Protection des compartiments avec SnapMirror S3

ONTAP 9

NetApp
January 08, 2026

Sommaire

Protection des compartiments avec SnapMirror S3

En savoir plus sur ONTAP SnapMirror S3

Depuis ONTAP 9.10.1, vous pouvez protéger les compartiments dans des magasins d'objets ONTAP S3 à l'aide de la fonctionnalité de mise en miroir et de sauvegarde SnapMirror. À la différence d'SnapMirror standard, SnapMirror S3 permet la mise en miroir et les sauvegardes vers des destinations non-NetApp telles qu'AWS S3.

SnapMirror S3 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	Oui.	Oui.
StorageGRID	Non	Oui.
AWS S3	Non	Oui.
Cloud Volumes ONTAP pour Azure	Oui.	Oui.
Cloud Volumes ONTAP pour AWS	Oui.	Oui.
Cloud Volumes ONTAP pour Google Cloud	Oui.	Oui.

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

Configuration requise pour SnapMirror S3

- Version ONTAP

  ONTAP 9.10.1 ou version ultérieure doit s'exécuter sur les clusters source et cible.

  SnapMirror S3 n'est pas pris en charge dans les configurations MetroCluster.

- Licences

  Les licences suivantes sont disponibles dans le "ONTAP One" Une suite logicielle est requise sur les systèmes source et de destination ONTAP pour permettre l'accès aux éléments suivants :

- Protocole et stockage ONTAP S3
- SnapMirror S3 pour cibler d'autres cibles de magasin d'objets NetApp (ONTAP S3, StorageGRID et Cloud Volumes ONTAP)
- SnapMirror S3 pour cibler des magasins d'objets tiers, y compris AWS S3 (disponible dans le "Pack de compatibilité ONTAP One")
- Si votre cluster exécute ONTAP 9.10.1, un "Licence FabricPool" est requis.

- 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 d'autorité de certification utilisés pour signer les certificats des serveurs S3 doivent être installés sur la machine virtuelle de stockage d'administration des clusters qui hébergent 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) et les LIFs intercluster du cluster source et destination peuvent se connecter aux LIFs de données du serveur S3 source et destination.
  - 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
  - Toutes les relations SnapMirror S3 requièrent une règle SnapMirror spécifique à 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).

> Notez que lorsque deux compartiments S3 se trouvent dans une relation SnapMirror, si des règles de cycle de vie sont configurées de façon à ce que la version actuelle d'un objet expire (est supprimée), la même action est répliquée dans le compartiment partenaire. C'est vrai même si le compartiment partenaire est en lecture seule ou passif.

- Clés d'utilisateur root les clés d'accès utilisateur root de Storage VM sont requises pour les relations SnapMirror S3 ; ONTAP ne les attribue pas par défaut. La première fois que vous créez une relation SnapMirror S3, vous devez vérifier que les clés existent sur les machines virtuelles de stockage source et de destination et 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 de ONTAP 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)"

Relations SnapMirror prises en charge

SnapMirror S3 prend en charge les relations en éventail et en cascade. Pour une présentation, voir "Déploiements de la protection des données en cascade et « Fan-Out »" .

SnapMirror S3 ne prend pas en charge les 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 entre plusieurs clusters vers un seul cluster secondaire, mais chaque compartiment source doit avoir son propre compartiment de destination sur le cluster secondaire.

SnapMirror S3 n'est pas pris en charge dans les environnements MetroCluster.

Contrôle de l'accès aux compartiments S3

Lorsque vous créez de nouveaux compartiments, vous pouvez contrôler l'accès en créant des utilisateurs et des groupes.

SnapMirror S3 réplique les objets du compartiment source vers un compartiment de destination, mais il ne réplique pas les utilisateurs, les groupes et les règles du magasin d'objets source vers le magasin d'objets de destination.

Les utilisateurs, les règles de groupe, les autorisations et d'autres composants similaires doivent être configurés sur le magasin d'objets de destination afin que les clients puissent accéder au compartiment de destination lors d'un événement de basculement.

Les utilisateurs source et de destination peuvent utiliser les mêmes clés d'accès et secrètes, à condition que les clés source soient fournies manuellement lors de la création de l'utilisateur sur le cluster de destination. Par exemple :

```
vserver object-store-server user create -vserver svm1 -user user1 -access
-key "20-characters" -secret-key "40-characters"
```

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)"

Verrouillage des objets S3 et gestion des versions avec SnapMirror S3

Vous pouvez utiliser SnapMirror S3 sur des compartiments ONTAP avec verrouillage d'objet et gestion des

versions, en tenant compte de plusieurs considérations :

- Pour répliquer un compartiment source avec le verrouillage d'objet activé, le verrouillage d'objet doit également être activé dans le compartiment de destination. De plus, la gestion des versions doit être activée pour la source et la destination. Cela évite les problèmes de mise en miroir des suppressions dans le compartiment de destination lorsque les deux compartiments ont des règles de conservation par défaut différentes.
- S3 SnapMirror ne réplique pas les versions historiques des objets. Seule la version actuelle d'un objet est répliquée.

Les objets verrouillés sont mis en miroir dans un compartiment de destination afin de conserver leur temps de conservation d'origine. Si des objets déverrouillés sont répliqués, ils adopteront la période de conservation par défaut du compartiment de destination. Par exemple :

- La période de conservation par défaut du compartiment A est de 30 jours et celle du compartiment B est de 60 jours. Les objets répliqués depuis le compartiment A vers le compartiment B conservent leur période de conservation de 30 jours, même s'ils sont inférieurs à la période de conservation par défaut du compartiment B.
- Le compartiment A ne dispose pas de période de conservation par défaut et le compartiment B possède une période de conservation par défaut de 60 jours. Lorsque les objets déverrouillés sont répliqués du compartiment A vers le compartiment B, ils adoptent la période de conservation de 60 jours. Si un objet est verrouillé manuellement dans le compartiment A, il conserve sa période de conservation d'origine lorsqu'il est répliqué dans le compartiment B.
- La période de conservation par défaut du compartiment A est de 30 jours et celle du compartiment B n'est pas définie par défaut. Les objets répliqués depuis le compartiment A vers le compartiment B conservent leur période de conservation de 30 jours.

Protection en miroir et sauvegarde sur un cluster distant

Créez une relation de miroir pour un nouveau compartiment ONTAP S3 sur le cluster distant

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

Description de la tâche

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

Avant de commencer

- 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.

System Manager

1. S'il s'agit de la première relation SnapMirror S3 pour cette VM de stockage, vérifiez qu'il existe des clés utilisateur root pour les machines virtuelles de stockage source et de destination, 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 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. 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, cliquez sur **Paramètres**, puis cliquez sous S3.

   Voir "Ajoutez des utilisateurs et des groupes S3" pour en savoir plus.
3. Sur le cluster source, créez une stratégie SnapMirror S3 si vous n'en avez pas déjà une et que vous ne souhaitez pas utiliser la stratégie par défaut :
   a. Cliquez sur **protection > vue d'ensemble**, puis sur **Paramètres de stratégie locale**.
   b. Cliquez sur en regard de **politiques de protection**, puis cliquez sur **Ajouter**.
      - Entrez le nom et la description de la stratégie.
      - Sélectionner la « policy scope », le cluster ou le SVM
      - Sélectionnez **continu** 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*.

5. Cochez **utilisez le même certificat sur la destination** si vous utilisez un certificat signé par un fournisseur de CA externe.
6. 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.
7. Cliquez sur **Enregistrer**. Un nouveau compartiment est créé dans la VM de stockage source, et il est mis en miroir dans un nouveau compartiment créé pour la VM de stockage de destination.

Recul des godets verrouillés

À partir de ONTAP 9.14.1, vous pouvez sauvegarder des compartiments S3 verrouillés et les restaurer selon vos besoins.

Lorsque vous définissez les paramètres de protection d'un compartiment nouveau ou existant, vous pouvez activer le verrouillage des objets dans les compartiments de destination, à condition que les clusters source et de destination exécutent ONTAP 9.14.1 ou version ultérieure et que le verrouillage des objets est activé dans le compartiment source. Le mode de verrouillage d'objet et la durée de conservation du verrou du compartiment source deviennent applicables aux objets répliqués sur le compartiment de destination. Vous pouvez également définir une période de rétention de verrouillage différente pour le compartiment de destination dans la section **Paramètres de destination**. Cette période de conservation s'applique également à tout objet non verrouillé répliqué à partir du compartiment source et des interfaces S3.

Pour plus d'informations sur l'activation du verrouillage d'objet sur un compartiment, reportez-vous à la section "Créer un compartiment".

CLI

1. S'il s'agit de la première relation SnapMirror S3 pour ce SVM, vérifier que les clés utilisateur root existent pour les SVM source et de destination et les régénérer si ce n'est pas le cas :

   ```
   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,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. Sur la SVM source, créez une stratégie SnapMirror S3 si vous n'en avez pas déjà une et que vous ne souhaitez pas utiliser la stratégie 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` : seul type de règle pour les relations SnapMirror S3 (obligatoire).
   - `-rpo` - spécifie le temps pour l'objectif de point de récupération, en secondes (facultatif).
   - `-throttle` - spécifie la limite supérieure de 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.

Pour en savoir plus, `security certificate install` consultez le "Référence de commande ONTAP".

6. Sur la SVM source, créez 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`

Informations associées

- "création snapmirror"
- "création de politique snapmirror"
- "spectacle snapmirror"

Créez une relation de miroir pour un compartiment ONTAP S3 existant sur le 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.

Description de la tâche

Vous devez effectuer des tâches sur les clusters source et cible.

Avant de commencer

- 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.

Étapes

Vous pouvez créer une relation de miroir à l'aide de System Manager ou de l'interface de ligne de commandes

de ONTAP.

System Manager

1. S'il s'agit de la première relation SnapMirror S3 pour cette VM de stockage, vérifiez qu'il existe des clés utilisateur root pour les machines virtuelles de stockage source et de destination, puis régénérez-les si ce n'est pas le cas :
   a. Sélectionnez **stockage > Storage VM**, puis sélectionnez la VM de stockage.
   b. Dans l'onglet **Paramètres**, cliquez sur 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 des utilisateurs et des groupes existants sont présents et disposent des droits d'accès appropriés dans les VM de stockage source et de destination : sélectionnez **stockage > VM de stockage,** puis sélectionnez la VM de stockage, puis l'onglet **Paramètres**. Enfin, localisez la mosaïque **S3**, sélectionnez , puis l'onglet **utilisateurs** et l'onglet **groupes** pour afficher les paramètres d'accès des utilisateurs et des groupes.

   Voir " Ajoutez des utilisateurs et des groupes S3" pour en savoir plus.
3. Sur le cluster source, créez une stratégie SnapMirror S3 si vous n'en avez pas déjà une et que vous ne souhaitez pas utiliser la stratégie par défaut :
   a. Sélectionnez **protection > vue d'ensemble**, puis cliquez sur **Paramètres de stratégie locale**.
   b. Sélectionnez en regard de **politiques de protection**, puis cliquez sur **Ajouter**.
   c. Entrez le nom et la description de la stratégie.
   d. Sélectionner la portée de la règle : cluster ou SVM
   e. Sélectionnez **continu** 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 **autorisations**, cliquez sur **Modifier**, puis 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*.

6. Cochez **utilisez le même certificat sur la destination** si vous utilisez un certificat signé par un fournisseur de CA externe.
7. 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.
8. Cliquez sur **Enregistrer**. Le compartiment existant est mis en miroir vers un nouveau compartiment dans la VM de stockage de destination.

Recul des godets verrouillés

À partir de ONTAP 9.14.1, vous pouvez sauvegarder des compartiments S3 verrouillés et les restaurer selon vos besoins.

Lorsque vous définissez les paramètres de protection d'un compartiment nouveau ou existant, vous pouvez activer le verrouillage des objets dans les compartiments de destination, à condition que les clusters source et de destination exécutent ONTAP 9.14.1 ou version ultérieure et que le verrouillage des objets est activé dans le compartiment source. Le mode de verrouillage d'objet et la durée de conservation du verrou du compartiment source deviennent applicables aux objets répliqués sur le compartiment de destination. Vous pouvez également définir une période de rétention de verrouillage différente pour le compartiment de destination dans la section **Paramètres de destination**. Cette période de conservation s'applique également à tout objet non verrouillé répliqué à partir du compartiment source et des interfaces S3.

Pour plus d'informations sur l'activation du verrouillage d'objet sur un compartiment, reportez-vous à la section "Créer un compartiment".

CLI

1. S'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 et régénérez-les si ce n'est pas le cas : `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 régénérez pas 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 politiques 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,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. Sur la SVM source, créez une stratégie SnapMirror S3 si vous n'en avez pas déjà une et que vous ne souhaitez pas utiliser la stratégie 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.

   Pour en savoir plus, `security certificate install` consultez le "Référence de commande

ONTAP".

6. Sur la SVM source, créez 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`

Informations associées

- "création snapmirror"
- "création de politique snapmirror"
- "spectacle snapmirror"

Profitez du compartiment ONTAP S3 de destination sur le 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 est converti en lecture-écriture, inversant ainsi 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.

SnapMirror S3 réplique les objets du compartiment source vers un compartiment de destination, mais il ne réplique pas les utilisateurs, les groupes et les règles du magasin d'objets source vers le magasin d'objets de destination.

Les utilisateurs, les règles de groupe, les autorisations et d'autres composants similaires doivent être configurés sur le magasin d'objets de destination afin que les clients puissent accéder au compartiment de destination lors d'un événement de basculement.

Les utilisateurs source et de destination peuvent utiliser les mêmes clés d'accès et secrètes, à condition que les clés source soient fournies manuellement lors de la création de l'utilisateur sur le cluster de destination. Par

exemple :

```
vserver object-store-server user create -vserver svm1 -user user1 -access
-key "20-characters" -secret-key "40-characters"
```

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**.

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
   ```

Informations associées

- "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)"
- "démarrage du basculement de SnapMirror"
- "spectacle snapmirror"

Restaurer un compartiment ONTAP S3 à partir du SVM de destination sur le cluster distant

En cas de perte ou de corruption des données d'un compartiment source, vous pouvez restaurer les objets 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 par le 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.

System Manager

Restaurez les données sauvegardées :

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.
     - Nom du nouveau compartiment, niveau de service de capacité et de performance. 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.

Restaurer les compartiments verrouillés

À partir de ONTAP 9.14.1, vous pouvez sauvegarder les compartiments verrouillés et les restaurer si nécessaire.

Vous pouvez restaurer un compartiment verrouillé par objet vers un nouveau compartiment ou un compartiment existant. Vous pouvez sélectionner un compartiment verrouillé par objet comme destination dans les scénarios suivants :

- **Restaurer dans un nouveau compartiment** : lorsque le verrouillage d'objet est activé, un compartiment peut être restauré en créant un compartiment pour lequel le verrouillage d'objet est également activé. Lorsque vous restaurez un compartiment verrouillé, le mode de verrouillage des objets et la période de conservation du compartiment d'origine sont répliqués. Vous pouvez également définir une période de conservation de verrouillage différente pour le nouveau compartiment. Cette période de conservation est appliquée aux objets non verrouillés provenant d'autres sources.
- **Restaurer dans un compartiment existant** : un compartiment verrouillé par objet peut être restauré dans un compartiment existant, tant que la gestion des versions et un mode de verrouillage d'objet similaire sont activés sur le compartiment existant. La durée de conservation du godet d'origine est maintenue.
- **Restore non-locked bucket** : même si le verrouillage d'objet n'est pas activé sur un compartiment, vous pouvez le restaurer dans un compartiment dont le verrouillage d'objet est activé et qui se trouve sur le cluster source. Lorsque vous restaurez le compartiment, tous les objets non verrouillés sont verrouillés et le mode de conservation et la durée de conservation du compartiment de destination s'appliquent.

CLI

1. Créez le compartiment de destination à restaurer. Pour plus d'informations, voir "Création d'une relation de sauvegarde cloud pour un nouveau compartiment ONTAP S3".

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
```

Pour en savoir plus, `snapmirror restore` consultez le "Référence de commande ONTAP".

Mise en miroir et protection des sauvegardes sur le cluster local

Créez une relation de miroir pour un nouveau compartiment ONTAP S3 sur le cluster local

Lorsque vous créez de nouveaux buckets 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.

Avant de commencer

- 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.

System Manager

1. S'il s'agit de la première relation SnapMirror S3 pour cette VM de stockage, vérifiez qu'il existe des clés utilisateur root pour les machines virtuelles de stockage source et de destination, 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. Modifiez la machine virtuelle de stockage pour ajouter des utilisateurs et ajouter des utilisateurs à des groupes, dans les machines virtuelles de stockage source et de destination : cliquez sur **stockage > machines virtuelles de stockage**, cliquez sur la machine virtuelle de stockage, cliquez sur **Paramètres**, puis cliquez sous S3.

   Voir "Ajoutez des utilisateurs et des groupes S3" pour en savoir plus.
3. Créez une politique SnapMirror S3 si vous n'en avez pas déjà une et que vous ne souhaitez pas utiliser la politique par défaut :
   a. Cliquez sur **protection > vue d'ensemble**, puis sur **Paramètres de stratégie locale**.
   b. Cliquez sur en regard de **politiques de protection**, puis cliquez sur **Ajouter**.
      - Entrez le nom et la description de la stratégie.
      - Sélectionner la « policy scope », le cluster ou le SVM
      - Sélectionnez **continu** 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 local.
  - **VM de STOCKAGE** : sélectionnez une VM de stockage sur le cluster local.
  - **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.

5. Cochez **utilisez le même certificat sur la destination** si vous utilisez un certificat signé par un fournisseur de CA externe.
6. 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.
7. Cliquez sur **Enregistrer**. Un nouveau compartiment est créé dans la VM de stockage source, et il est mis en miroir dans un nouveau compartiment créé pour la VM de stockage de destination.

Recul des godets verrouillés

À partir de ONTAP 9.14.1, vous pouvez sauvegarder des compartiments S3 verrouillés et les restaurer selon vos besoins.

Lorsque vous définissez les paramètres de protection d'un compartiment nouveau ou existant, vous pouvez activer le verrouillage des objets dans les compartiments de destination, à condition que les clusters source et de destination exécutent ONTAP 9.14.1 ou version ultérieure et que le verrouillage des objets est activé dans le compartiment source. Le mode de verrouillage d'objet et la durée de conservation du verrou du compartiment source deviennent applicables aux objets répliqués sur le compartiment de destination. Vous pouvez également définir une période de rétention de verrouillage différente pour le compartiment de destination dans la section **Paramètres de destination**. Cette période de conservation s'applique également à tout objet non verrouillé répliqué à partir du compartiment source et des interfaces S3.

Pour plus d'informations sur l'activation du verrouillage d'objet sur un compartiment, reportez-vous à la section "Créer un compartiment".

CLI

1. S'il s'agit de la première relation SnapMirror S3 pour ce SVM, vérifier que les clés utilisateur root existent pour les SVM source et de destination et les régénérer si ce n'est pas le cas :
   `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,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. Créez une politique SnapMirror S3 si vous n'en avez pas déjà une et que vous ne souhaitez pas utiliser la politique 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 de CA externe, il vous suffit d'installer ce certificat sur le SVM d'administration.

      Pour en savoir plus, `security certificate install` consultez le "Référence de commande ONTAP".

6. 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.

```
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`

Informations associées

- "création snapmirror"
- "création de politique snapmirror"
- "spectacle snapmirror"

Créez une relation de miroir pour un compartiment ONTAP S3 existant sur le 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.

Avant de commencer

- 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.

System Manager

1. S'il s'agit de la première relation SnapMirror S3 pour cette VM de stockage, vérifiez qu'il existe des clés utilisateur root pour les machines virtuelles de stockage source et de destination, 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 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 des utilisateurs et des groupes existants sont présents et disposent des droits d'accès appropriés dans les VM de stockage source et de destination : sélectionnez **stockage > VM de stockage,** puis sélectionnez la VM de stockage, puis l'onglet **Paramètres**. Enfin, localisez la mosaïque **S3**, sélectionnez , puis l'onglet **utilisateurs** et l'onglet **groupes** pour afficher les paramètres d'accès des utilisateurs et des groupes.

   Voir "Ajoutez des utilisateurs et des groupes S3" pour en savoir plus.
3. Créez une politique SnapMirror S3 si vous n'en avez pas déjà une et que vous ne souhaitez pas utiliser la politique par défaut :
   a. Cliquez sur **protection > vue d'ensemble**, puis sur **Paramètres de stratégie locale**.
   b. Cliquez sur en regard de **politiques de protection**, puis cliquez sur **Ajouter**.
      - Entrez le nom et la description de la stratégie.
      - Sélectionner la « policy scope », le cluster ou le SVM
      - Sélectionnez **continu** 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 **autorisations**, cliquez sur **Modifier**, puis 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*.

6. Cochez **utilisez le même certificat sur la destination** si vous utilisez un certificat signé par un fournisseur de CA externe.
7. 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.
8. Cliquez sur **Enregistrer**. Le compartiment existant est mis en miroir vers un nouveau compartiment dans la VM de stockage de destination.

Recul des godets verrouillés

À partir de ONTAP 9.14.1, vous pouvez sauvegarder des compartiments S3 verrouillés et les restaurer selon vos besoins.

Lorsque vous définissez les paramètres de protection d'un compartiment nouveau ou existant, vous pouvez activer le verrouillage des objets dans les compartiments de destination, à condition que les clusters source et de destination exécutent ONTAP 9.14.1 ou version ultérieure et que le verrouillage des objets est activé dans le compartiment source. Le mode de verrouillage d'objet et la durée de conservation du verrou du compartiment source deviennent applicables aux objets répliqués sur le compartiment de destination. Vous pouvez également définir une période de rétention de verrouillage différente pour le compartiment de destination dans la section **Paramètres de destination**. Cette période de conservation s'applique également à tout objet non verrouillé répliqué à partir du compartiment source et des interfaces S3.

Pour plus d'informations sur l'activation du verrouillage d'objet sur un compartiment, reportez-vous à la section "Créer un compartiment".

CLI

1. S'il s'agit de la première relation SnapMirror S3 pour ce SVM, vérifier que les clés utilisateur root existent pour les SVM source et de destination et les régénérer si ce n'est pas le cas :
   `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,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. Créez une politique SnapMirror S3 si vous n'en avez pas déjà une et que vous ne souhaitez pas utiliser la politique 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 de CA externe, il vous suffit d'installer ce certificat sur le SVM d'administration.

Pour en savoir plus, `security certificate install` consultez le "Référence de commande ONTAP".

6. 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`

Informations associées

- "création snapmirror"
- "création de politique snapmirror"
- "spectacle snapmirror"

Profitez du compartiment ONTAP S3 de destination sur le 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 est converti en lecture-écriture, inversant ainsi 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.

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**.

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
```

Informations associées

- "démarrage du basculement de SnapMirror"
- "spectacle snapmirror"

Restaurer un compartiment ONTAP S3 à partir du SVM de destination sur le cluster local

En cas de perte ou de corruption des données d'un compartiment source, vous pouvez restaurer des objets 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 par le 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 lancée à partir du cluster local.

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.
     - Nom du nouveau compartiment, niveau de service de capacité et de performance. 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.

Restaurer les compartiments verrouillés

À partir de ONTAP 9.14.1, vous pouvez sauvegarder les compartiments verrouillés et les restaurer si nécessaire.

Vous pouvez restaurer un compartiment verrouillé par objet vers un nouveau compartiment ou un compartiment existant. Vous pouvez sélectionner un compartiment verrouillé par objet comme destination dans les scénarios suivants :

- **Restaurer dans un nouveau compartiment** : lorsque le verrouillage d'objet est activé, un compartiment peut être restauré en créant un compartiment pour lequel le verrouillage d'objet est également activé. Lorsque vous restaurez un compartiment verrouillé, le mode de verrouillage des objets et la période de conservation du compartiment d'origine sont répliqués. Vous pouvez également définir une période de conservation de verrouillage différente pour le nouveau compartiment. Cette période de conservation est appliquée aux objets non verrouillés provenant d'autres sources.
- **Restaurer dans un compartiment existant** : un compartiment verrouillé par objet peut être restauré dans un compartiment existant, tant que la gestion des versions et un mode de verrouillage d'objet similaire sont activés sur le compartiment existant. La durée de conservation du godet d'origine est maintenue.
- **Restore non-locked bucket** : même si le verrouillage d'objet n'est pas activé sur un compartiment, vous pouvez le restaurer dans un compartiment dont le verrouillage d'objet est activé et qui se trouve sur le cluster source. Lorsque vous restaurez le compartiment, tous les objets non verrouillés sont verrouillés et le mode de conservation et la durée de conservation du compartiment de destination s'appliquent.

CLI

1. Si vous restaurez des objets dans un nouveau compartiment, créez le nouveau compartiment. Pour

plus d'informations, voir "Création d'une relation de sauvegarde cloud pour un nouveau compartiment ONTAP S3".

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
```

Pour en savoir plus, `snapmirror restore` consultez le "Référence de commande ONTAP".

Protection des sauvegardes avec des cibles cloud

Conditions requises pour les relations ONTAP SnapMirror S3 Cloud cible

Assurez-vous que vos environnements source et cible respectent les exigences de protection de sauvegarde SnapMirror S3 sur des cibles cloud.

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

Les LIF intercluster et un IPspace doivent être configurés sur le cluster avant que le cluster ne puisse se connecter à un magasin d'objets cloud. Vous devez créer des LIF intercluster sur chaque nœud afin de transférer de manière transparente les données du stockage local vers le référentiel de stockage en mode objet 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

De plus, le certificat CA utilisé pour signer le certificat du serveur StorageGRID doit être installé sur la machine virtuelle de stockage d'administration du cluster ONTAP S3 à l'aide de `security certificate install` commande. Pour plus d'informations, reportez-vous à "Installation d'un certificat CA" la section 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 pouvoir résoudre les noms de domaine complets (s'ils sont utilisés) en adresses IP.

Informations associées

- "installation du certificat de sécurité"

Création d'une relation de sauvegarde cloud pour un nouveau compartiment ONTAP S3

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

Avant de commencer

- 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 nom de domaine complet de la cible.

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, cliquez sur **Paramètres**, puis cliquez 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 politique SnapMirror S3 si vous n'en avez pas déjà une et que vous ne souhaitez pas utiliser la politique par défaut :
   a. Cliquez sur **protection > vue d'ensemble**, puis sur **Paramètres de stratégie locale**.
   b. Cliquez sur en regard de **politiques de protection**, puis cliquez sur **Ajouter**.
      - Entrez le nom et la description de la stratégie.
      - Sélectionner la « policy scope », le cluster ou le SVM
      - Sélectionnez **continu** 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 ou les `_(bucketname, bucketname/*)` 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.

CLI

1. S'il s'agit de la première relation SnapMirror S3 pour ce SVM, vérifier que les clés utilisateur root existent pour les SVM source et de destination et les régénérer si ce n'est pas le cas :
   `vserver object-store-server user show` + Confirmez 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 régénérez pas 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,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

4. Créez une politique SnapMirror S3 si vous n'en avez pas déjà une et que vous ne souhaitez pas utiliser la politique 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` – 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` – indique la limite supérieure de 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`

   Pour en savoir plus, `security certificate install` consultez le "Référence de commande ONTAP".

6. Définissez le magasin d'objets de destination SnapMirror S3 :
`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 du magasin d'objets sur le système ONTAP local. * `-usage` – à utiliser `data` pour ce flux de travail. * `-provider-type` – `AWS_S3` Et `SGWS` (StorageGRID) cibles sont prises en charge. * `-server` – Le nom de domaine complet ou l'adresse IP du serveur cible. * `-is-ssl-enabled` –L'activation de SSL est facultative mais recommandée. + en savoir plus sur `snapmirror object-store config create` dans le "Référence de commande ONTAP".

   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. Créer 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 du 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 règle 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`

Informations associées

- "création snapmirror"
- "création de politique snapmirror"
- "spectacle snapmirror"

Création d'une relation de sauvegarde cloud pour un compartiment ONTAP S3 existant

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.

Avant de commencer

- 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.

System Manager

1. Vérifiez que les utilisateurs et les groupes sont correctement définis : cliquez sur **stockage > machines virtuelles de stockage**, cliquez sur la machine virtuelle de stockage, cliquez sur **Paramètres**, puis sur sous S3.

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

2. Créez une politique SnapMirror S3 si vous n'en avez pas déjà une et que vous ne souhaitez pas utiliser la politique par défaut :
   a. Cliquez sur **protection > vue d'ensemble**, puis sur **Paramètres de stratégie locale**.
   b. Cliquez sur en regard de **politiques de protection**, 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 **continu** 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 **autorisations**, cliquez sur **Modifier**, puis 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. Sauvegarder le compartiment à l'aide de SnapMirror S3 :
   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.

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,GetObjectAc
   l,ListBucketMultipartUploads,ListMultipartUploadParts -principal -
   -resource test-bucket, test-bucket /*
   ```

2. Créez une politique SnapMirror S3 si vous n'en avez pas déjà une et que vous ne souhaitez pas utiliser la politique 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` – 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` – indique la limite supérieure de 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`

   Pour en savoir plus, `security certificate install` consultez le "Référence de commande ONTAP".

4. Définissez le magasin d'objets de destination SnapMirror S3 :
   `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 du magasin d'objets sur le système ONTAP local. * `-usage` – à utiliser `data` pour ce flux de travail. * `-provider-type` – `AWS_S3` Et `SGWS` (StorageGRID) cibles sont prises en charge. * `-server` – Le nom de domaine complet ou l'adresse IP du serveur cible. * `-is-ssl-enabled` –L'activation de SSL est facultative mais recommandée. + en savoir plus sur `snapmirror object-store config create` dans le "Référence de commande ONTAP".

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. Créer 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 du 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 règle 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`

Informations associées

- "création snapmirror"
- "création de politique snapmirror"
- "spectacle snapmirror"

Restaurer un compartiment ONTAP S3 à partir d'une cible cloud

En cas de perte ou de corruption des données d'un compartiment source, vous pouvez les remplir à nouveau 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.

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. Créez le compartiment de destination à restaurer. 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
   ```

   Pour en savoir plus, `snapmirror restore` consultez le "Référence de commande ONTAP".

Modification d'une règle ONTAP SnapMirror S3

Vous pouvez modifier une règle SnapMirror S3 si vous souhaitez ajuster les valeurs de RPO et d'accélération.

System Manager

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

CLI

Modifier une politique SnapMirror S3 :
`snapmirror policy modify -vserver <svm_name> -policy <policy_name> [-rpo <integer>] [-throttle <throttle_type>] [-comment <text>]`

Paramètres :

- `-rpo`: Indique le temps de l'objectif de point de récupération, en secondes.
- `-throttle`: Indique la limite supérieure de débit/bande passante, en kilo-octets/secondes.

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

Informations associées

- "modification de la politique snapmirror"

Informations sur le copyright

Informations sur les marques commerciales