Protezione del backup con destinazioni cloud

ONTAP 9

NetApp
April 24, 2024

This PDF was generated from https://docs.netapp.com/it-it/ontap/s3-snapmirror/requirements-cloud-targets-concept.html on April 24, 2024. Always check docs.netapp.com for the latest.

Sommario

Protezione del backup con destinazioni cloud

Requisiti per le relazioni di destinazione del cloud

Assicurati che gli ambienti di origine e di destinazione soddisfino i requisiti per la protezione di backup di S3 SnapMirror verso le destinazioni cloud.

Per accedere al bucket di dati, è necessario disporre di credenziali account valide con il provider dell'archivio di oggetti.

Le interfacce di rete tra cluster e un IPSpace devono essere configurati sul cluster prima che il cluster possa connettersi a un archivio di oggetti cloud. È necessario creare interfacce di rete del cluster di invio su ciascun nodo per trasferire senza problemi i dati dallo storage locale all'archivio di oggetti cloud.

Per gli obiettivi StorageGRID, è necessario conoscere le seguenti informazioni:

- Nome del server, espresso come nome di dominio completo (FQDN) o indirizzo IP
- nome bucket; il bucket deve già esistere
- tasto di accesso
- chiave segreta

Inoltre, il certificato CA utilizzato per firmare il certificato del server StorageGRID deve essere installato sulla macchina virtuale di storage amministrativa del cluster ONTAP S3 utilizzando `security certificate install command`. Per ulteriori informazioni, vedere "Installazione di un certificato CA" Se si utilizza StorageGRID.

Per i target AWS S3, è necessario conoscere le seguenti informazioni:

- Nome del server, espresso come nome di dominio completo (FQDN) o indirizzo IP
- nome bucket; il bucket deve già esistere
- tasto di accesso
- chiave segreta

Il server DNS per la VM di storage amministrativa del cluster ONTAP deve essere in grado di risolvere gli FQDN (se utilizzati) in indirizzi IP.

Creare una relazione di backup per un nuovo bucket (target cloud)

Quando crei nuovi bucket S3, puoi eseguirne immediatamente il backup su un bucket di destinazione di S3 SnapMirror su un provider di archivi di oggetti, che può essere un sistema StorageGRID o un'implementazione di Amazon S3.

Prima di iniziare

- Si dispone di credenziali account e informazioni di configurazione valide per il provider dell'archivio di oggetti.
- Le interfacce di rete tra cluster e un IPSpace sono state configurate sul sistema di origine.

- • La configurazione DNS per la VM dello storage di origine deve essere in grado di risolvere il FQDN della destinazione.

System Manager

1. Modificare la VM di storage per aggiungere utenti e utenti ai gruppi:
   a. Fare clic su **Storage > Storage VMS**, fare clic sulla VM di storage, fare clic su **Settings** (Impostazioni), quindi su Sotto **S3**.

      Vedere "Aggiungere utenti e gruppi S3" per ulteriori informazioni.

2. Aggiungere un Cloud Object Store sul sistema di origine:
   a. Fare clic su **protezione > Panoramica**, quindi selezionare **Cloud Object Stores**.
   b. Fare clic su **Aggiungi**, quindi selezionare **Amazon S3** o **StorageGRID**.
   c. Immettere i seguenti valori:
      - Nome archivio oggetti cloud
      - Stile URL (path o virtual-hosted)
      - Storage VM (abilitato per S3)
      - Nome server archivio oggetti (FQDN)
      - Certificato dell'archivio di oggetti
      - Tasto di accesso
      - Chiave segreta
      - Nome del container (bucket)
3. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:
   a. Fare clic su **protezione > Panoramica**, quindi su **Impostazioni policy locale**.
   b. Fare clic su Accanto a **Criteri di protezione**, quindi fare clic su **Aggiungi**.
      - Immettere il nome e la descrizione della policy.
      - Selezionare l'ambito del criterio, il cluster o SVM
      - Selezionare **Continuous** per le relazioni di S3 SnapMirror.
      - Inserire i valori **Throttle** e **Recovery Point Objective**.
4. Crea un bucket con la protezione SnapMirror:
   a. Fare clic su **Storage > Bucket**, quindi su **Add** (Aggiungi).
   b. Immettere un nome, selezionare la VM di storage, immettere una dimensione, quindi fare clic su **altre opzioni**.
   c. In **Permissions**, fare clic su **Add** (Aggiungi). La verifica delle autorizzazioni è facoltativa ma consigliata.
      - **Principal** e **Effect** - selezionare i valori corrispondenti alle impostazioni del gruppo di utenti o accettare le impostazioni predefinite.
      - **Azioni** - assicurarsi che vengano visualizzati i seguenti valori:

```
`GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetO
bjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
```

- **Risorse** - utilizzare le impostazioni predefinite _`(bucketname, bucketname/*)` o altri valori di cui hai bisogno.

  Vedere "Gestire l'accesso degli utenti ai bucket" per ulteriori informazioni su questi campi.

d. In **protezione**, selezionare **attiva SnapMirror (ONTAP o Cloud)**, selezionare **archiviazione cloud**, quindi selezionare **Archivio oggetti cloud**.

Facendo clic su **Save** (Salva), viene creato un nuovo bucket nella VM dello storage di origine e viene eseguito il backup nell'archivio di oggetti cloud.

CLI

1. Se questa è la prima relazione di S3 SnapMirror per questa SVM, verificare che le chiavi utente root esistano sia per le SVM di origine che di destinazione e rigenerarle in caso contrario:
   `vserver object-store-server user show`+ confermare che esiste una chiave di accesso per l'utente root. In caso contrario, immettere:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user` *`root`*+ non rigenerare la chiave se ne esiste già una.

2. Creare un bucket nella SVM di origine:
   `vserver object-store-server bucket create -vserver` *`svm_name`* `-bucket` *`bucket_name`* `[-size` *`integer`*`[KB|MB|GB|TB|PB]] [-comment` *`text`*`] [`*`additional_options`*`]`

3. Aggiungere regole di accesso alla policy bucket predefinita:
   `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`*`]`

   Esempio

   ```
   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. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo` *`integer`*`] [-throttle` *`throttle_type`*`] [-comment` *`text`*`] [`*`additional_options`*`]`

   Parametri: * `type continuous` – L'unico tipo di policy per le relazioni di S3 SnapMirror (obbligatorio). * `-rpo` – specifica il tempo per l'obiettivo del punto di ripristino, in secondi (facoltativo). * `-throttle` – specifica il limite massimo di throughput/larghezza di banda, in kilobyte/secondi (opzionale).

Esempio

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

5. Se la destinazione è un sistema StorageGRID, installare il certificato del server CA StorageGRID sulla SVM amministrativa del cluster di origine:
`security certificate install -type server-ca -vserver` *`src_admin_svm`* `-cert -name` *`storage_grid_server_certificate`*

   Vedere `security certificate install` pagina man per i dettagli.

6. Definire l'archivio di oggetti di destinazione di 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`*

   Parametri: * `-object-store-name` – Il nome della destinazione dell'archivio di oggetti nel sistema ONTAP locale. * `-usage` – utilizzare `data` per questo flusso di lavoro. * `-provider-type` – `AWS_S3` e. `SGWS` Sono supportati i target (StorageGRID). * `-server` – L'indirizzo FQDN o IP del server di destinazione. * `-is-ssl-enabled` –L'abilitazione di SSL è facoltativa ma consigliata. + vedere `snapmirror object-store config create` pagina man per i dettagli.

   Esempio

```
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. Creare una relazione SnapMirror S3:
`snapmirror create -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination -path` *`object_store_name`*`:/objstore -policy` *`policy_name`*

   Parametri:
   * `-destination-path` - il nome dell'archivio oggetti creato nel passo precedente e il valore fisso `objstore`.

   È possibile utilizzare un criterio creato o accettare quello predefinito.

   Esempio

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

8. Verificare che il mirroring sia attivo:
`snapmirror show -policy-type continuous -fields status`

Creare una relazione di backup per un bucket esistente (target cloud)

È possibile iniziare il backup dei bucket S3 esistenti in qualsiasi momento, ad esempio se è stata aggiornata una configurazione S3 da una release precedente a ONTAP 9.10.1.

Prima di iniziare

- Si dispone di credenziali account e informazioni di configurazione valide per il provider dell'archivio di oggetti.
- Le interfacce di rete tra cluster e un IPSpace sono state configurate sul sistema di origine.
- La configurazione DNS per la VM dello storage di origine deve essere in grado di risolvere l'FQDN della destinazione.

System Manager

1. Verificare che gli utenti e i gruppi siano definiti correttamente: Fare clic su **Storage > Storage VM**, fare clic sulla VM di storage, fare clic su **Settings** (Impostazioni) e quindi su Sotto S3.

   Vedere "Aggiungere utenti e gruppi S3" per ulteriori informazioni.

2. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:
   a. Fare clic su **protezione > Panoramica**, quindi su **Impostazioni policy locale**.
   b. Fare clic su Accanto a **Criteri di protezione**, quindi fare clic su **Aggiungi**.
   c. Immettere il nome e la descrizione della policy.
   d. Selezionare l'ambito del criterio, il cluster o SVM
   e. Selezionare **Continuous** per le relazioni di S3 SnapMirror.
   f. Inserire i valori **Throttle** e **Recovery Point Objective**.
3. Aggiungere un Cloud Object Store sul sistema di origine:
   a. Fare clic su **protezione > Panoramica**, quindi selezionare **Cloud Object Store**.
   b. Fare clic su **Aggiungi**, quindi selezionare **Amazon S3** o **altri** per StorageGRID webscale.
   c. Immettere i seguenti valori:
      - Nome archivio oggetti cloud
      - Stile URL (path o virtual-hosted)
      - Storage VM (abilitato per S3)
      - Nome server archivio oggetti (FQDN)
      - Certificato dell'archivio di oggetti
      - Tasto di accesso
      - Chiave segreta
      - Nome del container (bucket)
4. Verificare che la policy di accesso al bucket del bucket esistente soddisfi ancora le proprie esigenze:
   a. Fare clic su **Storage** > **Bucket** e selezionare il bucket che si desidera proteggere.
   b. Nella scheda **Permissions**, fare clic su **Modifica**, quindi fare clic su **Aggiungi** in **permessi**.
      - **Principal** e **Effect** - selezionare i valori corrispondenti alle impostazioni del gruppo di utenti o accettare le impostazioni predefinite.
      - **Azioni** - assicurarsi che vengano visualizzati i seguenti valori: `GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
      - **Risorse** - utilizzare le impostazioni predefinite *(`bucketname`, `bucketname/*`)* o altri valori di cui hai bisogno.

        Vedere "Gestire l'accesso degli utenti ai bucket" per ulteriori informazioni su questi campi.
5. Eseguire il backup del bucket utilizzando S3 SnapMirror:
   a. Fare clic su **Storage** > **Bucket**, quindi selezionare il bucket di cui si desidera eseguire il backup.

b. Fare clic su **Protect**, selezionare **Cloud Storage** sotto **Target**, quindi selezionare **Cloud Object Store**.

Facendo clic su **Save** (Salva), viene eseguito il backup del bucket esistente nell'archivio di oggetti cloud.

CLI

1. Verificare che le regole di accesso nel criterio bucket predefinito siano corrette:
   `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`*`]`

   Esempio

   ```
   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. Creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera utilizzare quello predefinito:
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo` *`integer`*`] [-throttle` *`throttle_type`*`] [-comment` *`text`*`] [`*`additional_options`*`]`

   Parametri: * `type continuous` – L'unico tipo di policy per le relazioni di S3 SnapMirror (obbligatorio). * `-rpo` – specifica il tempo per l'obiettivo del punto di ripristino, in secondi (facoltativo). * `-throttle` – specifica il limite massimo di throughput/larghezza di banda, in kilobyte/secondi (opzionale).

   Esempio

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

3. Se la destinazione è un sistema StorageGRID, installare il certificato CA StorageGRID sulla SVM amministrativa del cluster di origine:
   `security certificate install -type server-ca -vserver` *`src_admin_svm`* `-cert -name` *`storage_grid_server_certificate`*

   Vedere `security certificate install` pagina man per i dettagli.

4. Definire l'archivio di oggetti di destinazione di 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`*

Parametri: * `-object-store-name` – Il nome della destinazione dell'archivio di oggetti nel sistema ONTAP locale. * `-usage` – utilizzare `data` per questo flusso di lavoro. * `-provider-type` – `AWS_S3` e. `SGWS` Sono supportati i target (StorageGRID). * `-server` – L'indirizzo FQDN o IP del server di destinazione. * `-is-ssl-enabled` –L'abilitazione di SSL è facoltativa ma consigliata. + vedere `snapmirror object-store config create` pagina man per i dettagli.

Esempio

```
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. Creare una relazione SnapMirror S3:
`snapmirror create -source-path svm_name:/bucket/bucket_name -destination -path object_store_name:/objstore -policy policy_name`

   Parametri:
   * `-destination-path` - il nome dell'archivio oggetti creato nel passo precedente e il valore fisso `objstore`.

   È possibile utilizzare un criterio creato o accettare quello predefinito.

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

6. Verificare che il mirroring sia attivo:
`snapmirror show -policy-type continuous -fields status`

Ripristinare un bucket da un target cloud

In caso di perdita o danneggiamento dei dati in un bucket di origine, sarà possibile ricompilare i dati ripristinandoli da un bucket di destinazione.

A proposito di questa attività

È possibile ripristinare il bucket di destinazione su un bucket esistente o su un nuovo bucket. Il bucket di destinazione per l'operazione di ripristino deve essere più grande dello spazio logico utilizzato del bucket di destinazione.

Se si utilizza un bucket esistente, questo deve essere vuoto quando si avvia un'operazione di ripristino. Il ripristino non "esegue il rollback" di un bucket nel tempo, ma popola un bucket vuoto con i contenuti precedenti.

System Manager

Ripristinare i dati di backup:

1. Fare clic su **protezione > Relazioni**, quindi selezionare **S3 SnapMirror**.
2. Fare clic su ⋮ Quindi selezionare **Ripristina**.
3. In **Source** (origine), selezionare **Existing Bucket** (bucket esistente) (impostazione predefinita) o **New Bucket** (nuovo bucket).
   - Per ripristinare un **bucket esistente** (impostazione predefinita), completare le seguenti azioni:
     - Selezionare il cluster e la VM di storage per cercare il bucket esistente.
     - Selezionare il bucket esistente.
     - Copiare e incollare il contenuto del certificato CA del server S3 *destination*.
   - Per ripristinare un **nuovo bucket**, immettere i seguenti valori:
     - Il cluster e la VM di storage per ospitare il nuovo bucket.
     - Il nome, la capacità e il livello di servizio delle performance del nuovo bucket. Vedere "Livelli di servizio dello storage" per ulteriori informazioni.
     - Contenuto del certificato CA del server S3 di destinazione.
4. In **destinazione**, copiare e incollare il contenuto del certificato CA del server S3 *origine*.
5. Fare clic su **protezione > Relazioni** per monitorare l'avanzamento del ripristino.

Procedura CLI

1. Creare il nuovo bucket di destinazione per il ripristino. Per ulteriori informazioni, vedere "Creare una relazione di backup per un bucket (target cloud)".
2. Avviare un'operazione di ripristino per il bucket di destinazione:
   `snapmirror restore -source-path object_store_name:/objstore -destination -path svm_name:/bucket/bucket_name`

   Esempio

   Nell'esempio seguente viene ripristinato un bucket di destinazione in un bucket esistente.
   ```
   clusterA::> snapmirror restore -source-path sgws.store:/objstore
   -destination-path vs0:/bucket/test-bucket
   ```

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.