Protezione del mirroring e del backup su un cluster remoto

ONTAP 9

NetApp
April 24, 2024

Sommario

Protezione del mirroring e del backup su un cluster remoto

Creare una relazione mirror per un nuovo bucket (cluster remoto)

Quando si creano nuovi bucket S3, è possibile proteggerli immediatamente a una destinazione S3 SnapMirror 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 della prima relazione di S3 SnapMirror per questa VM di storage, verificare che le chiavi utente root esistano sia per le VM di storage di origine che 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 su 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 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.

3. Nel cluster di origine, creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera 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 **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). 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. 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
   ```

   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. Nella SVM di origine, crea una policy SnapMirror S3 se non ne hai già una e non vuoi utilizzare la policy predefinita:
   `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 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

     ```
     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.

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

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`

Creare una relazione mirror per un bucket esistente (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 della prima relazione di S3 SnapMirror per questa VM di storage, verificare che le chiavi utente root esistano sia per le VM di storage di origine che di destinazione e rigenerarle in caso contrario:
   a. Selezionare **Storage > Storage VM**, quindi selezionare la VM di storage.
   b. Nella scheda **Impostazioni**, fare clic su 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 l'accesso a utenti e gruppi sia corretto sia nelle macchine virtuali storage di origine che di destinazione:
   Selezionare **Storage > Storage VM,** quindi selezionare la VM di archiviazione, quindi **Settings**. Infine, selezionare Sotto **S3**.

   Vedere "Aggiungere utenti e gruppi S3" per ulteriori informazioni.
3. Nel cluster di origine, creare un criterio S3 SnapMirror se non si dispone di un criterio esistente e non si desidera 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. 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**.
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 **Modifica**, quindi fare clic su **Aggiungi** in **permessi**.
      - **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. Proteggi un bucket esistente con la protezione di S3 SnapMirror:
   a. Fare clic su **Storage** > **Bucket**, quindi 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 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`+ verificare 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 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 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. Sulla SVM di origine, creare un criterio S3 SnapMirror se non si dispone di uno esistente e non si desidera 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 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

     ```
     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.

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

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`

Acquisizione e distribuzione dei dati dal bucket di destinazione (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 di S3 SnapMirror.

Quando il bucket di origine disattivato è nuovamente disponibile, S3 SnapMirror 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.

System Manager

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

1. Fare clic su **protezione > Relazioni**, quindi selezionare **S3 SnapMirror**.
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
   ```

Ripristinare un bucket dalla VM di storage di destinazione (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 **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 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 per un nuovo bucket (target cloud)".
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
```