



Protection des sauvegardes avec des cibles cloud

ONTAP 9

NetApp
March 24, 2023

Table des matières

- Protection des sauvegardes avec des cibles cloud 1
 - Exigences relatives aux relations cibles cloud 1
 - Création d'une relation de sauvegarde pour un nouveau compartiment (cible cloud) 1
 - Création d'une relation de sauvegarde pour un compartiment existant (cible cloud) 5
 - Restauration d'un compartiment à partir d'une cible cloud 8

Protection des sauvegardes avec des cibles cloud

Exigences relatives aux relations cibles cloud

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

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

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

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

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

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

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

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

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

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

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


Ce dont vous aurez besoin


- Vous disposez d'informations d'identification de compte et de configuration valides pour le fournisseur de

magasin d'objets.

- Les interfaces réseau intercluster et un IPspace ont été configurés sur le système source.
- La configuration DNS pour la machine virtuelle de stockage source doit pouvoir résoudre le FQDN de la cible.

Procédure de System Manager

1. Modifiez la machine virtuelle de stockage pour ajouter des utilisateurs et ajouter des utilisateurs aux groupes :
 - a. Cliquez sur **stockage > machines virtuelles de stockage**, cliquez sur la machine virtuelle de stockage, puis sur **Paramètres** et enfin sur  Sous **S3**.

Voir "[Ajoutez des utilisateurs et des groupes S3](#)" pour en savoir plus.
2. Ajouter un magasin d'objets cloud sur le système source :
 - a. Cliquez sur **protection > vue d'ensemble**, puis sélectionnez **magasins d'objets Cloud**.
 - b. Cliquez sur **Ajouter**, puis sélectionnez **Amazon S3** ou **StorageGRID**.
 - c. Saisissez les valeurs suivantes :
 - Nom du magasin d'objets cloud
 - Style d'URL (chemin d'accès ou hébergement virtuel)
 - Machine virtuelle de stockage (activée pour S3)
 - Nom du serveur de magasin d'objets (FQDN)
 - Certificat de magasin d'objets
 - Touche d'accès
 - Clé secrète
 - Nom du conteneur (compartiment)
3. Créez une règle SnapMirror S3 si vous ne disposez pas d'une règle existante et que vous ne souhaitez pas utiliser la règle par défaut :
 - a. Cliquez sur **protection > vue d'ensemble**, puis sur **Paramètres de stratégie locale**.
 - b. Cliquez sur  En regard de **protection Politiques**, puis cliquez sur **Ajouter**.
 - Entrez le nom et la description de la stratégie.
 - Sélectionner la « policy scope », le cluster ou le SVM
 - Sélectionnez **Continuous** pour les relations SnapMirror S3.
 - Saisissez les valeurs **accélérateur** et **objectif de point de récupération**.
4. Création d'un compartiment avec la protection SnapMirror :
 - a. Cliquez sur **stockage > compartiments**, puis sur **Ajouter**.
 - b. Entrez un nom, sélectionnez la VM de stockage, entrez une taille, puis cliquez sur **plus d'options**.
 - c. Sous **permissions**, cliquez sur **Ajouter**. La vérification des autorisations est facultative mais recommandée.
 - **Principal** et **effet** - sélectionnez les valeurs correspondant aux paramètres de votre groupe d'utilisateurs ou acceptez les valeurs par défaut.
 - **Actions** - Assurez-vous que les valeurs suivantes sont affichées :

`GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts`

- **Ressources** - utilisez les valeurs par défaut `_(bucketname, bucketname/*)` ou d'autres valeurs dont vous avez besoin.

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

- d. Sous **protection**, cochez **Activer SnapMirror (ONTAP ou Cloud)**, sélectionnez **stockage cloud**, puis sélectionnez **stockage objet cloud**.

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

Procédure CLI

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

`vserver object-store-server user show+` Vérifiez qu'il y a une clé d'accès pour l'utilisateur root. Si ce n'est pas le cas, entrez :

`vserver object-store-server user regenerate-keys -vserver svm_name -user root+` ne pas régénérer la clé si elle existe déjà.

2. Création d'un compartiment dans le SVM source :

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

3. Ajout de règles d'accès à la politique de compartiment par défaut :

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

Exemple

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

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

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

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

Exemple

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

5. Si la cible est un système StorageGRID, installez le certificat du serveur StorageGRID CA sur le SVM admin du cluster source :

```
security certificate install -type server-ca -vserver src_admin_svm -cert-name
storage_grid_server_certificate
```

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

6. Définissez le magasin d'objets de destination S3 SnapMirror :

```
snapmirror object-store config create -vserver svm_name -object-store-name
target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN
-container-name remote_bucket_name -is-ssl-enabled true -port port_number
-access-key target_access_key -secret-password target_secret_key
```

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

Exemple

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

7. Création d'une relation SnapMirror S3 :

```
snapmirror create -source-path svm_name:/bucket/bucket_name -destination-path
object_store_name:/objstore -policy policy_name
```

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

Exemple

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

8. Vérifiez que la mise en miroir est active :

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


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

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

Ce dont vous aurez besoin


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

Procédure de System Manager

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

Voir "[Ajoutez des utilisateurs et des groupes S3](#)" pour en savoir plus.

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

- a. Cliquez sur **protection > vue d'ensemble**, puis sur **Paramètres de stratégie locale**.
- b. Cliquez sur  En regard de **protection Politiques**, puis cliquez sur **Ajouter**.
- c. Entrez le nom et la description de la stratégie.
- d. Sélectionner la « policy scope », le cluster ou le SVM
- e. Sélectionnez **Continuous** pour les relations SnapMirror S3.
- f. Saisissez les valeurs **accélérateur** et **objectif de point de récupération**.


3. Ajouter un magasin d'objets cloud sur le système source :

- a. Cliquez sur **protection > Présentation**, puis sélectionnez **Cloud Object Store**.
- b. Cliquez sur **Ajouter**, puis sélectionnez **Amazon S3** ou **autres** pour StorageGRID Webscale.

- c. Saisissez les valeurs suivantes :

- Nom du magasin d'objets cloud
- Style d'URL (chemin d'accès ou hébergement virtuel)
- Machine virtuelle de stockage (activée pour S3)
- Nom du serveur de magasin d'objets (FQDN)
- Certificat de magasin d'objets
- Touche d'accès
- Clé secrète
- Nom du conteneur (compartiment)

4. Vérifiez que la politique d'accès au compartiment du compartiment existant répond toujours à vos besoins :

- a. Cliquez sur **stockage > godets**, puis sélectionnez le compartiment à protéger.
- b. Dans l'onglet **permissions**, cliquez sur  **Modifier**, puis cliquez sur **Ajouter** sous **autorisations**.
 - **Principal et effet** - sélectionnez les valeurs correspondant aux paramètres de votre groupe d'utilisateurs ou acceptez les valeurs par défaut.
 - **Actions** - Assurez-vous que les valeurs suivantes sont affichées :
`GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts`
 - **Ressources** - utilisez les valeurs par défaut (`bucketname, bucketname/*`) ou d'autres valeurs dont vous avez besoin.

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

5. Sauvegarde du compartiment à l'aide de S3 SnapMirror :
 - a. Cliquez sur **stockage > godets**, puis sélectionnez le compartiment à sauvegarder.
 - b. Cliquez sur **protéger**, sélectionnez **Cloud Storage** sous **cible**, puis sélectionnez **Cloud Object Store**.

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

Procédure CLI

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

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

Exemple

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

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

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

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

Exemple

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

3. Si la cible est un système StorageGRID, installez le certificat StorageGRID CA sur le SVM admin du cluster source :

```
security certificate install -type server-ca -vserver src_admin_svm -cert-name
storage_grid_server_certificate
```

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

4. Définissez le magasin d'objets de destination S3 SnapMirror :

```
snapmirror object-store config create -vserver svm_name -object-store-name
target_store_name -usage data -provider-type {AWS_S3|SGWS} -server target_FQDN
-container-name remote_bucket_name -is-ssl-enabled true -port port_number
-access-key target_access_key -secret-password target_secret_key
```

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

Exemple

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

5. Création d'une relation SnapMirror S3 :

```
snapmirror create -source-path svm_name:/bucket/bucket_name -destination-path
object_store_name:/objstore -policy policy_name
```

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

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

6. Vérifiez que la mise en miroir est active :

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

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

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

Description de la tâche

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

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

Procédure de System Manager

Restaurer les données de sauvegarde :

1. Cliquez sur **protection > relations**, puis sélectionnez **SnapMirror S3**.
2. Cliquez sur  Puis sélectionnez **Restaurer**.
3. Sous **Source**, sélectionnez **Pot existant** (valeur par défaut) ou **Nouveau godet**.
 - Pour restaurer un **compartiment existant** (valeur par défaut), procédez comme suit :
 - Sélectionnez le cluster et la VM de stockage pour rechercher le compartiment existant.
 - Sélectionner le godet existant.
 - Copiez et collez le contenu du certificat CA du serveur *destination* S3.
 - Pour restaurer un **Nouveau godet**, entrez les valeurs suivantes :
 - Machine virtuelle de cluster et de stockage pour héberger le nouveau compartiment.
 - Le nouveau compartiment : niveau de service du nom, de la capacité et des performances. Voir "[Niveaux de services de stockage](#)" pour en savoir plus.
 - Contenu du certificat d'autorité de certification du serveur S3 de destination.
4. Sous **destination**, copiez et collez le contenu du certificat CA du serveur *source* S3.
5. Cliquez sur **protection > relations** pour contrôler la progression de la restauration.

Procédure CLI

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

```
snapmirror restore -source-path object_store_name:/objstore -destination-path svm_name:/bucket/bucket_name
```

Exemple

L'exemple suivant illustre la restauration d'un compartiment de destination vers un compartiment existant.

```
clusterA::> snapmirror restore -source-path sgws.store:/objstore -destination-path vs0:/bucket/test-bucket
```

Informations sur le copyright

Copyright © 2023 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

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

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

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

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

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

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

Informations sur les marques commerciales

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