Proteggere le benne con SnapMirror S3

ONTAP 9

NetApp
February 12, 2026

Sommario

Proteggere le benne con SnapMirror S3

Scopri ONTAP SnapMirror S3

A partire da ONTAP 9.10.1, puoi proteggere i bucket in archivi di oggetti ONTAP S3 usando la funzionalità di mirroring e backup di SnapMirror. A differenza del SnapMirror standard, SnapMirror S3 consente il mirroring e i backup in destinazioni non NetApp come AWS S3.

SnapMirror S3 supporta i mirror attivi e i Tier di backup da bucket ONTAP S3 nelle seguenti destinazioni:

Destinazione	Supporta mirror attivi e Takeover?	Supporta backup e ripristino?
ONTAP S3 • Bucket nella stessa SVM • Bucket in diverse SVM sullo stesso cluster • Bucket in SVM su cluster diversi	Sì	Sì
StorageGRID	No	Sì
AWS S3	No	Sì
Cloud Volumes ONTAP per Azure	Sì	Sì
Cloud Volumes ONTAP per AWS	Sì	Sì
Cloud Volumes ONTAP per Google Cloud	Sì	Sì

È possibile proteggere i bucket esistenti sui server ONTAP S3 o creare nuovi bucket con la protezione dei dati attivata immediatamente.

Requisiti di SnapMirror S3

- Versione di ONTAP

  ONTAP 9.10.1 o versione successiva deve essere in esecuzione sui cluster di origine e di destinazione.

  SnapMirror S3 non è supportato nelle configurazioni MetroCluster.

- Licensing

  Le seguenti licenze sono disponibili in "ONTAP uno" La suite software è necessaria sui sistemi di origine e destinazione ONTAP per accedere a:

  - Protocollo e storage ONTAP S3
  - SnapMirror S3 destinato ad altre destinazioni dell'archivio di oggetti NetApp (ONTAP S3, StorageGRID e Cloud Volumes ONTAP)
  - SnapMirror S3 per gli archivi di oggetti di terze parti, incluso AWS S3 (disponibile in "Pacchetto di compatibilità ONTAP One")

- Se il cluster esegue ONTAP 9.10.1, è necessario un"Licenza FabricPool".

- ONTAP S3
  - I server ONTAP S3 devono eseguire SVM di origine e di destinazione.
  - Si consiglia, ma non è obbligatorio, di installare i certificati CA per l'accesso TLS sui sistemi che ospitano server S3.
    - I certificati CA utilizzati per firmare i certificati dei server S3 devono essere installati sulla VM di storage di amministrazione dei cluster che ospitano server S3.
    - È possibile utilizzare un certificato CA autofirmato o un certificato firmato da un fornitore CA esterno.
    - Se le VM di storage di origine o di destinazione non sono in ascolto su HTTPS, non è necessario installare i certificati CA.
- Peering (per target ONTAP S3)
  - È necessario configurare le LIF (per destinazioni ONTAP remote) mentre le LIF intercluster del cluster di origine e destinazione possono connettersi alle LIF dati server di origine e destinazione S3.
  - I cluster di origine e di destinazione vengono peering (per le destinazioni ONTAP remote).
  - Le VM storage di origine e di destinazione sono in peering (per tutte le destinazioni ONTAP).
- Policy di SnapMirror
  - È necessario un criterio SnapMirror specifico per S3 per tutte le relazioni di SnapMirror S3, ma è possibile utilizzare lo stesso criterio per più relazioni.
  - È possibile creare un criterio personalizzato o accettare il criterio **continuo** predefinito, che include i seguenti valori:
    - Throttle (limite superiore di throughput/larghezza di banda) - illimitato.
    - Tempo per l'obiettivo del punto di ripristino: 1 ora (3600 secondi).

> Devi tenere presente che quando due bucket S3 si trovano in una relazione di SnapMirror, se esistono policy del ciclo di vita configurate in modo che scade la versione corrente di un oggetto (che viene eliminata), la stessa azione viene replicata nel bucket partner. Ciò è vero anche se il bucket partner è di sola lettura o passivo.

- Chiavi utente root le chiavi di accesso utente root della VM di storage sono necessarie per le relazioni con SnapMirror S3; ONTAP non le assegna per impostazione predefinita. La prima volta che si crea una relazione SnapMirror S3, è necessario verificare che le chiavi siano presenti sia sulle VM di archiviazione di origine che su quelle di destinazione e rigenerarle in caso contrario. Se è necessario rigenerarli, è necessario assicurarsi che tutti i client e tutte le configurazioni dell'archivio di oggetti SnapMirror che utilizzano la coppia di chiavi di accesso e segrete siano aggiornati con le nuove chiavi.

Per informazioni sulla configurazione del server S3, consultare i seguenti argomenti:

- "Abilitare un server S3 su una VM di storage"
- "Informazioni sul processo di configurazione di ONTAP S3"

Per informazioni sul peering delle macchine virtuali di storage e cluster, consultare il seguente argomento:

- "Preparazione per il mirroring e il vaulting (System Manager, fasi 1-6)"
- "Peering cluster e SVM (CLI)"

Relazioni SnapMirror supportate

SnapMirror S3 supporta relazioni fan-out e a cascata. Per una panoramica, vedere "Implementazioni di protezione dei dati fan-out e cascata" .

SnapMirror S3 non supporta le implementazioni fan-in (relazioni di data Protection tra più bucket di origine e un singolo bucket di destinazione). SnapMirror S3 può supportare più mirror bucket da cluster multipli a un singolo cluster secondario, ma ogni bucket di origine deve avere il proprio bucket di destinazione sul cluster secondario.

SnapMirror S3 non è supportato negli ambienti MetroCluster.

Controllare l'accesso alle benne S3

Quando si creano nuovi bucket, è possibile controllare l'accesso creando utenti e gruppi.

Sebbene SnapMirror S3 replica gli oggetti dal bucket di origine a un bucket di destinazione, non replica utenti, gruppi e policy dall'archivio di oggetti di origine all'archivio di oggetti di destinazione.

Gli utenti, le policy di gruppo, le autorizzazioni e componenti simili devono essere configurati nell'archivio di oggetti di destinazione in modo che i client possano accedere al bucket di destinazione durante un evento di failover.

Gli utenti di origine e destinazione possono utilizzare le stesse chiavi di accesso e segrete, a condizione che le chiavi di origine vengano fornite manualmente quando l'utente viene creato nel cluster di destinazione. Ad esempio:

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

Per ulteriori informazioni, consulta i seguenti argomenti:

- "Aggiunta di utenti e gruppi S3 (System Manager)"
- "Creazione di un utente S3 (CLI)"
- "Creare o modificare gruppi S3 (CLI)"

Utilizzare blocco oggetti S3 e versione con SnapMirror S3

È possibile utilizzare SnapMirror S3 su bucket ONTAP abilitati per blocco oggetti e versione, con alcune considerazioni:

- Per replicare un bucket di origine con blocco oggetti attivato, anche il bucket di destinazione deve avere blocco oggetti attivato. Inoltre, sia l'origine che la destinazione devono avere la versione abilitata. In questo modo si evitano problemi di mirroring delle eliminazioni nel bucket di destinazione quando entrambi i bucket hanno policy di conservazione predefinite diverse.
- S3 SnapMirror non replicherà le versioni storiche degli oggetti. Viene replicata solo la versione corrente di un oggetto.

Quando gli oggetti bloccati vengono replicati in un bucket di destinazione, mantengono il tempo di conservazione originale. Se gli oggetti sbloccati vengono replicati, essi adotteranno il periodo di conservazione predefinito del bucket di destinazione. Ad esempio:

- Il bucket A ha un periodo di conservazione predefinito di 30 giorni e il bucket B ha un periodo di conservazione predefinito di 60 giorni. Gli oggetti replicati dal bucket A al bucket B manterranno il periodo di conservazione di 30 giorni, anche se è inferiore al periodo di conservazione predefinito del bucket B.
- Il bucket A non ha un periodo di conservazione predefinito e il bucket B ha un periodo di conservazione predefinito di 60 giorni. Quando gli oggetti sbloccati vengono replicati dal bucket A al bucket B, essi adotteranno il periodo di conservazione di 60 giorni. Se un oggetto viene bloccato manualmente nel bucket A, manterrà il periodo di conservazione originale quando viene replicato nel bucket B.
- Il bucket A ha un periodo di conservazione predefinito di 30 giorni e il bucket B non ha un periodo di conservazione predefinito. Gli oggetti replicati dal bucket A al bucket B manterranno il periodo di conservazione di 30 giorni.

Protezione del mirroring e del backup su un cluster remoto

Creare una relazione di mirroring per un nuovo bucket di ONTAP S3 sul cluster remoto

Quando crei nuovi bucket S3, puoi proteggerli immediatamente in una destinazione SnapMirror S3 su un cluster remoto.

A proposito di questa attività

È necessario eseguire attività sui sistemi di origine e di destinazione.

Prima di iniziare

- I requisiti per le versioni di ONTAP, le licenze e la configurazione del server S3 sono stati completati.
- Esiste una relazione di peering tra i cluster di origine e di destinazione e esiste una relazione di peering tra le VM di storage di origine e di destinazione.
- I certificati CA sono necessari per le macchine virtuali di origine e di destinazione. È possibile utilizzare certificati CA autofirmati o certificati firmati da un vendor CA esterno.

System Manager

1. Se si tratta del primo rapporto di SnapMirror S3 per questa VM storage, verificare la presenza delle chiavi dell'utente root per le VM di storage di origine e di destinazione e rigenerarle in caso contrario:
   a. Fare clic su **Storage > Storage VM** (Storage VM), quindi selezionare la VM di storage.
   b. Nella scheda **Impostazioni**, fare clic nel riquadro **S3**.
   c. Nella scheda **utenti**, verificare che sia presente una chiave di accesso per l'utente root.
   d. In caso contrario, fare clic su accanto a **root**, quindi fare clic su **Rigenera chiave**. Non rigenerare la chiave se ne esiste già una.
2. Modificare la VM di storage per aggiungere utenti e utenti ai gruppi, sia nelle VM di storage di origine che di destinazione:

   Fare clic su **Storage > Storage VM**, fare clic sulla VM di archiviazione, fare clic su **Impostazioni**, quindi su sotto S3.

   Vedere "Aggiungere utenti e gruppi S3" per ulteriori informazioni.
3. Nel cluster di origine, crea un criterio SnapMirror S3 se non ne hai uno esistente e non vuoi utilizzare il criterio 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 **continuo** per le relazioni SnapMirror S3.
      - 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). La verifica delle autorizzazioni è facoltativa ma consigliata.
   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).
      - **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.
   d. In **protezione**, selezionare **attiva SnapMirror (ONTAP o Cloud)**. Quindi, immettere i seguenti valori:

- Destinazione
  - **DESTINAZIONE: Sistema ONTAP**
  - **CLUSTER**: Selezionare il cluster remoto.
  - **STORAGE VM**: Selezionare una storage VM sul cluster remoto.
  - **Certificato CA del SERVER S3**: Copia e incolla il contenuto del certificato *source*.
- Origine
  - **CERTIFICATO CA del SERVER S3:** copiare e incollare il contenuto del certificato *destination*.

5. Selezionare **Use the same certificate on the destination** (Usa lo stesso certificato sulla destinazione) se si utilizza un certificato firmato da un vendor CA esterno.
6. Se si fa clic su **Destination Settings** (Impostazioni destinazione), è anche possibile inserire i propri valori al posto dei valori predefiniti per il nome del bucket, la capacità e il livello di servizio delle performance.
7. Fare clic su **Save** (Salva). Viene creato un nuovo bucket nella VM per lo storage di origine e viene eseguito il mirroring in un nuovo bucket che viene creato la VM per lo storage di destinazione.

Backup delle benne bloccate

A partire da ONTAP 9.14.1, è possibile eseguire il backup di bucket S3 bloccati e ripristinarli secondo necessità.

Quando si definiscono le impostazioni di protezione per un bucket nuovo o esistente, è possibile attivare il blocco di oggetti nei bucket di destinazione, a condizione che i cluster di origine e di destinazione eseguano ONTAP 9.14.1 o versioni successive e che il blocco degli oggetti sia abilitato nel bucket di origine. La modalità di blocco degli oggetti e il mantenimento del blocco del bucket di origine diventano applicabili agli oggetti replicati nel bucket di destinazione. È inoltre possibile definire un periodo di blocco diverso per il bucket di destinazione nella sezione **Impostazioni destinazione**. Questo periodo di conservazione viene applicato anche a tutti gli oggetti non bloccati replicati dal bucket di origine e dalle interfacce S3.

Per informazioni su come attivare il blocco degli oggetti in un bucket, vedere "Creare un bucket".

CLI

1. In questo caso si tratta della prima relazione di SnapMirror S3 per questa SVM, verificare la presenza delle chiavi utente root per le SVM di origine e di destinazione e rigenerarle, se non:

   ```
   vserver object-store-server user show
   ```

   Verificare che sia presente 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 bucket nelle SVM di origine e di destinazione:

   ```
   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 alle policy di bucket predefinite nelle SVM di origine e di destinazione:

   `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

   ```
   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. Sull'SVM di origine, crea un criterio SnapMirror S3 se non ne hai uno esistente e non vuoi utilizzare il criterio predefinito:
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parametri:

   - Tipo `continuous` - l'unico tipo di criterio per le relazioni SnapMirror S3 (obbligatorio).
   - `-rpo` - specifica il tempo per l'obiettivo del punto di ripristino, in secondi (facoltativo).
   - `-throttle` - specifica il limite superiore di throughput/larghezza di banda, in kilobyte/secondi (opzionale).

     Esempio

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

5. Installare i certificati del server CA sulle SVM amministrative dei cluster di origine e di destinazione:

   a. Nel cluster di origine, installare il certificato CA che ha firmato il certificato del server S3 *destination*:
      `security certificate install -type server-ca -vserver src_admin_svm -cert-name dest_server_certificate`

   b. Nel cluster di destinazione, installare il certificato CA che ha firmato il certificato del server S3 *source*:
      `security certificate install -type server-ca -vserver dest_admin_svm -cert-name src_server_certificate`

      Se si utilizza un certificato firmato da un vendor CA esterno, installare lo stesso certificato sulla SVM amministrativa di origine e destinazione.

   Ulteriori informazioni su `security certificate install` nella "Riferimento al comando ONTAP".

6. Sulla SVM di origine, creare una relazione SnapMirror S3:

   ```
   snapmirror create -source-path src_svm_name:/bucket/bucket_name
   -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy
   policy_name]
   ```

   È possibile utilizzare un criterio creato o accettare quello predefinito.

   Esempio

   ```
   src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
   bucket -destination-path vs1-dest:bucket/test-bucket-mirror -policy
   test-policy
   ```

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

Informazioni correlate

- "creazione di snapmirror"
- "creazione di policy SnapMirror"
- "spettacolo snapmirror"

Creare una relazione di mirroring per un bucket ONTAP S3 esistente sul cluster remoto

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

A proposito di questa attività

Devi eseguire i task sui cluster di origine e destinazione.

Prima di iniziare

- I requisiti per le versioni di ONTAP, le licenze e la configurazione del server S3 sono stati completati.
- Esiste una relazione di peering tra i cluster di origine e di destinazione e esiste una relazione di peering tra le VM di storage di origine e di destinazione.
- I certificati CA sono necessari per le macchine virtuali di origine e di destinazione. È possibile utilizzare certificati CA autofirmati o certificati firmati da un vendor CA esterno.

Fasi

È possibile creare una relazione di mirroring utilizzando System Manager o l'interfaccia a riga di comando di ONTAP.

System Manager

1. Se si tratta del primo rapporto di SnapMirror S3 per questa VM storage, verificare la presenza delle chiavi dell'utente root per le VM di storage di origine e di destinazione e rigenerarle in caso contrario:
   a. Selezionare **Storage > Storage VM**, quindi selezionare la VM di storage.
   b. Nella scheda **Impostazioni**, fare clic nel riquadro **S3**.
   c. Nella scheda **utenti**, verificare che sia presente una chiave di accesso per l'utente root.
   d. In caso contrario, fare clic su accanto a **root**, quindi fare clic su **Rigenera chiave.** Non rigenerare la chiave se ne esiste già una.
2. Verificare che gli utenti e i gruppi esistenti siano presenti e abbiano accesso corretto sia nelle VM di storage di origine che di destinazione: Selezionare **Storage > Storage VM,** quindi selezionare la VM di storage, quindi la scheda **Settings**. Infine, individuare il riquadro **S3**, selezionare e selezionare la scheda **utenti**, quindi la scheda **gruppi** per visualizzare le impostazioni di accesso degli utenti e dei gruppi.

   Vedere "Aggiungere utenti e gruppi S3" per ulteriori informazioni.
3. Nel cluster di origine, crea un criterio SnapMirror S3 se non ne hai uno esistente e non vuoi utilizzare il criterio predefinito:
   a. Selezionare **protezione > Panoramica**, quindi fare clic su **Impostazioni criteri locali**.
   b. Selezionare accanto a **Criteri di protezione**, quindi fare clic su **Aggiungi**.
   c. Immettere il nome e la descrizione della policy.
   d. Seleziona l'ambito della policy: Cluster o SVM.
   e. Selezionare **continuo** per le relazioni SnapMirror S3.
   f. Inserire i valori **Throttle** e **Recovery Point Objective**.
4. Verificare che la policy di accesso al bucket del bucket esistente soddisfi ancora le proprie esigenze:
   a. Fare clic su **Storage > Bucket** (Storage > bucket), quindi selezionare il bucket che si desidera proteggere.
   b. Nella scheda **Permissions**, fare clic su **Edit**, quindi su **Add** in **Permissions**.
      - **Principal and Effect** (principale ed effetto): Selezionare i valori corrispondenti alle impostazioni del gruppo di utenti o accettare le impostazioni predefinite.
      - **Azioni**: Verificare 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. Proteggere una benna esistente con la protezione SnapMirror S3:
   a. Fare clic su **Storage** > **Bucket** e selezionare il bucket che si desidera proteggere.
   b. Fare clic su **Protect** (protezione) e immettere i seguenti valori:

- Destinazione
  - **DESTINAZIONE**: Sistema ONTAP
  - **CLUSTER**: Selezionare il cluster remoto.
  - **STORAGE VM**: Selezionare una storage VM sul cluster remoto.
  - **Certificato CA del SERVER S3**: Copia e incolla il contenuto del certificato *source*.
- Origine
  - **Certificato CA server S3**: Copia e incolla il contenuto del certificato *destination*.

6. Selezionare **Use the same certificate on the destination** (Usa lo stesso certificato sulla destinazione) se si utilizza un certificato firmato da un vendor CA esterno.
7. Se si fa clic su **Destination Settings** (Impostazioni destinazione), è anche possibile inserire i propri valori al posto dei valori predefiniti per il nome del bucket, la capacità e il livello di servizio delle performance.
8. Fare clic su **Save** (Salva). Viene eseguito il mirroring del bucket esistente in un nuovo bucket nella VM di storage di destinazione.

Backup delle benne bloccate

A partire da ONTAP 9.14.1, è possibile eseguire il backup di bucket S3 bloccati e ripristinarli secondo necessità.

Quando si definiscono le impostazioni di protezione per un bucket nuovo o esistente, è possibile attivare il blocco di oggetti nei bucket di destinazione, a condizione che i cluster di origine e di destinazione eseguano ONTAP 9.14.1 o versioni successive e che il blocco degli oggetti sia abilitato nel bucket di origine. La modalità di blocco degli oggetti e il mantenimento del blocco del bucket di origine diventano applicabili agli oggetti replicati nel bucket di destinazione. È inoltre possibile definire un periodo di blocco diverso per il bucket di destinazione nella sezione **Impostazioni destinazione**. Questo periodo di conservazione viene applicato anche a tutti gli oggetti non bloccati replicati dal bucket di origine e dalle interfacce S3.

Per informazioni su come attivare il blocco degli oggetti in un bucket, vedere "Creare un bucket".

CLI

1. Se si tratta del primo rapporto di SnapMirror S3 per questa SVM, verificare la presenza delle chiavi dell'utente root per le SVM di origine e di destinazione e rigenerarle in caso contrario: `vserver object-store-server user show` + verificare che sia disponibile 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 già esistente.
2. Creare un bucket sulla SVM di destinazione come destinazione mirror:

   ```
   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. Verificare che le regole di accesso delle policy di bucket predefinite siano corrette sia nelle SVM di origine che di destinazione:

   ```
   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

```
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. Sull'SVM di origine, crea un criterio SnapMirror S3 se non ne hai uno esistente e non vuoi utilizzare il criterio predefinito:

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

   Parametri:

   - `continuous` – L'unico tipo di criterio per le relazioni SnapMirror S3 (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

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

5. Installare i certificati CA sulle SVM amministrative dei cluster di origine e di destinazione:

   a. Nel cluster di origine, installare il certificato CA che ha firmato il certificato del server S3 *destination*:
   `security certificate install -type server-ca -vserver src_admin_svm -cert-name dest_server_certificate`

   b. Nel cluster di destinazione, installare il certificato CA che ha firmato il certificato del server S3 *source*:
   `security certificate install -type server-ca -vserver dest_admin_svm -cert-name src_server_certificate`+ se si utilizza un certificato firmato da un vendor CA esterno, installare lo stesso certificato sulla SVM amministrativa di origine e destinazione.

   Ulteriori informazioni su `security certificate install` nella "Riferimento al comando ONTAP".

6. Sulla SVM di origine, creare una relazione SnapMirror S3:

   `snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy policy_name]`

È possibile utilizzare un criterio creato o accettare quello predefinito.

Esempio

```
src_cluster::> snapmirror create -source-path vs0:/bucket/test-
bucket -destination-path vs1:/bucket/test-bucket-mirror -policy
test-policy
```

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

Informazioni correlate

- "creazione di snapmirror"
- "creazione di policy SnapMirror"
- "spettacolo snapmirror"

Takeover dal bucket ONTAP S3 di destinazione nel cluster remoto

Se i dati in un bucket di origine non sono più disponibili, è possibile interrompere la relazione SnapMirror per rendere il bucket di destinazione scrivibile e iniziare a fornire i dati.

A proposito di questa attività

Quando viene eseguita un'operazione di takeover, il bucket di origine viene convertito in sola lettura e il bucket di destinazione originale viene convertito in lettura-scrittura, invertendo così la relazione SnapMirror S3.

Quando il bucket sorgente disabilitato è nuovamente disponibile, SnapMirror S3 risincronizza automaticamente il contenuto dei due bucket. Non è necessario risincronizzare esplicitamente la relazione, come richiesto per le implementazioni di SnapMirror dei volumi.

L'operazione di Takeover deve essere avviata dal cluster remoto.

Sebbene SnapMirror S3 replica gli oggetti dal bucket di origine a un bucket di destinazione, non replica utenti, gruppi e policy dall'archivio di oggetti di origine all'archivio di oggetti di destinazione.

Gli utenti, le policy di gruppo, le autorizzazioni e componenti simili devono essere configurati nell'archivio di oggetti di destinazione in modo che i client possano accedere al bucket di destinazione durante un evento di failover.

Gli utenti di origine e destinazione possono utilizzare le stesse chiavi di accesso e segrete, a condizione che le chiavi di origine vengano fornite manualmente quando l'utente viene creato nel cluster di destinazione. Ad esempio:

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

System Manager

Eseguire il failover dal bucket non disponibile e iniziare a fornire i dati:

1. Fare clic su **protezione > Relazioni**, quindi selezionare **SnapMirror S3**.
2. Fare clic su ⋮, selezionare **failover**, quindi fare clic su **failover**.

CLI

1. Avviare un'operazione di failover per il bucket di destinazione:
   `snapmirror failover start -destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*
2. Verificare lo stato dell'operazione di failover:
   `snapmirror show -fields status`

   Esempio

   ```
   dest_cluster::> snapmirror failover start -destination-path
   dest_svm1:/bucket/test-bucket-mirror
   ```

Informazioni correlate

- "Aggiunta di utenti e gruppi S3 (System Manager)"
- "Creazione di un utente S3 (CLI)"
- "Creare o modificare gruppi S3 (CLI)"
- "avvio del failover di SnapMirror"
- "spettacolo snapmirror"

Ripristino di un bucket ONTAP S3 dalla SVM di destinazione sul cluster remoto

In caso di perdita o danneggiamento dei dati in un bucket di origine, sarà possibile ripopolare i dati ripristinando gli oggetti 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 utilizzato logico 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.

L'operazione di ripristino deve essere avviata dal cluster remoto.

System Manager

Ripristinare i dati di backup:

1. Fare clic su **protezione > Relazioni**, quindi selezionare **SnapMirror S3**.
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 prestazioni della nuova benna. Vedere "Livelli di servizio dello storage" per ulteriori informazioni.
     - Il contenuto del certificato CA del server S3 *destination*.
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.

Ripristinare i bucket bloccati

A partire da ONTAP 9.14.1, puoi eseguire il backup dei bucket bloccati e ripristinarli in base alle necessità.

È possibile ripristinare un bucket object-locked in un bucket nuovo o esistente. È possibile selezionare un bucket a blocco di oggetti come destinazione nei seguenti scenari:

- **Ripristina in un nuovo bucket**: Quando il blocco degli oggetti è attivato, è possibile ripristinare un bucket creando un bucket che ha anche il blocco degli oggetti attivato. Quando si ripristina un bucket bloccato, la modalità di blocco degli oggetti e il periodo di conservazione del bucket originale vengono replicati. È inoltre possibile definire un periodo di blocco diverso per la nuova benna. Questo periodo di conservazione viene applicato a oggetti non bloccati provenienti da altre origini.
- **Ripristina in un bucket esistente**: Un bucket a blocco di oggetti può essere ripristinato in un bucket esistente, purché nel bucket esistente siano attivate la versione e una simile modalità di blocco di oggetti. Viene mantenuto il mantenimento del mantenimento della posizione di ritenzione della benna originale.
- **Restore non-locked bucket**: Anche se il blocco degli oggetti non è abilitato in un bucket, è possibile ripristinarlo in un bucket che ha il blocco degli oggetti attivato e si trova nel cluster di origine. Quando si ripristina il bucket, tutti gli oggetti non bloccati vengono bloccati e la modalità di conservazione e il mantenimento del bucket di destinazione diventano applicabili.

CLI

1. Creare il nuovo bucket di destinazione per il ripristino. Per ulteriori informazioni, vedere "Creare una relazione di backup cloud per un nuovo bucket ONTAP S3".
2. Avviare un'operazione di ripristino per il bucket di destinazione:
   `snapmirror restore -source-path svm_name:/bucket/bucket_name -destination -path svm_name:/bucket/bucket_name`

Esempio

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

Ulteriori informazioni su `snapmirror restore` nella "Riferimento al comando ONTAP".

Protezione del mirroring e del backup sul cluster locale

Creare una relazione di mirroring per un nuovo bucket di ONTAP S3 nel cluster locale

Quando crei nuovi bucket S3, puoi proteggerli immediatamente in una destinazione SnapMirror S3 sullo stesso cluster. È possibile eseguire il mirroring dei dati su un bucket in una VM di storage diversa o nella stessa VM di storage di origine.

Prima di iniziare

- I requisiti per le versioni di ONTAP, le licenze e la configurazione del server S3 sono stati completati.
- Esiste una relazione di peering tra le VM storage di origine e di destinazione.
- I certificati CA sono necessari per le macchine virtuali di origine e di destinazione. È possibile utilizzare certificati CA autofirmati o certificati firmati da un vendor CA esterno.

System Manager

1. Se si tratta del primo rapporto di SnapMirror S3 per questa VM storage, verificare la presenza delle chiavi dell'utente root per le VM di storage di origine e di destinazione e rigenerarle in caso contrario:
   a. Fare clic su **Storage > Storage VM** (Storage VM), quindi selezionare la VM di storage.
   b. Nella scheda **Impostazioni**, fare clic nel riquadro S3.
   c. Nella scheda **utenti**, verificare che sia presente una chiave di accesso per l'utente root
   d. In caso contrario, fare clic su accanto a **root**, quindi fare clic su **Rigenera chiave**. Non rigenerare la chiave se ne esiste già una.
2. Modificare la VM di storage per aggiungere utenti e per aggiungere utenti ai gruppi, nelle VM di storage di origine e di destinazione: Fare clic su **Storage > Storage VM**, fare clic sulla VM di storage, fare clic su **Settings** e quindi su sotto S3.

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

3. Crea un criterio SnapMirror S3 se non ne hai già uno e non vuoi utilizzare il criterio predefinito:
   a. Fare clic su **protezione > Panoramica**, quindi fare clic su **Impostazioni criteri locali**.
   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 **continuo** per le relazioni SnapMirror S3.
      - Inserire i valori **Throttle** e **Recovery Point Objective**.
4. Crea un bucket con la protezione SnapMirror:
   a. Fare clic su **Storage > Bucket** (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,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.

   d. In **protezione**, selezionare **attiva SnapMirror (ONTAP o Cloud)**. Quindi, immettere i seguenti valori:
      - Destinazione

        - **DESTINAZIONE**: Sistema ONTAP
        - **CLUSTER**: Selezionare il cluster locale.
        - **VM di STORAGE**: Selezionare una VM di storage sul cluster locale.
        - **Certificato CA del SERVER S3**: Copia e incolla il contenuto del certificato di origine.
    - Origine
        - **Certificato CA del SERVER S3**: Copia e incolla il contenuto del certificato di destinazione.
5. Selezionare **Use the same certificate on the destination** (Usa lo stesso certificato sulla destinazione) se si utilizza un certificato firmato da un vendor CA esterno.
6. Se si fa clic su **Destination Settings** (Impostazioni destinazione), è anche possibile inserire i propri valori al posto dei valori predefiniti per il nome del bucket, la capacità e il livello di servizio delle performance.
7. Fare clic su **Save** (Salva). Viene creato un nuovo bucket nella VM per lo storage di origine e viene eseguito il mirroring in un nuovo bucket che viene creato la VM per lo storage di destinazione.

Backup delle benne bloccate

A partire da ONTAP 9.14.1, è possibile eseguire il backup di bucket S3 bloccati e ripristinarli secondo necessità.

Quando si definiscono le impostazioni di protezione per un bucket nuovo o esistente, è possibile attivare il blocco di oggetti nei bucket di destinazione, a condizione che i cluster di origine e di destinazione eseguano ONTAP 9.14.1 o versioni successive e che il blocco degli oggetti sia abilitato nel bucket di origine. La modalità di blocco degli oggetti e il mantenimento del blocco del bucket di origine diventano applicabili agli oggetti replicati nel bucket di destinazione. È inoltre possibile definire un periodo di blocco diverso per il bucket di destinazione nella sezione **Impostazioni destinazione**. Questo periodo di conservazione viene applicato anche a tutti gli oggetti non bloccati replicati dal bucket di origine e dalle interfacce S3.

Per informazioni su come attivare il blocco degli oggetti in un bucket, vedere "Creare un bucket".

CLI

1. In questo caso si tratta della prima relazione di SnapMirror S3 per questa SVM, verificare la presenza delle chiavi utente root per le SVM di origine e di destinazione e rigenerarle, se non:
   `vserver object-store-server user show`

   Verificare che sia presente 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 bucket nelle SVM di origine e di destinazione:

   ```
   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 alle policy di bucket predefinite nelle SVM di origine e di destinazione:

   ```
   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. Crea un criterio SnapMirror S3 se non ne hai già uno e non vuoi utilizzare il criterio predefinito:
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parametri:

   - `continuous` – L'unico tipo di criterio per le relazioni SnapMirror S3 (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

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

5. Installare i certificati del server CA sulla SVM amministrativa:
   a. Installare il certificato CA che ha firmato il certificato del server S3 *source* sulla SVM amministrativa:
   `security certificate install -type server-ca -vserver admin_svm -cert -name src_server_certificate`
   b. Installare il certificato CA che ha firmato il certificato del server S3 di destinazione sulla SVM amministrativa:
   `security certificate install -type server-ca -vserver admin_svm -cert -name dest_server_certificate`+ se si utilizza un certificato firmato da un vendor CA esterno, è necessario installare questo certificato solo sulla SVM amministrativa.

      Ulteriori informazioni su `security certificate install` nella "Riferimento al comando ONTAP".

6. Crea una relazione SnapMirror S3:
`snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination-path dest_peer_svm_name:/bucket/bucket_name, …} [-policy policy_name]`

   È possibile utilizzare un criterio creato o accettare quello predefinito.

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:/vs1/bucket/test-bucket-mirror
-policy test-policy
```

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

Informazioni correlate

- "creazione di snapmirror"
- "creazione di policy SnapMirror"
- "spettacolo snapmirror"

Creare una relazione di mirroring per un bucket ONTAP S3 esistente nel cluster locale

È possibile iniziare a proteggere i bucket S3 esistenti sullo stesso cluster in qualsiasi momento, ad esempio se è stata aggiornata una configurazione S3 da una release precedente a ONTAP 9.10.1. È possibile eseguire il mirroring dei dati su un bucket in una VM di storage diversa o nella stessa VM di storage di origine.

Prima di iniziare

- I requisiti per le versioni di ONTAP, le licenze e la configurazione del server S3 sono stati completati.
- Esiste una relazione di peering tra le VM storage di origine e di destinazione.
- I certificati CA sono necessari per le macchine virtuali di origine e di destinazione. È possibile utilizzare certificati CA autofirmati o certificati firmati da un vendor CA esterno.

System Manager

1. Se si tratta del primo rapporto di SnapMirror S3 per questa VM storage, verificare la presenza delle chiavi dell'utente root per le VM di storage di origine e di destinazione e rigenerarle in caso contrario:
   a. Fare clic su **Storage > Storage VM** (Storage VM), quindi selezionare la VM di storage.
   b. Nella scheda **Impostazioni**, fare clic nel riquadro **S3**.
   c. Nella scheda **utenti**, verificare che sia presente una chiave di accesso per l'utente root.
   d. In caso contrario, fare clic su accanto a **root**, quindi fare clic su **Rigenera chiave**. Non rigenerare la chiave se ne esiste già una
2. Verificare che gli utenti e i gruppi esistenti siano presenti e che abbiano accesso corretto sia nelle VM di storage di origine che di destinazione: Selezionare **Storage > Storage VM,** quindi selezionare la VM di storage, quindi la scheda **Settings**. Infine, individuare il riquadro **S3**, selezionare e selezionare la scheda **utenti**, quindi la scheda **gruppi** per visualizzare le impostazioni di accesso degli utenti e dei gruppi.

   Vedere "Aggiungere utenti e gruppi S3" per ulteriori informazioni.
3. Crea un criterio SnapMirror S3 se non ne hai già uno e non vuoi utilizzare il criterio predefinito:
   a. Fare clic su **protezione > Panoramica**, quindi su **impostazione 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 **continuo** per le relazioni SnapMirror S3.
      - Inserire i valori **Throttle** e **Recovery Point Objective**.
4. Verificare che la policy di accesso al bucket del bucket esistente continui a soddisfare le proprie esigenze:
   a. Fare clic su **Storage > Bucket** (Storage > bucket), quindi selezionare il bucket che si desidera proteggere.
   b. Nella scheda **Permissions**, fare clic su **Edit**, quindi su **Add** in **Permissions**.
      - **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. Proteggere una benna esistente con SnapMirror S3:
   a. Fare clic su **Storage** > **Bucket** e selezionare il bucket che si desidera proteggere.
   b. Fare clic su **Protect** (protezione) e immettere i seguenti valori:

- Destinazione
  - **DESTINAZIONE**: Sistema ONTAP
  - **CLUSTER**: Selezionare il cluster locale.
  - **STORAGE VM**: Consente di selezionare la stessa o una diversa storage VM.
  - **Certificato CA del SERVER S3**: Copia e incolla il contenuto del certificato *source*.
- Origine
  - **Certificato CA server S3**: Copia e incolla il contenuto del certificato *destination*.

6. Selezionare **Use the same certificate on the destination** (Usa lo stesso certificato sulla destinazione) se si utilizza un certificato firmato da un vendor CA esterno.
7. Se si fa clic su **Destination Settings** (Impostazioni destinazione), è anche possibile inserire i propri valori al posto dei valori predefiniti per il nome del bucket, la capacità e il livello di servizio delle performance.
8. Fare clic su **Save** (Salva). Viene eseguito il mirroring del bucket esistente in un nuovo bucket nella VM di storage di destinazione.

Backup delle benne bloccate

A partire da ONTAP 9.14.1, è possibile eseguire il backup di bucket S3 bloccati e ripristinarli secondo necessità.

Quando si definiscono le impostazioni di protezione per un bucket nuovo o esistente, è possibile attivare il blocco di oggetti nei bucket di destinazione, a condizione che i cluster di origine e di destinazione eseguano ONTAP 9.14.1 o versioni successive e che il blocco degli oggetti sia abilitato nel bucket di origine. La modalità di blocco degli oggetti e il mantenimento del blocco del bucket di origine diventano applicabili agli oggetti replicati nel bucket di destinazione. È inoltre possibile definire un periodo di blocco diverso per il bucket di destinazione nella sezione **Impostazioni destinazione**. Questo periodo di conservazione viene applicato anche a tutti gli oggetti non bloccati replicati dal bucket di origine e dalle interfacce S3.

Per informazioni su come attivare il blocco degli oggetti in un bucket, vedere "Creare un bucket".

CLI

1. In questo caso si tratta della prima relazione di SnapMirror S3 per questa SVM, verificare la presenza delle chiavi utente root per le SVM di origine e di destinazione e rigenerarle, se non:
   `vserver object-store-server user show`

   Verificare che sia presente 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 sulla SVM di destinazione come destinazione mirror:

   `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. Verificare che le regole di accesso alle policy di bucket predefinite siano corrette sia nelle SVM di origine che di destinazione:

`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. Crea un criterio SnapMirror S3 se non ne hai già uno e non vuoi utilizzare il criterio predefinito:

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

   Parametri:

   - `continuous` – L'unico tipo di criterio per le relazioni SnapMirror S3 (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. Installare i certificati del server CA sulla SVM amministrativa:

   a. Installare il certificato CA che ha firmato il certificato del server S3 *source* sulla SVM amministrativa:
   `security certificate install -type server-ca -vserver *admin_svm* -cert -name *src_server_certificate*`

   b. Installare il certificato CA che ha firmato il certificato del server S3 di destinazione sulla SVM amministrativa:
   `security certificate install -type server-ca -vserver *admin_svm* -cert -name *dest_server_certificate*`+ se si utilizza un certificato firmato da un vendor CA esterno, è necessario installare questo certificato solo sulla SVM amministrativa.

   Ulteriori informazioni su `security certificate install` nella "Riferimento al comando ONTAP".

6. Crea una relazione SnapMirror S3:
   `snapmirror create -source-path *src_svm_name*:/bucket/*bucket_name* -destination-path *dest_peer_svm_name*:/bucket/*bucket_name*, …} [-policy policy_name]`

È possibile utilizzare un criterio creato o accettare quello predefinito.

Esempio

```
src_cluster::> snapmirror create -source-path vs0-src:/bucket/test-
bucket -destination-path vs1-dest:/bucket/test-bucket-mirror -policy
test-policy
```

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

Informazioni correlate

- "creazione di snapmirror"
- "creazione di policy SnapMirror"
- "spettacolo snapmirror"

Takeover del bucket ONTAP S3 di destinazione nel cluster locale

Se i dati in un bucket di origine non sono più disponibili, è possibile interrompere la relazione SnapMirror per rendere il bucket di destinazione scrivibile e iniziare a fornire i dati.

A proposito di questa attività

Quando viene eseguita un'operazione di takeover, il bucket di origine viene convertito in sola lettura e il bucket di destinazione originale viene convertito in lettura-scrittura, invertendo così la relazione SnapMirror S3.

Quando il bucket sorgente disabilitato è nuovamente disponibile, SnapMirror S3 risincronizza automaticamente il contenuto dei due bucket. Non è necessario risincronizzare esplicitamente la relazione, come richiesto per le implementazioni di SnapMirror di volumi standard.

Se il bucket di destinazione si trova su un cluster remoto, l'operazione di Takeover deve essere avviata dal cluster remoto.

System Manager

Eseguire il failover dal bucket non disponibile e iniziare a fornire i dati:

1. Fare clic su **protezione > Relazioni**, quindi selezionare **SnapMirror S3**.
2. Fare clic su ⋮, selezionare **failover**, quindi fare clic su **failover**.

CLI

1. Avviare un'operazione di failover per il bucket di destinazione:
   `snapmirror failover start -destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*
2. Verificare lo stato dell'operazione di failover:
   `snapmirror show -fields status`

Esempio

```
clusterA::> snapmirror failover start -destination-path vs1:/bucket/test-
bucket-mirror
```

Informazioni correlate

- "avvio del failover di SnapMirror"
- "spettacolo snapmirror"

Ripristino di un bucket ONTAP S3 dalla SVM di destinazione sul cluster locale

In caso di perdita o danneggiamento dei dati in un bucket di origine, sarà possibile ripopolare i dati ripristinando gli oggetti 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 utilizzato logico 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.

L'operazione di ripristino deve essere avviata dal cluster locale.

System Manager

Ripristinare i dati di backup:

1. Fare clic su **protezione > Relazioni**, quindi selezionare il bucket.
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.
4. Copiare e incollare il contenuto del certificato CA del server S3 di destinazione.
   - 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 prestazioni della nuova benna. Vedere "Livelli di servizio dello storage" per ulteriori informazioni.
     - Contenuto del certificato CA del server S3 di destinazione.
5. In **destinazione**, copiare e incollare il contenuto del certificato CA del server S3 di origine.
6. Fare clic su **protezione** > Relazioni per monitorare l'avanzamento del ripristino.

Ripristinare i bucket bloccati

A partire da ONTAP 9.14.1, puoi eseguire il backup dei bucket bloccati e ripristinarli in base alle necessità.

È possibile ripristinare un bucket object-locked in un bucket nuovo o esistente. È possibile selezionare un bucket a blocco di oggetti come destinazione nei seguenti scenari:

- **Ripristina in un nuovo bucket**: Quando il blocco degli oggetti è attivato, è possibile ripristinare un bucket creando un bucket che ha anche il blocco degli oggetti attivato. Quando si ripristina un bucket bloccato, la modalità di blocco degli oggetti e il periodo di conservazione del bucket originale vengono replicati. È inoltre possibile definire un periodo di blocco diverso per la nuova benna. Questo periodo di conservazione viene applicato a oggetti non bloccati provenienti da altre origini.
- **Ripristina in un bucket esistente**: Un bucket a blocco di oggetti può essere ripristinato in un bucket esistente, purché nel bucket esistente siano attivate la versione e una simile modalità di blocco di oggetti. Viene mantenuto il mantenimento del mantenimento della posizione di ritenzione della benna originale.
- **Restore non-locked bucket**: Anche se il blocco degli oggetti non è abilitato in un bucket, è possibile ripristinarlo in un bucket che ha il blocco degli oggetti attivato e si trova nel cluster di origine. Quando si ripristina il bucket, tutti gli oggetti non bloccati vengono bloccati e la modalità di conservazione e il mantenimento del bucket di destinazione diventano applicabili.

CLI

1. Se si ripristinano oggetti in un nuovo bucket, creare il nuovo bucket. Per ulteriori informazioni, vedere "Creare una relazione di backup cloud per un nuovo bucket ONTAP S3".
2. Avviare un'operazione di ripristino per il bucket di destinazione:
   `snapmirror restore -source-path svm_name:/bucket/bucket_name -destination -path svm_name:/bucket/bucket_name`

Esempio

```
clusterA::> snapmirror restore -source-path vs0:/bucket/test-bucket
-destination-path vs1:/bucket/test-bucket-mirror
```

Ulteriori informazioni su `snapmirror restore` nella "Riferimento al comando ONTAP".

Protezione del backup con destinazioni cloud

Requisiti per le relazioni delle destinazioni cloud ONTAP SnapMirror S3

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

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

Intercluster LIF e un IPSpace devono essere configurati sul cluster prima che il cluster possa connettersi a un archivio di oggetti cloud. È consigliabile creare LIF intercluster in ciascun nodo per un trasferimento perfetto dei 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 VM di archiviazione di amministrazione del cluster ONTAP S3 utilizzando `security certificate install` comando. 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 amministrativo del cluster ONTAP deve essere in grado di risolvere gli FQDN (se utilizzati) agli indirizzi IP.

Informazioni correlate

- "installazione del certificato di sicurezza"

Creare una relazione di backup cloud per un nuovo bucket ONTAP S3

Quando crei nuovi bucket S3, puoi eseguirne immediatamente il backup su un bucket di destinazione SnapMirror S3 su un provider di archiviazione oggetti, che può essere un sistema StorageGRID o una distribuzione 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 VM**, fare clic sulla VM di archiviazione, fare clic su **Impostazioni**, quindi su **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. Crea un criterio SnapMirror S3 se non ne hai già uno e non vuoi utilizzare il criterio predefinito:
   a. Fare clic su **protezione > Panoramica**, quindi fare clic su **Impostazioni criteri locali**.
   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 **continuo** per le relazioni SnapMirror S3.
      - 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 utenti o accettare le impostazioni predefinite.
      - **Azioni**: Accertarsi che siano visualizzati i seguenti valori:

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

      - **Risorse**: Utilizzare i valori predefiniti `_(bucketname, bucketname/*)` o altri valori

necessari.

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 si tratta del primo rapporto di SnapMirror S3 per questa SVM, verificare la presenza delle chiavi dell'utente root per le SVM di origine e di destinazione e rigenerarle in caso contrario:
`vserver object-store-server user show` + confermare la presenza di 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 già esistente.

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. Crea un criterio SnapMirror S3 se non ne hai già uno e non vuoi utilizzare il criterio 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 SnapMirror S3 (obbligatorio). * `-rpo` – specifica il tempo per l'obiettivo del punto di ripristino, in secondi (facoltativo). * `-throttle` – specifica il limite superiore 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`

   Ulteriori informazioni su `security certificate install` nella "Riferimento al comando ONTAP".

6. Definire l'archivio oggetti di destinazione 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`

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

   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. Crea 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`

Informazioni correlate

- "creazione di snapmirror"

- "creazione di policy SnapMirror"
- "spettacolo snapmirror"

Creare una relazione di backup cloud per un bucket ONTAP S3 esistente

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 **archiviazione > VM di archiviazione**, fare clic sulla VM di archiviazione, fare clic su **Impostazioni**, quindi fare clic su sotto S3.

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

2. Crea un criterio SnapMirror S3 se non ne hai già uno e non vuoi utilizzare il criterio 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 **continuo** per le relazioni SnapMirror S3.
   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 **Edit**, quindi su **Add** in **Permissions**.
      - **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 della benna utilizzando SnapMirror S3:
   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. Crea un criterio SnapMirror S3 se non ne hai già uno e non vuoi utilizzare il criterio 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 SnapMirror S3 (obbligatorio). * `-rpo` – specifica il tempo per l'obiettivo del punto di ripristino, in secondi (facoltativo). * `-throttle` – specifica il limite superiore 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`

   Ulteriori informazioni su `security certificate install` nella "Riferimento al comando ONTAP".

4. Definire l'archivio oggetti di destinazione 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`

   Parametri: * `-object-store-name` – Il nome della destinazione dell'archivio oggetti nel sistema

ONTAP locale. * `-usage` – utilizzare `data` per questo flusso di lavoro. Sono supportati i target * `-provider-type` – `AWS_S3` e `SGWS` (StorageGRID). * `-server` – L'indirizzo FQDN o IP del server di destinazione. * `-is-ssl-enabled` – L'attivazione di SSL è facoltativa ma consigliata. + ulteriori informazioni su `snapmirror object-store config create` nella "Riferimento al comando ONTAP".

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. Crea 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`

Informazioni correlate

- "creazione di snapmirror"
- "creazione di policy SnapMirror"
- "spettacolo snapmirror"

Ripristino di un bucket ONTAP S3 da una destinazione 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 **SnapMirror S3**.
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
   ```

   Ulteriori informazioni su `snapmirror restore` nella "Riferimento al comando ONTAP".

Modificare un criterio ONTAP SnapMirror S3

È possibile modificare un criterio SnapMirror S3 quando si desidera regolare i valori di RPO e acceleratore.

System Manager

1. Fare clic su **protezione > Relazioni**, quindi selezionare il criterio di protezione per la relazione che si desidera modificare.
2. Fare clic su ⋮ accanto al nome del criterio, quindi fare clic su **Modifica**.

CLI

Modificare un criterio SnapMirror S3:
`snapmirror policy modify -vserver <svm_name> -policy <policy_name> [-rpo <integer>] [-throttle <throttle_type>] [-comment <text>]`

Parametri:

- `-rpo`: Specifica il tempo per l'obiettivo del punto di ripristino, in secondi.
- `-throttle`: Specifica il limite superiore di throughput/larghezza di banda, in kilobyte/secondi.

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

Informazioni correlate

- "modifica della politica di SnapMirror"

Informazioni sul copyright

Informazioni sul marchio commerciale