



Mise en miroir et protection des sauvegardes sur le cluster local

ONTAP 9

NetApp
March 24, 2023

Table des matières

- Mise en miroir et protection des sauvegardes sur le cluster local 1
 - Création d'une relation de miroir pour un nouveau compartiment (cluster local) 1
 - Création d'une relation de miroir pour un compartiment existant (cluster local) 4
 - Basculement et accès aux données depuis le compartiment de destination (cluster local) 7
 - Restauration d'un compartiment à partir de la machine virtuelle de stockage de destination (cluster distant) 8

Mise en miroir et protection des sauvegardes sur le cluster local




Création d'une relation de miroir pour un nouveau compartiment (cluster local)


Lorsque vous créez de nouveaux compartiments S3, vous pouvez les protéger immédiatement vers une destination SnapMirror S3 sur le même cluster. Il est possible de mettre en miroir les données sur un compartiment de machines virtuelles de stockage différentes ou sur la même machine virtuelle de stockage que la source.

Ce dont vous avez besoin

- Les exigences relatives aux versions ONTAP, aux licences et à la configuration des serveurs S3 sont terminées.
- Une relation de peering existe entre les machines virtuelles de stockage source et de destination.
- Des certificats CA sont nécessaires pour les machines virtuelles source et cible. Vous pouvez utiliser des certificats d'autorité de certification auto-signés ou des certificats signés par un fournisseur d'autorité de certification externe.

Procédure de System Manager

1. S'il s'agit de la première relation SnapMirror S3 pour cette machine virtuelle de stockage, vérifiez qu'il existe des clés utilisateur root pour les machines virtuelles de stockage source et cible, puis régénérez-les si ce n'est pas le cas :
 - a. Cliquez sur **Storage > Storage VM**, puis sélectionnez la VM de stockage.
 - b. Dans l'onglet **Paramètres**, cliquez sur  Dans la mosaïque S3.
 - c. Dans l'onglet **Users**, vérifiez qu'il y a une clé d'accès pour l'utilisateur root
 - d. Si ce n'est pas le cas, cliquez sur  En regard de **root**, puis cliquez sur **régénérer clé**. Ne pas régénérer la clé si elle existe déjà.
2. Modifiez la machine virtuelle de stockage pour ajouter des utilisateurs et, pour ajouter des utilisateurs aux groupes, dans les machines virtuelles de stockage source et de destination : cliquez sur **stockage > VM de stockage**, cliquez sur la VM de stockage, cliquez sur **Paramètres**, puis sur  Sous S3.

Voir "[Ajoutez des utilisateurs et des groupes S3](#)" pour en savoir plus.
3. Créez une règle SnapMirror S3 si vous ne disposez pas d'une règle existante et que vous ne souhaitez pas utiliser la règle par défaut :
 - a. Cliquez sur **protection > vue d'ensemble**, puis sur **Paramètres de stratégie locale**.
 - b. Cliquez sur  En regard de **protection Politiques**, puis cliquez sur **Ajouter**.
 - Entrez le nom et la description de la stratégie.
 - Sélectionner la « policy scope », le cluster ou le SVM
 - Sélectionnez **Continuous** pour les relations SnapMirror S3.
 - Saisissez les valeurs **accélérateur** et **objectif de point de récupération**.
4. Création d'un compartiment avec la protection SnapMirror :

- a. Cliquez sur **stockage > compartiments**, puis sur **Ajouter**.
- b. Entrez un nom, sélectionnez la VM de stockage, entrez une taille, puis cliquez sur **plus d'options**.
- c. Sous **permissions**, cliquez sur **Ajouter**. La vérification des autorisations est facultative mais recommandée.
 - **Principal et effet** - sélectionnez les valeurs correspondant aux paramètres de votre groupe d'utilisateurs ou acceptez les valeurs par défaut.
 - **Actions** - Assurez-vous que les valeurs suivantes sont affichées : `GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts`
 - **Ressources** - utilisez les valeurs par défaut (`bucketname, bucketname/*`) ou d'autres valeurs dont vous avez besoin

Voir "[Gérer l'accès des utilisateurs aux compartiments](#)" pour plus d'informations sur ces champs.

- d. Sous **protection**, cochez **Activer SnapMirror (ONTAP ou Cloud)**. Saisissez ensuite les valeurs suivantes :
 - Destination
 - **CIBLE** : système ONTAP
 - **CLUSTER** : sélectionnez le cluster distant.
 - **VM DE STOCKAGE** : sélectionnez une VM de stockage sur le cluster distant.
 - **CERTIFICAT d'autorité de certification DU SERVEUR S3** : copiez et collez le contenu du certificat source.
 - Source
 - **CERTIFICAT d'autorité de certification DU SERVEUR S3** : copiez et collez le contenu du certificat de destination.

Cochez **utilisez le même certificat sur la destination** si vous utilisez un certificat signé par un fournisseur de CA externe.

Si vous cliquez sur **Paramètres de destination**, vous pouvez également saisir vos propres valeurs à la place des valeurs par défaut pour le nom de compartiment, la capacité et le niveau de service de performances.

Lorsque vous cliquez sur **Enregistrer**, un nouveau compartiment est créé dans la machine virtuelle de stockage source et est mis en miroir dans un nouveau compartiment qui est créé la machine virtuelle de stockage de destination.

Procédure CLI

1. Si il s'agit de la première relation SnapMirror S3 pour ce SVM, vérifiez que des clés utilisateur root existent pour les SVM source et de destination, puis régénèrent-les s'ils ne :

```
vserver object-store-server user show
```

Vérifiez qu'il existe une clé d'accès pour l'utilisateur root. Si ce n'est pas le cas, entrez :

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

Ne pas régénérer la clé si elle existe déjà.

2. Création de compartiments dans les SVM source et destination :

```
vserver object-store-server bucket create -vserver svm_name -bucket
bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]
[additional_options]
```

3. Ajout de règles d'accès aux règles de compartiment par défaut dans les SVM source et destination :

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid text]
[-index integer]
```

```
src_cluster::> vserver object-store-server bucket policy add-statement
-bucket test-bucket -effect allow -action
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li
stBucketMultipartUploads,ListMultipartUploadParts -principal - -resource
test-bucket, test-bucket /*
```

4. Créez une règle SnapMirror S3 si vous ne disposez pas d'une règle existante et que vous ne souhaitez pas utiliser la règle par défaut :

```
snapmirror policy create -vserver svm_name -policy policy_name -type
continuous [-rpo integer] [-throttle throttle_type] [-comment text]
[additional_options]
```

Paramètres :

- `continuous` – Le seul type de règle pour les relations SnapMirror S3 (obligatoire).
- `-rpo` – indique le temps de l'objectif de point de récupération, en secondes (facultatif).
- `-throttle` – spécifie la limite supérieure sur le débit/bande passante, en kilo-octets/seconde (facultatif).

Exemple

```
src_cluster::> snapmirror policy create -vserver vs0 -type continuous
-rpo 0 -policy test-policy
```

5. Installer les certificats de serveur CA sur le SVM admin :

a. Installez le certificat CA qui a signé le certificat du serveur *source* S3 sur le SVM admin :

```
security certificate install -type server-ca -vserver admin_svm -cert-name
src_server_certificate
```

b. Installez le certificat CA qui a signé le certificat du serveur *destination* S3 sur le SVM admin :

```
security certificate install -type server-ca -vserver admin_svm -cert-name
dest_server_certificate+ si vous utilisez un certificat signé par un fournisseur d'autorité de
certification externe, vous n'avez qu'à installer ce certificat sur la SVM d'administration.
```

Voir la `security certificate install` page de manuel pour plus de détails.

6. Création d'une relation SnapMirror S3 :

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination
```

```
-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy policy_name]`
```

Vous pouvez utiliser une stratégie que vous avez créée ou accepter la règle par défaut.

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-  
bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror -policy  
test-policy
```

7. Vérifiez que la mise en miroir est active :

```
snapmirror show -policy-type continuous -fields status
```




Création d'une relation de miroir pour un compartiment existant (cluster local)

Vous pouvez commencer à protéger à tout moment les compartiments S3 existants sur le même cluster. Par exemple, si vous mettez à niveau une configuration S3 à partir d'une version antérieure à ONTAP 9.10.1. Il est possible de mettre en miroir les données sur un compartiment de machines virtuelles de stockage différentes ou sur la même machine virtuelle de stockage que la source.

Ce dont vous aurez besoin


- Les exigences relatives aux versions ONTAP, aux licences et à la configuration des serveurs S3 sont terminées.
- Une relation de peering existe entre les machines virtuelles de stockage source et de destination.
- Des certificats CA sont nécessaires pour les machines virtuelles source et cible. Vous pouvez utiliser des certificats d'autorité de certification auto-signés ou des certificats signés par un fournisseur d'autorité de certification externe.

Procédure de System Manager

1. S'il s'agit de la première relation SnapMirror S3 pour cette machine virtuelle de stockage, vérifiez qu'il existe des clés utilisateur root pour les machines virtuelles de stockage source et cible, puis régénérez-les si ce n'est pas le cas :
 - a. Cliquez sur **Storage > Storage VM**, puis sélectionnez la VM de stockage.
 - b. Dans l'onglet **Paramètres**, cliquez sur  Dans la mosaïque **S3**.
 - c. Dans l'onglet **Users**, vérifiez qu'il y a une clé d'accès pour l'utilisateur root.
 - d. Si ce n'est pas le cas, cliquez sur  En regard de **root**, puis cliquez sur **régénérer clé**. Ne pas régénérer la clé si elle existe déjà
2. Vérifiez que l'accès des utilisateurs et des groupes est correct dans les VM de stockage source et de destination :
 - Cliquez sur **stockage > machines virtuelles de stockage**, cliquez sur la machine virtuelle de stockage, puis sur **Paramètres** et enfin sur  Sous S3.

Voir "[Ajoutez des utilisateurs et des groupes S3](#)" pour en savoir plus.
3. Créez une règle SnapMirror S3 si vous ne disposez pas d'une règle existante et que vous ne souhaitez

pas utiliser la règle par défaut :

- a. Cliquez sur **protection > vue d'ensemble**, puis sur **Paramètres de stratégie locale**.
 - b. Cliquez sur → En regard de **protection Politcies**, puis cliquez sur **Ajouter**.
 - Entrez le nom et la description de la stratégie.
 - Sélectionner la « policy scope », le cluster ou le SVM
 - Sélectionnez **Continuous** pour les relations SnapMirror S3.
 - Saisissez les valeurs **accélérateur** et **objectif de point de récupération**.
4. Vérifiez que la politique d'accès au compartiment du compartiment existant répond toujours à vos besoins :
- a. Cliquez sur **stockage > godets**, puis sélectionnez le compartiment à protéger.
 - b. Dans l'onglet **permissions**, cliquez sur  **Modifier**, puis cliquez sur **Ajouter** sous **autorisations**.
 - **Principal et effet** - sélectionnez les valeurs correspondant aux paramètres de votre groupe d'utilisateurs ou acceptez les valeurs par défaut.
 - **Actions** - Assurez-vous que les valeurs suivantes sont affichées : `GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts`
 - **Ressources** - utilisez les valeurs par défaut (`bucketname, bucketname/*`) ou d'autres valeurs dont vous avez besoin.

Voir "[Gérer l'accès des utilisateurs aux compartiments](#)" pour plus d'informations sur ces champs.

5. Protection d'un compartiment existant avec SnapMirror S3 :

- a. Cliquez sur **stockage > godets**, puis sélectionnez le compartiment à protéger.
- b. Cliquez sur **Protect** et saisissez les valeurs suivantes :
 - Destination
 - **CIBLE** : système ONTAP
 - **CLUSTER** : sélectionnez le cluster local.
 - **VM DE STOCKAGE** : sélectionnez la même machine virtuelle de stockage ou une autre.
 - **CERTIFICAT d'autorité de certification DU SERVEUR S3** : copiez et collez le contenu du certificat *source*.
 - Source
 - **CERTIFICAT d'autorité de certification DU SERVEUR S3** : copiez et collez le contenu du certificat *destination*.

Cochez **utilisez le même certificat sur la destination** si vous utilisez un certificat signé par un fournisseur de CA externe.

Si vous cliquez sur **Paramètres de destination**, vous pouvez également saisir vos propres valeurs à la place des valeurs par défaut pour le nom de compartiment, la capacité et le niveau de service de performances.

Lorsque vous cliquez sur **Enregistrer**, le compartiment existant est mis en miroir vers un nouveau compartiment dans la machine virtuelle de stockage de destination.

Procédure CLI

1. Si il s'agit de la première relation SnapMirror S3 pour ce SVM, vérifiez que des clés utilisateur root existent pour les SVM source et de destination, puis régénèrent-les s'ils ne :

```
vserver object-store-server user show
```

Vérifiez qu'il existe une clé d'accès pour l'utilisateur root. Si ce n'est pas le cas, entrez :

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root
```

Ne pas régénérer la clé si elle existe déjà.

2. Créer un compartiment sur le SVM de destination pour être la cible du miroir :

```
vserver object-store-server bucket create -vserver svm_name -bucket  
dest_bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text]  
[additional_options]
```

3. Vérifier que les règles d'accès aux règles de compartiment par défaut sont correctes dans les SVM source et destination :

```
vserver object-store-server bucket policy add-statement -vserver svm_name  
-bucket bucket_name -effect {allow|deny} -action object_store_actions  
-principal user_and_group_names -resource object_store_resources [-sid text]  
[-index integer]
```

Exemple

```
clusterA::> vserver object-store-server bucket policy add-statement  
-bucket test-bucket -effect allow -action  
GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,Li  
stBucketMultipartUploads,ListMultipartUploadParts -principal - -resource  
test-bucket, test-bucket /*
```

4. Créez une règle SnapMirror S3 si vous ne disposez pas d'une règle existante et que vous ne souhaitez pas utiliser la règle par défaut :

```
snapmirror policy create -vserver svm_name -policy policy_name -type  
continuous [-rpo integer] [-throttle throttle_type] [-comment text]  
[additional_options]
```

Paramètres :

- *continuous* – Le seul type de règle pour les relations SnapMirror S3 (obligatoire).
- *-rpo* – indique le temps de l'objectif de point de récupération, en secondes (facultatif).
- *-throttle* – spécifie la limite supérieure sur le débit/bande passante, en kilo-octets/seconde (facultatif).

Exemple

```
clusterA::> snapmirror policy create -vserver vs0 -type continuous
-rpo 0 -policy test-policy
```

5. Installer les certificats de serveur CA sur le SVM admin :

- a. Installez le certificat CA qui a signé le certificat du serveur *source* S3 sur le SVM admin :

```
security certificate install -type server-ca -vserver admin_svm -cert-name
src_server_certificate
```

- b. Installez le certificat CA qui a signé le certificat du serveur *destination* S3 sur le SVM admin :

```
security certificate install -type server-ca -vserver admin_svm -cert-name
dest_server_certificate+ si vous utilisez un certificat signé par un fournisseur d'autorité de
certification externe, vous n'avez qu'à installer ce certificat sur la SVM d'administration.
```

Voir la `security certificate install` page de manuel pour plus de détails.

6. Création d'une relation SnapMirror S3 :

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination
-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy policy_name]
```

Vous pouvez utiliser une stratégie que vous avez créée ou accepter la règle par défaut.

Exemple

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy
test-policy
```

7. Vérifiez que la mise en miroir est active :

```
snapmirror show -policy-type continuous -fields status
```

Basculement et accès aux données depuis le compartiment de destination (cluster local)

Si les données d'un compartiment source ne sont plus disponibles, vous pouvez interrompre la relation SnapMirror pour rendre le compartiment de destination inscriptible et commencer à transférer les données.

Description de la tâche


Lorsqu'une opération de basculement est effectuée, le compartiment source est converti en lecture seule et le compartiment de destination d'origine en lecture/écriture, ce qui inverse la relation SnapMirror S3.

Lorsque le compartiment source désactivé est de nouveau disponible, SnapMirror S3 resynchronise automatiquement le contenu des deux compartiments. Vous n'avez pas besoin de resynchroniser explicitement la relation, comme cela est requis pour les déploiements de SnapMirror volume standard.

Si le compartiment de destination se trouve sur un cluster distant, l'opération de basculement doit être démarrée à partir du cluster distant.

Procédure de System Manager

Le basculement depuis le compartiment non disponible et début du service des données :

1. Cliquez sur **protection > relations**, puis sélectionnez **SnapMirror S3**.
2. Cliquez sur , Sélectionnez **basculement**, puis cliquez sur **basculement**.

Procédure CLI

1. Lancer une opération de basculement pour le compartiment de destination :
`snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. Vérifier l'état de l'opération de basculement :
`snapmirror show -fields status`

Exemple

```
clusterA::> snapmirror failover start -destination-path vs1:/bucket/test-bucket-mirror
```

Restauration d'un compartiment à partir de la machine virtuelle de stockage de destination (cluster distant)

En cas de perte ou de corruption des données dans un compartiment source, vous reremplissez vos données en les restaurant à partir d'un compartiment de destination.

Description de la tâche


Ce compartiment de destination peut être restauré vers un compartiment existant ou vers un nouveau compartiment. Le compartiment cible pour l'opération de restauration doit être supérieur à l'espace logique utilisé du compartiment de destination.

Si vous utilisez un compartiment existant, celui-ci doit être vide au démarrage d'une opération de restauration. La restauration ne « restaure » pas un compartiment à la fois ; le contenu du compartiment est alors vide.

L'opération de restauration doit être démarrée à partir du cluster distant.

Procédure de System Manager

Restaurer les données de sauvegarde :

1. Cliquez sur **protection > relations**, puis sélectionnez le compartiment.
2. Cliquez sur  Puis sélectionnez **Restaurer**.
3. Sous **Source**, sélectionnez **Pot existant** (valeur par défaut) ou **Nouveau godet**.
 - Pour restaurer un **compartiment existant** (valeur par défaut), procédez comme suit :
 - Sélectionnez le cluster et la VM de stockage pour rechercher le compartiment existant.
 - Sélectionner le godet existant.
4. Copiez et collez le contenu du certificat AC du serveur S3 de destination.
 - Pour restaurer un **Nouveau godet**, entrez les valeurs suivantes :
 - Machine virtuelle de cluster et de stockage pour héberger le nouveau compartiment.

- Le nouveau compartiment : niveau de service du nom, de la capacité et des performances. Voir ["Niveaux de services de stockage"](#) pour en savoir plus.
 - Contenu du certificat d'autorité de certification du serveur S3 de destination.
5. Sous **destination**, copiez et collez le contenu du certificat d'autorité de certification du serveur S3 source.
 6. Cliquez sur **protection** > relations pour contrôler la progression de la restauration.

Procédure CLI

1. Si vous effectuez une restauration vers un nouveau compartiment, créez-le. Pour plus d'informations, voir ["Création d'une relation de sauvegarde pour un nouveau compartiment \(cible cloud\)"](#).
2. Lancer une opération de restauration pour le compartiment de destination :
`snapmirror restore -source-path svm_name:/bucket/bucket_name -destination-path svm_name:/bucket/bucket_name`

Exemple

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket  
-destination-path vs1:/bucket/test-bucket-mirror
```

Informations sur le copyright

Copyright © 2023 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.