Mise en miroir et protection des sauvegardes sur le cluster local

ONTAP 9

NetApp
September 12, 2024

Sommaire

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.

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 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 **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 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 de CA externe, il vous suffit d'installer ce certificat sur le 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.

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 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 **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 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 de CA externe, il vous suffit d'installer ce certificat sur le 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 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
```

Restaurer un compartiment depuis la VM de stockage de destination (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 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
```