Protection des compartiments avec SnapMirror S3

ONTAP 9

NetApp
March 24, 2023

Table des matières

Protection des compartiments avec SnapMirror S3

Présentation de SnapMirror S3

À partir de ONTAP 9.10.1, vous pouvez protéger les compartiments dans les magasins d'objets ONTAP S3 à l'aide de la fonctionnalité familière de mise en miroir et de sauvegarde de SnapMirror. En outre, contrairement à SnapMirror standard, SnapMirror S3 peut avoir des destinations non NetApp.

S3 SnapMirror prend en charge les miroirs actifs et les tiers de sauvegarde à partir de compartiments ONTAP S3 vers les destinations suivantes :

Cible	Prend en charge les miroirs actifs et le basculement ?	Prend en charge la sauvegarde et la restauration ?
ONTAP S3 • Compartiments dans le même SVM • Compartiments dans différents SVM sur le même cluster • Compartiments dans les SVM sur différents clusters	✔	✔
StorageGRID		✔
AWS S3		✔
Cloud Volumes ONTAP pour Azure		✔

Vous pouvez protéger les compartiments existants sur les serveurs ONTAP S3 ou créer immédiatement des compartiments avec la protection des données activée.

SnapMirror S3 prend en charge les relations « fan-out » et les relations en cascade. Pour une vue d'ensemble, voir "Déploiements de la protection des données en cascade et « Fan-Out »".

Exigences relatives à SnapMirror S3

- ONTAP version ONTAP 9.10.1 ou ultérieure doit exécuter des clusters source et de destination.
- Une licence est requise pour les systèmes ONTAP source et de destination.
  - Bundle principal pour le protocole et le stockage ONTAP S3
  - Bundle de protection des données pour SnapMirror S3 pour cibler d'autres cibles de magasin d'objets NetApp (ONTAP S3, StorageGRID et Cloud Volumes ONTAP).
  - Bundle de protection des données et bundle de cloud hybride pour SnapMirror S3 pour cibler les magasins d'objets tiers (AWS S3).
- ONTAP S3
  - Les serveurs ONTAP S3 doivent exécuter les SVM source et destination.

    - Il est recommandé, mais pas nécessaire, que des certificats CA pour l'accès TLS soient installés sur des systèmes hébergeant des serveurs S3.
        - Les certificats CA utilisés pour signer les certificats des serveurs S3 doivent être installés sur la VM de stockage admin des clusters hébergeant des serveurs S3.
        - Vous pouvez utiliser un certificat d'autorité de certification auto-signé ou un certificat signé par un fournisseur d'autorité de certification externe.
        - Si les VM de stockage source ou cible ne sont pas à l'écoute via HTTPS, il n'est pas nécessaire d'installer des certificats CA.
- Peering (pour les cibles ONTAP S3)
    - Les LIFs intercluster doivent être configurées (pour les cibles ONTAP distantes).
    - Les clusters source et de destination sont associés (pour les cibles ONTAP distantes).
    - Les machines virtuelles de stockage source et de destination sont peering (pour toutes les cibles ONTAP).
- Règle SnapMirror
    - Une règle SnapMirror spécifique au S3 est requise pour toutes les relations SnapMirror S3, mais vous pouvez utiliser la même règle pour plusieurs relations.
    - Vous pouvez créer votre propre stratégie ou accepter la stratégie par défaut **continu**, qui comprend les valeurs suivantes :
        - Accélérateur (limite supérieure sur le débit/bande passante) - illimité.
        - Délai pour l'objectif de point de restauration : 1 heure (3600 secondes).
- Clés utilisateur root les clés d'accès utilisateur root de la machine virtuelle de stockage sont requises pour les relations SnapMirror S3. ONTAP ne les attribue pas par défaut. Lors de la première création d'une relation SnapMirror S3, vous devez vérifier que les clés existent sur les machines virtuelles de stockage source et de destination, puis les régénérer si ce n'est pas le cas. Si vous devez les régénérer, vous devez vous assurer que tous les clients et toutes les configurations du magasin d'objets SnapMirror utilisant la paire de clés Access et secret sont mis à jour avec les nouvelles clés.

Pour plus d'informations sur la configuration d'un serveur S3, consultez les rubriques suivantes :

- "Activez un serveur S3 sur une machine virtuelle de stockage"
- "À propos du processus de configuration S3"

Pour plus d'informations sur le cluster et le peering de machine virtuelle de stockage, consultez la rubrique suivante :

- "Préparation à la mise en miroir et à l'archivage (System Manager, étapes 1 à 6)"
- "Cluster et SVM peering (interface de ligne de commandes)"

Considérations et restrictions de S3 SnapMirror

Lorsque vous créez de nouveaux compartiments, vous pouvez contrôler l'accès en créant des utilisateurs et des groupes. Pour plus d'informations, consultez les rubriques suivantes :

- "Ajout d'utilisateurs et de groupes S3 (System Manager)"
- "Création d'un utilisateur S3 (interface de ligne de commandes)"
- "Création ou modification de groupes S3 (interface de ligne de commandes)"

La fonctionnalité SnapMirror standard suivante n'est pas prise en charge dans la version actuelle de SnapMirror S3 :

- Déploiements « Fan-In » (relations de protection des données entre plusieurs compartiments source et un compartiment de destination unique)

  SnapMirror S3 peut prendre en charge plusieurs miroirs de compartiments depuis plusieurs clusters jusqu'à un seul cluster secondaire, mais chaque compartiment source doit disposer de son propre compartiment de destination sur le cluster secondaire.

Protection en miroir et sauvegarde sur un cluster distant

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

Lorsque vous créez de nouveaux compartiments S3, vous pouvez les protéger immédiatement vers une destination SnapMirror S3 sur un cluster distant.

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 clusters source et destination, et une relation de peering existe entre les machines virtuelles de stockage source et 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.

Description de la tâche

Vous devez effectuer des tâches sur les systèmes source et de destination.

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 ajoutez des utilisateurs à des groupes, sur les machines virtuelles de stockage source et cible :

   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. Sur le cluster source, créez une règle SnapMirror S3 si vous ne en possédez pas déjà une 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 Policies**, 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**. La vérification des autorisations est facultative mais recommandée.

b. Entrez un nom, sélectionnez la VM de stockage, entrez une taille, puis cliquez sur **plus d'options**.

c. Sous **permissions**, cliquez sur **Ajouter**.

- **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 CA 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**, 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]
```

Exemple

```
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. Sur la SVM source, créez une règle SnapMirror S3 si vous ne en possédez pas déjà une 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 :

- type `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/secondes (facultatif).

Exemple

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

5. Installez les certificats de serveur CA sur les SVM admin des clusters source et destination :

a. Sur le cluster source, installez le certificat de l'autorité de certification qui a signé le certificat du serveur

destination S3 :
`security certificate install -type server-ca -vserver src_admin_svm -cert -name dest_server_certificate`

b. Sur le cluster de destination, installez le certificat de l'autorité de certification qui a signé le certificat du serveur *source* S3 :
`security certificate install -type server-ca -vserver dest_admin_svm -cert -name src_server_certificate`

Si vous utilisez un certificat signé par un fournisseur d'autorité de certification externe, installez le même certificat sur le SVM d'administration source et de destination.

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

6. Sur le SVM source, créer 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`

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

Vous pouvez commencer à protéger les compartiments S3 à tout moment. Par exemple, si vous avez mis à niveau une configuration S3 à partir d'une version antérieure à ONTAP 9.10.1.

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 clusters source et destination, et une relation de peering existe entre les machines virtuelles de stockage source et 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.

Description de la tâche

Les tâches doivent être réalisées sur les clusters source et cible.

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 la clé.** ne pas régénérer la clé si elle existe déjà.
2. Vérifiez que l'accès utilisateur et groupe est correct dans les machines virtuelles de stockage source et de destination : cliquez sur **stockage > machines virtuelles de stockage,** cliquez sur la VM de stockage, cliquez sur **Paramètres**, puis cliquez sur Sous **S3**.

   Voir "Ajoutez des utilisateurs et des groupes S3" pour en savoir plus.
3. Sur le cluster source, créez une règle SnapMirror S3 si vous ne en possédez pas déjà une 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 Policies**, puis cliquez sur **Ajouter**.
   c. Entrez le nom et la description de la stratégie.
   d. Sélectionner la « policy scope », le cluster ou le SVM
   e. Sélectionnez **Continuous** pour les relations SnapMirror S3.
   f. 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 la protection 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 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 *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 des 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

   ```
   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. Sur la SVM source, créez une règle SnapMirror S3 si vous ne en possédez pas déjà une 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/secondes (facultatif).

Exemple

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

5. Installez les certificats CA sur les SVM admin des clusters source et destination :
   a. Sur le cluster source, installez le certificat de l'autorité de certification qui a signé le certificat du serveur *destination* S3 :
   `security certificate install -type server-ca -vserver src_admin_svm -cert -name dest_server_certificate`
   b. Sur le cluster de destination, installez le certificat de l'autorité de certification qui a signé le certificat du serveur *source* S3 :
   `security certificate install -type server-ca -vserver dest_admin_svm -cert -name src_server_certificate`+ si vous utilisez un certificat signé par un fournisseur d'autorité de certification externe, installez le même certificat sur le SVM d'administration source et de destination.

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

6. Sur le SVM source, créer 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:/bucket/test-bucket
   -destination-path vs1:/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 distant)

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. Il n'est pas nécessaire de resynchroniser explicitement la relation, comme cela est requis pour les déploiements de SnapMirror volume.

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

```
dest_cluster::> snapmirror failover start -destination-path
dest_svm1:/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 **SnapMirror S3**.

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.
     - Copiez et collez le contenu du certificat CA du serveur *destination* S3.
   - 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 CA du serveur *destination* S3.
4. Sous **destination**, copiez et collez le contenu du certificat CA du serveur *source* S3.
5. 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

```
dest_cluster::> snapmirror restore -source-path src_vs1:/bucket/test-
bucket -destination-path dest_vs1:/bucket/test-bucket-mirror
```

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 Policies**, 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/secondes (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 Policies**, 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/secondes (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
```

Protection des sauvegardes avec des cibles cloud

Exigences relatives aux relations cibles cloud

Vérifiez que vos environnements source et cible répondent aux exigences de protection des sauvegardes S3 SnapMirror vers les cibles dans le cloud.

Pour accéder au compartiment de données, vous devez disposer d'identifiants de compte valides auprès du fournisseur de magasin d'objets.

Les interfaces réseau intercluster et un IPspace doivent être configurées sur le cluster avant que le cluster ne puisse se connecter à un magasin d'objets cloud. Vous devez créer des interfaces réseau du cluster sur chaque nœud pour transférer les données de manière transparente du stockage local vers le magasin d'objets cloud.

Pour les cibles StorageGRID, vous devez connaître les informations suivantes :

- Nom du serveur, exprimé sous forme de nom de domaine complet (FQDN) ou d'adresse IP
- nom de compartiment : ce compartiment doit déjà exister
- touche d'accès
- clé secrète

En outre, le certificat d'autorité de certification utilisé pour signer le certificat de serveur StorageGRID doit être installé sur la machine virtuelle de stockage d'administration du cluster ONTAP S3 à l'aide de `security certificate install command`. Pour plus d'informations, voir "Installation d'un certificat CA" Si vous utilisez StorageGRID.

Pour les cibles AWS S3, vous devez connaître les informations suivantes :

- Nom du serveur, exprimé sous forme de nom de domaine complet (FQDN) ou d'adresse IP
- nom de compartiment : ce compartiment doit déjà exister
- touche d'accès
- clé secrète

Le serveur DNS de la machine virtuelle de stockage admin du cluster ONTAP doit être capable de résoudre les FQDN (si utilisé) aux adresses IP.

Création d'une relation de sauvegarde pour un nouveau compartiment (cible cloud)

Lorsque vous créez de nouveaux compartiments S3, vous pouvez les sauvegarder immédiatement dans un compartiment cible SnapMirror S3 d'un fournisseur de magasin d'objets, qui peut être un système StorageGRID ou un déploiement AWS S3.

Ce dont vous aurez besoin

- Vous disposez d'informations d'identification de compte et de configuration valides pour le fournisseur de magasin d'objets.
- Les interfaces réseau intercluster et un IPspace ont été configurés sur le système source.
- • La configuration DNS pour la machine virtuelle de stockage source doit pouvoir résoudre le FQDN de la cible.

Procédure de System Manager

1. Modifiez la machine virtuelle de stockage pour ajouter des utilisateurs et ajouter des utilisateurs aux groupes :
   a. 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.

2. Ajouter un magasin d'objets cloud sur le système source :
   a. Cliquez sur **protection > vue d'ensemble**, puis sélectionnez **magasins d'objets Cloud**.
   b. Cliquez sur **Ajouter**, puis sélectionnez **Amazon S3** ou **StorageGRID**.
   c. Saisissez les valeurs suivantes :
      - Nom du magasin d'objets cloud
      - Style d'URL (chemin d'accès ou hébergement virtuel)
      - Machine virtuelle de stockage (activée pour S3)
      - Nom du serveur de magasin d'objets (FQDN)
      - Certificat de magasin d'objets
      - Touche d'accès
      - Clé secrète
      - Nom du conteneur (compartiment)
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 Policies**, 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)**, sélectionnez **stockage cloud**, puis sélectionnez **stockage objet cloud**.

Lorsque vous cliquez sur **Enregistrer**, un nouveau compartiment est créé dans la machine virtuelle de stockage source et il est sauvegardé dans le magasin d'objets cloud.

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 y a 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 d'un compartiment dans le SVM source :
`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 à la politique de compartiment par défaut :
`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 : * `type 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/secondes (facultatif).

   Exemple

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

5. Si la cible est un système StorageGRID, installez le certificat du serveur StorageGRID CA sur le SVM admin du cluster source :
`security certificate install -type server-ca -vserver src_admin_svm -cert-name`

storage_grid_server_certificate

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

6. Définissez le magasin d'objets de destination S3 SnapMirror :
`snapmirror object-store config create -vserver` *svm_name* `-object-store-name` *target_store_name* `-usage data -provider-type {AWS_S3|SGWS} -server` *target_FQDN* `-container-name` *remote_bucket_name* `-is-ssl-enabled true -port` *port_number* `-access-key target_access_key -secret-password` *target_secret_key*

   Paramètres : * `-object-store-name` – Le nom de la cible de magasin d'objets sur le système ONTAP local. * `-usage` – utiliser `data` pour ce flux de travail. * `-provider-type` – `AWS_S3` et `SGWS` Les cibles (StorageGRID) sont prises en charge. * `-server` – Le FQDN ou l'adresse IP du serveur cible. * `-is-ssl-enabled` –L'activation de SSL est facultative mais recommandée. + Voir le `snapmirror object-store config create` page de manuel pour plus de détails.

   Exemple

   ```
   src_cluster::> snapmirror object-store config create -vserver vs0
   -object-store-name sgws-store -usage data -provider-type SGWS -server
   sgws.example.com -container-name target-test-bucket -is-ssl-enabled true
   -port 443 -access-key abc123 -secret-password xyz890
   ```

7. Création d'une relation SnapMirror S3 :
`snapmirror create -source-path` *svm_name*`:/bucket/`*bucket_name* `-destination-path` *object_store_name*`:/objstore -policy` *policy_name*

   Paramètres : * `-destination-path` – le nom de magasin d'objets que vous avez créé à l'étape précédente et la valeur fixe `objstore`. + vous pouvez utiliser une stratégie que vous avez créée ou accepter la valeur par défaut.

   Exemple

   ```
   src_cluster::> snapmirror create -source-path vs0:/bucket/test-bucket
   -destination-path sgws-store:/objstore -policy test-policy
   ```

8. Vérifiez que la mise en miroir est active :
`snapmirror show -policy-type continuous -fields status`

Création d'une relation de sauvegarde pour un compartiment existant (cible cloud)

Vous pouvez commencer à sauvegarder des compartiments S3 à tout moment. Par exemple, si vous avez mis à niveau une configuration S3 à partir d'une version antérieure à ONTAP 9.10.1.

Ce dont vous aurez besoin

- Vous disposez d'informations d'identification de compte et de configuration valides pour le fournisseur de magasin d'objets.
- Les interfaces réseau intercluster et un IPspace ont été configurés sur le système source.

- La configuration DNS de la machine virtuelle de stockage source doit pouvoir résoudre le FQDN de la cible.

Procédure de System Manager

1. Vérifiez que les utilisateurs et les groupes sont correctement définis : cliquez sur **Storage > Storage VM**, cliquez sur la VM de stockage, cliquez sur **Settings**, puis sur Sous S3.

   Voir "Ajoutez des utilisateurs et des groupes S3" pour en savoir plus.

2. 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 Policies**, puis cliquez sur **Ajouter**.
   c. Entrez le nom et la description de la stratégie.
   d. Sélectionner la « policy scope », le cluster ou le SVM
   e. Sélectionnez **Continuous** pour les relations SnapMirror S3.
   f. Saisissez les valeurs **accélérateur** et **objectif de point de récupération**.
3. Ajouter un magasin d'objets cloud sur le système source :
   a. Cliquez sur **protection > Présentation**, puis sélectionnez **Cloud Object Store**.
   b. Cliquez sur **Ajouter**, puis sélectionnez **Amazon S3** ou **autres** pour StorageGRID Webscale.
   c. Saisissez les valeurs suivantes :
      - Nom du magasin d'objets cloud
      - Style d'URL (chemin d'accès ou hébergement virtuel)
      - Machine virtuelle de stockage (activée pour S3)
      - Nom du serveur de magasin d'objets (FQDN)
      - Certificat de magasin d'objets
      - Touche d'accès
      - Clé secrète
      - Nom du conteneur (compartiment)
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. Sauvegarde du compartiment à l'aide de S3 SnapMirror :
   a. Cliquez sur **stockage** > **godets**, puis sélectionnez le compartiment à sauvegarder.
   b. Cliquez sur **protéger**, sélectionnez **Cloud Storage** sous **cible**, puis sélectionnez **Cloud Object Store**.

Lorsque vous cliquez sur **Enregistrer**, le compartiment existant est sauvegardé dans le magasin d'objets cloud.

Procédure CLI

1. Vérifiez que les règles d'accès dans la politique de compartiment par défaut sont correctes :
   `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 /*
   ```

2. 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 : * `type 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/secondes (facultatif).

   Exemple

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

3. Si la cible est un système StorageGRID, installez le certificat StorageGRID CA sur le SVM admin du cluster source :
   `security certificate install -type server-ca -vserver src_admin_svm -cert-name storage_grid_server_certificate`

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

4. Définissez le magasin d'objets de destination S3 SnapMirror :
   `snapmirror object-store config create -vserver svm_name -object-store-name target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN -container-name remote_bucket_name -is-ssl-enabled true -port port_number -access-key target_access_key -secret-password target_secret_key`

Paramètres : * `-object-store-name` – Le nom de la cible de magasin d'objets sur le système ONTAP local. * `-usage` – utiliser `data` pour ce flux de travail. * `-provider-type` – `AWS_S3` et `SGWS` Les cibles (StorageGRID) sont prises en charge. * `-server` – Le FQDN ou l'adresse IP du serveur cible. * `-is-ssl-enabled` –L'activation de SSL est facultative mais recommandée. + Voir le `snapmirror object-store config create` page de manuel pour plus de détails.

Exemple

```
src_cluster::> snapmirror object-store config create -vserver vs0
-object-store-name sgws-store -usage data -provider-type SGWS -server
sgws.example.com -container-name target-test-bucket -is-ssl-enabled true
-port 443 -access-key abc123 -secret-password xyz890
```

5. Création d'une relation SnapMirror S3 :
`snapmirror create -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination-path` *`object_store_name`*`:/objstore -policy` *`policy_name`*

   Paramètres : * `-destination-path` – le nom de magasin d'objets que vous avez créé à l'étape précédente et la valeur fixe `objstore`. + vous pouvez utiliser une stratégie que vous avez créée ou accepter la valeur par défaut.

```
src_cluster::> snapmirror create -source-path vs0:/bucket/buck-evp
-destination-path sgws-store:/objstore -policy test-policy
```

6. Vérifiez que la mise en miroir est active :
`snapmirror show -policy-type continuous -fields status`

Restauration d'un compartiment à partir d'une cible cloud

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.

Procédure de System Manager

Restaurer les données de sauvegarde :

1. Cliquez sur **protection > relations**, puis sélectionnez **SnapMirror S3**.
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.
        - Copiez et collez le contenu du certificat CA du serveur *destination* S3.
    - 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.
4. Sous **destination**, copiez et collez le contenu du certificat CA du serveur *source* S3.
5. 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 compartiment (cible cloud)".
2. Lancer une opération de restauration pour le compartiment de destination :
`snapmirror restore -source-path` *`object_store_name`*`:/objstore -destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*

   Exemple

   L'exemple suivant illustre la restauration d'un compartiment de destination vers un compartiment existant.
```
clusterA::> snapmirror restore -source-path sgws.store:/objstore -destination
-path vs0:/bucket/test-bucket
```

Modifier une règle de miroir

Il peut être nécessaire de modifier une règle de miroir S3, par exemple pour ajuster les valeurs RPO et papillon.

Procédure de System Manager

Si vous souhaitez modifier ces valeurs, vous pouvez modifier une stratégie de protection existante.

1. Cliquez sur **protection > relations**, puis sélectionnez la stratégie de protection de la relation que vous souhaitez modifier.
2. Cliquez sur ⋮ En regard du nom de la stratégie, cliquez sur **Modifier**.

Procédure CLI

Modification d'une règle SnapMirror S3 :
`snapmirror policy modify -vserver svm_name -policy policy_name [-rpo` *`integer`*`] [-throttle` *`throttle_type`*`] [-comment` *`text`*`]`

Paramètres :

- `-rpo` – spécifie le temps de l'objectif de point de récupération, en secondes.

- `-throttle` – spécifie la limite supérieure sur le débit/bande passante, en kilo-octets/secondes.

```
clusterA::> snapmirror policy modify -vserver vs0 -policy test-policy -rpo
60
```