



# **Réplication et protection des données**

## **Cloud Manager 3.7**

NetApp  
March 25, 2024

# Sommaire

- Réplication et protection des données . . . . . 1
  - Détection et gestion des clusters ONTAP . . . . . 1
  - Réplication des données entre les systèmes . . . . . 3
  - Sauvegarde des données dans Amazon S3 . . . . . 10
  - Synchronisation des données vers Amazon S3 . . . . . 20

# Réplication et protection des données

## Détection et gestion des clusters ONTAP

Cloud Manager peut découvrir les clusters ONTAP dans votre environnement sur site, dans une configuration de stockage privé NetApp et dans IBM Cloud. La découverte de ces clusters vous permet de répliquer facilement des données dans votre environnement cloud hybride directement à partir de Cloud Manager.

### Découverte des clusters ONTAP

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

#### Avant de commencer

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

Cloud Manager détecte les clusters ONTAP à l'aide de HTTPS. Si vous utilisez des stratégies de pare-feu personnalisées, elles doivent répondre aux exigences suivantes :

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

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

- Le cluster ONTAP doit autoriser l'accès HTTPS entrant via le port 443.

La stratégie de pare-feu " mgmt " par défaut permet l'accès HTTPS entrant à partir de toutes les adresses IP. Si vous avez modifié cette stratégie par défaut ou si vous avez créé votre propre stratégie de pare-feu, vous devez associer le protocole HTTPS à cette stratégie et activer l'accès à partir de l'hôte Cloud Manager.

#### Étapes

1. Sur la page environnements de travail, cliquez sur **découvrir** et sélectionnez **Cluster ONTAP**.
2. Sur la page **ONTAP Détails du cluster**, entrez l'adresse IP de gestion du cluster, le mot de passe du compte utilisateur admin et l'emplacement du cluster.

#### ONTAP Cluster Details

Provide a few details about your ONTAP cluster so Cloud Manager can discover it.

##### Cluster Details

Cluster management IP address

170.10.15.32

User name

admin

Password

\*\*\*\*\*

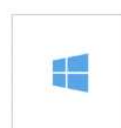
##### Cluster Location



On Premises



IBM Cloud



Microsoft  
Azure



Amazon  
Web Services



Google Cloud

3. Sur la page Détails, entrez un nom et une description pour l'environnement de travail, puis cliquez sur **Go**.

## Résultat

Cloud Manager détecte le cluster. Vous pouvez désormais créer des volumes, répliquer des données vers et depuis le cluster et lancer OnCommand System Manager pour effectuer des tâches avancées.

## Provisionnement des volumes sur des clusters ONTAP

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

### Avant de commencer

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

### Description de la tâche

Vous pouvez créer des volumes sur des agrégats existants. Vous ne pouvez pas créer de nouveaux agrégats à partir de Cloud Manager.

### Étapes

1. Sur la page Working Environments, double-cliquez sur le nom du cluster ONTAP sur lequel vous souhaitez provisionner des volumes.
2. Cliquez sur **Ajouter nouveau volume**.
3. Sur la page Créer un nouveau volume, entrez les détails du volume, puis cliquez sur **Créer**.

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

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

# Réplication des données entre les systèmes

Vous pouvez répliquer des données entre des environnements de travail en choisissant une réplication de données unique pour le transfert de données, ou un planning récurrent pour la reprise sur incident ou la conservation à long terme. Par exemple, vous pouvez configurer la réplication des données depuis un système ONTAP sur site vers Cloud Volumes ONTAP pour la reprise après incident.

Cloud Manager simplifie la réplication des données entre les volumes sur des systèmes distincts à l'aide des technologies SnapMirror et SnapVault. Il vous suffit d'identifier le volume source et le volume de destination, puis de choisir une stratégie et un planning de réplication. Cloud Manager achète les disques requis, configure les relations, applique la stratégie de réplication, puis lance le transfert de base entre les volumes.



Le transfert de base inclut une copie complète des données source. Les transferts ultérieurs contiennent des copies différentielles des données source.

## Exigences de réplication des données

Avant de pouvoir répliquer des données, vous devez confirmer que des exigences spécifiques sont respectées pour les systèmes Cloud Volumes ONTAP et les clusters ONTAP.

### Exigences de version

Vérifiez que les volumes source et de destination exécutent des versions ONTAP compatibles avant de répliquer les données. Pour plus d'informations, reportez-vous à la ["Guide d'alimentation de la protection des données"](#).

### Exigences spécifiques à Cloud Volumes ONTAP

- Le groupe de sécurité de l'instance doit inclure les règles d'entrée et de sortie requises : plus précisément, les règles d'ICMP et les ports 10000, 11104 et 11105.

Ces règles sont incluses dans le groupe de sécurité prédéfini.

- Pour répliquer des données entre deux systèmes Cloud Volumes ONTAP dans différents sous-réseaux, les sous-réseaux doivent être routés ensemble (paramètre par défaut).
- Pour répliquer des données entre un système Cloud Volumes ONTAP dans AWS et un système dans Azure, vous devez disposer d'une connexion VPN entre AWS VPC et Azure VNet.

### Exigences spécifiques aux clusters ONTAP

- Une licence SnapMirror active doit être installée.
- Si le cluster se trouve sur votre site, vous devez disposer d'une connexion entre votre réseau d'entreprise et AWS ou Azure, qui est généralement une connexion VPN.
- Les clusters ONTAP doivent répondre à des exigences supplémentaires en termes de sous-réseau, de port, de pare-feu et de cluster.

Pour plus d'informations, reportez-vous au Cluster and SVM Peering Express Guide de votre version d'ONTAP.

## Configuration de la réplication des données entre les systèmes

Vous pouvez répliquer des données entre les systèmes Cloud Volumes ONTAP et les clusters ONTAP en choisissant une réplication de données unique, qui peut vous aider à déplacer des données vers et depuis le cloud, ou un planning récurrent, qui peut vous aider à la reprise sur incident ou à la conservation à long terme.

### Description de la tâche

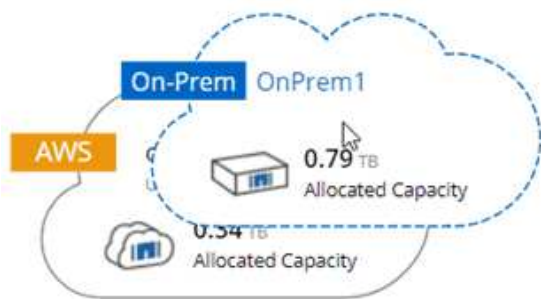
Cloud Manager prend en charge des configurations de protection des données simples, en panne et en cascade :

- Dans une configuration simple, la réplication s'effectue du volume A au volume B.
- Dans une configuration en panne, la réplication se produit du volume A vers plusieurs destinations.
- Dans une configuration en cascade, la réplication s'effectue du volume A au volume B et du volume B au volume C.

Vous pouvez configurer les configurations en cascade et en panne dans Cloud Manager en configurant plusieurs réplications de données entre les systèmes. Par exemple, en répliquant un volume du système A vers le système B, puis en répliquant le même volume du système B vers le système C.

### Étapes

1. Sur la page Working Environments (Environnements de travail), sélectionnez l'environnement de travail qui contient le volume source, puis faites-le glisser vers l'environnement de travail vers lequel vous souhaitez répliquer le volume :



2. Si les pages Configuration de la mise en valeur de la source et de la destination s'affichent, sélectionnez tous les LIF intercluster pour la relation d'homologues du cluster.

Le réseau intercluster doit être configuré de sorte que les pairs de cluster disposent d'une connectivité « full-mesh » au niveau des paires, ce qui signifie que chaque paire de clusters d'une relation cluster peer-to-peer dispose d'une connectivité parmi l'ensemble de leurs LIFs intercluster.

Ces pages s'affichent si un cluster ONTAP disposant de plusieurs LIF est la source ou la destination.

3. Sur la page Sélection du volume source, sélectionnez le volume que vous souhaitez répliquer.
4. Sur la page Nom du volume de destination et Tiering, spécifiez le nom du volume de destination, choisissez un type de disque sous-jacent, modifiez l'une des options avancées, puis cliquez sur **Continuer**.

Si la destination est un cluster ONTAP, vous devez également spécifier le SVM de destination et l'agrégat.

5. Sur la page Taux de transfert maximal, spécifiez le débit maximal (en mégaoctets par seconde) auquel les données peuvent être transférées.

6. Sur la page Stratégie de réplication, choisissez l'une des stratégies par défaut ou cliquez sur **stratégies supplémentaires**, puis sélectionnez l'une des stratégies avancées.

Pour obtenir de l'aide, voir "[Choix d'une stratégie de réplication](#)".

Si vous choisissez une stratégie de sauvegarde personnalisée (SnapVault), les étiquettes associées à la stratégie doivent correspondre aux étiquettes des copies Snapshot sur le volume source. Pour plus d'informations, voir "[Fonctionnement des stratégies de sauvegarde](#)".

7. Sur la page Programmation, choisissez une copie unique ou un planning récurrent.

Plusieurs plannings par défaut sont disponibles. Si vous souhaitez un autre planning, vous devez créer une nouvelle planification sur le cluster *destination* à l'aide de System Manager.

8. Sur la page Revue, vérifiez vos sélections, puis cliquez sur **Go**.

## Résultat

Cloud Manager démarre le processus de réplication des données. Vous pouvez afficher des informations détaillées sur la réplication dans la page Etat de la réplication.

## Gestion des planifications et des relations de réplication des données

Après avoir configuré la réplication des données entre deux systèmes, vous pouvez gérer le planning et la relation de réplication des données à partir de Cloud Manager.

### Étapes

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

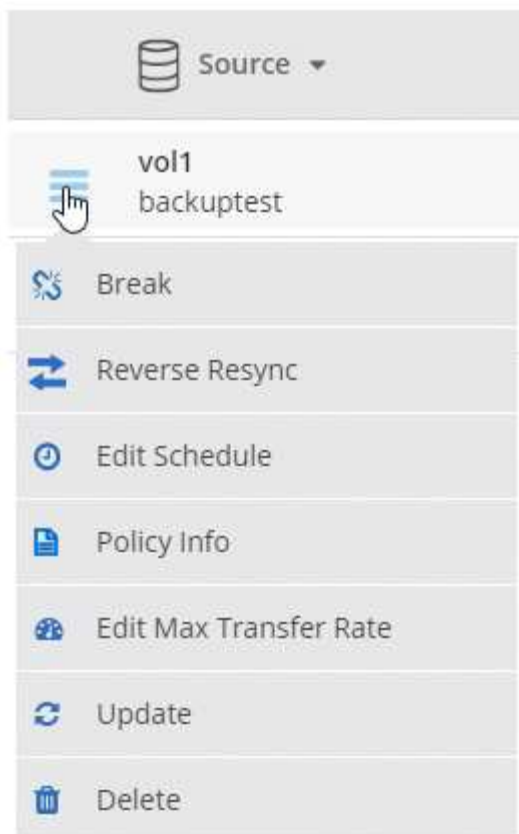
| Option  | Action   |
|---|--|
| Tous les environnements de travail de l'espace de travail | En haut de Cloud Manager, cliquez sur <b>Replication Status</b> .      |
| Un environnement de travail spécifique                    | Ouvrez l'environnement de travail et cliquez sur <b>réplications</b> . |

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                     | Romp 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 <a href="#">Guide ONTAP 9 Volume Disaster Recovery Express Guide</a> .                      |
| Resynchroniser            | <p>Rétablit une relation interrompue entre les volumes et reprend la réplication des données selon le planning défini.</p> <div>  <p>Lorsque vous resynchronisez les volumes, le contenu du volume de destination est remplacé par le contenu du volume source.</p> </div> <p>Pour effectuer une resynchronisation inverse, qui resynchronise les données du volume de destination vers le volume source, consultez la <a href="#">"Guide rapide de reprise après incident de volumes ONTAP 9"</a>.</p> |
| Resynchronisation inverse | Inverse les rôles des volumes source et de destination. Le contenu du volume source d'origine est remplacé par le contenu du volume de destination. Ceci est utile lorsque vous souhaitez réactiver un volume source hors ligne. Toutes les données écrites sur le volume source d'origine entre la dernière réplication de données et l'heure à laquelle le volume source a été désactivé ne sont pas conservées.   |



| Action                                | Description  |
|---------------------------------------|--|
| Modifier le planning                  | Vous permet de choisir un planning différent pour la réplication des données.  |
| Informations sur les règles           | Affiche la stratégie de protection attribuée à la relation de réplication des données.   |
| Modifier le taux de transfert maximal | Permet de modifier le taux maximal (en kilo-octets par seconde) auquel les données peuvent être transférées.   |
| Mise à jour                           | Lance un transfert incrémentiel pour mettre à jour le volume de destination.   |
| Supprimer                             | Supprime la relation de protection des données entre les volumes source et de destination, ce qui signifie que la réplication des données n'a plus lieu entre les volumes. Cette action n'active pas le volume de destination pour l'accès aux données. Cette action supprime également la relation d'homologues de cluster et la relation d'homologues de la machine virtuelle de stockage (SVM), si aucune autre relation de protection des données n'existe entre les systèmes. |

## Résultat

Après avoir sélectionné une action, Cloud Manager met à jour la relation ou le planning.

## Choix d'une stratégie de réplication

Vous aurez peut-être besoin d'aide pour choisir une règle de réplication lorsque vous configurez la réplication des données dans Cloud Manager. Une stratégie de réplication définit la manière dont le système de stockage réplique les données d'un volume source vers un volume de destination.

### Quelles sont les règles de réplication

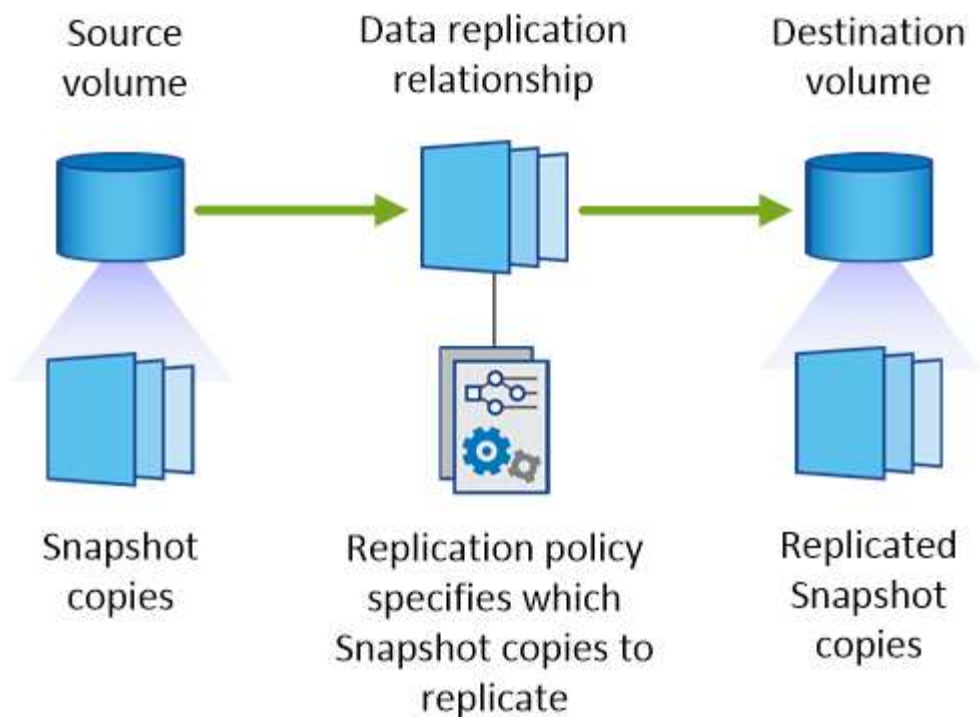
Le système d'exploitation ONTAP crée automatiquement des sauvegardes appelées copies Snapshot. Une copie Snapshot est une image en lecture seule d'un volume qui capture l'état du système de fichiers à un moment donné.

Lorsque vous répliquez des données entre des systèmes, vous répliquez des copies Snapshot d'un volume source vers un volume de destination. Une stratégie de réplication spécifie les copies Snapshot à répliquer du volume source vers le volume de destination.



Les règles de réplication sont également appelées « stratégies de protection » car elles sont optimisées par les technologies SnapMirror et SnapVault, qui assurent la protection de la reprise après incident ainsi que la sauvegarde et la restauration disque à disque.

L'image suivante montre la relation entre les copies Snapshot et les règles de réplication :



### Types de règles de réplication

Il existe trois types de règles de réplication :

- Une règle *Mirror* réplique les copies Snapshot nouvellement créées vers un volume de destination.

Vous pouvez utiliser ces copies Snapshot pour protéger le volume source en vue de la reprise après incident ou de la réplication de données unique. Vous pouvez activer le volume de destination pour l'accès aux données à tout moment.

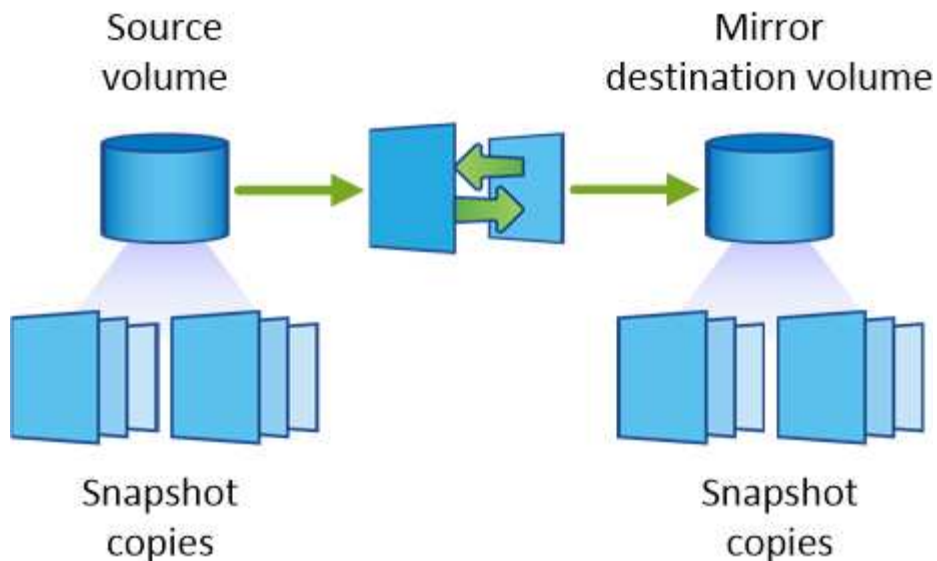
- Une règle *Backup* réplique des copies Snapshot spécifiques sur un volume de destination et les conserve généralement pendant une période plus longue que sur le volume source.

Vous pouvez restaurer des données à partir de ces copies Snapshot lorsque les données sont corrompues ou perdues, et les conserver à des fins de conformité aux normes et à d'autres fins liées à la gouvernance.

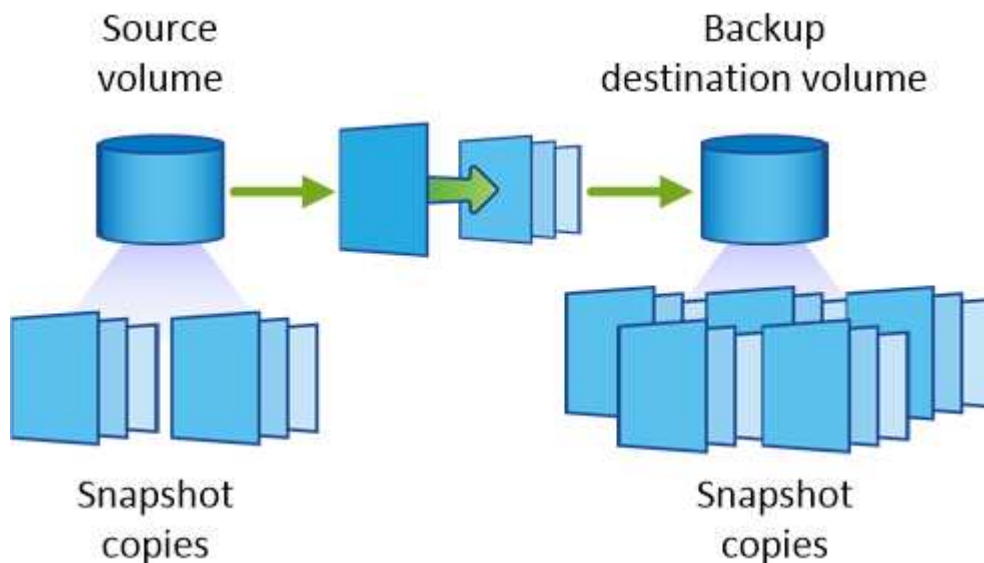
- Une politique *Mirror et Backup* permet la reprise sur incident et la conservation à long terme.

Chaque système inclut une stratégie de mise en miroir et de sauvegarde par défaut, qui fonctionne bien dans de nombreuses situations. Si vous avez besoin de règles personnalisées, vous pouvez créer vos propres règles à l'aide de System Manager.

Les images suivantes montrent la différence entre les stratégies Miroir et Sauvegarde. Une stratégie Miroir reflète les copies Snapshot disponibles sur le volume source.



Une stratégie de sauvegarde conserve généralement les copies Snapshot plus longtemps qu'elles ne sont conservées sur le volume source :



### Fonctionnement des stratégies de sauvegarde

Contrairement aux stratégies Mirror, les stratégies de sauvegarde (SnapVault) répliquent des copies Snapshot spécifiques vers un volume de destination. Il est important de comprendre le fonctionnement des stratégies de sauvegarde si vous souhaitez utiliser vos propres règles au lieu des règles par défaut.

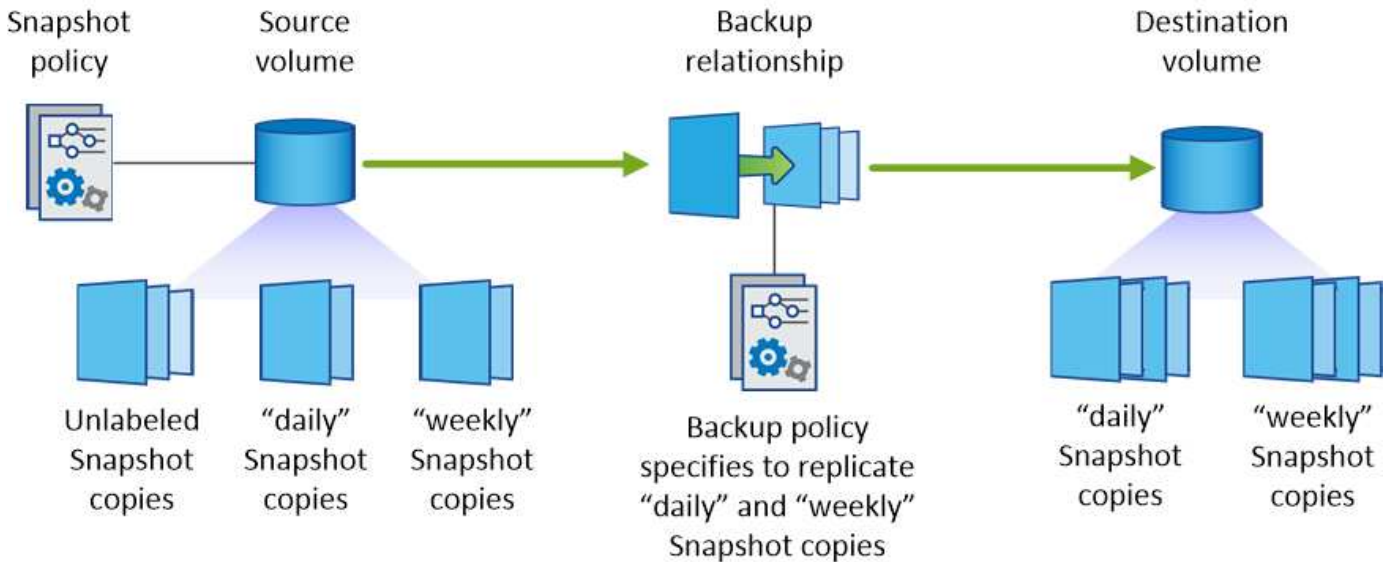
#### Comprendre la relation entre les étiquettes de copie Snapshot et les stratégies de sauvegarde

Une stratégie Snapshot définit la façon dont le système crée des copies Snapshot de volumes. La stratégie indique quand créer les copies Snapshot, le nombre de copies à conserver et comment les étiqueter. Par exemple, un système peut créer une copie Snapshot tous les jours à 12 h 10, conserver les deux copies les plus récentes et les étiqueter "quotidiennement".

Une stratégie de sauvegarde inclut des règles qui spécifient les copies Snapshot à répliquer sur un volume de destination et le nombre de copies à conserver. Les étiquettes définies dans une stratégie de sauvegarde doivent correspondre à une ou plusieurs étiquettes définies dans une stratégie Snapshot. Dans le cas

contraire, le système ne peut pas répliquer de copies Snapshot.

Par exemple, une stratégie de sauvegarde qui inclut les étiquettes " quotidiennes " et " hebdomadaires " entraîne la réplication des copies Snapshot qui n'incluent que ces étiquettes. Aucune autre copie Snapshot n'est répliquée, comme illustré dans l'image suivante :



#### Règles par défaut et règles personnalisées

La stratégie Snapshot par défaut crée des copies Snapshot toutes les heures, quotidiennes et hebdomadaires, conservant six copies Snapshot toutes les heures, deux copies quotidiennes et deux copies Snapshot hebdomadaires.

Vous pouvez facilement utiliser une stratégie de sauvegarde par défaut avec la stratégie Snapshot par défaut. Les règles de sauvegarde par défaut répliquent les copies Snapshot quotidiennes et hebdomadaires, en conservant sept copies Snapshot quotidiennes et 52 copies Snapshot hebdomadaires.

Si vous créez des règles personnalisées, les étiquettes définies par ces règles doivent correspondre. Vous pouvez créer des règles personnalisées à l'aide de System Manager.

## Sauvegarde des données dans Amazon S3

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

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

["Rendez-vous sur NetApp Cloud Central pour plus d'informations sur les tarifs".](#)

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

## Démarrage rapide

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



### Vérifiez la prise en charge de votre configuration

Vérifiez les points suivants :

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

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

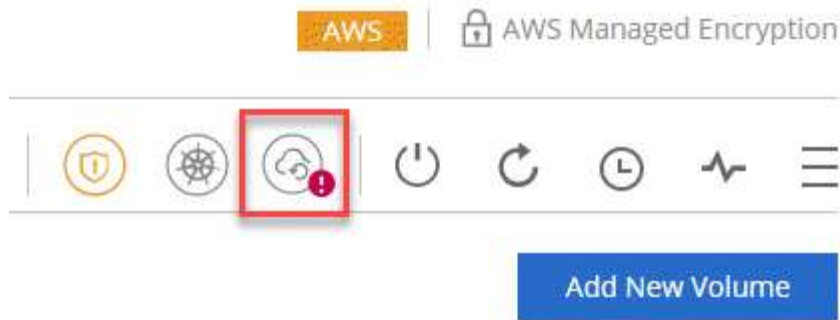
- Cloud Manager peut allouer jusqu'à deux terminaux VPC d'interface dans le VPC (la limite AWS par VPC est de 20)
- Cloud Manager est autorisé à utiliser les autorisations du terminal VPC indiquées dans les dernières versions ["Politique de Cloud Manager"](#):

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



### Activation de Backup vers S3 sur votre système nouveau ou existant

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



3

Si nécessaire, modifiez la stratégie de sauvegarde

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



Backup to S3

Backup Working Environment

☒ Automatically back up all volumes

Policy - Retention & Schedule

Backup every

Day

Number of backups to retain

30

Save

Cancel

4

Restaurez vos données à la demande

En haut de Cloud Manager, cliquez sur **Backup & Restore**, sélectionnez un volume, sélectionnez une sauvegarde, puis restaurez les données de la sauvegarde vers un nouveau volume.

vol1

Select the backup you want to restore



## De formation

Avant de commencer à sauvegarder des volumes sur S3, lisez les informations suivantes pour vous assurer que votre configuration est prise en charge.

### Versions de ONTAP prises en charge

Cloud Volume ONTAP 9.4 et versions ultérieures prennent en charge la sauvegarde vers S3.

### Régions AWS prises en charge

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

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

### Autorisations AWS requises

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

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

### Obligation d'abonnement AWS

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

### Configuration requise pour les ports

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

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

### Accès Internet sortant

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

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

## Interface des terminaux VPC

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

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

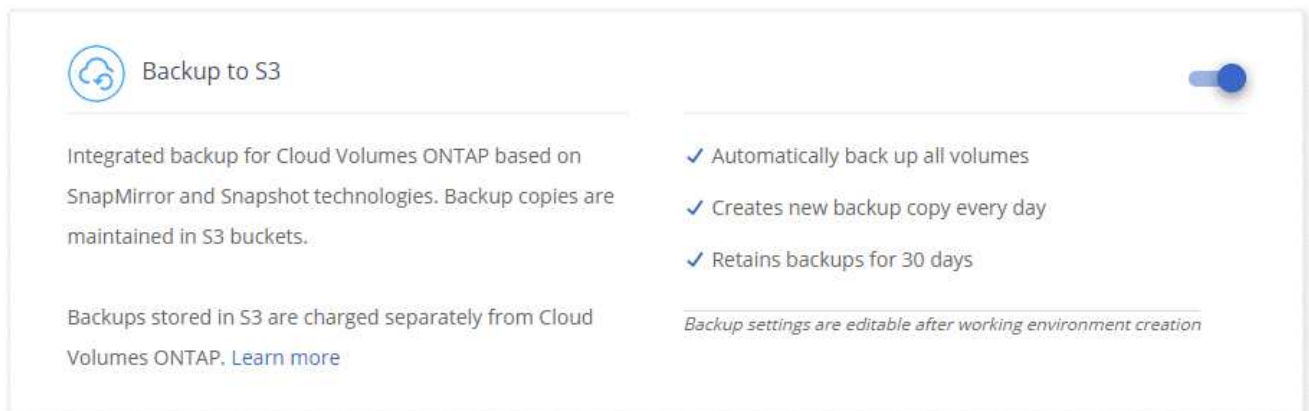
"La limite par défaut des terminaux VPC de l'interface est de 20 par VPC". Assurez-vous que votre VPC n'a pas atteint la limite avant d'activer la fonctionnalité.

## Activation des sauvegardes dans S3 sur un nouveau système

La fonctionnalité Backup to S3 est activée par défaut dans l'assistant de l'environnement de travail. Assurez-vous de conserver l'option activée.

### Étapes

1. Cliquez sur **Créer Cloud Volumes ONTAP**.
2. Sélectionnez Amazon Web Services en tant que fournisseur cloud, puis choisissez un système à un seul nœud ou haute disponibilité.
3. Remplissez la page Détails et références.
4. Sur la page sauvegarde vers S3, laissez la fonction activée et cliquez sur **Continuer**.



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

### Résultat

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

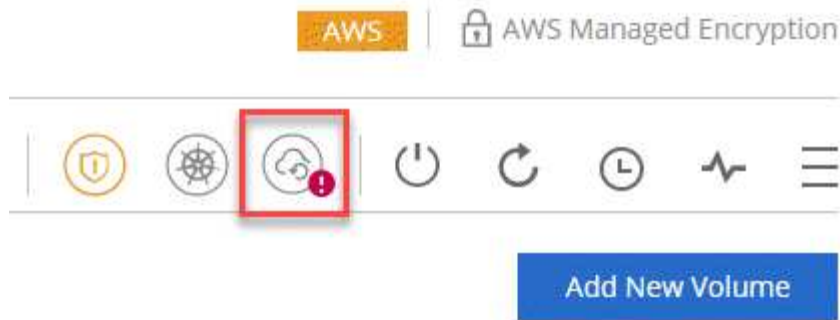
## Activation des sauvegardes dans S3 sur un système existant

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

### Étapes

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





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

#### Backup to S3

Backup Working Environment

☒ Automatically back up all volumes

Policy - Retention & Schedule

Backup every

Day

Number of backups to retain

30

Save

Cancel

#### Résultat

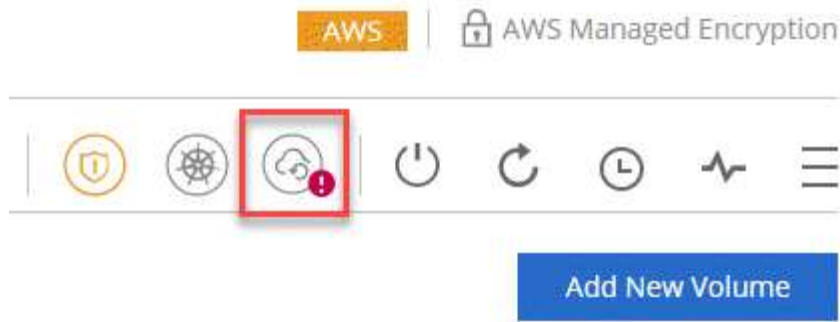
La fonctionnalité Backup vers S3 commence à effectuer les sauvegardes initiales de chaque volume.

### Modification de la conservation des sauvegardes

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

#### Étapes

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



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

Backup to S3

**Backup Working Environment** ☒ Automatically back up all volumes

---

**Policy - Retention & Schedule**

Backup every: Day Number of backups to retain: 30

Save Cancel

## Restauration d'un volume

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

### Étapes

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

| Working Environment   | Source Volume    | Last Backup                   | Policy | Retention | Relationship Status |                                  |
|-----------------------|------------------|-------------------------------|--------|-----------|---------------------|----------------------------------|
| BackupandRestore (On) | vol1 (Available) | Aug 21, 2019 05:01:34 PM U... | Daily  | 30        | Active (Idle)       | <a href="#">View Backup List</a> |

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

vol1

Select the backup you want to restore


---


Aug 21, 2019 05:01:34 PM UTC



---

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

 vol1

 **Restore Backup to a new volume**  
Aug 21, 2019 05:01:34 PM UTC

---

Select Working Environment

BackupandRestore ▾

Volume Name

vol1\_restore

**Volume Info**

Volume Size: 100 GB

Snapshot Policy: Default

NFS Protocol: Custom export policy, 172.31.0.0/16

Storage Efficiency: ON

Disk Type: GP2

Tiering: auto

---

**Restore**

Cancel

## Suppression de sauvegardes

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

### Étapes

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

vol1

Select the backup you want to restore

Aug 21, 2019 05:01:34 PM UTC



4. Confirmez la suppression de la sauvegarde.

## Désactivation des sauvegardes dans S3

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

### Étapes

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



AWS Managed Encryption



Add New Volume

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

## Fonctionnement de Backup vers S3

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

## L'emplacement des sauvegardes

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

## Les sauvegardes sont incrémentielles

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

## Les sauvegardes sont effectuées à minuit

Les sauvegardes quotidiennes commencent juste après minuit chaque jour. Pour l'instant, vous ne pouvez pas planifier les opérations de sauvegarde à un moment donné par l'utilisateur.

## Les copies de sauvegarde sont associées à votre compte Cloud Central

Les copies de sauvegarde sont associées à l' "[Compte Cloud Central](#)" Où réside Cloud Manager.

Si plusieurs systèmes Cloud Manager se trouvent dans le même compte Cloud Central, chaque système Cloud Manager affiche la même liste de sauvegardes. Cela inclut les sauvegardes associées aux instances Cloud Volumes ONTAP d'autres systèmes Cloud Manager.

## La stratégie de sauvegarde est à l'échelle du système

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

## Sécurité

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

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

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

## Limites

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

dans S3.

Par exemple, si vous créez un volume depuis l'interface de ligne de commandes ONTAP, l'API ONTAP ou System Manager, le volume ne sera pas automatiquement sauvegardé.

Si vous souhaitez sauvegarder ces volumes, désactivez Backup sur S3, puis activez-les à nouveau.

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

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

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

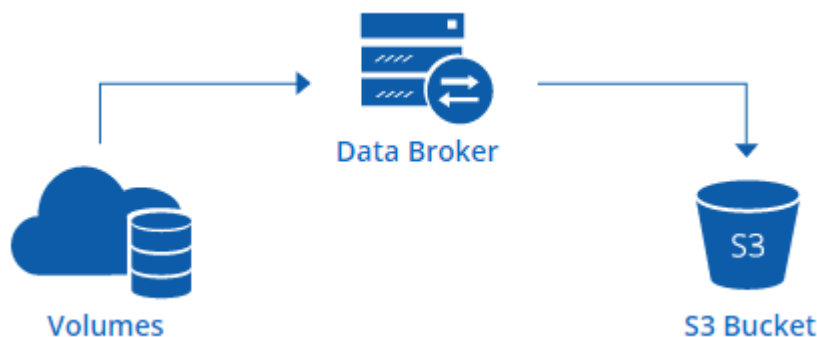
## Synchronisation des données vers Amazon S3

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

### Fonctionnement de la fonction de synchronisation vers S3

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

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



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

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

## Essai gratuit de 14 jours

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

## Comment obtenir de l'aide

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

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

## Intégration d'un environnement de travail au service Cloud Sync

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

 | [https://img.youtube.com/vi/3hOtLs70\\_xE/maxresdefault.jpg](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.

## Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

**LÉGENDE DE RESTRICTION DES DROITS :** L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

## Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.