Spiegelung und Backup-Schutz auf dem lokalen Cluster

ONTAP 9

NetApp
May 09, 2024

Inhalt

Spiegelung und Backup-Schutz auf dem lokalen Cluster

Erstellen einer Spiegelbeziehung für einen neuen Bucket (lokales Cluster)

Wenn Sie neue S3-Buckets erstellen, können Sie sie unmittelbar in einem S3-SnapMirror-Ziel im selben Cluster sichern. Sie können Daten auf einen Bucket in einer anderen Storage-VM oder auf derselben Storage-VM wie die Quelle spiegeln.

Bevor Sie beginnen

- Die Anforderungen für ONTAP-Versionen, Lizenzierung und S3-Serverkonfiguration wurden erfüllt.
- Zwischen Quell- und Ziel-Storage-VMs besteht eine Peering-Beziehung.
- FÜR die Quell- und Ziel-VMs SIND CA-Zertifikate erforderlich. Sie können selbstsignierte CA-Zertifikate oder -Zertifikate verwenden, die von einem externen CA-Anbieter signiert wurden.

System Manager

1. Wenn dies die erste S3 SnapMirror Beziehung für diese Storage-VM ist, überprüfen Sie, ob die Root-Benutzerschlüssel für Quell- und Ziel-Storage VMs vorhanden sind, und generieren Sie sie erneut, wenn sie nicht:
   a. Klicken Sie auf **Storage > Storage VMs** und wählen Sie dann die Speicher-VM aus.
   b. Klicken Sie auf der Registerkarte **Einstellungen** auf Im S3-Tile.
   c. Überprüfen Sie auf der Registerkarte **Benutzer**, ob für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist
   d. Falls nicht, klicken Sie auf Klicken Sie neben **root** auf **Schlüssel neu generieren**. Generieren Sie den Schlüssel nicht neu, wenn er bereits vorhanden ist.
2. Bearbeiten Sie die Speicher-VM, um Benutzer hinzuzufügen und um Benutzer zu Gruppen hinzuzufügen, sowohl in den Quell- und Ziel-Speicher-VMs: Klicken Sie auf **Storage > Speicher-VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und klicken Sie dann auf Unter S3.

   Siehe "Fügen Sie S3-Benutzer und -Gruppen hinzu" Finden Sie weitere Informationen.
3. Erstellen Sie eine S3 SnapMirror Politik wenn Sie keine bestehende haben und Sie die Standardrichtlinie nicht verwenden möchten:
   a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Einstellungen für lokale Richtlinien**.
   b. Klicken Sie Auf Klicken Sie neben **Schutzrichtlinien** auf **Hinzufügen**.
      - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
      - Wählen Sie den Richtlinienumfang, das Cluster oder die SVM aus
      - Wählen Sie * Continuous* für S3 SnapMirror Beziehungen.
      - Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
4. Erstellung eines Buckets mit SnapMirror Sicherung:
   a. Klicken Sie auf **Storage > Buckets** und dann auf **Hinzufügen**.
   b. Geben Sie einen Namen ein, wählen Sie die Speicher-VM aus, geben Sie eine Größe ein und klicken Sie dann auf **Weitere Optionen**.
   c. Klicken Sie unter **Berechtigungen** auf **Hinzufügen**. Die Überprüfung der Berechtigungen ist optional, wird aber empfohlen.
      - **Principal** und **Effect** - Wählen Sie Werte aus, die Ihren Benutzergruppeneinstellungen entsprechen, oder übernehmen Sie die Standardeinstellungen.
      - **Aktionen** - stellen Sie sicher, dass die folgenden Werte angezeigt werden:

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

      - **Ressourcen** - Verwenden Sie die Standardeinstellungen `(bucketname, bucketname/*)` Oder andere Werte, die Sie benötigen

        Siehe "Management des Benutzerzugriffs auf Buckets" Weitere Informationen zu diesen Feldern.

d. Aktivieren Sie unter **Schutz Enable SnapMirror (ONTAP oder Cloud)**. Geben Sie anschließend die folgenden Werte ein:
   - Ziel
     - **ZIEL**: ONTAP-System
     - **CLUSTER**: Wählen Sie den lokalen Cluster aus.
     - **STORAGE VM**: Wählen Sie eine Storage VM auf dem lokalen Cluster aus.
     - **S3 SERVER CA-ZERTIFIKAT**: Kopieren Sie den Inhalt des Quellzertifikats und fügen Sie ihn ein.
   - Quelle
     - **S3 SERVER CA-ZERTIFIKAT**: Kopieren Sie den Inhalt des Zielzertifikats und fügen Sie ihn ein.

5. Überprüfen Sie **Verwenden Sie dasselbe Zertifikat auf dem Ziel**, wenn Sie ein Zertifikat verwenden, das von einem externen CA-Anbieter signiert wurde.
6. Wenn Sie auf **Zieleinstellungen** klicken, können Sie Ihre eigenen Werte anstelle der Standardeinstellungen für Bucket-Name, -Kapazität und -Service-Level eingeben.
7. Klicken Sie Auf **Speichern**. Ein neuer Bucket wird in der Quell-Storage-VM erstellt und in einem neuen Bucket gespiegelt, der die Ziel-Storage-VM erstellt wurde.

Sichern Sie gesperrte Buckets

Ab ONTAP 9.14.1 können Sie gesperrte S3-Buckets sichern und nach Bedarf wiederherstellen.

Wenn Sie die Schutzeinstellungen für einen neuen oder vorhandenen Bucket definieren, können Sie die Objektsperrung für Ziel-Buckets aktivieren, sofern auf den Quell- und Ziel-Clustern ONTAP 9.14.1 oder höher ausgeführt wird und die Objektsperrung auf dem Quell-Bucket aktiviert ist. Der Sperrmodus für Objekte und die Aufbewahrungsdauer der Quell-Buckets werden für die replizierten Objekte auf dem Ziel-Bucket angewendet. Sie können auch eine andere Sperrfrist für den Ziel-Bucket im Abschnitt **Zieleinstellungen** definieren. Dieser Aufbewahrungszeitraum wird auch auf alle nicht gesperrten Objekte angewendet, die aus den Quell-Bucket und S3-Schnittstellen repliziert werden.

Informationen zum Aktivieren der Objektsperrung auf einem Bucket finden Sie unter "Erstellen eines Buckets".

CLI

1. Wenn dies die erste S3 SnapMirror Beziehung für diese SVM ist, überprüfen Sie, ob die Root-Benutzerschlüssel für Quell- und Ziel-SVMs vorhanden sind, und generieren Sie sie erneut, wenn sie dies nicht tun:
   ```
   vserver object-store-server user show
   ```

   Vergewissern Sie sich, dass für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist. Falls nicht, geben Sie Folgendes ein:
   ```
   vserver object-store-server user regenerate-keys -vserver svm_name -user
   root
   ```

   Generieren Sie den Schlüssel nicht neu, wenn er bereits vorhanden ist.

2. Buckets für die Quell- und Ziel-SVMs erstellen:

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

[*additional_options*]

3. Fügen Sie Zugriffsregeln den Standard-Bucket-Richtlinien sowohl in den Quell- als auch in Ziel-SVMs hinzu:

   `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. Erstellen Sie eine S3 SnapMirror Politik wenn Sie keine bestehende haben und Sie die Standardrichtlinie nicht verwenden möchten:
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parameter:

   - `continuous` – Der einzige Richtlinientyp für S3 SnapMirror Beziehungen (erforderlich).
   - `-rpo` – Gibt die Zeit für den Wiederherstellungspunkt in Sekunden an (optional).
   - `-throttle` – Gibt die obere Grenze für Durchsatz/Bandbreite in Kilobyte/Sekunden an (optional).

     Beispiel

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

5. Installieren Sie CA-Serverzertifikate auf der Admin-SVM:

   a. Installieren Sie das CA-Zertifikat, das das Zertifikat des *Source* S3-Servers auf der Admin-SVM signiert hat:
      `security certificate install -type server-ca -vserver admin_svm -cert -name src_server_certificate`

   b. Installieren Sie das CA-Zertifikat, das das Zertifikat des *Destination* S3-Servers auf der Admin-SVM signiert hat:
      `security certificate install -type server-ca -vserver admin_svm -cert -name dest_server_certificate`+ Wenn Sie ein Zertifikat verwenden, das von einem externen CA-Anbieter signiert wurde, müssen Sie dieses Zertifikat nur auf der Admin-SVM installieren.

      Siehe `security certificate install` Man-Page für Details.

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

   Sie können eine von Ihnen erstellte Richtlinie verwenden oder die Standardeinstellung übernehmen.

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

7. Überprüfen Sie, ob die Spiegelung aktiv ist:
   `snapmirror show -policy-type continuous -fields status`

Erstellen einer Spiegelbeziehung für einen vorhandenen Bucket (lokales Cluster)

Sie können vorhandene S3-Buckets für das gleiche Cluster jederzeit schützen, wenn Sie beispielsweise eine S3-Konfiguration von einer Version vor ONTAP 9.10.1 aktualisiert haben. Sie können Daten auf einen Bucket in einer anderen Storage-VM oder auf derselben Storage-VM wie die Quelle spiegeln.

Bevor Sie beginnen

- Die Anforderungen für ONTAP-Versionen, Lizenzierung und S3-Serverkonfiguration wurden erfüllt.
- Zwischen Quell- und Ziel-Storage-VMs besteht eine Peering-Beziehung.
- FÜR die Quell- und Ziel-VMs SIND CA-Zertifikate erforderlich. Sie können selbstsignierte CA-Zertifikate oder -Zertifikate verwenden, die von einem externen CA-Anbieter signiert wurden.

System Manager

1. Wenn dies die erste S3 SnapMirror Beziehung für diese Storage-VM ist, überprüfen Sie, ob die Root-Benutzerschlüssel für Quell- und Ziel-Storage VMs vorhanden sind, und generieren Sie sie erneut, wenn sie nicht:
   a. Klicken Sie auf **Storage > Storage VMs** und wählen Sie dann die Speicher-VM aus.
   b. Klicken Sie auf der Registerkarte **Einstellungen** auf In der Kachel **S3**.
   c. Überprüfen Sie auf der Registerkarte **Benutzer**, ob für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist.
   d. Falls nicht, klicken Sie auf Klicken Sie neben **root** auf **Schlüssel neu generieren**. Generieren Sie den Schlüssel nicht neu, wenn er bereits vorhanden ist
2. Vergewissern Sie sich, dass der Benutzer- und Gruppenzugriff sowohl auf den Quell- als auch auf den Ziel-Storage-VMs korrekt ist:
   - Klicken Sie auf **Storage > Storage VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und dann auf Unter S3.

     Siehe "Fügen Sie S3-Benutzer und -Gruppen hinzu" Finden Sie weitere Informationen.
3. Erstellen Sie eine S3 SnapMirror Politik wenn Sie keine bestehende haben und Sie die Standardrichtlinie nicht verwenden möchten:
   a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Lokale Richtlinieneinstellung**.
   b. Klicken Sie Auf Klicken Sie neben **Schutzrichtlinien** auf **Hinzufügen**.
      - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
      - Wählen Sie den Richtlinienumfang, das Cluster oder die SVM aus
      - Wählen Sie * Continuous* für S3 SnapMirror Beziehungen.
      - Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
4. Vergewissern Sie sich, dass die Bucket-Zugriffsrichtlinie des vorhandenen Buckets nach wie vor die Anforderungen erfüllt:
   a. Klicken Sie auf **Speicher > Eimer** und wählen Sie dann den Eimer aus, den Sie schützen möchten.
   b. Klicken Sie auf der Registerkarte **Berechtigungen** auf **Bearbeiten**, dann klicken Sie unter **Berechtigungen** auf **Hinzufügen**.
      - **Principal** und **Effect** - Wählen Sie Werte aus, die Ihren Benutzergruppeneinstellungen entsprechen, oder übernehmen Sie die Standardeinstellungen.
      - **Aktionen** - stellen Sie sicher, dass die folgenden Werte angezeigt werden:

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

      - **Ressourcen** - Verwenden Sie die Standardeinstellungen *(bucketname, bucketname/*)* Oder andere Werte, die Sie benötigen.

        Siehe "Management des Benutzerzugriffs auf Buckets" Weitere Informationen zu diesen Feldern.

5. Schutz eines vorhandenen Buckets durch S3 SnapMirror:
   a. Klicken Sie auf **Storage** > **Buckets** und wählen Sie dann den Eimer aus, den Sie schützen möchten.
   b. Klicken Sie auf **Protect** und geben Sie die folgenden Werte ein:
      - Ziel
        - **ZIEL**: ONTAP-System
        - **CLUSTER**: Wählen Sie den lokalen Cluster aus.
        - **STORAGE VM**: Wählen Sie dieselbe oder eine andere Storage VM.
        - **S3-SERVER-CA-ZERTIFIKAT**: Kopieren Sie den Inhalt des *source*-Zertifikats.
      - Quelle
        - **S3-SERVER-CA-ZERTIFIKAT**: Kopieren Sie den Inhalt des *Destination*-Zertifikats.
6. Überprüfen Sie **Verwenden Sie dasselbe Zertifikat auf dem Ziel**, wenn Sie ein Zertifikat verwenden, das von einem externen CA-Anbieter signiert wurde.
7. Wenn Sie auf **Zieleinstellungen** klicken, können Sie Ihre eigenen Werte anstelle der Standardeinstellungen für Bucket-Name, -Kapazität und -Service-Level eingeben.
8. Klicken Sie Auf **Speichern**. Der vorhandene Bucket wird zu einem neuen Bucket in der Ziel-Storage-VM gespiegelt.

Sichern Sie gesperrte Buckets

Ab ONTAP 9.14.1 können Sie gesperrte S3-Buckets sichern und nach Bedarf wiederherstellen.

Wenn Sie die Schutzeinstellungen für einen neuen oder vorhandenen Bucket definieren, können Sie die Objektsperrung für Ziel-Buckets aktivieren, sofern auf den Quell- und Ziel-Clustern ONTAP 9.14.1 oder höher ausgeführt wird und die Objektsperrung auf dem Quell-Bucket aktiviert ist. Der Sperrmodus für Objekte und die Aufbewahrungsdauer der Quell-Buckets werden für die replizierten Objekte auf dem Ziel-Bucket angewendet. Sie können auch eine andere Sperrfrist für den Ziel-Bucket im Abschnitt **Zieleinstellungen** definieren. Dieser Aufbewahrungszeitraum wird auch auf alle nicht gesperrten Objekte angewendet, die aus den Quell-Bucket und S3-Schnittstellen repliziert werden.

Informationen zum Aktivieren der Objektsperrung auf einem Bucket finden Sie unter "Erstellen eines Buckets".

CLI

1. Wenn dies die erste S3 SnapMirror Beziehung für diese SVM ist, überprüfen Sie, ob die Root-Benutzerschlüssel für Quell- und Ziel-SVMs vorhanden sind, und generieren Sie sie erneut, wenn sie dies nicht tun:
   `vserver object-store-server user show`

   Vergewissern Sie sich, dass für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist. Falls nicht, geben Sie Folgendes ein:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   Generieren Sie den Schlüssel nicht neu, wenn er bereits vorhanden ist.

2. Erstellen eines Buckets für die Ziel-SVM als Ziel-Ziel:

   `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. Vergewissern Sie sich, dass die Zugriffsregeln für die Standard-Bucket-Richtlinien sowohl in den Quell- als auch in den Ziel-SVMs korrekt sind:

   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*]`

   Beispiel

   ```
   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. Erstellen Sie eine S3 SnapMirror Politik wenn Sie keine bestehende haben und Sie die Standardrichtlinie nicht verwenden möchten:

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

   Parameter:

   - `continuous` – Der einzige Richtlinientyp für S3 SnapMirror Beziehungen (erforderlich).
   - `-rpo` – Gibt die Zeit für den Wiederherstellungspunkt in Sekunden an (optional).
   - `-throttle` – Gibt die obere Grenze für Durchsatz/Bandbreite in Kilobyte/Sekunden an (optional).

     Beispiel

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

5. Installieren Sie CA-Serverzertifikate auf der Admin-SVM:

   a. Installieren Sie das CA-Zertifikat, das das Zertifikat des *Source* S3-Servers auf der Admin-SVM signiert hat:
      security certificate install -type server-ca -vserver *admin_svm* -cert -name *src_server_certificate*

   b. Installieren Sie das CA-Zertifikat, das das Zertifikat des *Destination* S3-Servers auf der Admin-SVM signiert hat:
      security certificate install -type server-ca -vserver *admin_svm* -cert -name *dest_server_certificate*+ Wenn Sie ein Zertifikat verwenden, das von einem externen CA-Anbieter signiert wurde, müssen Sie dieses Zertifikat nur auf der Admin-SVM installieren.

Siehe `security certificate install` Man-Page für Details.

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

   Sie können eine von Ihnen erstellte Richtlinie verwenden oder die Standardeinstellung übernehmen.

   Beispiel

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

7. Überprüfen Sie, ob die Spiegelung aktiv ist:
   `snapmirror show -policy-type continuous -fields status`

Übernahme und Bereitstellung von Daten aus dem Ziel-Bucket (lokaler Cluster)

Wenn die Daten in einem Quell-Bucket nicht mehr verfügbar sind, können Sie die SnapMirror Beziehung unterbrechen, um den Ziel-Bucket beschreibbar zu machen und mit der Bereitstellung von Daten zu beginnen.

Über diese Aufgabe

Wenn ein Takeover-Vorgang durchgeführt wird, wird der Quell-Bucket in schreibgeschützt umgewandelt und der ursprüngliche Ziel-Bucket in Lese-/Schreibzugriff umgewandelt, sodass die S3 SnapMirror Beziehung rückgängig gemacht wird.

Wenn der deaktivierte Quell-Bucket wieder verfügbar ist, werden die Inhalte der beiden Buckets von S3 SnapMirror automatisch neu synchronisiert. Sie müssen die Beziehung nicht explizit neu synchronisieren, wie es für standardmäßige Volume SnapMirror Implementierungen erforderlich ist.

Wenn der Ziel-Bucket auf einem Remote-Cluster liegt, muss der Takeover-Vorgang vom Remote-Cluster aus initiiert werden.

System Manager

Failover aus dem nicht verfügbaren Bucket und Beginn der Datenbereitstellung:

1. Klicken Sie auf **Schutz > Beziehungen** und wählen Sie dann **S3 SnapMirror**.
2. Klicken Sie Auf ⋮ Wählen Sie **Failover** und klicken Sie dann auf **Failover**.

CLI

1. Initiieren eines Failover-Vorgangs für den Ziel-Bucket:
   `snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. Überprüfen Sie den Status des Failover-Vorgangs:
   `snapmirror show -fields status`

Beispiel

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

Wiederherstellen eines Buckets aus der Ziel-Storage-VM (lokales Cluster)

Wenn Daten in einem Quell-Bucket verloren gehen oder beschädigt sind, können Sie Ihre Daten neu befüllen, indem Sie Objekte aus einem Ziel-Bucket wiederherstellen.

Über diese Aufgabe

Sie können den Ziel-Bucket auf einem vorhandenen oder einem neuen Bucket wiederherstellen. Der Ziel-Bucket für den Wiederherstellungsvorgang muss größer sein als der logische genutzte Zielspeicherplatz.

Wenn Sie einen vorhandenen Bucket verwenden, muss er beim Starten eines Wiederherstellungsvorgangs leer sein. Beim Restore wird ein Bucket nicht rechtzeitig „zurück“, sondern es füllt einen leeren Bucket mit den vorherigen Inhalten aus.

Der Wiederherstellungsvorgang muss vom lokalen Cluster aus gestartet werden.

System Manager

Wiederherstellen der Backup-Daten:

1. Klicken Sie auf **Schutz > Beziehungen** und wählen Sie dann den Bucket aus.
2. Klicken Sie Auf ⋮ Und wählen Sie dann **Wiederherstellen**.
3. Wählen Sie unter **Quelle vorhandener Bucket** (Standard) oder **Neuer Bucket** aus.
   - Um einen **vorhandenen Bucket** (die Standardeinstellung) wiederherzustellen, führen Sie die folgenden Aktionen aus:
     - Wählen Sie das Cluster und die Storage-VM aus, um nach dem vorhandenen Bucket zu suchen.
     - Wählen Sie den vorhandenen Bucket aus.
4. Kopieren Sie den Inhalt des S3-Zielserver-CA-Zertifikats und fügen Sie ihn ein.
   - Um einen **neuen Bucket** wiederherzustellen, geben Sie die folgenden Werte ein:
     - Der Cluster und die Storage-VM zum Hosten des neuen Buckets.
     - Name, Kapazität und Performance des neuen Bucket
       Siehe "Storage Service Level" Finden Sie weitere Informationen.
     - Der Inhalt des CA-Zertifikats des Ziel-S3-Servers.
5. Kopieren Sie unter **Destination** den Inhalt des Quell-S3-Server-CA-Zertifikats und fügen Sie ihn ein.
6. Klicken Sie auf **Schutz** > Beziehungen, um den Wiederherstellungsfortschritt zu überwachen.

Gesperrte Buckets wiederherstellen

Ab ONTAP 9.14.1 können Sie gesperrte Buckets sichern und nach Bedarf wiederherstellen.

Sie können einen objektgesperrten Bucket in einem neuen oder bestehenden Bucket wiederherstellen. In den folgenden Szenarien können Sie einen objektgesperrten Bucket als Ziel auswählen:

- **Wiederherstellung auf einen neuen Bucket**: Wenn die Objektsperrung aktiviert ist, kann ein Bucket wiederhergestellt werden, indem ein Bucket erstellt wird, für den auch die Objektsperrung aktiviert ist. Wenn Sie einen gesperrten Bucket wiederherstellen, werden der Objektsperrmodus und der Aufbewahrungszeitraum des ursprünglichen Buckets repliziert. Sie können auch eine andere Sperrfrist für den neuen Bucket definieren. Diese Aufbewahrungsfrist wird auf nicht gesperrte Objekte aus anderen Quellen angewendet.
- **Wiederherstellung auf einen vorhandenen Bucket**: Ein Object-Locked Bucket kann in einen bestehenden Bucket wiederhergestellt werden, sofern auf dem bestehenden Bucket Versionierung und ein ähnlicher Object-Locking-Modus aktiviert sind. Die Aufbewahrungsdauer des ursprünglichen Eimers wird beibehalten.
- **Nicht gesperrte Buckets wiederherstellen**: Selbst wenn die Objektsperrung auf einem Bucket nicht aktiviert ist, können Sie sie in einem Bucket wiederherstellen, der die Objektsperrung aktiviert hat und sich auf dem Quellcluster befindet. Wenn Sie den Bucket wiederherstellen, werden alle nicht gesperrten Objekte gesperrt, und der Aufbewahrungszeitraum und die Dauer des Ziel-Buckets werden für sie anwendbar.

CLI

1. Wenn Sie Objekte in einem neuen Bucket wiederherstellen, erstellen Sie den neuen Bucket. Weitere Informationen finden Sie unter "Backup-Beziehung für einen neuen Bucket erstellen (Cloud-Ziel)".
2. Initiieren eines Restore-Vorgangs für den Ziel-Bucket:

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

Beispiel

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