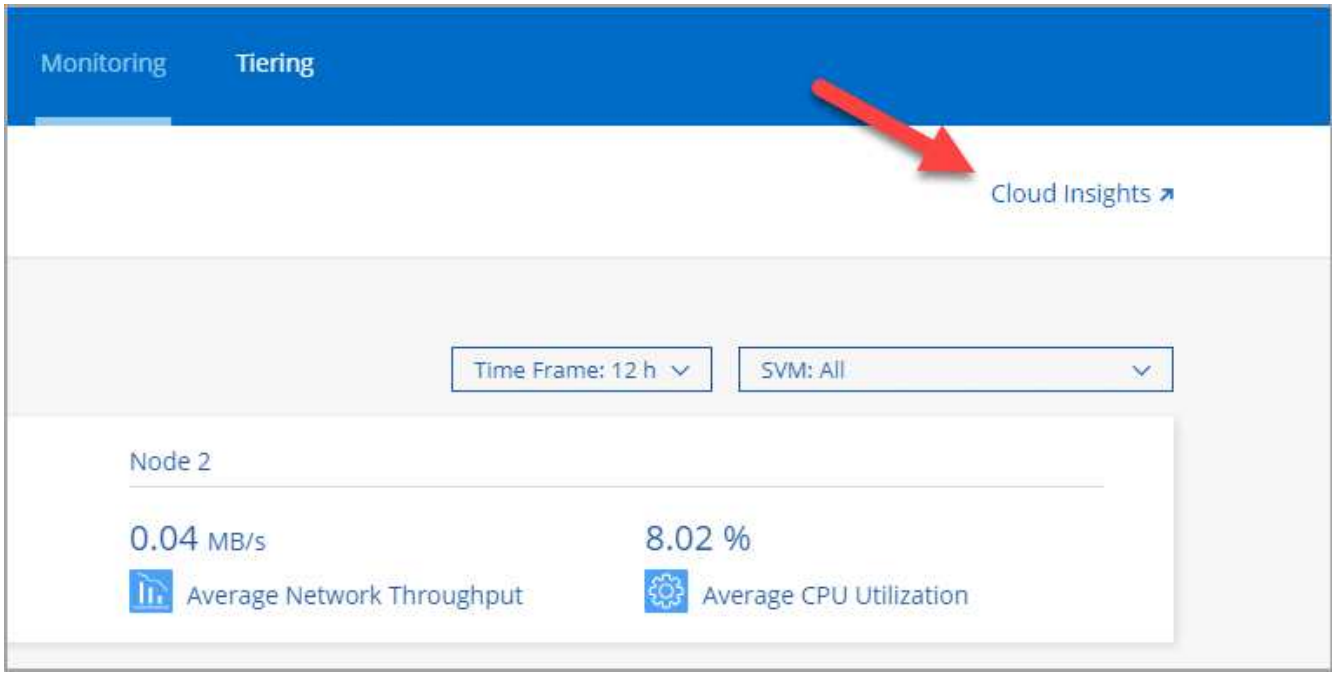
4. Utilisez ces données pour identifier les problèmes de performances et minimiser l'impact sur les utilisateurs et les applications.

Obtenir de plus amples informations sur Cloud Insights

L'onglet Monitoring de Cloud Manager fournit des données de performance de base pour vos volumes. Vous pouvez accéder à l'interface Web de Cloud Insights depuis votre navigateur pour effectuer un contrôle plus approfondi et configurer des alertes pour vos systèmes Cloud Volumes ONTAP.

Étapes

1. En haut de Cloud Manager, cliquez sur **Monitoring**.
2. Cliquez sur le lien **Cloud Insights**.



Résultat

Cloud Insights s'ouvre dans un nouvel onglet du navigateur. Si vous avez besoin d'aide, reportez-vous au "Documentation Cloud Insights".

Désactivation de la surveillance

Si vous ne souhaitez plus surveiller Cloud Volumes ONTAP, vous pouvez désactiver le service à tout moment.

> Si vous désactivez la surveillance de chacun de vos environnements de travail, vous devrez supprimer vous-même l'instance EC2. L'instance s'appelle *AcquisitionUnit* avec un hachage (UUID) généré concaténé. Par exemple : *AcquisitionUnit-FAN7FqeH*

Étapes

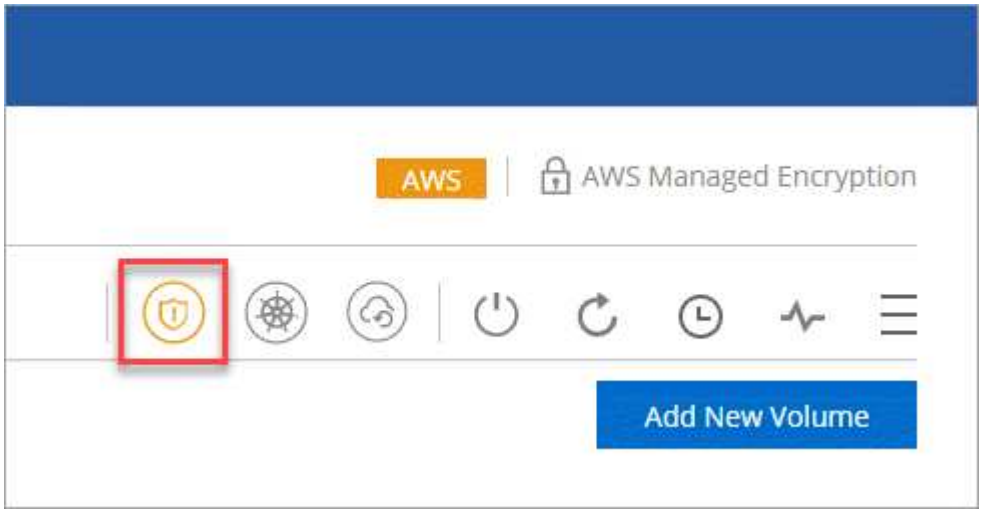
1. En haut de Cloud Manager, cliquez sur **environnements de travail**.
2. Sélectionnez un environnement de travail.
3. Dans le volet de droite, cliquez sur Et sélectionnez **Désactiver l'acquisition**.

Renforcer la protection contre les attaques par ransomware

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

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône **ransomware**.

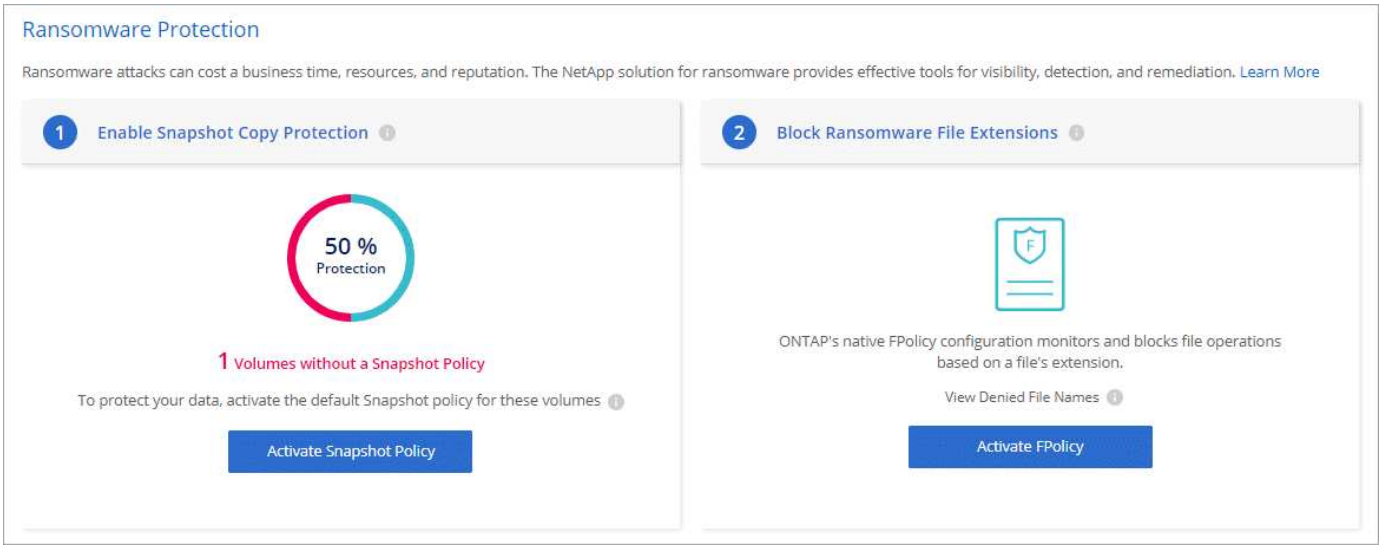


2. Implémentez la solution NetApp en cas d'attaque par ransomware :
   a. Cliquez sur **Activer la stratégie de snapshot**, si des volumes n'ont pas de règle de snapshot activée.

      La technologie Snapshot de NetApp offre la meilleure solution du secteur pour résoudre les problèmes liés aux attaques par ransomware. Le mieux pour réussir la récupération est d'effectuer une restauration à partir de sauvegardes non infectées. Les copies Snapshot sont en lecture seule, ce qui empêche la corruption par ransomware. Ils peuvent également assurer la granularité pour créer des images d'une copie de fichiers unique ou d'une solution complète de reprise après incident.

   b. Cliquez sur **Activer FPolicy** pour activer la solution FPolicy d'ONTAP, qui peut bloquer les opérations de fichiers en fonction de l'extension d'un fichier.

      Cette solution préventive améliore la protection contre les attaques par ransomware en bloquant les types de fichiers généralement utilisés.



Administration

Enregistrement des systèmes de paiement à l'utilisation

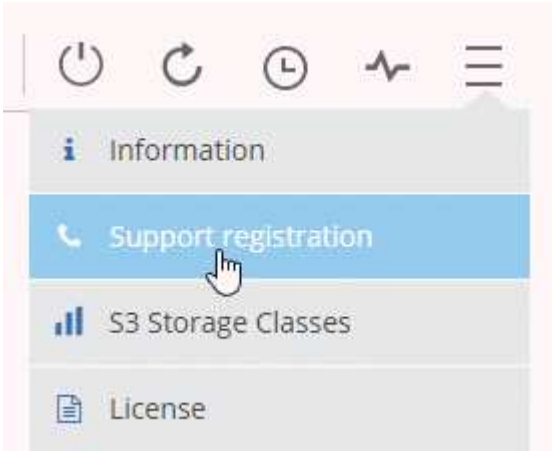
Le support de NetApp est inclus avec les systèmes Cloud Volumes ONTAP Explore, Standard et Premium, mais vous devez au préalable activer le support en enregistrant les systèmes à NetApp.

Étapes

1. Si vous n'avez pas encore ajouté votre compte du site de support NetApp à Cloud Manager, accédez à **Paramètres de compte** et ajoutez-le maintenant.

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

2. Sur la page Working Environments, double-cliquez sur le nom du système que vous souhaitez enregistrer.
3. Cliquez sur l'icône du menu, puis sur **support Registration** :



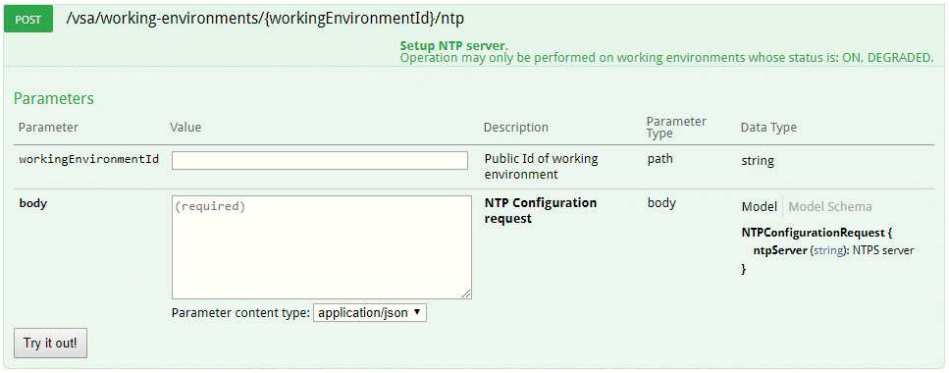
4. Sélectionnez un compte sur le site de support NetApp et cliquez sur **Register**.

Résultat

Cloud Manager enregistre le système avec NetApp.

Configuration de Cloud Volumes ONTAP

Après avoir déployé Cloud Volumes ONTAP, vous pouvez le configurer en synchronisant l'heure du système à l'aide de NTP et en effectuant quelques tâches facultatives à partir de System Manager ou de l'interface de ligne de commande.

Tâche	Description
Synchronisez l'heure du système à l'aide du protocole NTP	La spécification d'un serveur NTP synchronise l'heure entre les systèmes de votre réseau, ce qui peut aider à éviter les problèmes dus aux différences de temps. Spécifiez un serveur NTP via l'API Cloud Manager ou depuis l'interface utilisateur lors de la configuration d'un serveur CIFS. • "Modification du serveur CIFS" • "Guide du développeur de l'API Cloud Manager" Par exemple, voici l'API d'un système à un seul nœud dans AWS : 
Facultatif : configuration d'AutoSupport	AutoSupport surveille de manière proactive l'état de votre système et envoie automatiquement des messages au support technique NetApp par défaut. Si l'administrateur de comptes a ajouté un serveur proxy à Cloud Manager avant de lancer votre instance, Cloud Volumes ONTAP est configuré pour utiliser ce serveur proxy pour les messages AutoSupport. Vous devez tester AutoSupport pour vous assurer qu'il peut envoyer des messages. Pour obtenir ces instructions, consultez l'aide de System Manager ou le "Référence de l'administration du système ONTAP 9".
Facultatif : configurez Cloud Manager en tant que proxy AutoSupport	Si votre environnement requiert un serveur proxy pour envoyer des messages AutoSupport, vous pouvez configurer Cloud Manager pour qu'il fonctionne comme proxy. Aucune configuration de Cloud Manager n'est requise, autre que l'accès Internet. Il vous suffit de accéder à l'interface de ligne de commandes pour Cloud Volumes ONTAP et d'exécuter la commande suivante : `system node autosupport modify -proxy-url <cloud-manager-ip-address>`

Tâche	Description
En option : Configurer EMS	Le système de gestion des événements (EMS) collecte et affiche des informations sur les événements qui se produisent sur les systèmes Cloud Volumes ONTAP. Pour recevoir des notifications d'événements, vous pouvez définir des destinations d'événements (adresses e-mail, hôtes de trap SNMP ou serveurs syslog) et des routes d'événements pour un événement particulier. Vous pouvez configurer EMS à l'aide de l'interface de ligne de commande. Pour obtenir des instructions, reportez-vous au "Guide de configuration rapide de ONTAP 9 EMS".
Facultatif : créez une interface réseau de gestion SVM (LIF) pour les systèmes HA dans plusieurs zones de disponibilité AWS	Une interface de réseau de gestion de machine virtuelle de stockage (LIF) est requise si vous souhaitez utiliser SnapCenter ou SnapDrive pour Windows avec une paire haute disponibilité. La LIF de gestion du SVM doit utiliser une adresse IP *flottante* lors de l'utilisation d'une paire HA sur plusieurs zones de disponibilité AWS. Cloud Manager vous invite à spécifier l'adresse IP flottante lors du lancement de la paire HA. Si vous n'avez pas spécifié l'adresse IP, vous pouvez créer le LIF de gestion SVM vous-même à partir de System Manager ou de l'interface de ligne de commande. L'exemple suivant montre comment créer le LIF à partir de l'interface de ligne de commande : `network interface create -vserver svm_cloud -lif svm_mgmt -role data -data-protocol none -home-node cloud-01 -home-port e0a -address 10.0.2.126 -netmask 255.255.255.0 -status-admin up -firewall -policy mgmt`
Facultatif : modifiez l'emplacement de sauvegarde des fichiers de configuration	Cloud Volumes ONTAP crée automatiquement des fichiers de sauvegarde de la configuration qui contiennent des informations sur les options configurables dont il a besoin pour fonctionner correctement. Par défaut, Cloud Volumes ONTAP sauvegarde les fichiers sur l'hôte Connector toutes les huit heures. Si vous souhaitez envoyer les sauvegardes à un autre emplacement, vous pouvez modifier l'emplacement vers un serveur FTP ou HTTP dans votre data center ou dans AWS. Par exemple, vous pouvez déjà disposer d'un emplacement de sauvegarde pour vos systèmes de stockage FAS. Vous pouvez modifier l'emplacement de sauvegarde à l'aide de l'interface de ligne de commande. Voir la "Référence de l'administration du système ONTAP 9".

Gestion des licences BYOL pour Cloud Volumes ONTAP

Ajoutez une licence système BYOL Cloud Volumes ONTAP pour ajouter de la capacité, mettre à jour une licence système existante et gérer les licences BYOL pour la sauvegarde dans le cloud.

Gestion des licences système

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

736 To à Cloud Volumes ONTAP. Vous pouvez également acheter quatre licences pour obtenir jusqu'à 1.4 po.

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

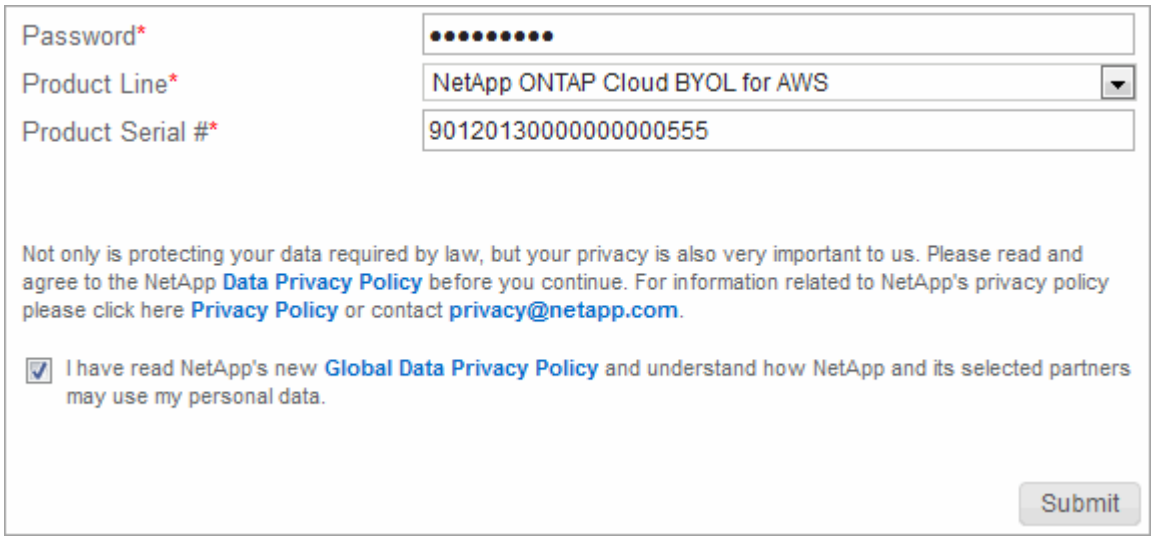
Obtention d'un fichier de licence système

Dans la plupart des cas, Cloud Manager peut obtenir automatiquement votre fichier de licence en utilisant votre compte sur le site de support NetApp. Si ce n'est pas le cas, vous devrez charger manuellement le fichier de licence. Si vous n'avez pas le fichier de licence, vous pouvez l'obtenir sur netapp.com.

Étapes

1. Accédez au "Générateur de fichiers de licences NetApp" Et connectez-vous en utilisant vos identifiants du site du support NetApp.
2. Entrez votre mot de passe, choisissez votre produit, entrez le numéro de série, confirmez que vous avez lu et accepté la politique de confidentialité, puis cliquez sur **Envoyer**.

   Exemple



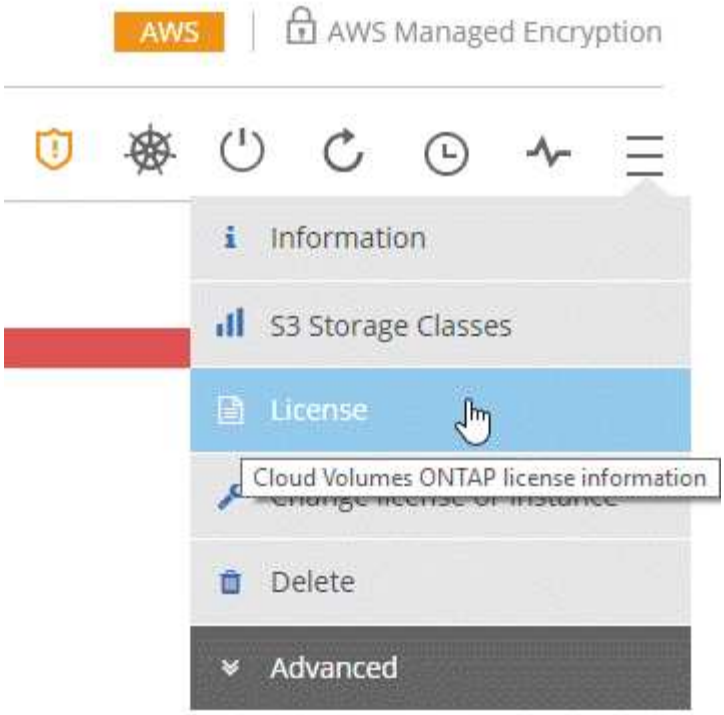
3. Choisissez si vous souhaitez recevoir le fichier numéro de série.NLF JSON par e-mail ou par téléchargement direct.

Ajout d'une nouvelle licence système

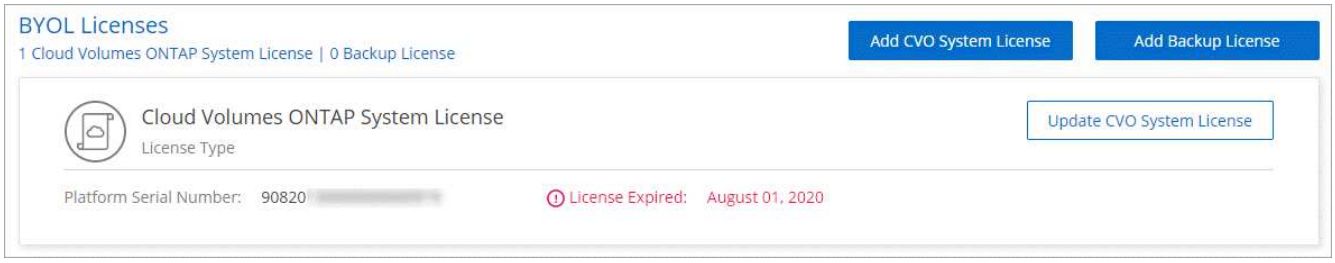
Ajoutez une nouvelle licence système BYOL à tout moment pour allouer une capacité supplémentaire de 368 To à votre système Cloud Volumes ONTAP BYOL.

Étapes

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



3. Cliquez sur **Ajouter la licence système CVO**.



4. Indiquez le numéro de série ou téléchargez le fichier de licence.
5. Cliquez sur **Ajouter une licence**.

Résultat

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

Mise à jour d'une licence système

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

Si Cloud Manager ne peut pas accéder au fichier de licence via la connexion Internet sécurisée, vous pouvez obtenir le fichier vous-même, puis le charger manuellement dans Cloud Manager.

Étapes

1. Dans Cloud Manager, ouvrez l'environnement de travail Cloud Volumes ONTAP BYOL.
2. Cliquez sur l'icône du menu, puis sur **Licence**.
3. Cliquez sur **mettre à jour la licence système CVO**.

4. Cliquez sur **Télécharger le fichier** et sélectionnez le fichier de licence.
5. Cliquez sur **mettre à jour la licence**.

Résultat

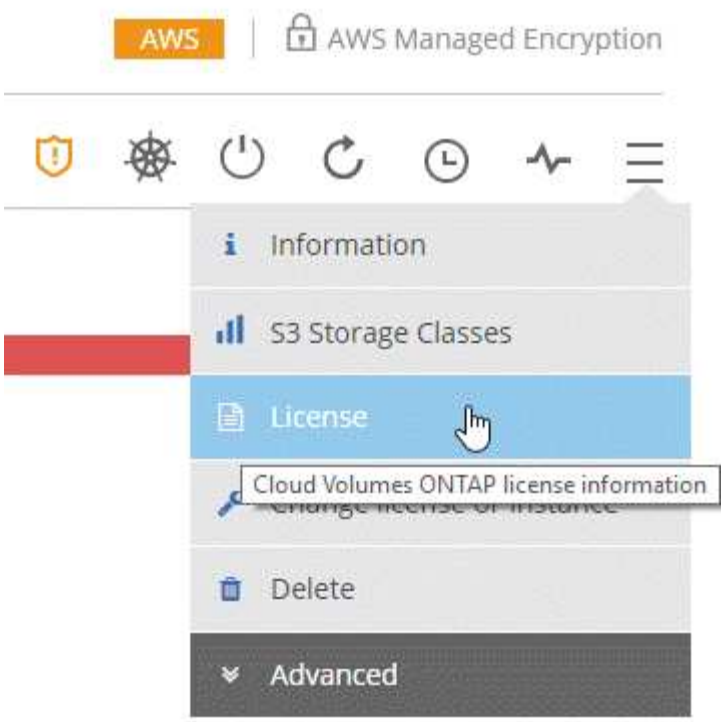
Cloud Manager met à jour la licence sur le système Cloud Volumes ONTAP.

Ajout et mise à jour de votre licence Backup BYOL

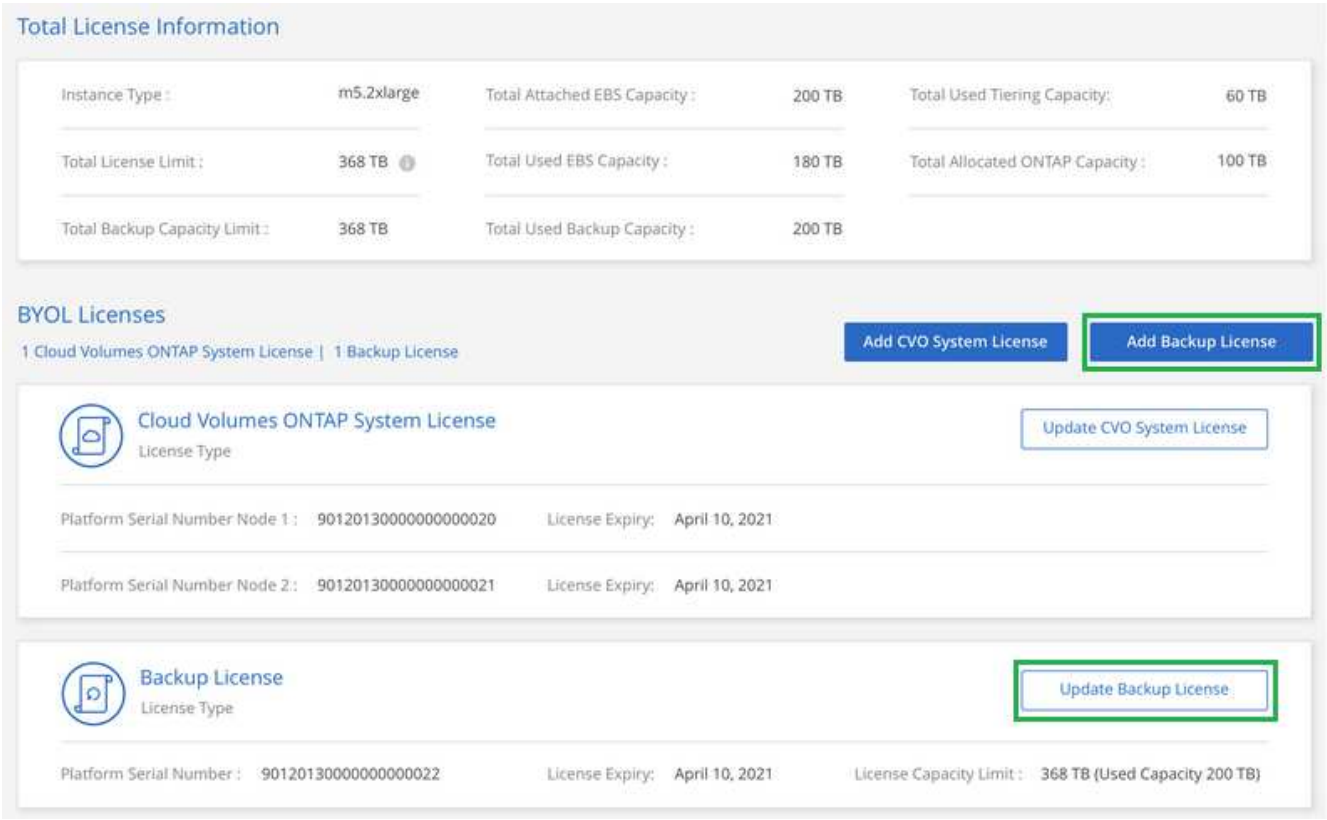
La page des licences BYOL permet d'ajouter ou de mettre à jour votre licence Backup BYOL.

Étapes

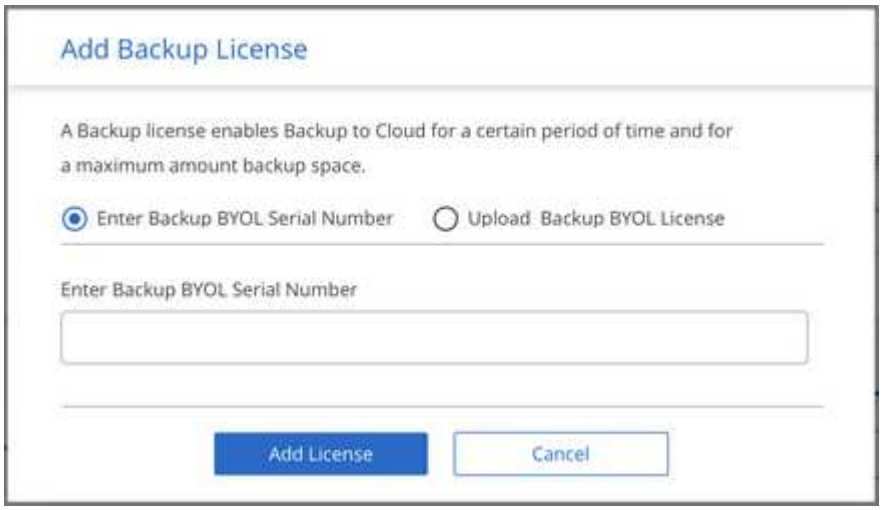
1. Dans Cloud Manager, ouvrez l'environnement de travail Cloud Volumes ONTAP BYOL.
2. Cliquez sur l'icône du menu, puis sur **Licence**.



3. Cliquez sur **Ajouter une licence de sauvegarde** ou **mettre à jour la licence de sauvegarde** selon que vous ajoutez une nouvelle licence ou mettez à jour une licence existante.



4. Entrez les informations de licence et cliquez sur **Ajouter une licence** :
   - Si vous disposez du numéro de série, sélectionnez l'option **entrer le numéro de série BYOL** et entrez le numéro de série.
   - Si vous disposez du fichier de licence de sauvegarde, sélectionnez l'option **Télécharger la licence BYOL** de sauvegarde et suivez les invites pour joindre le fichier.



Résultat

Cloud Manager ajoute ou met à jour la licence pour que votre service Backup vers Cloud soit actif.

Mise à jour du logiciel Cloud Volumes ONTAP

Cloud Manager inclut plusieurs options que vous pouvez utiliser pour mettre à niveau

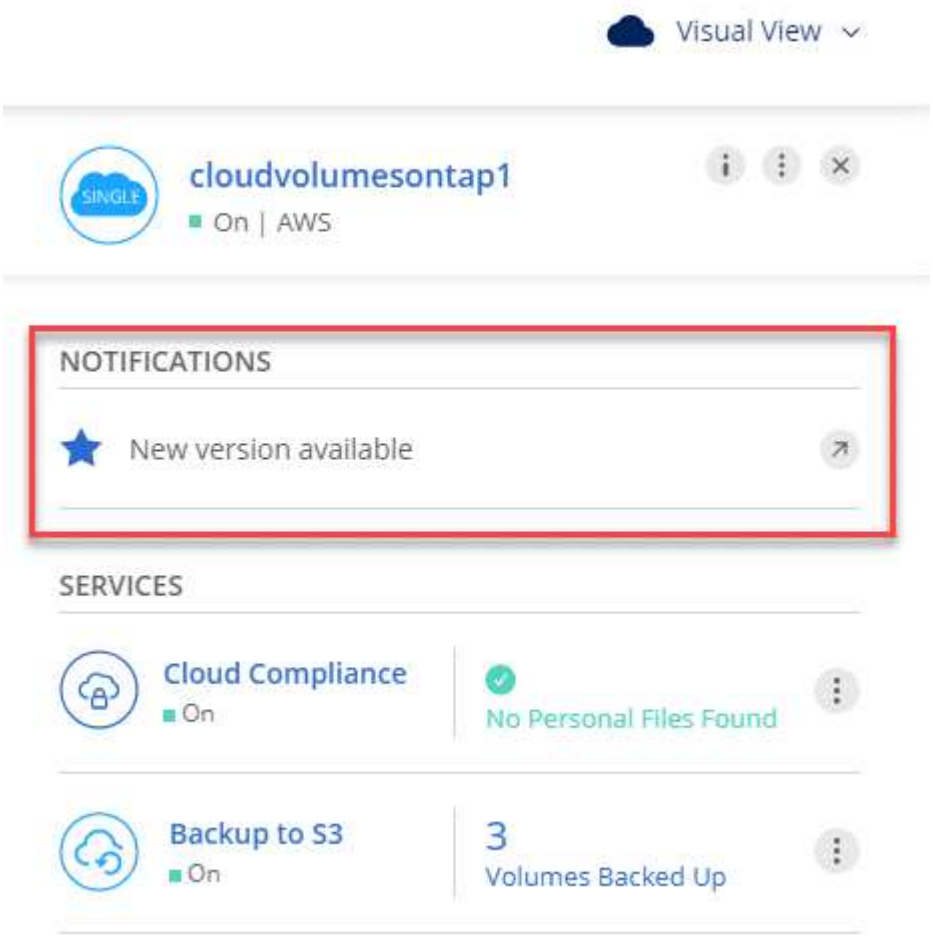
vers la version actuelle de Cloud Volumes ONTAP ou pour mettre à niveau Cloud Volumes ONTAP vers une version antérieure. Vous devez préparer les systèmes Cloud Volumes ONTAP avant de mettre à niveau ou de mettre à niveau le logiciel.

Les mises à jour logicielles doivent être effectuées par Cloud Manager

La mise à niveau d'Cloud Volumes ONTAP doit être effectuée depuis Cloud Manager. Vous ne devez pas mettre à niveau Cloud Volumes ONTAP à l'aide de System Manager ou de l'interface de ligne de commandes. Cela peut affecter la stabilité du système.

Méthodes de mise à jour de Cloud Volumes ONTAP

Cloud Manager affiche une notification dans les environnements de travail Cloud Volumes ONTAP lorsqu'une nouvelle version de Cloud Volumes ONTAP est disponible :



Vous pouvez lancer le processus de mise à niveau à partir de cette notification, qui automatise le processus en obtenant l'image logicielle à partir d'un compartiment S3, en installant l'image, puis en redémarrant le système. Pour plus de détails, voir Mise à niveau d'Cloud Volumes ONTAP à partir des notifications Cloud Manager.

Pour les systèmes HA dans AWS, Cloud Manager peut mettre à niveau le médiateur HA dans le cadre du processus de mise à niveau.

Options avancées pour les mises à jour logicielles

Cloud Manager propose également les options avancées suivantes pour la mise à jour du logiciel Cloud Volumes ONTAP :

- Mises à jour logicielles à l'aide d'une image sur une URL externe

  Cette option est utile si Cloud Manager ne peut pas accéder à la rubrique S3 pour mettre à niveau le logiciel, si un correctif vous a été fourni, ou si vous souhaitez rétrograder le logiciel vers une version spécifique.

  Pour plus de détails, voir Mise à niveau ou mise à niveau vers une version antérieure de Cloud Volumes ONTAP à l'aide d'un serveur HTTP ou FTP.

- Mises à jour logicielles à l'aide de l'autre image du système

  Vous pouvez utiliser cette option pour revenir à la version précédente en faisant de l'image logicielle alternative l'image par défaut. Cette option n'est pas disponible pour les paires HA.

  Pour plus de détails, voir Déclassement de Cloud Volumes ONTAP à l'aide d'une image locale.

Préparation de la mise à jour du logiciel Cloud Volumes ONTAP

Avant d'effectuer une mise à niveau ou une mise à niveau vers une version antérieure, vous devez vérifier que vos systèmes sont prêts et apporter les modifications de configuration requises.

- Planifier des temps d'indisponibilité
- Révision des exigences de version
- Vérifier que le rétablissement automatique est toujours activé
- Suspension des transferts SnapMirror
- Vérifier que les agrégats sont en ligne

Planifier des temps d'indisponibilité

Lorsque vous mettez à niveau un système à un seul nœud, le processus de mise à niveau met le système hors ligne pendant 25 minutes au cours desquelles les E/S sont interrompues.

La mise à niveau d'une paire haute disponibilité s'effectue sans interruption et les E/S sont continues. Au cours de ce processus de mise à niveau sans interruption, chaque nœud est mis à niveau en tandem afin de continuer à traiter les E/S aux clients.

Révision des exigences de version

La version de ONTAP que vous pouvez mettre à niveau ou rétrograder varie en fonction de la version de ONTAP actuellement exécutée sur votre système.

Pour comprendre les exigences de version, reportez-vous à la section "Documentation ONTAP 9 : configuration requise pour la mise à jour du cluster".

Vérifier que le rétablissement automatique est toujours activé

Le rétablissement automatique doit être activé sur une paire Cloud Volumes ONTAP HA (paramètre par défaut). Si ce n'est pas le cas, l'opération échouera.

"Documentation ONTAP 9 : commandes pour la configuration du rétablissement automatique"

Suspension des transferts SnapMirror

Si un système Cloud Volumes ONTAP a des relations SnapMirror actives, il est préférable de suspendre les transferts avant de mettre à jour le logiciel Cloud Volumes ONTAP. La suspension des transferts empêche les défaillances de SnapMirror. Vous devez suspendre les transferts depuis le système de destination.

Description de la tâche

Ces étapes décrivent l'utilisation de System Manager pour la version 9.3 et ultérieure.

Étapes

1. "Connectez-vous à System Manager" à partir du système de destination.
2. Cliquez sur **protection > relations**.
3. Sélectionnez la relation et cliquez sur **opérations > Quiesce**.

Vérifier que les agrégats sont en ligne

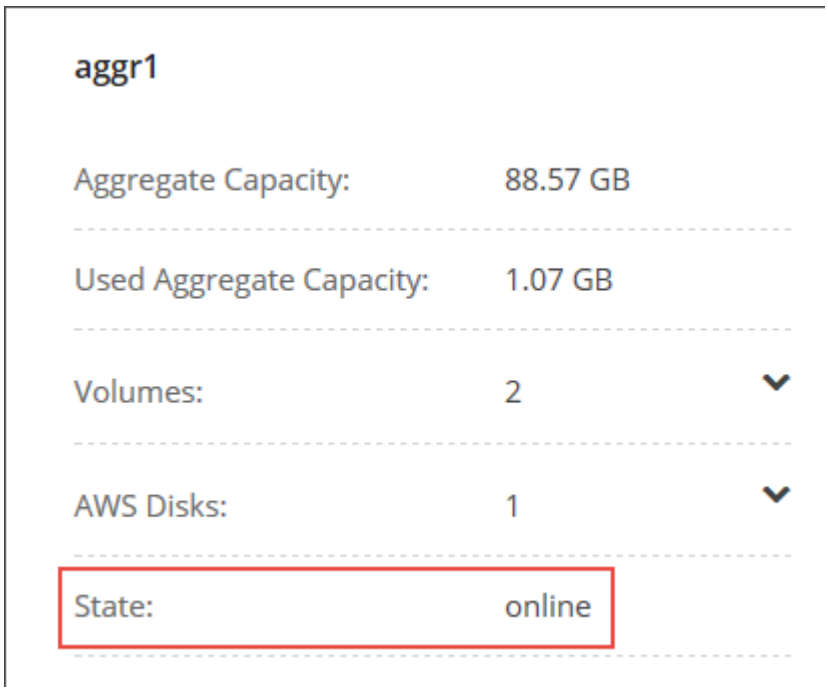
Les agrégats pour Cloud Volumes ONTAP doivent être en ligne avant de mettre à jour le logiciel. Les agrégats doivent être en ligne dans la plupart des configurations, mais si ce n'est pas le cas, vous devez les mettre en ligne.

Description de la tâche

Ces étapes décrivent l'utilisation de System Manager pour la version 9.3 et ultérieure.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > allocation avancée**.
2. Sélectionnez un agrégat, cliquez sur **Info**, puis vérifiez que l'état est en ligne.



3. Si l'agrégat est hors ligne, utilisez System Manager pour mettre l'agrégat en ligne :
   a. "Connectez-vous à System Manager".

b. Cliquez sur **stockage > agrégats et disques > agrégats**.

c. Sélectionnez l'agrégat, puis cliquez sur **plus d'actions > État > en ligne**.

Mise à niveau d'Cloud Volumes ONTAP à partir des notifications Cloud Manager

Cloud Manager vous avertit lorsqu'une nouvelle version d'Cloud Volumes ONTAP est disponible. Cliquez sur la notification pour lancer le processus de mise à niveau.

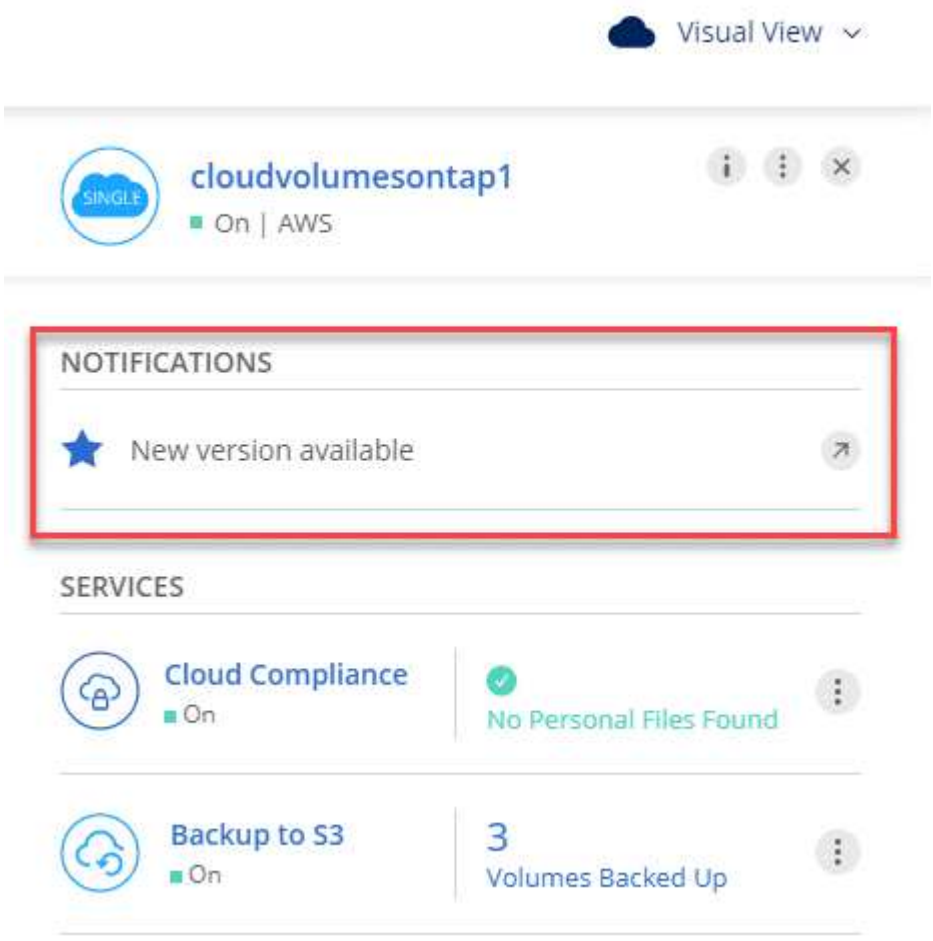
Avant de commencer

Les opérations de Cloud Manager telles que la création de volumes ou d'agrégats ne doivent pas être en cours pour le système Cloud Volumes ONTAP.

Étapes

1. Cliquez sur **environnements de travail**.
2. Sélectionnez un environnement de travail.

   Une notification s'affiche dans le volet droit si une nouvelle version est disponible :



3. Si une nouvelle version est disponible, cliquez sur **Upgrade**.
4. Dans la page informations sur la version, cliquez sur le lien pour lire les notes de version de la version spécifiée, puis cochez la case **J'ai lu…**.

5. Dans la page du contrat de licence utilisateur final (CLUF), lisez le CLUF, puis sélectionnez **J'ai lu et approuvé le CLUF**.
6. Dans la page Revue et approbation, lisez les notes importantes, sélectionnez **Je comprends…**, puis cliquez sur **Go**.

Résultat

Cloud Manager démarre la mise à niveau logicielle. Vous pouvez effectuer des actions sur l'environnement de travail une fois la mise à jour logicielle terminée.

Une fois que vous avez terminé

Si vous avez suspendu les transferts SnapMirror, utilisez System Manager pour reprendre les transferts.

Mise à niveau ou mise à niveau vers une version antérieure de Cloud Volumes ONTAP à l'aide d'un serveur HTTP ou FTP

Vous pouvez placer l'image du logiciel Cloud Volumes ONTAP sur un serveur HTTP ou FTP, puis lancer la mise à jour du logiciel à partir de Cloud Manager. Vous pouvez utiliser cette option si Cloud Manager ne peut pas accéder à la rubrique S3 pour mettre à niveau le logiciel ou si vous souhaitez mettre à niveau le logiciel.

Étapes

1. Configurez un serveur HTTP ou FTP pouvant héberger l'image du logiciel Cloud Volumes ONTAP.
2. Si vous disposez d'une connexion VPN au réseau virtuel, vous pouvez placer l'image logicielle Cloud Volumes ONTAP sur un serveur HTTP ou un serveur FTP de votre propre réseau. Sinon, vous devez placer le fichier sur un serveur HTTP ou FTP dans le cloud.
3. Si vous utilisez votre propre groupe de sécurité pour Cloud Volumes ONTAP, assurez-vous que les règles de sortie autorisent les connexions HTTP ou FTP pour que Cloud Volumes ONTAP puisse accéder à l'image logicielle.

   Le groupe de sécurité Cloud Volumes ONTAP prédéfini autorise les connexions HTTP et FTP sortantes par défaut.

4. Obtenez l'image logicielle de "Le site de support NetApp".
5. Copiez l'image du logiciel dans le répertoire du serveur HTTP ou FTP à partir duquel le fichier sera servi.
6. Dans l'environnement de travail de Cloud Manager, cliquez sur l'icône de menu, puis sur **Avancé > mettre à jour Cloud Volumes ONTAP**.
7. Sur la page de mise à jour du logiciel, choisissez **sélectionnez une image disponible à partir d'une URL**, saisissez l'URL, puis cliquez sur **Modifier l'image**.
8. Cliquez sur **Continuer** pour confirmer.

Résultat

Cloud Manager démarre la mise à jour logicielle. Vous pouvez effectuer des actions sur l'environnement de travail une fois la mise à jour logicielle terminée.

Une fois que vous avez terminé

Si vous avez suspendu les transferts SnapMirror, utilisez System Manager pour reprendre les transferts.

Déclassement de Cloud Volumes ONTAP à l'aide d'une image locale

Le passage de Cloud Volumes ONTAP à une version antérieure dans la même famille de versions (par exemple, 9.5 à 9.4) est appelé une version antérieure. Vous pouvez rétrograder sans assistance lors de la

rétrogradation de clusters nouveaux ou de tests, mais vous devez contacter le support technique si vous souhaitez rétrograder un cluster de production.

Chaque système Cloud Volumes ONTAP peut contenir deux images logicielles : l'image en cours d'exécution et une autre image que vous pouvez démarrer. Cloud Manager peut modifier l'image alternative comme image par défaut. Vous pouvez utiliser cette option pour revenir à la version précédente de Cloud Volumes ONTAP, si vous rencontrez des problèmes avec l'image actuelle.

Description de la tâche

Ce processus de mise à niveau vers une version antérieure est uniquement disponible pour les systèmes Cloud Volumes ONTAP. Il n'est pas disponible pour les paires HA.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > mettre à jour Cloud Volumes ONTAP**.
2. Sur la page mise à jour du logiciel, sélectionnez l'image de remplacement, puis cliquez sur **changer l'image**.
3. Cliquez sur **Continuer** pour confirmer.

Résultat

Cloud Manager démarre la mise à jour logicielle. Vous pouvez effectuer des actions sur l'environnement de travail une fois la mise à jour logicielle terminée.

Une fois que vous avez terminé

Si vous avez suspendu les transferts SnapMirror, utilisez System Manager pour reprendre les transferts.

Modification des systèmes Cloud Volumes ONTAP

Il peut être nécessaire de modifier la configuration des systèmes Cloud Volumes ONTAP au fur et à mesure de l'évolution de vos besoins de stockage. Vous pouvez, par exemple, choisir entre les configurations de paiement à l'utilisation, modifier le type d'instance ou d'ordinateur virtuel, et bien plus encore.

Modification de l'instance ou du type de machine pour Cloud Volumes ONTAP

Vous pouvez choisir parmi plusieurs types d'instances ou de machines lors du lancement d'Cloud Volumes ONTAP dans AWS, Azure ou GCP. Vous pouvez modifier l'instance ou le type de machine à tout moment si vous déterminez qu'elle est sous-dimensionnée ou surdimensionnée en fonction de vos besoins.

Description de la tâche

- Le rétablissement automatique doit être activé sur une paire Cloud Volumes ONTAP HA (paramètre par défaut). Si ce n'est pas le cas, l'opération échouera.

  "Documentation ONTAP 9 : commandes pour la configuration du rétablissement automatique"

- La modification de l'instance ou du type de machine affecte les frais de service du fournisseur cloud.
- L'opération redémarre Cloud Volumes ONTAP.

  Pour les systèmes à nœud unique, les E/S sont interrompues.

  Pour les paires HA, le changement n'est pas perturbateur. Les paires HA continuent de servir les données.

Cloud Manager modifie aisément un nœud à la fois en lançant le basculement et en attendant les frais de retour. L'équipe d'assurance qualité de NetApp a testé l'écriture et la lecture des fichiers pendant ce processus et n'a rencontré aucun problème côté client. Au fur et à mesure des changements de connexion, nous avons constaté des tentatives d'E/S au niveau des E/S, mais la couche applicative a pu faire face à ces courtes « connexions » NFS/CIFS.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **changer la licence ou l'instance** pour AWS, **changer la licence ou VM** pour Azure ou **changer la licence ou la machine** pour GCP.
2. Si vous utilisez une configuration payante, vous pouvez choisir une licence différente.
3. Sélectionnez une instance ou un type de machine, cochez la case pour confirmer que vous comprenez les implications du changement, puis cliquez sur **OK**.

Résultat

Cloud Volumes ONTAP redémarre avec la nouvelle configuration.

Changement entre les configurations de paiement à la demande

Une fois que vous avez lancé les systèmes Cloud Volumes ONTAP à la demande, vous pouvez modifier les configurations Explorer, Standard et Premium à tout moment en modifiant la licence. La modification de la licence augmente ou réduit la limite de capacité brute et vous permet de choisir entre différents types d'instances AWS ou de machines virtuelles Azure.

Dans GCP, un seul type de machine est disponible pour chaque configuration avec paiement à l'utilisation. Vous ne pouvez pas choisir entre différents types de machine.

Description de la tâche

Notez ce qui suit au sujet de la modification entre les licences de paiement à la demande :

- L'opération redémarre Cloud Volumes ONTAP.

  Pour les systèmes à nœud unique, les E/S sont interrompues.

  Pour les paires HA, le changement n'est pas perturbateur. Les paires HA continuent de servir les données.

- La modification de l'instance ou du type de machine affecte les frais de service du fournisseur cloud.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **changer la licence ou l'instance** pour AWS, **changer la licence ou VM** pour Azure ou **changer la licence ou la machine** pour GCP.
2. Sélectionnez un type de licence et un type d'instance ou de machine, cochez la case pour confirmer que vous comprenez les implications du changement, puis cliquez sur **OK**.

Résultat

Cloud Volumes ONTAP redémarre avec la nouvelle licence, le type d'instance, le type de machine ou les deux.

Passage à une autre configuration Cloud Volumes ONTAP

Si vous souhaitez basculer entre un abonnement avec paiement à l'utilisation et un abonnement BYOL, ou entre un système Cloud Volumes ONTAP unique et une paire haute disponibilité, vous devez déployer un

nouveau système avant de répliquer les données depuis le système existant vers le nouveau système.

Étapes

1. Créez un nouvel environnement de travail Cloud Volumes ONTAP.

   "Lancement d'Cloud Volumes ONTAP dans AWS"
   "Lancement d'Cloud Volumes ONTAP dans Azure"
   "Lancement d'Cloud Volumes ONTAP dans GCP"

2. "Configuration de la réplication des données unique" entre les systèmes pour chaque volume que vous devez répliquer.
3. Terminez le système Cloud Volumes ONTAP dont vous n'avez plus besoin par "suppression de l'environnement de travail d'origine".

Modification de la vitesse d'écriture sur normale ou élevée

Cloud Manager permet de choisir un paramètre de vitesse d'écriture pour les systèmes Cloud Volumes ONTAP à un seul nœud. La vitesse d'écriture par défaut est normale. Vous pouvez passer à une vitesse d'écriture élevée si vos workloads nécessitent des performances d'écriture rapides. Avant de modifier la vitesse d'écriture, vous devez "comprendre les différences entre les réglages normaux et élevés".

Description de la tâche

- Assurez-vous que les opérations telles que la création de volume ou d'agrégat ne sont pas en cours.
- Notez que cette modification redémarre Cloud Volumes ONTAP, ce qui signifie que les E/S sont interrompues.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > vitesse d'écriture**.
2. Sélectionnez **Normal** ou **Haut**.

   Si vous choisissez Haut, vous devrez lire l'énoncé « Je comprends… » et confirmer en cochant la case.

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

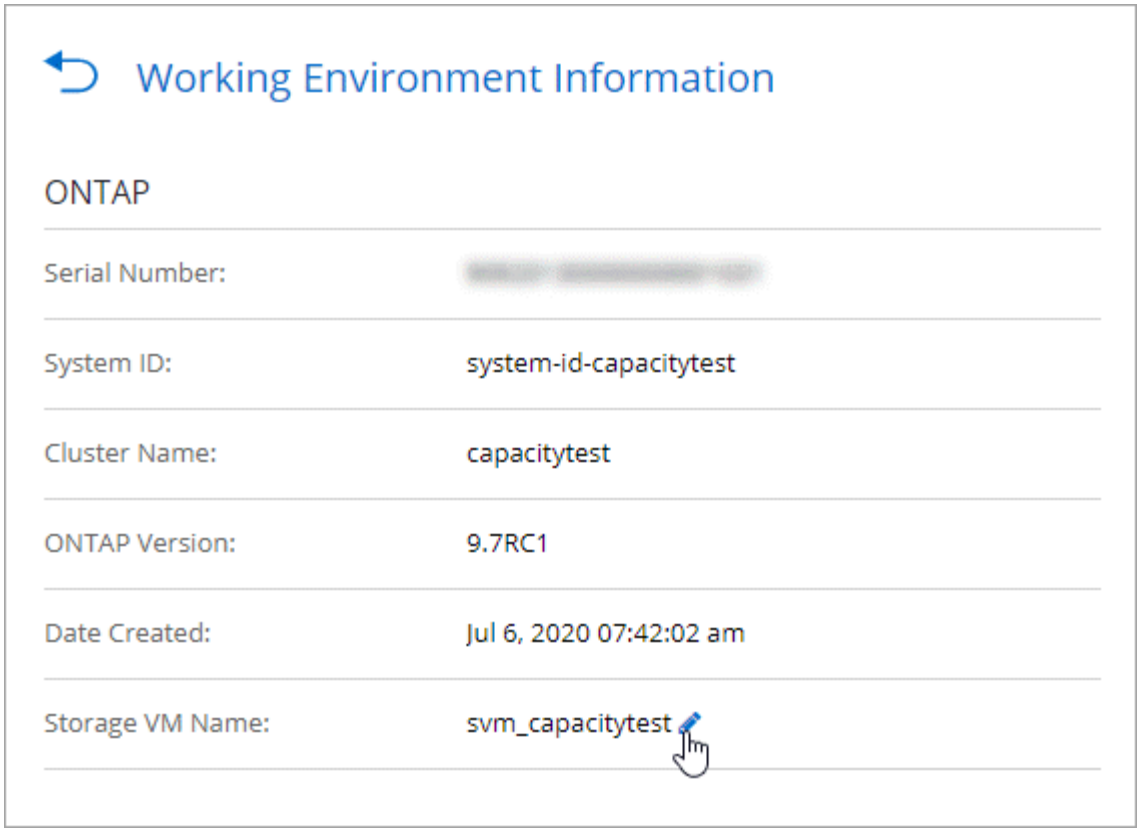
Modification du nom de la machine virtuelle de stockage

Cloud Manager nomme automatiquement la machine virtuelle de stockage (SVM) créée pour Cloud Volumes ONTAP. Vous pouvez modifier le nom du SVM si vous disposez de normes strictes en matière de nommage. Par exemple, vous pouvez indiquer le nom des SVM dans vos clusters ONTAP.

Mais si vous avez créé des SVM supplémentaires pour Cloud Volumes ONTAP, vous ne pouvez pas renommer les SVM de Cloud Manager. Pour ce faire, vous devez utiliser System Manager ou l'interface de ligne de commandes directement dans Cloud Volumes ONTAP.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **informations**.
2. Cliquez sur l'icône d'édition située à droite du nom de la VM de stockage.



3. Dans la boîte de dialogue Modifier le nom du SVM, modifiez le nom, puis cliquez sur **Enregistrer**.

Modification du mot de passe de Cloud Volumes ONTAP

Cloud Volumes ONTAP inclut un compte d'administration de cluster. Si nécessaire, vous pouvez modifier le mot de passe de ce compte à partir de Cloud Manager.

> Vous ne devez pas modifier le mot de passe du compte admin via System Manager ou l'interface de ligne de commande. Le mot de passe ne sera pas pris en compte dans Cloud Manager. Par conséquent, Cloud Manager ne peut pas contrôler l'instance correctement.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > définir mot de passe**.
2. Saisissez le nouveau mot de passe deux fois, puis cliquez sur **Enregistrer**.

   Le nouveau mot de passe doit être différent de l'un des six derniers mots de passe utilisés.

Modification de la MTU réseau pour les instances c4.4xlarge et c4.8xlarge

Par défaut, Cloud Volumes ONTAP est configuré pour utiliser 9 000 MTU (également appelés trames Jumbo) lorsque vous choisissez l'instance c4.4xlarge ou l'instance c4.8xlarge dans AWS. Vous pouvez modifier la MTU réseau à 1 500 octets si cela est plus approprié pour votre configuration réseau.

Description de la tâche

Une unité de transmission réseau maximale (MTU) de 9 000 octets peut fournir le débit réseau maximal le plus élevé possible pour des configurations spécifiques.

9 000 MTU sont un bon choix si les clients du même VPC communiquent avec le système Cloud Volumes

ONTAP et que certains ou tous ces clients prennent également en charge 9 000 MTU. Si le trafic quitte le VPC, la fragmentation des paquets peut se produire, ce qui dégrade les performances.

Un MTU réseau de 1 500 octets est un bon choix si les clients ou les systèmes extérieurs au VPC communiquent avec le système Cloud Volumes ONTAP.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > utilisation du réseau**.
2. Sélectionnez **Standard** ou **Jumbo Frames**.
3. Cliquez sur **Modifier**.

Modification des tables de routage associées aux paires HA dans plusieurs AZS d'AWS

Vous pouvez modifier les tables de routage AWS incluant des routes vers les adresses IP flottantes pour une paire haute disponibilité. Vous pouvez le faire si les nouveaux clients NFS ou CIFS ont besoin d'accéder à une paire haute disponibilité dans AWS.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **informations**.
2. Cliquez sur **tables de routage**.
3. Modifiez la liste des tables de routage sélectionnées, puis cliquez sur **Enregistrer**.

Résultat

Cloud Manager envoie une requête AWS pour modifier les tables de routage.

Gestion de l'état du Cloud Volumes ONTAP

Vous pouvez arrêter et lancer Cloud Volumes ONTAP depuis Cloud Manager pour gérer les coûts de calcul du cloud.

Planification des arrêts automatiques de Cloud Volumes ONTAP

Vous pouvez arrêter Cloud Volumes ONTAP à des intervalles réguliers afin de réduire les coûts de calcul. Au lieu de le faire manuellement, vous pouvez configurer Cloud Manager de sorte qu'il s'arrête automatiquement, puis redémarre les systèmes à des moments spécifiques.

Description de la tâche

Lorsque vous planifiez un arrêt automatique de votre système Cloud Volumes ONTAP, Cloud Manager reporte l'arrêt du système si un transfert de données actif est en cours. Cloud Manager arrête le système une fois le transfert terminé.

Cette tâche planifie les arrêts automatiques des deux nœuds d'une paire haute disponibilité.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône horloge :

2. Spécifiez la planification de l'arrêt :

a. Choisissez si vous souhaitez arrêter le système tous les jours, tous les jours de semaine, tous les week-ends ou toute combinaison des trois options.

b. Indiquez quand vous souhaitez désactiver le système et pendant combien de temps vous voulez le désactiver.

Exemple

L'image suivante montre un calendrier qui indique à Cloud Manager d'arrêter le système tous les samedis à 12:00 pendant 48 heures. Cloud Manager redémarre le système tous les lundis à 12:00

3. Cliquez sur **Enregistrer**.

Résultat

Cloud Manager enregistre la planification. L'icône de l'horloge change pour indiquer qu'un programme est défini : 

Arrêt d'Cloud Volumes ONTAP

L'arrêt de Cloud Volumes ONTAP vous permet d'économiser de l'espace de calcul et de créer des snapshots des disques racines et de démarrage, ce qui peut être utile pour la résolution des problèmes.

Description de la tâche

Lorsque vous arrêtez une paire HA, Cloud Manager arrête les deux nœuds.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône **Désactiver**.

2. Conservez l'option de création de snapshots activés car les snapshots peuvent activer la récupération du système.
3. Cliquez sur **Désactiver**.

   L'arrêt du système peut prendre jusqu'à quelques minutes. Vous pouvez redémarrer les systèmes ultérieurement à partir de la page de l'environnement de travail.

Contrôle des coûts des ressources AWS

Avec Cloud Manager, vous pouvez consulter les coûts associés aux ressources pour l'exécution de Cloud Volumes ONTAP dans AWS. Vous pouvez également voir les économies réalisées grâce aux fonctionnalités NetApp qui permettent de réduire les coûts de stockage.

Description de la tâche

Cloud Manager met à jour les coûts lorsque vous actualisez la page. Vous devez vous référer à AWS pour plus de détails sur le coût final.

Étape

1. Vérifiez que Cloud Manager peut obtenir des informations de coûts depuis AWS :
   a. Assurez-vous que la politique IAM qui fournit les autorisations à Cloud Manager inclut les actions suivantes :

      ```
      "ce:GetReservationUtilization",
      "ce:GetDimensionValues",
      "ce:GetCostAndUsage",
      "ce:GetTags"
      ```

      Ces actions sont incluses dans la dernière "Politique de Cloud Manager". Les nouveaux systèmes déployés à partir de NetApp Cloud Central incluent automatiquement ces autorisations.

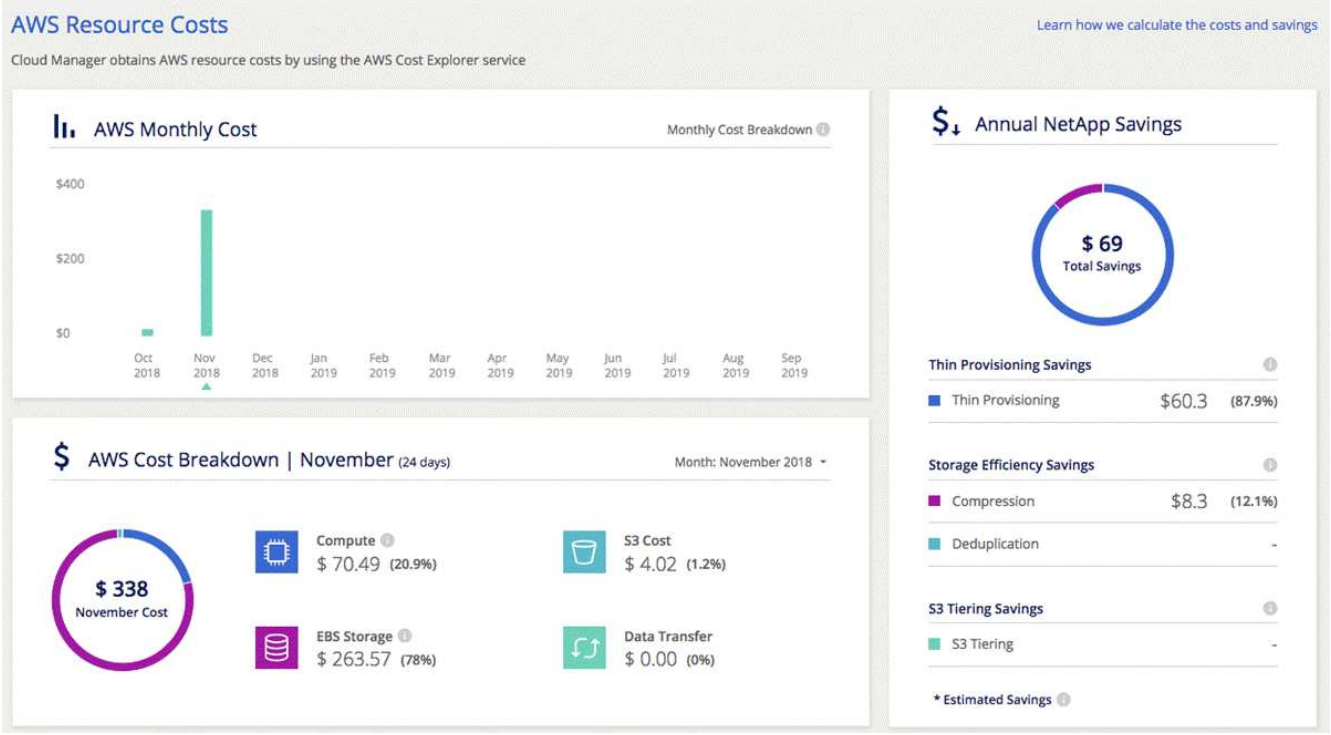
   b. "Activer la balise **WorkingEnvironnement**".

      Pour suivre vos coûts AWS, Cloud Manager attribue une balise d'allocation des coûts aux instances Cloud Volumes ONTAP. Après avoir créé votre premier environnement de travail, activez la balise **WorkingEnvironment,Id**. Les balises définies par l'utilisateur n'apparaissent pas dans les rapports de facturation AWS tant que vous ne les activez pas dans la console de facturation et de gestion des coûts.

2. Sur la page environnements de travail, sélectionnez un environnement de travail Cloud Volumes ONTAP, puis cliquez sur **coût**.

   La page coûts affiche les coûts des mois actuels et précédents et présente vos économies annuelles sur les produits NetApp, si vous avez activé les fonctions d'économies de volumes offertes par NetApp.

   L'image suivante montre un exemple de page de coût :



Connexion à Cloud Volumes ONTAP

Si vous avez besoin d'une gestion avancée de Cloud Volumes ONTAP, vous pouvez le faire à l'aide d'OnCommand System Manager ou de l'interface de ligne de commande.

Connexion à System Manager

Vous devrez peut-être effectuer certaines tâches Cloud Volumes ONTAP à partir de System Manager, un outil de gestion basé sur un navigateur qui s'exécute sur le système Cloud Volumes ONTAP. Par exemple, vous devez utiliser System Manager pour créer des LUN.

Avant de commencer

L'ordinateur à partir duquel vous accédez à Cloud Manager doit disposer d'une connexion réseau à Cloud Volumes ONTAP. Par exemple, vous devrez peut-être vous connecter à Cloud Manager à partir d'un hôte de saut dans AWS ou Azure.

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

Étapes

1. Sur la page Working Environments, double-cliquez sur le système Cloud Volumes ONTAP que vous souhaitez gérer avec System Manager.
2. Cliquez sur l'icône de menu, puis sur **Avancé > System Manager**.
3. Cliquez sur **lancer**.

   System Manager se charge dans un nouvel onglet de navigateur.

4. Sur l'écran de connexion, saisissez **admin** dans le champ Nom d'utilisateur, saisissez le mot de passe que vous avez spécifié lors de la création de l'environnement de travail, puis cliquez sur **connexion**.

Résultat

La console System Manager se charge. Vous pouvez désormais l'utiliser pour gérer Cloud Volumes ONTAP.

Connexion à l'interface de ligne de commande Cloud Volumes ONTAP

L'interface de ligne de commande Cloud Volumes ONTAP vous permet d'exécuter toutes les commandes administratives et constitue un bon choix pour les tâches avancées ou si vous êtes plus à l'aise avec l'interface de ligne de commande. Vous pouvez vous connecter à l'interface de ligne de commande à l'aide de Secure Shell (SSH).

Avant de commencer

L'hôte à partir duquel vous utilisez SSH pour vous connecter à Cloud Volumes ONTAP doit disposer d'une connexion réseau à Cloud Volumes ONTAP. Par exemple, vous devrez peut-être utiliser SSH à partir d'un hôte de saut dans AWS ou Azure.

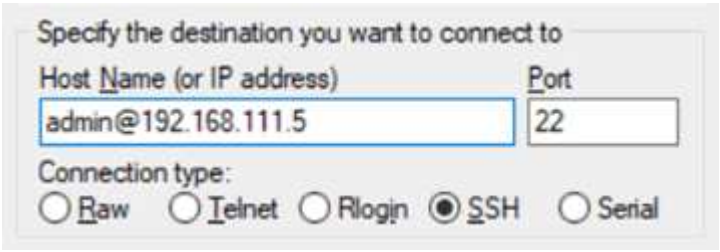
Lorsqu'elles sont déployées dans plusieurs environnements AZS, les configurations Cloud Volumes ONTAP HA utilisent une adresse IP flottante pour l'interface de gestion de cluster, ce qui signifie que le routage externe n'est pas disponible. Vous devez vous connecter à partir d'un hôte faisant partie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

Étapes

1. Dans Cloud Manager, identifiez l'adresse IP de l'interface de gestion du cluster :
   a. Sur la page Working Environments, sélectionnez le système Cloud Volumes ONTAP.
   b. Copiez l'adresse IP de gestion du cluster qui apparaît dans le volet droit.
2. Utilisez SSH pour vous connecter à l'adresse IP de l'interface de gestion du cluster à l'aide du compte admin.

   Exemple

   L'image suivante montre un exemple utilisant PuTTY :



3. À l'invite de connexion, entrez le mot de passe du compte admin.

   Exemple

```
Password: ********
COT2::>
```

Ajout de systèmes Cloud Volumes ONTAP existants à Cloud Manager

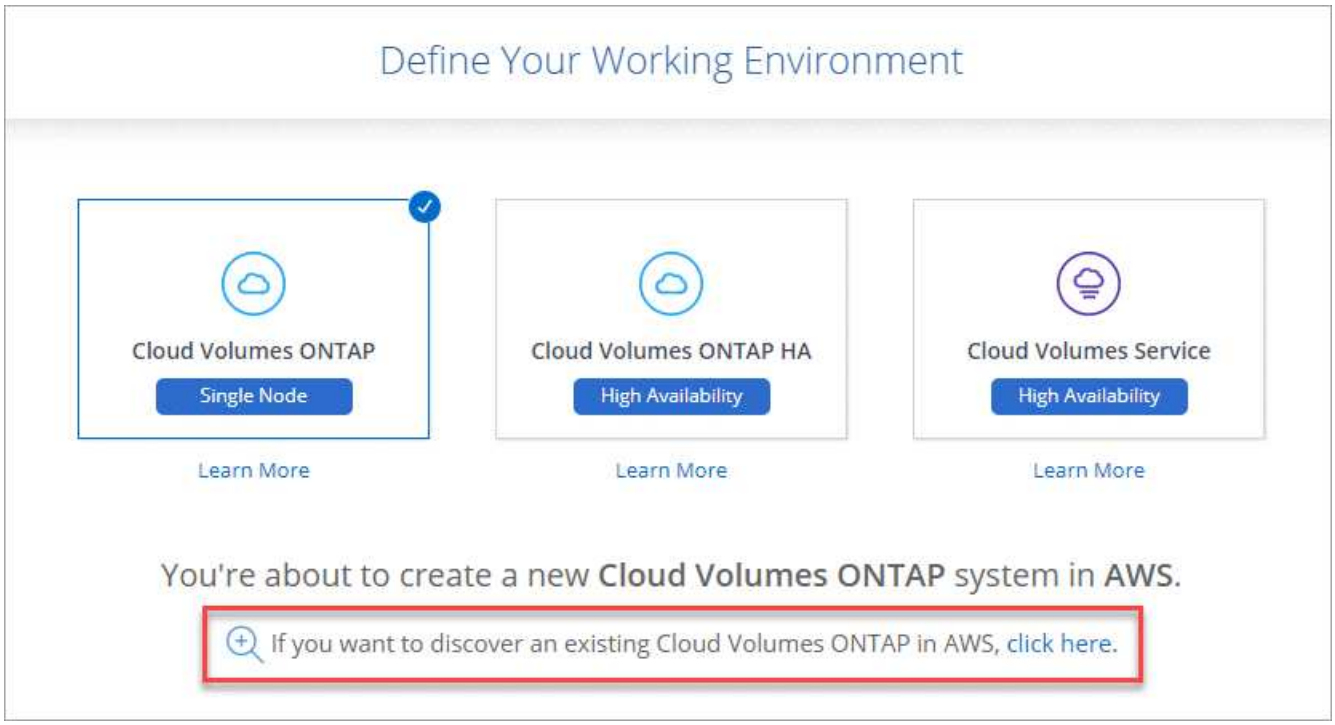
Vous pouvez découvrir et ajouter des systèmes Cloud Volumes ONTAP existants à Cloud Manager. Cette opération peut être possible si vous avez déployé un nouveau système Cloud Manager.

Avant de commencer

Vous devez connaître le mot de passe du compte d'administrateur Cloud Volumes ONTAP.

Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail**.
2. Sélectionnez le fournisseur de cloud dans lequel réside le système.
3. Choisissez le type de système Cloud Volumes ONTAP.
4. Cliquez sur le lien pour découvrir un système existant.



5. Sur la page Région, choisissez la région dans laquelle les instances sont exécutées, puis sélectionnez les instances.
6. Sur la page informations d'identification, entrez le mot de passe de l'utilisateur administrateur Cloud Volumes ONTAP, puis cliquez sur **Go**.

Résultat

Cloud Manager ajoute les instances Cloud Volumes ONTAP à l'espace de travail.

Suppression d'un environnement de travail Cloud Volumes ONTAP

Il est préférable de supprimer les systèmes Cloud Volumes ONTAP de Cloud Manager, plutôt que de la console de votre fournisseur cloud. Par exemple, si vous mettez fin à une instance Cloud Volumes ONTAP sous licence depuis AWS, vous ne pouvez pas utiliser la

clé de licence pour une autre instance. Vous devez supprimer l'environnement de travail de Cloud Manager pour libérer la licence.

Description de la tâche

Lorsque vous supprimez un environnement de travail, Cloud Manager met fin aux instances, supprime les disques et les snapshots.

> Les instances de Cloud Volumes ONTAP bénéficient d'une protection de terminaison pour empêcher la fermeture accidentelle d'AWS. Cependant, si vous arrêtez une instance Cloud Volumes ONTAP d'AWS, vous devez accéder à la console AWS CloudFormation et supprimer la pile de l'instance. Le nom de la pile est le nom de l'environnement de travail.

Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Supprimer**.
2. Saisissez le nom de l'environnement de travail, puis cliquez sur **Supprimer**.

   La suppression de l'environnement de travail peut prendre jusqu'à 5 minutes.

Informations sur le copyright

Informations sur les marques commerciales