# Documentation sur Cloud Manager et Cloud Volumes ONTAP

## Cloud Manager 3.6

NetApp
June 27, 2025

# Sommaire


Documentation sur Cloud Manager et Cloud Volumes ONTAP . . . 1
- BlueXP . . . 1
- Découvrez les nouveautés . . . 1
- Commencez . . . 1
- Automatisez avec les API . . . 1
- Connectez-vous avec vos pairs, obtenez de l'aide et trouvez plus d'informations . . . 1

Notes de mise à jour . . . 2
- Le gestionnaire Cloud . . . 2
  - Nouveautés de Cloud Manager 3.6 . . . 2
  - Problèmes connus . . . 16
  - Limites connues . . . 16

Concepts . . . 18
- Présentation de Cloud Manager et de Cloud Volumes ONTAP . . . 18
  - Le gestionnaire Cloud . . . 18
  - Cloud Volumes ONTAP . . . 18
- NetApp Cloud Central . . . 19
- Comptes et autorisations des fournisseurs cloud . . . 20
  - Comptes et autorisations AWS . . . 20
  - Comptes et autorisations Azure . . . 22
- Stockage . . . 24
  - Utilisation du stockage cloud par Cloud Volumes ONTAP . . . 24
  - Vue d'ensemble du hiérarchisation des données . . . 26
  - Gestion du stockage . . . 30
  - Stockage WORM . . . 37
- Paires haute disponibilité . . . 38
  - Paires haute disponibilité dans AWS . . . 38
  - Paires haute disponibilité dans Azure . . . 44
- L'évaluation . . . 47
- Licences . . . 47
- Sécurité . . . 48
  - Cryptage des données au repos . . . 48
  - Analyse antivirus ONTAP . . . 49
  - Protection par ransomware . . . 49
- Performance . . . 50

Pour commencer . . . 51
- Présentation du déploiement . . . 51
  - Installation de Cloud Manager . . . 51
  - Configuration de Cloud Manager . . . 51
  - Déploiement de Cloud Volumes ONTAP . . . 51
- Mise en route de Cloud Volumes ONTAP dans AWS . . . 52
- Mise en route de Cloud Volumes ONTAP dans Azure . . . 53
- Configuration de Cloud Manager . . . 54
  - Ajout de comptes de fournisseurs cloud à Cloud Manager . . . 54

Ajout de comptes du site de support NetApp à Cloud Manager . . . 64
Installation d'un certificat HTTPS pour un accès sécurisé . . . 65
Configuration des utilisateurs et des locataires . . . 66
Configuration du système AWS KMS . . . 67
Configuration réseau requise . . . 70
Configuration réseau requise pour Cloud Manager . . . 70
Configuration réseau requise pour Cloud Volumes ONTAP dans AWS . . . 73
Configuration d'une passerelle de transit AWS pour les paires HA dans plusieurs AZS . . . 80
Configuration réseau requise pour Cloud Volumes ONTAP dans Azure . . . 84
D'autres options de déploiement . . . 85
Conditions de l'hôte Cloud Manager . . . 85
Installation de Cloud Manager sur un hôte Linux existant . . . 86
Lancement de Cloud Manager à partir d'AWS Marketplace . . . 88
Déploiement de Cloud Manager à partir d'Azure Marketplace . . . 89
Déploiement de Cloud Manager dans une région Azure Government . . . 91
Installation de Cloud Manager dans une région Azure Allemagne . . . 93
Le déploiement de Cloud Volumes ONTAP . . . 95
Avant de créer des systèmes Cloud Volumes ONTAP . . . 95
Connectez-vous à Cloud Manager . . . 95
Planification de votre configuration Cloud Volumes ONTAP . . . 96
Choix d'un type de licence . . . 96
Compréhension des limites de stockage . . . 96
Dimensionnement de votre système dans AWS . . . 97
Dimensionnement du système dans Azure . . . 98
Sélection d'une vitesse d'écriture . . . 99
Choix d'un profil d'utilisation du volume . . . 99
Fiche technique d'informations sur le réseau AWS . . . 100
Fiche d'informations sur le réseau Azure . . . 101
Activation de Flash cache sur Cloud Volumes ONTAP dans AWS . . . 101
Lancement d'Cloud Volumes ONTAP dans AWS . . . 102
Lancement d'un seul système Cloud Volumes ONTAP dans AWS . . . 102
Lancement d'une paire Cloud Volumes ONTAP HA dans AWS . . . 106
Lancement d'Cloud Volumes ONTAP dans Azure . . . 111
Enregistrement des systèmes de paiement à l'utilisation . . . 116
Configuration de Cloud Volumes ONTAP . . . 116
Provisionnement du stockage . . . 119
Provisionnement du stockage . . . 119
Volumes de provisionnement . . . 119
Provisionnement des volumes sur le second nœud dans une configuration haute disponibilité . . . 121
Création d'agrégats . . . 122
Provisionnement des LUN iSCSI . . . 122
Tiering des données inactives vers un stockage objet à faible coût . . . 123
Configurations prenant en charge le tiering des données . . . 123
Exigences relatives aux données de hiérarchisation dans AWS . . . 123
Configuration requise pour le tiering des données dans Microsoft Azure . . . 124

Hiérarchisation des données sur les volumes en lecture-écriture . . . 124
Hiérarchisation des données sur les volumes de protection des données . . . 125
Modification du niveau de hiérarchisation . . . 125
Avec Cloud Volumes ONTAP comme stockage persistant pour Kubernetes . . . 126
Chiffrement de volumes avec NetApp Volume Encryption . . . 128
Gestion du stockage existant . . . 129
Gestion des volumes existants . . . 130
Gestion des agrégats existants . . . 131
Modification du serveur CIFS . . . 132
Déplacement d'un volume pour éviter les problèmes de capacité . . . 133
Provisionnement des volumes NFS depuis la vue du volume . . . 136
Passage à la vue de volume . . . 136
Création et montage de volumes NFS . . . 136
Gestion des volumes NFS . . . 139
Gestion des données dans le cloud hybride . . . 142
Détection et gestion des clusters ONTAP . . . 142
Découverte des clusters ONTAP . . . 142
Provisionnement des volumes sur des clusters ONTAP . . . 143
Réplication des données depuis et vers le cloud . . . 144
Choix d'une stratégie de réplication . . . 144
Exigences de réplication des données . . . 147
Réplication des données entre les systèmes . . . 148
Gestion des planifications et des relations de réplication des données . . . 149
Synchronisation des données vers AWS S3 . . . 151
Fonctionnement de la fonction de synchronisation vers S3 . . . 152
Intégration d'un environnement de travail au service Cloud Sync . . . 153
Gestion des relations de synchronisation des volumes . . . 153
Administration d'Cloud Volumes ONTAP . . . 154
Connexion à Cloud Volumes ONTAP . . . 154
Connexion à OnCommand System Manager . . . 154
Connexion à l'interface de ligne de commande Cloud Volumes ONTAP . . . 154
Mise à jour du logiciel Cloud Volumes ONTAP . . . 155
Présentation . . . 155
Préparation de la mise à jour du logiciel Cloud Volumes ONTAP . . . 157
Mise à niveau de Cloud Volumes ONTAP vers la dernière version . . . 158
Mise à niveau ou mise à niveau vers une version antérieure de Cloud Volumes ONTAP à l'aide d'un serveur HTTP ou FTP . . . 159
Déclassement de Cloud Volumes ONTAP à l'aide d'une image locale . . . 160
Modification des systèmes Cloud Volumes ONTAP . . . 161
Installation de fichiers de licence sur les systèmes Cloud Volumes ONTAP BYOL . . . 161
Modification du type d'instance ou de machine virtuelle pour Cloud Volumes ONTAP . . . 162
Changement entre les configurations de paiement à la demande . . . 163
Passage à une autre configuration Cloud Volumes ONTAP . . . 163
Modification du nom de la machine virtuelle de stockage . . . 164
Modification du mot de passe de Cloud Volumes ONTAP . . . 164

Modification de la MTU réseau pour les instances c4.4xlarge et c4.8xlarge . . . 164
Modification des tables de routage associées aux paires HA dans plusieurs AZS d'AWS . . . 165
Gestion de l'état du Cloud Volumes ONTAP . . . 165
Planification des arrêts automatiques de Cloud Volumes ONTAP . . . 165
Arrêt d'Cloud Volumes ONTAP . . . 166
Contrôle des coûts des ressources AWS . . . 166
Renforcer la protection contre les attaques par ransomware . . . 168
Ajout de systèmes Cloud Volumes ONTAP existants à Cloud Manager . . . 169
Suppression d'un environnement de travail Cloud Volumes ONTAP . . . 170
Administration de Cloud Manager . . . 171
Mise à jour de Cloud Manager . . . 171
Activation des mises à jour automatiques . . . 171
Mise à jour de Cloud Manager vers la dernière version . . . 171
Mise à jour de Cloud Manager avec un correctif . . . 172
Sauvegarde et restauration de Cloud Manager . . . 172
Sauvegarde de Cloud Manager . . . 173
Restauration de Cloud Manager à partir d'une sauvegarde . . . 173
Suppression des environnements de travail Cloud Volumes ONTAP . . . 173
Modification des comptes utilisateur . . . 174
Configuration de Cloud Manager pour utiliser un serveur proxy . . . 175
Renouvellement du certificat HTTPS de Cloud Manager . . . 175
Désinstallation de Cloud Manager . . . 176
API et automatisation . . . 177
Exemples d'automatisation pour l'infrastructure-as-code . . . 177
Référence . . . 178
Questions les plus fréquemment posées : intégrer Cloud Manager avec NetApp Cloud Central . . . 178
Qu'est-ce que NetApp Cloud Central ? . . . 178
Pourquoi NetApp intègre-t-il mon système Cloud Manager avec Cloud Central ? . . . 178
Que se passe-t-il pendant le processus d'intégration ? . . . 178
Comment fonctionne l'authentification centralisée des utilisateurs ? . . . 178
Dois-je m'inscrire à un compte utilisateur Cloud Central ? . . . 178
Et si j'ai déjà un compte utilisateur Cloud Central ? . . . 178
Que se passe-t-il si mon système Cloud Manager dispose de plusieurs comptes utilisateur ? . . . 178
Que se passe-t-il si j'ai un compte utilisateur qui utilise la même adresse e-mail sur plusieurs systèmes Cloud Manager ? . . . 179
Que se passe-t-il si mon compte d'utilisateur local utilise une adresse e-mail non valide ? . . . 179
Et si j'ai des scripts d'automatisation pour les API Cloud Manager ? . . . 179
Que se passe-t-il si mon système Cloud Manager utilise LDAP ? . . . 179
Est-ce que j'ai installé mon système Cloud Manager ? . . . 179
Règles de groupe de sécurité pour AWS . . . 179
Règles pour Cloud Manager . . . 179
Règles pour Cloud Volumes ONTAP . . . 181
Règles pour le groupe de sécurité externe du médiateur de haute disponibilité . . . 185
Règles pour le groupe de sécurité interne du médiateur de haute disponibilité . . . 186
Règles de groupe de sécurité pour Azure . . . 187

Règles pour Cloud Manager . . . 187
Règles pour Cloud Volumes ONTAP . . . 189
Autorisations AWS et Azure pour Cloud Manager . . . 193
Ce que fait Cloud Manager avec les autorisations AWS . . . 193
Ce que fait Cloud Manager avec les autorisations Azure . . . 195
Configurations par défaut . . . 197
Configuration par défaut de Cloud Manager sous Linux . . . 198
Configuration par défaut pour Cloud Volumes ONTAP . . . 198
Données de démarrage et de racine pour Cloud Volumes ONTAP . . . 199
Rôles utilisateur . . . 200
Où obtenir de l’aide et trouver plus d’informations . . . 201
Mentions légales . . . 203
Droits d’auteur . . . 203
Marques déposées . . . 203
Brevets . . . 203
Politique de confidentialité . . . 203
Source ouverte . . . 203

# Documentation sur Cloud Manager et Cloud Volumes ONTAP

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

## BlueXP

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

"Consultez la documentation BlueXP"

## Découvrez les nouveautés

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

## Commencez

- "Commencez dans AWS"
- "Commencez à Azure"
- "Recherchez les configurations prises en charge pour Cloud Volumes ONTAP"
- "Passez en revue les exigences de réseau détaillées pour Cloud Manager"
- "Passez en revue les exigences de réseau détaillées pour Cloud Volumes ONTAP pour AWS"
- "Passez en revue les exigences de réseau détaillées pour Cloud Volumes ONTAP pour Azure"
- "Planifiez votre configuration Cloud Volumes ONTAP"

## Automatisez avec les API

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

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

- "Communauté NetApp : services de données cloud"
- "Prise en charge de NetApp Cloud Volumes ONTAP"
- "Où obtenir de l'aide et trouver plus d'informations"

# Notes de mise à jour

## Le gestionnaire Cloud

### Nouveautés de Cloud Manager 3.6

OnCOMMAND Cloud Manager introduit généralement une nouvelle version chaque mois pour vous apporter de nouvelles fonctionnalités, améliorations et corrections de bogues.

Vous recherchez une version précédente ?"Nouveautés de la version 3.5"
"Nouveautés de la version 3.4"

#### Prise en charge de l'environnement AWS C2S (2 mai 2019)

Cloud Volumes ONTAP 9.5 et Cloud Manager 3.6.4 sont désormais disponibles pour les États-Unis Intelligence Community (IC) via l'environnement AWS commercial Cloud Services (C2S). Vous pouvez déployer des paires HA et des systèmes à un seul nœud dans C2S.

"Guide d'aide à la vente des environnements de services clouds AWS commercial"

#### Cloud Manager 3.6.6 (1er mai 2019)

- Prise en charge des disques de 6 To dans AWS
- Prise en charge de nouvelles tailles de disques avec des systèmes à un seul nœud dans Azure
- Prise en charge des SSD standard avec des systèmes à un seul nœud dans Azure
- Découverte automatique des clusters Kubernetes créés avec NetApp Kubernetes Service
- Possibilité de configurer un serveur NTP

##### Prise en charge des disques de 6 To dans AWS

Vous pouvez désormais choisir une taille de disque EBS de 6 To avec Cloud Volumes ONTAP pour AWS. Avec le récent "Performance accrue des SSD polyvalents", Un disque de 6 To est désormais le meilleur choix pour des performances maximales.

Cette modification est prise en charge par Cloud Volumes ONTAP 9.5, 9.4 et 9.3.

##### Prise en charge de nouvelles tailles de disques avec des systèmes à un seul nœud dans Azure

Vous pouvez désormais utiliser des disques de 8 To, 16 To et 32 To avec des systèmes à un seul nœud dans Azure. Grâce aux capacités de disque améliorées, vous pouvez atteindre jusqu'à 368 To de capacité système sur des disques seuls, en cas d'utilisation des licences Premium ou BYOL.

Cette modification est prise en charge par Cloud Volumes ONTAP 9.5, 9.4 et 9.3.

##### Prise en charge des SSD standard avec des systèmes à un seul nœud dans Azure

Les disques gérés SSD standard sont désormais pris en charge par les systèmes à un seul nœud dans Azure. Ces disques offrent un niveau de performances entre les SSD Premium et les disques HDD standard.

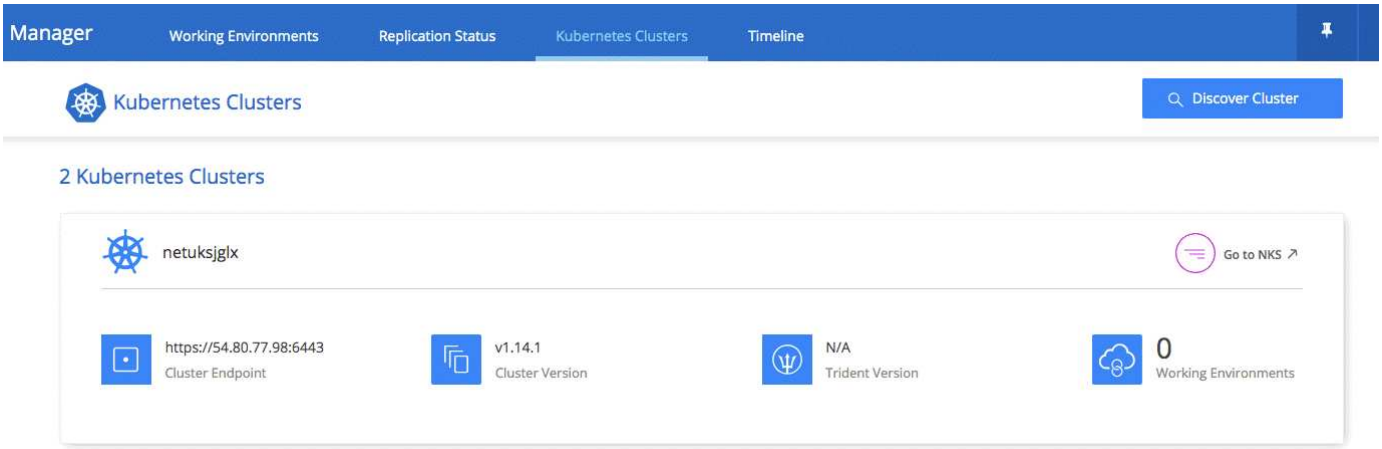
Cette modification est prise en charge par Cloud Volumes ONTAP 9.5, 9.4 et 9.3.

"En savoir plus sur les SSD standard".

#### Découverte automatique des clusters Kubernetes créés avec NetApp Kubernetes Service

Cloud Manager peut désormais détecter automatiquement les clusters Kubernetes que vous déployez à l'aide de NetApp Kubernetes Service. Cela vous permet de connecter les clusters Kubernetes à vos systèmes Cloud Volumes ONTAP, de sorte que vous puissiez les utiliser comme stockage persistant pour vos conteneurs.

L'image suivante montre un cluster Kubernetes détecté automatiquement. Le lien « Go to NKS » vous amène directement au service NetApp Kubernetes.



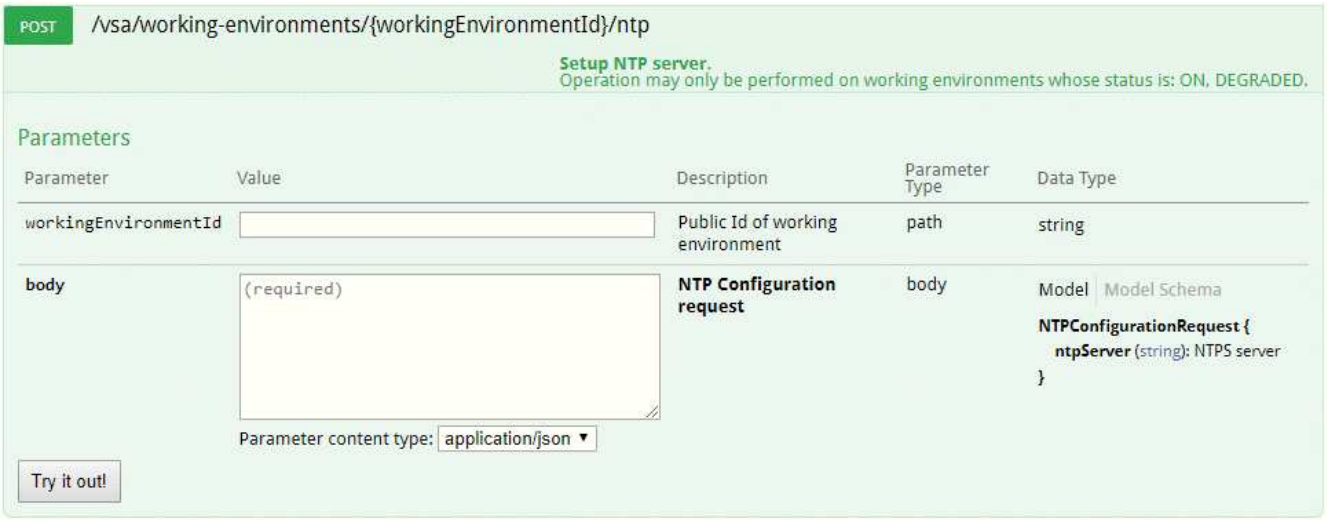

"Découvrez comment connecter vos environnements de travail aux clusters Kubernetes".

#### Possibilité de configurer un serveur NTP

Vous pouvez désormais configurer Cloud Volumes ONTAP de manière à utiliser un serveur NTP (Network Time Protocol). 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.

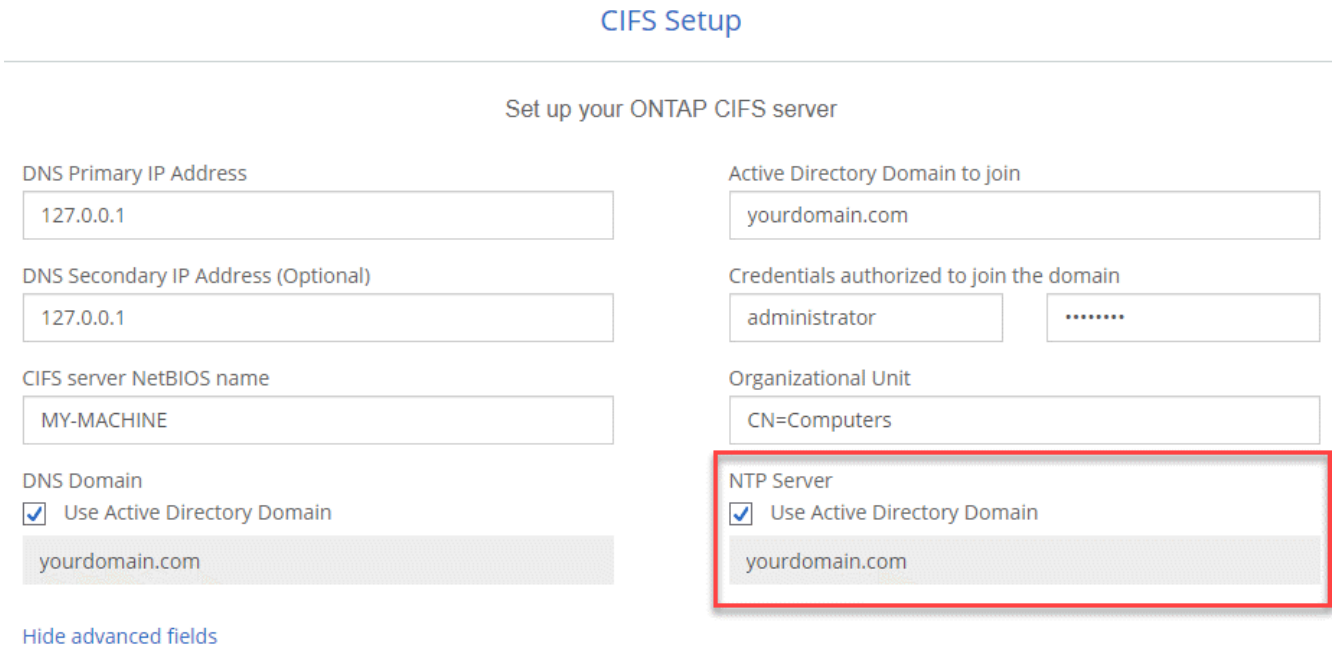
Spécifiez un serveur NTP via l'API Cloud Manager ou depuis l'interface utilisateur lors de la configuration d'un serveur CIFS :

- Le "API Cloud Manager" Vous permet de spécifier n'importe quelle adresse pour le serveur NTP. Voici l'API d'un système à un seul nœud dans AWS :



- Lors de la configuration d'un serveur CIFS, l'interface utilisateur de Cloud Manager vous permet de spécifier un serveur NTP qui utilise le domaine Active Directory. Si vous devez utiliser une autre adresse, vous devez utiliser l'API.

  L'image suivante montre le champ serveur NTP, qui est disponible lors de la configuration de CIFS.




### Cloud Manager 3.6.5 (2 avril 2019)

Cloud Manager 3.6.5 comprend plusieurs améliorations :

- Améliorations de Kubernetes
- Les comptes du site de support NetApp sont désormais gérés au niveau du système
- Les passerelles de transport AWS peuvent permettre l'accès aux adresses IP flottantes
- Les groupes de ressources Azure sont maintenant verrouillés
- NFS 4 et NFS 4.1 sont désormais activés par défaut
- Une nouvelle API vous permet de supprimer les copies Snapshot ONTAP

#### Améliorations de Kubernetes

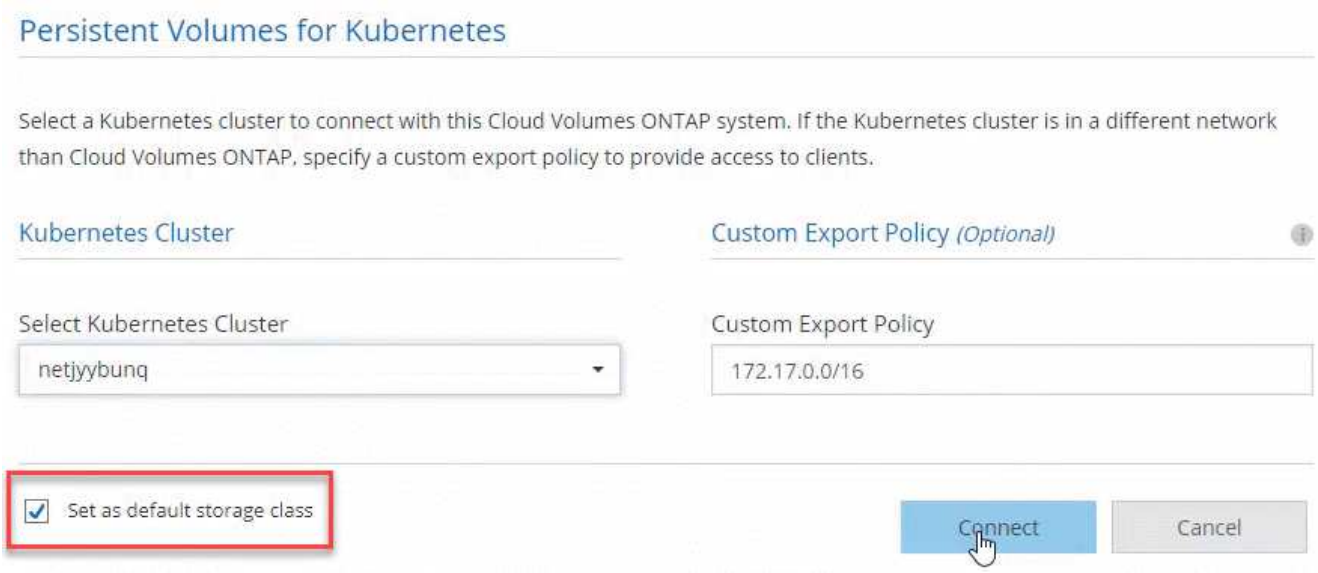
Nous avons apporté quelques améliorations qui vous permettent d'utiliser Cloud Volumes ONTAP en tant que stockage persistant pour les conteneurs :

- Vous pouvez à présent ajouter plusieurs clusters Kubernetes à Cloud Manager.

  Cela vous permet de connecter différents clusters à différents systèmes Cloud Volumes ONTAP et à plusieurs clusters sur le même système Cloud Volumes ONTAP.

- Lorsque vous connectez un cluster, vous pouvez désormais définir Cloud Volumes ONTAP comme classe de stockage par défaut pour le cluster Kubernetes.

  Lorsqu'un utilisateur crée un volume persistant, le cluster Kubernetes peut utiliser Cloud Volumes ONTAP comme stockage back-end par défaut :



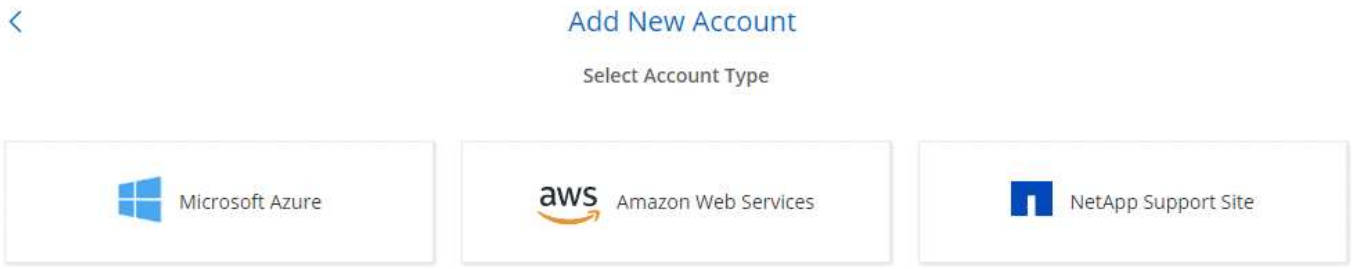

- Nous avons modifié la façon dont Cloud Manager nomme les classes de stockage Kubernetes pour les identifier plus facilement :
  - **netapp-fichier** : pour lier un volume persistant à un système Cloud Volumes ONTAP à un seul nœud
  - **NetApp-file-redondant** : pour relier un volume persistant à une paire HA Cloud Volumes ONTAP
- La version de NetApp Trident que Cloud Manager installe a été mise à jour vers la dernière version.

"Découvrez comment utiliser Cloud Volumes ONTAP comme stockage persistant pour Kubernetes".

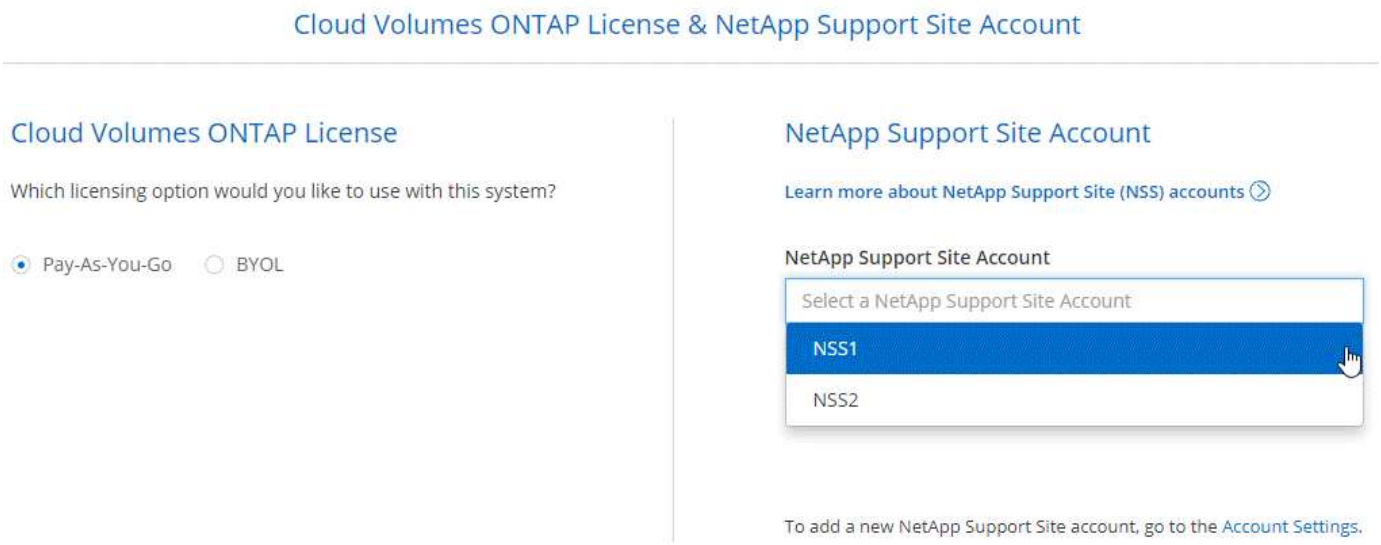
#### Les comptes du site de support NetApp sont désormais gérés au niveau du système

La gestion des comptes du site de support NetApp dans Cloud Manager est désormais plus simple.

Dans les versions précédentes, vous aviez besoin de lier un compte sur le site de support NetApp à un locataire spécifique. Les comptes sont désormais gérés au niveau du système Cloud Manager, au même endroit que vous gérez les comptes des fournisseurs cloud. Vous pouvez choisir entre plusieurs comptes du site de support NetApp lors de l'enregistrement de vos systèmes Cloud Volumes ONTAP.




Lorsque vous créez un nouvel environnement de travail, il vous suffit de sélectionner le compte du site de support NetApp pour enregistrer le système Cloud Volumes ONTAP avec :




Lorsque Cloud Manager est mis à jour vers 3.6.5, il ajoute automatiquement des comptes sur le site de support NetApp si vous aviez déjà associé des locataires avec un compte.

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

#### Les passerelles de transport AWS peuvent permettre l'accès aux adresses IP flottantes

Une paire haute disponibilité dans plusieurs zones de disponibilité AWS utilise *des adresses IP flottantes* pour l'accès aux données NAS et pour les interfaces de gestion. Jusqu'à présent, ces adresses IP flottantes n'étaient pas accessibles en dehors du VPC où réside la paire haute disponibilité.

Nous avons vérifié que vous pouvez utiliser un "Passerelle de transit AWS" Pour permettre l'accès aux adresses IP flottantes depuis l'extérieur du VPC. Cela signifie que les outils de gestion NetApp et les clients NAS qui se trouvent en dehors du VPC peuvent accéder aux adresses IP flottantes et tirer parti du basculement automatique.

"Découvrez comment configurer une passerelle de transit AWS pour les paires haute disponibilité dans plusieurs AZS".

#### Les groupes de ressources Azure sont maintenant verrouillés

Cloud Manager verrouille désormais les groupes de ressources Cloud Volumes ONTAP dans Azure lors de leur création. Le verrouillage des groupes de ressources empêche les utilisateurs de supprimer ou de modifier accidentellement des ressources critiques.

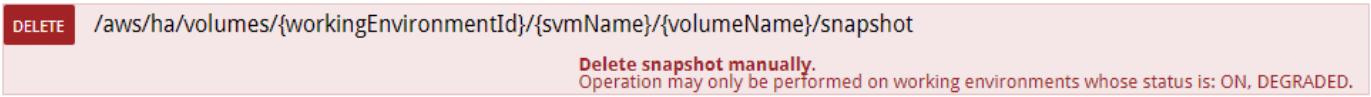
#### NFS 4 et NFS 4.1 sont désormais activés par défaut

Cloud Manager active désormais les protocoles NFS 4 et NFS 4.1 sur chaque nouveau système Cloud Volumes ONTAP créé. Cette modification vous fait gagner du temps car vous n'avez plus besoin d'activer ces protocoles vous-même manuellement.

#### Une nouvelle API vous permet de supprimer les copies Snapshot ONTAP

Vous pouvez désormais supprimer des copies Snapshot de volumes en lecture/écriture via un appel d'API Cloud Manager.

Voici un exemple de l'appel d'API pour un système HA dans AWS :




Des appels d'API similaires sont disponibles pour les systèmes à un seul nœud dans AWS, et pour les systèmes à un seul nœud et HA dans Azure.

"Guide du développeur de l'API OnCOMMAND Cloud Manager"

### Mise à jour de Cloud Manager 3.6.4 (18 mars 2019)

Cloud Manager a été mis à jour pour prendre en charge la version 9.5 de correctif P1 pour Cloud Volumes ONTAP. Avec cette version de correctif, les paires haute disponibilité dans Azure sont maintenant généralement disponibles (GA).

Voir la "Notes de version de Cloud Volumes ONTAP 9.5" Pour plus d'informations, notamment sur la prise en charge des paires haute disponibilité dans la région Azure.

### Cloud Manager 3.6.4 (3 mars 2019)

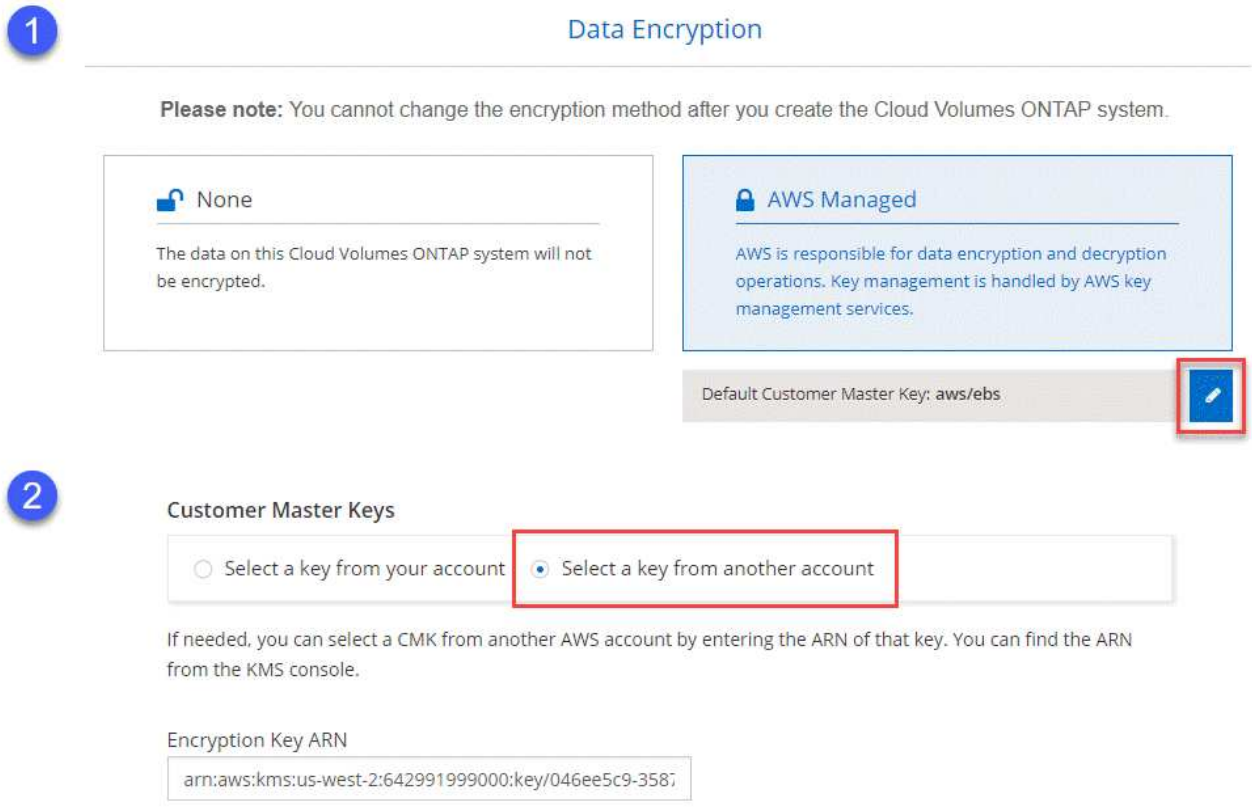
Cloud Manager 3.6.4 comprend plusieurs améliorations :

- Chiffrement géré par AWS avec une clé d'un autre compte
- Restauration des disques défaillants
- Les comptes de stockage Azure sont activés pour HTTPS lors du Tiering des données dans les conteneurs de objets blob

#### Chiffrement géré par AWS avec une clé d'un autre compte

Lorsque vous lancez un système Cloud Volumes ONTAP dans AWS, vous pouvez maintenant activer "Chiffrement géré par AWS" Utilisation d'une clé maître client (CMK) d'un autre compte utilisateur AWS.

Les images suivantes montrent comment sélectionner l'option lors de la création d'un nouvel environnement de travail :




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

**Restauration des disques défaillants**

Cloud Manager tente désormais de récupérer les disques défectueux à partir des systèmes Cloud Volumes ONTAP. Les tentatives réussies sont indiquées dans les rapports de notification par e-mail. Voici un exemple de notification :


Vous pouvez activer les rapports de notification en modifiant votre compte utilisateur.

**Les comptes de stockage Azure sont activés pour HTTPS lors du Tiering des données dans les conteneurs de objets blob**

Lorsque vous configurez un système Cloud Volumes ONTAP pour hiérarchiser les données inactives vers un conteneur Azure Blob, Cloud Manager crée un compte de stockage Azure pour ce conteneur. À partir de cette version, Cloud Manager permet désormais la création de nouveaux comptes de stockage avec transfert sécurisé (HTTPS). Les comptes de stockage existants continuent d'utiliser HTTP.

### Cloud Manager 3.6.3 (4 février 2019)

Cloud Manager 3.6.3 comprend plusieurs améliorations :

- Prise en charge de Cloud Volumes ONTAP 9.5 GA
- Limite de capacité de 368 To pour toutes les configurations Premium et BYOL
- Prise en charge des nouvelles régions AWS
- Prise en charge du Tiering intelligent S3
- Possibilité de désactiver le Tiering des données sur l'agrégat initial
- Type d'instance EC2 recommandé maintenant t3.medium pour Cloud Manager
- Report des arrêts programmés pendant les transferts de données

#### Prise en charge de Cloud Volumes ONTAP 9.5 GA

Cloud Manager prend désormais en charge la version GA d'Cloud Volumes ONTAP 9.5, dont la disponibilité générale est désormais prise en charge. Notamment la prise en charge des instances M5 et R5 dans AWS. Pour plus d'informations sur la version 9.5, consultez le "Notes de version de Cloud Volumes ONTAP 9.5".

#### Limite de capacité de 368 To pour toutes les configurations Premium et BYOL

La limite de capacité système pour Cloud Volumes ONTAP Premium et BYOL est désormais de 368 To sur toutes les configurations : un seul nœud et une haute disponibilité, à la fois sur AWS et Azure. Cette modification s'applique à Cloud Volumes ONTAP 9.5, 9.4 et 9.3 (AWS uniquement avec 9.3).

Pour certaines configurations, les limites de disque vous empêchent d'atteindre la limite de capacité de 368 To en utilisant uniquement des disques. Dans ce cas, vous pouvez atteindre la limite de capacité de 368 To de "tiering des données inactives vers le stockage objet". Par exemple, un système à un seul nœud dans Azure peut disposer d'une capacité sur disque de 252 To, ce qui permet d'atteindre jusqu'à 116 To de données inactives dans le stockage Azure Blob.

Pour plus d'informations sur les limites de disque, reportez-vous à la section limites de stockage dans le "Notes de version de Cloud Volumes ONTAP".

#### Prise en charge des nouvelles régions AWS

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

- Europe (Stockholm)

  Systèmes à un seul nœud uniquement. Les paires HAUTE DISPONIBILITÉ ne sont pas prises en charge pour le moment.

- GovCloud (USA-est)

  Cette fonctionnalité vient en outre du support pour la région AWS GovCloud (USA-West).

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

#### Prise en charge du Tiering intelligent S3

Lorsque vous activez le Tiering des données dans AWS, Cloud Volumes ONTAP transfère par défaut les données inactives vers la classe de stockage S3 Standard. Vous pouvez désormais modifier le niveau de

hiérarchisation en classe de stockage *Intelligent Tiering*. Cette classe de stockage optimise les coûts de stockage en déplaçant les données entre deux niveaux au fur et à mesure de l'évolution des modèles d'accès aux données. L'un des niveaux est destiné aux accès fréquents et l'autre à des accès rares.

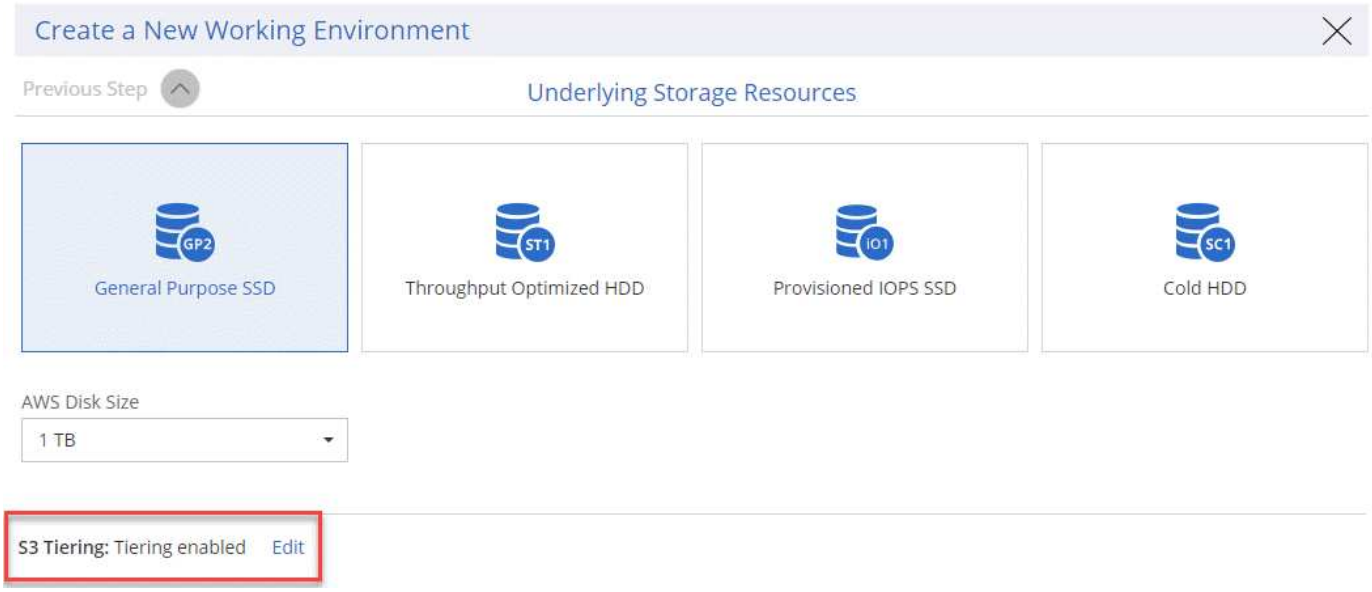
Tout comme dans les versions précédentes, vous pouvez également utiliser le niveau Standard-Infrequent Access et le niveau One zone-Infrequent Access.

"En savoir plus sur le Tiering des données" et "découvrez comment changer la classe de stockage".

#### Possibilité de désactiver le Tiering des données sur l'agrégat initial

Dans les versions précédentes, Cloud Manager avait automatiquement activé le Tiering des données sur l'agrégat Cloud Volumes ONTAP initial. Vous pouvez désormais choisir de désactiver le Tiering des données sur cet agrégat initial. (Vous pouvez également activer ou désactiver le Tiering des données sur les agrégats suivants.)

Cette nouvelle option est disponible lors du choix des ressources de stockage sous-jacentes. L'image suivante montre un exemple lors du lancement d'un système dans AWS :




#### Type d'instance EC2 recommandé maintenant t3.medium pour Cloud Manager

Le type d'instance de Cloud Manager est désormais t3.medium lors du déploiement de Cloud Manager dans AWS à partir de NetApp Cloud Central. Il s'agit également du type d'instance recommandé dans AWS Marketplace. Cette modification permet la prise en charge dans les dernières régions AWS et réduit les coûts d'instance. Le type d'instance recommandé était auparavant t2.medium, qui est toujours pris en charge.

#### Report des arrêts programmés pendant les transferts de données

Si vous avez planifié un arrêt automatique de votre système Cloud Volumes ONTAP, Cloud Manager reporte à l'arrêt automatique du système si un transfert de données actif est en cours. Cloud Manager arrête le système une fois le transfert terminé.

### Cloud Manager 3.6.2 (2 janvier 2019)

Cloud Manager 3.6.2 inclut de nouvelles fonctionnalités et améliorations.

- AWS répartit le groupe de placement pour Cloud Volumes ONTAP HA en une seule zone de disponibilité
- Protection par ransomware
- Nouvelles règles de réplication des données
- Contrôle d'accès de volume pour Kubernetes

#### AWS répartit le groupe de placement pour Cloud Volumes ONTAP HA en une seule zone de disponibilité

Lorsque vous déployez Cloud Volumes ONTAP HA dans une seule zone de disponibilité AWS, Cloud Manager crée désormais 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.

Cloud Manager requiert de nouvelles autorisations pour cette fonctionnalité. Assurez-vous que la politique IAM qui fournit les autorisations à Cloud Manager inclut les actions suivantes :

```
"ec2:CreatePlacementGroup",
"ec2:DeletePlacementGroup"
```

Vous trouverez la liste complète des autorisations requises dans le "Dernières règles AWS pour Cloud Manager".

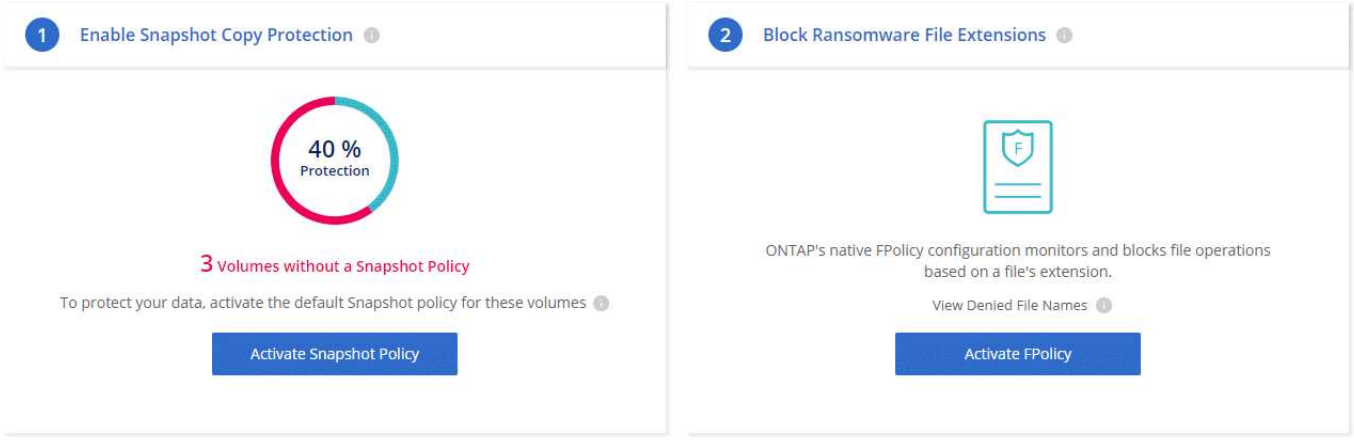
#### Protection par ransomware

Les attaques par ransomware peuvent coûter du temps, des ressources et de la réputation à l'entreprise. Cloud Manager vous permet désormais 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".

#### Nouvelles règles de réplication des données

Cloud Manager inclut cinq nouvelles règles de réplication des données que vous pouvez utiliser pour la protection des données.

Trois stratégies configurent la reprise après incident et la conservation à long terme des sauvegardes sur le même volume de destination. Chaque règle offre une période de conservation différente :

- Miroir et sauvegarde (durée de conservation de 7 ans)
- Mise en miroir et sauvegarde (conservation sur 7 ans avec davantage de sauvegardes hebdomadaires)
- Miroir et sauvegarde (conservation mensuelle d'un an)

Les règles restantes offrent davantage d'options pour la conservation à long terme des sauvegardes :

- Sauvegarde (conservation d'un mois)
- Sauvegarde (conservation d'une semaine)

Il vous suffit de glisser-déposer un environnement de travail pour sélectionner l'une des nouvelles stratégies.

#### Contrôle d'accès de volume pour Kubernetes

Vous pouvez maintenant configurer l'export policy pour les volumes persistants Kubernetes. La export policy peut activer l'accès aux clients si le cluster Kubernetes se trouve dans un réseau différent de celui du système Cloud Volumes ONTAP.

Vous pouvez configurer l'export policy lorsque vous connectez un environnement de travail à un cluster Kubernetes et en modifiant un volume existant.

### Cloud Manager 3.6.1 (4 décembre 2018)

Cloud Manager 3.6.1 inclut de nouvelles fonctionnalités et améliorations.

- Prise en charge d'Cloud Volumes ONTAP 9.5 dans Azure
- Comptes fournisseurs cloud
- Améliorations apportées au rapport sur les coûts AWS
- Prise en charge des nouvelles régions Azure

#### Prise en charge d'Cloud Volumes ONTAP 9.5 dans Azure

Cloud Manager prend désormais en charge Cloud Volumes ONTAP 9.5 dans Microsoft Azure, avec un aperçu des paires haute disponibilité. Vous pouvez demander une licence de présentation pour une paire Azure HA en nous contactant à l'adresse ng-Cloud-Volume-ONTAP-preview@netapp.com.

Pour plus d'informations sur la version 9.5, consultez le "Notes de version de Cloud Volumes ONTAP 9.5".

### Nouvelles autorisations Azure requises pour Cloud Volumes ONTAP 9.5

Cloud Manager requiert de nouvelles autorisations Azure pour ses principales fonctionnalités de la version Cloud Volumes ONTAP 9.5. Pour vous assurer que Cloud Manager peut déployer et gérer les systèmes Cloud Volumes ONTAP 9.5, il est conseillé de mettre à jour votre politique Cloud Manager en ajoutant les autorisations suivantes :

```
"Microsoft.Network/loadBalancers/read",
"Microsoft.Network/loadBalancers/write",
"Microsoft.Network/loadBalancers/delete",
"Microsoft.Network/loadBalancers/backendAddressPools/read",
"Microsoft.Network/loadBalancers/backendAddressPools/join/action",
"Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
"Microsoft.Network/loadBalancers/loadBalancingRules/read",
"Microsoft.Network/loadBalancers/probes/read",
"Microsoft.Network/loadBalancers/probes/join/action",
"Microsoft.Network/routeTables/join/action"
"Microsoft.Authorization/roleDefinitions/write",
"Microsoft.Authorization/roleAssignments/write",
"Microsoft.Web/sites/*"
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/usages/read",
```

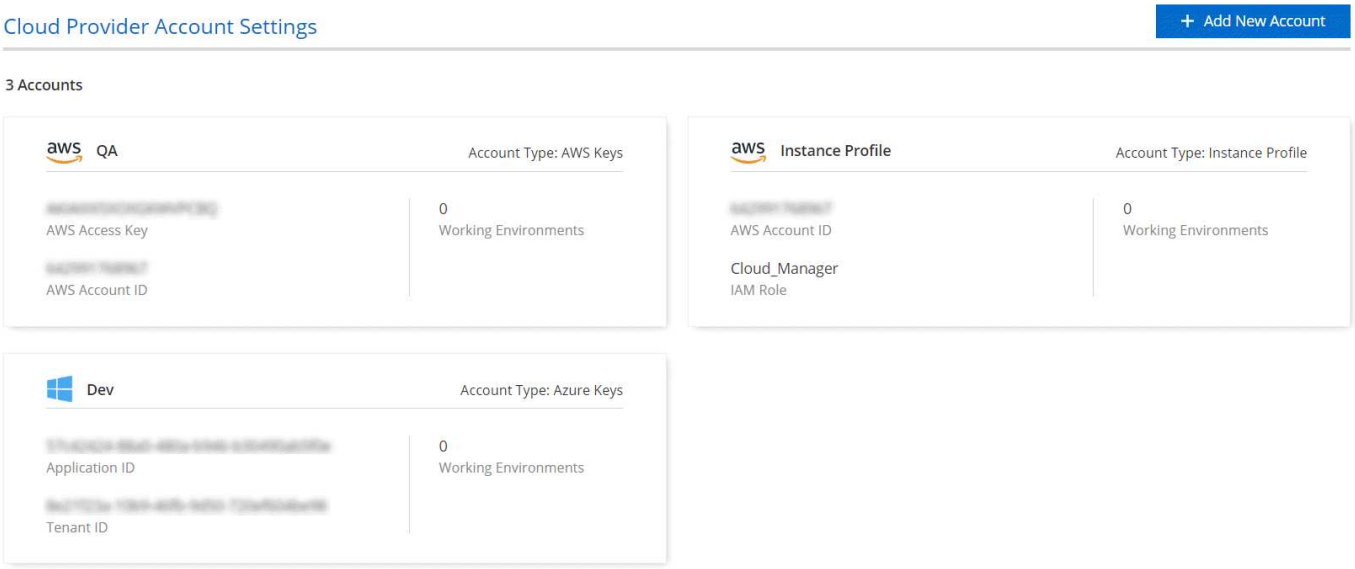
Vous trouverez la liste complète des autorisations requises dans le "Dernières règles Azure pour Cloud Manager".

"Découvrez comment Cloud Manager utilise ces autorisations".

#### Comptes fournisseurs cloud

Il est désormais plus simple de gérer plusieurs comptes AWS et Azure dans Cloud Manager via Cloud Provider Accounts.

Dans les versions précédentes, vous aviez besoin de spécifier les autorisations de fournisseur de cloud pour chaque compte utilisateur Cloud Manager. Les autorisations sont désormais gérées au niveau du système Cloud Manager à l'aide de Cloud Provider Accounts.




Lorsque vous créez un nouvel environnement de travail, il vous suffit de sélectionner le compte dans lequel vous voulez déployer le système Cloud Volumes ONTAP :


Lorsque vous passez à la version 3.6.1, Cloud Manager crée automatiquement des comptes fournisseurs de services cloud pour vous, en fonction de votre configuration actuelle. Si vous avez des scripts, la rétrocompatibilité est en place, aucune interruption.

- "Découvrez comment fonctionnent les comptes et les autorisations des fournisseurs de services clouds"
- "Découvrez comment configurer et ajouter des comptes de fournisseurs de services clouds à Cloud Manager"

**Améliorations apportées au rapport sur les coûts AWS**

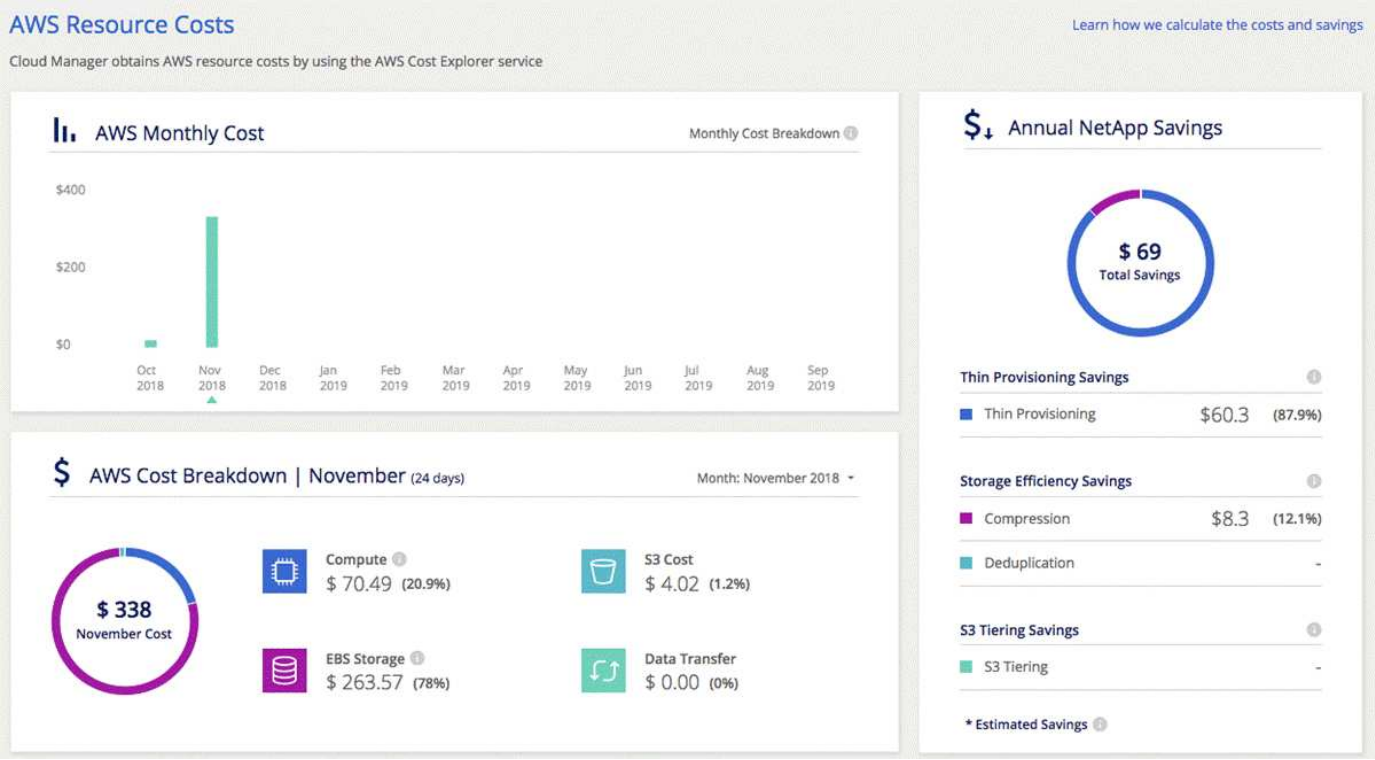
Le rapport sur les coûts d'AWS fournit maintenant plus d'informations et est plus facile à configurer.

- Ce rapport identifie les coûts mensuels associés aux ressources en cours d'exécution de Cloud Volumes ONTAP dans AWS. Vous pouvez afficher les coûts mensuels pour le calcul, le stockage EBS (y compris les snapshots EBS), le stockage S3 et le transfert des données.
- Le rapport présente les économies réalisables avec le Tiering des données inactives vers S3.
- Nous avons également simplifié la façon dont Cloud Manager obtient les données de coût sur AWS.

  Cloud Manager n'a plus besoin d'accéder aux rapports de facturation que vous stockez dans un compartiment S3. Cloud Manager utilise plutôt l'API de l'explorateur de coûts. Il vous suffit de vous assurer 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 fournie par NetApp". Les nouveaux systèmes déployés à partir de NetApp Cloud Central incluent automatiquement ces autorisations.




#### Prise en charge des nouvelles régions Azure

Vous pouvez désormais déployer Cloud Manager et Cloud Volumes ONTAP dans la région France Central.

### Cloud Manager 3.6 (4 novembre 2018)

Cloud Manager 3.6 inclut une nouvelle fonctionnalité.

#### Utilisation de Cloud Volumes ONTAP en tant que stockage persistant pour un cluster Kubernetes

Cloud Manager peut désormais automatiser le déploiement de "NetApp Trident" Sur un seul cluster Kubernetes, vous pouvez utiliser Cloud Volumes ONTAP comme stockage persistant pour les conteneurs. Les utilisateurs peuvent ensuite demander et gérer des volumes persistants à l'aide d'interfaces et de constructions natives Kubernetes, tout en tirant parti des fonctionnalités avancées de gestion des données d'ONTAP, sans en connaître l'existence.

"Découvrez comment connecter des systèmes Cloud Volumes ONTAP à un cluster Kubernetes"

## Problèmes connus

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

Cette version de Cloud Manager ne présente aucun problème connu.

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

## Limites connues

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

#### Cloud Manager ne prend pas en charge les volumes FlexGroup

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

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

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

#### Limites de la région AWS GovCloud (US)

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

#### Limites de la vue 3D

- La vue en volume n'est pas prise en charge dans la région AWS GovCloud (États-Unis), dans l'environnement AWS Commercial Cloud Services et dans Microsoft Azure.
- La vue Volume vous permet de créer des volumes NFS uniquement.
- Cloud Manager ne lance pas les instances Cloud Volumes ONTAP BYOL dans Volume View.

#### Cloud Manager ne configure pas les volumes iSCSI

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

### Limitation de la machine virtuelle de stockage (SVM)

Cloud Volumes ONTAP prend en charge un SVM de service de données et un ou plusieurs SVM utilisés pour la reprise après incident.

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

# Concepts

## Présentation de Cloud Manager et de Cloud Volumes ONTAP

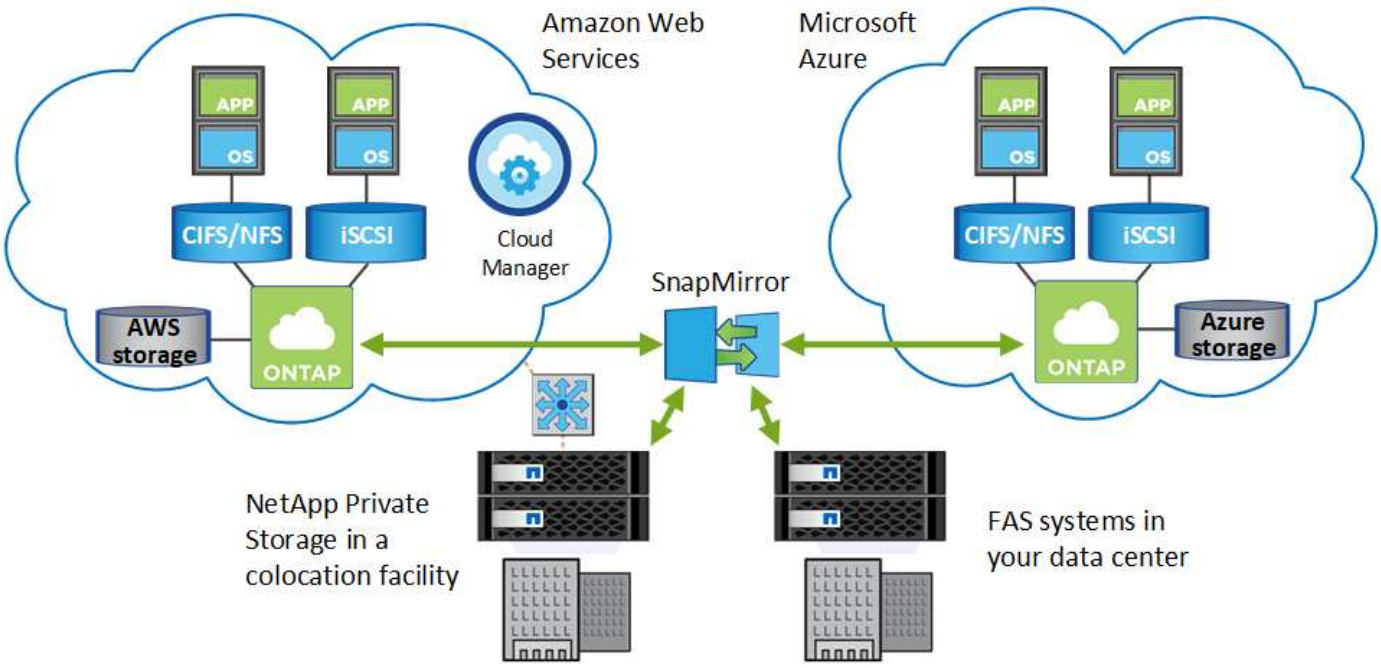
OnCOMMAND Cloud Manager vous permet de déployer Cloud Volumes ONTAP, qui offre des fonctionnalités d'entreprise pour votre stockage cloud, et de répliquer facilement des données sur des clouds hybrides basés sur NetApp.

### Le gestionnaire Cloud

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

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

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




"En savoir plus sur Cloud Manager"

### Cloud Volumes ONTAP

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

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

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

Les licences pour fonctionnalités ONTAP sont incluses avec Cloud Volumes ONTAP, à l'exception de NetApp Volume Encryption.

"Afficher les configurations Cloud Volumes ONTAP prises en charge"

"En savoir plus sur Cloud Volumes ONTAP"

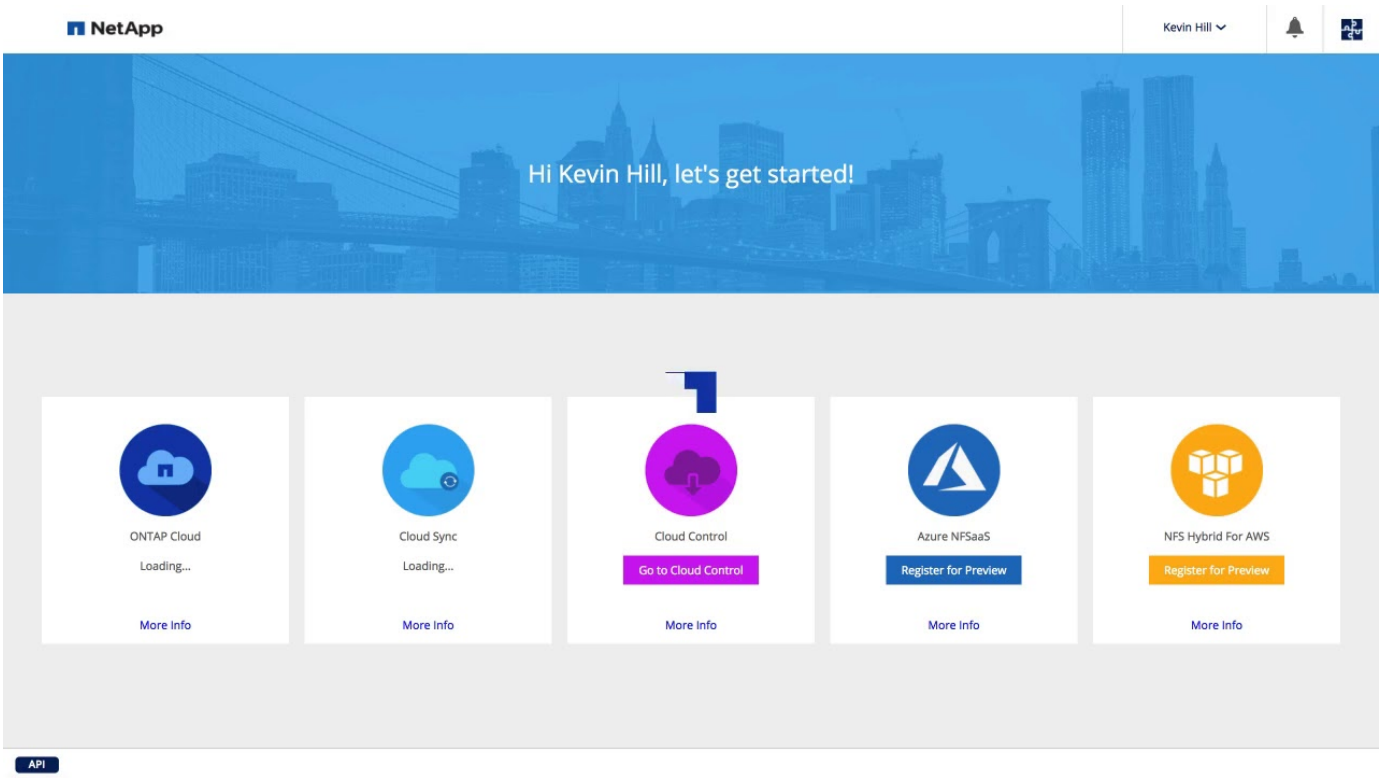
# NetApp Cloud Central

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

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

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

La vidéo suivante présente NetApp Cloud Central :




# Comptes et autorisations des fournisseurs cloud

Cloud Manager vous permet de choisir le *compte fournisseur cloud* où vous voulez déployer un système Cloud Volumes ONTAP. Avant d'ajouter les comptes à Cloud Manager, il est important de connaître les conditions d'autorisation requises.

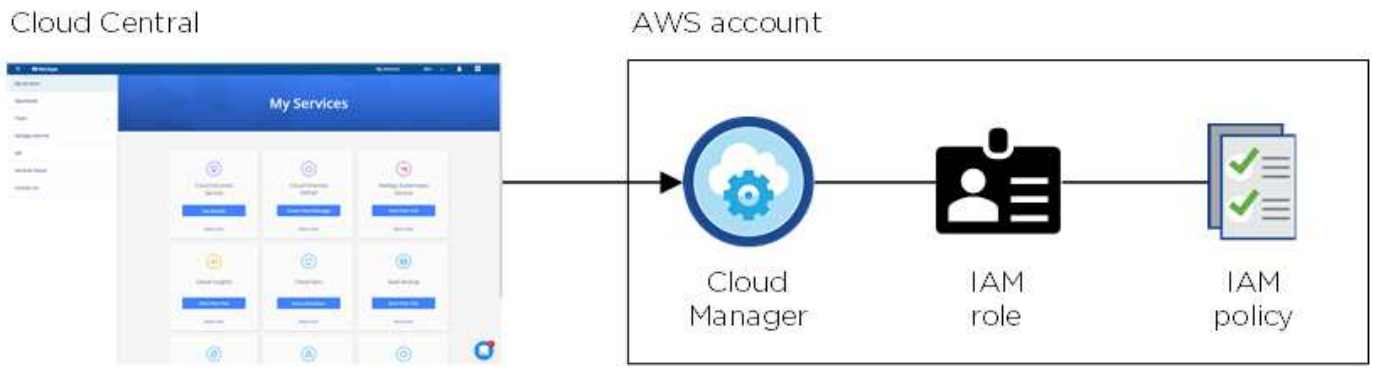
## Comptes et autorisations AWS

Vous pouvez déployer tous les systèmes Cloud Volumes ONTAP sur le compte AWS initial, ou configurer d'autres comptes.

### Compte AWS initial

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

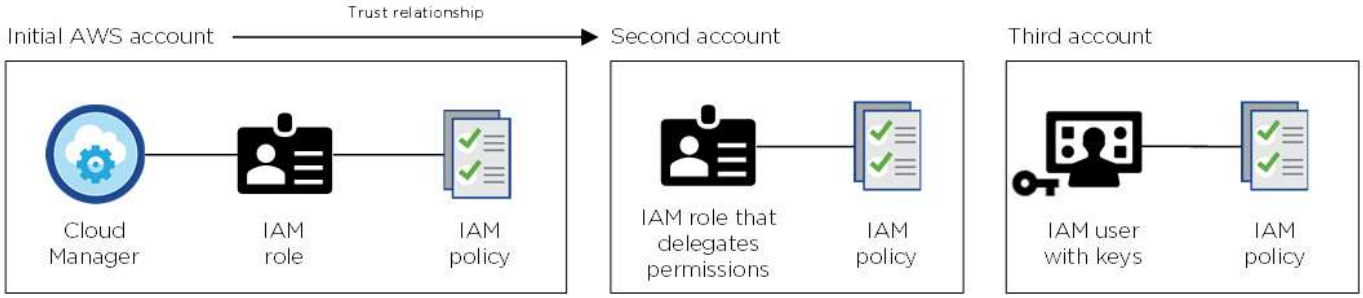
Lorsque Cloud Central lance l'instance Cloud Manager dans AWS, il crée un rôle IAM et un profil d'instance pour l'instance. Il attache également une règle qui fournit les autorisations nécessaires à cloud Manager pour déployer et gérer Cloud Volumes ONTAP dans ce compte AWS. "Examinez comment Cloud Manager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




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

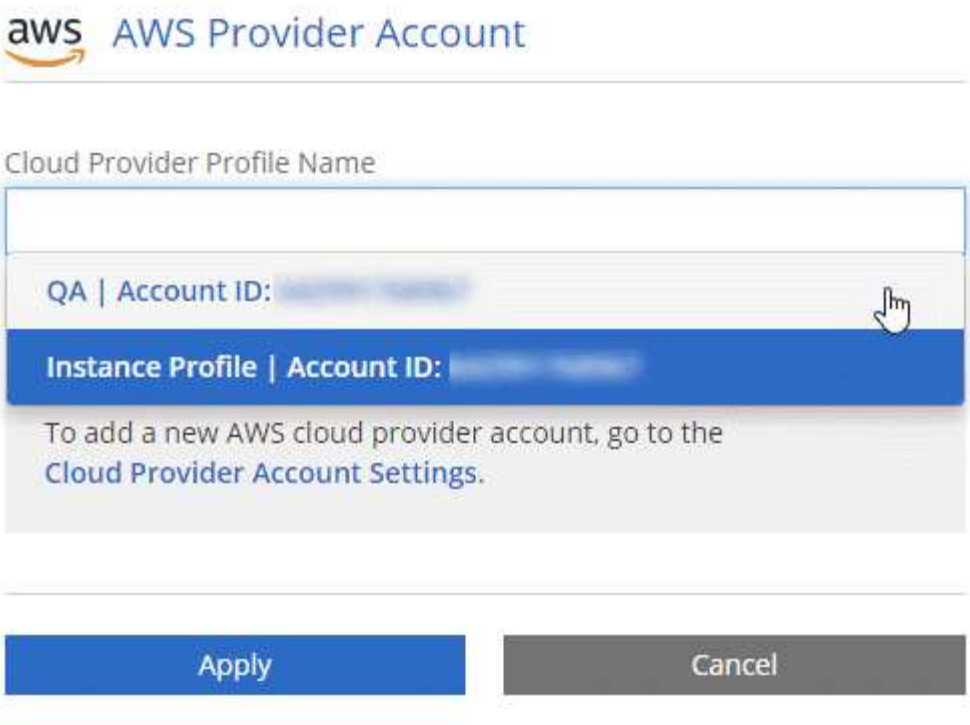

### Autres comptes AWS

Si vous souhaitez lancer Cloud Volumes ONTAP sur différents comptes AWS, vous pouvez l'un ou l'autre "Fournir des clés AWS pour un utilisateur IAM ou le numéro ARN d'un rôle dans un compte de confiance". L'image suivante montre deux comptes supplémentaires, l'un avec des autorisations par le biais d'un rôle IAM dans un compte de confiance et l'autre avec les clés AWS d'un utilisateur IAM :




Vous le feriez alors "Ajoutez les comptes des fournisseurs de services clouds à Cloud Manager" En spécifiant le nom de ressource Amazon (ARN) du rôle IAM ou les clés AWS pour l'utilisateur IAM.

Après avoir ajouté un autre compte, vous pouvez le basculer lors de la création d'un nouvel environnement de travail :




## Comptes et autorisations Azure

Vous pouvez déployer tous les systèmes Cloud Volumes ONTAP sur le compte Azure initial, ou configurer d'autres comptes.

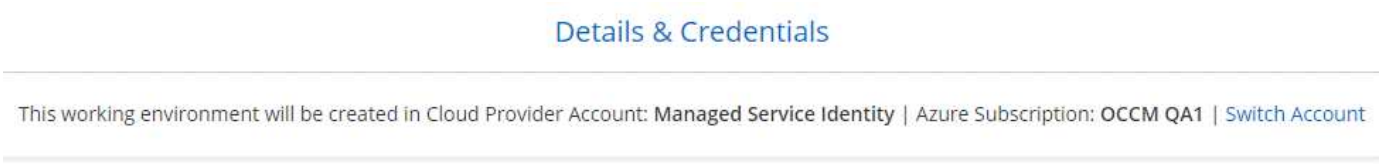
### Compte Azure initial

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

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


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

environnement de travail :

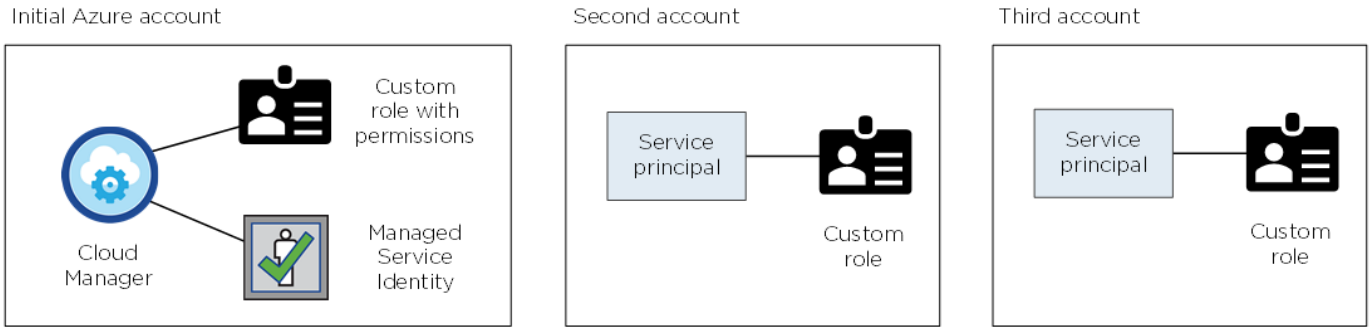



### Abonnements Azure supplémentaires pour le compte initial

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

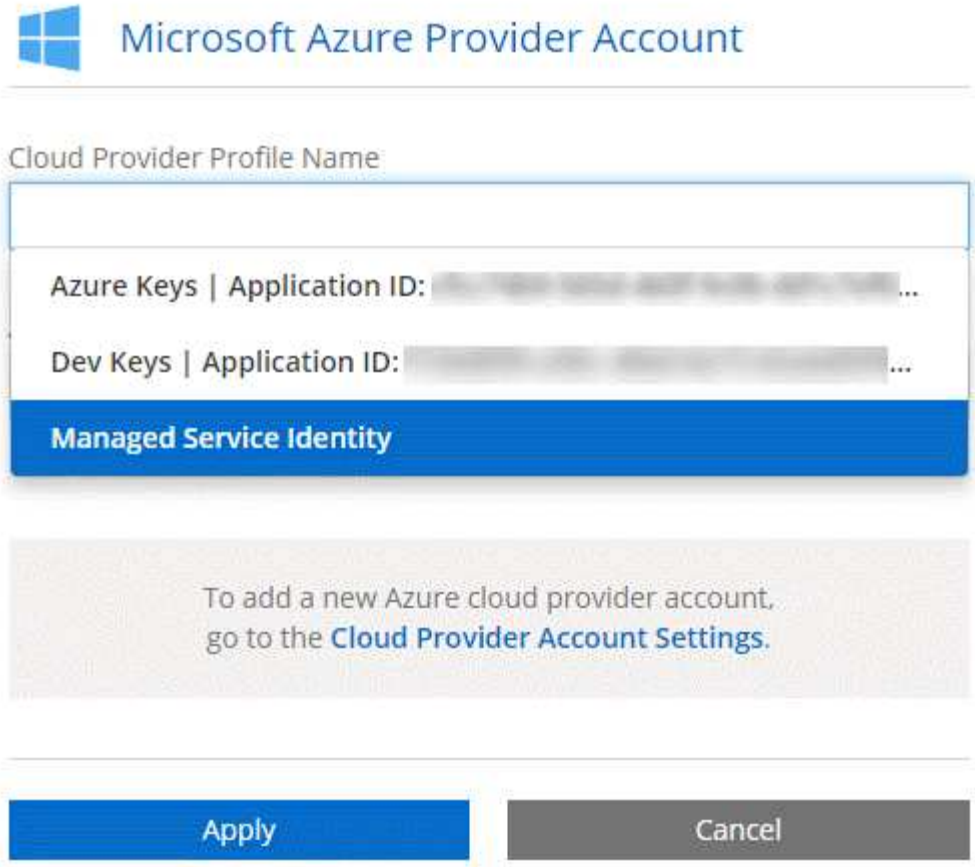
### Autres comptes Azure

Si vous souhaitez déployer Cloud Volumes ONTAP sur différents comptes Azure, vous devez accorder les autorisations requises par "Création et configuration d'une entité de service dans Azure Active Directory" Pour chaque compte Azure. L'image suivante montre deux comptes supplémentaires, chacun étant doté d'un rôle principal de service et personnalisé qui fournit des autorisations :




Vous le feriez alors "Ajoutez les comptes des fournisseurs de services clouds à Cloud Manager" En fournissant des détails sur le principal du service AD.

Après avoir ajouté un autre compte, vous pouvez le basculer lors de la création d'un nouvel environnement de travail :




### Qu'en est-il des déploiements Marketplace et des déploiements sur site ?

Les sections ci-dessus décrivent la méthode de déploiement recommandée de NetApp Cloud Central. Vous pouvez également déployer Cloud Manager à partir du "AWS Marketplace", le "Azure Marketplace", et vous pouvez "Installez Cloud Manager sur site".

Si vous utilisez l'un ou l'autre des Marketplaces, les autorisations sont fournies de la même façon. Il vous suffit de créer et de configurer manuellement le rôle IAM ou l'identité gérée pour Cloud Manager, puis de fournir les autorisations nécessaires pour tous les comptes supplémentaires.

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

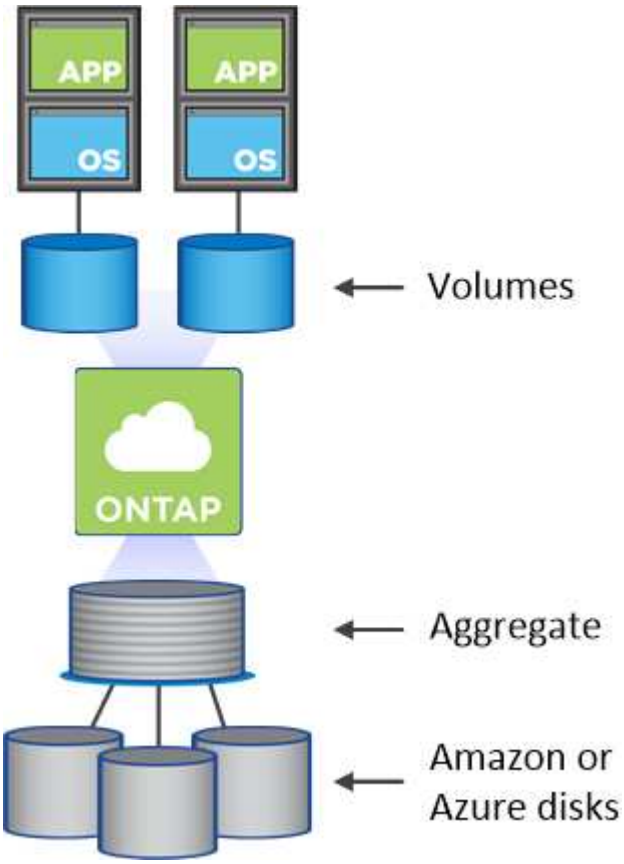
# Stockage

## Utilisation du stockage cloud par Cloud Volumes ONTAP

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

### Présentation

Cloud Volumes ONTAP utilise les volumes AWS et Azure comme stockage back-end. Il considère ces volumes comme des disques et les regroupe en un ou plusieurs agrégats. Les agrégats fournissent du stockage à un ou plusieurs volumes.




Plusieurs types de disques clouds sont pris en charge. Vous choisissez le type de disque lors de la création de volumes et la taille de disque par défaut lorsque vous déployez Cloud Volumes ONTAP.

Le volume total de stockage acheté auprès d'AWS ou d'Azure 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, 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 également coupler un disque EBS avec Amazon S3 pour "tiering des données".

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.

Pour plus de détails sur les cas d'utilisation de ces disques, reportez-vous à "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".

#### 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 pour "tiering des données".

#### Paires HA

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

Pour plus d'informations sur les cas d'utilisation de ces disques, reportez-vous à la section "Documentation Microsoft Azure : présentation du stockage Microsoft Azure".

"Découvrez comment choisir les types et les tailles de disques pour vos systèmes dans Azure".

"Consultez les limites de stockage pour Cloud Volumes ONTAP".

## Vue d'ensemble du hiérarchisation des données

Réduisez vos coûts de stockage grâce au Tiering automatisé des données inactives vers un stockage objet à faible coût. Les données actives restent dans des disques SSD ou

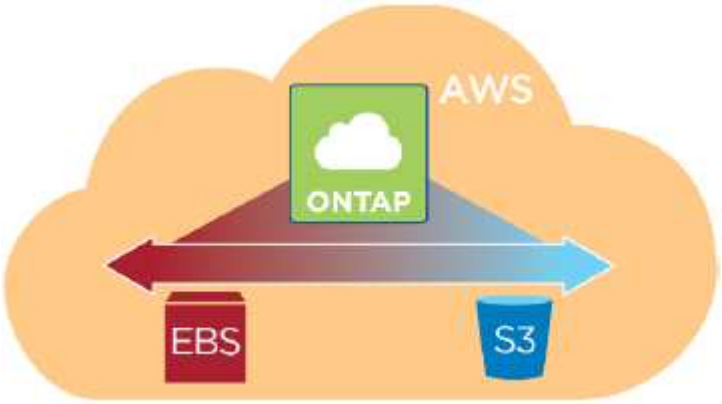
des disques durs haute performance (niveau de performance), tandis que les données inactives sont hiérarchisées en stockage objet à faible coût (niveau de capacité). Vous pouvez ainsi récupérer de l'espace sur votre stockage principal et réduire le stockage secondaire.

Cloud Volumes ONTAP prend en charge la hiérarchisation des données dans AWS et dans Microsoft Azure. La hiérarchisation des données est optimisée par la technologie FabricPool.

Vous n'avez pas besoin d'installer une licence de fonctionnalité pour activer le tiering des données.

### Fonctionnement du 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 :




#### Niveau de performance 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.

#### Niveau de capacité dans AWS

Par défaut, Cloud Volumes ONTAP transfère les données inactives vers la classe de stockage S3 *Standard*. La norme est idéale pour les données fréquemment consultées stockées dans plusieurs zones de disponibilité.

Si vous ne prévoyez pas d'accéder aux données inactives, réduisez vos coûts de stockage en modifiant le niveau de Tiering d'un système à l'une des conditions suivantes, après le déploiement de Cloud Volumes ONTAP :

**Hiérarchisation intelligente**
: Optimise les coûts du stockage en déplaçant les données entre deux niveaux au fur et à mesure de l'évolution des modèles d'accès aux données. L'un des niveaux est destiné aux accès fréquents et l'autre à des accès rares.

**Un seul accès à Zone-Infrequent**
: Pour les données rarement accessibles stockées dans une seule zone de disponibilité.

**Accès autonome et peu fréquent**

Pour les données rarement accessibles stockées dans plusieurs zones de disponibilité.

Les coûts d'accès sont plus élevés si vous accédez aux données. Vous devez donc en tenir compte avant de modifier le niveau de hiérarchisation. Pour plus d'informations sur les classes de stockage S3, reportez-vous à "Documentation AWS".

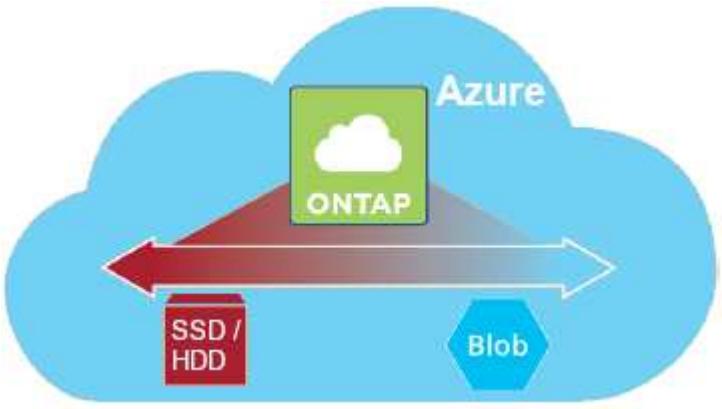
Lorsque vous modifiez le niveau de Tiering, les données inactives commencent dans la classe de stockage Standard et sont déplacées vers la classe de stockage que vous avez sélectionnée, si les données ne sont pas accessibles après 30 jours. Pour plus d'informations sur la modification du niveau de hiérarchisation, voir "Tiering des données inactives vers un stockage objet à faible coût".

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

Un environnement de travail Cloud Volumes ONTAP utilise un compartiment S3 pour toutes les données à plusieurs niveaux du système. Un autre compartiment S3 n'est pas utilisé pour chaque volume. Cela inclut un environnement de travail haute disponibilité. Cloud Manager crée un compartiment S3 et le nomme « fabric-pool-_cluster unique ».

### Fonctionnement du tiering des données dans Microsoft Azure

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




#### Niveau de performance à Azure

Le niveau de performance peut être soit Premium Storage (SSD), soit Standard Storage (HDD).

#### Niveau de capacité à Azure

Par défaut, Cloud Volumes ONTAP transfère les données inactives vers le niveau de stockage Azure *hot*, idéal pour les données fréquemment utilisées.

Si vous ne prévoyez pas d'accéder aux données inactives, vous pouvez réduire vos coûts de stockage en modifiant le niveau de Tiering d'un système vers le niveau de stockage Azure *cool* après le déploiement de Cloud Volumes ONTAP. Le niveau cool est idéal pour les données rarement accessibles qui résident dans le niveau pendant au moins 30 jours.

Les coûts d'accès sont plus élevés si vous accédez aux données. Vous devez donc en tenir compte avant de modifier le niveau de hiérarchisation. Pour plus d'informations sur les niveaux de stockage Azure Blob,

consultez "Documentation Azure".

Lorsque vous modifiez le niveau de Tiering, les données inactives commencent dans le Tier de stockage à chaud et sont déplacées vers le Tier de stockage froid, si les données ne sont pas accessibles après 30 jours. Pour plus d'informations sur la modification du niveau de hiérarchisation, voir "Tiering des données inactives vers un stockage objet à faible coût".

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

> Un environnement de travail Cloud Volumes ONTAP utilise un conteneur Azure Blob pour toutes les données hiérarchisées du système. Un autre conteneur n'est pas utilisé pour chaque volume. Cloud Manager crée un nouveau compte de stockage avec un conteneur pour chaque système Cloud Volumes ONTAP. Le nom du compte de stockage est aléatoire.

#### Comment le tiering des données affecte les 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 Volumes ONTAP prend en charge les stratégies de hiérarchisation suivantes :

**Snapshot uniquement**

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

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

**Auto**

Après avoir atteint une capacité de 50 %, Cloud Volumes ONTAP met à niveau des blocs de données à froid dans un volume vers un niveau de capacité. Les données à froid comprennent non seulement des copies Snapshot, mais aussi des données utilisateur à froid provenant du système de fichiers actif. La période de refroidissement est d'environ 31 jours.

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

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

**Sauvegarde**

Lorsque vous répliquez un volume pour la reprise après incident ou la conservation à long terme, les données du volume de destination commencent dans le niveau de capacité. Si vous activez le volume de destination, les données passent progressivement au niveau de performance tel qu'il est lu.

**Aucune**

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

#### 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 de Cloud Manager 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 Cloud Manager peut choisir si Cloud Manager vous informe des décisions relatives à la 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

Si l'administrateur Cloud Manager définit le mode de gestion de la capacité sur automatique, Cloud Manager achète automatiquement de nouveaux disques pour les instances Cloud Volumes ONTAP lorsque vous avez besoin de plus de capacité, supprime les collections de disques (agrégats) inutilisées, déplace des volumes entre les agrégats si nécessaire et tente d'annuler la défaillance des disques.

Les exemples suivants illustrent le fonctionnement de ce mode :

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

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

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

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

#### Gestion manuelle de la capacité

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

### Isolation du stockage à l'aide de locataires

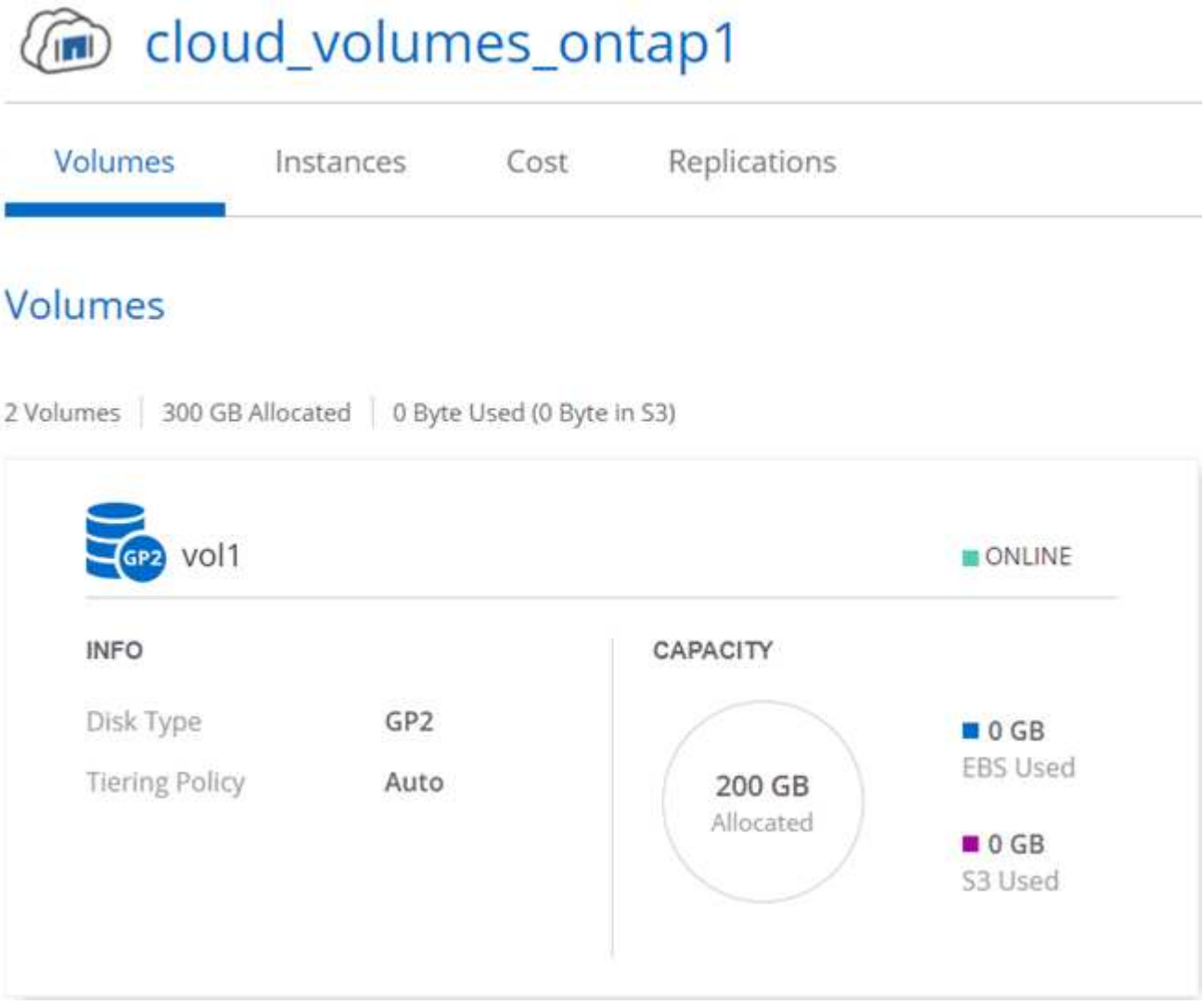
Cloud Manager vous permet de provisionner et de gérer le stockage dans des groupes isolés appelés locataires. Vous devez décider comment organiser les utilisateurs de Cloud Manager et leurs environnements de travail entre les locataires.

#### Environnements de travail

Cloud Manager représente les systèmes de stockage comme *environnements de travail*. Un environnement de travail est l'un des suivants :

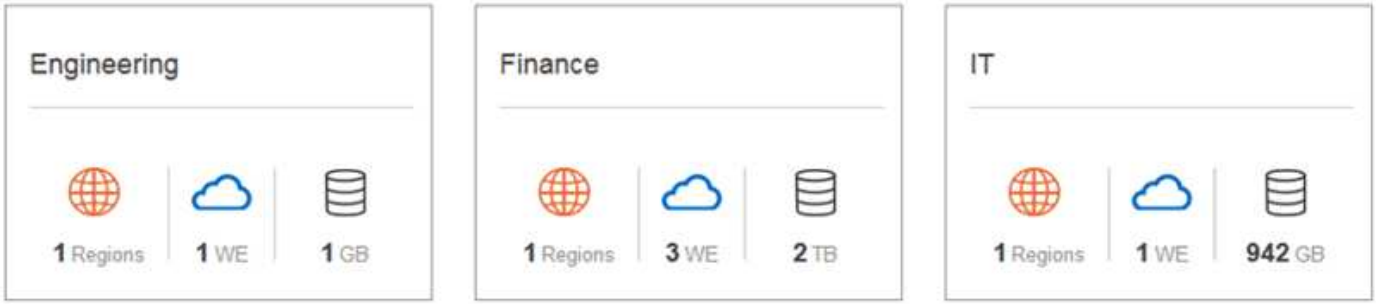
- Un seul système Cloud Volumes ONTAP ou une paire HA
- Un cluster ONTAP sur site dans votre réseau
- Un cluster ONTAP dans une configuration de stockage privé NetApp

L'image suivante montre un environnement de travail Cloud Volumes ONTAP :




#### Locataires

Un *tenant* isole les environnements de travail dans les groupes. Vous créez un ou plusieurs environnements de travail au sein d'un locataire. L'image suivante montre trois locataires définis dans Cloud Manager :




#### Gestion des utilisateurs des locataires et des environnements de travail

Les locataires et les environnements de travail que les utilisateurs de Cloud Manager peuvent gérer dépendent du rôle et des affectations des utilisateurs. Les trois rôles d'utilisateur distincts sont les suivants :

**Administrateur de Cloud Manager**
: Gère le produit et peut accéder à tous les locataires et environnements de travail.

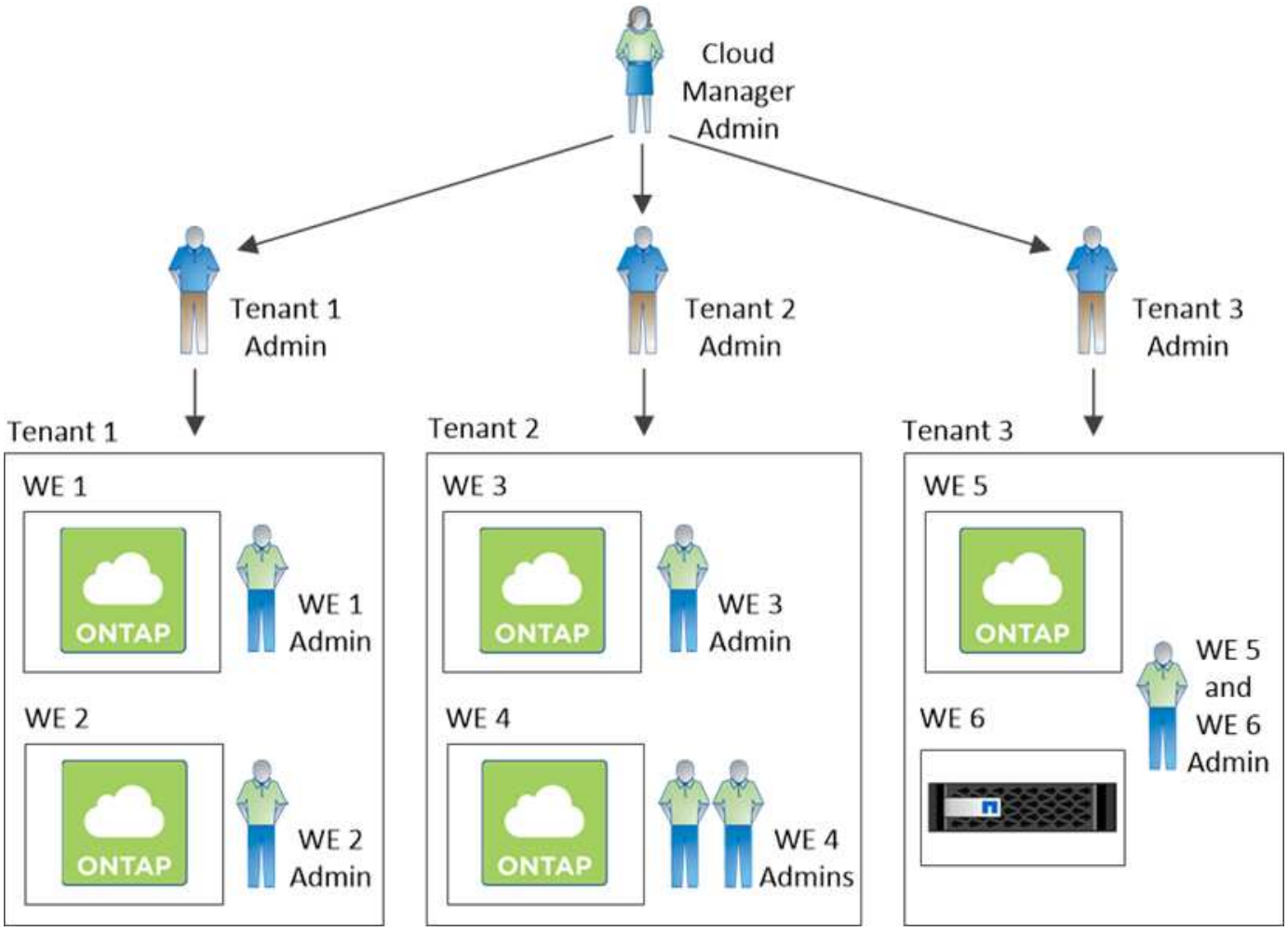
**Administration des locataires**
: Administre un locataire unique. Permet de créer et de gérer tous les environnements de travail et tous les utilisateurs du locataire.

**Administration de l'environnement de travail**
: Peut créer et gérer un ou plusieurs environnements de travail dans un locataire.

#### Exemple de création de locataires et d'utilisateurs

Si votre organisation dispose de services indépendants, il est préférable d'avoir un locataire pour chaque ministère.

Par exemple, vous pouvez créer trois locataires pour trois services distincts. Vous créerez ensuite un administrateur de locataires pour chaque locataire. Au sein de chaque locataire, un ou plusieurs administrateurs d'environnement de travail gèrent les environnements de travail. L'image suivante illustre ce scénario :

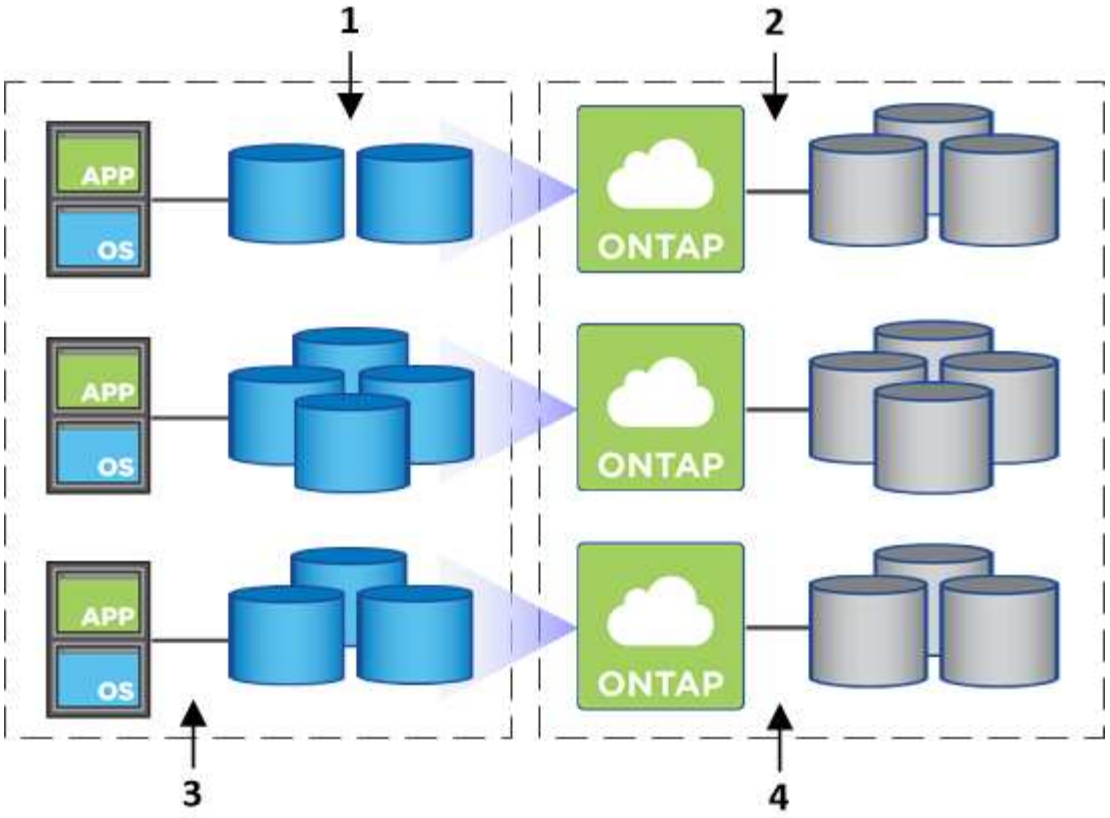



**Gestion simplifiée du stockage à l'aide de Volume View**

Cloud Manager offre une vue de gestion distincte appelée *Volume View*, qui simplifie encore davantage la gestion du stockage dans AWS.

La vue en volume vous permet de spécifier simplement les volumes NFS dont vous avez besoin dans AWS, puis Cloud Manager gère le reste : il déploie les systèmes Cloud Volumes ONTAP selon vos besoins et prend les décisions d'allocation de capacité à mesure que les volumes augmentent. Cette vue vous offre les avantages du stockage d'entreprise dans le cloud avec très peu de gestion du stockage.

L'image suivante montre comment vous interagissez avec Cloud Manager dans la vue 3D :

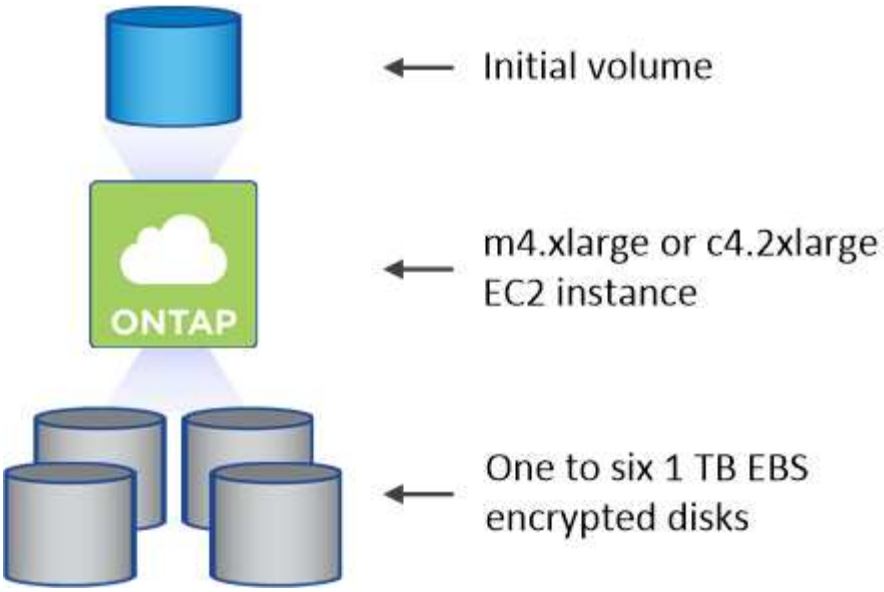



1. Vous créez des volumes NFS.
2. Cloud Manager lance des instances Cloud Volumes ONTAP dans AWS pour de nouveaux volumes ou crée des volumes sur des instances existantes. Il achète également du stockage EBS physique pour les volumes.
3. Vous mettez les volumes à la disposition de vos hôtes et applications.
4. Cloud Manager prend des décisions d'allocation de capacité à mesure que vos volumes augmentent.

   Cela signifie que vous avez simplement besoin d'interagir avec les volumes (l'image à gauche), tandis que Cloud Manager interagit avec le système de stockage et son stockage sous-jacent (l'image à droite).

#### Allocation des ressources cloud pour le volume initial

Lorsque vous créez votre premier volume, Cloud Manager lance une instance Cloud Volumes ONTAP ou une paire Cloud Volumes ONTAP HA dans AWS et achète le stockage Amazon EBS pour le volume :




La taille du volume initial détermine le type d'instance EC2 et le nombre de disques EBS.

Cloud Manager lance une instance Cloud Volumes ONTAP Explore ou Standard, en fonction de la taille initiale du volume. Lorsque les volumes augmentent, Cloud Manager peut vous inviter à modifier une instance AWS, ce qui signifie qu'il doit mettre à niveau la licence de l'instance vers Standard ou Premium. La mise à niveau augmente la limite de capacité brute EBS, ce qui permet à vos volumes de croître.

Cloud Manager ne lance pas les instances Cloud Volumes ONTAP BYOL dans Volume View. Si vous avez acheté une licence Cloud Volumes ONTAP, vous devez utiliser Cloud Manager dans Storage System View.

#### Allocation de ressources cloud pour des volumes supplémentaires

Lorsque vous créez des volumes supplémentaires, Cloud Manager crée les volumes sur des instances Cloud Volumes ONTAP existantes ou sur de nouvelles instances Cloud Volumes ONTAP. Cloud Manager peut créer un volume sur une instance existante si l'emplacement et le type de disque AWS de l'instance correspondent au volume demandé, et si l'espace est suffisant.

#### Fonctionnalités d'efficacité du stockage NetApp et coûts du stockage

Cloud Manager active automatiquement les fonctionnalités d'efficacité du stockage NetApp sur tous les volumes. Ces gains d'efficacité peuvent réduire la quantité totale de stockage dont vous avez besoin. Vous constaterez peut-être une différence entre votre capacité allouée et la capacité AWS achetée, ce qui peut entraîner des économies de coûts de stockage.

#### Décisions d'allocation de capacité prises automatiquement par Cloud Manager

- Cloud Manager achète des disques EBS supplémentaires lorsque les seuils de capacité sont dépassés. Cela se produit à mesure que vos volumes augmentent.
- Cloud Manager supprime les jeux inutilisés de disques EBS si les disques ne contiennent aucun volume pendant 12 heures.
- Cloud Manager déplace les volumes entre des jeux de disques pour éviter les problèmes de capacité.

  Dans certains cas, cela nécessite l'achat de disques EBS supplémentaires. Il libère également de l'espace

sur l’ensemble de disques d’origine pour les volumes nouveaux et existants.

## Stockage WORM

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

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

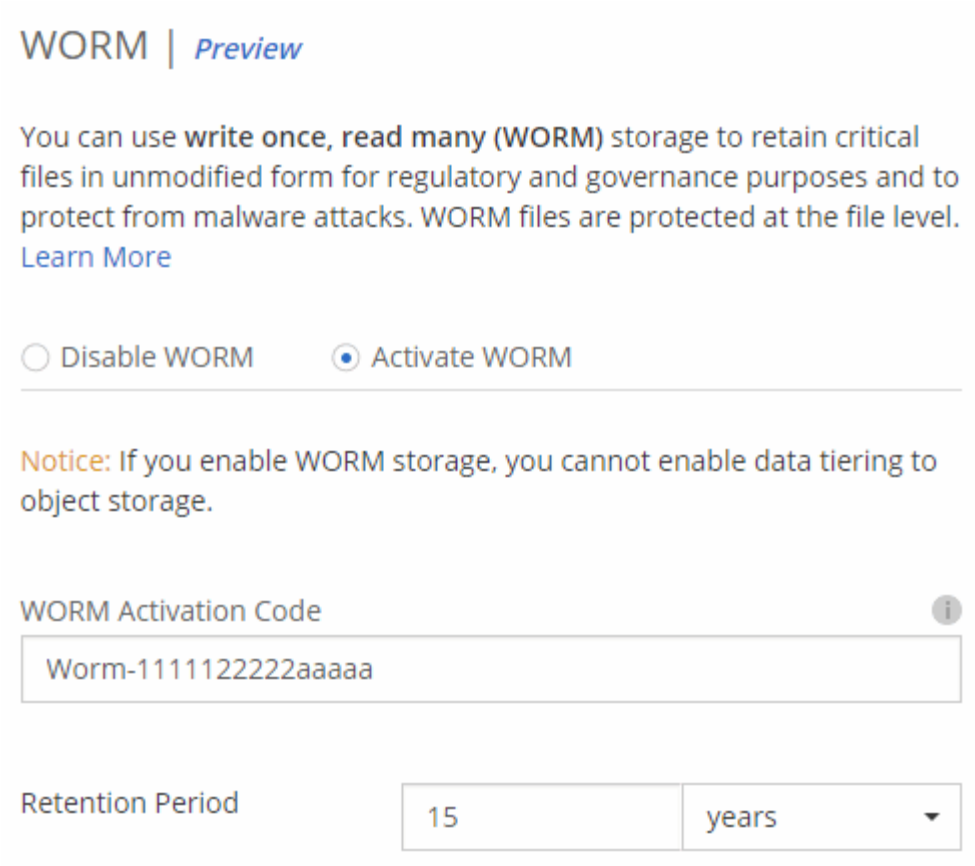
Une fois la période de conservation écoulée, vous êtes responsable de la suppression des fichiers dont vous n’avez plus besoin.

#### Activation du stockage WORM

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

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

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




**Validation de fichiers sur WORM**

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

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

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

**Limites**

- Si vous supprimez ou déplacez un disque directement depuis AWS ou Azure, un volume peut être supprimé avant sa date d'expiration.
- Lorsque le stockage WORM est activé, la hiérarchisation des données vers le stockage objet ne peut pas être activée.

# Paires haute disponibilité

## Paires haute disponibilité dans AWS

Une configuration haute disponibilité (HA) Cloud Volumes ONTAP assure des opérations

sans interruption et une tolérance aux pannes. Dans AWS, les données sont mises en miroir de manière synchrone entre les deux nœuds.

### Présentation

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

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

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

#### Reprise et remise du stockage

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

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

#### RPO et RTO

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

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

#### Modèles de déploiement HA

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

### Cloud Volumes ONTAP HA dans plusieurs zones de disponibilité

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

#### Accès aux données NFS et CIFS

Lorsqu'une configuration haute disponibilité est répartie entre plusieurs zones de disponibilité, *adresses IP flottantes* activez l'accès client NAS. Les adresses IP flottantes, qui doivent se trouver en dehors des blocs CIDR pour tous les VPC de la région, peuvent migrer entre les nœuds en cas de défaillance. Les clients ne sont pas accessibles de manière native en dehors du VPC, sauf si vous "Configuration d'une passerelle de transit AWS".

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

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

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

#### Accès aux données iSCSI

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

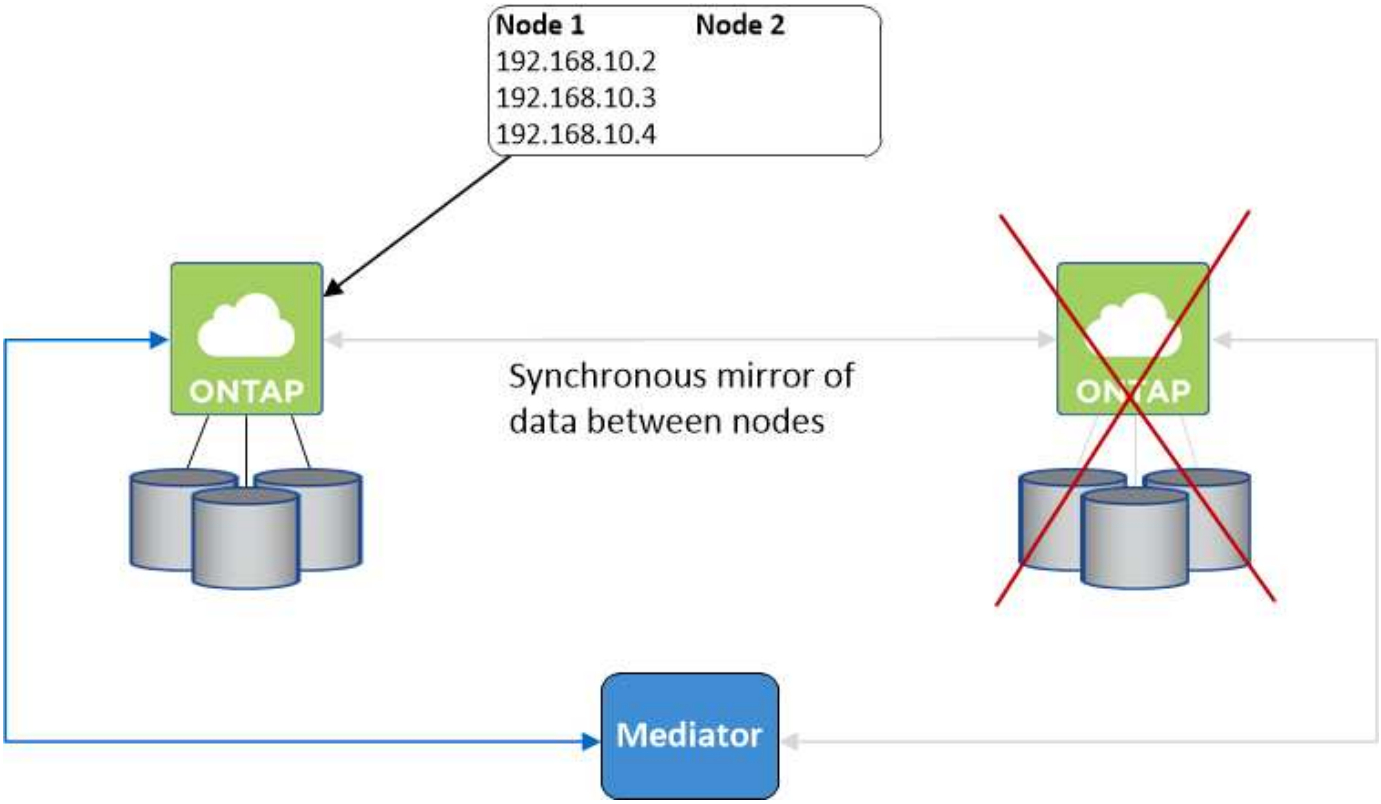
#### Reprise et remise du stockage pour iSCSI

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

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

#### Reprise et remise du stockage pour NAS

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




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

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

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

### Cloud Volumes ONTAP HA dans une seule zone de disponibilité

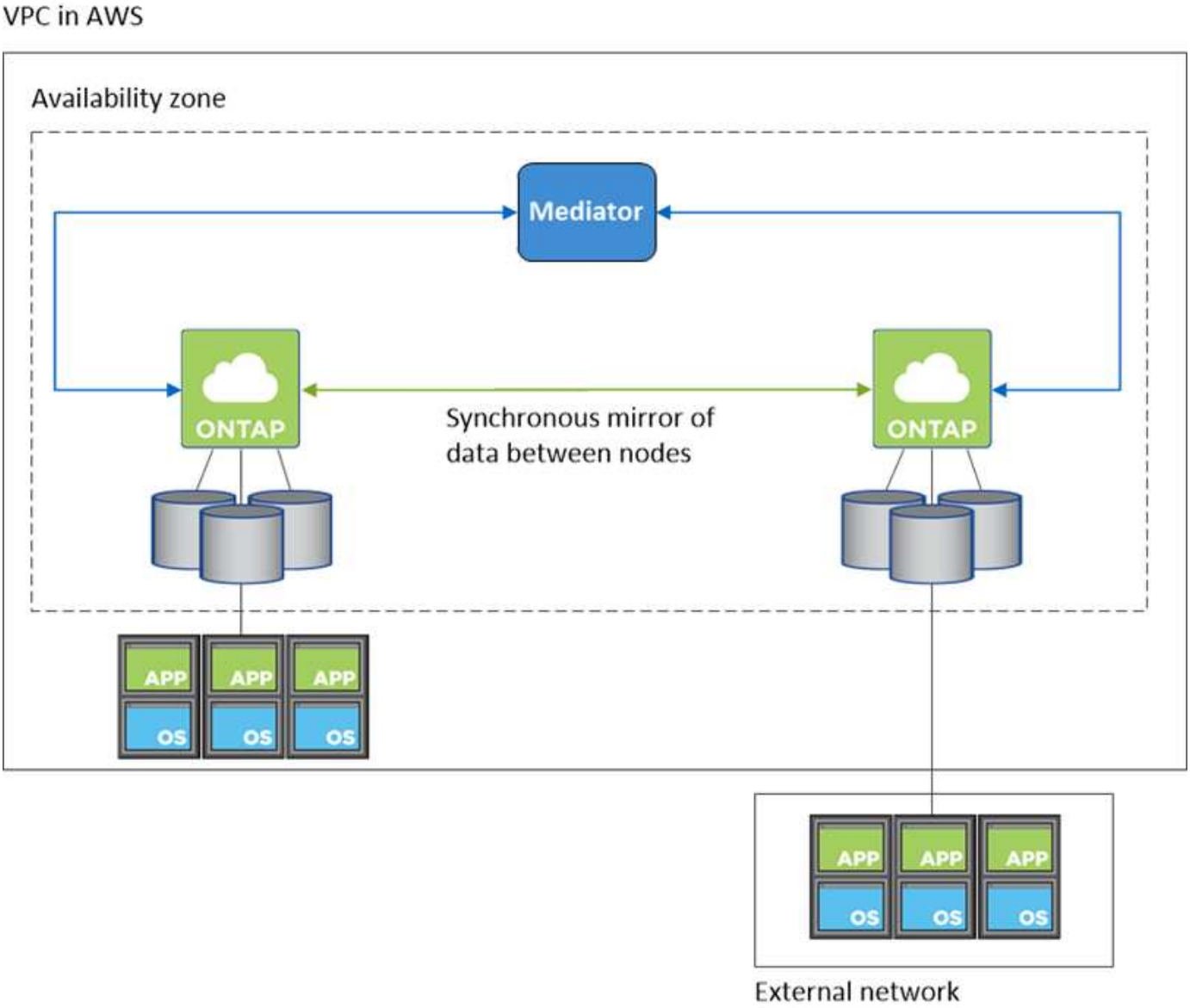
Le déploiement d'une configuration HA dans une seule zone de disponibilité (AZ) peut garantir une haute disponibilité de vos données en cas de défaillance d'une instance exécutant un nœud Cloud Volumes ONTAP. Toutes les données sont accessibles en mode natif depuis l'extérieur du VPC.

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

#### Accès aux données

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

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




#### Reprise et remise du stockage

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

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

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

### Fonctionnement du stockage dans une paire haute disponibilité

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

#### Allocation du stockage

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

#### Configurations de stockage

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

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

#### Attentes en matière de performances pour une configuration haute disponibilité

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

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

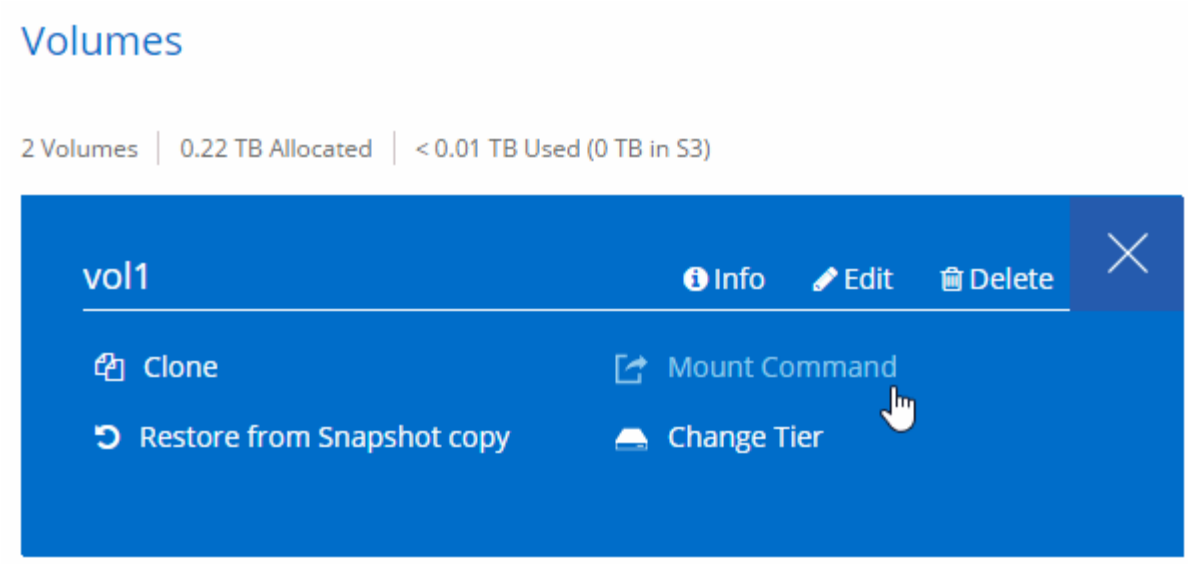
Pour plus d'informations sur les performances de Cloud Volumes ONTAP, reportez-vous à "Performance".

#### Accès client au stockage

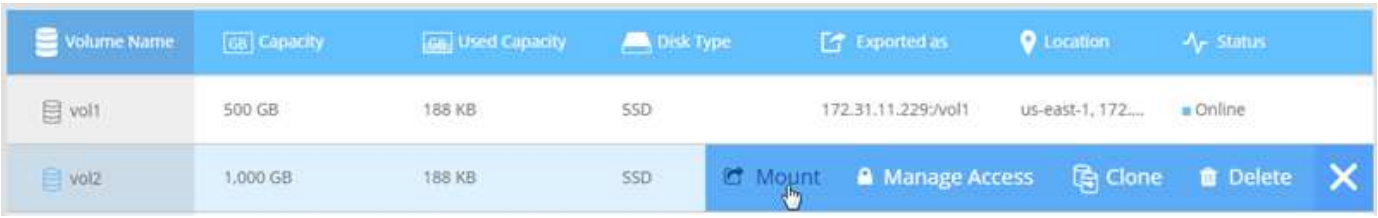
Les clients doivent accéder aux volumes NFS et CIFS en utilisant l'adresse IP de données du nœud sur lequel réside le volume. Si les clients NAS accèdent à un volume en utilisant l'adresse IP du nœud partenaire, le trafic passe entre les deux nœuds, ce qui réduit les performances.

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

Vous pouvez facilement identifier l'adresse IP correcte à partir de Cloud Manager. L'image suivante présente la vue du système de stockage :




L'image suivante montre la vue Volume :

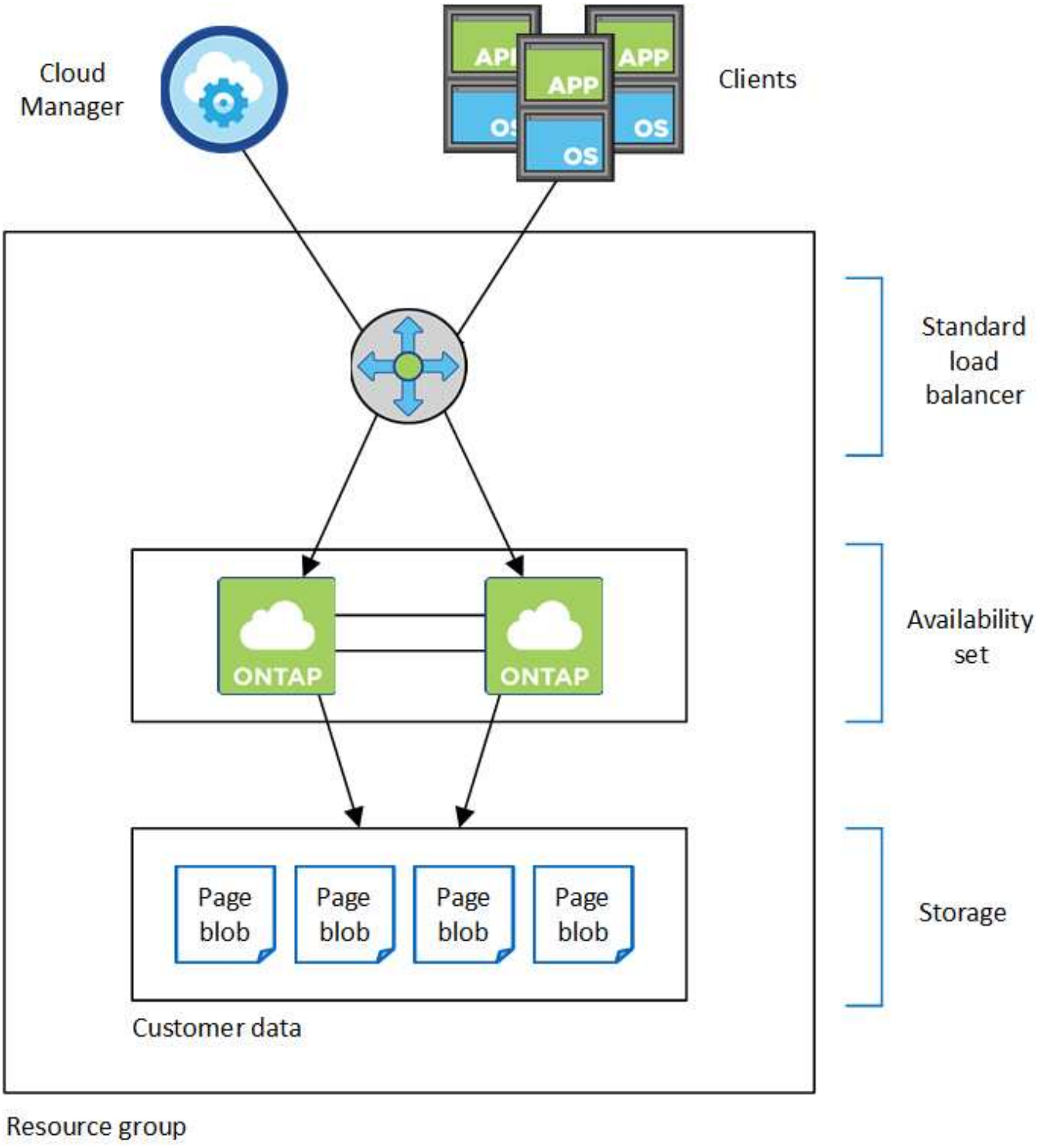



## Paires haute disponibilité dans Azure

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.

### Stockage

Les données client résident sur les blobs de la page Premium Storage. Chaque nœud a accès au stockage de l'autre nœud. Un stockage supplémentaire est également nécessaire pour les données de démarrage et de racine :

- Les données de démarrage d'un nœud résident sur un disque géré Premium SSD.
- Les données racine d'un nœud résident sur un objet blob de page Premium Storage.

### 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.
- Le Tiering des données n'est pas pris en charge.
- NFSv4 n'est pas pris en charge. NFSv3 est pris en charge.
- Les paires HA ne sont pas prises en charge dans certaines régions.

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

"Découvrez comment déployer un système HA dans Azure".

# L'évaluation

Vous pouvez évaluer Cloud Volumes ONTAP avant d'investir dans le logiciel.

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

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

# Licences

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

### Gestion des licences pour un nouveau système

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

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

Si Cloud Manager ne peut pas accéder au fichier de licence via la connexion Internet sécurisée, vous pouvez obtenir le fichier vous-même, puis le télécharger manuellement dans Cloud Manager. Pour obtenir des instructions, reportez-vous à la section "Installation de fichiers de licence sur les systèmes Cloud Volumes ONTAP BYOL".

### Expiration de la licence

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


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

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

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

#### Renouvellement de la licence

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

Si Cloud Manager ne peut pas accéder au fichier de licence via la connexion Internet sécurisée, vous pouvez obtenir le fichier vous-même, puis le télécharger manuellement dans Cloud Manager. Pour obtenir des instructions, reportez-vous à la section "Installation de fichiers de licence sur les systèmes Cloud Volumes ONTAP BYOL".

# Sécurité

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

## Cryptage des données au repos

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

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

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

#### NetApp Volume Encryption

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

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

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

#### Service de gestion des clés AWS

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

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

#### Chiffrement de service de stockage Azure

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

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

## Analyse antivirus ONTAP

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

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

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

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

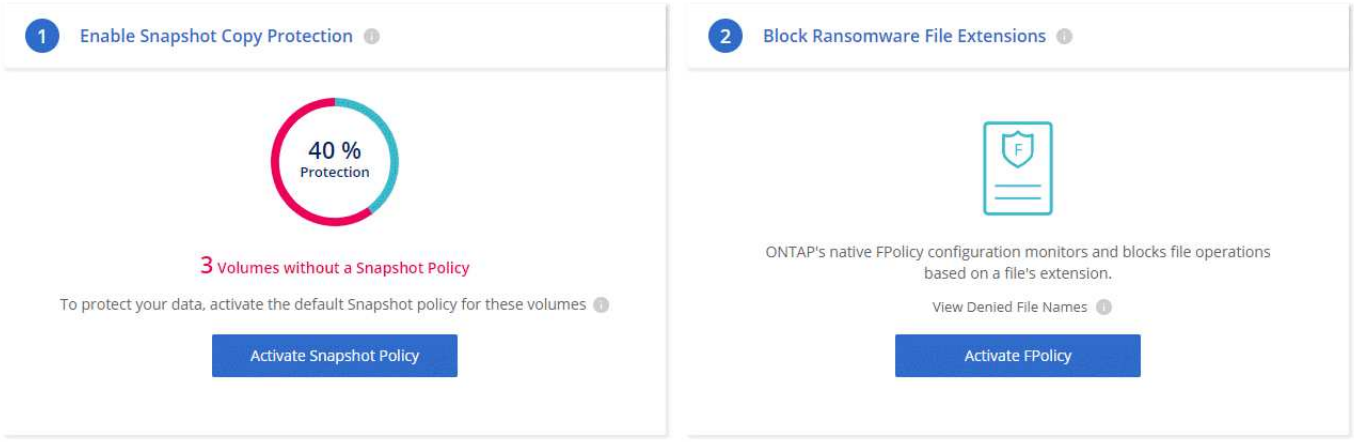
## Protection par ransomware

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

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

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

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



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

# Performance

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

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

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

# Pour commencer

## Présentation du déploiement

Avant de commencer, vous pouvez mieux comprendre vos options de déploiement d'OnCommand Cloud Manager et de Cloud Volumes ONTAP.

### Installation de Cloud Manager

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

- Services Web Amazon (AWS)
- Microsoft Azure
- Cloud IBM
- Dans votre propre réseau

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

| Emplacement | Comment déployer Cloud Manager |
|---|---|
| AWS | "Déployez Cloud Manager à partir de NetApp Cloud Central" |
| AWS C2S | "Déployez Cloud Manager depuis le Marketplace de la communauté AWS Intelligence" |
| Azure région disponible actuellement | "Déployez Cloud Manager à partir de NetApp Cloud Central" |
| Gouvernement Azure | "Déployez Cloud Manager depuis Azure Government Marketplace" |
| Azure Allemagne | "Téléchargez et installez le logiciel sur un hôte Linux" |
| Cloud IBM | "Téléchargez et installez le logiciel sur un hôte Linux" |
| Réseau sur site | "Téléchargez et installez le logiciel sur un hôte Linux" |

### Configuration de Cloud Manager

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

- "Ajout de comptes de fournisseurs de services clouds à Cloud Manager"
- "Installation d'un certificat HTTPS"
- "Configuration des utilisateurs et des locataires"
- "Configuration du système AWS KMS"

### Déploiement de Cloud Volumes ONTAP

Une fois Cloud Manager activé, vous pouvez commencer à déployer Cloud Volumes ONTAP dans AWS et dans Microsoft Azure.

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

- "Configurations prises en charge pour Cloud Volumes ONTAP 9.5"
- "Planification de votre configuration"
- "Lancement d'Cloud Volumes ONTAP dans AWS"
- "Lancement d'Cloud Volumes ONTAP dans Azure"

# Mise en route de Cloud Volumes ONTAP dans AWS

Vous pouvez commencer à utiliser Cloud Volumes ONTAP dans AWS à partir de NetApp Cloud Central.

**Configurez votre réseau**

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

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

2. Configurez un terminal VPC sur le service S3.

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

**Abonnez-vous à Cloud Volumes ONTAP depuis AWS Marketplace**

Abonnement de "AWS Marketplace" est obligatoire pour accepter les termes du logiciel. Vous ne devez vous abonner qu'à partir du Marketplace. Le lancement de Cloud Volumes ONTAP n'importe où, mais Cloud Manager n'est pas pris en charge.

**Fournissez les autorisations AWS requises**

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

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

**Lancez Cloud Manager à partir de NetApp Cloud Central**

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

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

**Lancez Cloud Volumes ONTAP à l'aide de Cloud Manager**

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

**Liens connexes**

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

# Mise en route de Cloud Volumes ONTAP dans Azure

Vous pouvez commencer à utiliser Cloud Volumes ONTAP dans Azure à partir de NetApp Cloud Central. Des instructions distinctes sont disponibles pour déployer Cloud Manager dans le "Les régions du gouvernement des États-Unis Azure" et po "Les régions Azure Germany".

**Configurez votre réseau**

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

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

**Fournissez les autorisations Azure requises**

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

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

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

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

**Lancez Cloud Manager à partir de NetApp Cloud Central**

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

**Lancez Cloud Volumes ONTAP à l'aide de Cloud Manager**

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

**Liens connexes**

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

# Configuration de Cloud Manager

## Ajout de comptes de fournisseurs cloud à Cloud Manager

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

Lorsque vous déployez Cloud Manager depuis Cloud Central, Cloud Manager ajoute automatiquement un "compte de fournisseur cloud" Pour le compte dans lequel vous avez déployé Cloud Manager. Aucun compte de fournisseur cloud initial n'est ajouté si vous avez installé manuellement le logiciel Cloud Manager sur un système existant.

### Configuration et ajout de comptes AWS à Cloud Manager

Si vous souhaitez déployer Cloud Volumes ONTAP sur différents comptes AWS, vous devez fournir les autorisations requises à ces comptes, puis ajouter les informations à Cloud Manager. La manière dont vous fournissez les autorisations dépend de votre choix si vous souhaitez fournir Cloud Manager avec des clés AWS ou le NRA d'un rôle dans un compte de confiance.

- Octroi d'autorisations lors de l'utilisation de clés AWS

- Octroi d'autorisations en assumant des rôles IAM dans d'autres comptes

#### Octroi d'autorisations lors de l'utilisation de clés AWS

Si vous souhaitez fournir Cloud Manager avec des clés AWS pour un utilisateur IAM, vous devez accorder les autorisations requises à cet utilisateur. La stratégie IAM de Cloud Manager définit les actions et les ressources AWS que Cloud Manager est autorisé à utiliser.

**Étapes**

1. Téléchargez la politique IAM de Cloud Manager à partir du "Page Cloud Manager Policies".
2. À partir de la console IAM, créez votre propre stratégie en copiant et en collant le texte de la stratégie IAM de Cloud Manager.

   "Documentation AWS : création de règles IAM"

3. Joignez la politique à un rôle IAM ou à un utilisateur IAM.
   - "Documentation AWS : création de rôles IAM"
   - "Documentation AWS : ajout et suppression de règles IAM"

**Résultat**

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

#### Octroi d'autorisations en assumant des rôles IAM dans d'autres comptes

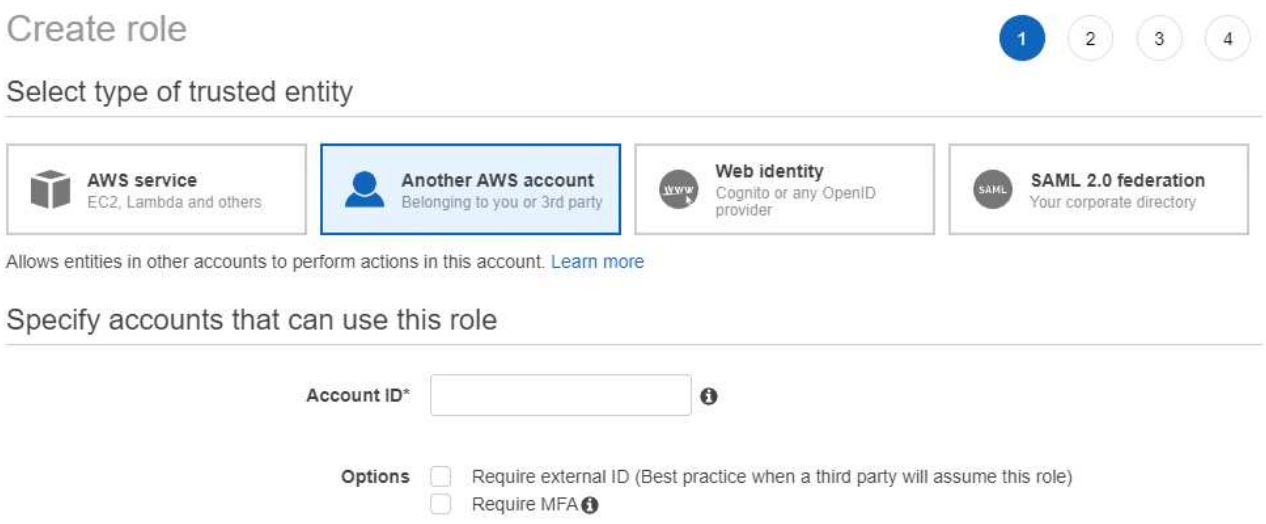
Vous pouvez définir une relation de confiance entre le compte AWS source dans lequel vous avez déployé l'instance Cloud Manager et d'autres comptes AWS en utilisant les rôles IAM. Vous pouvez ensuite fournir à Cloud Manager l'ARN des rôles IAM depuis les comptes de confiance.

**Étapes**

1. Accédez au compte cible sur lequel vous souhaitez déployer Cloud Volumes ONTAP et créez un rôle IAM en sélectionnant **un autre compte AWS**.

   Assurez-vous de faire ce qui suit :

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



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

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

   b. Ajoutez l'action « sts:AssumeRole » et l'ARN du rôle que vous avez créé dans le compte cible.

      **Exemple**

```
{
 "Version": "2012-10-17",
 "Statement": {
   "Effect": "Allow",
   "Action": "sts:AssumeRole",
   "Resource": "arn:aws:iam::ACCOUNT-B-ID:role/ACCOUNT-B-ROLENAME"
}
}
```

**Résultat**

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

#### Ajout de comptes AWS à Cloud Manager

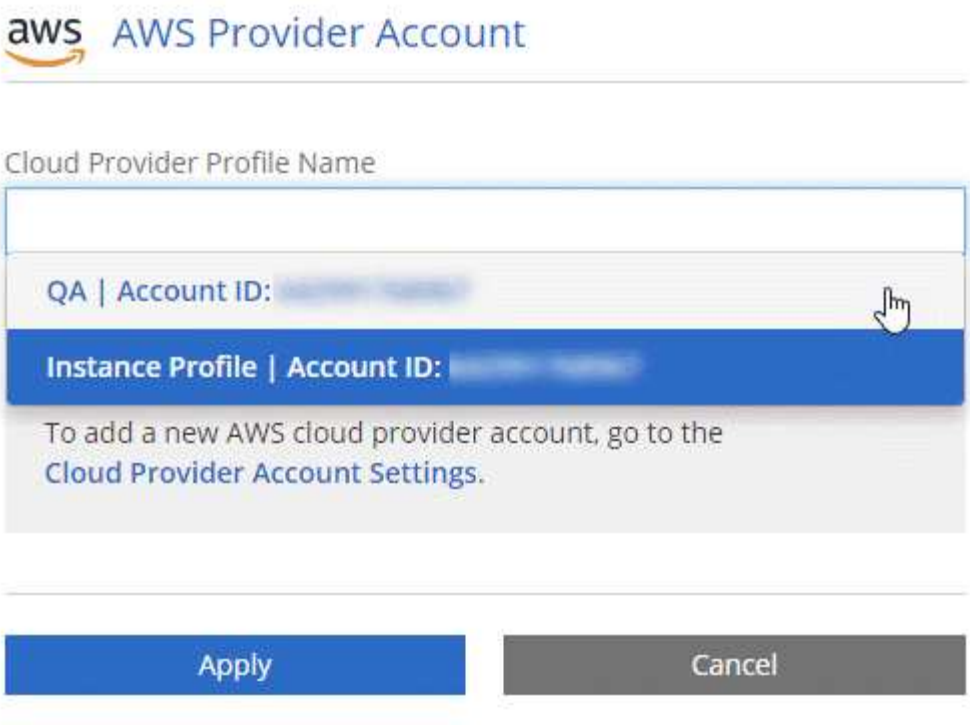
Une fois que vous avez passé un compte AWS avec les autorisations requises, vous pouvez ajouter le compte à Cloud Manager. Vous pouvez ainsi lancer les systèmes Cloud Volumes ONTAP de ce compte.

**Étapes**

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur la liste déroulante des tâches, puis sélectionnez **Paramètres du compte**.
2. Cliquez sur **Ajouter un nouveau compte** et sélectionnez **AWS**.
3. Indiquez si vous souhaitez fournir des clés AWS ou l'ARN d'un rôle IAM approuvé.
4. Vérifiez que les exigences de la stratégie ont été respectées, puis cliquez sur **Créer un compte**.

**Résultat**

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




### Configuration et ajout de comptes Azure dans Cloud Manager

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

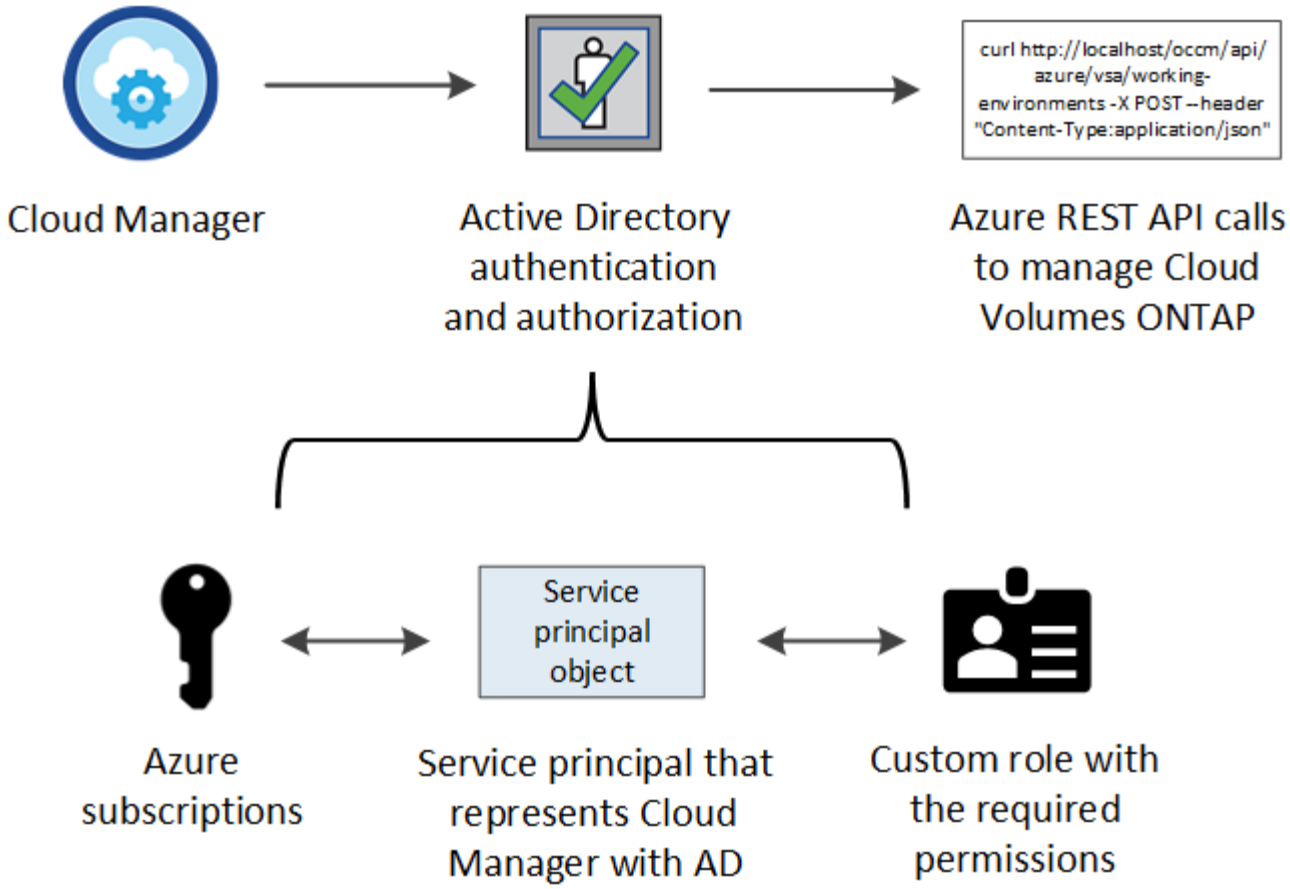
- Octroi d'autorisations Azure à l'aide d'une entité de sécurité de service
- Ajout de comptes Azure à Cloud Manager

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

Cloud Manager a besoin d'autorisations pour effectuer des actions dans Azure. Vous pouvez accorder les autorisations requises à un compte Azure en créant et en configurant une entité de sécurité de service dans Azure Active Directory et en obtenant les informations d'identification Azure requises par Cloud Manager.

**Description de la tâche**

L'image suivante illustre comment Cloud Manager obtient les autorisations nécessaires pour effectuer des opérations dans Azure. Un objet principal de service, lié à un ou plusieurs abonnements Azure, représente Cloud Manager dans Azure Active Directory et est affecté à un rôle personnalisé qui permet les autorisations requises.




Les étapes suivantes utilisent le nouveau portail Azure. Si vous rencontrez des problèmes, vous devez utiliser le portail Azure classique.

**Étapes**

1. Créez un rôle personnalisé avec les autorisations Cloud Manager requises.
2. Créez un principal de service Active Directory.
3. Attribuez le rôle d'opérateur Cloud Manager personnalisé à l'entité principal de service.

### Création d'un rôle personnalisé avec les autorisations Cloud Manager requises

Un rôle personnalisé est requis pour fournir à Cloud Manager les autorisations dont il a besoin pour lancer et gérer Cloud Volumes ONTAP dans Azure.

**Étapes**

1. Téléchargez le "Politique de Cloud Manager Azure".
2. Modifiez le fichier JSON en ajoutant des identifiants d'abonnement Azure à l'étendue assignable.

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

   **Exemple**

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

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

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

   **Définition de rôle az create --role-definition C:\Policy_for_Cloud_Manager_Azure_3.6.1.json**

**Résultat**

Vous devez maintenant disposer d'un rôle personnalisé appelé opérateur OnCommand Cloud Manager.

### Création d'un principal de service Active Directory

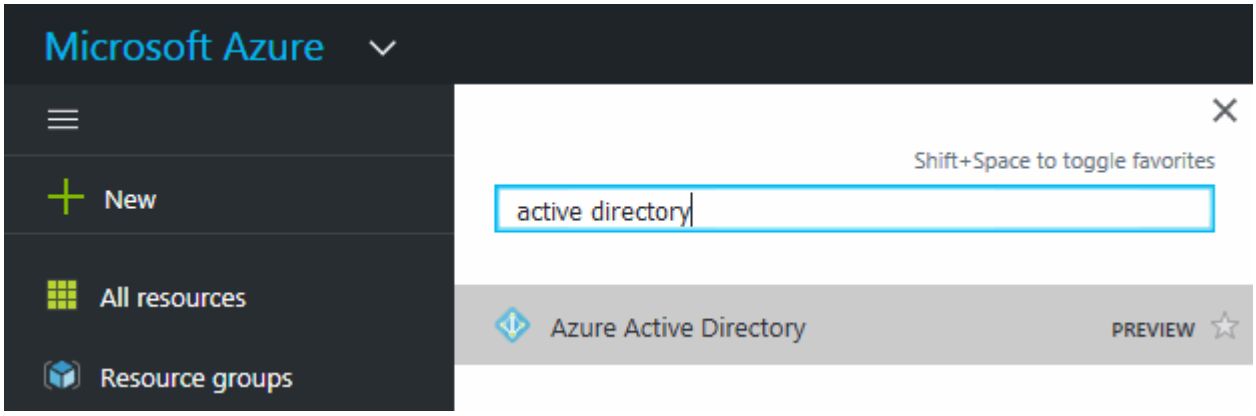
Vous devez créer un principal de service Active Directory pour que Cloud Manager puisse s'authentifier auprès d'Azure Active Directory.

**Avant de commencer**

Vous devez disposer des autorisations appropriées dans Azure pour créer une application Active Directory et attribuer l'application à un rôle. Pour plus de détails, reportez-vous à "Documentation Microsoft Azure : utilisez le portail pour créer une application Active Directory et un service principal pouvant accéder aux ressources".

**Étapes**

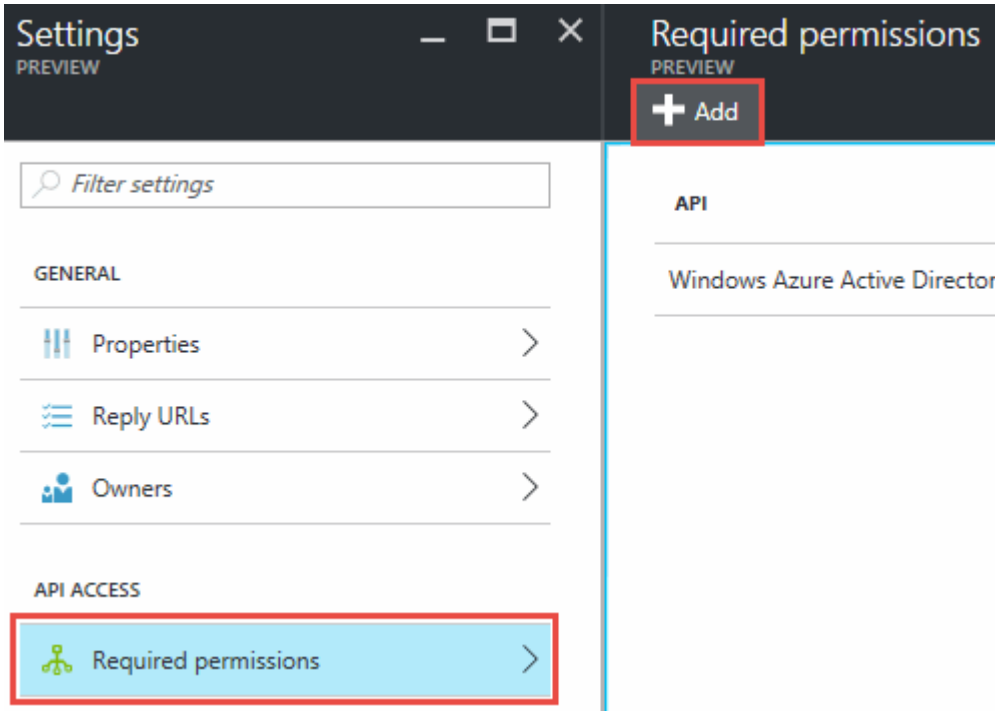
1. À partir du portail Azure, ouvrez le service **Azure Active Directory**.



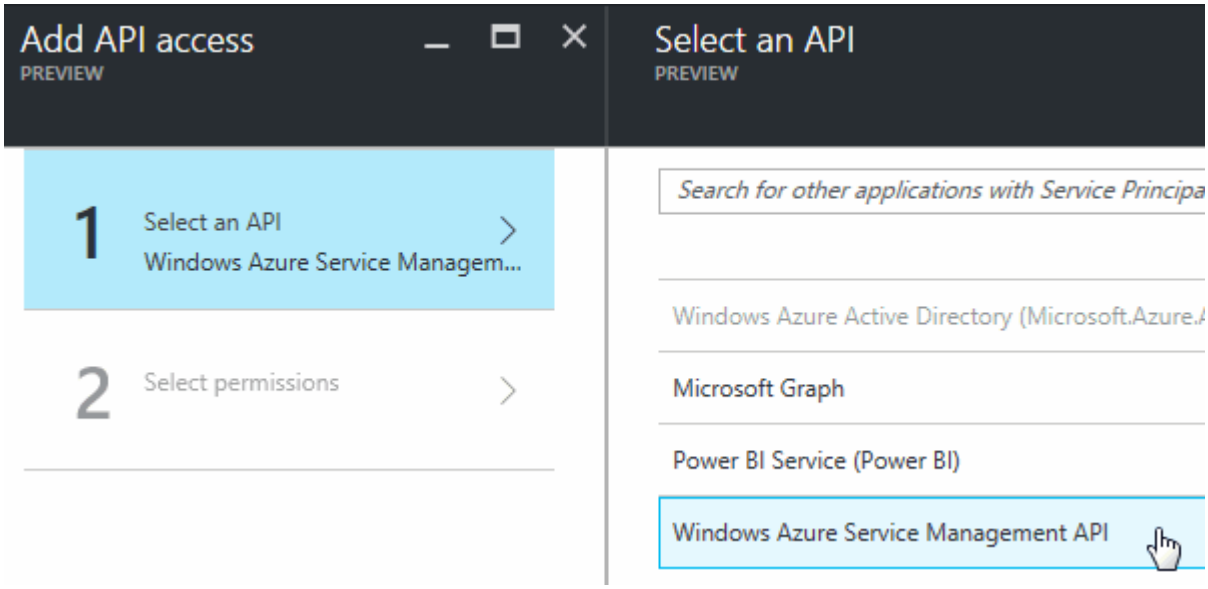

2. Dans le menu, cliquez sur **enregistrements d'applications (Legacy)**.
3. Créez le principal de service :
   a. Cliquez sur **enregistrement de la nouvelle application**.
   b. Entrez un nom pour l'application, conservez **Web app / API** sélectionnée, puis entrez une URL, par exemple, http://url
   c. Cliquez sur **Créer**.
4. Modifiez l'application pour ajouter les autorisations requises :

a. Sélectionnez l'application créée.

b. Sous Paramètres, cliquez sur **autorisations requises**, puis sur **Ajouter**.




c. Cliquez sur **sélectionnez une API**, sélectionnez **Windows Azure Service Management API**, puis cliquez sur **Select**.




d. Cliquez sur **Access Azure Service Management en tant qu'utilisateurs d'organisation**, cliquez sur **Select**, puis sur **Done**.

5. Créez une clé pour le principal de service :

a. Sous Paramètres, cliquez sur **touches**.

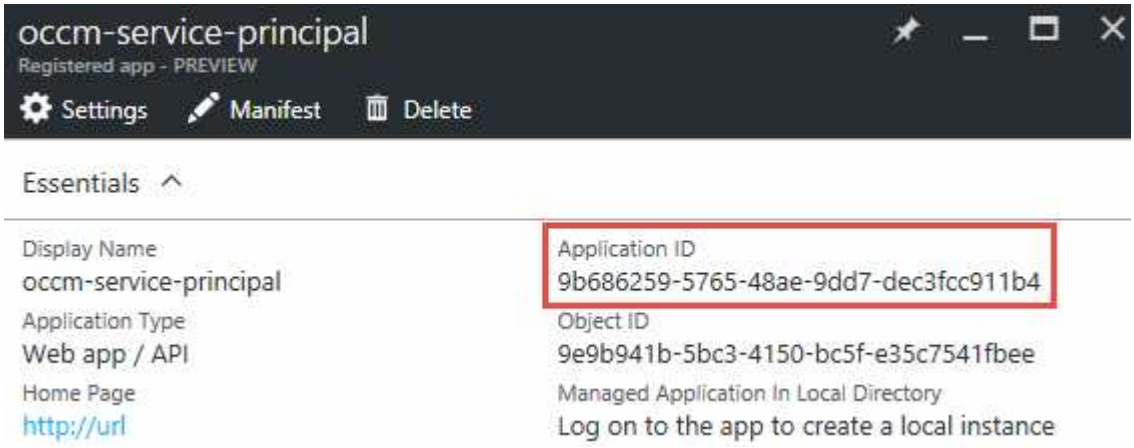
b. Entrez une description, sélectionnez une durée, puis cliquez sur **Enregistrer**.

c. Copiez la valeur de la clé.

Vous devez saisir la valeur clé lorsque vous ajoutez un compte de fournisseur cloud à Cloud Manager.

d. Cliquez sur **Propriétés**, puis copiez l'ID de l'application pour le principal de service.

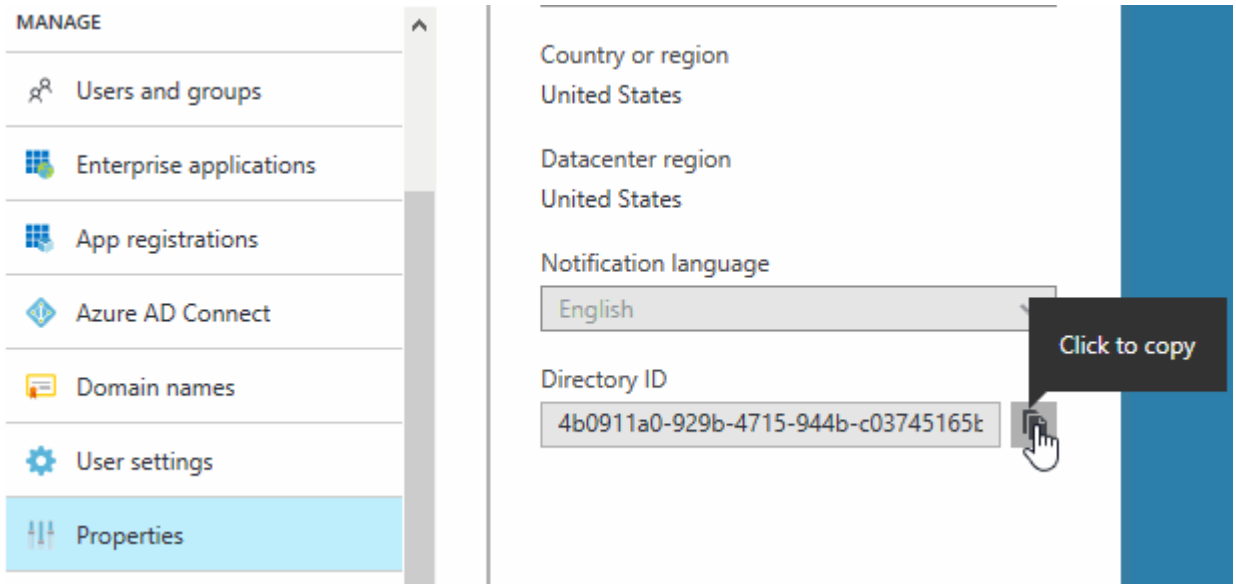
Comme la clé, vous devez saisir l'ID d'application dans Cloud Manager lorsque vous ajoutez un compte de fournisseur cloud à Cloud Manager.




6. Obtenez l'ID du locataire Active Directory pour votre entreprise :

a. Dans le menu Active Directory, cliquez sur **Propriétés**.

b. Copiez l'ID du répertoire.




Comme l'ID d'application et la clé d'application, vous devez entrer l'ID de locataire Active Directory lorsque vous ajoutez un compte de fournisseur cloud à Cloud Manager.

**Résultat**

Vous devez maintenant disposer d'un principal de service Active Directory et copier l'ID de l'application, la clé d'application et l'ID du locataire Active Directory. Vous devez saisir ces informations dans Cloud Manager lorsque vous ajoutez un compte de fournisseur cloud.

### Attribution du rôle d'opérateur Cloud Manager au principal de service

Vous devez associer le principal de service à un ou plusieurs abonnements Azure et lui attribuer le rôle d'opérateur Cloud Manager pour que Cloud Manager dispose des autorisations dans Azure.

#### Description de la tâche

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

#### Étapes

1. Dans le portail Azure, sélectionnez **abonnements** dans le volet gauche.
2. Sélectionnez l'abonnement.
3. Cliquez sur **contrôle d'accès (IAM)**, puis sur **Ajouter**.
4. Sélectionnez le rôle **opérateur OnCommand Cloud Manager**.
5. Recherchez le nom de l'application (vous ne pouvez pas le trouver dans la liste en faisant défiler).
6. Sélectionnez l'application, cliquez sur **Sélectionner**, puis sur **OK**.

#### Résultat

Le principal de service de Cloud Manager dispose désormais des autorisations Azure requises.

##### Ajout de comptes Azure à Cloud Manager

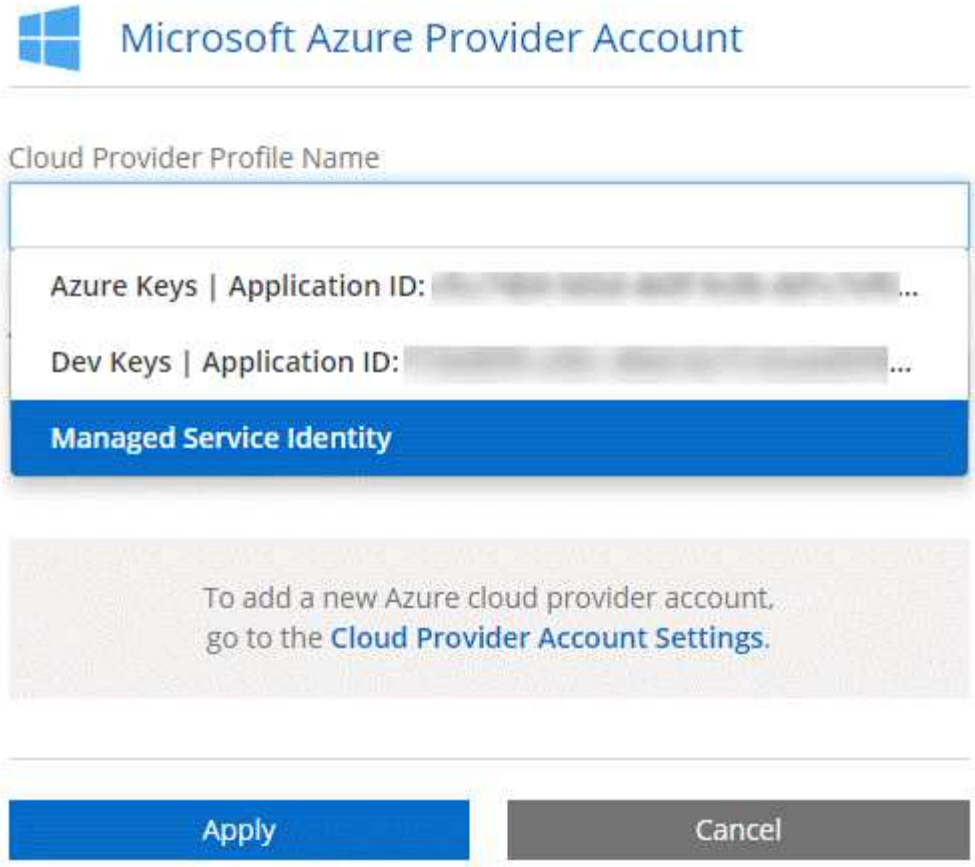
Une fois que vous avez autorisé à fournir un compte Azure, vous pouvez l'ajouter à Cloud Manager. Vous pouvez ainsi lancer les systèmes Cloud Volumes ONTAP de ce compte.

#### Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur la liste déroulante des tâches, puis sélectionnez **Paramètres du compte**.
2. Cliquez sur **Ajouter un nouveau compte** et sélectionnez **Microsoft Azure**.
3. Entrez des informations sur l'entité de sécurité du service Azure Active Directory qui accorde les autorisations requises.
4. Vérifiez que les exigences de la stratégie ont été respectées, puis cliquez sur **Créer un compte**.

#### Résultat

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




### Association d'abonnements Azure supplémentaires à une identité gérée

Cloud Manager vous permet de choisir le compte et l'abonnement Azure dans lesquels vous souhaitez déployer Cloud Volumes ONTAP. Vous ne pouvez pas sélectionner un autre abonnement Azure pour le profil d'identité gérée à moins d'associer le "identité gérée" avec ces abonnements.

#### Description de la tâche

Une identité gérée est la première "compte de fournisseur cloud" Lorsque vous déployez Cloud Manager à partir de NetApp Cloud Central. Lorsque vous avez déployé Cloud Manager, Cloud Central a créé le rôle OnCommand Cloud Manager Operator et l'a affecté à la machine virtuelle Cloud Manager.

#### Étapes

1. Connectez-vous au portail Azure.
2. Ouvrez le service **abonnements**, puis sélectionnez l'abonnement dans lequel vous souhaitez déployer des systèmes Cloud Volumes ONTAP.
3. Cliquez sur **contrôle d'accès (IAM)**.
   a. Cliquez sur **Ajouter** > **Ajouter une affectation de rôle**, puis ajoutez les autorisations suivantes :
      - Sélectionnez le rôle **opérateur OnCommand Cloud Manager**.

        L'opérateur OnCommand Cloud Manager est le nom par défaut fourni dans "Politique de Cloud Manager". Si vous avez choisi un autre nom pour le rôle, sélectionnez-le à la place.

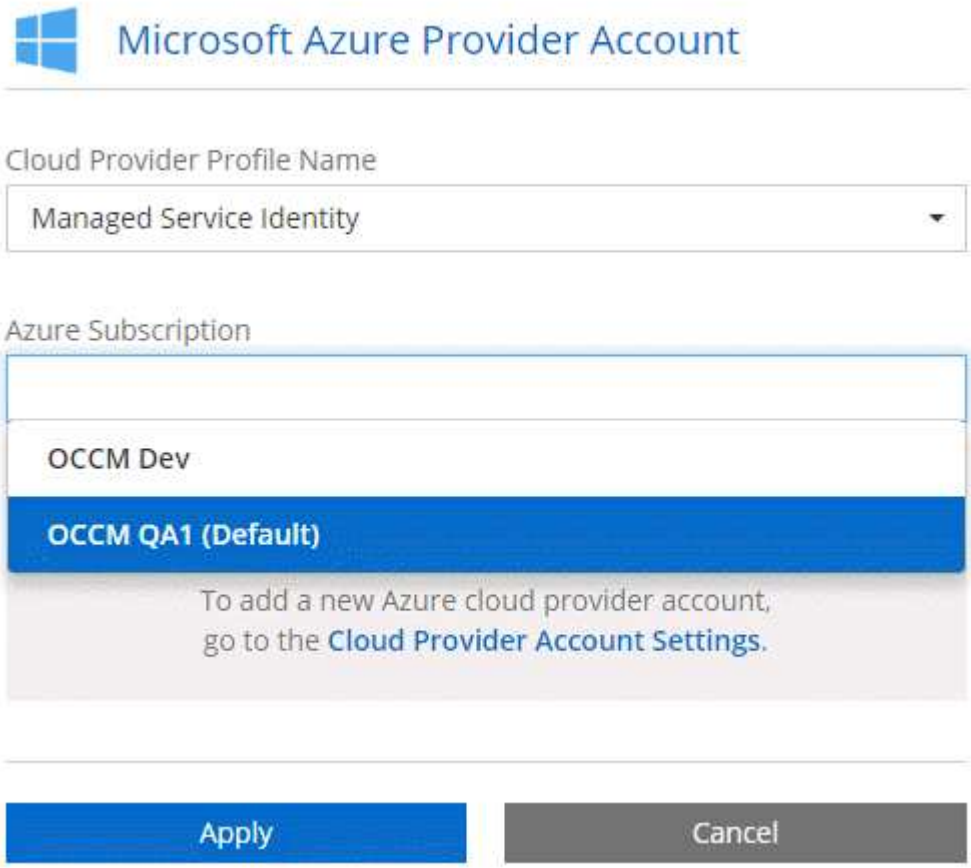
      - Attribuez l'accès à une **machine virtuelle**.

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

4. Répétez ces étapes pour les abonnements supplémentaires.

**Résultat**

Lorsque vous créez un nouvel environnement de travail, vous devriez désormais pouvoir sélectionner plusieurs abonnements Azure pour le profil d'identité géré.




## Ajout de comptes du site de support NetApp à Cloud Manager

Vous devez ajouter votre compte sur le site de support NetApp à Cloud Manager pour déployer un système BYOL. Il est également nécessaire d'enregistrer des systèmes avec paiement à l'utilisation et de mettre à niveau le logiciel ONTAP.

Découvrez dans cette vidéo comment ajouter des comptes sur le site de support NetApp à Cloud Manager. Ou faites défiler vers le bas pour lire les étapes.

[] | *https://img.youtube.com/vi/V2fLTyztqYQ/maxresdefault.jpg*

**Étapes**

1. Si vous ne disposez pas encore d'un compte sur le site de support NetApp, "inscrivez-vous pour en créer un".

2. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur la liste déroulante des tâches, puis sélectionnez **Paramètres du compte**.
3. Cliquez sur **Ajouter un compte** et sélectionnez **site de support NetApp**.
4. Spécifiez un nom pour le compte, puis entrez le nom d'utilisateur et le mot de passe.
   - Le compte doit être un compte de niveau client (et non un compte invité ou temporaire).
   - Si vous prévoyez de déployer des systèmes BYOL :
     - Le compte doit être autorisé à accéder aux numéros de série des systèmes BYOL.
     - Si vous avez acheté un abonnement BYOL sécurisé, un compte NSS sécurisé est requis.
5. Cliquez sur **Créer un compte.**

**Et la suite ?**

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

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

## Installation d'un certificat HTTPS pour un accès sécurisé

Par défaut, Cloud Manager utilise un certificat auto-signé pour l'accès HTTPS à la console Web. Vous pouvez installer un certificat signé par une autorité de certification (CA), qui offre une meilleure protection de la sécurité qu'un certificat auto-signé.

**Étapes**

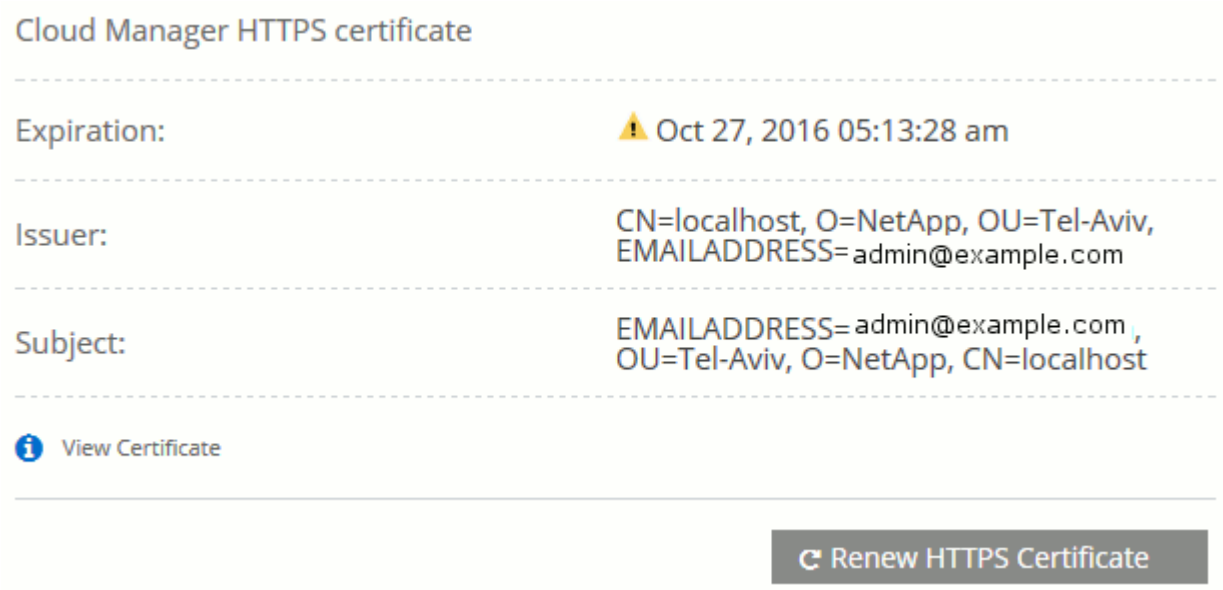
1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur la liste déroulante des tâches, puis sélectionnez **HTTPS Setup**.
2. Dans la page Configuration HTTPS, installez un certificat en générant une requête de signature de certificat (CSR) ou en installant votre propre certificat signé par l'autorité de certification :

| Option | Description |
|---|---|
| Générez une RSC | a. Entrez le nom d'hôte ou le DNS de l'hôte Cloud Manager (son nom commun), puis cliquez sur **generate CSR**.<br><br>Cloud Manager affiche une demande de signature de certificat.<br><br>b. Utilisez la RSC pour envoyer une demande de certificat SSL à une autorité de certification.<br><br>Le certificat doit utiliser le format X.509 encodé au format PEM (Privacy Enhanced Mail) Base-64.<br><br>c. Copiez le contenu du certificat signé, collez-le dans le champ certificat, puis cliquez sur **installer**. |

| Option | Description |
| --- | --- |
| Installez votre propre certificat signé par l'autorité de certification | a. Sélectionnez **installer le certificat signé CA**.<br>b. Chargez le fichier de certificat et la clé privée, puis cliquez sur **installer**.<br>Le certificat doit utiliser le format X.509 encodé au format PEM (Privacy Enhanced Mail) Base-64. |

**Résultat**

Cloud Manager utilise désormais le certificat signé par l'autorité de certification pour fournir un accès HTTPS sécurisé. L'image suivante montre un système Cloud Manager configuré pour un accès sécurisé :




## Configuration des utilisateurs et des locataires

Cloud Manager vous permet d'ajouter des utilisateurs Cloud Central à Cloud Manager et d'isoler les environnements de travail à l'aide de locataires.

### Ajout d'utilisateurs à Cloud Manager

Si d'autres utilisateurs doivent utiliser votre système Cloud Manager, ils doivent s'inscrire à un compte dans NetApp Cloud Central. Vous pouvez ensuite ajouter les utilisateurs à Cloud Manager.

**Étapes**

1. Si l'utilisateur n'a pas encore de compte dans NetApp Cloud Central, envoyez-lui un lien vers votre système Cloud Manager et demandez-lui de s'inscrire.

   Attendez que l'utilisateur confirme qu'il s'est inscrit à un compte.

2. Dans Cloud Manager, cliquez sur l'icône de l'utilisateur, puis sur **Afficher les utilisateurs**.
3. Cliquez sur **nouvel utilisateur**.
4. Entrez l'adresse e-mail associée au compte d'utilisateur, sélectionnez un rôle et cliquez sur **Ajouter**.

**Et la suite ?**

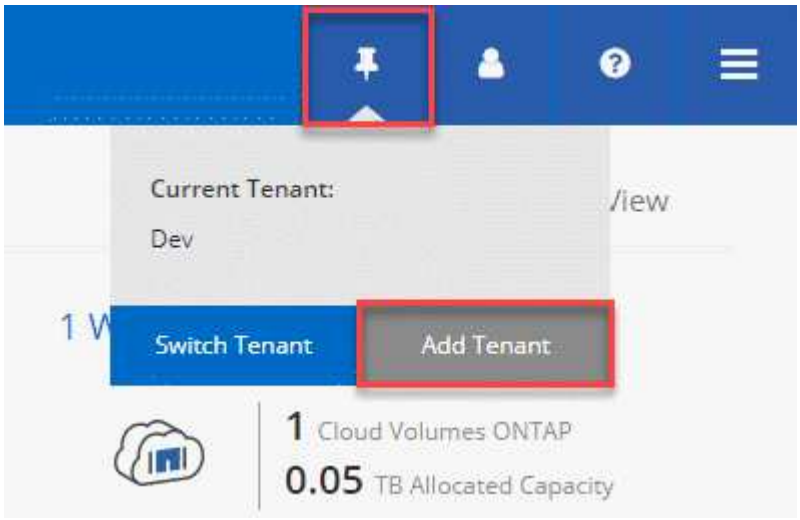
Informez l'utilisateur qu'il peut désormais se connecter au système Cloud Manager.

### Création de locataires

Les locataires vous permettent d'isoler vos environnements de travail en groupes distincts. Vous créez un ou plusieurs environnements de travail au sein d'un locataire. "En savoir plus sur les locataires".

**Étapes**

1. Cliquez sur l'icône locataires, puis sur **Ajouter locataire**.




2. Entrez un nom, une description et un centre de coûts, si nécessaire.
3. Cliquez sur **Enregistrer**.

**Et la suite ?**

Vous pouvez à présent passer à ce nouveau locataire et ajouter à ce locataire les administrateurs des locataires et de l'environnement de travail.

## 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.

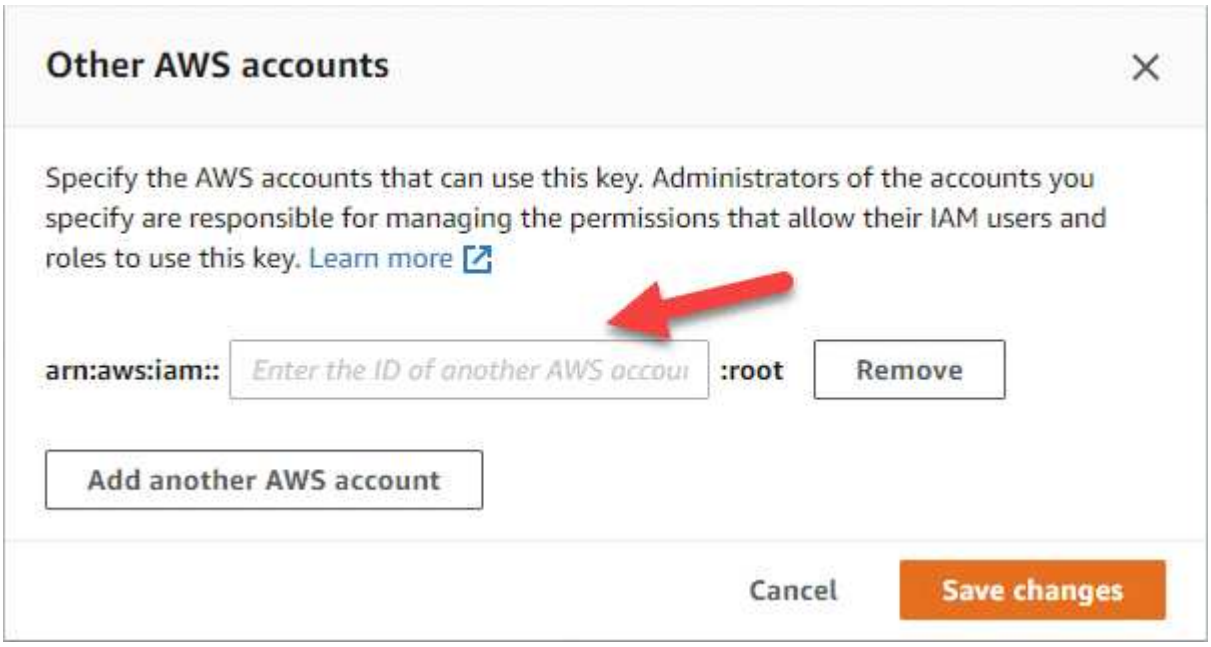
   b. Sélectionnez la touche.

   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".

# Configuration réseau requise

## Configuration réseau requise pour Cloud Manager

Vous devez configurer votre réseau pour que Cloud Manager puisse déployer les systèmes Cloud Volumes ONTAP dans AWS ou dans Microsoft Azure. L'étape la plus importante consiste à garantir l'accès Internet sortant à différents terminaux.

Si votre réseau utilise un serveur proxy pour toutes les communications avec Internet, Cloud Manager vous invite à spécifier le proxy lors de la configuration. Vous pouvez également spécifier le serveur proxy à partir de la page Paramètres. Reportez-vous à la section "Configuration de Cloud Manager pour utiliser un serveur proxy".

### Connexion aux réseaux cibles

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

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

### Accès Internet sortant

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

Les sections suivantes identifient les terminaux spécifiques.

#### Accès Internet sortant pour gérer Cloud Volumes ONTAP dans AWS

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

| Terminaux | Objectif |
|---|---|
| Services AWS (amazonaws.com):<br>• CloudFormation<br>• Cloud de calcul élastique (EC2)<br>• Service de gestion des clés (KMS)<br>• Service de jetons de sécurité (STS)<br>• Service de stockage simple (S3)<br>Le noeud final exact dépend de la région dans laquelle vous déployez Cloud Volumes ONTAP. "Reportez-vous à la documentation AWS pour plus de détails." | Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans AWS. |
| https://api.services.cloud.netapp.com:443 | Demandes d'API à NetApp Cloud Central. |

| Terminaux | Objectif |
| --- | --- |
| https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com | Permet d'accéder aux images logicielles, aux manifestes et aux modèles. |
| https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com | Permet à Cloud Manager d'accéder aux manifestes, aux modèles et aux images de mise à niveau Cloud Volumes ONTAP et de les télécharger. |
| https://kinesis.us-east-1.amazonaws.com | Permet à NetApp de diffuser des données à partir d'enregistrements d'audit. |
| https://cloudmanager.cloud.netapp.com | Communication avec le service Cloud Manager, notamment les comptes Cloud Central. |
| https://netapp-cloud-account.auth0.com | Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs. |
| https://support.netapp.com/aods/asupmessage https://support.netapp.com/asupprod/post/1.0/postAsup | Communication avec NetApp AutoSupport. |
| https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement | Communication avec NetApp pour l'enregistrement des licences et du support. |
| 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 :<br>• https://repo1.maven.org/maven2<br>• https://oss.sonatype.org/content/repositories<br>• https://repo.typesafe.org<br>Les emplacements tiers sont sujets à modification. | Lors des mises à niveau, Cloud Manager télécharge les derniers packages pour les dépendances tierces. |

### Accès Internet sortant pour gérer Cloud Volumes ONTAP à Azure

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

| Terminaux | Objectif |
| --- | --- |
| https://management.azure.com https://login.microsoftonline.com | Permet à Cloud Manager de déployer et de gérer Cloud Volumes ONTAP dans la plupart des régions d'Azure. |
| 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. |

| Terminaux | Objectif |
| --- | --- |
| https://api.services.cloud.netapp.com:443 | Demandes d'API à NetApp Cloud Central. |
| https://cloud.support.netapp.com.s3.us-west-1.amazonaws.com | Permet d'accéder aux images logicielles, aux manifestes et aux modèles. |
| https://cognito-idp.us-east-1.amazonaws.com https://cognito-identity.us-east-1.amazonaws.com https://sts.amazonaws.com | Permet à Cloud Manager d'accéder aux manifestes, aux modèles et aux images de mise à niveau Cloud Volumes ONTAP et de les télécharger. |
| https://kinesis.us-east-1.amazonaws.com | Permet à NetApp de diffuser des données à partir d'enregistrements d'audit. |
| https://netapp-cloud-account.auth0.com | Communication avec NetApp Cloud Central pour une authentification centralisée des utilisateurs. |
| https://mysupport.netapp.com | Communication avec NetApp AutoSupport. |
| https://support.netapp.com/svcgw https://support.netapp.com/ServiceGW/entitlement | Communication avec NetApp pour l'enregistrement des licences et du support. |
| 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 :<br>• https://repo1.maven.org/maven2<br>• https://oss.sonatype.org/content/repositories<br>• https://repo.typesafe.org<br>Les emplacements tiers sont sujets à modification. | Lors des mises à niveau, Cloud Manager télécharge les derniers packages pour les dépendances tierces. |

**Accès Internet sortant à partir de votre navigateur Web**

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

| Terminaux | Objectif |
| --- | --- |
| L'hôte Cloud Manager | Vous devez entrer l'adresse IP de l'hôte depuis un navigateur Web pour charger la console Cloud Manager.<br><br>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 :<br><br>• Une adresse IP privée fonctionne si vous disposez d'un VPN et d'un accès direct à votre réseau virtuel<br>• Un IP public fonctionne dans tous les scénarios de mise en réseau<br><br>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. |

**Accès Internet sortant pour installer Cloud Manager sur un hôte Linux**

Le programme d'installation de Cloud Manager doit accéder aux URL suivantes pendant le processus d'installation :

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

**Ports et groupes de sécurité**

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

## Configuration réseau requise pour Cloud Volumes ONTAP dans AWS

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

Vous recherchez la liste des terminaux auxquels Cloud Manager a besoin d'un accès ? Ils sont désormais gérés dans un seul emplacement. "Cliquez ici pour plus de détails".

### Configuration réseau AWS générale requise pour Cloud Volumes ONTAP

Les exigences suivantes doivent être respectées dans AWS.

#### Accès Internet sortant pour les nœuds Cloud Volumes ONTAP

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

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

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

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

#### Accès Internet sortant pour le médiateur haute disponibilité

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

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

#### 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 Quick Start Reference Deployment".

### Configuration réseau AWS requise pour Cloud Volumes ONTAP HA dans plusieurs AZS

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

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

### Zones de disponibilité

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

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

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

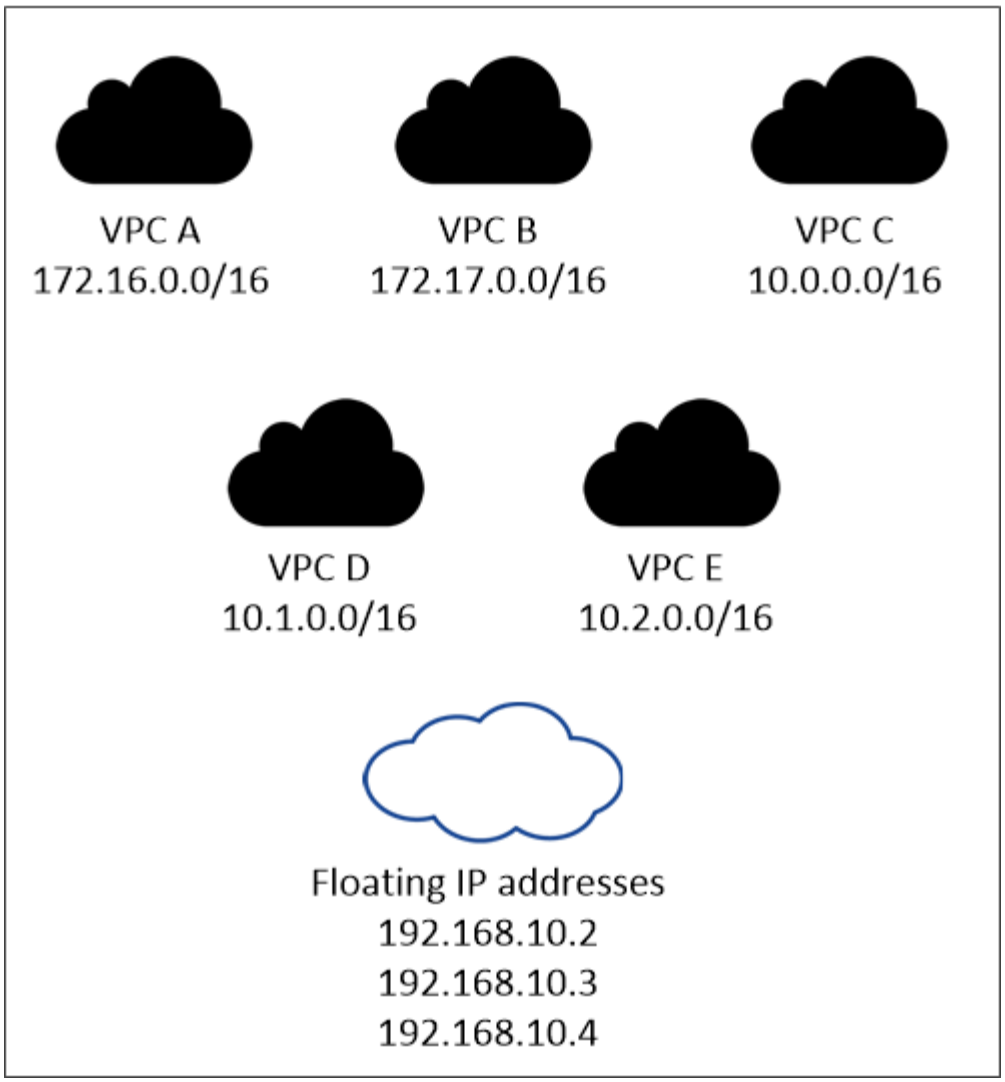
Une adresse IP flottante concerne la gestion du cluster, l'une concerne les données NFS/CIFS sur le nœud 1 et l'autre les données NFS/CIFS sur le nœud 2. Une quatrième adresse IP flottante est facultative pour la gestion des SVM.

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

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

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

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




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

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

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

**Tables de routage**

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

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

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

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

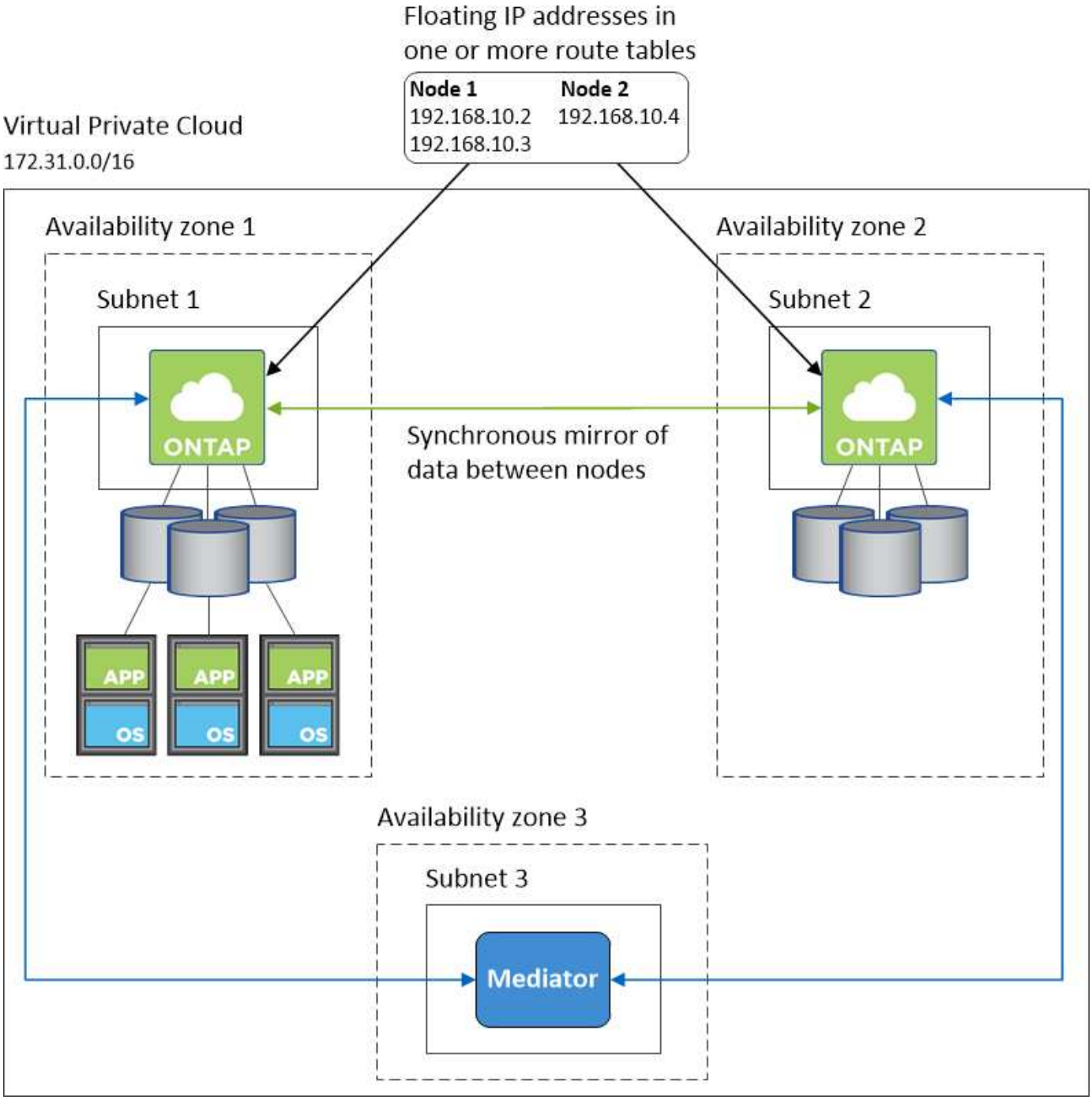
### Connexion aux outils de gestion NetApp

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

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

#### Exemple de configuration

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




### Exemples de configurations VPC

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

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

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

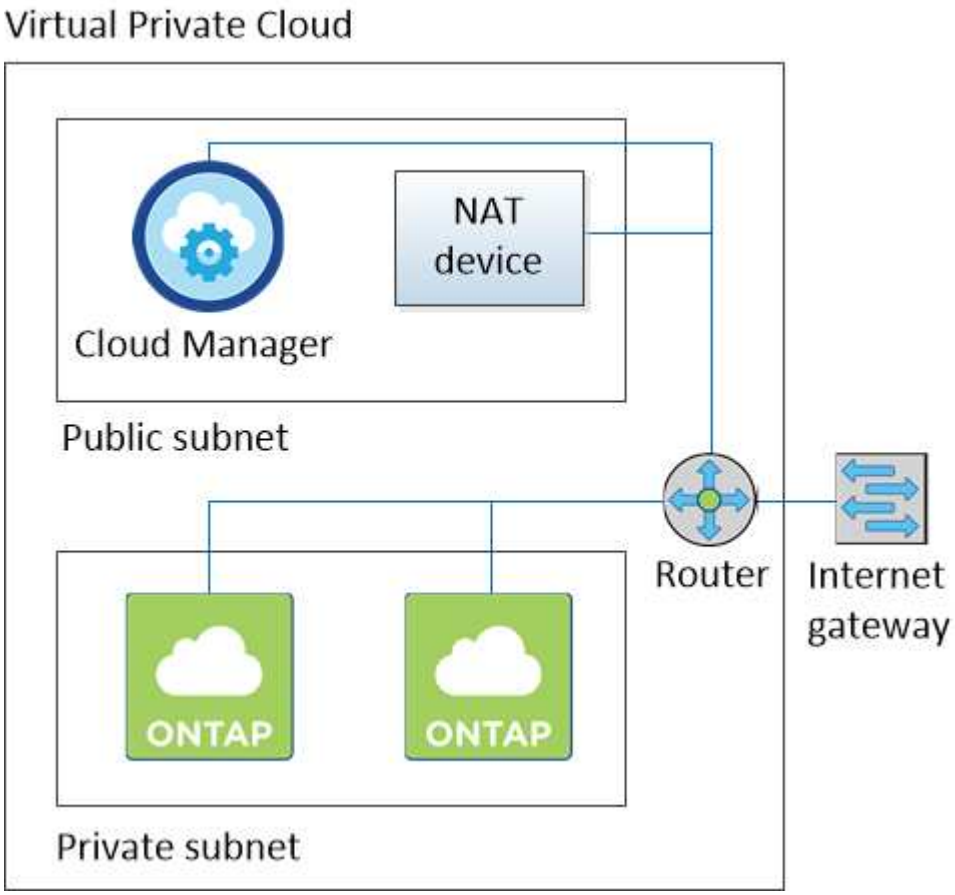
Cette configuration VPC inclut des sous-réseaux publics et privés, une passerelle Internet qui connecte le VPC à Internet et une passerelle NAT ou une instance NAT dans le sous-réseau public qui active le trafic Internet

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

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

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

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




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

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

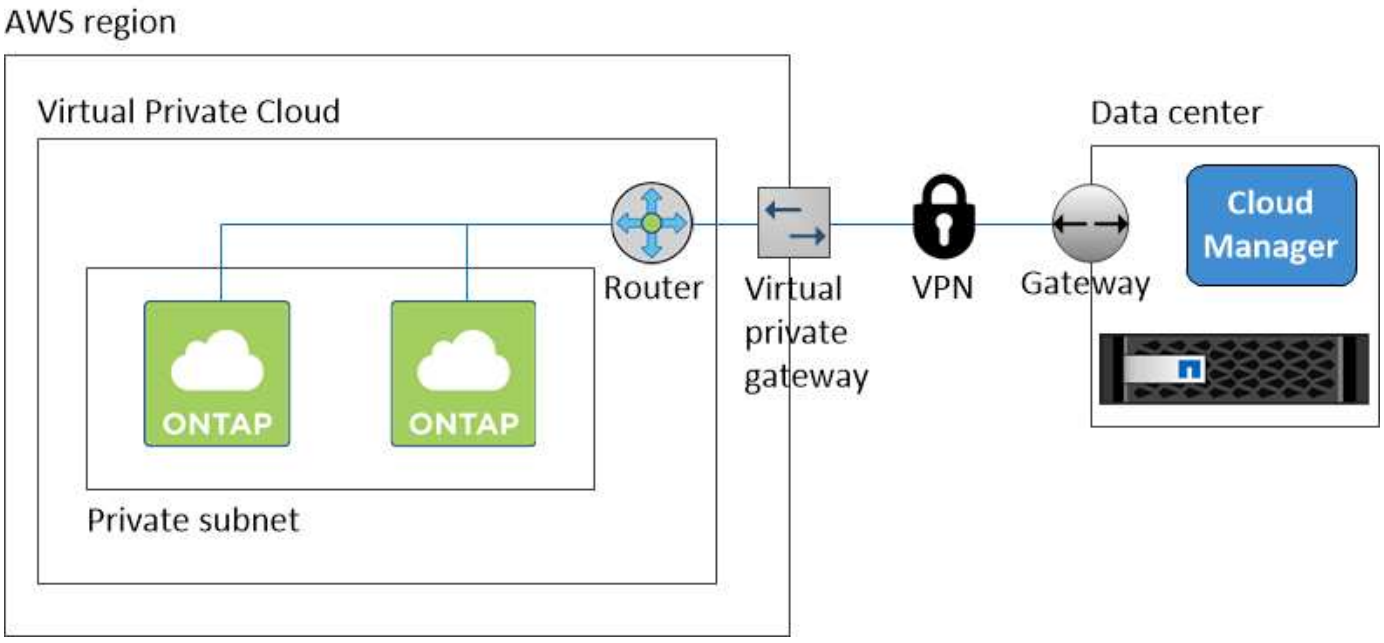
Vous pouvez également utiliser un serveur proxy dans cette configuration pour autoriser l'accès à Internet. Le serveur proxy peut se trouver dans votre data center ou dans AWS.

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

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

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

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




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

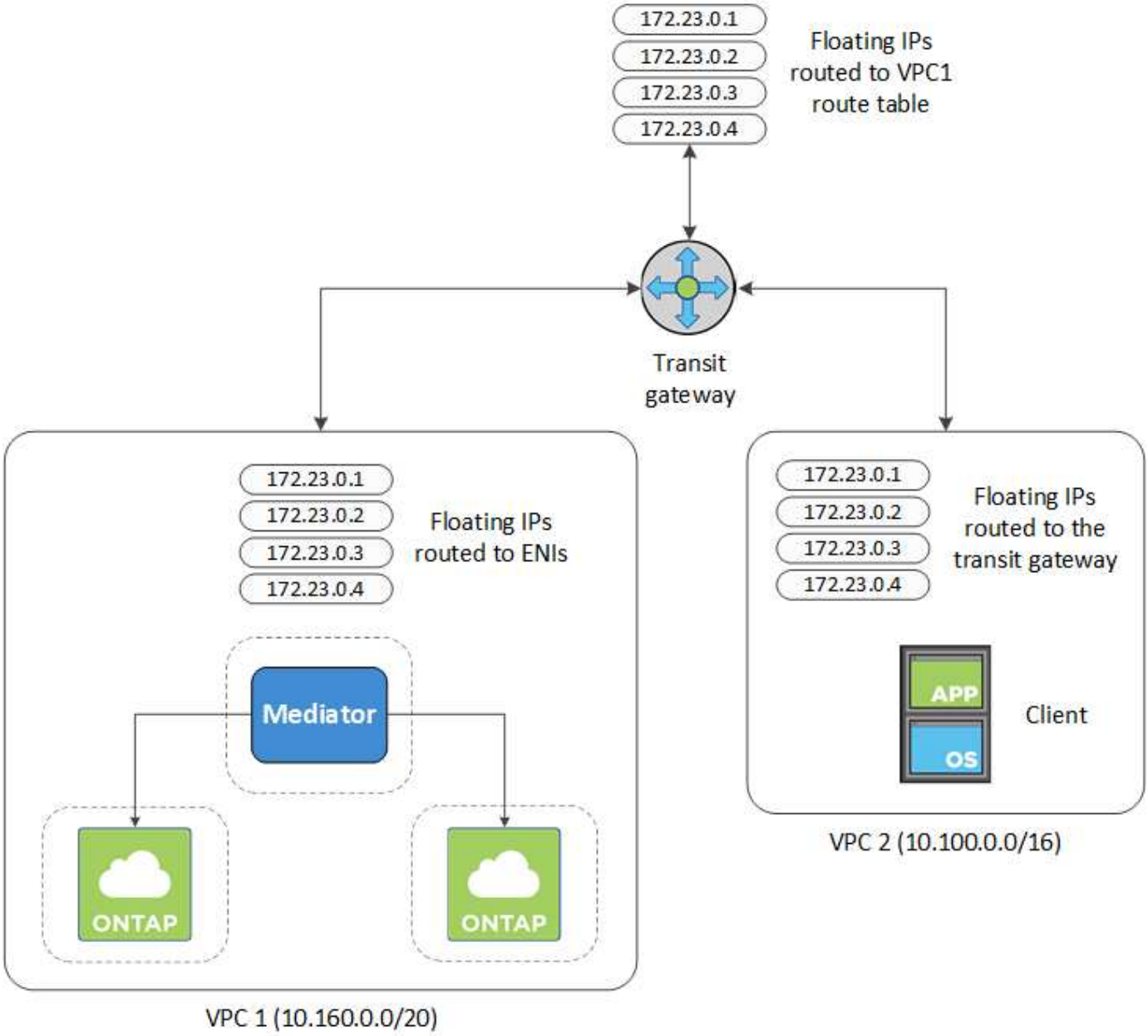
Configurez une passerelle de transit AWS pour permettre l'accès aux adresses IP flottantes d'une paire HA à l'extérieur du VPC où réside la paire HA.

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

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

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

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

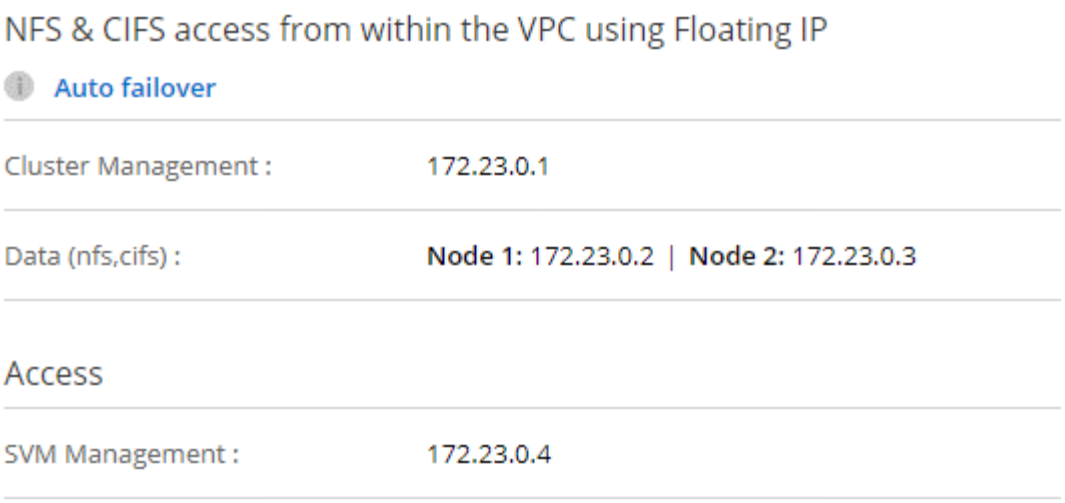



Les étapes suivantes montrent comment configurer une configuration similaire.

**Étapes**

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

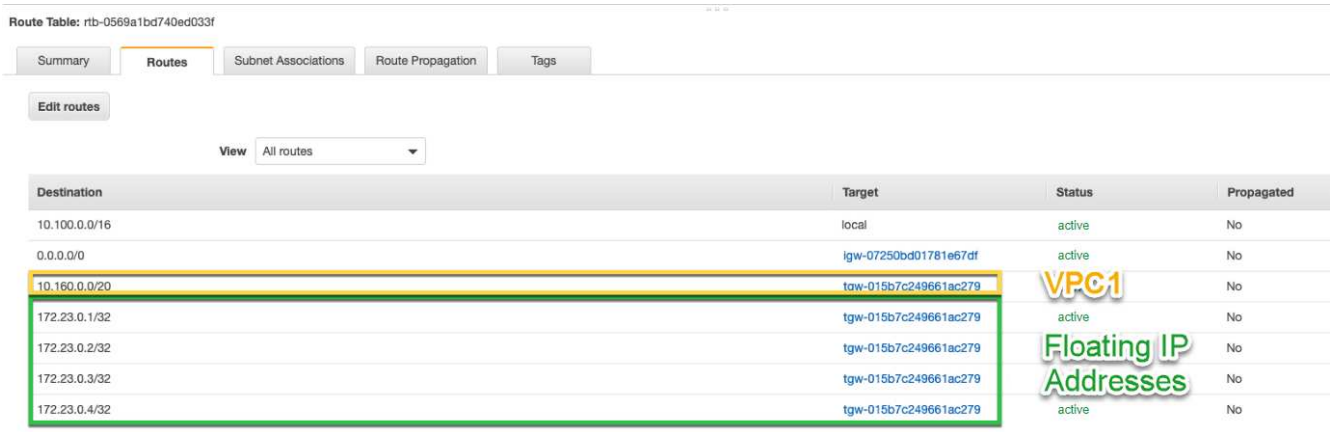
   Les adresses IP flottantes se trouvent sur la page des informations sur l'environnement de travail dans Cloud Manager. Voici un exemple :




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


3. Modifiez la table de routage des VPC qui doivent accéder aux adresses IP flottantes.
   a. Ajoutez des entrées de route aux adresses IP flottantes.
   b. Ajoutez une entrée de route au bloc CIDR du VPC où réside la paire HA.

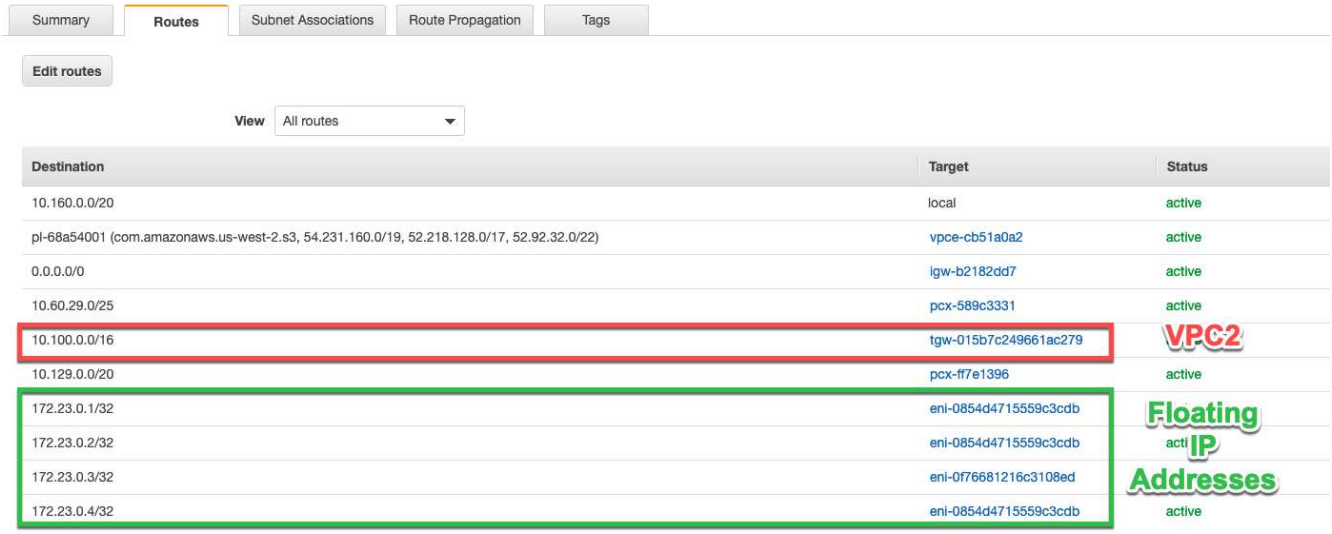
      L'exemple d'image suivant montre la table de route pour VPC 2, qui comprend les routes vers VPC 1 et les adresses IP flottantes.




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

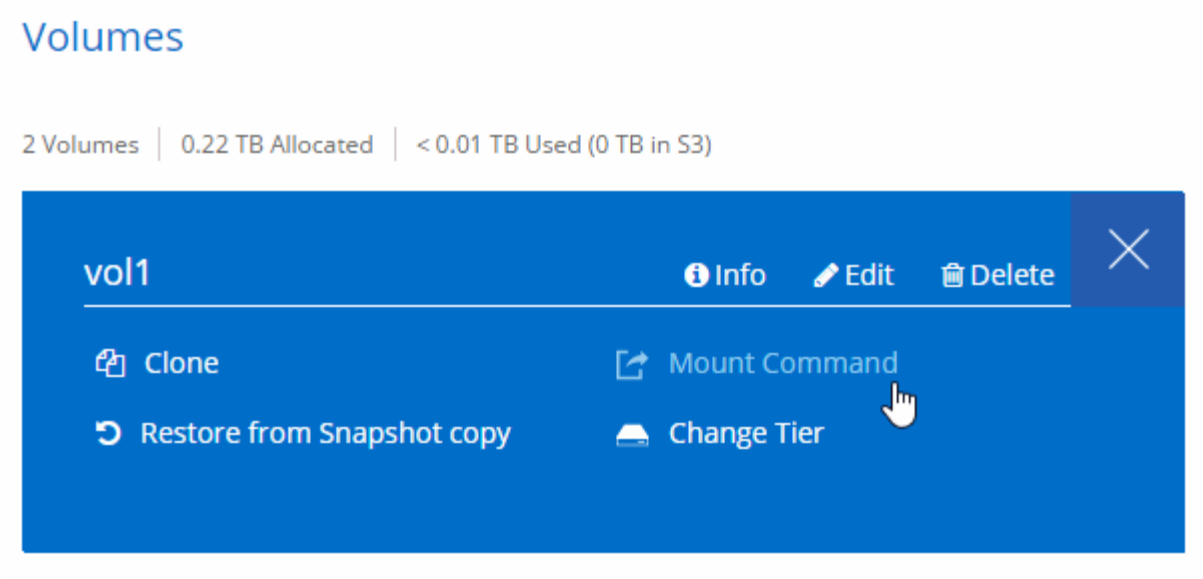
   Cette étape est importante car elle termine le routage entre les VPC.

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




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

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




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

## Configuration réseau requise pour Cloud Volumes ONTAP dans Azure

Vous devez configurer votre réseau Azure pour que les systèmes Cloud Volumes ONTAP puissent fonctionner correctement.

Vous recherchez la liste des terminaux auxquels Cloud Manager a besoin d'un accès ? Ils sont désormais gérés dans un seul emplacement. "Cliquez ici pour plus de détails".

### 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 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

### 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 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 un terminal de service VNet tant que Cloud Manager dispose des autorisations requises :

```
"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".

# D'autres options de déploiement

## Conditions de l'hôte Cloud Manager

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

**Types d'instances AWS EC2 pris en charge**

t3.medium (recommandé), t2.medium et m4.large

**Tailles de VM Azure prises en charge**

A2, D2 v2 ou D2 v3 (selon disponibilité)

**Systèmes d'exploitation pris en charge**

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

  Le système Red Hat Enterprise Linux doit être enregistré avec Red Hat Subscription Management. S'il n'est pas enregistré, le système ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis lors de l'installation de Cloud Manager.

  Cloud Manager est pris en charge sur les versions anglaises de ces systèmes d'exploitation.

**Hyperviseur**

Un hyperviseur bare Metal ou hébergé certifié pour exécuter CentOS ou Red Hat Enterprise Linuxhttps://access.redhat.com/certified-hypervisors["Solution Red Hat : quels hyperviseurs sont certifiés

pour l'exécution de Red Hat Enterprise Linux ?"^]

**CPU**

2,27 GHz ou plus avec deux cœurs

**RAM**

4 Go

**Espace disque disponible**

50 Go

**Accès Internet sortant**

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

**Ports**

Les ports suivants doivent être disponibles :

- 80 pour l'accès HTTP
- 443 pour l'accès HTTPS
- 3306 pour la base de données Cloud Manager
- 8080 pour le proxy API Cloud Manager

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

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

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

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

## Installation de Cloud Manager sur un hôte Linux existant

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

**Avant de commencer**

- Un système Red Hat Enterprise Linux doit être enregistré avec Red Hat Subscription Management. S'il n'est pas enregistré, le système ne peut pas accéder aux référentiels pour mettre à jour les logiciels tiers requis lors de l'installation de Cloud Manager.

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

**Description de la tâche**

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

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

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

**Étapes**

1. Examen des exigences de mise en réseau :
   - "Configuration réseau requise pour Cloud Manager"
   - "Configuration réseau requise pour Cloud Volumes ONTAP pour AWS"
   - "Configuration réseau requise pour Cloud Volumes ONTAP pour Azure"
2. Révision "Conditions de l'hôte Cloud Manager".
3. Téléchargez le logiciel à partir du "Site de support NetApp", Puis copiez-le sur l'hôte Linux.

   Pour obtenir de l'aide sur la connexion et la copie du fichier vers une instance EC2 dans AWS, reportez-vous à la section "Documentation AWS : connexion à votre instance Linux à l'aide de SSH".

4. Attribuez des autorisations pour exécuter le script.

   **Exemple**

   ```
    chmod +x OnCommandCloudManager-V3.6.3.sh
   . Exécutez le script d'installation :
   ```

   ```
   ./OnCommandCloudManager-V3.6.3.sh [silent] [proxy=ipaddress]
   [proxyport=port] [proxyuser=user_name] [proxypwd=password]
   ```

   *silent* exécute l'installation sans vous demander des informations.

   *Proxy* est requis si l'hôte Cloud Manager se trouve derrière un serveur proxy.

   *proxyport* est le port du serveur proxy.

   *proxyuser* est le nom d'utilisateur du serveur proxy, si une authentification de base est requise.

   *proxypwd* est le mot de passe du nom d'utilisateur que vous avez spécifié.

5. Sauf si vous avez spécifié le paramètre silencieux, tapez **y** pour continuer le script, puis entrez les ports HTTP et HTTPS lorsque vous y êtes invité.

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

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

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

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

   <a href="https://<em>ipaddress</em>:<em>port</em>" class="bare">https://<em>ipaddress</em>:<em>port</em></a>

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

   <em>Port</em> est nécessaire si vous avez modifié les ports HTTP (80) ou HTTPS (443) par défaut. Par exemple, si le port HTTPS a été modifié en 8443, vous pouvez entrer <a href="https://<em>ipaddress</em>:8443" class="bare">https://<em>ipaddress</em>:8443</a>

7. Inscrivez-vous à un compte NetApp Cloud Central ou connectez-vous si vous en possédez déjà un.
8. Lorsque vous vous inscrivez ou que vous vous connectez, Cloud Manager ajoute automatiquement votre compte utilisateur en tant qu'administrateur de ce système.
9. Après vous être connecté, entrez un nom pour ce système Cloud Manager.

**Une fois que vous avez terminé**

Configurez des autorisations pour vos comptes AWS et Azure afin que Cloud Manager puisse déployer Cloud Volumes ONTAP :

- Si vous souhaitez déployer Cloud Volumes ONTAP dans AWS, "Configurez un compte AWS, puis ajoutez-le à Cloud Manager".
- Si vous souhaitez déployer Cloud Volumes ONTAP dans Azure, "Configurez un compte Azure, puis ajoutez-le à Cloud Manager".

## Lancement de Cloud Manager à partir d'AWS Marketplace

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

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

**Description de la tâche**

La procédure suivante décrit le lancement de l'instance à partir de la console EC2, car la console vous permet d'associer un rôle IAM à l'instance Cloud Manager. Cette opération n'est pas possible avec l'option 1-clic.

**Étapes**

1. Créer une règle IAM et un rôle pour l'instance EC2 :

a. Téléchargez la politique IAM de Cloud Manager à partir de l'emplacement suivant :

"NetApp OnCommand Cloud Manager : Politiques AWS et Azure"

b. À partir de la console IAM, créez votre propre stratégie en copiant et en collant le texte de la stratégie IAM de Cloud Manager.

c. Créez un rôle IAM avec le type de rôle Amazon EC2 et associez la stratégie que vous avez créée à l'étape précédente au rôle.

2. Accédez au "Page Cloud Manager sur AWS Marketplace".
3. Cliquez sur **Continuer**.
4. Dans l'onglet lancement personnalisé, cliquez sur **lancer avec la console EC2** pour votre région, puis effectuez vos sélections :

a. Selon la disponibilité de la région, choisissez le type d'instance t3.medium (recommandé), t2.medium ou m4.large.

b. Sélectionnez un VPC, un sous-réseau, un rôle IAM et d'autres options de configuration qui répondent à vos besoins.

c. Conservez les options de stockage par défaut.

d. Entrez des étiquettes pour l'instance, si vous le souhaitez.

e. Spécifiez les méthodes de connexion requises pour l'instance de Cloud Manager : SSH, HTTP et HTTPS.

f. Cliquez sur **lancer**.

**Résultat**

AWS lance le logiciel avec les paramètres spécifiés. L'instance et le logiciel Cloud Manager doivent être exécutés en cinq minutes environ.

**Une fois que vous avez terminé**

Connectez-vous à Cloud Manager en entrant l'adresse IP publique ou l'adresse IP privée dans un navigateur Web, puis terminez l'assistant d'installation.

## Déploiement de Cloud Manager à partir d'Azure Marketplace

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

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

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

**Déploiement de Cloud Manager dans Azure**

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

**Étapes**

1. "Accédez à la page Azure Marketplace pour Cloud Manager".

2. Cliquez sur **l'obtenir maintenant**, puis sur **Continuer**.
3. Sur le portail Azure, cliquez sur **Créer** et suivez les étapes de configuration de la machine virtuelle.

   Noter les éléments suivants lors de la configuration de la machine virtuelle :

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

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

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

     Ce paramètre est important, car une identité gérée permet à la machine virtuelle de Cloud Manager de s'identifier à Azure Active Directory sans fournir d'informations d'identification. "En savoir plus sur les identités gérées pour les ressources Azure".

4. Dans la page **Revue + créer**, vérifiez vos sélections et cliquez sur **Créer** pour démarrer le déploiement.

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

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

   <a href="http://<em>ipaddress</em>:80" class="bare">http://<em>ipaddress</em>:80</a>

   Lorsque vous vous connectez, Cloud Manager ajoute automatiquement votre compte utilisateur en tant qu'administrateur de ce système.

6. Après vous être connecté, entrez un nom pour le système Cloud Manager.

**Résultat**

Cloud Manager est maintenant installé et configuré. Vous devez accorder des autorisations Azure avant que les utilisateurs puissent déployer Cloud Volumes ONTAP dans Azure.

### Octroi d'autorisations Azure à Cloud Manager

Lorsque vous avez déployé Cloud Manager dans Azure, vous devez avoir activé une "identité gérée attribuée par le système". Vous devez maintenant accorder les autorisations Azure requises en créant un rôle personnalisé, puis en attribuant le rôle à la machine virtuelle Cloud Manager pour un ou plusieurs abonnements.

**Étapes**

1. Créez un rôle personnalisé à l'aide de la stratégie Cloud Manager :

   a. Téléchargez le "Politique de Cloud Manager Azure".

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

      Vous devez ajouter l'ID de chaque abonnement Azure à partir duquel les utilisateurs créeront des

systèmes Cloud Volumes ONTAP.

**Exemple**

« Assigner les Scopes » : [ »/abonnements/d333af45-0d07-4154-943d-c25fbzzzzzzzzzzz », «/abonnements/54b91999-b3e6-4599-908e-416e0zzzzzz », «/abonnements/8e474b-94b-4b-4b-4b-4b-4439-4b-4b-4b-4b-4b-4b-4b-4b-4b-4b-

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

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

**Définition de rôle az create --role-definition C:\Policy_for_Cloud_Manager_Azure_3.6.1.json**

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

2. Attribuez le rôle à la machine virtuelle Cloud Manager pour un ou plusieurs abonnements :
   a. Ouvrez le service **abonnements**, puis sélectionnez l'abonnement dans lequel vous souhaitez déployer des systèmes Cloud Volumes ONTAP.
   b. Cliquez sur **contrôle d'accès (IAM)**.
   c. Cliquez sur **Ajouter** > **Ajouter une affectation de rôle**, puis ajoutez les autorisations suivantes :
      - Sélectionnez le rôle **opérateur OnCommand Cloud Manager**.

        L'opérateur OnCommand Cloud Manager est le nom par défaut fourni dans "Politique de Cloud Manager". Si vous avez choisi un autre nom pour le rôle, sélectionnez-le à la place.

      - Attribuez l'accès à une **machine virtuelle**.
      - Sélectionnez l'abonnement dans lequel la machine virtuelle Cloud Manager a été créée.
      - Sélectionnez la machine virtuelle Cloud Manager.
      - Cliquez sur **Enregistrer**.
   d. Si vous souhaitez déployer Cloud Volumes ONTAP à partir d'abonnements supplémentaires, passez à cet abonnement, puis répétez ces étapes.

**Résultat**

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

## Déploiement de Cloud Manager dans une région Azure Government

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

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

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

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

**Étapes**

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

   Notez les éléments suivants lors de la configuration de la machine virtuelle :

   - Cloud Manager peut fonctionner de manière optimale avec des disques durs ou SSD.
   - Choisissez l'une des tailles de machine virtuelle recommandées : A2, D2 v2 ou D2 v3 (selon disponibilité).
   - Pour le groupe de sécurité réseau, il est préférable de choisir **Advanced**.

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

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

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

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

   <a href="http://<em>ipaddress</em>:80" class="bare">http://<em>ipaddress</em>:80</a>

   Lorsque vous vous connectez, Cloud Manager ajoute automatiquement votre compte utilisateur en tant qu'administrateur de ce système.

5. Après vous être connecté, entrez un nom pour le système Cloud Manager.

**Résultat**

Cloud Manager est maintenant installé et configuré. Vous devez accorder des autorisations Azure avant que les utilisateurs puissent déployer Cloud Volumes ONTAP dans Azure.

### Octroi d'autorisations Azure à Cloud Manager à l'aide d'une identité gérée

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

**Étapes**

1. Activer une identité gérée sur la machine virtuelle Cloud Manager :
   a. Accédez à la machine virtuelle Cloud Manager et sélectionnez **Identity**.
   b. Sous **System Assigned**, cliquez sur **On**, puis sur **Save**.
2. Créez un rôle personnalisé à l'aide de la stratégie Cloud Manager :

   a. Téléchargez le "Politique de Cloud Manager Azure".

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

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

   **Exemple**

   « Assigner les Scopes » : [ »/abonnements/d333af45-0d07-4154-943d-c25fbzzzzzzzzzz », «/abonnements/54b91999-b3e6-4599-908e-416e0zzzzzz », «/abonnements/8e474b-94b-4b-4b-4b-4b-4439-4b-4b-4b-4b-4b-4b-4b-4b-4b-4b-

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

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

   **Définition de rôle az create --role-definition C:\Policy_for_Cloud_Manager_Azure_3.6.1.json**

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

3. Attribuez le rôle à la machine virtuelle Cloud Manager pour un ou plusieurs abonnements :
   a. Ouvrez le service **abonnements**, puis sélectionnez l'abonnement dans lequel vous souhaitez déployer des systèmes Cloud Volumes ONTAP.
   b. Cliquez sur **contrôle d'accès (IAM)**.
   c. Cliquez sur **Ajouter**, cliquez sur **Ajouter une affectation de rôle**, puis ajoutez les autorisations :
      - Sélectionnez le rôle **opérateur OnCommand Cloud Manager**.

        L'opérateur OnCommand Cloud Manager est le nom par défaut fourni dans "Politique de Cloud Manager". Si vous avez choisi un autre nom pour le rôle, sélectionnez-le à la place.

      - Attribuez l'accès à une **machine virtuelle**.
      - Sélectionnez l'abonnement dans lequel la machine virtuelle Cloud Manager a été créée.
      - Saisissez le nom de la machine virtuelle, puis sélectionnez-la.
      - Cliquez sur **Enregistrer**.
   d. Si vous souhaitez déployer Cloud Volumes ONTAP à partir d'abonnements supplémentaires, passez à cet abonnement, puis répétez ces étapes.

**Résultat**

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

## Installation de Cloud Manager dans une région Azure Allemagne

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

**Étapes**

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

**Une fois que vous avez terminé**

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

# Le déploiement de Cloud Volumes ONTAP

## Avant de créer des systèmes Cloud Volumes ONTAP

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

Votre administrateur doit avoir suivi les instructions pour se mettre en route "Dans AWS" ou "Dans Azure", et éventuellement "Configurez Cloud Manager".

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

- Les exigences de mise en réseau AWS et Azure ont été respectées pour Cloud Manager et Cloud Volumes ONTAP.
- Cloud Manager dispose d'autorisations pour effectuer des opérations dans AWS et Azure en votre nom.
- Chaque produit Cloud Volumes ONTAP que les utilisateurs déploieront a été souscrit à partir d'AWS Marketplace.
- Cloud Manager a été installé.
- (Facultatif) Des locataires supplémentaires ont été définis.
- (Facultatif) Des comptes utilisateur supplémentaires ont été créés, qui peuvent inclure les administrateurs locataires et les administrateurs d'environnement de travail.

## Connectez-vous à Cloud Manager

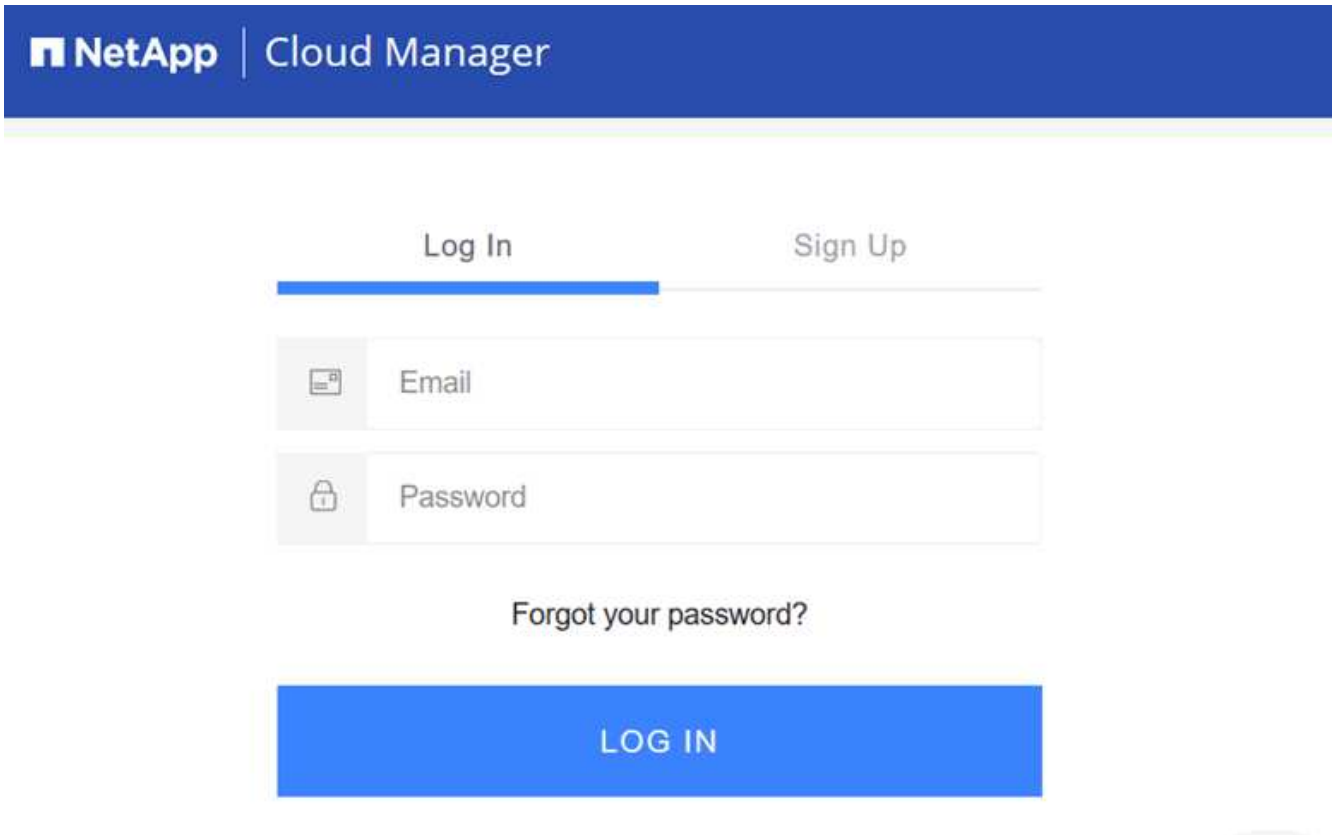
Vous pouvez vous connecter à Cloud Manager à partir de n'importe quel navigateur Web disposant d'une connexion au système Cloud Manager. Vous devez vous connecter à l'aide d'un "NetApp Cloud Central" compte utilisateur.

**Étapes**

1. Ouvrez un navigateur Web et connectez-vous à "NetApp Cloud Central".
2. Cliquez sur **allez dans Services de données cloud** et sélectionnez **Cloud Volumes ONTAP**.
3. Cliquez sur **accédez à Cloud Manager** pour le système Cloud Manager auquel vous souhaitez accéder.

   Si aucun système n'est répertorié, assurez-vous que l'administrateur Cloud Manager a ajouté votre compte NetApp Cloud Central au système.

4. Connectez-vous à Cloud Manager à l'aide de votre compte NetApp Cloud Central.




# Planification de votre configuration Cloud Volumes ONTAP

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

## Choix d'un type de licence

Cloud Volumes ONTAP est disponible dans AWS et Azure avec deux options de tarification : 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 9.5"
- "Configurations prises en charge pour Cloud Volumes ONTAP 9.4"
- "Configurations prises en charge pour ONTAP Cloud 9.3"

## 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 9.5"

- "Limites de stockage pour Cloud Volumes ONTAP 9.4"
- "Limites de stockage pour le cloud ONTAP 9.3"

## 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*

## Dimensionnement du système dans Azure

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

### Type de machine virtuelle

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

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

### Type de disque Azure

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

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

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

  Pour plus d'informations sur les cas d'utilisation de ces disques, reportez-vous à la section "Documentation Microsoft Azure : présentation du stockage Microsoft Azure".

### Taille des disques Azure

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

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

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

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

Avec un stockage standard, les performances sont les mêmes pour toutes les tailles de disques. Choisissez la taille de disque en fonction de la capacité dont vous avez besoin.

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

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

## 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.

## 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 | |

| Informations sur AWS | Votre valeur |
| --- | --- |
| Adresse IP flottante pour les données du nœud 2 | |
| Tables de routage pour les adresses IP flottantes | |

### 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) | |

# Activation de Flash cache sur Cloud Volumes ONTAP dans AWS

Certains types d'instances EC2 incluent le stockage NVMe local, que Cloud Volumes ONTAP utilise *Flash cache*. Flash cache accélère l'accès aux données grâce à la mise en cache intelligente en temps réel des données utilisateur et des métadonnées NetApp lues récemment. Il est efficace pour les charges de travail exigeant une capacité de lecture aléatoire maximale, dont les bases de données, la messagerie et les services de fichiers.

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

**Étapes**

1. Sélectionnez l'un des types d'instances EC2 suivants, disponibles avec les licences Premium et BYOL :
   - c5d.4xlarge
   - c5d.9xlarge
   - r5d.2xlarge
2. Désactiver la compression sur tous les volumes.

   La compression doit être désactivée sur tous les volumes pour tirer parti des améliorations des performances de Flash cache. Vous pouvez choisir aucune efficacité du stockage lors de la création d'un volume depuis Cloud Manager, ou encore créer un volume, puis "Désactiver la compression des données à l'aide de l'interface de ligne de commande".

# Lancement d’Cloud Volumes ONTAP dans AWS

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

## Lancement d’un seul système Cloud Volumes ONTAP dans AWS

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

### Avant de commencer

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

### Description de la tâche

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

### Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail**.
2. Sous Créer, sélectionnez **Cloud Volumes ONTAP**.
3. Sur la page Détails et informations d’identification, modifiez éventuellement le compte AWS, entrez un nom d’environnement de travail, ajoutez des étiquettes 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 :

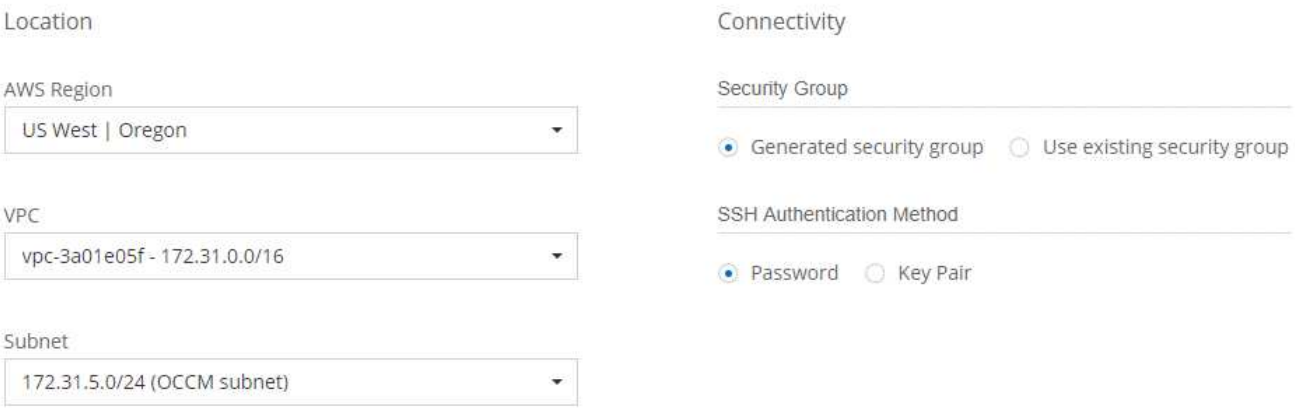
| Champ | Description |
|---|---|
| Changer de compte | Vous pouvez choisir un autre compte si vous avez ajouté d’autres comptes de fournisseurs de services clouds. Pour plus de détails, voir "Ajout de comptes de fournisseurs de services clouds à Cloud Manager". |
| Nom de l’environnement de travail | Cloud Manager utilise le nom de l’environnement de travail pour nommer à la fois le système Cloud Volumes ONTAP et l’instance Amazon EC2. 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 AWS sont des métadonnées pour vos ressources AWS. Cloud Manager ajoute les balises à l'instance Cloud Volumes ONTAP et à chaque ressource AWS associée à l'instance. Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section "Documentation AWS : balisage des ressources Amazon EC2". |
| Informations d'identification | Il s'agit des informations d'identification du compte d'administration du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via OnCommand System Manager ou sa CLI. |

Si les clés AWS n'ont pas été spécifiées pour votre compte Cloud Manager, vous êtes invité à les saisir après avoir cliqué sur Continuer. Vous devez les saisir avant de pouvoir continuer.

4. Sur la page emplacement et connectivité, entrez les informations de réseau que vous avez enregistrées dans la fiche AWS, puis cliquez sur **Continuer**.

   L'image suivante montre la page emplacement et connectivité remplie :




5. Sur la page Data Encryption, choisissez aucun chiffrement de données ou chiffrement 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.

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

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

6. Sur la page de compte du site de licence et de support, indiquez si vous souhaitez utiliser le paiement à l'utilisation ou BYOL, puis spécifiez 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. Sur la page modules 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.

8. Sur la page IAM Role (Rôle IAM), vous devez conserver l'option par défaut pour permettre à Cloud Manager de créer le rôle qui vous convient.

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

9. Sur la page licences, modifiez la version de Cloud Volumes ONTAP selon vos besoins, sélectionnez une licence, un type d'instance, la location d'instance, puis cliquez sur **Continuer**.

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

   > Si une version plus récente de Release Candidate, General Availability ou patch est disponible pour la version sélectionnée, Cloud Manager met à jour le système à cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.4 RC1 et 9.4 GA. La mise à jour ne se produit pas d'une version à une autre, par exemple de la version 9.3 à la version 9.4.

10. Sur la page sous-jacente Storage Resources, choisissez les paramètres de l'agrégat initial : un type de disque, une taille pour chaque disque et le Tiering S3 doit être activé ou non.

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

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

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

11. Sur la page vitesse d'écriture et WORM, choisissez **Normal** ou **vitesse d'écriture élevée** et activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

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

    "En savoir plus sur le stockage WORM".

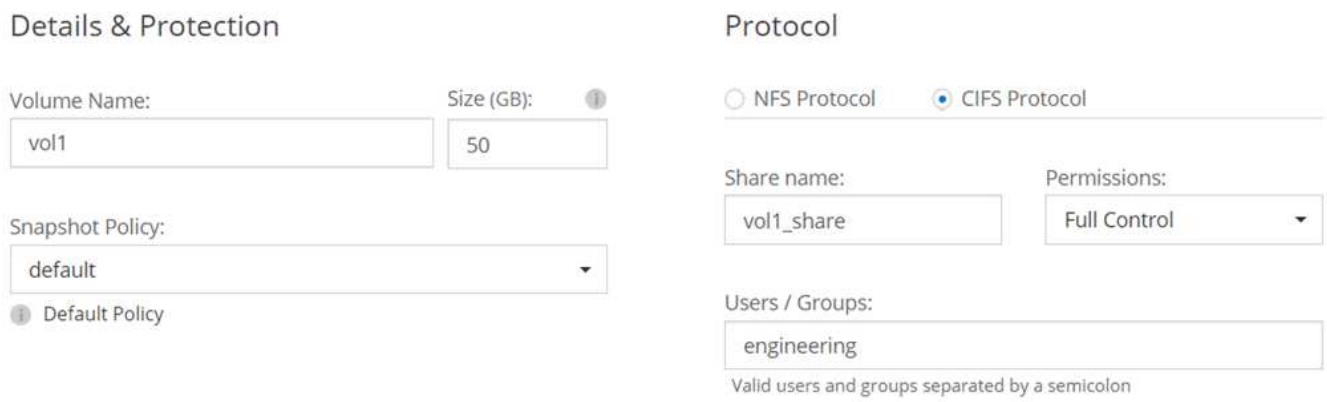
12. Sur la page Créer un volume, entrez les détails du nouveau volume, puis cliquez sur **Continuer**.

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

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

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

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




13. Si vous avez choisi le protocole CIFS, configurez un serveur CIFS sur la page d'installation CIFS :

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

| Champ | Description |
| --- | --- |
| Nom NetBIOS du serveur CIFS | Nom de serveur CIFS unique dans le domaine AD. |
| Unité organisationnelle | Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. |
| Domaine DNS | Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD. |
| Serveur NTP | Sélectionnez **utiliser le domaine Active Directory** pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la "Guide du développeur de l'API Cloud Manager" pour plus d'informations. |

14. Sur la page Profil d'utilisation, Type de disque et Stratégie de hiérarchisation, choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifiez la stratégie de hiérarchisation S3, si nécessaire.

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

15. Sur la page Review & Approve, vérifiez et confirmez vos sélections :
    a. Consultez les détails de la configuration.
    b. Cliquez sur **plus d'informations** pour en savoir plus sur le support et les ressources AWS que Cloud Manager achètera.
    c. Cochez les cases **Je comprends…**.
    d. Cliquez sur **Go**.

**Résultat**

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

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

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

**Une fois que vous avez terminé**

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

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

## Lancement d'une paire Cloud Volumes ONTAP HA dans AWS

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

de travail HA dans Cloud Manager.

**Avant de commencer**

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

**Description de la tâche**

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

**Étapes**

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail**.
2. Sous Créer, sélectionnez **Cloud Volumes ONTAP HA**.
3. Sur la page Détails et informations d'identification, modifiez éventuellement le compte AWS, entrez un nom d'environnement de travail, ajoutez des étiquettes 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 |
|---|---|
| Changer de compte | Vous pouvez choisir un autre compte si vous avez ajouté d'autres comptes de fournisseurs de services clouds. Pour plus de détails, voir "Ajout de comptes de fournisseurs de services clouds à Cloud Manager". |
| Nom de l'environnement de travail | Cloud Manager utilise le nom de l'environnement de travail pour nommer à la fois le système Cloud Volumes ONTAP et 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. Pour plus d'informations sur les étiquettes, reportez-vous à la section "Documentation AWS : balisage des ressources Amazon EC2". |
| Informations d'identification | Il s'agit des informations d'identification du compte d'administration du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via OnCommand System Manager ou sa CLI. |

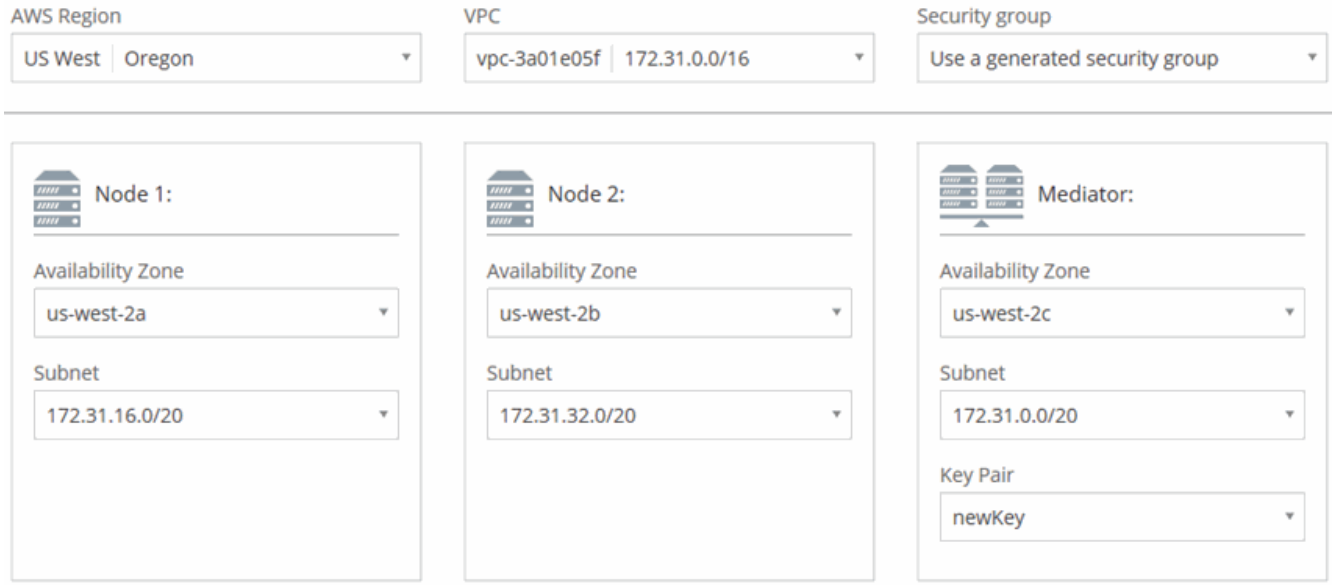
Si les clés AWS n'ont pas été spécifiées pour votre compte Cloud Manager, vous êtes invité à les saisir après avoir cliqué sur Continuer. Vous devez entrer les clés AWS avant de continuer.

4. Sur la page HA Deployment Models (Modèles de déploiement haute disponibilité), choisissez une configuration haute disponibilité.

   Pour obtenir un aperçu des modèles de déploiement, voir "Cloud Volumes ONTAP HA pour AWS".

5. Sur la page région et VPC, entrez les informations de réseau que vous avez enregistrées dans la fiche AWS, puis cliquez sur **Continuer**.

   L'image suivante montre la page d'emplacement remplie pour une configuration AZ multiple :




6. Sur la page Connectivité et authentification SSH, choisissez les méthodes de connexion pour la paire HA et le médiateur.
7. Si vous choisissez plusieurs AZS, spécifiez les adresses IP flottantes, puis cliquez sur **Continuer**.

   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".

8. Si vous choisissez plusieurs AZS, sélectionnez les tables de routage qui doivent inclure des routes vers les adresses IP flottantes, puis cliquez sur **Continuer**.

   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".

9. Sur la page Data Encryption, choisissez aucun chiffrement de données ou chiffrement 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.

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

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

10. Sur la page de compte du site de licence et de support, indiquez si vous souhaitez utiliser le paiement à l'utilisation ou BYOL, puis spécifiez 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".

11. Sur la page modules 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.

12. Sur la page IAM Role (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".

13. Sur la page licences, modifiez la version de Cloud Volumes ONTAP selon vos besoins, sélectionnez une licence, un type d'instance, la location d'instance, puis cliquez sur **Continuer**.

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

    > Si une version plus récente de Release Candidate, General Availability ou patch est disponible pour la version sélectionnée, Cloud Manager met à jour le système à cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.4 RC1 et 9.4 GA. La mise à jour ne se produit pas d'une version à une autre, par exemple de la version 9.3 à la version 9.4.

14. Sur la page sous-jacente Storage Resources, choisissez les paramètres de l'agrégat initial : un type de disque, une taille pour chaque disque et le Tiering S3 doit être activé ou non.

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

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

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

15. Sur la page WORM, activez l'écriture une seule fois, lisez de nombreux systèmes de stockage (WORM), si vous le souhaitez.

    "En savoir plus sur le stockage WORM".

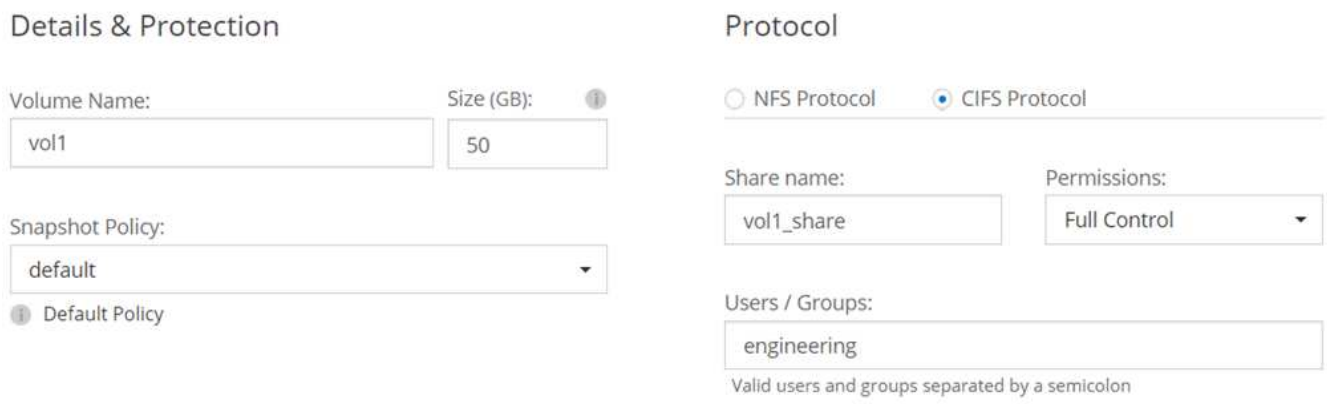
16. Sur la page Créer un volume, entrez les détails du nouveau volume, puis cliquez sur **Continuer**.

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

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

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

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




17. Si vous avez sélectionné le protocole CIFS, configurez un serveur CIFS sur la page d'installation CIFS :

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

| Champ | Description |
| --- | --- |
| Nom NetBIOS du serveur CIFS | Nom de serveur CIFS unique dans le domaine AD. |
| Unité organisationnelle | Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. |
| 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. |

18. Sur la page Profil d'utilisation, Type de disque et Stratégie de hiérarchisation, choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifiez la stratégie de hiérarchisation S3, si nécessaire.

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

19. Sur la page Review & Approve, vérifiez et confirmez vos sélections :
    a. Consultez les détails de la configuration.
    b. Cliquez sur **plus d'informations** pour en savoir plus sur le support et les ressources AWS que Cloud Manager achètera.
    c. Cochez les cases **Je comprends…**.
    d. Cliquez sur **Go**.

**Résultat**

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

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

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

**Une fois que vous avez terminé**

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

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

# Lancement d'Cloud Volumes ONTAP dans Azure

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

**Avant de commencer**

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

  "Consultez les nouvelles autorisations requises pour déployer les systèmes HA".

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

**Description de la tâche**

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

**Étapes**

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail**
2. Sous Créer, sélectionnez un système à un seul nœud dans Azure ou une paire HA dans Azure.
3. Sur la page Détails et informations d'identification, vous pouvez modifier le compte ou l'abonnement Azure, spécifier un nom de cluster et un nom de groupe de ressources, ajouter des balises si nécessaire, puis spécifier des informations d'identification.

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

| Champ | Description |
|---|---|
| Changer de compte | Vous pouvez choisir un autre compte ou abonnement si vous le souhaitez "Ajout de comptes fournisseurs de services clouds supplémentaires". |
| Nom de l'environnement de travail | Cloud Manager utilise le nom de l'environnement de travail pour nommer à la fois le système Cloud Volumes ONTAP et la machine virtuelle Azure. Il utilise également le nom comme préfixe pour le groupe de sécurité prédéfini, si vous sélectionnez cette option. |
| Nom du groupe de ressources | Si vous décochez la case **utiliser par défaut**, vous pouvez entrer le nom d'un nouveau groupe de ressources. Si vous souhaitez utiliser un groupe de ressources existant, vous devez utiliser l'API. |
| Étiquettes | Les étiquettes sont des métadonnées pour vos ressources Azure. Cloud Manager ajoute les balises au système Cloud Volumes ONTAP et à chaque ressource Azure associée au système. Vous pouvez ajouter jusqu'à quatre balises à partir de l'interface utilisateur lors de la création d'un environnement de travail, puis en ajouter d'autres après sa création. Notez que l'API ne vous limite pas à quatre balises lors de la création d'un environnement de travail. Pour plus d'informations sur les étiquettes, reportez-vous à la section "Documentation Microsoft Azure : utilisation des balises pour organiser vos ressources Azure". |

| Champ | Description |
| --- | --- |
| Informations d'identification | Il s'agit des informations d'identification du compte d'administration du cluster Cloud Volumes ONTAP. Vous pouvez utiliser ces informations d'identification pour vous connecter à Cloud Volumes ONTAP via OnCommand System Manager ou sa CLI. |

4. Sur la page emplacement, sélectionnez un emplacement et un groupe de sécurité, cochez la case pour confirmer la connectivité réseau, puis cliquez sur **Continuer**.
5. Sur la page de compte du site de licence et de support, indiquez si vous souhaitez utiliser le paiement à l'utilisation ou BYOL, puis spécifiez 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. Sur la page modules 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. Sur la page licences, modifiez la version de Cloud Volumes ONTAP selon vos besoins, sélectionnez une licence et un type de machine virtuelle, puis cliquez sur **Continuer**.

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

   > Si une version plus récente de Release Candidate, General Availability ou patch est disponible pour la version sélectionnée, Cloud Manager met à jour le système à cette version lors de la création de l'environnement de travail. Par exemple, la mise à jour se produit si vous sélectionnez Cloud Volumes ONTAP 9.5 RC1 et 9.5 GA est disponible. La mise à jour ne se produit pas d'une version à l'autre, par exemple de 9.4 à 9.5.

8. Sur la page Azure Marketplace, suivez les étapes ci-dessous si Cloud Manager n'a pas pu activer les déploiements programmatiques de Cloud Volumes ONTAP.
9. Sur la page sous-jacente Storage Resources, choisissez les paramètres de l'agrégat initial : un type de disque, une taille pour chaque disque et si le Tiering doit être activé.

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

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

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

10. Sur la page vitesse d'écriture et WORM, choisissez **Normal** ou **vitesse d'écriture élevée** et activez le stockage WORM (Write Once, Read Many), si vous le souhaitez.

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

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

"En savoir plus sur le stockage WORM".

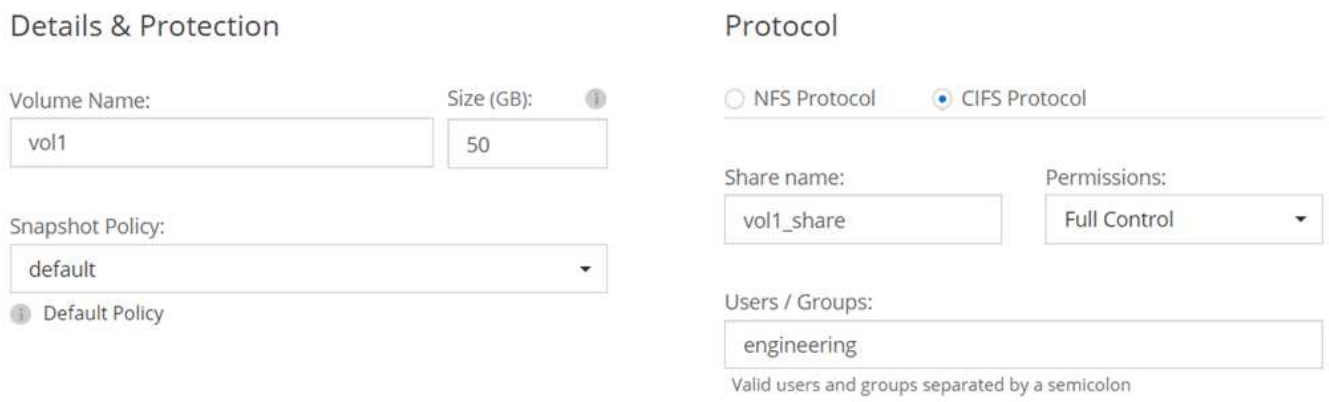
11. Sur la page Créer un volume, entrez les détails du nouveau volume, puis cliquez sur **Continuer**.

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

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

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

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



12. Si vous avez choisi le protocole CIFS, configurez un serveur CIFS sur la page d'installation 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. |
| 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. Sur la page Profil d'utilisation, Type de disque et Stratégie de hiérarchisation, choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage et modifiez la stratégie de hiérarchisation, si nécessaire.

    Le Tiering du stockage est pris en charge avec les systèmes à un seul nœud.

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

14. Sur la page Review & Approve, vérifiez et confirmez vos sélections :
    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.

# Enregistrement des systèmes de paiement à l'utilisation

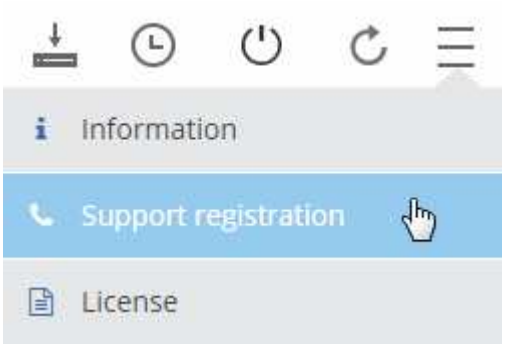
Le support de NetApp est inclus avec les systèmes Cloud Volumes ONTAP Explore, Standard et Premium, mais vous devez au préalable activer le support en enregistrant les systèmes à NetApp.

**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** :



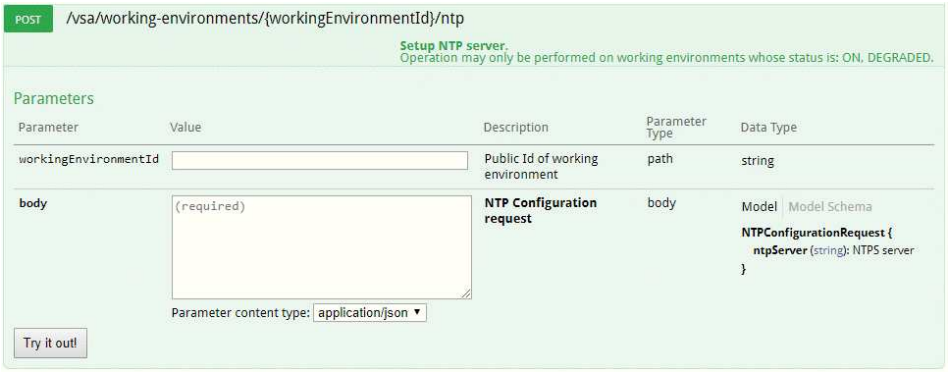

4. Sélectionnez un compte sur le site de support NetApp et cliquez sur **Register**.

**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.<br><br>Spécifiez un serveur NTP via l'API Cloud Manager ou depuis l'interface utilisateur lors de la configuration d'un serveur CIFS.<br><br>• "Modification du serveur CIFS"<br>• "Guide du développeur de l'API Cloud Manager"<br><br>Par exemple, voici l'API d'un système à un seul nœud dans AWS :<br><br>  |
| 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 Cloud Manager Admin a ajouté un serveur proxy à Cloud Manager avant de lancer votre instance, Cloud Volumes ONTAP est configuré pour utiliser ce serveur proxy pour les messages AutoSupport. Vous devez tester AutoSupport pour vous assurer qu'il peut envoyer des messages. Pour obtenir ces instructions, consultez l'aide de System Manager ou le "Référence de l'administration du système ONTAP 9". |
| En option : Configurer EMS | Le système de gestion des événements (EMS) collecte et affiche des informations sur les événements qui se produisent sur les systèmes Cloud Volumes ONTAP. Pour recevoir des notifications d'événements, vous pouvez définir des destinations d'événements (adresses e-mail, hôtes de trap SNMP ou serveurs syslog) et des routes d'événements pour un événement particulier. Vous pouvez configurer EMS à l'aide de l'interface de ligne de commande. Pour obtenir des instructions, reportez-vous au "Guide de configuration rapide de ONTAP 9 EMS". |

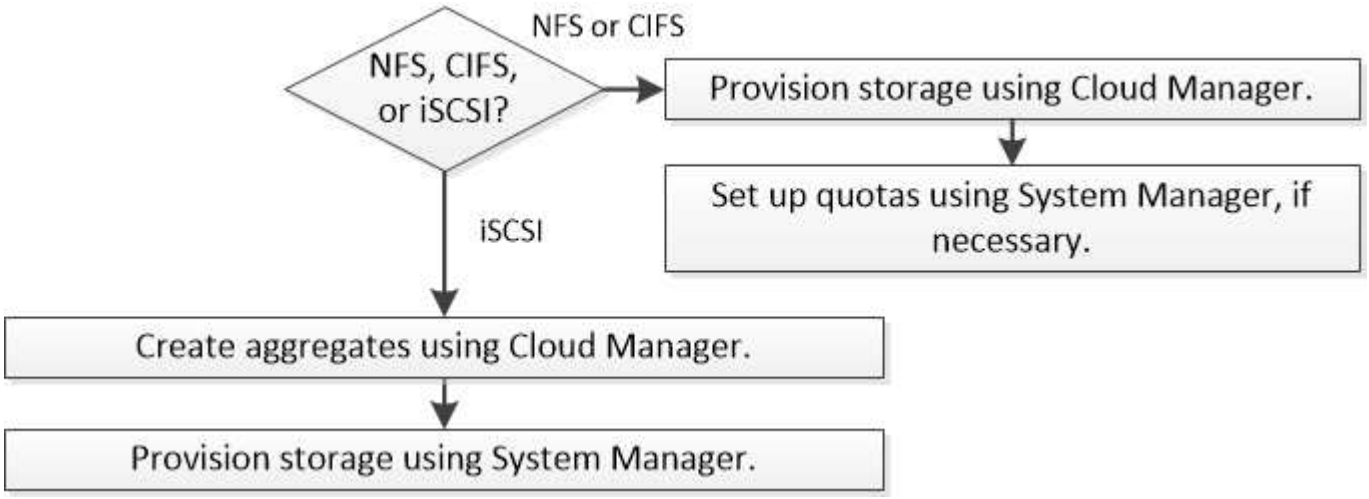
| Tâche | Description |
| --- | --- |
| Facultatif : créez une interface réseau de gestion SVM (LIF) pour les systèmes HA dans plusieurs zones de disponibilité AWS | Une interface de réseau de gestion de machine virtuelle de stockage (LIF) est requise si vous souhaitez utiliser SnapCenter ou SnapDrive pour Windows avec une paire haute disponibilité. La LIF de gestion du SVM doit utiliser une adresse IP *flottante* lors de l'utilisation d'une paire HA sur plusieurs zones de disponibilité AWS.<br><br>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 :<br><br>`network interface create -vserver svm_cloud -lif svm_mgmt -role data -data-protocol none -home-node cloud-01 -home-port e0a -address 10.0.2.126 -netmask 255.255.255.0 -status-admin up -firewall -policy mgmt` |
| Facultatif : modifiez l'emplacement de sauvegarde des fichiers de configuration | Cloud Volumes ONTAP crée automatiquement des fichiers de sauvegarde de la configuration qui contiennent des informations sur les options configurables dont il a besoin pour fonctionner correctement. Par défaut, Cloud Volumes ONTAP sauvegarde les fichiers sur l'hôte Cloud Manager toutes les huit heures. Si vous souhaitez envoyer les sauvegardes à un autre emplacement, vous pouvez modifier l'emplacement vers un serveur FTP ou HTTP dans votre data center ou dans AWS. Par exemple, vous pouvez déjà disposer d'un emplacement de sauvegarde pour vos systèmes de stockage FAS. Vous pouvez modifier l'emplacement de sauvegarde à l'aide de l'interface de ligne de commande. Voir la "Référence de l'administration du système ONTAP 9". |

# Provisionnement du stockage

## Provisionnement du stockage

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

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




### Volumes de provisionnement

Si vous avez besoin de plus de stockage après le lancement d'un système Cloud Volumes ONTAP, vous pouvez provisionner de nouveaux volumes NFS et CIFS à partir de Cloud Manager.

#### Avant de commencer

Si vous souhaitez utiliser CIFS dans AWS, vous devez avoir configuré DNS et Active Directory. Pour plus de détails, voir "Configuration réseau requise pour Cloud Volumes ONTAP pour AWS".

#### Étapes

1. Sur la page Working Environments, double-cliquez sur le nom du système Cloud Volumes ONTAP sur lequel vous souhaitez provisionner des volumes.
2. Créez un nouveau volume sur un agrégat ou sur un agrégat spécifique :

| Action | Étapes |
| --- | --- |
| Créez un nouveau volume et laissez Cloud Manager choisir l'agrégat contenant | Cliquez sur **Ajouter nouveau volume**. |

| Action | Étapes |
| --- | --- |
| Créez un nouveau volume sur un agrégat spécifique | a. Cliquez sur l'icône du menu, puis sur **Avancé > attribution avancée**.<br>b. Cliquez sur le menu correspondant à un agrégat.<br>c. Cliquez sur **Créer un volume**. |

3. Entrez les détails du nouveau volume, puis cliquez sur **Continuer**.

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

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

4. Si vous avez choisi le protocole CIFS et que le serveur CIFS n'a pas été configuré, spécifiez les détails du serveur dans la boîte de dialogue Créer un serveur CIFS, puis cliquez sur **Enregistrer et continuer** :

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

| Champ | Description |
| --- | --- |
| Nom NetBIOS du serveur CIFS | Nom de serveur CIFS unique dans le domaine AD. |
| Unité organisationnelle | Unité organisationnelle du domaine AD à associer au serveur CIFS. La valeur par défaut est CN=Computers. |
| 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 Stratégie de hiérarchisation, choisissez si vous souhaitez activer les fonctionnalités d'efficacité du stockage, choisissez un type de disque et modifiez la stratégie de hiérarchisation S3, 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.

## Provisionnement des volumes sur le second nœud dans une configuration haute disponibilité

Par défaut, Cloud Manager crée des volumes sur le premier nœud d'une configuration HA. Si vous avez besoin d'une configuration active-active, dans laquelle les deux nœuds servent les données aux clients, vous devez créer des agrégats et des volumes sur le second nœud.

**Étapes**

1. Sur la page Working Environments, double-cliquez sur le nom de l'environnement de travail Cloud Volumes ONTAP sur lequel vous souhaitez gérer les agrégats.
2. Cliquez sur l'icône du menu, puis sur **Avancé > attribution avancée**.

3. Cliquez sur **Ajouter agrégat**, puis créez l'agrégat.
4. Pour le nœud principal, choisissez le second nœud dans la paire HA.
5. Une fois que Cloud Manager a créé l'agrégat, sélectionnez-le, puis cliquez sur **Create volume**.
6. Entrez les détails du nouveau volume, puis cliquez sur **Créer**.

**Une fois que vous avez terminé**

Vous pouvez créer des volumes supplémentaires sur cet agrégat si nécessaire.

Pour les paires HA déployées dans plusieurs zones de disponibilité AWS, vous devez monter le volume sur les clients en utilisant l'adresse IP flottante du nœud sur lequel réside le volume.

## Création d'agrégats

Vous pouvez créer des agrégats vous-même ou laisser Cloud Manager le faire lorsque vous créez des volumes. L'avantage de créer des agrégats vous-même est de choisir la taille du disque sous-jacent, ce qui vous permet de dimensionner l'agrégat en fonction de la capacité ou des performances requises.

**Étapes**

1. Sur la page Working Environments, double-cliquez sur le nom de l'instance Cloud Volumes ONTAP sur laquelle vous souhaitez gérer les agrégats.
2. Cliquez sur l'icône du menu, puis sur **Avancé > attribution avancée**.
3. Cliquez sur **Ajouter agrégat**, puis spécifiez les détails de l'agrégat.

   Pour obtenir de l'aide sur le type et la taille du disque, reportez-vous à la section "Planification de votre configuration".

4. Cliquez sur **Go**, puis sur **approuver et acheter**.

## Provisionnement des LUN iSCSI

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

**Avant de commencer**

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

**Description de la tâche**

Ces étapes décrivent l'utilisation de System Manager pour la version 9.3 et ultérieure.

**Étapes**

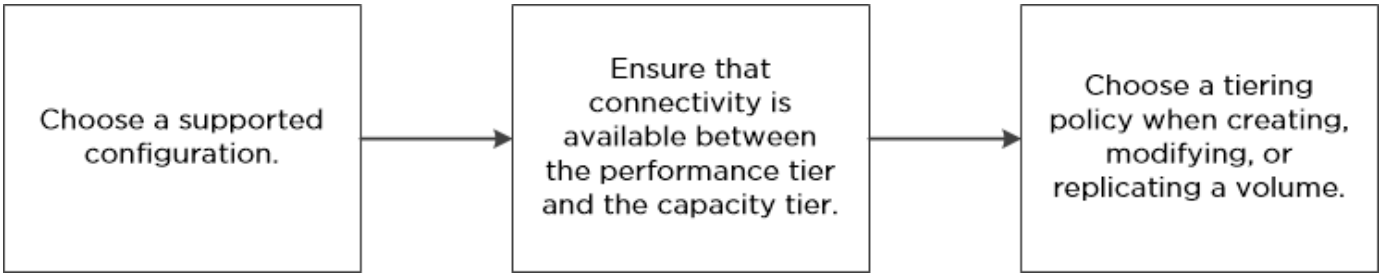
1. "Connectez-vous à System Manager".
2. Cliquez sur **stockage > LUN**.
3. Cliquez sur **Créer** et suivez les invites pour créer la LUN.
4. Connectez-vous à la LUN à partir de vos hôtes.

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

# Tiering des données inactives vers un stockage objet à faible coût

Vous pouvez réduire les coûts de stockage dans AWS et Azure 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 :




**Quelles sont les's non requis pour le Tiering des données**

- Vous n'avez pas besoin d'installer une licence de fonctionnalité pour activer le tiering des données.
- Vous n'avez pas besoin de créer le niveau de capacité (soit un conteneur S3 ou un conteneur Azure Blob). 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 :

- La hiérarchisation des données est prise en charge par Cloud Volumes ONTAP Standard, Premium et BYOL, à partir de la version 9.2 d'AWS et de la version 9.4 de Microsoft Azure.
  - Le Tiering des données n'est pas pris en charge avec les paires HA dans Microsoft Azure.
  - 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.
- Le Tiering des données est pris en charge grâce aux technologies de chiffrement.
- Le provisionnement fin doit être activé sur les volumes.

## Exigences relatives aux données de hiérarchisation dans AWS

Vous devez vous assurer 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 ?".

## Configuration requise pour le tiering des données dans Microsoft Azure

Vous n'avez pas besoin de configurer une connexion entre le niveau de performance et le niveau de capacité tant que Cloud Manager dispose des autorisations requises. Cloud Manager active un point de terminaison de service VNet pour vous si la stratégie Cloud Manager dispose des autorisations appropriées :

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

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

## Hiérarchisation des données sur les volumes en lecture-écriture

Cloud Volumes ONTAP peut déplacer les données inactives sur des volumes en lecture/écriture vers un stockage objet économique, libérant ainsi le Tier de performance pour les données actives.

**Étapes**

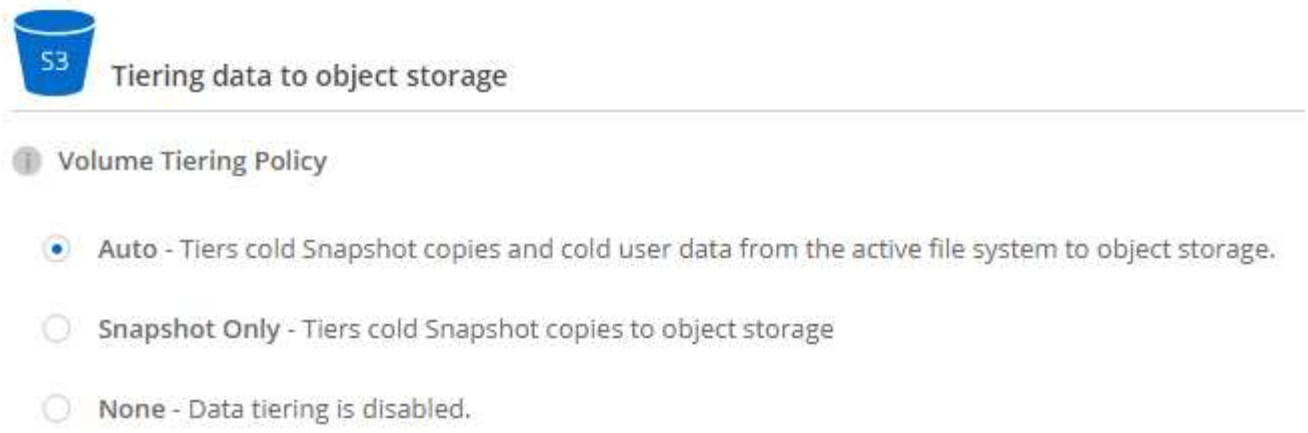
1. Dans l'environnement de travail, créez un nouveau volume ou modifiez le niveau d'un volume existant :

| Tâche | Action |
|---|---|
| Créez un nouveau volume | Cliquez sur **Ajouter nouveau volume**. |
| Modifier un volume existant | Sélectionnez le volume et cliquez sur **Modifier le type de disque et la stratégie de hiérarchisation**. |

2. Sélectionnez la stratégie Snapshot Only ou Auto.

   Pour obtenir une description de ces politiques, reportez-vous à la section "Vue d'ensemble du hiérarchisation des données".

   **Exemple**




Cloud Manager crée un nouvel agrégat pour le volume si un agrégat compatible avec le hiérarchisation des données n'existe pas déjà.

Si vous préférez créer vous-même des agrégats, vous pouvez activer le tiering des données sur les agrégats lorsque vous les créez.

## Hiérarchisation des données sur les volumes de protection des données

Cloud Volumes ONTAP permet de hiérarchiser les données d'un volume de protection des données vers un niveau de capacité. Si vous activez le volume de destination, les données passent progressivement au niveau de performance tel qu'il est lu.

**Étapes**

1. Sur la page Working Environments (Environnements de travail), sélectionnez l'environnement de travail qui contient le volume source, puis faites-le glisser vers l'environnement de travail vers lequel vous souhaitez répliquer le volume.
2. Suivez les invites jusqu'à ce que vous atteigniez la page de hiérarchisation et que vous activiez le tiering des données vers le stockage d'objets.

   **Exemple**


   Pour obtenir de l'aide sur la réplication des données, voir "Réplication des données depuis et vers le cloud".

## Modification du niveau de hiérarchisation

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

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

**Description de la tâche**

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

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

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

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

Pour plus d'informations sur le fonctionnement des niveaux de hiérarchisation, voir "Vue d'ensemble du hiérarchisation des données".

**Étapes**

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **niveau de hiérarchisation**.
2. Choisissez le niveau de hiérarchisation, 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, vous pouvez utiliser Cloud Volumes ONTAP comme stockage persistant pour les conteneurs. La mise en route comprend quelques étapes.

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

**Vérifiez la connectivité réseau**

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

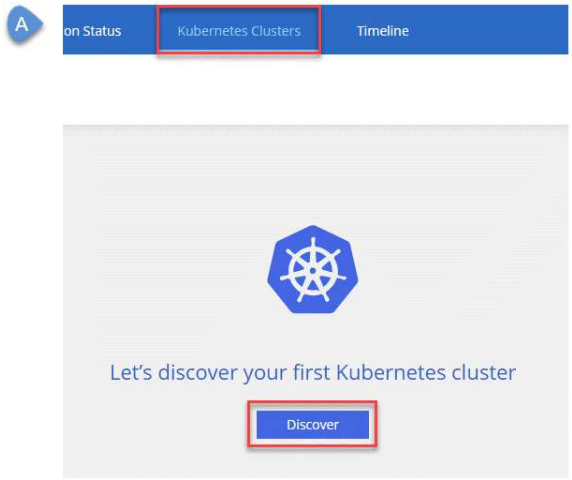
   https://packages.cloud.google.com/yum https://github.com/NetApp/trident/releases/download/

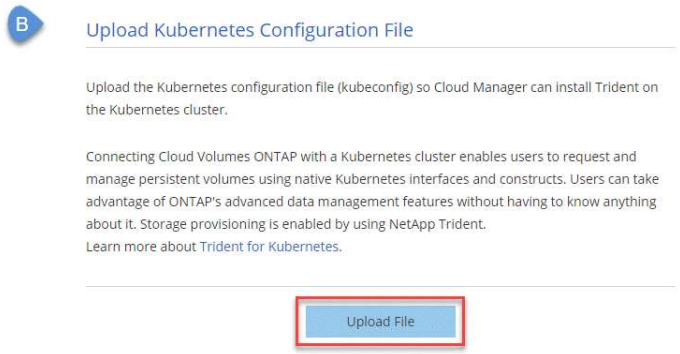
   Cloud Manager installe Trident sur un cluster Kubernetes lorsque vous connectez un environnement de travail au cluster.

## Téléchargez les fichiers de configuration Kubernetes dans Cloud Manager

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

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

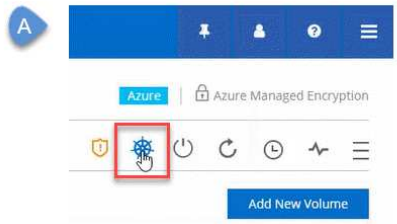


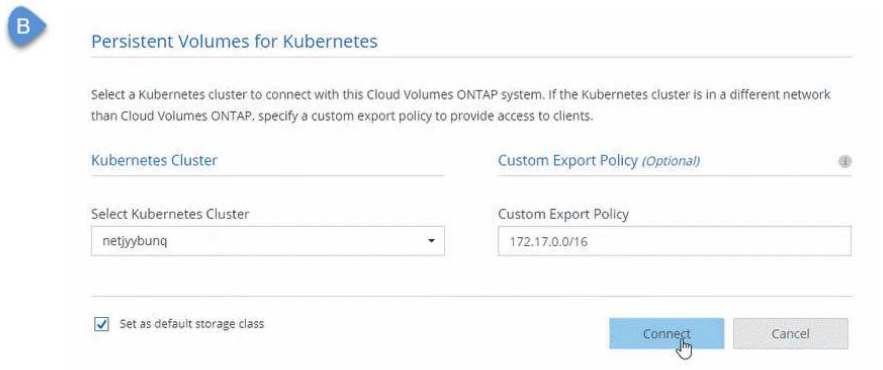




## Connectez vos environnements de travail aux clusters Kubernetes

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

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




## Commencez le provisionnement des volumes persistants

Demandez et gérez les volumes persistants à l'aide d'interfaces et de constructions Kubernetes natives. Cloud

Manager crée deux classes de stockage Kubernetes que vous pouvez utiliser pour le provisionnement des volumes persistants :

- **netapp-fichier** : pour liaison de volumes persistants aux systèmes Cloud Volumes ONTAP à un seul nœud
- **netapp-file-redondant** : pour la liaison de volumes persistants aux paires HA Cloud Volumes ONTAP

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

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

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

### Qu'est-ce que les volumes trident_trident ?

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

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

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

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

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

# Chiffrement de volumes avec NetApp Volume Encryption

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

#### Description de la tâche

Pour l'instant, Cloud Volumes ONTAP prend en charge NetApp Volume Encryption avec un serveur de gestion externe des clés. Un gestionnaire de clés intégré n'est pas pris en charge.

Vous devez configurer NetApp Volume Encryption à partir de l'interface de ligne de commande d'ONTAP. Vous

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

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

**Étapes**

1. Consultez la liste des gestionnaires de clés pris en charge dans le "Matrice d'interopérabilité NetApp".

   Recherchez la solution **gestionnaires de clés**.

2. "Connectez-vous à l'interface de ligne de commandes de Cloud Volumes ONTAP".
3. Installez une licence NetApp Volume Encryption sur le système Cloud Volumes ONTAP.

   "Guide de l'alimentation en chiffrement ONTAP 9 : installation de la licence"

4. 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"

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

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

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

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

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

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

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

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

# Gestion du stockage existant

Cloud Manager vous permet de gérer les volumes, les agrégats et les serveurs CIFS. Il vous invite également à déplacer des volumes afin d'éviter les problèmes de capacité.

## Gestion des volumes existants

Vous pouvez gérer les volumes existants à mesure que vos besoins de stockage changent. Vous pouvez afficher, modifier, cloner, restaurer et supprimer des volumes.

**Étapes**

1. Sur la page Working Environments, double-cliquez sur l'environnement de travail Cloud Volumes ONTAP sur lequel vous souhaitez gérer les volumes.
2. Gérez vos volumes :

| Tâche | Action |
|---|---|
| Afficher des informations sur un volume | Sélectionnez un volume, puis cliquez sur **Info**. |
| Modifier un volume (volumes en lecture-écriture uniquement) | a. Sélectionnez un volume, puis cliquez sur **Modifier**.<br>b. Modifiez la stratégie Snapshot du volume, la liste de contrôle d'accès NFS ou les autorisations de partage, puis cliquez sur **Update**. |
| Clonez un volume | a. Sélectionnez un volume, puis cliquez sur **Clone**.<br>b. Modifiez le nom du clone selon vos besoins, puis cliquez sur **Clone**.<br>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.<br>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**.<br>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**.<br>b. Modifiez le nom, si nécessaire, puis cliquez sur **Créer**. |
| Obtenez la commande NFS mount | a. Sélectionnez un volume, puis cliquez sur **Mount Command**.<br>b. Cliquez sur **Copier**. |

| Tâche | Action |
| --- | --- |
| Modifiez le type de disque sous-jacent | a. Sélectionnez un volume, puis cliquez sur **Modifier le type de disque et la stratégie de hiérarchisation**.<br>b. Sélectionnez le type de disque, puis cliquez sur **changer**.<br>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**.<br>b. Cliquez sur **Modifier la stratégie**.<br>c. Sélectionnez une autre stratégie et cliquez sur **Modifier**.<br>Cloud Manager déplace le volume vers un agrégat existant qui utilise le type de disque sélectionné avec hiérarchisation ou crée un nouvel agrégat pour le volume. |
| Activer ou désactiver la synchronisation vers S3 pour un volume | Sélectionnez un volume, puis cliquez sur **Synchroniser avec S3** ou sur **Supprimer la relation de synchronisation**.<br>La fonction de synchronisation vers S3 doit être activée avant de pouvoir utiliser ces options. Pour obtenir des instructions, reportez-vous à la section "Synchronisation des données vers AWS S3" |
| Supprimer un volume | a. Sélectionnez un volume, puis cliquez sur **Supprimer**.<br>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**.<br>b. Sélectionnez le nombre de disques que vous souhaitez ajouter et cliquez sur **Ajouter**.<br>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**.<br>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. |

| Tâche | Action |
| --- | --- |
| Domaine DNS | Le domaine DNS de la machine virtuelle de stockage Cloud Volumes ONTAP (SVM). Dans la plupart des cas, le domaine est identique au domaine AD. |
| Serveur NTP | Sélectionnez **utiliser le domaine Active Directory** pour configurer un serveur NTP à l'aide du DNS Active Directory. Si vous devez configurer un serveur NTP à l'aide d'une autre adresse, vous devez utiliser l'API. Voir la "Guide du développeur de l'API Cloud Manager" pour plus d'informations. |

3. Cliquez sur **Enregistrer**.

**Résultat**

Cloud Volumes ONTAP met à jour le serveur CIFS avec les modifications.

## Déplacement d'un volume pour éviter les problèmes de capacité

Cloud Manager peut afficher un message Action requise indiquant que le déplacement d'un volume est nécessaire pour éviter les problèmes de capacité, mais qu'il ne peut pas fournir de recommandations pour corriger le problème. Dans ce cas, vous devez identifier comment corriger le problème, puis déplacer un ou plusieurs volumes.

**Étapes**

1. Identifier la manière de corriger le problème.
2. En fonction de votre analyse, déplacez les volumes pour éviter les problèmes de capacité :
   - Déplacement des volumes vers un autre système.
   - Déplacement des volumes vers un autre agrégat du même système.

### Identifier comment corriger les problèmes de capacité

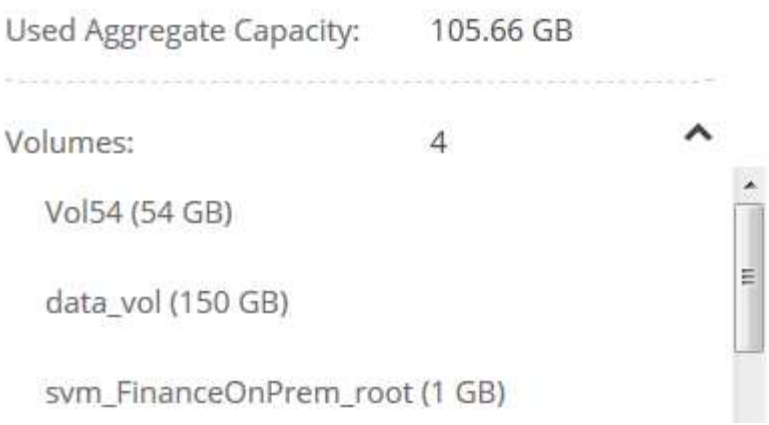
Si Cloud Manager ne peut pas fournir de recommandations pour le déplacement d'un volume afin d'éviter les problèmes de capacité, vous devez identifier les volumes que vous devez déplacer et indiquer si vous devez les déplacer vers un autre agrégat sur le même système ou vers un autre système.

**Étapes**

1. Consultez les informations avancées du message Action requise pour identifier l'agrégat ayant atteint sa limite de capacité.

   Par exemple, l'information avancée devrait dire quelque chose de similaire à ce qui suit : aggr1 global a atteint sa limite de capacité.

2. Identifiez un ou plusieurs volumes à sortir de l'agrégat :
   a. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > allocation avancée**.
   b. Sélectionnez l'agrégat, puis cliquez sur **Info**.
   c. Développez la liste des volumes.




d. Passez en revue la taille de chaque volume et choisissez un ou plusieurs volumes pour sortir de l'agrégat.

   Vous devez choisir des volumes suffisamment volumineux pour libérer de l'espace dans l'agrégat afin d'éviter d'autres problèmes de capacité à l'avenir.

3. Si le système n'a pas atteint la limite de disque, vous devez déplacer les volumes vers un agrégat existant ou vers un nouvel agrégat sur le même système.

   Pour plus de détails, voir "Déplacement des volumes vers un autre agrégat pour éviter les problèmes de capacité".

4. Si le système a atteint la limite de disque, effectuez l'une des opérations suivantes :
   a. Supprimez tous les volumes inutilisés.
   b. Réorganiser les volumes pour libérer de l'espace sur un agrégat.

      Pour plus de détails, voir "Déplacement des volumes vers un autre agrégat pour éviter les problèmes de capacité".

   c. Déplacez deux volumes ou plus vers un autre système disposant d'espace.

      Pour plus de détails, voir "Déplacement des volumes vers un autre système pour éviter les problèmes de capacité".

### Déplacement des volumes vers un autre système pour éviter les problèmes de capacité

Vous pouvez déplacer un ou plusieurs volumes vers un autre système Cloud Volumes ONTAP pour éviter les problèmes de capacité. Vous devrez peut-être le faire si le système a atteint sa limite de disque.

#### Description de la tâche

Vous pouvez suivre les étapes de cette tâche pour corriger le message Action requise suivant :

```
 Moving a volume is necessary to avoid capacity issues; however, Cloud
Manager cannot perform this action for you because the system has reached
the disk limit.
.Étapes
. Identifiez un système Cloud Volumes ONTAP doté de la capacité disponible
ou déployez un nouveau système.
. Faites glisser et déposez l'environnement de travail source sur
l'environnement de travail cible pour effectuer une réplication unique du
volume.
```

+
Pour plus de détails, voir "Réplication des données entre les systèmes".

1. Accédez à la page Etat de la réplication, puis rompez la relation SnapMirror pour convertir le volume répliqué d'un volume de protection des données en volume en lecture/écriture.

   Pour plus de détails, voir "Gestion des planifications et des relations de réplication des données".

2. Configurez le volume pour l'accès aux données.

   Pour plus d'informations sur la configuration d'un volume de destination pour l'accès aux données, reportez-vous à la section "Guide rapide de reprise après incident de volumes ONTAP 9".

3. Supprimez le volume d'origine.

   Pour plus de détails, voir "Gestion des volumes existants".

#### Déplacement des volumes vers un autre agrégat pour éviter les problèmes de capacité

Vous pouvez déplacer un ou plusieurs volumes vers un autre agrégat pour éviter les problèmes de capacité.

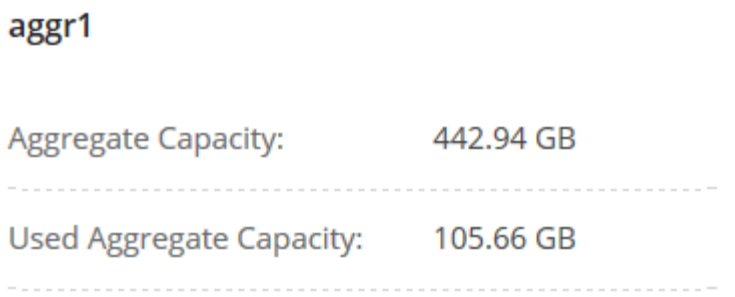
##### Description de la tâche

Vous pouvez suivre les étapes de cette tâche pour corriger le message Action requise suivant :

```
 Moving two or more volumes is necessary to avoid capacity issues;
however, Cloud Manager cannot perform this action for you.
.Étapes
. Vérifiez si un agrégat existant a la capacité disponible pour les
volumes que vous devez déplacer :
```

+
.. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > allocation avancée**.
.. Sélectionnez chaque agrégat, cliquez sur **Info**, puis affichez la capacité disponible (capacité d'agrégat moins la capacité d'agrégat utilisée).

+




1. Si nécessaire, ajoutez des disques à un agrégat existant :
   a. Sélectionner l'agrégat, puis cliquer sur **Add disks**.
   b. Sélectionnez le nombre de disques à ajouter, puis cliquez sur **Ajouter**.
2. Si aucun agrégat n'a de capacité disponible, créez un nouvel agrégat.

   Pour plus de détails, voir "Création d'agrégats".
3. Utilisez System Manager ou l'interface de ligne de commande pour déplacer les volumes vers l'agrégat.
4. Dans la plupart des cas, vous pouvez utiliser System Manager pour déplacer des volumes.

   Pour obtenir des instructions, reportez-vous au "Guide de migration de volumes ONTAP 9 Express".

# Provisionnement des volumes NFS depuis la vue du volume

## Passage à la vue de volume

Cloud Manager offre deux vues de gestion : Storage System View pour la gestion des systèmes de stockage sur un cloud hybride et Volume View pour la création de volumes dans AWS sans avoir à gérer les systèmes de stockage. Vous pouvez basculer entre ces vues, mais ces instances doivent être rares car une vue unique doit répondre à vos besoins.

Pour plus d'informations sur l'affichage du volume, reportez-vous à la section "Gestion simplifiée du stockage à l'aide de Volume View".

**Étapes**

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur le menu, puis sur **View Selection**.
2. Sur la page sélection de la vue, sélectionnez **Affichage du système de stockage**, puis cliquez sur **basculer**.

**Résultat**

Cloud Manager passe à l'affichage du volume.

## Création et montage de volumes NFS

Vous pouvez utiliser Cloud Manager pour créer des volumes NFS qui fournissent des fonctionnalités d'entreprise au-dessus du stockage AWS.

### Création de volumes NFS

Vous pouvez créer un volume associé à une seule instance AWS ou à une instance mise en miroir d'une autre instance afin d'assurer une haute disponibilité.

#### Étapes

1. Dans l'onglet volumes, cliquez sur **Créer un nouveau volume**.
2. Sur la page Créer un nouveau volume, sélectionnez un type de volume :

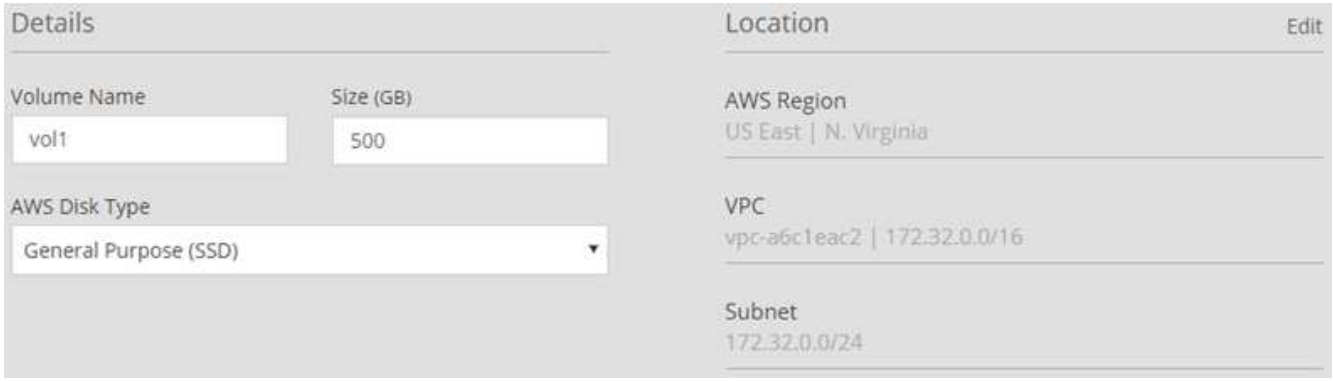
| Option | Description |
|---|---|
| Créer un volume | Crée un volume associé à une seule instance AWS. |
| Créer un volume haute disponibilité | Crée un volume associé à une seule instance AWS et mis en miroir sur une autre instance pour assurer une haute disponibilité en cas de défaillance. Cliquez sur l'icône Infos pour afficher des informations supplémentaires sur les instances requises pour un volume haute disponibilité. |

3. Si vous avez choisi Créer un volume, spécifiez les détails de votre premier volume, puis cliquez sur **Créer**.

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

| Champ | Description |
|---|---|
| Taille | La taille maximale du volume dépend de la capacité disponible sur les systèmes de stockage existants. Le provisionnement fin est automatiquement activé sur le volume, ce qui vous permet de créer un volume supérieur au stockage physique actuellement disponible. Au lieu de préallouer de l'espace de stockage, l'espace est alloué à chaque volume lors de l'écriture des données. |
| Type de disque AWS | Vous devez choisir le disque qui répond à vos besoins en termes de performances et de coûts.<br>• Les disques SSD à usage général permettent d'équilibrer les coûts et les performances d'un large éventail de charges de travail. La performance est définie en termes d'IOPS.<br>• Débit Les disques HDD optimisés sont destinés aux charges de travail fréquemment utilisées qui nécessitent un débit rapide et cohérent à un prix inférieur.<br>• Les disques durs à froid sont conçus pour les sauvegardes, ou les données rarement accessibles, car les performances sont très faibles. Tout comme les disques HDD optimisés en termes de débit, les performances sont définies en termes de débit.<br>Pour plus de détails, reportez-vous à "Documentation AWS : types de volume EBS". |

   L'image suivante montre la page Créer un volume remplie :

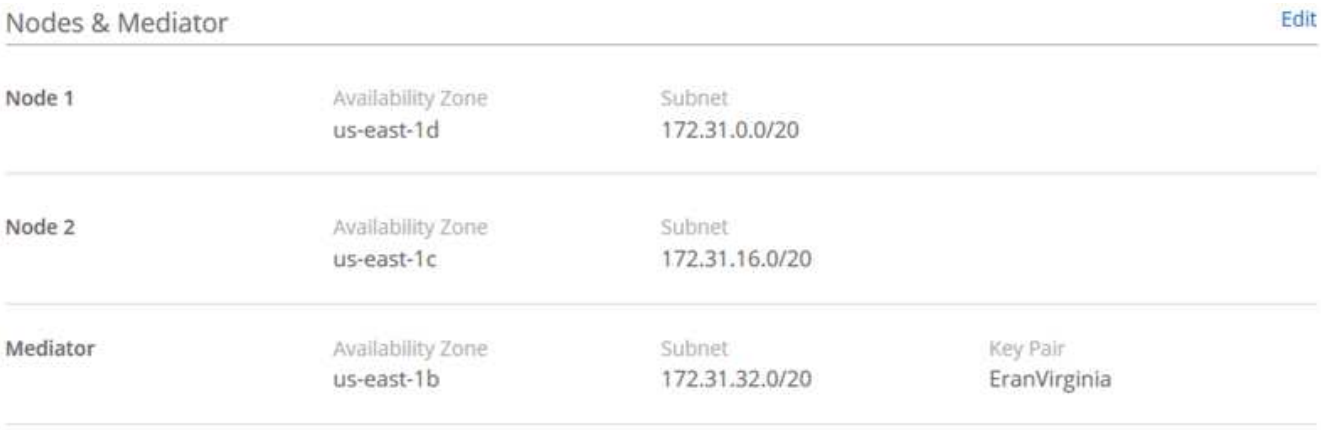



4. Si vous choisissez Créer un volume HA, spécifiez les détails du volume, puis cliquez sur **Créer**.

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

| Champ | Description |
|---|---|
| Taille | La taille maximale du volume dépend de la capacité disponible sur les systèmes de stockage existants. Le provisionnement fin est automatiquement activé sur le volume, ce qui vous permet de créer un volume supérieur au stockage physique actuellement disponible. Au lieu de préallouer de l'espace de stockage, l'espace est alloué à chaque volume lors de l'écriture des données. |
| Type de disque AWS | Vous devez choisir le disque qui répond à vos besoins en termes de performances et de coûts.<br>• Les disques SSD à usage général permettent d'équilibrer les coûts et les performances d'un large éventail de charges de travail. La performance est définie en termes d'IOPS.<br>• Débit Les disques HDD optimisés sont destinés aux charges de travail fréquemment utilisées qui nécessitent un débit rapide et cohérent.<br>Pour plus de détails, reportez-vous à "Documentation AWS : types de volume EBS". |
| Emplacement | Vous devez choisir un VPC qui inclut trois sous-réseaux dans trois zones de disponibilité distinctes. |
| Nœuds et médiateur | Dans la mesure du possible, Cloud Manager choisit des zones de disponibilité distinctes pour chaque instance, car il s'agit de la configuration optimale et prise en charge. |
| IP flottante | Les adresses IP doivent se trouver en dehors du bloc CIDR pour tous les VPC de la région. |
| Table de routage | 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 haute disponibilité. Pour plus de détails, reportez-vous à "Documentation AWS : tables de routage". |

   L'image suivante montre la page Noeuds and Mediator. Chaque instance se trouve dans une zone de disponibilité distincte.




**Résultat**

Cloud Manager crée le volume sur un système existant ou sur un nouveau système. Si un nouveau système est nécessaire, la création du volume peut prendre environ 25 minutes.

### Montage de volumes sur des hôtes Linux

Après avoir créé un volume, vous devez le monter sur vos hôtes afin qu'ils puissent accéder au volume.

**Étapes**

1. Dans l'onglet volumes, placez le curseur de la souris sur le volume, sélectionnez l'icône de menu, puis cliquez sur **Mount**.
2. Cliquez sur **Copier**.
3. Sur vos hôtes Linux, modifiez le texte copié en modifiant le répertoire de destination, puis entrez la commande permettant de monter le volume.

## Gestion des volumes NFS

Vous pouvez gérer les volumes NFS en les clonant, en gérant l'accès aux données, en modifiant le type de disque sous-jacent, etc.

### Clonage de volumes

Si vous avez besoin d'une copie instantanée de vos données sans utiliser beaucoup d'espace disque, vous pouvez créer un clone d'un volume existant.

**Description de la tâche**

Le volume cloné est une copie inscriptible, ponctuelle et efficace en termes d'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.

**Étapes**

1. Dans l'onglet volumes, placez le curseur de la souris sur le volume, sélectionnez l'icône de menu, puis cliquez sur **Clone**.
2. Modifiez le nom du volume cloné, si nécessaire, puis cliquez sur **Clone**.

**Résultat**

Cloud Manager crée un nouveau volume qui est un clone d'un volume existant.

### Gestion de l'accès aux données des volumes

Lorsque vous créez un volume, Cloud Manager met le volume à la disposition de toutes les instances EC2 du VPC dans lesquelles le volume a été créé. Vous pouvez modifier cette valeur par défaut si vous devez limiter l'accès aux données au volume.

#### Étapes

1. Dans l'onglet volumes, placez le curseur de la souris sur le volume, sélectionnez l'icône de menu, puis cliquez sur **gérer l'accès**.
2. Modifiez la liste d'accès au volume, puis cliquez sur **Enregistrer**.

### Modification du disque AWS sous-jacent pour un volume

Vous pouvez modifier le disque AWS sous-jacent qu'un volume utilise pour fournir du stockage. Par exemple, si des performances plus élevées sont nécessaires, vous pouvez passer d'un disque dur optimisé pour le débit à un disque SSD à usage général.

#### Étapes

1. Dans l'onglet volumes, placez le curseur de la souris sur le volume, sélectionnez l'icône de menu, puis cliquez sur **changer disque**.
2. Sélectionnez le type de disque AWS et cliquez sur **Modifier**.

#### Résultat

Cloud Manager déplace le volume vers un agrégat existant qui utilise le type de disque sélectionné ou crée un nouvel agrégat pour le volume.

### Affichage et modification des ressources AWS

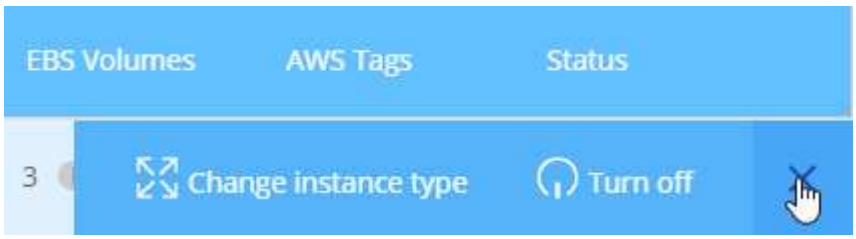
Lorsque vous créez un nouveau volume, Cloud Manager alloue les instances AWS et le stockage EBS requis pour ce volume. Si nécessaire, vous pouvez afficher des informations détaillées sur les instances AWS et le stockage EBS, modifier les types d'instance et désactiver et activer les instances.

#### Étapes

1. Cliquez sur **Ressources AWS**.

   La liste des instances AWS s'affiche. Vous pouvez afficher des détails tels que le type d'instance, l'emplacement AWS et les volumes rattachés à l'instance.

2. Si nécessaire, sélectionnez l'icône de menu située en regard de la colonne État, puis choisissez l'une des actions disponibles :




### Suppression de volumes

Vous pouvez supprimer des volumes dont vous n'avez plus besoin.

**Étapes**

1. Dans l’onglet volumes, placez le curseur de la souris sur le volume, sélectionnez l’icône de menu, puis cliquez sur **Supprimer**.
2. Cliquez sur **Supprimer** pour confirmer la suppression du volume.

# Gestion des données dans le cloud hybride

## Détection et gestion des clusters ONTAP

Cloud Manager peut découvrir les clusters ONTAP dans votre environnement sur site, dans une configuration de stockage privé NetApp et dans IBM Cloud. La découverte de ces clusters vous permet de répliquer facilement des données dans votre environnement cloud hybride directement à partir de Cloud Manager.

### Découverte des clusters ONTAP

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

#### Avant de commencer

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

Cloud Manager détecte les clusters ONTAP à l'aide de HTTPS. Si vous utilisez des stratégies de pare-feu personnalisées, elles doivent répondre aux exigences suivantes :

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

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

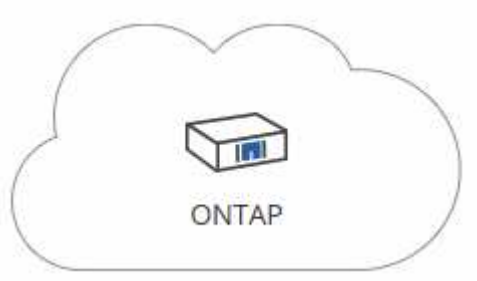
- Le cluster ONTAP doit autoriser l'accès HTTPS entrant via le port 443.

  La stratégie de pare-feu " mgmt " par défaut permet l'accès HTTPS entrant à partir de toutes les adresses IP. Si vous avez modifié cette stratégie par défaut ou si vous avez créé votre propre stratégie de pare-feu, vous devez associer le protocole HTTPS à cette stratégie et activer l'accès à partir de l'hôte Cloud Manager.

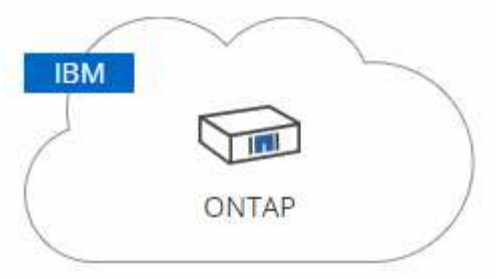
#### Étapes

1. Sur la page environnements de travail, cliquez sur **Ajouter un environnement de travail**.
2. Sous **Discover**, sélectionnez l'une des icônes pour découvrir un cluster ONTAP.

   L'icône suivante vous permet de découvrir un cluster sur site ou une configuration de stockage privé NetApp :




   L'icône suivante vous permet de découvrir ONTAP dans IBM Cloud :




3. Sur la page **ONTAP Cluster Details**, entrez l'adresse IP de gestion du cluster et le mot de passe du compte utilisateur admin.

   Si vous avez sélectionné la première icône, vous devez également choisir le type d'environnement de travail : soit un cluster sur site, soit une configuration de stockage privé NetApp.

4. Sur la page Détails, entrez un nom et une description pour l'environnement de travail, puis cliquez sur **Go**.

**Résultat**

Cloud Manager détecte le cluster. Vous pouvez désormais créer des volumes, répliquer des données vers et depuis le cluster et lancer OnCommand System Manager pour effectuer des tâches avancées.

## Provisionnement des volumes sur des clusters ONTAP

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

**Avant de commencer**

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

**Description de la tâche**

Vous pouvez créer des volumes sur des agrégats existants. Vous ne pouvez pas créer de nouveaux agrégats à partir de Cloud Manager.

**Étapes**

1. Sur la page Working Environments, double-cliquez sur le nom du cluster ONTAP sur lequel vous souhaitez provisionner des volumes.
2. Cliquez sur **Ajouter nouveau volume**.
3. Sur la page Créer un nouveau volume, entrez les détails du volume, puis cliquez sur **Créer**.

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

| Champ | Description |
|---|---|
| Taille | La taille maximale que vous pouvez saisir dépend en grande partie de l'activation du provisionnement fin, ce qui vous permet de créer un volume plus grand que le stockage physique actuellement disponible. |
| Contrôle d'accès (pour NFS uniquement) | Une stratégie d'exportation définit les clients du sous-réseau qui peuvent accéder au volume. Par défaut, Cloud Manager entre une valeur qui donne accès à toutes les instances du sous-réseau. |

| 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. |
| Profil d'utilisation | Les profils d'utilisation définissent les fonctionnalités d'efficacité du stockage NetApp qui sont activées pour un volume. |
| Stratégie Snapshot | Une stratégie de copie Snapshot spécifie la fréquence et le nombre de copies Snapshot créées automatiquement. Une copie Snapshot de NetApp est une image système de fichiers instantanée qui n'a aucun impact sur les performances et nécessite un stockage minimal. Vous pouvez choisir la règle par défaut ou aucune. Vous pouvez en choisir aucune pour les données transitoires : par exemple, tempdb pour Microsoft SQL Server. |

# Réplication des données depuis et vers le cloud

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.

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.

## Choix d'une stratégie de réplication

Une stratégie de réplication définit la manière dont le système de stockage réplique les données d'un volume source vers un volume de destination. Vous devez choisir une stratégie de réplication lorsque vous configurez la réplication des données dans Cloud Manager.

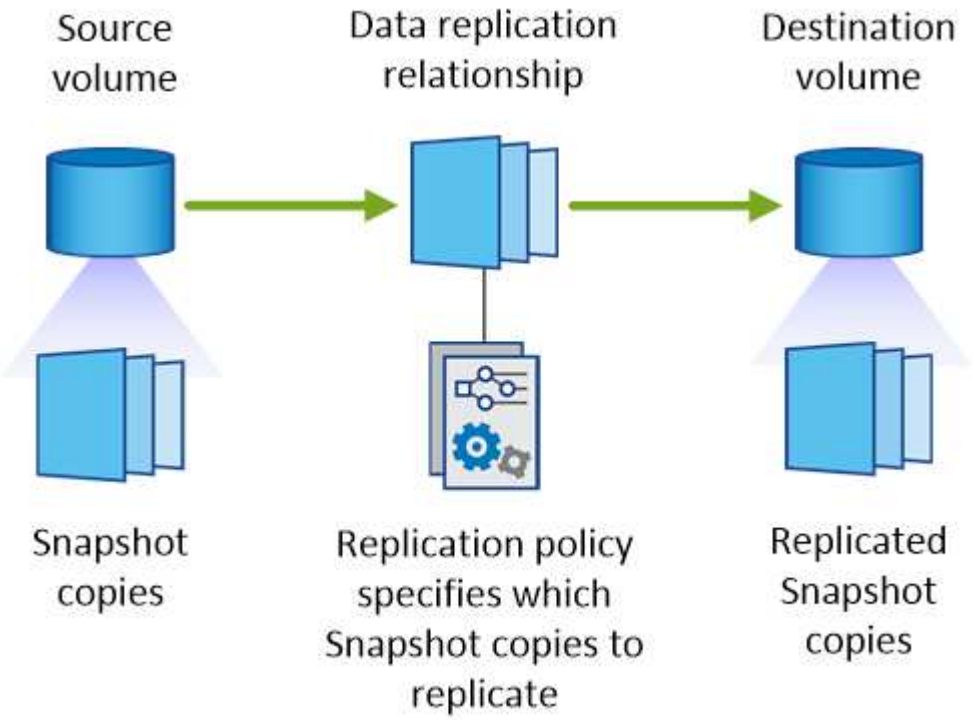
### Quelles sont les règles de réplication

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.

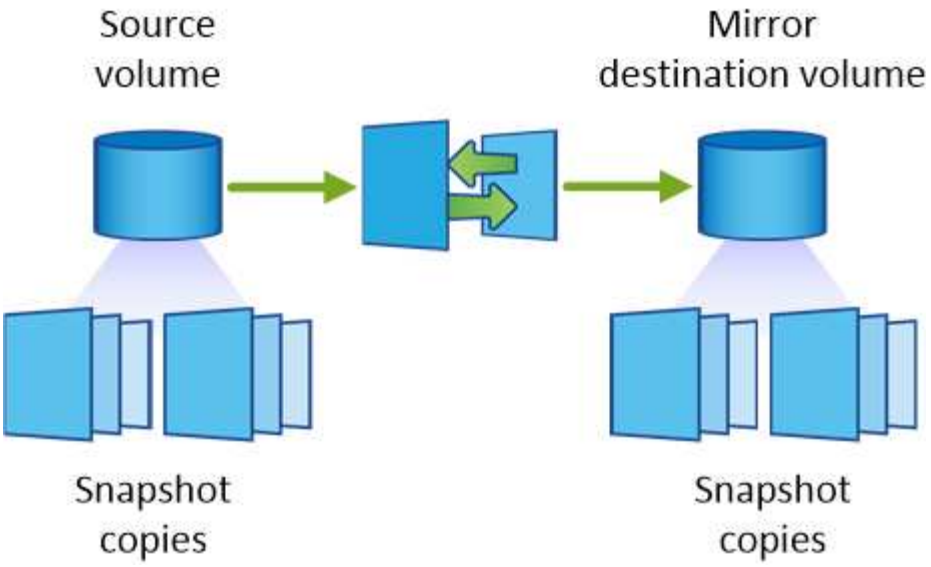
- Une règle *Backup* réplique des copies Snapshot spécifiques sur un volume de destination et les conserve généralement pendant une période plus longue que sur le volume source.

  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.

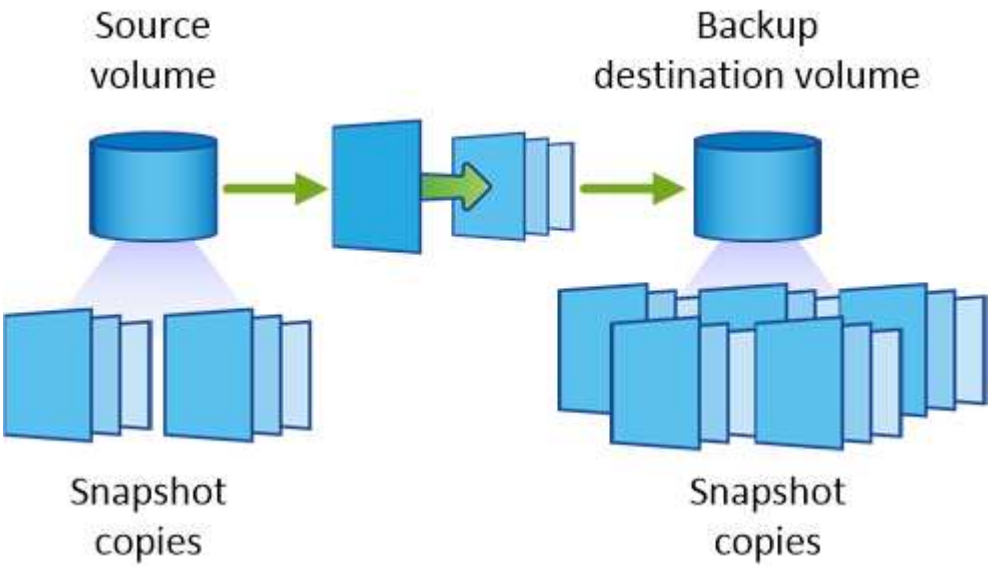
- Une politique *Mirror et Backup* permet la reprise sur incident et la conservation à long terme.

  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.

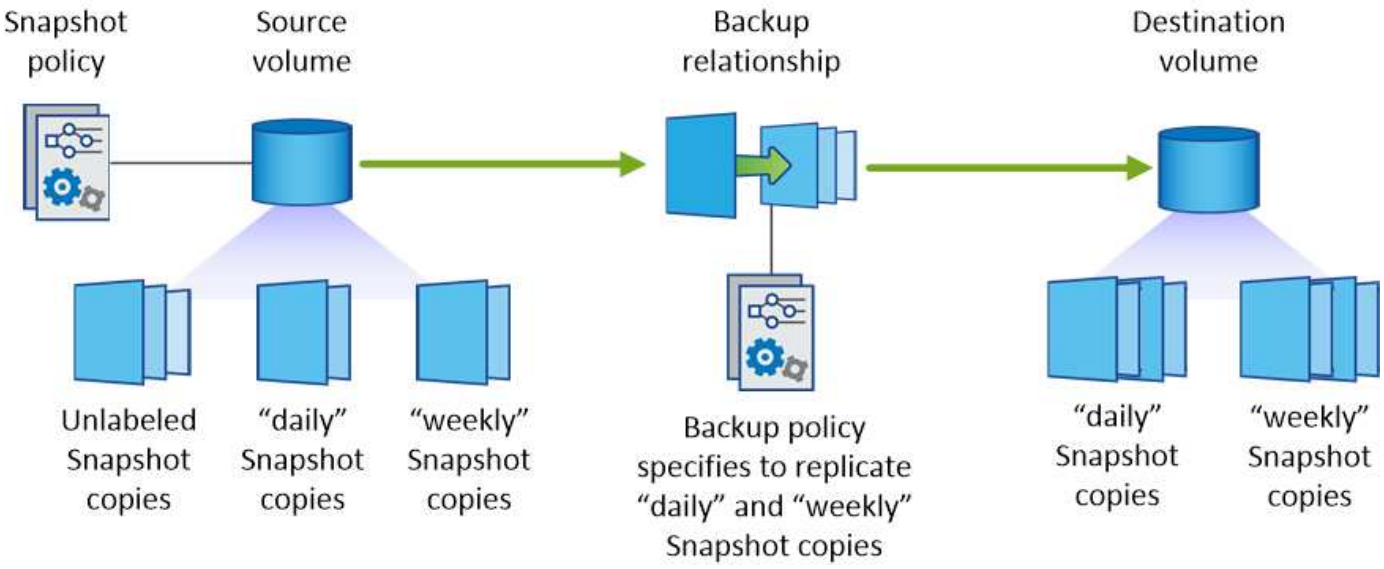
#### Comprendre la relation entre les étiquettes de copie Snapshot et les stratégies de sauvegarde

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.

## Exigences de réplication des données

Avant de pouvoir répliquer des données, vous devez confirmer que des exigences spécifiques sont respectées pour les systèmes Cloud Volumes ONTAP et les clusters ONTAP.

### Exigences de version

Vérifiez que les volumes source et de destination exécutent des versions ONTAP compatibles avant de répliquer les données. Pour plus d'informations, reportez-vous à la "Guide d'alimentation de la protection des données".

### Exigences spécifiques à Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'ICMP et les ports 10000, 11104 et 11105.

  Ces règles sont incluses dans le groupe de sécurité prédéfini.

- Pour répliquer des données entre deux systèmes Cloud Volumes ONTAP dans différents sous-réseaux, les sous-réseaux doivent être routés ensemble (paramètre par défaut).

- Pour répliquer des données entre un système Cloud Volumes ONTAP dans AWS et un système dans Azure, vous devez disposer d'une connexion VPN entre AWS VPC et Azure VNet.

**Exigences spécifiques aux clusters ONTAP**

- Une licence SnapMirror active doit être installée.
- Si le cluster se trouve sur votre site, vous devez disposer d'une connexion entre votre réseau d'entreprise et AWS ou Azure, qui est généralement une connexion VPN.
- Les clusters ONTAP doivent répondre à des exigences supplémentaires en termes de sous-réseau, de port, de pare-feu et de cluster.

  Pour plus d'informations, reportez-vous au Cluster and SVM Peering Express Guide de votre version d'ONTAP.

## 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.

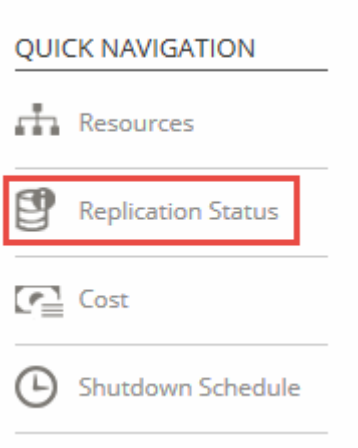
## Gestion des planifications et des relations de réplication des données

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 attribués dans le locataire ou pour un environnement de travail spécifique :

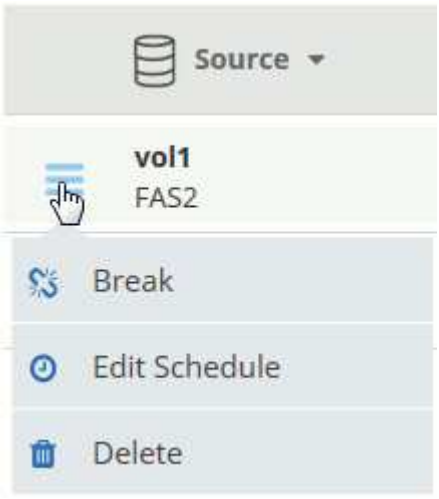
| Option | Action |
| --- | --- |
| Tous les environnements de travail attribués dans le locataire | Cliquez sur Etat de la réplication dans la barre de navigation.<br>  |

| Option | Action |
| --- | --- |
| Un environnement de travail spécifique | Sélectionnez l'environnement de travail, puis cliquez sur Etat de la réplication.<br>  |

2. Vérifiez l'état des relations de réplication des données pour vérifier qu'elles sont en bon état.

Si l'état d'une relation est inactif et que l'état Miroir n'est pas initialisé, vous devez initialiser la relation à partir du système de destination pour que la réplication des données se produise selon le planning défini. Vous pouvez initialiser la relation à l'aide de System Manager ou de l'interface de ligne de commande (CLI). Ces états peuvent apparaître en cas de défaillance du système de destination, puis revenir en ligne.

3. Sélectionnez l'icône de menu située en regard du volume source, puis choisissez l'une des actions disponibles.




Le tableau suivant décrit les actions disponibles :

| Action | Description |
| --- | --- |
| Pause | Rompt la relation entre les volumes source et de destination et active le volume de destination pour l'accès aux données. Cette option est généralement utilisée lorsque le volume source ne peut pas servir de données en raison d'événements tels que la corruption des données, la suppression accidentelle ou un état hors ligne. Pour plus d'informations sur la configuration d'un volume de destination pour l'accès aux données et la réactivation d'un volume source, reportez-vous au Guide ONTAP 9 Volume Disaster Recovery Express Guide. |
| Resynchroniser | Rétablit une relation interrompue entre les volumes et reprend la réplication des données selon le planning défini.<br><br>Lorsque vous resynchronisez les volumes, le contenu du volume de destination est remplacé par le contenu du volume source.<br><br>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. |
| 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.

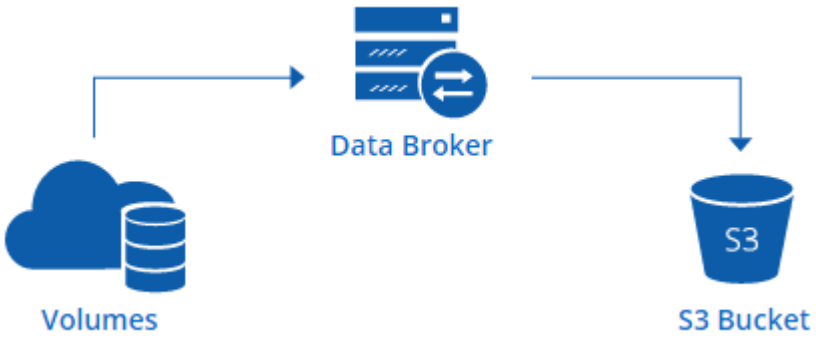
# Synchronisation des données vers AWS S3

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

## Fonctionnement de la fonction de synchronisation vers S3

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

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




Si vous souhaitez effectuer des actions Cloud Sync avancées, accédez directement au service Cloud Sync. De là, vous pouvez effectuer des actions telles que la synchronisation de S3 vers un serveur NFS, le choix de compartiments S3 différents pour les volumes et la modification des plannings.

La fonctionnalité de synchronisation vers S3 est disponible uniquement pour les administrateurs et les administrateurs de service partagé de Cloud Manager.

### Essai gratuit de 14 jours

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

### Comment obtenir de l'aide

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

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

## Intégration d’un environnement de travail au service Cloud Sync

Si vous souhaitez synchroniser des volumes vers AWS S3 directement à partir de Cloud Manager, vous devez intégrer l’environnement de travail au service Cloud Sync.

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

**Étapes**

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

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

## Gestion des relations de synchronisation des volumes

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

**Étapes**

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

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

# Administration d'Cloud Volumes ONTAP

## Connexion à Cloud Volumes ONTAP

Si vous avez besoin d'une gestion avancée de Cloud Volumes ONTAP, vous pouvez le faire à l'aide d'OnCommand System Manager ou de l'interface de ligne de commande.

### Connexion à OnCommand System Manager

Vous devrez peut-être effectuer certaines tâches Cloud Volumes ONTAP à partir d'OnCommand System Manager, un outil de gestion basé sur un navigateur qui s'exécute sur le système Cloud Volumes ONTAP. Par exemple, vous devez utiliser System Manager pour créer des LUN.

#### Avant de commencer

L'ordinateur à partir duquel vous accédez à Cloud Manager doit disposer d'une connexion réseau à Cloud Volumes ONTAP. Par exemple, vous devrez peut-être vous connecter à Cloud Manager à partir d'un hôte de saut dans AWS ou Azure.

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

#### Étapes

1. Sur la page Working Environments, double-cliquez sur le système Cloud Volumes ONTAP que vous souhaitez gérer avec System Manager.
2. Cliquez sur l'icône de menu, puis sur **Avancé > System Manager**.
3. Cliquez sur **lancer**.

   System Manager se charge dans un nouvel onglet de navigateur.

4. Sur l'écran de connexion, saisissez **admin** dans le champ Nom d'utilisateur, saisissez le mot de passe que vous avez spécifié lors de la création de l'environnement de travail, puis cliquez sur **connexion**.

#### Résultat

La console System Manager se charge. Vous pouvez désormais l'utiliser pour gérer Cloud Volumes ONTAP.

### Connexion à l'interface de ligne de commande Cloud Volumes ONTAP

L'interface de ligne de commande Cloud Volumes ONTAP vous permet d'exécuter toutes les commandes administratives et constitue un bon choix pour les tâches avancées ou si vous êtes plus à l'aise avec l'interface de ligne de commande. Vous pouvez vous connecter à l'interface de ligne de commande à l'aide de Secure Shell (SSH).

#### Avant de commencer

L'hôte à partir duquel vous utilisez SSH pour vous connecter à Cloud Volumes ONTAP doit disposer d'une connexion réseau à Cloud Volumes ONTAP. Par exemple, vous devrez peut-être utiliser SSH à partir d'un hôte de saut dans AWS ou Azure.

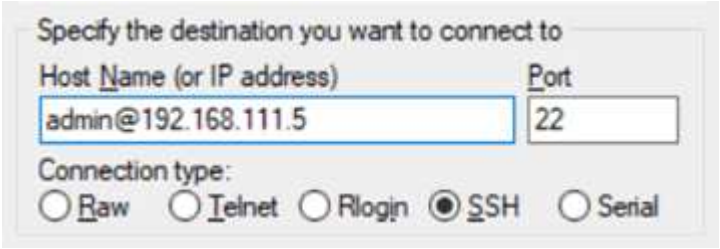
Lorsqu'elles sont déployées dans plusieurs environnements AZS, les configurations Cloud Volumes ONTAP HA utilisent une adresse IP flottante pour l'interface de gestion de cluster, ce qui signifie que le routage externe n'est pas disponible. Vous devez vous connecter à partir d'un hôte faisant partie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

**Étapes**

1. Dans Cloud Manager, identifiez l'adresse IP de l'interface de gestion du cluster :
   a. Sur la page Working Environments, sélectionnez le système Cloud Volumes ONTAP.
   b. Copiez l'adresse IP de gestion du cluster qui apparaît dans le volet droit.
2. Utilisez SSH pour vous connecter à l'adresse IP de l'interface de gestion du cluster à l'aide du compte admin.

   **Exemple**

   L'image suivante montre un exemple utilisant PuTTY :

3. À l'invite de connexion, entrez le mot de passe du compte admin.

   **Exemple**

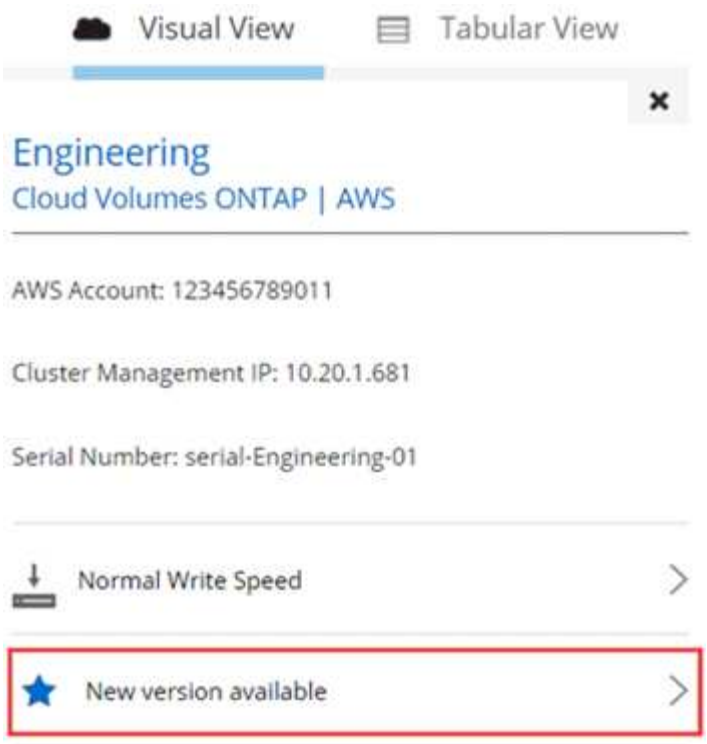
```
Password: ********
COT2::>
```

# Mise à jour du logiciel Cloud Volumes ONTAP

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

## Présentation

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 de Cloud Volumes ONTAP vers la dernière version.

Pour les systèmes HA, 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
- 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.

Les mises à niveau des paires HA sont sans interruption. Une mise à niveau sans interruption met à niveau les deux nœuds d'une paire haute disponibilité simultanément tout en maintenant le service 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".

### 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.

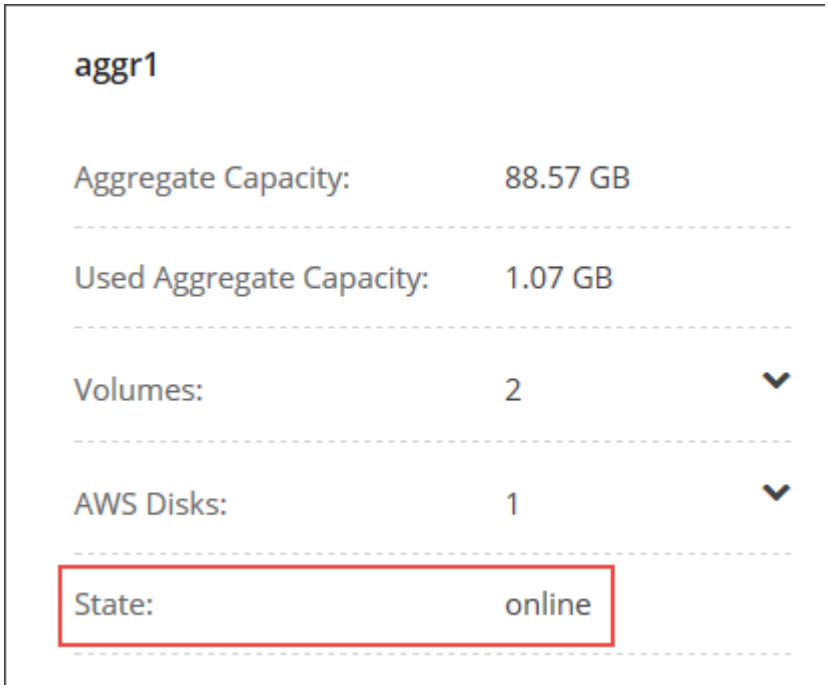
#### Description de la tâche

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 de Cloud Volumes ONTAP vers la dernière version

Vous pouvez effectuer une mise à niveau vers la dernière version de Cloud Volumes ONTAP directement à partir de Cloud Manager. Cloud Manager vous avertit lorsqu'une nouvelle version est disponible.

### 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.

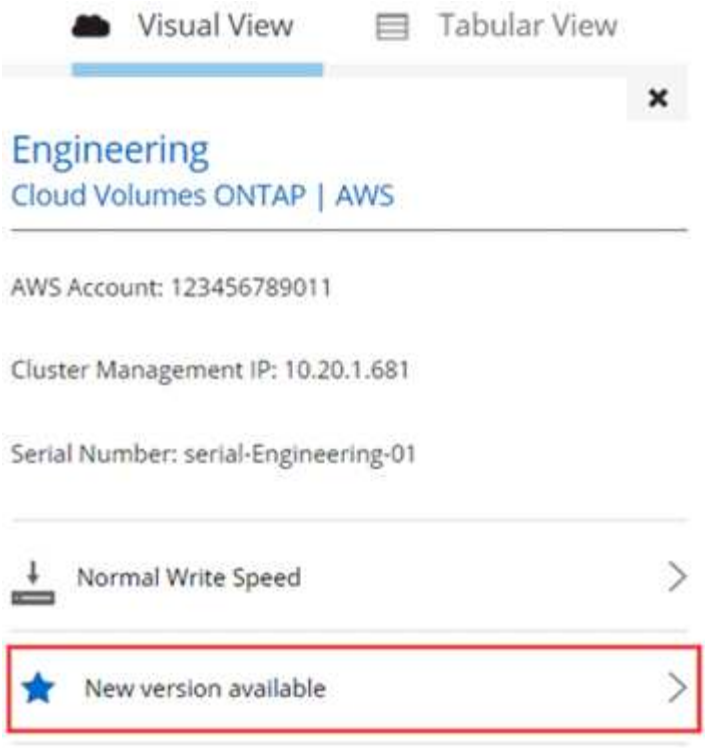
### Description de la tâche

- 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.
- Les mises à niveau des paires HA sont sans interruption. Une mise à niveau sans interruption met à niveau les deux nœuds d'une paire haute disponibilité simultanément tout en maintenant le service aux clients.

### 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.

**Description de la tâche**

- 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.
- Les mises à niveau des paires HA sont sans interruption. Une mise à niveau sans interruption met à niveau les deux nœuds d'une paire haute disponibilité simultanément tout en maintenant le service aux clients.

### 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 avec le VPC, vous pouvez placer l'image du logiciel Cloud Volumes ONTAP sur un serveur HTTP ou FTP de votre propre réseau. Sinon, vous devez placer le fichier sur un serveur HTTP ou FTP dans AWS.
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. Le processus met le système Cloud Volumes ONTAP hors ligne jusqu'à 25 minutes.

### Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > mettre à jour Cloud Volumes ONTAP**.
2. Sur la page mise à jour du logiciel, sélectionnez l'image de remplacement, puis cliquez sur **changer l'image**.

3. Cliquez sur **Continuer** pour confirmer.

**Résultat**

Cloud Manager démarre la mise à jour logicielle. Vous pouvez effectuer des actions sur l'environnement de travail une fois la mise à jour logicielle terminée.

**Une fois que vous avez terminé**

Si vous avez suspendu les transferts SnapMirror, utilisez System Manager pour reprendre les transferts.

# Modification des systèmes Cloud Volumes ONTAP

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

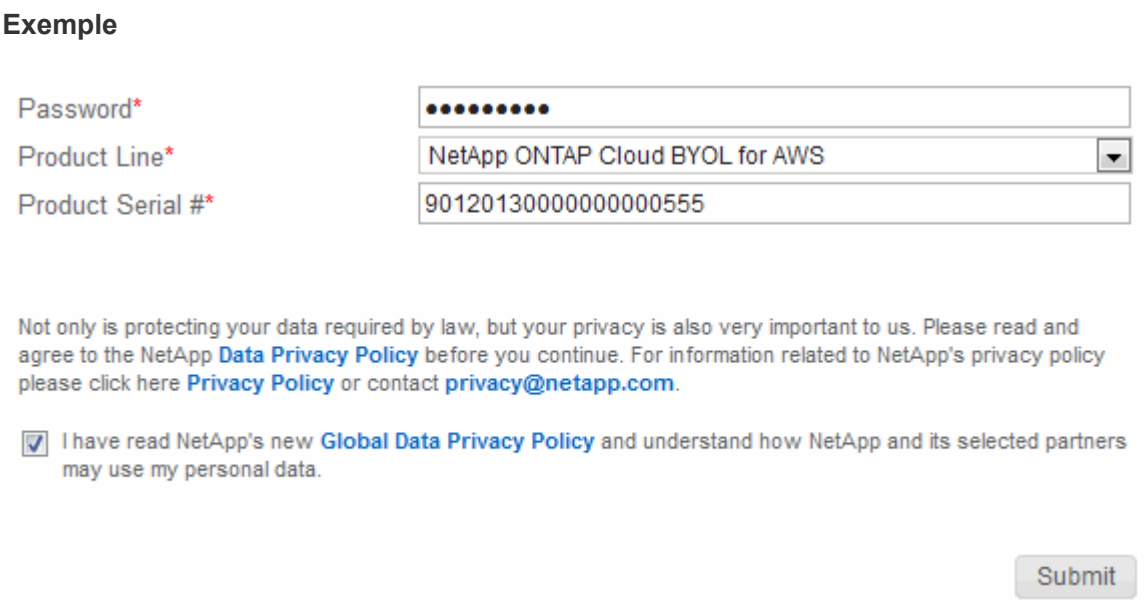
## Installation de fichiers de licence sur les systèmes Cloud Volumes ONTAP BYOL

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

**Étapes**

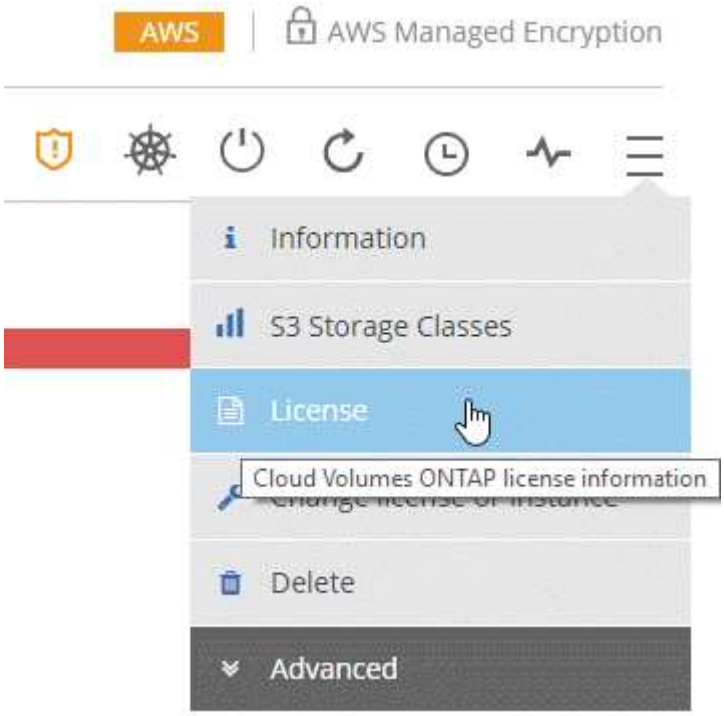
1. Accédez au "Générateur de fichiers de licences NetApp" Et connectez-vous en utilisant vos identifiants du site du support NetApp.
2. Entrez votre mot de passe, sélectionnez votre produit (**NetApp Cloud Volumes ONTAP BYOL pour AWS**, **NetApp Cloud Volumes ONTAP BYOL pour Azure** ou **NetApp Cloud Volumes ONTAP BYOL pour AWS**), entrez le numéro de série, confirmez que vous avez lu et accepté la déclaration de confidentialité, puis cliquez sur **Envoyer**.

   **Exemple**




3. Choisissez si vous souhaitez recevoir le fichier numéro de série.NLF JSON par e-mail ou par téléchargement direct.

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




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

**Résultat**

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

## Modification du type d'instance ou de machine virtuelle pour Cloud Volumes ONTAP

Vous pouvez choisir parmi plusieurs types d'instance ou de machine virtuelle lorsque vous lancez Cloud Volumes ONTAP dans AWS ou Azure. Vous pouvez modifier le type d'instance ou de machine virtuelle à tout moment si vous déterminez qu'il est sous-dimensionné ou surdimensionné en fonction de vos besoins.

**Description de la tâche**

- 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 du type d'instance ou de machine virtuelle affecte les frais de service AWS ou Azure.

**Étapes**

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **changer la licence ou l'instance** pour AWS ou cliquez sur **changer la licence ou VM** pour Azure.
2. Si vous utilisez une configuration payante, vous pouvez choisir une licence différente.

3. Sélectionnez une instance ou un type de machine virtuelle, 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 diminue la limite de capacité brute et vous permet de choisir entre différents types d'instance EC2 ou de machine virtuelle Azure.

**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 du type d'instance ou de machine virtuelle affecte les frais de service AWS ou Azure.

**Étapes**

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **changer la licence ou l'instance** pour AWS ou cliquez sur **changer la licence ou VM** pour Azure.
2. Sélectionnez un type de licence et un type d'instance ou de machine virtuelle, cochez la case pour confirmer que vous comprenez les implications de la modification, puis cliquez sur **OK**.

**Résultat**

Cloud Volumes ONTAP redémarre avec la nouvelle licence, le type d'instance ou le type de machine virtuelle, ou les deux.

## Passage à une autre configuration Cloud Volumes ONTAP

Si vous souhaitez passer d'un abonnement payant à un abonnement BYOL ou d'un système Cloud Volumes ONTAP à une paire HA, vous pouvez déployer un nouveau système, puis répliquer les données du système existant vers le nouveau système.

**Étapes**

1. Créez un nouvel environnement de travail Cloud Volumes ONTAP.

   "Lancement d'Cloud Volumes ONTAP dans AWS"
   "Lancement d'Cloud Volumes ONTAP dans Azure"

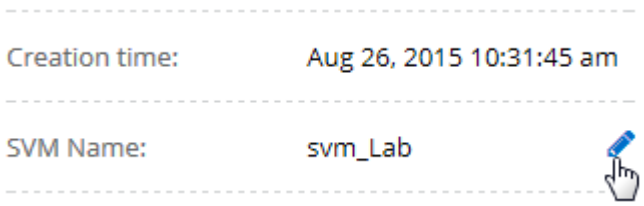
2. "Configuration de la réplication des données unique" entre les systèmes pour chaque volume que vous devez répliquer.
3. Terminez le système Cloud Volumes ONTAP dont vous n'avez plus besoin par "suppression de l'environnement de travail d'origine".

## Modification du nom de la machine virtuelle de stockage

Cloud Manager nomme automatiquement la machine virtuelle de stockage (SVM) pour Cloud Volumes ONTAP. Vous pouvez modifier le nom du SVM si vous disposez de normes strictes en matière de nommage. Par exemple, vous pouvez le faire correspondre à la façon dont vous nommez les SVM pour vos clusters ONTAP.

### Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **informations**.
2. Cliquez sur l'icône d'édition située à droite du nom SVM.




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

## Modification du mot de passe de Cloud Volumes ONTAP

Cloud Volumes ONTAP inclut un compte d'administration de cluster. Si nécessaire, vous pouvez modifier le mot de passe de ce compte à partir de Cloud Manager.

> Vous ne devez pas modifier le mot de passe du compte admin via System Manager ou l'interface de ligne de commande. Le mot de passe ne sera pas pris en compte dans Cloud Manager. Par conséquent, Cloud Manager ne peut pas contrôler l'instance correctement.

### Étapes

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > définir mot de passe**.
2. Saisissez le nouveau mot de passe deux fois, puis cliquez sur **Enregistrer**.

   Le nouveau mot de passe doit être différent de l'un des six derniers mots de passe utilisés.

## Modification de la MTU réseau pour les instances c4.4xlarge et c4.8xlarge

Par défaut, Cloud Volumes ONTAP est configuré pour utiliser 9 000 MTU (également appelés trames Jumbo) lorsque vous choisissez l'instance c4.4xlarge ou l'instance c4.8xlarge dans AWS. Vous pouvez modifier la MTU réseau à 1 500 octets si cela est plus approprié pour votre configuration réseau.

### Description de la tâche

Une unité de transmission réseau maximale (MTU) de 9 000 octets peut fournir le débit réseau maximal le plus élevé possible pour des configurations spécifiques.

9 000 MTU sont un bon choix si les clients du même VPC communiquent avec le système Cloud Volumes ONTAP et que certains ou tous ces clients prennent également en charge 9 000 MTU. Si le trafic quitte le VPC, la fragmentation des paquets peut se produire, ce qui dégrade les performances.

Un MTU réseau de 1 500 octets est un bon choix si les clients ou les systèmes extérieurs au VPC communiquent avec le système Cloud Volumes ONTAP.

**Étapes**

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Avancé > utilisation du réseau**.
2. Sélectionnez **Standard** ou **Jumbo Frames**.
3. Cliquez sur **Modifier**.

## Modification des tables de routage associées aux paires HA dans plusieurs AZS d'AWS

Vous pouvez modifier les tables de routage AWS incluant des routes vers les adresses IP flottantes pour une paire haute disponibilité. Vous pouvez le faire si les nouveaux clients NFS ou CIFS ont besoin d'accéder à une paire haute disponibilité dans AWS.

**Étapes**

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **informations**.
2. Cliquez sur **tables de routage**.
3. Modifiez la liste des tables de routage sélectionnées, puis cliquez sur **Enregistrer**.

**Résultat**

Cloud Manager envoie une requête AWS pour modifier les tables de routage.

# Gestion de l'état du Cloud Volumes ONTAP

Vous pouvez arrêter et lancer Cloud Volumes ONTAP depuis Cloud Manager pour gérer les coûts de calcul du cloud.

## Planification des arrêts automatiques de Cloud Volumes ONTAP

Vous pouvez arrêter Cloud Volumes ONTAP à des intervalles réguliers afin de réduire les coûts de calcul. Au lieu de le faire manuellement, vous pouvez configurer Cloud Manager de sorte qu'il s'arrête automatiquement, puis redémarre les systèmes à des moments spécifiques.

**Description de la tâche**

Lorsque vous planifiez un arrêt automatique de votre système Cloud Volumes ONTAP, Cloud Manager reporte l'arrêt du système si un transfert de données actif est en cours. Cloud Manager arrête le système une fois le transfert terminé.

Cette tâche planifie les arrêts automatiques des deux nœuds d'une paire haute disponibilité.

**Étapes**

1. Dans l'environnement de travail, cliquez sur l'icône horloge :

2. Spécifiez la planification de l'arrêt :

   a. Choisissez si vous souhaitez arrêter le système tous les jours, tous les jours de semaine, tous les week-ends ou toute combinaison des trois options.

   b. Indiquez quand vous souhaitez désactiver le système et pendant combien de temps vous voulez le désactiver.

**Exemple**

L'image suivante montre un calendrier qui indique à Cloud Manager d'arrêter le système tous les samedis à 12:00 pendant 48 heures. Cloud Manager redémarre le système tous les lundis à 12:00


3. Cliquez sur **Enregistrer**.

**Résultat**

Cloud Manager enregistre la planification. L'icône de l'horloge change pour indiquer qu'un programme est défini : 

## Arrêt d'Cloud Volumes ONTAP

L'arrêt de Cloud Volumes ONTAP vous permet d'économiser de l'espace de calcul et de créer des snapshots des disques racines et de démarrage, ce qui peut être utile pour la résolution des problèmes.

**Description de la tâche**

Lorsque vous arrêtez une paire HA, Cloud Manager arrête les deux nœuds.

**Étapes**

1. Dans l'environnement de travail, cliquez sur l'icône **Désactiver**.

2. Conservez l'option de création de snapshots activés car les snapshots peuvent activer la récupération du système.
3. Cliquez sur **Désactiver**.

   L'arrêt du système peut prendre jusqu'à quelques minutes. Vous pouvez redémarrer les systèmes ultérieurement à partir de la page de l'environnement de travail.

# Contrôle des coûts des ressources AWS

Avec Cloud Manager, vous pouvez consulter les coûts associés aux ressources pour l'exécution de Cloud Volumes ONTAP dans AWS. Vous pouvez également voir les économies réalisées grâce aux fonctionnalités NetApp qui permettent de réduire les coûts de stockage.

**Description de la tâche**

Cloud Manager met à jour les coûts lorsque vous actualisez la page. Vous devez vous référer à AWS pour plus de détails sur le coût final.

**Étape**

1. Vérifiez que Cloud Manager peut obtenir des informations de coûts depuis AWS :
   a. Assurez-vous que la politique IAM qui fournit les autorisations à Cloud Manager inclut les actions suivantes :

      ```
      "ce:GetReservationUtilization",
      "ce:GetDimensionValues",
      "ce:GetCostAndUsage",
      "ce:GetTags"
      ```

      Ces actions sont incluses dans la dernière "Politique de Cloud Manager". Les nouveaux systèmes déployés à partir de NetApp Cloud Central incluent automatiquement ces autorisations.

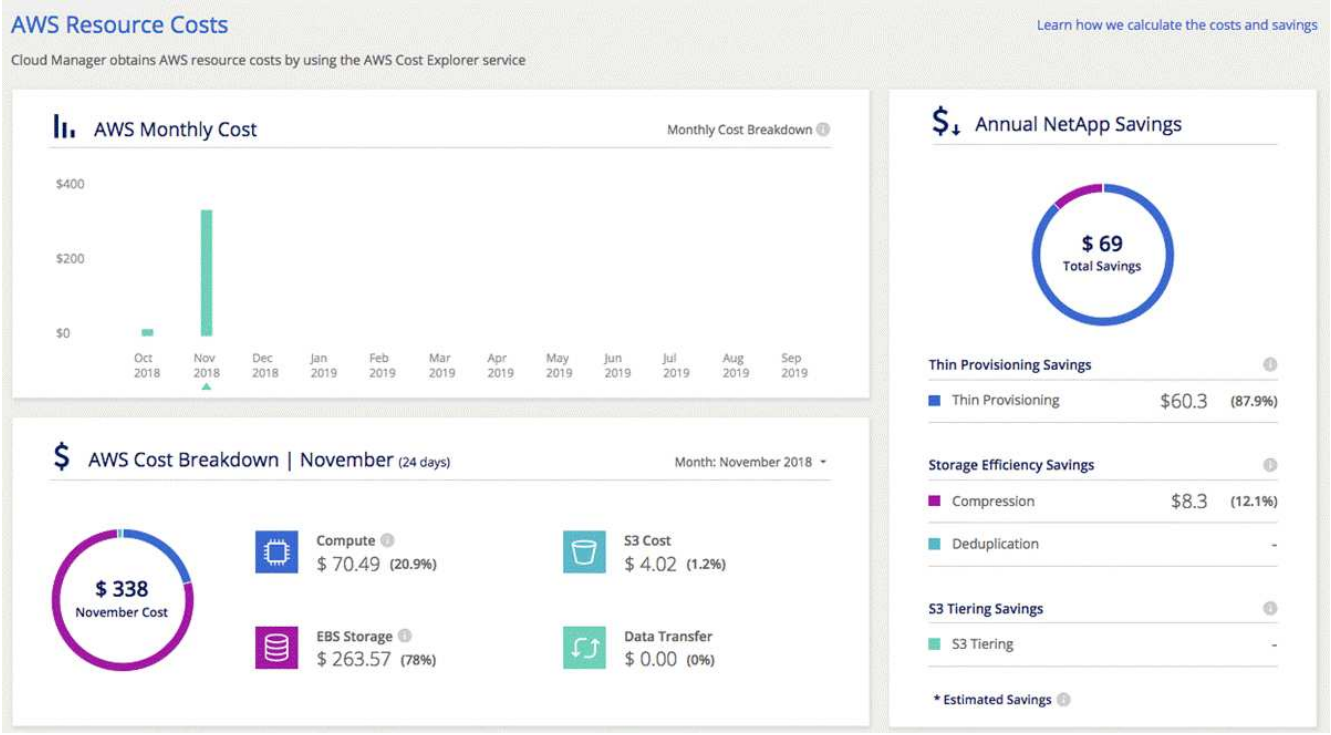
   b. "Activer la balise **WorkingEnvironnement**".

      Pour suivre vos coûts AWS, Cloud Manager attribue une balise d'allocation des coûts aux instances Cloud Volumes ONTAP. Après avoir créé votre premier environnement de travail, activez la balise **WorkingEnvironment,Id**. Les balises définies par l'utilisateur n'apparaissent pas dans les rapports de facturation AWS tant que vous ne les activez pas dans la console de facturation et de gestion des coûts.

2. Sur la page environnements de travail, sélectionnez un environnement de travail Cloud Volumes ONTAP, puis cliquez sur **coût**.

   La page coûts affiche les coûts des mois actuels et précédents et présente vos économies annuelles sur les produits NetApp, si vous avez activé les fonctions d'économies de volumes offertes par NetApp.

   L'image suivante montre un exemple de page de coût :

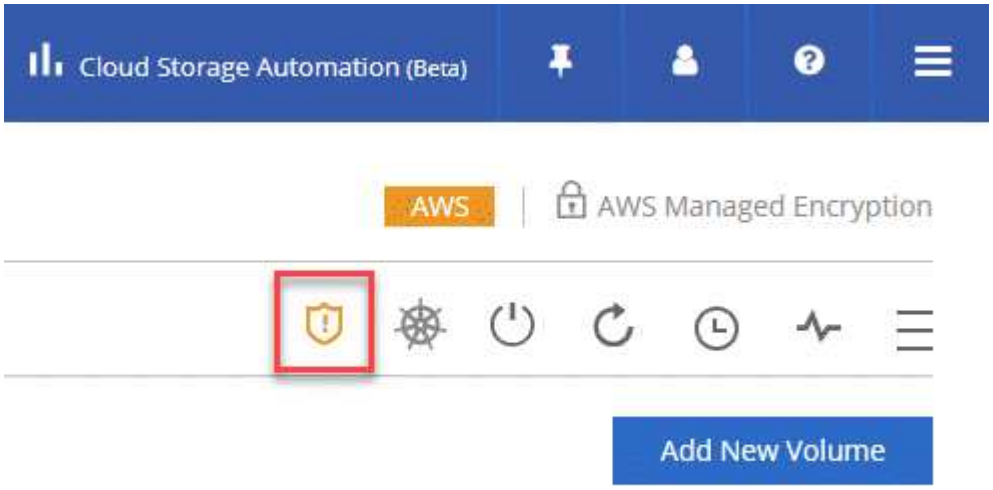



# Renforcer la protection contre les attaques par ransomware

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

**Étapes**

1. Dans l'environnement de travail, cliquez sur l'icône **ransomware**.

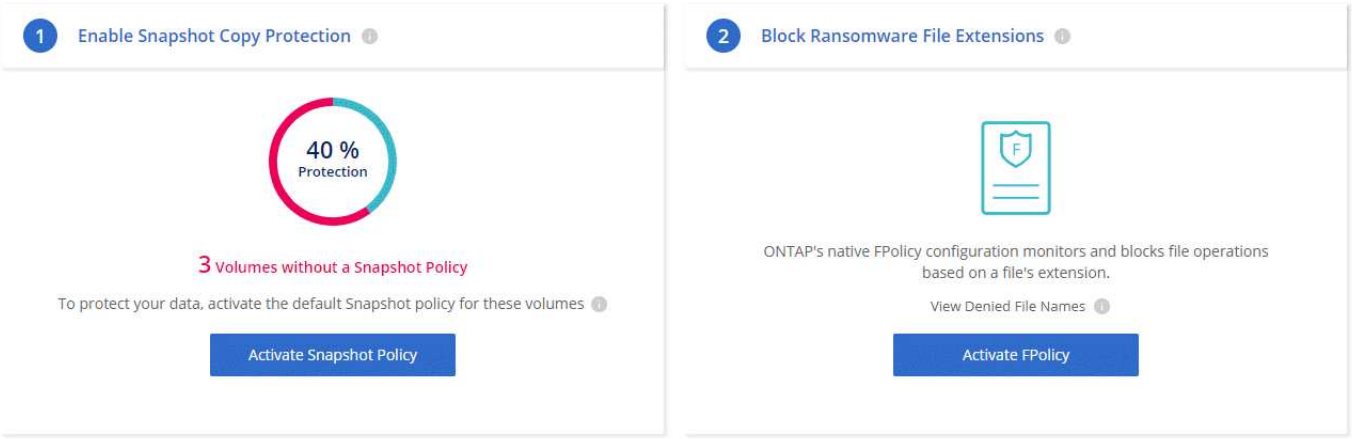



2. Implémentez la solution NetApp en cas d'attaque par ransomware :
   a. Cliquez sur **Activer la stratégie de snapshot**, si des volumes n'ont pas de règle de snapshot activée.

La technologie Snapshot de NetApp offre la meilleure solution du secteur pour résoudre les problèmes liés aux attaques par ransomware. Le mieux pour réussir la récupération est d'effectuer une restauration à partir de sauvegardes non infectées. Les copies Snapshot sont en lecture seule, ce qui empêche la corruption par ransomware. Ils peuvent également assurer la granularité pour créer des images d'une copie de fichiers unique ou d'une solution complète de reprise après incident.

b. Cliquez sur **Activer FPolicy** pour activer la solution FPolicy d'ONTAP, qui peut bloquer les opérations de fichiers en fonction de l'extension d'un fichier.

   Cette solution préventive améliore la protection contre les attaques par ransomware en bloquant les types de fichiers généralement utilisés.




# Ajout de systèmes Cloud Volumes ONTAP existants à Cloud Manager

Vous pouvez découvrir et ajouter des systèmes Cloud Volumes ONTAP existants à Cloud Manager. Vous pouvez le faire si votre système Cloud Manager est devenu inutilisable et que vous avez lancé un nouveau système, mais que vous n'avez pas pu restaurer tous les systèmes Cloud Volumes ONTAP à partir d'une sauvegarde Cloud Manager récente.

### 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. Sous découvrir, sélectionnez **Cloud Volumes ONTAP**.

3. Sur la page Région, choisissez la région dans laquelle les instances sont exécutées, puis sélectionnez les instances.
4. Sur la page informations d'identification, entrez le mot de passe de l'utilisateur administrateur Cloud Volumes ONTAP, puis cliquez sur **Go**.

**Résultat**

Cloud Manager ajoute les instances Cloud Volumes ONTAP au locataire.

# Suppression d'un environnement de travail Cloud Volumes ONTAP

Il est préférable de supprimer les systèmes Cloud Volumes ONTAP de Cloud Manager plutôt que d'AWS ou Azure. Par exemple, si vous mettez fin à une instance Cloud Volumes ONTAP sous licence depuis AWS, vous ne pouvez pas utiliser la clé de licence pour une autre instance. Vous devez supprimer l'environnement de travail de Cloud Manager pour libérer la licence.

**Description de la tâche**

Lorsque vous supprimez un environnement de travail, Cloud Manager met fin aux instances, supprime les disques et les snapshots.

> Les instances de Cloud Volumes ONTAP bénéficient d'une protection de terminaison pour empêcher la fermeture accidentelle d'AWS. Cependant, si vous arrêtez une instance Cloud Volumes ONTAP d'AWS, vous devez accéder à la console AWS CloudFormation et supprimer la pile de l'instance. Le nom de la pile est le nom de l'environnement de travail.

**Étapes**

1. Dans l'environnement de travail, cliquez sur l'icône de menu, puis sur **Supprimer**.
2. Saisissez le nom de l'environnement de travail, puis cliquez sur **Supprimer**.

   La suppression de l'environnement de travail peut prendre jusqu'à 5 minutes.

# Administration de Cloud Manager

## Mise à jour de Cloud Manager

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

### Activation des mises à jour automatiques

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

#### Description de la tâche

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

#### Étapes

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur la liste déroulante des tâches, puis sélectionnez **Paramètres**.
2. Cochez la case sous mises à jour automatiques de Cloud Manager, puis cliquez sur **Enregistrer**.

### Mise à jour de Cloud Manager vers la dernière version

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

#### Avant de commencer

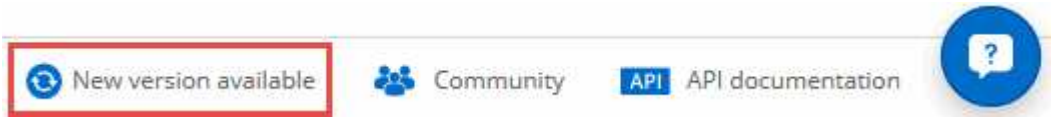
Vous devriez avoir passé en revue "nouveautés de la version" identifier les nouvelles exigences et les changements en matière de support

#### Description de la tâche

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

#### Étapes

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




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

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

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

5. Complétez la boîte de dialogue de confirmation, puis cliquez sur **OK** :
    a. Conservez l'option de téléchargement d'une sauvegarde car vous pouvez l'utiliser pour restaurer la configuration de Cloud Manager, si nécessaire.
    b. Lisez les termes et conditions, puis cochez la case **J'ai lu et approuvé les termes et conditions (CLUF)**.
6. Lorsque vous y êtes invité, enregistrez la sauvegarde de Cloud Manager.

**Résultat**

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

## Mise à jour de Cloud Manager avec un correctif

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

**Description de la tâche**

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

**Étapes**

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur la liste déroulante des tâches, puis sélectionnez **Update**.
2. Cliquez sur le lien pour mettre à jour Cloud Manager avec le correctif fourni.


3. Complétez la boîte de dialogue de confirmation, puis cliquez sur **OK** :
    a. Conservez l'option de téléchargement d'une sauvegarde activée car vous pouvez l'utiliser pour restaurer la configuration de Cloud Manager, si nécessaire.
    b. Lisez les termes et conditions, puis cochez la case **J'ai lu et approuvé les termes et conditions (CLUF)**.
4. Sélectionnez le correctif que vous avez fourni.
5. Lorsque vous y êtes invité, enregistrez la sauvegarde de Cloud Manager.

**Résultat**

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

# Sauvegarde et restauration de Cloud Manager

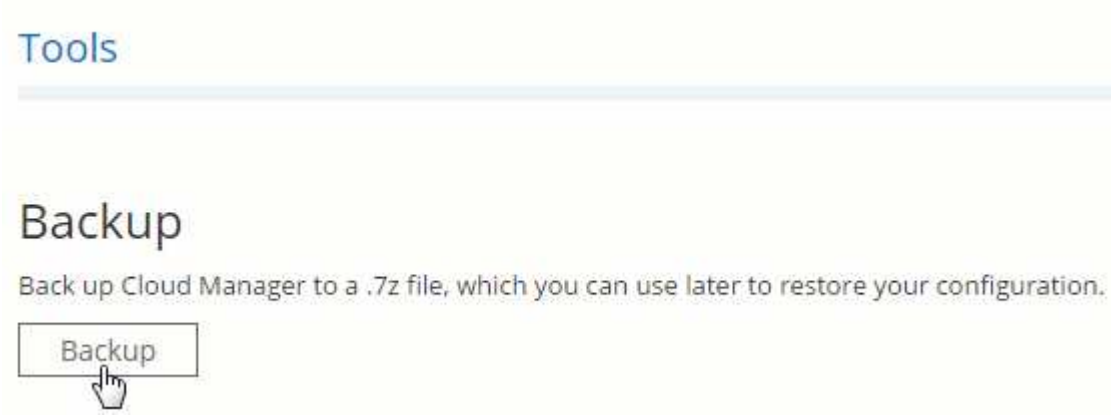
Cloud Manager vous permet de sauvegarder et de restaurer sa base de données afin de protéger votre configuration et de résoudre les problèmes.

## Sauvegarde de Cloud Manager

Il est recommandé de sauvegarder régulièrement la base de données Cloud Manager. Si vous rencontrez des problèmes, vous pouvez restaurer Cloud Manager à partir d'une sauvegarde précédente.

**Étapes**

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur la liste déroulante des tâches, puis sélectionnez **Outils**.
2. Cliquez sur **Backup**.




3. Lorsque vous y êtes invité, enregistrez le fichier de sauvegarde dans un emplacement sécurisé afin de pouvoir le récupérer au besoin.

## Restauration de Cloud Manager à partir d'une sauvegarde

La restauration de Cloud Manager à partir d'une sauvegarde remplace les données existantes par celles de la sauvegarde.

**Étapes**

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur la liste déroulante des tâches, puis sélectionnez **Outils**.
2. Cliquez sur **Restaurer**.
3. Cliquez sur **OK** pour confirmer.
4. Sélectionnez la sauvegarde.

**Résultat**

Cloud Manager restaure la base de données à partir du fichier de sauvegarde.

# Suppression des environnements de travail Cloud Volumes ONTAP

Cloud Manager Admin peut supprimer un environnement de travail Cloud Volumes ONTAP pour le déplacer vers un autre système ou pour résoudre les problèmes de découverte.

**Description de la tâche**

La suppression d'un environnement de travail Cloud Volumes ONTAP le supprime de Cloud Manager. Il ne

supprime pas le système Cloud Volumes ONTAP. Vous pourrez par la suite redécouvrir l'environnement de travail.

La suppression d'un environnement de travail de Cloud Manager vous permet d'effectuer les opérations suivantes :

- Redécouvrez-le dans un autre locataire
- Redécouvrez-le à partir d'un autre système Cloud Manager
- Redécouvrez-le si vous avez rencontré des problèmes lors de la découverte initiale

**Étapes**

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur la liste déroulante des tâches, puis sélectionnez **Outils**.
2. Dans la page Outils, cliquez sur **lancer**.
3. Sélectionnez l'environnement de travail Cloud Volumes ONTAP que vous souhaitez supprimer.
4. Sur la page Revue et approbation, cliquez sur **Go**.

**Résultat**

Cloud Manager supprime l'environnement de travail. Les utilisateurs peuvent à tout moment redécouvrir cet environnement de travail à partir de la page des environnements de travail.

# Modification des comptes utilisateur

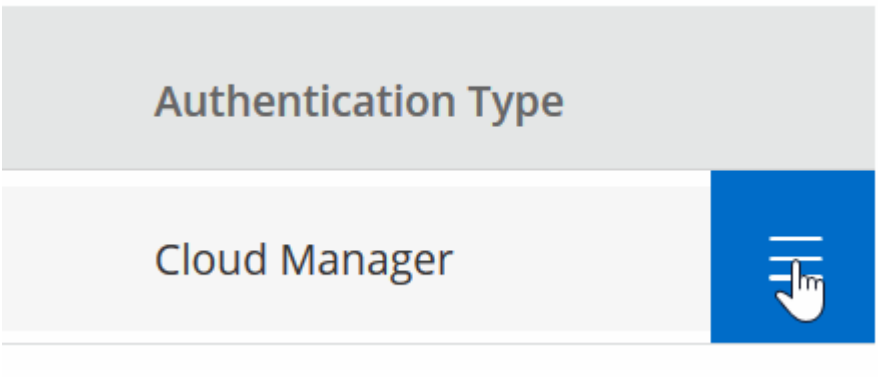
Vous pouvez modifier les comptes utilisateur dans Cloud Manager en activant et désactivant le rapport de notification.

**Description de la tâche**

Le mot de passe et les informations utilisateur doivent être modifiés dans "NetApp Cloud Central".

**Étapes**

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur l'icône utilisateur, puis sélectionnez **View Users**.
2. Sélectionnez l'icône de menu à la fin de la ligne et cliquez sur **Modifier l'utilisateur**.




3. Dans la page Paramètres utilisateur, modifiez le compte utilisateur.

# Configuration de Cloud Manager pour utiliser un serveur proxy

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

**Description de la tâche**

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

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

**Étapes**

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur la liste déroulante des tâches, puis sélectionnez **Paramètres**.
2. Sous Proxy HTTP, entrez le serveur à l’aide de la syntaxe <a href="http://<em>address:port</em>" class="bare">http://<em>address:port</em></a>, Indiquez un nom d’utilisateur et un mot de passe si une authentification de base est requise pour le serveur, puis cliquez sur <strong>Enregistrer</strong>.

   Cloud Manager ne prend pas en charge les mots de passe qui incluent le caractère @.

**Résultat**

Après avoir spécifié le serveur proxy, les nouveaux systèmes Cloud Volumes ONTAP sont automatiquement configurés pour utiliser le serveur proxy lors de l'envoi de messages AutoSupport. Si vous ne spécifiez pas le serveur proxy avant que les utilisateurs ne créent des systèmes Cloud Volumes ONTAP, ils doivent utiliser System Manager pour définir manuellement le serveur proxy dans les options AutoSupport pour chaque système.

# Renouvellement du certificat HTTPS de Cloud Manager

Vous devez renouveler le certificat HTTPS de Cloud Manager avant son expiration pour garantir un accès sécurisé à la console Web de Cloud Manager. Si vous ne renouvelez pas le certificat avant son expiration, un avertissement s'affiche lorsque les utilisateurs accèdent à la console Web via HTTPS.

**Étapes**

1. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur la liste déroulante des tâches, puis sélectionnez **HTTPS Setup**.

   Des informations détaillées sur le certificat Cloud Manager s'affichent, y compris la date d'expiration.

2. Cliquez sur **renouveler le certificat HTTPS** et suivez les étapes pour générer une RSC ou installer votre propre certificat signé par une CA.

**Résultat**

Cloud Manager utilise le nouveau certificat signé par l'autorité de certification pour fournir un accès HTTPS

sécurisé.

# Désinstallation de Cloud Manager

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

**Étapes**

1. Si vous souhaitez réinstaller Cloud Manager, sauvegardez la base de données avant de désinstaller le logiciel :
   a. Dans le coin supérieur droit de la console Cloud Manager, cliquez sur la liste déroulante des tâches, puis sélectionnez **Outils**.
   b. Cliquez sur **Backup** et enregistrez le fichier de sauvegarde sur votre ordinateur local.
2. À partir de l'hôte Linux, exécutez le script de désinstallation :

   **/opt/application/netapp/cloudmanager/bin/uninstall.sh [silencieux]**

   *silent* exécute le script sans vous demander de confirmer.

# API et automatisation

## Exemples d’automatisation pour l’infrastructure-as-code

Utilisez les ressources disponibles sur cette page pour obtenir de l’aide sur l’intégration de Cloud Manager et de Cloud Volumes ONTAP avec votre "infrastructure-as-code".

Les équipes DevOps utilisent plusieurs outils pour automatiser la configuration de nouveaux environnements et traiter l’infrastructure comme du code. Deux outils de ce type sont Ansible et Terraform. Nous avons développé des exemples Ansible et Terraform que l’équipe DevOps peut utiliser avec Cloud Manager pour automatiser et intégrer Cloud Volumes ONTAP avec l’infrastructure-as-code.

"Afficher les échantillons d’automatisation".

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

- Liens connexes*
- "Blog sur le cloud NetApp : utilisation d’API REST de Cloud Manager avec un accès fédéré"
- "Blog sur le cloud NetApp : l’automatisation du cloud avec Cloud Volumes ONTAP et REST"
- "Blog sur le cloud NetApp : clonage automatisé des données pour le test des applications logicielles basé sur le cloud"
- "Blog NetApp : IAC (Infrastructure-as-Code) accéléré avec Ansible + NetApp"
- "NetApp thePub : gestion de la configuration et automatisation avec Ansible"
- "NetApp thePub : rôles pour l’utilisation d’Ansible ONTAP"

# Référence

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

Lors de la mise à niveau vers Cloud Manager 3.5, NetApp choisira des systèmes Cloud Manager spécifiques à intégrer à NetApp Cloud Central, s'ils ne sont pas déjà intégrés. Cette FAQ peut répondre aux questions que vous pourriez avoir sur le processus.

### Qu'est-ce que NetApp Cloud Central ?

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

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

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

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

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

### Comment fonctionne l'authentification centralisée des utilisateurs ?

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

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

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

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

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

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

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

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

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

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

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

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

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

### Que se passe-t-il si mon système Cloud Manager utilise LDAP ?

Si votre système utilise LDAP, NetApp ne peut pas intégrer automatiquement le système à Cloud Central. Vous devez effectuer manuellement les opérations suivantes :

1. Déployez un nouveau système Cloud Manager à partir de "NetApp Cloud Central".
2. "Configuration d'LDAP avec le nouveau système".
3. "Découvrir les systèmes Cloud Volumes ONTAP existants" À partir du nouveau système Cloud Manager.
4. Supprimez l'ancien système Cloud Manager.

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

Non NetApp intégrera des systèmes avec Cloud Central, quel que soit leur emplacement, qu'il s'agisse d'AWS, d'Azure ou sur votre site.

La seule exception est l'environnement AWS Commercial Cloud Services.

# Règles de groupe de sécurité pour AWS

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

## Règles pour Cloud Manager

Le groupe de sécurité de Cloud Manager requiert à la fois des règles entrantes et sortantes.

#### Règles entrantes pour Cloud Manager

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

| Protocole | Port | Objectif |
|---|---|---|
| SSH | 22 | Fournit un accès SSH à l'hôte Cloud Manager |
| HTTP | 80 | Fournit un accès HTTP depuis les navigateurs Web clients vers la console Web de Cloud Manager |
| HTTPS | 443 | Fournit un accès HTTPS depuis les navigateurs Web clients vers la console Web Cloud Manager |

### Règles de sortie pour Cloud Manager

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

#### Règles de base pour les appels sortants

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

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

#### Règles de sortie avancées

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

L'adresse IP source est l'hôte Cloud Manager.

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

## Règles pour Cloud Volumes ONTAP

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

### Règles entrantes pour Cloud Volumes ONTAP

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

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

#### Règles de sortie pour Cloud Volumes ONTAP

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

#### Règles de base pour les appels sortants

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

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

#### Règles de sortie avancées

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

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

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

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

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

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

### Règles entrantes

La source des règles entrantes est 0.0.0.0/0.

| Protocole | Port | Objectif |
|---|---|---|
| SSH | 22 | Connexions SSH au médiateur haute disponibilité |
| TCP | 3000 | Accès à l'API reposant depuis Cloud Manager |

### Règles de sortie

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

#### Règles de base pour les appels sortants

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

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

#### Règles de sortie avancées

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

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

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

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

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

### Règles entrantes

Le groupe de sécurité prédéfini inclut les règles entrantes suivantes.

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

#### Règles de sortie

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

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

# Règles de groupe de sécurité pour Azure

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

## Règles pour Cloud Manager

Le groupe de sécurité de Cloud Manager requiert à la fois des règles entrantes et sortantes.

#### Règles entrantes pour Cloud Manager

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

| Protocole | Port | Objectif |
|---|---|---|
| SSH | 22 | Fournit un accès SSH à l'hôte Cloud Manager |
| HTTP | 80 | Fournit un accès HTTP depuis les navigateurs Web clients vers la console Web de Cloud Manager |
| HTTPS | 443 | Fournit un accès HTTPS depuis les navigateurs Web clients vers la console Web Cloud Manager |

#### Règles de sortie pour Cloud Manager

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

##### Règles de base pour les appels sortants

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

| Protocole | Port | Objectif |
|---|---|---|
| Tous les protocoles TCP | Tout | Tout le trafic sortant |

| Protocole | Port | Objectif |
| --- | --- | --- |
| Tous les protocoles UDP | Tout | Tout le trafic sortant |

#### Règles de sortie avancées

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

L'adresse IP source est l'hôte Cloud Manager.

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

| Service | Protocole | Port | Destination | Objectif |
|---|---|---|---|---|
| DNS | UDP | 53 | DNS | Utilisé pour la résolution DNS par Cloud Manager |

## Règles pour Cloud Volumes ONTAP

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

### Règles entrantes pour les systèmes à nœud unique

| Priorité | Nom | Port | Protocole | Source | Destination | Action | Description |
|---|---|---|---|---|---|---|---|
| 1000 | ssh_entrant | 22 | TCP | Toutes | Toutes | Autoriser | 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 | Toutes | Toutes | Autoriser | 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 | Toutes | Toutes | Autoriser | Appel de procédure à distance pour NFS |
| 1003 | inbound_111_udp | 111 | UDP | Toutes | Toutes | Autoriser | Appel de procédure à distance pour NFS |
| 1004 | entrant_139 | 139 | TCP | Toutes | Toutes | Autoriser | Session de service NetBIOS pour CIFS |
| 1005 | inbound_161-162 _tcp | 161-162 | TCP | Toutes | Toutes | Autoriser | Protocole de gestion de réseau simple |
| 1006 | inbound_161-162 _udp | 161-162 | UDP | Toutes | Toutes | Autoriser | Protocole de gestion de réseau simple |
| 1007 | entrant_443 | 443 | TCP | Toutes | Toutes | Autoriser | 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 | Toutes | Toutes | Autoriser | Microsoft SMB/CIFS sur TCP avec encadrement NetBIOS |
| 1009 | inbound_635_tcp | 658 | TCP | Toutes | Toutes | Autoriser | Montage NFS |
| 1010 | inbound_635_udp | 658 | TCP | Toutes | Toutes | Autoriser | Montage NFS |
| 1011 | entrant_749 | 749 | TCP | Toutes | Toutes | Autoriser | Kerberos |
| 1012 | inbound_2049_tcp | 2049 | TCP | Toutes | Toutes | Autoriser | Démon du serveur NFS |

| Priorité | Nom | Port | Protocole | Source | Destination | Action | Description |
|---|---|---|---|---|---|---|---|
| 1013 | inbound_2049_udp | 2049 | UDP | Toutes | Toutes | Autoriser | Démon du serveur NFS |
| 1014 | entrant_3260 | 3260 | TCP | Toutes | Toutes | Autoriser | Accès iSCSI via le LIF de données iSCSI |
| 1015 | inbound_4045-4046_tcp | 4045-4046 | TCP | Toutes | Toutes | Autoriser | Démon de verrouillage NFS et contrôle de l'état du réseau |
| 1016 | inbound_4045-4046_udp | 4045-4046 | UDP | Toutes | Toutes | Autoriser | Démon de verrouillage NFS et contrôle de l'état du réseau |
| 1017 | entrant_10000 | 10000 | TCP | Toutes | Toutes | Autoriser | Sauvegarde avec NDMP |
| 1018 | entrant_11104-11105 | 11104-11105 | TCP | Toutes | Toutes | Autoriser | Transfert de données SnapMirror |
| 3000 | inbound_deny _all_tcp | Toutes | TCP | Toutes | Toutes | Refuser | Bloquer tout autre trafic TCP entrant |
| 3001 | inbound_deny _all_udp | Toutes | UDP | Toutes | Toutes | Refuser | Bloquer tout autre trafic entrant UDP |
| 65000 | AllowVnetInBound | Toutes | Toutes | VirtualNetwork | VirtualNetwork | Autoriser | Trafic entrant depuis le réseau VNet |
| 65001 | AllowAzureLoad BalancerInBound | Toutes | Toutes | Équilibreur de charge AzureLoadBalancer | Toutes | Autoriser | Le trafic de données à partir d'Azure Standard Load Balancer |
| 65500 | DenyAllInBound | Toutes | Toutes | Toutes | Toutes | Refuser | Bloquer tout autre trafic entrant |

### Règles entrantes pour les systèmes HA

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 | Nom | Port | Protocole | Source | Destination | Action | Description |
|---|---|---|---|---|---|---|---|
| 100 | entrant_443 | 443 | Toutes | Toutes | Toutes | Autoriser | 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 | Toutes | Toutes | Toutes | Autoriser | Appel de procédure à distance pour NFS |

| Priorité | Nom | Port | Protocole | Source | Destination | Action | Description |
|---|---|---|---|---|---|---|---|
| 102 | inbound_2049_tcp | 2049 | Toutes | Toutes | Toutes | Autoriser | Démon du serveur NFS |
| 111 | ssh_entrant | 22 | Toutes | Toutes | Toutes | Autoriser | Accès SSH à l'adresse IP du LIF de gestion de cluster ou d'un LIF de gestion de nœud |
| 121 | entrant_53 | 53 | Toutes | Toutes | Toutes | Autoriser | DNS et CIFS |
| 65000 | AllowVnetInBound | Toutes | Toutes | VirtualNetwork | VirtualNetwork | Autoriser | Trafic entrant depuis le réseau VNet |
| 65001 | AllowAzureLoad BalancerInBound | Toutes | Toutes | Équilibreur de charge AzureLoadBalancer | Toutes | Autoriser | Le trafic de données à partir d'Azure Standard Load Balancer |
| 65500 | DenyAllInBound | Toutes | Toutes | Toutes | Toutes | Refuser | Bloquer tout autre trafic entrant |

### Règles de sortie pour Cloud Volumes ONTAP

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

#### Règles de base pour les appels sortants

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

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

#### Règles de sortie avancées

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

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

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

| Service | Protocole | Port | Source | Destination | Objectif |
|---|---|---|---|---|---|
| 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 |

# Autorisations AWS et Azure pour Cloud Manager

Cloud Manager requiert des autorisations pour effectuer des actions dans AWS et Azure en votre nom. Ces autorisations sont incluses dans "Règles fournies par NetApp". Vous pouvez comprendre ce que fait Cloud Manager avec ces autorisations.

## Ce que fait Cloud Manager avec les autorisations AWS

Cloud Manager utilise un compte AWS pour effectuer des appels API vers plusieurs services AWS, notamment EC2, S3, CloudFormation, IAM, Security Token Service (STS) et le service de gestion des clés (KMS).

| Actions | Objectif |
|---|---|
| "ec2:StartInstances", "ec2:StopInstances", "ec2:Décrivez les occurrences", "ec2:Ddescriptif InstanceStatus", "ec2:RunInstances", « ec2:TerminateInstances », « ec2:ModimodificationAttribute », | Lance une instance Cloud Volumes ONTAP et arrête, démarre et surveille l'instance. |

| Actions | Objectif |
| --- | --- |
| "EC2:DescribeInstanceAttribute", | Vérifie que la mise en réseau améliorée est activée pour les types d'instance pris en charge. |
| "ec2:descriptifs", "ec2:descriptifs", | Lance une configuration Cloud Volumes ONTAP HA. |
| "EC2:CreateTags", | Marque chaque ressource créée par Cloud Manager à l'aide des balises WorkingEnvironment et WorkingEnvironmentId. Cloud Manager utilise ces balises pour la maintenance et l'allocation des coûts. |
| « ec2:CreateVolume », « ec2:Describevolumes », « ec2:ModityVolumeAttribute », « ec2:AttachVolume », « ec2:DeleteVolume », « ec2:DetachVolume », | Gère les volumes EBS utilisés par Cloud Volumes ONTAP en tant que stockage back-end. |
| « ec2:CreateSecurityGroup », « ec2:DeleteSecurityGroup », « ec2:descriptif SecurityGroups », « ec2:RevokeSecurityGroupEgress », « ec2:AuthoreSecurityGroupEgress », « ec2:AuthoreSecurityGroupEgress », « ec2:AuthoreSecurityGroupIngress », « ec2:RevokeSecurityGroupIngress », | Crée des groupes de sécurité prédéfinis pour Cloud Volumes ONTAP. |
| « ec2:CreateNetworkinterface », « ec2:DescribeNetworkinterfaces », « ec2:DeleteNetworkinterface », « ec2:ModityNetworkInterfaceAttribute », | Crée et gère des interfaces réseau pour Cloud Volumes ONTAP dans le sous-réseau cible. |
| "ec2:DescribeSubnets", "ec2:DescribeVpcs", | Récupère la liste des sous-réseaux de destination et des groupes de sécurité nécessaires à la création d'un nouvel environnement de travail pour Cloud Volumes ONTAP. |
| "EC2:DescribeDhcpOptions", | Détermine les serveurs DNS et le nom de domaine par défaut lors du lancement des instances Cloud Volumes ONTAP. |
| « ec2:CreateSnapshot », « ec2:DeleteSnapshot », « ec2:Ddescriptif », | Prend des snapshots des volumes EBS lors de la configuration initiale et chaque fois qu'une instance Cloud Volumes ONTAP est arrêtée. |
| " EC2:GetConsoleOutput ", | Capture la console Cloud Volumes ONTAP, associée aux messages AutoSupport. |
| "EC2:DécribeKeyPair", | Obtient la liste des paires de clés disponibles lors du lancement d'instances. |
| "EC2:DécribeRegions", | Récupère une liste des régions AWS disponibles. |
| « ec2:DeleteTags », « ec2:Ddescriptif », | Gère les balises des ressources associées aux instances Cloud Volumes ONTAP. |
| "Cloudformation:CreateStack", "cloudformation:DeleteStack", "cloudformation:DescribeSacks", "cloudformation:DescribeStackEvents", "cloudformation:ValidateTemplate", | Lance les instances Cloud Volumes ONTAP. |

| Actions | Objectif |
| --- | --- |
| « iam:PassRole », « iam:CreateRole », « iam:DeleteRole », « iam:PutRolePolicy », « iam:CreateInstanceProfile », "iam:DeleteRolePolicy", "iam:AddRoleToInstanceProfile", "iam:RemoveRoleFromInstanceProfile", "iam:DeleteInstanceProfile", | Lance une configuration Cloud Volumes ONTAP HA. |
| « iam:ListenInstanceProfiles », « sts:DecodeAuthorationmessage », « ec2:AssociationIamInstanceProfile », « ec2:DécrideIamInstanceInstanceProfileassociations », « ec2:DisassociateIamInstanceProfile », | Gère les profils d'instance des instances Cloud Volumes ONTAP. |
| « s3:GetBuckeTagging », « s3:GetBuckeLocation », « s3:ListAllMyPets », « s3:ListBucket » | Obtenez des informations sur les compartiments AWS S3 pour que Cloud Manager puisse s'intégrer au service NetApp Data Fabric Cloud Sync. |
| « s3:CreateBucket », « s3:DeleteBucket », « s3:GetLifecyclConfiguration », « s3:PutLifecycleConfiguration », « s3:PutBuckeTagging », « s3:ListBuckeVersions », | Gère le compartiment S3 qu'un système Cloud Volumes ONTAP utilise comme niveau de capacité. |
| « Km:liste* », « km:décrire* » | Obtenez des informations sur les clés à partir du service AWS Key Management Service. |
| "ce:GetReservationUtilization", "ce:GetDimensionValues", "ce:GetCostAndUsage", "ce:GetTags" | Obtient les données de coût AWS pour Cloud Volumes ONTAP. |
| « ec2:CreatePlaceGroup », « ec2:Deleteplacer GroupeDe » | Lorsque vous déployez une configuration HA dans une seule zone de disponibilité AWS, Cloud Manager lance les deux nœuds HA et le médiateur dans un groupe de placement AWS. |

## Ce que fait Cloud Manager avec les autorisations Azure

La stratégie Cloud Manager Azure inclut les autorisations dont Cloud Manager a besoin pour déployer et gérer Cloud Volumes ONTAP dans Azure.

| Actions | Objectif |
| --- | --- |
| « Microsoft.Compute/locations/operations/read", « Microsoft.Compute/locations/vmSizes/read", « Microsoft.Compute/operations/read", « Microsoft.Compute/virtualMachines/instanceView/read", « Microsoft.Compute/virtualMachines/powerOff/action", « Microsoft.Compute/virtualMachines/read", « Microsoft.Compute/virtualMachines/restart/action", « Microsoft.Compute/virtualMachines/start/action", « Microsoft.Compute/virtualMachines/deallocate/action", « Microsoft.Compute/virtualMachines/vmSizes/read", « Microsoft.Compute/virtualMachines/write", | Crée Cloud Volumes ONTAP et arrête, démarre, supprime et obtient l'état du système. |

| Actions | Objectif |
| --- | --- |
| « Microsoft.Compute/images/write", « Microsoft.Compute/images/read", | Permet le déploiement de Cloud Volumes ONTAP à partir d'un disque VHD. |
| « Microsoft.Compute/disks/delete", « Microsoft.Compute/disks/read", « Microsoft.Compute/disks/write", Microsoft.Storage/checkkamedisponibilité/read », « Microsoft.Storage/Operations/read », « Microsoft.Storage/storageAccounts/listkeys/action », « Microsoft.Storage/storageAccounts/read », « Microsoft.Storage/storageAccounts/redynamekey/action », « Microsoft.Storage/storageAccounts/write » « Microsoft.Storage/StorageAccounts/delete », « Microsoft.Storage/eancs/read », | Gère les comptes et les disques de stockage Azure et les connecte à Cloud Volumes ONTAP. |
| « Microsoft.Network/networkInterfaces/read", « Microsoft.Network/networkInterfaces/write", « Microsoft.Network/networkInterfaces/join/action", | Crée et gère des interfaces réseau pour Cloud Volumes ONTAP dans le sous-réseau cible. |
| « Microsoft.Network/networkSecurityGroups/read", « Microsoft.Network/networkSecurityGroups/write", « Microsoft.Network/networkSecurityGroups/join/action", | Crée des groupes de sécurité réseau prédéfinis pour Cloud Volumes ONTAP. |
| « Microsoft.Resources/abonnements/emplacements/lecture », « Microsoft.Network/locations/operationResults/read", « Microsoft.Network/locations/operations/read", « Microsoft.Network/virtualNetworks/read", « Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read", » « Microsoft.Network/virtualNetworks/subnets/read", « Microsoft.Network/virtualNetworks/subnets/virtualMachines/read", « Microsoft.Network/virtualNetworks/virtualMachines/read", « Microsoft.Network/virtualNetworks/subnets/join/action", | Récupère les informations réseau sur les régions, le VNet cible et le sous-réseau, et ajoute Cloud Volumes ONTAP aux VNets. |
| « Microsoft.Network/virtualNetworks/subnets/write", « Microsoft.Network/routeTables/join/action", | Active les terminaux de service VNet pour le hiérarchisation des données. |
| « Microsoft.Resources/déploiements/opérations/lecture », « Microsoft.Resources/déploiements/lecture », « Microsoft.Resources/déploiements/écriture », | Déploie Cloud Volumes ONTAP à partir d'un modèle. |

| Actions | Objectif |
| --- | --- |
| « Microsoft.Resources/déploiements/opérations/lecture », « Microsoft.Resources/déploiements/lecture », « Microsoft.Resources/déploiements/écriture », « Microsoft.Resources/Resources/read », « Microsoft.Resources/abonnements/résultats d'opération/lecture », « Microsoft.Resources/souscriptions/resourceGroups/delete », « Microsoft.Resources/souscriptions/resourceGroups/read », « Microsoft.Resources/souscriptions/resourcesgroupe/resources/read », « Microsoft.Resources/souscriptions/resourceGroups/write », | Crée et gère des groupes de ressources pour Cloud Volumes ONTAP. |
| « Microsoft.Compute/snapshots/write", « Microsoft.Compute/snapshots/read", « Microsoft.Compute/disks/beginGetAccess/action" | Crée et gère les snapshots gérés par Azure. |
| « Microsoft.Compute/availabilitySets/write", « Microsoft.Compute/availabilitySets/read", | Crée et gère des ensembles de disponibilité pour Cloud Volumes ONTAP. |
| « Microsoft.MarketplaceOrdering/Offres/éditeurs/offres/plans/accords/lecture », « Microsoft.MarketplaceOrdering/Offres/Offres/plans/accords/write » | Permet des déploiements programmatiques depuis Azure Marketplace. |
| « Microsoft.Network/loadBalancers/read", « Microsoft.Network/loadBalancers/write", « Microsoft.Network/loadBalancers/delete", « Microsoft.Network/loadBalancers/backendAddressPools/read", « Microsoft.Network/loadBalancers/backendAddressPools/join/action", « Microsoft.Network/loadBalancers/frontendIPConfigurations/read", « Microsoft.Network/loadBalancers/loadBalancingRules/read", « Microsoft.Network/loadBalancers/probes/read", « Microsoft.Network/loadBalancers/probes/join/action", | Gère un équilibreur de charge Azure pour les paires HA. |
| " Microsoft.Authorization/locks/* " | Permet la gestion des verrous sur les disques Azure. |
| "Microsoft.Authorization/roleDefinitions/écrire", "Microsoft.Authorization/roleassignations/écrire", "Microsoft.Web/sites/*" | Gestion du basculement pour les paires haute disponibilité. |

# Configurations par défaut

Par défaut, les informations sur la configuration de Cloud Manager et de Cloud Volumes ONTAP peuvent vous aider à administrer les systèmes.

## Configuration par défaut de Cloud Manager sous Linux

Si vous devez dépanner Cloud Manager ou votre hôte Linux, il peut vous aider à comprendre comment Cloud Manager est configuré.

- Si vous avez déployé Cloud Manager depuis NetApp Cloud Central (ou directement depuis AWS Marketplace ou Azure Marketplace), notez ce qui suit :
  - Dans AWS, le nom d'utilisateur de l'instance Linux EC2 est ec2-user.
  - Pour AWS et Azure, le système d'exploitation de l'image Cloud Manager est Red Hat Enterprise Linux 7.4 (HVM).

    Le système d'exploitation n'inclut pas d'interface graphique. Vous devez utiliser un terminal pour accéder au système.
- Le dossier d'installation de Cloud Manager se trouve à l'emplacement suivant :

  /opt/application/netapp/cloudmanager
- Les fichiers journaux se trouvent dans le dossier suivant :

  /opt/application/netapp/cloudmanager/log
- Le service Cloud Manager s'appelle occm.
- Le service occm dépend du service MySQL.

  Si le service MySQL est en panne, le service occm est également en panne.
- Cloud Manager installe les packages suivants sur l'hôte Linux, s'ils ne sont pas déjà installés :
  - 7Zip
  - AWSCLI
  - Java
  - Kubectl
  - MySQL
  - Tridentctl
  - Wget

## Configuration par défaut pour Cloud Volumes ONTAP

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

- Cloud Volumes ONTAP est disponible en tant que système à un seul nœud et en tant que paire HA dans AWS et Azure.
- Cloud Manager crée une SVM de service de données lorsqu'il déploie Cloud Volumes ONTAP. Bien que vous puissiez créer un autre SVM de service de données à partir de System Manager ou de l'interface de ligne de commande, plusieurs SVM de service de données ne sont pas pris en charge.
- Plusieurs interfaces réseau sont créées par défaut :
  - Un LIF de gestion de cluster

- Un FRV intercluster
- Un LIF de gestion des nœuds
- Un LIF de données iSCSI
- Un LIF de données CIFS et NFS

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

- Cloud Volumes ONTAP envoie des sauvegardes de configuration à Cloud Manager via HTTPS.
- Lorsque vous êtes connecté à Cloud Manager, les sauvegardes sont accessibles depuis https://ipaddress/occm/offboxconfig/
- Cloud Manager définit quelques attributs de volume différemment des autres outils de gestion (System Manager ou CLI, par exemple).

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

| Attribut | Valeur définie par Cloud Manager |
|---|---|
| Mode Autosize | Grandir |
| Positionnement automatique maximum | 1 000 pour cent<br>L'administrateur Cloud Manager 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

- Un disque SSD IOPS provisionné pour les données d'initialisation de Cloud Volumes ONTAP, soit environ 45 Go et 1 250 PIOPS

- Un disque SSD à usage général pour les données root de Cloud Volumes ONTAP, qui est d'environ 140 Go
- Un instantané EBS pour chaque disque d'initialisation et disque racine

Dans une paire HA, les deux nœuds Cloud Volumes ONTAP répliquent leur disque racine sur le nœud partenaire.

**Azure**

- Un disque SSD de stockage Premium pour les données d'initialisation de Cloud Volumes ONTAP, d'environ 73 Go
- Un disque SSD de stockage Premium pour les données root de Cloud Volumes ONTAP, qui est d'environ 140 Go
- Un snapshot Azure pour chaque disque d'initialisation et disque racine

**Où résident les disques**

Cloud Manager présente le stockage d'AWS et d'Azure comme suit :

- Les données d'amorçage résident sur un disque connecté à l'instance EC2 ou à la machine virtuelle Azure.

  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.

# Rôles utilisateur

Chaque compte utilisateur Cloud Manager se voit attribuer un rôle qui définit les autorisations.

| Tâche | Administrateur de Cloud Manager | Administration des locataires | Administration de l'environnement de travail |
|---|---|---|---|
| Gérer les locataires | Oui. | Non | Non |
| Gérer les environnements de travail | Oui. | Oui, pour le locataire affecté | Oui, pour les environnements de travail attribués |
| Intégrez un environnement de travail avec Cloud Sync | Oui. | Oui. | Non |
| Afficher l'état de la réplication des données | Oui. | Oui, pour le locataire affecté | Oui, pour les environnements de travail attribués |
| Afficher la chronologie | Oui. | Oui. | Oui. |

| Tâche | Administrateur de Cloud Manager | Administration des locataires | Administration de l'environnement de travail |
|---|---|---|---|
| Créer et supprimer des comptes utilisateur | Oui. | Oui, pour le locataire affecté | Non |
| Modifier les comptes utilisateur | Oui. | Oui, pour le locataire affecté | Oui, pour leur propre compte |
| Gérer les paramètres du compte | Oui. | Non | Non |
| Configuration Kubernetes | Oui. | Non | Non |
| Passez de l'affichage du système de stockage à l'affichage du volume | Oui. | Non | Non |
| Modifier les paramètres | Oui. | Non | Non |
| Afficher et gérer le tableau de bord du support | Oui. | Non | Non |
| Sauvegardez et restaurez Cloud Manager | Oui. | Non | Non |
| Supprimez un environnement de travail | Oui. | Non | Non |
| Mettez à jour Cloud Manager | Oui. | Non | Non |
| Installez un certificat HTTPS | Oui. | Non | Non |
| Configurez Active Directory | Oui. | Non | Non |
| Activez le rapport Cloud Storage Automation Report | Oui. | Non | Non |

# Où obtenir de l'aide et trouver plus d'informations

Vous pouvez obtenir de l'aide et obtenir plus d'informations sur Cloud Manager et Cloud Volumes ONTAP grâce à diverses ressources, notamment des vidéos, des forums et un support.

- "Vidéos pour Cloud Manager et Cloud Volumes ONTAP"

  Regardez des vidéos qui vous montrent comment déployer et gérer Cloud Volumes ONTAP dans AWS et Azure et comment répliquer des données sur votre cloud hybride.

- "Stratégies pour Cloud Manager"

  Téléchargez les fichiers JSON qui incluent les autorisations dont Cloud Manager a besoin pour effectuer des actions dans AWS et Azure.

- "Guide du développeur de l'API Cloud Manager"

  Consultez un aperçu des API, des exemples d'utilisation et une référence API.

- Formation pour Cloud Volumes ONTAP
  - "Notions fondamentales de Cloud Volumes ONTAP"
  - "Cloud Volumes ONTAP : déploiement et gestion pour Azure"
- Rapports techniques
  - "Rapport technique NetApp 4383 : caractérisation des performances de Cloud Volumes ONTAP dans Amazon Web Services avec des charges de travail applicatives"
  - "Rapport technique NetApp 4671 : caractérisation des performances de Cloud Volumes ONTAP dans Azure avec les charges de travail applicatives"
- "Cloud Volumes ONTAP 9 Guide Express de préparation à la reprise après incident SVM"

  Décrit comment configurer rapidement un SVM de destination en vue de la reprise après incident.

- "Cloud Volumes ONTAP 9 SVM Disaster Recovery Express Guide"

  Décrit comment activer rapidement une SVM de destination après un incident, puis réactiver la SVM source.

- "Centre de documentation ONTAP 9"

  Accédez à la documentation produit d'ONTAP, qui peut vous aider à utiliser Cloud Volumes ONTAP.

- "Prise en charge de NetApp Cloud Volumes ONTAP"

  Accédez aux ressources de support pour obtenir de l'aide et résoudre les problèmes liés à Cloud Volumes ONTAP.

- "Communauté NetApp : services de données cloud"

  Connectez-vous avec vos pairs, posez des questions, échangez des idées, trouvez des ressources et partagez les meilleures pratiques.

- "NetApp Cloud Central"

  Trouvez des informations sur d'autres produits et solutions NetApp pour le cloud.

- "Documentation produit NetApp"

  Recherchez des instructions, des ressources et des réponses dans la documentation produit NetApp.

# Mentions légales

Les mentions légales donnent accès aux déclarations de copyright, aux marques, aux brevets, etc.

## Droits d’auteur

"https://www.netapp.com/company/legal/copyright/"

## Marques déposées

NetApp, le logo NETAPP et les marques mentionnées sur la page des marques commerciales NetApp sont des marques commerciales de NetApp, Inc. Les autres noms de sociétés et de produits peuvent être des marques commerciales de leurs propriétaires respectifs.

"https://www.netapp.com/company/legal/trademarks/"

## Brevets

Vous trouverez une liste actuelle des brevets appartenant à NetApp à l’adresse suivante :

https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf

## Politique de confidentialité

"https://www.netapp.com/company/legal/privacy-policy/"

## Source ouverte

Les fichiers de notification fournissent des informations sur les droits d’auteur et les licences de tiers utilisés dans le logiciel NetApp.

- "Avis concernant OnCommand Cloud Manager 3.6.6"
- "Avis concernant OnCommand Cloud Manager 3.6.1"
- "Avis concernant OnCommand Cloud Manager 3.6"

## Informations sur le copyright



## Informations sur les marques commerciales