Buckets mit SnapMirror S3 schützen

ONTAP 9

NetApp
November 05, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/s3-snapmirror/index.html on November 05, 2026. Always check docs.netapp.com for the latest.

Inhalt

Buckets mit SnapMirror S3 schützen . . . 1
Informationen zu ONTAP SnapMirror S3 . . . 1
SnapMirror S3-Anforderungen . . . 1
Unterstützte SnapMirror Beziehungen . . . 3
Zugriff auf S3-Buckets steuern . . . 3
S3 Object Lock und Versionierung mit SnapMirror S3 . . . 3
Spiegelungs- und Backup-Schutz auf einem entfernten Cluster . . . 4
Eine Spiegelbeziehung für einen neuen ONTAP S3 Bucket auf dem Remote-Cluster erstellen . . . 4
Eine Spiegelbeziehung für einen vorhandenen ONTAP S3 Bucket auf dem Remote-Cluster erstellen . . . 8
Übernahme vom Ziel ONTAP S3-Bucket auf dem Remote-Cluster . . . 12
Ein ONTAP S3-Bucket kann von der Ziel-SVM auf dem Remote-Cluster wiederhergestellt werden . . . 13
Spiegelungs- und Backup-Schutz im lokalen Cluster . . . 15
Eine Spiegelbeziehung für einen neuen ONTAP S3 Bucket auf dem lokalen Cluster erstellen . . . 15
Eine Spiegelbeziehung für einen vorhandenen ONTAP S3 Bucket auf dem lokalen Cluster erstellen . . . 18
Übernahme vom Ziel-ONTAP S3 Bucket auf dem lokalen Cluster . . . 22
Ein ONTAP S3 Bucket kann von der Ziel-SVM auf dem lokalen Cluster wiederhergestellt werden . . . 23
Backup-Schutz mit Cloud-Zielen . . . 24
Anforderungen für ONTAP SnapMirror S3 Cloud-Zielbeziehungen . . . 24
Eine Cloud-Backup-Beziehung für einen neuen ONTAP S3 Bucket erstellen . . . 25
Eine Cloud-Backup-Beziehung für einen vorhandenen ONTAP S3 Bucket erstellen . . . 29
Wiederherstellung eines ONTAP S3-Buckets aus einem Cloud-Ziel . . . 32
Eine ONTAP SnapMirror S3-Richtlinie ändern . . . 33

Buckets mit SnapMirror S3 schützen

Informationen zu ONTAP SnapMirror S3

Ab ONTAP 9.10.1 ist der Schutz von Buckets in ONTAP S3 Objektspeichern mithilfe der SnapMirror Spiegelungs- und Sicherungsfunktionen möglich. Im Gegensatz zum Standard SnapMirror ermöglicht SnapMirror S3 die Spiegelung und Sicherung zu Nicht-NetApp-Zielen wie AWS S3.

SnapMirror S3 unterstützt aktive Spiegelungen und Backup-Ebenen von ONTAP S3-Buckets zu den folgenden Zielen:

Ziel	Unterstützt aktive Spiegel und Übernahme?	Unterstützt Backup und Wiederherstellung?
ONTAP S3 • Buckets in derselben SVM • Buckets in verschiedenen SVMs auf demselben Cluster • Buckets in SVMs auf verschiedenen Clustern	Ja	Ja
StorageGRID	Nein	Ja
AWS S3	Nein	Ja
Cloud Volumes ONTAP für Azure	Ja	Ja
Cloud Volumes ONTAP für AWS	Ja	Ja
Cloud Volumes ONTAP für Google Cloud	Ja	Ja

Sie können bestehende Buckets auf ONTAP S3 Servern schützen oder neue Buckets erstellen, bei denen die Datensicherung sofort aktiviert ist.

SnapMirror S3-Anforderungen

- ONTAP Version

  Auf dem Quell- und dem Zielcluster muss ONTAP 9.10.1 oder höher ausgeführt werden.

  In einer MetroCluster Konfiguration muss ONTAP 9.20.1 oder höher auf den Quell- und Ziel-Clustern ausgeführt werden.

- Lizenzierung

  Die folgenden Lizenzen sind in der "ONTAP One" Software-Suite verfügbar und werden auf ONTAP Quell- und Zielsystemen benötigt, um Zugriff zu ermöglichen:

  - ONTAP S3 Protokoll und Speicher
  - SnapMirror S3 zur Ansprache anderer NetApp Objektspeicher (ONTAP S3, StorageGRID und Cloud Volumes ONTAP)

- SnapMirror S3 zur Ansprache von Objektspeichern von Drittanbietern, einschließlich AWS S3 (verfügbar in der "ONTAP One Kompatibilitätspaket")
- Wenn auf Ihrem Cluster ONTAP 9.10.1 ausgeführt wird, ist ein "FabricPool Lizenz" erforderlich.
- In einer MetroCluster Konfiguration muss die SnapMirror S3-Lizenz auf beiden Clustern installiert sein.

- ONTAP S3
  - ONTAP S3-Server müssen auf Quell- und Ziel-SVMs ausgeführt werden.
  - Es wird empfohlen, aber nicht vorausgesetzt, dass CA-Zertifikate für den TLS-Zugriff auf Systemen installiert sind, die S3-Server hosten.
    - Die CA-Zertifikate, die zum Signieren der Zertifikate der S3-Server verwendet werden, müssen auf der Admin-Speicher-VM der Cluster installiert sein, die die S3-Server hosten.
    - Sie können ein selbstsigniertes CA-Zertifikat oder ein von einem externen CA-Anbieter signiertes Zertifikat verwenden.
    - Wenn die Quell- oder Ziel-Storage-VMs nicht auf HTTPS lauschen, ist die Installation von CA-Zertifikaten nicht erforderlich.
- Peering (für ONTAP S3-Ziele)
  - Intercluster-LIFs müssen konfiguriert werden (für entfernte ONTAP Ziele), und die Intercluster-LIFs des Quell- und Ziel-Cluster können eine Verbindung zu den Daten-LIFs des Quell- und Ziel-S3-Server herstellen.
  - Quell- und Ziel-Cluster sind per Peering verbunden (für entfernte ONTAP Ziele).
  - Quell- und Ziel-Storage-VMs sind per Peering verbunden (für alle ONTAP Ziele).
- SnapMirror Richtlinie
  - Eine S3-spezifische SnapMirror Richtlinie ist für alle SnapMirror S3-Beziehungen erforderlich, jedoch kann dieselbe Richtlinie für mehrere Beziehungen verwendet werden.
  - Sie können eine eigene Richtlinie erstellen oder die Standardrichtlinie **Continuous** akzeptieren, die die folgenden Werte enthält:
    - Drosselung (Obergrenze für Durchsatz/Bandbreite), unbegrenzt.
    - Zeit für Recovery Point Objective: 1 Stunde (3600 Sekunden).

> Es ist zu beachten, dass wenn zwei S3-Buckets in einer SnapMirror Beziehung stehen und Lebenszyklusrichtlinien so konfiguriert sind, dass die aktuelle Version eines Objekts abläuft (gelöscht wird), die gleiche Aktion auf den Partner-Bucket repliziert wird. Dies gilt auch, wenn der Partner-Bucket schreibgeschützt oder passiv ist.

- Root-Benutzerzugriffsschlüssel für Storage-VMs sind für SnapMirror S3-Beziehungen erforderlich; ONTAP weist diese nicht standardmäßig zu. Beim erstmaligen Erstellen einer SnapMirror S3-Beziehung ist zu überprüfen, ob die Schlüssel sowohl auf der Quell- als auch auf der Ziel-Storage-VM vorhanden sind, und sie sind neu zu generieren, falls sie fehlen. Falls eine Neugenerierung erforderlich ist, muss sichergestellt werden, dass alle Clients und alle SnapMirror Objektspeicherkonfigurationen, die das Zugriffsschlüssel- und geheime Schlüsselpaar verwenden, mit den neuen Schlüsseln aktualisiert werden.
- MetroCluster Ab ONTAP 9.20.1 wird SnapMirror S3 in MetroCluster Konfigurationen unterstützt. Die MetroCluster Konfiguration muss die folgenden Anforderungen erfüllen:
  - Die MetroCluster Konfiguration befindet sich in einem einwandfreien Zustand.
  - Auf beiden Clustern läuft ONTAP 9.20.1 oder höher.
  - Die SnapMirror S3 Lizenz ist auf beiden Clustern installiert.

Informationen zur S3-Serverkonfiguration sind in den folgenden Abschnitten verfügbar:

- "Einen S3-Server auf einer Storage-VM aktivieren"
- "Informationen zum ONTAP S3 Konfigurationsprozess"

Informationen zu Cluster- und Storage-VM-Peering sind im folgenden Thema verfügbar:

- "Vorbereitung auf Spiegelung und Archivierung (System Manager, Schritte 1-6)"
- "Cluster- und SVM-Peering (CLI)"

Unterstützte SnapMirror Beziehungen

SnapMirror S3 unterstützt Fan-Out- und Kaskadenbeziehungen. Eine Übersicht ist unter "Verzweigte und kaskadierte Datensicherungsbereitstellungen" zu finden.

SnapMirror S3 unterstützt keine Fan-In-Bereitstellungen (Datensicherungsbeziehungen zwischen mehreren Quell-Buckets und einem einzelnen Ziel-Bucket). SnapMirror S3 kann mehrere Bucket-Spiegelungen von mehreren Clustern auf einen einzelnen sekundären Cluster unterstützen, jedoch muss jeder Quell-Bucket einen eigenen Ziel-Bucket auf dem sekundären Cluster haben.

Zugriff auf S3-Buckets steuern

Beim Erstellen neuer Buckets können Sie den Zugriff durch das Erstellen von Benutzern und Gruppen steuern.

Obwohl SnapMirror S3 Objekte vom Quell-Bucket in einen Ziel-Bucket repliziert, werden Benutzer, Gruppen und Richtlinien nicht vom Quell-Objektspeicher in den Ziel-Objektspeicher repliziert.

Benutzer, Gruppenrichtlinien, Berechtigungen und ähnliche Komponenten müssen im Ziel-Objektspeicher konfiguriert werden, damit Clients während eines Failover-Ereignisses auf den Ziel-Bucket zugreifen können.

Quell- und Zielbenutzer können dieselben Zugriffs- und geheimen Schlüssel verwenden, sofern die Quellschlüssel bei der Erstellung des Benutzers im Ziel-Cluster manuell angegeben werden. Beispiel:

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

Weitere Informationen sind in den folgenden Abschnitten zu finden:

- "S3-Benutzer und Gruppen hinzufügen (System Manager)"
- "Erstellen eines S3-Benutzers (CLI)"
- "S3-Gruppen erstellen oder ändern (CLI)"

S3 Object Lock und Versionierung mit SnapMirror S3

Sie können SnapMirror S3 auf ONTAP Buckets mit aktivierter Objektsperre und Versionsverwaltung verwenden, wobei einige Punkte zu beachten sind:

- Um einen Quell-Bucket mit aktivierter Objektsperre zu replizieren, muss die Objektsperre auch im Ziel-Bucket aktiviert sein. Zusätzlich muss sowohl im Quell- als auch im Ziel-Bucket die Versionierung aktiviert sein. So werden Probleme beim Spiegeln von Löschvorgängen auf den Ziel-Bucket vermieden, wenn beide Buckets unterschiedliche Standard-Aufbewahrungsrichtlinien haben.

- S3 SnapMirror repliziert keine historischen Versionen von Objekten. Nur die aktuelle Version eines Objekts wird repliziert.

Wenn Object Locked-Objekte in einen Ziel-Bucket gespiegelt werden, behalten sie ihre ursprüngliche Aufbewahrungsdauer bei. Wenn entsperrte Objekte repliziert werden, übernehmen sie die Standardaufbewahrungsdauer des Ziel-Buckets. Beispiel:

- Bucket A hat eine Standardaufbewahrungsdauer von 30 Tagen und Bucket B hat eine Standardaufbewahrungsdauer von 60 Tagen. Objekte, die von Bucket A nach Bucket B repliziert werden, behalten ihre 30-tägige Aufbewahrungsdauer bei, auch wenn diese kürzer ist als die Standardaufbewahrungsdauer von Bucket B.
- Bucket A hat keine Standardaufbewahrungsfrist und Bucket B hat eine Standardaufbewahrungsfrist von 60 Tagen. Wenn nicht gesperrte Objekte von Bucket A nach Bucket B repliziert werden, übernehmen sie die 60-tägige Aufbewahrungsfrist. Wenn ein Objekt in Bucket A manuell gesperrt wird, behält es beim Replizieren nach Bucket B seine ursprüngliche Aufbewahrungsfrist bei.
- Bucket A hat eine standardmäßige Aufbewahrungsfrist von 30 Tagen und Bucket B hat keine standardmäßige Aufbewahrungsfrist. Objekte, die von Bucket A nach Bucket B repliziert werden, behalten ihre 30-tägige Aufbewahrungsfrist bei.

Spiegelungs- und Backup-Schutz auf einem entfernten Cluster

Eine Spiegelbeziehung für einen neuen ONTAP S3 Bucket auf dem Remote-Cluster erstellen

Wenn neue S3-Buckets erstellt werden, ist ein sofortiger Schutz auf einem SnapMirror S3-Ziel auf einem Remote-Cluster möglich.

Über diese Aufgabe

Aufgaben sind sowohl auf dem Quell- als auch auf dem Zielsystem durchzuführen.

Bevor Sie beginnen

- Die Anforderungen an ONTAP Versionen, Lizenzen und die S3-Serverkonfiguration wurden erfüllt.
- Zwischen Quell- und Ziel-Cluster besteht eine Peering-Beziehung, und zwischen Quell- und Ziel-Storage-VMs besteht eine Peering-Beziehung.
- Für die Quell- und Ziel-VMs werden CA-Zertifikate benötigt. Es können selbstsignierte CA-Zertifikate oder Zertifikate eines externen CA-Anbieters verwendet werden.

System Manager

1. Falls dies die erste SnapMirror S3-Beziehung für diese Storage-VM ist, sollte überprüft werden, ob Root-Benutzerschlüssel für sowohl die Quell- als auch die Ziel-Storage-VM vorhanden sind, und sie sollten neu generiert werden, falls dies nicht der Fall ist:
   a. Klicken Sie auf **Speicher > Speicher-VMs** und wählen Sie dann die Speicher-VM aus.
   b. Im Tab **Einstellungen** auf ✎ in der Kachel **S3** klicken.
   c. Auf der Registerkarte **Benutzer** ist zu überprüfen, ob ein Zugriffsschlüssel für den Root-Benutzer vorhanden ist.
   d. Falls kein Schlüssel vorhanden ist, auf ⋮ neben **root** und anschließend auf **Schlüssel neu**

generieren klicken. Der Schlüssel sollte nicht neu generiert werden, falls bereits einer existiert.

2. Die Storage-VM wird bearbeitet, um Benutzer hinzuzufügen und Benutzer Gruppen zuzuordnen, sowohl in der Quell- als auch in der Ziel-Storage-VM:

   Klicken Sie auf **Speicher > Speicher-VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und dann auf ✎ unter S3.

   Siehe "S3-Benutzer und Gruppen hinzufügen" für weitere Informationen.

3. Erstellen Sie auf dem Quell-Cluster eine SnapMirror S3-Richtlinie, falls noch keine vorhanden ist und Sie nicht die Standardrichtlinie verwenden möchten:
   a. **Schutz > Übersicht** und danach **Lokale Richtlinieneinstellungen** auswählen.
   b. Klicken Sie → neben **Schutzrichtlinien** und dann auf **Hinzufügen**.
      - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
      - Den Richtlinienbereich, den Cluster oder die SVM auswählen
      - **Kontinuierlich** für SnapMirror S3-Beziehungen auswählen.
      - Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
4. Einen Bucket mit SnapMirror-Schutz erstellen:
   a. Klicken Sie auf **Speicher > Buckets** und anschließend auf **Hinzufügen**. Die Überprüfung der Berechtigungen ist optional, aber empfehlenswert.
   b. Geben Sie einen Namen ein, wählen Sie die Storage-VM aus, geben Sie eine Größe ein und klicken Sie dann auf **Weitere Optionen**.
   c. Unter **Berechtigungen** auf **Hinzufügen** klicken.
      - **Principal** und **Effect** – Werte auswählen, die den Einstellungen Ihrer Benutzergruppe entsprechen, oder die Standardwerte übernehmen.
      - **Aktionen** – die folgenden Werte werden angezeigt:

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

      - **Ressourcen** – Standardwerte (*bucketname, bucketname/**) oder andere benötigte Werte verwenden.

        Weitere Informationen zu diesen Bereichen sind unter "Benutzerzugriff auf Buckets verwalten" zu finden.

   d. Unter **Schutz** die Option **Enable SnapMirror (ONTAP oder Cloud)** aktivieren. Anschließend die folgenden Werte eingeben:
      - Ziel
        - **ZIEL: ONTAP System**
        - **CLUSTER**: Der Remote-Cluster wird ausgewählt.
        - **STORAGE VM**: Eine Storage-VM auf dem Remote-Cluster auswählen.
        - **S3 SERVER CA-ZERTIFIKAT**: Den Inhalt des *Quell*-Zertifikats kopieren und einfügen.
      - Quelle

- **S3 SERVER CA-ZERTIFIKAT:** Den Inhalt des *Ziel*-Zertifikats kopieren und einfügen.

5. **Dasselbe Zertifikat auf dem Zielsystem verwenden** auswählen, wenn ein von einem externen CA-Anbieter signiertes Zertifikat verwendet wird.
6. Wenn Sie auf **Zieleinstellungen** klicken, können Sie anstelle der Standardwerte für Bucket-Name, Kapazität und Performance-Servicelevel auch eigene Werte eingeben.
7. Auf **Speichern** klicken. Ein neuer Bucket wird in der Quell-Speicher-VM erstellt und in einen neuen Bucket gespiegelt, der in der Ziel-Speicher-VM erstellt wird.

Verschlossene Buckets sichern

Ab ONTAP 9.14.1 ist es möglich, gesperrte S3-Buckets zu sichern und bei Bedarf wiederherzustellen.

Beim Festlegen der Schutzeinstellungen für einen neuen oder bestehenden Bucket kann die Objektsperrung für Ziel-Buckets aktiviert werden, sofern Quell- und Ziel-Cluster ONTAP 9.14.1 oder höher ausführen und die Objektsperrung im Quell-Bucket aktiviert ist. Der Objektsperrmodus und die Aufbewahrungsdauer der Sperre des Quell-Buckets gelten für die replizierten Objekte im Ziel-Bucket. Im Abschnitt **Zieleinstellungen** kann auch eine abweichende Aufbewahrungsdauer für den Ziel-Bucket definiert werden. Diese Aufbewahrungsdauer wird ebenfalls auf alle nicht gesperrten Objekte angewendet, die vom Quell-Bucket und über S3-Schnittstellen repliziert werden.

Informationen darüber, wie die Objektsperre für einen Bucket aktiviert wird, finden sich unter "Einen Bucket erstellen".

CLI

1. Falls dies die erste SnapMirror S3-Beziehung für diese SVM ist, sollte überprüft werden, ob Root-Benutzerschlüssel für sowohl die Quell- als auch die Ziel-SVM vorhanden sind, und diese gegebenenfalls neu generiert werden:

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

   Überprüfen Sie, ob ein Zugriffsschlüssel für den Root-Benutzer vorhanden ist. Falls nicht, Folgendes eingeben:

   ```
   vserver object-store-server user regenerate-keys -vserver svm_name -user root
   ```

   Der Schlüssel sollte nicht neu generiert werden, falls bereits einer existiert.

2. Buckets sowohl in der Quell- als auch in der Ziel-SVM 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. Zugriffsregeln zu den Standard-Bucket-Richtlinien sowohl in der Quell-SVM als auch in der Ziel-SVM hinzufügen:

   ```
   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

```
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. Auf der Quell-SVM eine SnapMirror S3-Richtlinie erstellen, falls noch keine vorhanden ist und die Standardrichtlinie nicht verwendet werden soll:
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parameter:

   - Typ `continuous` - der einzige Richtlinientyp für SnapMirror S3-Beziehungen (erforderlich).
   - `-rpo` - gibt die Zeit für das Recovery Point Objective in Sekunden an (optional).
   - `-throttle` - gibt die Obergrenze für Durchsatz/Bandbreite in Kilobyte/Sekunde an (optional).

   Beispiel

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

5. CA-Serverzertifikate auf den Admin-SVMs der Quell- und Ziel-Cluster installieren:

   a. Installieren Sie auf dem Quell-Cluster das CA-Zertifikat, das das *Ziel*-S3-Serverzertifikat signiert hat:
   `security certificate install -type server-ca -vserver src_admin_svm -cert-name dest_server_certificate`

   b. Installieren Sie auf dem Ziel-Cluster das CA-Zertifikat, das das *Quell*-S3-Serverzertifikat signiert hat:
   `security certificate install -type server-ca -vserver dest_admin_svm -cert-name src_server_certificate`

   Wenn ein von einem externen CA-Anbieter signiertes Zertifikat verwendet wird, ist dasselbe Zertifikat auf der Quell- und Ziel-Admin-SVM zu installieren.

   Weitere Informationen zu `security certificate install` finden sich in der "ONTAP-Befehlsreferenz".

6. Auf dem Quell-SVM eine SnapMirror S3-Beziehung erstellen:

   `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 Standardrichtlinie akzeptieren.

Beispiel

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

7. Es sollte überprüft werden, ob die Spiegelung aktiv ist:
`snapmirror show -policy-type continuous -fields status`

Verwandte Informationen

- "snapmirror create"
- "snapmirror policy create"
- "snapmirror show"

Eine Spiegelbeziehung für einen vorhandenen ONTAP S3 Bucket auf dem Remote-Cluster erstellen

Sie können jederzeit mit dem Schutz bestehender S3-Buckets beginnen, beispielsweise wenn eine S3-Konfiguration von einer Version vor ONTAP 9.10.1 aktualisiert wurde.

Über diese Aufgabe

Aufgaben sind sowohl auf dem Quell-Cluster als auch auf dem Ziel-Cluster durchzuführen.

Bevor Sie beginnen

- Die Anforderungen an ONTAP Versionen, Lizenzen und die S3-Serverkonfiguration wurden erfüllt.
- Zwischen Quell- und Ziel-Cluster besteht eine Peering-Beziehung, und zwischen Quell- und Ziel-Storage-VMs besteht eine Peering-Beziehung.
- Für die Quell- und Ziel-VMs werden CA-Zertifikate benötigt. Es können selbstsignierte CA-Zertifikate oder Zertifikate eines externen CA-Anbieters verwendet werden.

Schritte

Eine Spiegelbeziehung kann mithilfe des System Manager oder der ONTAP CLI erstellt werden.

System Manager

1. Falls dies die erste SnapMirror S3-Beziehung für diese Storage-VM ist, sollte überprüft werden, ob Root-Benutzerschlüssel für sowohl die Quell- als auch die Ziel-Storage-VM vorhanden sind, und sie sollten neu generiert werden, falls dies nicht der Fall ist:
   a. Wählen Sie **Speicher > Speicher-VMs** und anschließend die gewünschte Speicher-VM aus.
   b. Im Tab **Einstellungen** auf in der Kachel **S3** klicken.
   c. Auf der Registerkarte **Benutzer** ist zu überprüfen, ob ein Zugriffsschlüssel für den Root-Benutzer vorhanden ist.
   d. Falls kein Schlüssel vorhanden ist, auf neben **root** und anschließend auf **Schlüssel neu generieren** klicken. Der Schlüssel sollte nicht neu generiert werden, falls bereits einer existiert.
2. Es sollte überprüft werden, ob die vorhandenen Benutzer und Gruppen sowohl in der Quell- als auch in der Ziel-Speicher-VM vorhanden sind und über die korrekten Zugriffsrechte verfügen: **Storage >**

Storage VMs auswählen, dann die entsprechende Storage VM und anschließend die Registerkarte **Settings**. Abschließend die Kachel **S3** suchen, ✎ auswählen und dann die Registerkarte **Users** sowie anschließend die Registerkarte **Groups** auswählen, um die Zugriffsberechtigungen für Benutzer und Gruppen anzuzeigen.

Siehe "S3-Benutzer und Gruppen hinzufügen" für weitere Informationen.

3. Erstellen Sie auf dem Quell-Cluster eine SnapMirror S3-Richtlinie, falls noch keine vorhanden ist und Sie nicht die Standardrichtlinie verwenden möchten:
   a. **Schutz > Übersicht** auswählen und anschließend auf **Lokale Richtlinieneinstellungen** klicken.
   b. Wählen Sie → neben **Schutzrichtlinien** aus und klicken Sie dann auf **Hinzufügen**.
   c. Geben Sie den Namen und die Beschreibung der Richtlinie ein.
   d. Den Richtlinienbereich auswählen, entweder Cluster oder SVM.
   e. **Kontinuierlich** für SnapMirror S3-Beziehungen auswählen.
   f. Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
4. Es sollte geprüft werden, ob die Zugriffsrichtlinie des bestehenden Buckets weiterhin den eigenen Anforderungen entspricht:
   a. Klicken Sie auf **Storage > Buckets** und wählen Sie dann den Bucket aus, den Sie schützen möchten.
   b. Im Tab **Berechtigungen** auf ✎ **Bearbeiten** klicken, dann unter **Berechtigungen** auf **Hinzufügen** klicken.
      - **Prinzip und Wirkung**: Werte auswählen, die den Einstellungen Ihrer Benutzergruppe entsprechen, oder die Standardwerte übernehmen.
      - **Aktionen**: Die folgenden Werte sollten angezeigt werden:

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

      - **Ressourcen**: Standardwerte (*bucketname, bucketname/**) oder andere benötigte Werte verwenden.

        Weitere Informationen zu diesen Bereichen sind unter "Benutzerzugriff auf Buckets verwalten" zu finden.
5. Einen bestehenden Bucket mit SnapMirror S3-Schutz schützen:
   a. Klicken Sie auf **Speicher** > **Buckets** und wählen Sie dann den Bucket aus, den Sie schützen möchten.
   b. Auf **Schützen** klicken und die folgenden Werte eingeben:
      - Ziel
        - **ZIEL**: ONTAP System
        - **CLUSTER**: Der Remote-Cluster wird ausgewählt.
        - **STORAGE VM**: Eine Storage-VM auf dem Remote-Cluster auswählen.
        - **S3 SERVER CA-ZERTIFIKAT**: Den Inhalt des *Quell*-Zertifikats kopieren und einfügen.
      - Quelle

- **S3 SERVER CA-ZERTIFIKAT**: Den Inhalt des *Ziel*-Zertifikats kopieren und einfügen.

6. **Dasselbe Zertifikat auf dem Zielsystem verwenden** auswählen, wenn ein von einem externen CA-Anbieter signiertes Zertifikat verwendet wird.
7. Wenn Sie auf **Zieleinstellungen** klicken, können Sie anstelle der Standardwerte für Bucket-Name, Kapazität und Performance-Servicelevel auch eigene Werte eingeben.
8. Auf **Speichern** klicken. Der vorhandene Bucket wird in einen neuen Bucket auf der Ziel-Speicher-VM gespiegelt.

Verschlossene Buckets sichern

Ab ONTAP 9.14.1 ist es möglich, gesperrte S3-Buckets zu sichern und bei Bedarf wiederherzustellen.

Beim Festlegen der Schutzeinstellungen für einen neuen oder bestehenden Bucket kann die Objektsperrung für Ziel-Buckets aktiviert werden, sofern Quell- und Ziel-Cluster ONTAP 9.14.1 oder höher ausführen und die Objektsperrung im Quell-Bucket aktiviert ist. Der Objektsperrmodus und die Aufbewahrungsdauer der Sperre des Quell-Buckets gelten für die replizierten Objekte im Ziel-Bucket. Im Abschnitt **Zieleinstellungen** kann auch eine abweichende Aufbewahrungsdauer für den Ziel-Bucket definiert werden. Diese Aufbewahrungsdauer wird ebenfalls auf alle nicht gesperrten Objekte angewendet, die vom Quell-Bucket und über S3-Schnittstellen repliziert werden.

Informationen darüber, wie die Objektsperre für einen Bucket aktiviert wird, finden sich unter "Einen Bucket erstellen".

CLI

1. Wenn dies die erste SnapMirror S3-Beziehung für diese SVM ist, ist zu überprüfen, ob Root-Benutzer-Schlüssel für sowohl Quell- als auch Ziel-SVMs existieren, und diese gegebenenfalls neu zu generieren:
   `vserver object-store-server user show` + Es ist zu überprüfen, ob ein Zugriffsschlüssel für den Root-Benutzer vorhanden ist. Falls keiner vorhanden ist, ist Folgendes einzugeben:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root` + Der Schlüssel darf nicht neu generiert werden, wenn bereits einer existiert.
2. Einen Bucket auf der Ziel-SVM als Spiegelungsziel erstellen:

   `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. Es sollte sichergestellt werden, dass die Zugriffsregeln der Standard Bucket-Richtlinien sowohl in der Quell-SVM als auch in der Ziel-SVM 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

   ```
   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. Auf der Quell-SVM eine SnapMirror S3-Richtlinie erstellen, falls noch keine vorhanden ist und die Standardrichtlinie nicht verwendet werden soll:

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

   Parameter:

   - `continuous` – die einzige Richtlinienart für SnapMirror S3-Beziehungen (erforderlich).
   - `-rpo` gibt die Zeit für das Recovery Point Objective in Sekunden an (optional).
   - `-throttle` gibt die Obergrenze für Durchsatz/Bandbreite in Kilobyte/Sekunde an (optional).

   Beispiel

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

5. CA-Zertifikate auf den Admin-SVMs der Quell- und Ziel-Cluster installieren:
   a. Installieren Sie auf dem Quell-Cluster das CA-Zertifikat, das das *Ziel*-S3-Serverzertifikat signiert hat:
   `security certificate install -type server-ca -vserver src_admin_svm -cert-name dest_server_certificate`
   b. Auf dem Ziel-Cluster das CA-Zertifikat installieren, das das *Quell*-S3-Serverzertifikat signiert hat: `security certificate install -type server-ca -vserver dest_admin_svm -cert-name src_server_certificate` + Bei Verwendung eines von einem externen CA-Anbieter signierten Zertifikats ist dasselbe Zertifikat auf der Quell- und Ziel-Admin-SVM zu installieren.

      Weitere Informationen zu `security certificate install` finden sich in der "ONTAP-Befehlsreferenz".

6. Auf dem Quell-SVM eine SnapMirror S3-Beziehung erstellen:

   `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 Standardrichtlinie akzeptieren.

   Beispiel

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

7. Es sollte überprüft werden, ob die Spiegelung aktiv ist:
   `snapmirror show -policy-type continuous -fields status`

Verwandte Informationen

- "snapmirror create"
- "snapmirror policy create"
- "snapmirror show"

Übernahme vom Ziel ONTAP S3-Bucket auf dem Remote-Cluster

Wenn die Daten in einem Quell-Bucket nicht mehr verfügbar sind, kann die SnapMirror Beziehung unterbrochen werden, sodass der Ziel-Bucket beschreibbar ist und Daten bereitgestellt werden können.

Über diese Aufgabe

Bei einer Übernahmeoperation wird der Quell-Bucket in einen schreibgeschützten Bucket umgewandelt und der ursprüngliche Ziel-Bucket in einen Lese-/Schreib-Bucket, wodurch die SnapMirror S3-Beziehung umgekehrt wird.

Wenn der deaktivierte Quell-Bucket wieder verfügbar ist, resynchronisiert SnapMirror S3 die Inhalte der beiden Buckets automatisch. Eine explizite Resynchronisierung der Beziehung ist nicht erforderlich, wie sie bei Volume SnapMirror Deployments notwendig ist.

Die Übernahme muss vom Remote-Cluster aus initiiert werden.

Obwohl SnapMirror S3 Objekte vom Quell-Bucket in einen Ziel-Bucket repliziert, werden Benutzer, Gruppen und Richtlinien nicht vom Quell-Objektspeicher in den Ziel-Objektspeicher repliziert.

Benutzer, Gruppenrichtlinien, Berechtigungen und ähnliche Komponenten müssen im Ziel-Objektspeicher konfiguriert werden, damit Clients während eines Failover-Ereignisses auf den Ziel-Bucket zugreifen können.

Quell- und Zielbenutzer können dieselben Zugriffs- und geheimen Schlüssel verwenden, sofern die Quellschlüssel bei der Erstellung des Benutzers im Ziel-Cluster manuell angegeben werden. Beispiel:

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

System Manager

Failover vom nicht verfügbaren Bucket und Beginn der Datenbereitstellung:

1. **Schutz > Beziehungen** auswählen und dann **SnapMirror S3** wählen.
2. Klicken Sie auf ⋮, wählen Sie **Failover** und dann **Failover**.

CLI

1. Einen Failover-Vorgang für den Ziel-Bucket initiieren:
   `snapmirror failover start -destination-path` *`svm_name`*`:/bucket/`*`bucket_name`*
2. Der Status des Failover-Vorgangs kann überprüft werden:

```
snapmirror show -fields status
```

Beispiel

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

Verwandte Informationen

- "S3-Benutzer und Gruppen hinzufügen (System Manager)"
- "Erstellen eines S3-Benutzers (CLI)"
- "S3-Gruppen erstellen oder ändern (CLI)"
- "SnapMirror Failover Start"
- "snapmirror show"

Ein ONTAP S3-Bucket kann von der Ziel-SVM auf dem Remote-Cluster wiederhergestellt werden.

Wenn Daten in einem Quell-Bucket verloren gehen oder beschädigt werden, kann eine Wiederherstellung der Daten erfolgen, indem Objekte aus einem Ziel-Bucket wiederhergestellt werden.

Über diese Aufgabe

Sie können den Ziel-Bucket in einem vorhandenen Bucket oder in einem neuen Bucket wiederherstellen. Der Ziel-Bucket für die Wiederherstellung muss größer sein als der logisch genutzte Speicherplatz des Ziel-Buckets.

Wenn Sie einen vorhandenen Bucket verwenden, muss dieser beim Start einer Wiederherstellungsoperation leer sein. Die Wiederherstellung führt kein „Rollback“ eines Buckets in der Zeit durch, sondern füllt einen leeren Bucket mit seinem vorherigen Inhalt.

Der Wiederherstellungsvorgang muss vom Remote-Cluster aus gestartet werden.

System Manager

Die gesicherten Daten wiederherstellen:

1. **Schutz > Beziehungen** auswählen und dann **SnapMirror S3** wählen.
2. Klicken Sie ⋮ und wählen Sie dann **Wiederherstellen**.
3. Unter **Quelle Vorhandener Bucket** (Standardeinstellung) oder **Neuer Bucket** auswählen.
   - Um auf einen **vorhandenen Bucket** (Standardeinstellung) wiederherzustellen, sind folgende Schritte erforderlich:
     - Den Cluster und die Storage-VM auswählen, um nach dem vorhandenen Bucket zu suchen.
     - Wählen Sie den vorhandenen Bucket aus.
     - Kopieren und fügen Sie den Inhalt des *destination* S3-Server-CA-Zertifikats ein.
   - Für die Wiederherstellung in einem **neuen Bucket** sind die folgenden Werte anzugeben:

- Der Cluster und die Storage-VM zum Hosten des neuen Buckets.
- Name, Kapazität und Leistungsniveau des neuen Buckets. Siehe "Storage-Servicelevel" für weitere Informationen.
- Der Inhalt des *destination* S3 Server CA-Zertifikats.

4. Unter **Ziel** den Inhalt des CA-Zertifikats des *source* S3-Servers kopieren und einfügen.
5. **Schutz > Beziehungen** kann zur Überwachung des Wiederherstellungsfortschritts verwendet werden.

Gesperrte Buckets wiederherstellen

Ab ONTAP 9.14.1 ist es möglich, gesperrte Buckets zu sichern und bei Bedarf wiederherzustellen.

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

- **Wiederherstellung in einem neuen Bucket**: Wenn die Objektsperrung aktiviert ist, kann ein Bucket wiederhergestellt werden, indem ein Bucket erstellt wird, in dem die Objektsperrung ebenfalls aktiviert ist. Beim Wiederherstellen eines gesperrten Buckets werden der Objektsperrmodus und die Aufbewahrungsdauer des ursprünglichen Buckets übernommen. Es kann auch eine andere Aufbewahrungsdauer für die Sperre im neuen Bucket definiert werden. Diese Aufbewahrungsdauer gilt für nicht gesperrte Objekte aus anderen Quellen.
- **Wiederherstellung in einem bestehenden Bucket**: Ein objektgesperrter Bucket kann in einem bestehenden Bucket wiederhergestellt werden, sofern für den bestehenden Bucket Versionierung und ein ähnlicher Objektsperrmodus aktiviert sind. Die Aufbewahrungsdauer des ursprünglichen Buckets bleibt erhalten.
- **Nicht gesperrten Bucket wiederherstellen**: Selbst wenn die Objektsperrung für einen Bucket nicht aktiviert ist, kann er in einem Bucket wiederhergestellt werden, in dem die Objektsperrung aktiviert ist und der sich im Quell-Cluster befindet. Beim Wiederherstellen des Buckets werden alle nicht gesperrten Objekte gesperrt, und der Aufbewahrungsmodus sowie die Aufbewahrungsdauer des Ziel-Buckets gelten für diese Objekte.

CLI

1. Den neuen Ziel-Bucket für die Wiederherstellung erstellen. Weitere Informationen finden sich unter "Eine Cloud-Backup-Beziehung für einen neuen ONTAP S3 Bucket erstellen".
2. Einen Wiederherstellungsvorgang für den Ziel-Bucket initiieren:
   `snapmirror restore -source-path` *`svm_name`*`:/bucket/`*`bucket_name`* `-destination -path` *`svm_name`*`:/bucket/`*`bucket_name`*

   Beispiel

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

   Weitere Informationen zu `snapmirror restore` finden sich in der "ONTAP-Befehlsreferenz".

Spiegelungs- und Backup-Schutz im lokalen Cluster

Eine Spiegelbeziehung für einen neuen ONTAP S3 Bucket auf dem lokalen Cluster erstellen

Wenn neue S3-Buckets erstellt werden, ist deren sofortiger Schutz auf ein SnapMirror S3-Ziel im selben Cluster möglich. Gespiegelte Daten können in einen Bucket in einer anderen Storage-VM oder in derselben Storage-VM wie das Quell-System übertragen werden.

Bevor Sie beginnen

- Die Anforderungen an ONTAP Versionen, Lizenzen und die S3-Serverkonfiguration wurden erfüllt.
- Eine Peering-Beziehung besteht zwischen den Quell- und Ziel-Storage-VMs.
- Für die Quell- und Ziel-VMs werden CA-Zertifikate benötigt. Es können selbstsignierte CA-Zertifikate oder Zertifikate eines externen CA-Anbieters verwendet werden.

System Manager

1. Falls dies die erste SnapMirror S3-Beziehung für diese Storage-VM ist, sollte überprüft werden, ob Root-Benutzerschlüssel für sowohl die Quell- als auch die Ziel-Storage-VM vorhanden sind, und sie sollten neu generiert werden, falls dies nicht der Fall ist:
   a. Klicken Sie auf **Speicher > Speicher-VMs** und wählen Sie dann die Speicher-VM aus.
   b. Im Tab **Einstellungen** auf in der S3-Kachel klicken.
   c. Auf der Registerkarte **Benutzer** ist zu überprüfen, ob ein Zugriffsschlüssel für den Root-Benutzer vorhanden ist
   d. Falls kein Schlüssel vorhanden ist, auf neben **root** und anschließend auf **Schlüssel neu generieren** klicken. Der Schlüssel sollte nicht neu generiert werden, falls bereits einer existiert.
2. Die Storage-VM kann bearbeitet werden, um Benutzer hinzuzufügen und Benutzer zu Gruppen hinzuzufügen, sowohl in der Quell- als auch in der Ziel-Storage-VM: **Speicher > Storage-VMs** auswählen, die Storage-VM auswählen, **Einstellungen** auswählen und dann unter S3 auswählen.

   Siehe "S3-Benutzer und Gruppen hinzufügen" für weitere Informationen.
3. Eine SnapMirror S3-Richtlinie kann erstellt werden, wenn noch keine vorhanden ist und die Standardrichtlinie nicht verwendet werden soll:
   a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Lokale Richtlinieneinstellungen**.
   b. Klicken Sie neben **Schutzrichtlinien** und dann auf **Hinzufügen**.
      - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
      - Den Richtlinienbereich, den Cluster oder die SVM auswählen
      - **Kontinuierlich** für SnapMirror S3-Beziehungen auswählen.
      - Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
4. Einen Bucket mit SnapMirror-Schutz erstellen:
   a. Wählen Sie **Speicher > Buckets** und dann **Hinzufügen** aus.
   b. Geben Sie einen Namen ein, wählen Sie die Storage-VM aus, geben Sie eine Größe ein und

klicken Sie dann auf **Weitere Optionen**.

c. Unter **Berechtigungen** auf **Hinzufügen** klicken. Die Überprüfung der Berechtigungen ist optional, aber empfehlenswert.

- **Principal** und **Effect** – Werte auswählen, die den Einstellungen Ihrer Benutzergruppe entsprechen, oder die Standardwerte übernehmen.
- **Aktionen** – die folgenden Werte werden angezeigt:

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

- **Ressourcen** – Standardwerte `(bucketname, bucketname/*)` oder andere benötigte Werte verwenden

  Weitere Informationen zu diesen Bereichen sind unter "Benutzerzugriff auf Buckets verwalten" zu finden.

d. Unter **Schutz** die Option **Enable SnapMirror (ONTAP oder Cloud)** aktivieren. Anschließend die folgenden Werte eingeben:

- Ziel
  - **ZIEL**: ONTAP System
  - **CLUSTER**: Der lokale Cluster wird ausgewählt.
  - **STORAGE VM**: Eine Storage-VM im lokalen Cluster auswählen.
  - **S3 SERVER CA-ZERTIFIKAT**: Den Inhalt des Quellzertifikats kopieren und einfügen.
- Quelle
  - **S3 SERVER CA-ZERTIFIKAT**: Den Inhalt des Zielzertifikats kopieren und einfügen.

5. **Dasselbe Zertifikat auf dem Zielsystem verwenden** auswählen, wenn ein von einem externen CA-Anbieter signiertes Zertifikat verwendet wird.
6. Wenn Sie auf **Zieleinstellungen** klicken, können Sie anstelle der Standardwerte für Bucket-Name, Kapazität und Performance-Servicelevel auch eigene Werte eingeben.
7. Auf **Speichern** klicken. Ein neuer Bucket wird in der Quell-Speicher-VM erstellt und in einen neuen Bucket gespiegelt, der in der Ziel-Speicher-VM erstellt wird.

Verschlossene Buckets sichern

Ab ONTAP 9.14.1 ist es möglich, gesperrte S3-Buckets zu sichern und bei Bedarf wiederherzustellen.

Beim Festlegen der Schutzeinstellungen für einen neuen oder bestehenden Bucket kann die Objektsperrung für Ziel-Buckets aktiviert werden, sofern Quell- und Ziel-Cluster ONTAP 9.14.1 oder höher ausführen und die Objektsperrung im Quell-Bucket aktiviert ist. Der Objektsperrmodus und die Aufbewahrungsdauer der Sperre des Quell-Buckets gelten für die replizierten Objekte im Ziel-Bucket. Im Abschnitt **Zieleinstellungen** kann auch eine abweichende Aufbewahrungsdauer für den Ziel-Bucket definiert werden. Diese Aufbewahrungsdauer wird ebenfalls auf alle nicht gesperrten Objekte angewendet, die vom Quell-Bucket und über S3-Schnittstellen repliziert werden.

Informationen darüber, wie die Objektsperre für einen Bucket aktiviert wird, finden sich unter "Einen Bucket erstellen".

CLI

1. Falls dies die erste SnapMirror S3-Beziehung für diese SVM ist, sollte überprüft werden, ob Root-Benutzerschlüssel für sowohl Quell- als auch Ziel-SVMs vorhanden sind, und sie sollten neu generiert werden, falls sie nicht existieren:
   `vserver object-store-server user show`

   Überprüfen Sie, ob ein Zugriffsschlüssel für den Root-Benutzer vorhanden ist. Falls nicht, Folgendes eingeben:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   Der Schlüssel sollte nicht neu generiert werden, falls bereits einer existiert.

2. Buckets sowohl in der Quell- als auch in der Ziel-SVM 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. Zugriffsregeln zu den Standard-Bucket-Richtlinien sowohl in der Quell-SVM als auch in der Ziel-SVM hinzufügen:

   ```
   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 SnapMirror S3-Richtlinie, falls Sie noch keine haben und nicht die Standardrichtlinie verwenden möchten:
   `snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parameter:

   - `continuous` – die einzige Richtlinienart für SnapMirror S3-Beziehungen (erforderlich).
   - `-rpo` gibt die Zeit für das Recovery Point Objective in Sekunden an (optional).
   - `-throttle` gibt die Obergrenze für Durchsatz/Bandbreite in Kilobyte/Sekunde an (optional).

   Beispiel

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

5. CA-Serverzertifikate auf der Admin-SVM installieren:
   a. Das CA-Zertifikat, das das Zertifikat des *source* S3-Servers signiert hat, auf der Admin-SVM installieren:
   `security certificate install -type server-ca -vserver admin_svm -cert -name src_server_certificate`
   b. Das CA-Zertifikat, das das Zertifikat des *Ziel*-S3-Servers signiert hat, auf der Admin-SVM installieren
   `security certificate install -type server-ca -vserver admin_svm -cert -name dest_server_certificate`. Wenn ein von einem externen CA-Anbieter signiertes Zertifikat verwendet wird, ist nur die Installation dieses Zertifikats auf der Admin-SVM erforderlich.

   Weitere Informationen zu `security certificate install` finden sich in der "ONTAP-Befehlsreferenz".

6. Erstellen einer SnapMirror S3-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 Standardrichtlinie akzeptieren.

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

7. Es sollte überprüft werden, ob die Spiegelung aktiv ist:
   `snapmirror show -policy-type continuous -fields status`

Verwandte Informationen

- "snapmirror create"
- "snapmirror policy create"
- "snapmirror show"

Eine Spiegelbeziehung für einen vorhandenen ONTAP S3 Bucket auf dem lokalen Cluster erstellen

Sie können jederzeit mit dem Schutz bestehender S3-Buckets auf demselben Cluster beginnen, beispielsweise wenn eine S3-Konfiguration von einer Version vor ONTAP 9.10.1 aktualisiert wurde. Gespiegelte Daten können in einen Bucket in einer anderen Storage-VM oder in derselben Storage-VM wie das Quell-System übertragen werden.

Bevor Sie beginnen

- Die Anforderungen an ONTAP Versionen, Lizenzen und die S3-Serverkonfiguration wurden erfüllt.
- Eine Peering-Beziehung besteht zwischen den Quell- und Ziel-Storage-VMs.
- Für die Quell- und Ziel-VMs werden CA-Zertifikate benötigt. Es können selbstsignierte CA-Zertifikate oder Zertifikate eines externen CA-Anbieters verwendet werden.

System Manager

1. Falls dies die erste SnapMirror S3-Beziehung für diese Storage-VM ist, sollte überprüft werden, ob Root-Benutzerschlüssel für sowohl die Quell- als auch die Ziel-Storage-VM vorhanden sind, und sie sollten neu generiert werden, falls dies nicht der Fall ist:
   a. Klicken Sie auf **Speicher > Speicher-VMs** und wählen Sie dann die Speicher-VM aus.
   b. Im Tab **Einstellungen** auf in der Kachel **S3** klicken.
   c. Auf der Registerkarte **Benutzer** ist zu überprüfen, ob ein Zugriffsschlüssel für den Root-Benutzer vorhanden ist.
   d. Falls kein Schlüssel vorhanden ist, auf neben **root** und anschließend auf **Schlüssel neu generieren** klicken. Der Schlüssel sollte nicht neu generiert werden, falls bereits einer existiert.
2. Es sollte überprüft werden, ob die vorhandenen Benutzer und Gruppen sowohl auf der Quell- als auch auf der Ziel-Speicher-VM vorhanden sind und über die korrekten Zugriffsrechte verfügen: **Speicher > Speicher-VMs** auswählen, dann die gewünschte Speicher-VM und anschließend die Registerkarte **Einstellungen**. Abschließend die Kachel **S3** suchen, auswählen und dann die Registerkarte **Users** sowie anschließend die Registerkarte **Groups** auswählen, um die Zugriffsberechtigungen für Benutzer und Gruppen anzuzeigen.

   Siehe "S3-Benutzer und Gruppen hinzufügen" für weitere Informationen.
3. Eine SnapMirror S3-Richtlinie kann erstellt werden, wenn noch keine vorhanden ist und die Standardrichtlinie nicht verwendet werden soll:
   a. **Schutz > Übersicht** auswählen und anschließend **Lokale Richtlinieneinstellungen** öffnen.
   b. Klicken Sie neben **Schutzrichtlinien** und dann auf **Hinzufügen**.
      - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
      - Den Richtlinienbereich, den Cluster oder die SVM auswählen
      - **Kontinuierlich** für SnapMirror S3-Beziehungen auswählen.
      - Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
4. Es sollte geprüft werden, ob die Zugriffsrichtlinie des bestehenden Buckets weiterhin den Anforderungen entspricht:
   a. Klicken Sie auf **Storage > Buckets** und wählen Sie dann den Bucket aus, den Sie schützen möchten.
   b. Im Tab **Berechtigungen** auf **Bearbeiten** klicken, dann unter **Berechtigungen** auf **Hinzufügen** klicken.
      - **Principal** und **Effect** – Werte auswählen, die den Einstellungen Ihrer Benutzergruppe entsprechen, oder die Standardwerte übernehmen.
      - **Aktionen** – die folgenden Werte werden angezeigt:

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

      - **Ressourcen** – Standardwerte *(bucketname, bucketname/*)* oder andere benötigte Werte verwenden.

        Weitere Informationen zu diesen Bereichen sind unter "Benutzerzugriff auf Buckets verwalten"

zu finden.

5. Einen bestehenden Bucket mit SnapMirror S3 schützen:
   a. Klicken Sie auf **Speicher** > **Buckets** und wählen Sie dann den Bucket aus, den Sie schützen möchten.
   b. Auf **Schützen** klicken und die folgenden Werte eingeben:
      - Ziel
        - **ZIEL**: ONTAP System
        - **CLUSTER**: Der lokale Cluster wird ausgewählt.
        - **STORAGE VM**: Dieselbe oder eine andere Storage-VM kann ausgewählt werden.
        - **S3 SERVER CA-ZERTIFIKAT**: Den Inhalt des *Quell*-Zertifikats kopieren und einfügen.
      - Quelle
        - **S3 SERVER CA-ZERTIFIKAT**: Den Inhalt des *Ziel*-Zertifikats kopieren und einfügen.
6. **Dasselbe Zertifikat auf dem Zielsystem verwenden** auswählen, wenn ein von einem externen CA-Anbieter signiertes Zertifikat verwendet wird.
7. Wenn Sie auf **Zieleinstellungen** klicken, können Sie anstelle der Standardwerte für Bucket-Name, Kapazität und Performance-Servicelevel auch eigene Werte eingeben.
8. Auf **Speichern** klicken. Der vorhandene Bucket wird in einen neuen Bucket auf der Ziel-Speicher-VM gespiegelt.

Verschlossene Buckets sichern

Ab ONTAP 9.14.1 ist es möglich, gesperrte S3-Buckets zu sichern und bei Bedarf wiederherzustellen.

Beim Festlegen der Schutzeinstellungen für einen neuen oder bestehenden Bucket kann die Objektsperrung für Ziel-Buckets aktiviert werden, sofern Quell- und Ziel-Cluster ONTAP 9.14.1 oder höher ausführen und die Objektsperrung im Quell-Bucket aktiviert ist. Der Objektsperrmodus und die Aufbewahrungsdauer der Sperre des Quell-Buckets gelten für die replizierten Objekte im Ziel-Bucket. Im Abschnitt **Zieleinstellungen** kann auch eine abweichende Aufbewahrungsdauer für den Ziel-Bucket definiert werden. Diese Aufbewahrungsdauer wird ebenfalls auf alle nicht gesperrten Objekte angewendet, die vom Quell-Bucket und über S3-Schnittstellen repliziert werden.

Informationen darüber, wie die Objektsperre für einen Bucket aktiviert wird, finden sich unter "Einen Bucket erstellen".

CLI

1. Falls dies die erste SnapMirror S3-Beziehung für diese SVM ist, sollte überprüft werden, ob Root-Benutzerschlüssel für sowohl Quell- als auch Ziel-SVMs vorhanden sind, und sie sollten neu generiert werden, falls sie nicht existieren:
   `vserver object-store-server user show`

   Überprüfen Sie, ob ein Zugriffsschlüssel für den Root-Benutzer vorhanden ist. Falls nicht, Folgendes eingeben:
   `vserver object-store-server user regenerate-keys -vserver svm_name -user root`

   Der Schlüssel sollte nicht neu generiert werden, falls bereits einer existiert.

2. Einen Bucket auf der Ziel-SVM als Spiegelungsziel erstellen:

```
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. Es sollte sichergestellt sein, dass die Zugriffsregeln für die Standard-Bucket-Richtlinien sowohl in der Quell-SVM als auch in der Ziel-SVM 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. Eine SnapMirror S3-Richtlinie kann erstellt werden, wenn noch keine vorhanden ist und die Standardrichtlinie nicht verwendet werden soll:

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

   Parameter:

   - `continuous` – die einzige Richtlinienart für SnapMirror S3-Beziehungen (erforderlich).
   - `-rpo` gibt die Zeit für das Recovery Point Objective in Sekunden an (optional).
   - `-throttle` gibt die Obergrenze für Durchsatz/Bandbreite in Kilobyte/Sekunde an (optional).

     Beispiel

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

5. CA-Serverzertifikate auf der Admin-SVM installieren:

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

   b. Das CA-Zertifikat, das das Zertifikat des *Ziel*-S3-Servers signiert hat, auf der Admin-SVM installieren
   `security certificate install -type server-ca -vserver admin_svm -cert -name dest_server_certificate`. Wenn ein von einem externen CA-Anbieter signiertes Zertifikat verwendet wird, ist nur die Installation dieses Zertifikats auf der Admin-SVM erforderlich.

Weitere Informationen zu `security certificate install` finden sich in der "ONTAP-Befehlsreferenz".

6. Erstellen einer SnapMirror S3-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 Standardrichtlinie akzeptieren.

   Beispiel

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

7. Es sollte überprüft werden, ob die Spiegelung aktiv ist:
`snapmirror show -policy-type continuous -fields status`

Verwandte Informationen

- "snapmirror create"
- "snapmirror policy create"
- "snapmirror show"

Übernahme vom Ziel-ONTAP S3 Bucket auf dem lokalen Cluster

Wenn die Daten in einem Quell-Bucket nicht mehr verfügbar sind, kann die SnapMirror Beziehung unterbrochen werden, sodass der Ziel-Bucket beschreibbar ist und Daten bereitgestellt werden können.

Über diese Aufgabe

Bei einer Übernahmeoperation wird der Quell-Bucket in einen schreibgeschützten Bucket umgewandelt und der ursprüngliche Ziel-Bucket in einen Lese-/Schreib-Bucket, wodurch die SnapMirror S3-Beziehung umgekehrt wird.

Wenn der deaktivierte Quell-Bucket wieder verfügbar ist, resynchronisiert SnapMirror S3 die Inhalte der beiden Buckets automatisch. Eine explizite Resynchronisierung der Beziehung ist nicht erforderlich, wie es bei herkömmlichen Volume SnapMirror Deployments notwendig ist.

Befindet sich der Ziel-Bucket auf einem Remote-Cluster, muss die Übernahme vom Remote-Cluster aus initiiert werden.

System Manager

Failover vom nicht verfügbaren Bucket und Beginn der Datenbereitstellung:

1. **Schutz > Beziehungen** auswählen und dann **SnapMirror S3** wählen.
2. Klicken Sie auf ⋮, wählen Sie **Failover** und dann **Failover**.

CLI

1. Einen Failover-Vorgang für den Ziel-Bucket initiieren:
   `snapmirror failover start -destination-path svm_name:/bucket/bucket_name`
2. Der Status des Failover-Vorgangs kann überprüft werden:
   `snapmirror show -fields status`

Beispiel

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

Verwandte Informationen

- "SnapMirror Failover Start"
- "snapmirror show"

Ein ONTAP S3 Bucket kann von der Ziel-SVM auf dem lokalen Cluster wiederhergestellt werden.

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

Über diese Aufgabe

Sie können den Ziel-Bucket in einem vorhandenen Bucket oder in einem neuen Bucket wiederherstellen. Der Ziel-Bucket für die Wiederherstellung muss größer sein als der logisch genutzte Speicherplatz des Ziel-Buckets.

Wenn Sie einen vorhandenen Bucket verwenden, muss dieser beim Start einer Wiederherstellungsoperation leer sein. Die Wiederherstellung führt kein „Rollback“ eines Buckets in der Zeit durch, sondern füllt einen leeren Bucket mit seinem vorherigen Inhalt.

Der Wiederherstellungsvorgang muss vom lokalen Cluster aus gestartet werden.

System Manager

Die Sicherungsdaten wiederherstellen:

1. Klicken Sie auf **Schutz > Beziehungen** und wählen Sie dann den Bucket aus.
2. Klicken Sie ⋮ und wählen Sie dann **Wiederherstellen**.
3. Unter **Quelle Vorhandener Bucket** (Standardeinstellung) oder **Neuer Bucket** auswählen.
   - Um auf einen **vorhandenen Bucket** (Standardeinstellung) wiederherzustellen, sind folgende Schritte erforderlich:
     - Den Cluster und die Storage-VM auswählen, um nach dem vorhandenen Bucket zu suchen.
     - Wählen Sie den vorhandenen Bucket aus.
4. Kopieren und fügen Sie den Inhalt des CA-Zertifikats des Ziel-S3-Servers ein.
   - Für die Wiederherstellung in einem **neuen Bucket** sind die folgenden Werte anzugeben:
     - Der Cluster und die Storage-VM zum Hosten des neuen Buckets.
     - Name, Kapazität und Leistungsniveau des neuen Buckets. Siehe "Storage-Servicelevel" für

weitere Informationen.

- Der Inhalt des CA-Zertifikats des Ziel-S3-Servers.

5. Unter **Ziel** den Inhalt des CA-Zertifikats des Quell-S3-Servers kopieren und einfügen.
6. Klicken Sie auf **Schutz** > Beziehungen, um den Fortschritt der Wiederherstellung zu überwachen.

Gesperrte Buckets wiederherstellen

Ab ONTAP 9.14.1 ist es möglich, gesperrte Buckets zu sichern und bei Bedarf wiederherzustellen.

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

- **Wiederherstellung in einem neuen Bucket**: Wenn die Objektsperrung aktiviert ist, kann ein Bucket wiederhergestellt werden, indem ein Bucket erstellt wird, in dem die Objektsperrung ebenfalls aktiviert ist. Beim Wiederherstellen eines gesperrten Buckets werden der Objektsperrmodus und die Aufbewahrungsdauer des ursprünglichen Buckets übernommen. Es kann auch eine andere Aufbewahrungsdauer für die Sperre im neuen Bucket definiert werden. Diese Aufbewahrungsdauer gilt für nicht gesperrte Objekte aus anderen Quellen.
- **Wiederherstellung in einem bestehenden Bucket**: Ein objektgesperrter Bucket kann in einem bestehenden Bucket wiederhergestellt werden, sofern für den bestehenden Bucket Versionierung und ein ähnlicher Objektsperrmodus aktiviert sind. Die Aufbewahrungsdauer des ursprünglichen Buckets bleibt erhalten.
- **Nicht gesperrten Bucket wiederherstellen**: Selbst wenn die Objektsperrung für einen Bucket nicht aktiviert ist, kann er in einem Bucket wiederhergestellt werden, in dem die Objektsperrung aktiviert ist und der sich im Quell-Cluster befindet. Beim Wiederherstellen des Buckets werden alle nicht gesperrten Objekte gesperrt, und der Aufbewahrungsmodus sowie die Aufbewahrungsdauer des Ziel-Buckets gelten für diese Objekte.

CLI

1. Wenn Sie Objekte in einem neuen Bucket wiederherstellen, muss der neue Bucket erstellt werden. Weitere Informationen finden sich unter "Eine Cloud-Backup-Beziehung für einen neuen ONTAP S3 Bucket erstellen".
2. Einen Wiederherstellungsvorgang für den Ziel-Bucket initiieren:
   `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
   ```

   Weitere Informationen zu `snapmirror restore` finden sich in der "ONTAP-Befehlsreferenz".

Backup-Schutz mit Cloud-Zielen

Anforderungen für ONTAP SnapMirror S3 Cloud-Zielbeziehungen

Stellen Sie sicher, dass Ihre Quell- und Zielumgebungen die Anforderungen für

SnapMirror S3-Backup-Schutz in Cloud-Zielen erfüllen.

Sie benötigen gültige Zugangsdaten beim Objektspeicheranbieter, um auf den Daten-Bucket zugreifen zu können.

Intercluster LIFs und ein IPspace sollten auf dem Cluster konfiguriert werden, bevor der Cluster eine Verbindung zu einem Cloud Objektspeicher herstellen kann. Intercluster LIFs sollten auf jedem Knoten erstellt werden, um Daten nahtlos vom lokalen Speicher in den Cloud Objektspeicher zu übertragen.

Für StorageGRID Ziele sind folgende Informationen erforderlich:

- Servername, angegeben als vollqualifizierter Domänenname (FQDN) oder IP-Adresse
- Bucket Name; der Bucket muss bereits existieren
- Zugangsschlüssel
- geheimer Schlüssel

Zusätzlich muss das CA-Zertifikat, mit dem das StorageGRID Serverzertifikat signiert wurde, auf der Admin-Storage-VM des ONTAP S3-Clusters mithilfe des `security certificate install` Befehls installiert werden. Weitere Informationen finden sich unter "Installation eines CA-Zertifikats", wenn StorageGRID verwendet wird.

Für AWS S3-Ziele benötigen Sie die folgenden Informationen:

- Servername, angegeben als vollqualifizierter Domänenname (FQDN) oder IP-Adresse
- Bucket Name; der Bucket muss bereits existieren
- Zugangsschlüssel
- geheimer Schlüssel

Der DNS-Server für die Admin-Speicher-VM des ONTAP-Clusters muss in der Lage sein, FQDNs (falls verwendet) in IP-Adressen aufzulösen.

Verwandte Informationen

- "Sicherheitszertifikat installieren"

Eine Cloud-Backup-Beziehung für einen neuen ONTAP S3 Bucket erstellen

Wenn neue S3-Buckets erstellt werden, können diese sofort in einem SnapMirror S3-Ziel-Bucket bei einem Objektspeicher-Anbieter gesichert werden, wobei es sich um ein StorageGRID System oder eine Amazon S3-Bereitstellung handeln kann.

Bevor Sie beginnen

- Sie verfügen über gültige Kontoanmeldeinformationen und Konfigurationsinformationen für den Objektspeicheranbieter.
- Intercluster-Netzwerkschnittstellen und ein IPspace wurden auf dem Quellsystem konfiguriert.
- Die DNS-Konfiguration für die Quell-Speicher-VM muss den FQDN des Ziels auflösen können.

System Manager

1. Die Storage-VM wird bearbeitet, um Benutzer hinzuzufügen und Benutzer Gruppen zuzuordnen:

a. Klicken Sie auf **Speicher > Speicher-VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und dann auf unter **S3**.

   Siehe "S3-Benutzer und Gruppen hinzufügen" für weitere Informationen.

2. Einen Cloud-Objektspeicher zum Quellsystem hinzufügen:
   a. **Schutz > Übersicht** auswählen und anschließend **Cloud Object Stores** wählen.
   b. Klicken Sie auf **Hinzufügen** und wählen Sie dann **Amazon S3** oder **StorageGRID** aus.
   c. Geben Sie die folgenden Werte ein:
      - Name des Cloud-Objektspeichers
      - URL-Stil (Pfad oder virtual-hosted)
      - Storage VM (für S3 aktiviert)
      - Name des Objektspeicher-Servers (FQDN)
      - Objektspeicherzertifikat
      - Zugangsschlüssel
      - Geheimer Schlüssel
      - Containername (Bucket)
3. Eine SnapMirror S3-Richtlinie kann erstellt werden, falls keine vorhanden ist und die Standardrichtlinie nicht verwendet werden soll:
   a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Lokale Richtlinieneinstellungen**.
   b. Klicken Sie neben **Schutzrichtlinien** und dann auf **Hinzufügen**.
      - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
      - Den Richtlinienbereich, den Cluster oder die SVM auswählen
      - **Kontinuierlich** für SnapMirror S3-Beziehungen auswählen.
      - Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
4. Einen Bucket mit SnapMirror-Schutz erstellen:
   a. Klicken Sie auf **Speicher > Buckets** und anschließend auf **Hinzufügen**.
   b. Geben Sie einen Namen ein, wählen Sie die Storage-VM aus, geben Sie eine Größe ein und klicken Sie dann auf **Weitere Optionen**.
   c. Unter **Berechtigungen** auf **Hinzufügen** klicken. Die Überprüfung der Berechtigungen ist optional, aber empfehlenswert.
      - **Principal** und **Effect**: Werte auswählen, die den Einstellungen der Benutzergruppe entsprechen, oder die Standardwerte übernehmen.
      - **Aktionen**: Die folgenden Werte sollten angezeigt werden:

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

      - **Ressourcen**: Die Standardwerte `_(bucketname, bucketname/*)` oder andere benötigte Werte verwenden.

Weitere Informationen zu diesen Bereichen sind unter "Benutzerzugriff auf Buckets verwalten" zu finden.

d. Unter **Schutz** die Option **Enable SnapMirror (ONTAP oder Cloud)** aktivieren, **Cloud Storage** auswählen und dann den **Cloud Object Store** auswählen.

Wenn Sie auf **Speichern** klicken, wird ein neuer Bucket in der Quell-Speicher-VM erstellt und im Cloud-Objektspeicher gesichert.

CLI

1. Wenn dies die erste SnapMirror S3-Beziehung für diese SVM ist, muss überprüft werden, ob Root-Benutzerschlüssel für sowohl Quell- als auch Ziel-SVMs vorhanden sind, und sie müssen neu generiert werden, falls sie nicht existieren:
`vserver object-store-server user show` Es sollte bestätigt werden, dass ein Zugriffsschlüssel für den Root-Benutzer vorhanden ist. Falls keiner vorhanden ist, ist Folgendes einzugeben:
`vserver object-store-server user regenerate-keys -vserver svm_name -user root` + Der Schlüssel darf nicht neu generiert werden, wenn bereits einer existiert.

2. Erstellen eines Buckets in der Quell-SVM:
`vserver object-store-server bucket create -vserver svm_name -bucket bucket_name [-size integer[KB|MB|GB|TB|PB]] [-comment text] [additional_options]`

3. Zugriffsregeln zur Standard-Bucket-Richtlinie hinzufügen:
`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 SnapMirror S3-Richtlinie, falls Sie noch keine haben und nicht die Standardrichtlinie verwenden möchten:
`snapmirror policy create -vserver svm_name -policy policy_name -type continuous [-rpo integer] [-throttle throttle_type] [-comment text] [additional_options]`

   Parameter: * `type continuous` – der einzige Richtlinientyp für SnapMirror S3-Beziehungen (erforderlich). * `-rpo` – gibt die Zeit bis zum Wiederherstellungspunkt in Sekunden an (optional). * `-throttle` – gibt die Obergrenze für Durchsatz/Bandbreite in Kilobyte/Sekunde an (optional).

   Beispiel

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

```
-rpo 0 -policy test-policy
```

5. Wenn das Ziel ein StorageGRID System ist, das StorageGRID CA Serverzertifikat auf der Admin-SVM des Quell-Cluster installieren:
`security certificate install -type server-ca -vserver src_admin_svm -cert -name storage_grid_server_certificate`

   Weitere Informationen zu `security certificate install` finden sich in der "ONTAP-Befehlsreferenz".

6. Den SnapMirror S3 Objektspeicher als Ziel definieren:
`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`

   Parameter: * `-object-store-name` – der Name des Objektspeicherziels auf dem lokalen ONTAP System. * `-usage` – `data` für diesen Workflow verwenden. * `-provider-type` – `AWS_S3` und `SGWS` (StorageGRID) Ziele werden unterstützt. * `-server` – der FQDN oder die IP-Adresse des Zielservers. * `-is-ssl-enabled` – die Aktivierung von SSL ist optional, aber empfohlen. + Weitere Informationen zu `snapmirror object-store config create` in der "ONTAP-Befehlsreferenz".

   Beispiel

   ```
   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. Erstellen einer SnapMirror S3-Beziehung:
`snapmirror create -source-path svm_name:/bucket/bucket_name -destination -path object_store_name:/objstore -policy policy_name`

   Parameter: * `-destination-path` – der im vorherigen Schritt erstellte Objektspeichername und der feste Wert `objstore`. + Es kann eine selbst erstellte Richtlinie verwendet oder die Standardrichtlinie übernommen werden.

   Beispiel

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

8. Es sollte überprüft werden, ob die Spiegelung aktiv ist:
`snapmirror show -policy-type continuous -fields status`

Verwandte Informationen

- "snapmirror create"

- "snapmirror policy create"
- "snapmirror show"

Eine Cloud-Backup-Beziehung für einen vorhandenen ONTAP S3 Bucket erstellen

Sie können jederzeit mit der Sicherung bestehender S3 Buckets beginnen, beispielsweise wenn eine S3 Konfiguration von einer Version vor ONTAP 9.10.1 aktualisiert wurde.

Bevor Sie beginnen

- Sie verfügen über gültige Kontoanmeldeinformationen und Konfigurationsinformationen für den Objektspeicheranbieter.
- Intercluster-Netzwerkschnittstellen und ein IPspace wurden auf dem Quellsystem konfiguriert.
- Die DNS-Konfiguration für die Quell-Speicher-VM muss den FQDN des Ziels auflösen können.

System Manager

1. Überprüfen Sie, ob die Benutzer und Gruppen korrekt definiert sind: Klicken Sie auf **Speicher > Speicher-VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und dann auf unter S3.

   Siehe "S3-Benutzer und Gruppen hinzufügen" für weitere Informationen.

2. Eine SnapMirror S3-Richtlinie kann erstellt werden, wenn noch keine vorhanden ist und die Standardrichtlinie nicht verwendet werden soll:
   a. **Schutz > Übersicht** und danach **Lokale Richtlinieneinstellungen** auswählen.
   b. Klicken Sie → neben **Schutzrichtlinien** und dann auf **Hinzufügen**.
   c. Geben Sie den Namen und die Beschreibung der Richtlinie ein.
   d. Den Richtlinienbereich, den Cluster oder die SVM auswählen
   e. **Kontinuierlich** für SnapMirror S3-Beziehungen auswählen.
   f. Geben Sie Ihre **Throttle**- und **Recovery Point Objective**-Werte ein.
3. Einen Cloud-Objektspeicher zum Quellsystem hinzufügen:
   a. **Schutz > Übersicht** auswählen und anschließend **Cloud Object Store** wählen.
   b. Wählen Sie **Hinzufügen** und dann **Amazon S3** oder **Andere** für StorageGRID Webscale aus.
   c. Geben Sie die folgenden Werte ein:
      - Name des Cloud-Objektspeichers
      - URL-Stil (Pfad oder virtual-hosted)
      - Storage VM (für S3 aktiviert)
      - Name des Objektspeicher-Servers (FQDN)
      - Objektspeicherzertifikat
      - Zugangsschlüssel
      - Geheimer Schlüssel
      - Containername (Bucket)

4. Es sollte geprüft werden, ob die Zugriffsrichtlinie des bestehenden Buckets weiterhin den eigenen Anforderungen entspricht:
   a. Klicken Sie auf **Speicher** > **Buckets** und wählen Sie dann den Bucket aus, den Sie schützen möchten.
   b. Im Tab **Berechtigungen** auf **Bearbeiten** klicken, dann unter **Berechtigungen** auf **Hinzufügen** klicken.
      - **Principal** und **Effect** – Werte auswählen, die den Einstellungen Ihrer Benutzergruppe entsprechen, oder die Standardwerte übernehmen.
      - **Aktionen** – es wird sichergestellt, dass die folgenden Werte angezeigt werden: `GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts`
      - **Ressourcen** – Standardwerte *(bucketname, bucketname/*)* oder andere benötigte Werte verwenden.

        Weitere Informationen zu diesen Bereichen sind unter "Benutzerzugriff auf Buckets verwalten" zu finden.

5. Den Bucket mit SnapMirror S3 sichern:
   a. Klicken Sie auf **Speicher** > **Buckets** und wählen Sie dann den Bucket aus, den Sie sichern möchten.
   b. Klicken Sie auf **Schützen**, wählen Sie unter **Ziel Cloud-Speicher** und anschließend den **Cloud Object Store** aus.

Wenn Sie auf **Speichern** klicken, wird der bestehende Bucket im Cloud-Objektspeicher gesichert.

CLI

1. Es sollte überprüft werden, ob die Zugriffsregeln in der Standard Bucket-Richtlinie 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 /*
   ```

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

   Parameter: * `type continuous` – der einzige Richtlinientyp für SnapMirror S3-Beziehungen (erforderlich). * `-rpo` – gibt die Zeit bis zum Wiederherstellungspunkt in Sekunden an (optional). * `-throttle` – gibt die Obergrenze für Durchsatz/Bandbreite in Kilobyte/Sekunde an (optional).

Beispiel

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

3. Wenn das Ziel ein StorageGRID System ist, das StorageGRID CA-Zertifikat auf der Admin-SVM des Quell-Cluster installieren:
`security certificate install -type server-ca -vserver src_admin_svm -cert -name storage_grid_server_certificate`

   Weitere Informationen zu `security certificate install` finden sich in der "ONTAP-Befehlsreferenz".

4. Den SnapMirror S3 Objektspeicher als Ziel definieren:
`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`

   Parameter: * `-object-store-name` – der Name des Objektspeicherziels auf dem lokalen ONTAP System. * `-usage` – `data` für diesen Workflow verwenden. * `-provider-type` – `AWS_S3` und `SGWS` (StorageGRID) Ziele werden unterstützt. * `-server` – der FQDN oder die IP-Adresse des Zielservers. * `-is-ssl-enabled` – die Aktivierung von SSL ist optional, aber empfohlen. + Weitere Informationen zu `snapmirror object-store config create` in der "ONTAP-Befehlsreferenz".

   Beispiel

```
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. Erstellen einer SnapMirror S3-Beziehung:
`snapmirror create -source-path svm_name:/bucket/bucket_name -destination -path object_store_name:/objstore -policy policy_name`

   Parameter: * `-destination-path` – der im vorherigen Schritt erstellte Objektspeichername und der feste Wert `objstore`. + Es kann eine selbst erstellte Richtlinie verwendet oder die Standardrichtlinie übernommen werden.

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

6. Es sollte überprüft werden, ob die Spiegelung aktiv ist:
`snapmirror show -policy-type continuous -fields status`

Verwandte Informationen

- "snapmirror create"
- "snapmirror policy create"
- "snapmirror show"

Wiederherstellung eines ONTAP S3-Buckets aus einem Cloud-Ziel

Wenn Daten in einem Quell-Bucket verloren gehen oder beschädigt werden, lässt sich der Datenbestand durch Wiederherstellung aus einem Ziel-Bucket wieder auffüllen.

Über diese Aufgabe

Sie können den Ziel-Bucket in einem vorhandenen Bucket oder in einem neuen Bucket wiederherstellen. Der Ziel-Bucket für die Wiederherstellung muss größer sein als der logisch genutzte Speicherplatz des Ziel-Buckets.

Wenn Sie einen vorhandenen Bucket verwenden, muss dieser beim Start einer Wiederherstellungsoperation leer sein. Die Wiederherstellung führt kein „Rollback“ eines Buckets in der Zeit durch, sondern füllt einen leeren Bucket mit seinem vorherigen Inhalt.

System Manager

Die Sicherungsdaten wiederherstellen:

1. **Schutz > Beziehungen** auswählen und dann **SnapMirror S3** wählen.
2. Klicken Sie ⋮ und wählen Sie dann **Wiederherstellen**.
3. Unter **Quelle Vorhandener Bucket** (Standardeinstellung) oder **Neuer Bucket** auswählen.
   - Um auf einen **vorhandenen Bucket** (Standardeinstellung) wiederherzustellen, sind folgende Schritte erforderlich:
     - Den Cluster und die Storage-VM auswählen, um nach dem vorhandenen Bucket zu suchen.
     - Wählen Sie den vorhandenen Bucket aus.
     - Kopieren und fügen Sie den Inhalt des *destination* S3-Server-CA-Zertifikats ein.
   - Für die Wiederherstellung in einem **neuen Bucket** sind die folgenden Werte anzugeben:
     - Der Cluster und die Storage-VM zum Hosten des neuen Buckets.
     - Name, Kapazität und Leistungsservicelevel des neuen Buckets. Siehe "Storage-Servicelevel" für weitere Informationen.
     - Der Inhalt des CA-Zertifikats des Ziel-S3-Servers.
4. Unter **Ziel** den Inhalt des CA-Zertifikats des *source* S3-Servers kopieren und einfügen.
5. **Schutz > Beziehungen** kann zur Überwachung des Wiederherstellungsfortschritts verwendet werden.

CLI Prozedur

1. Den neuen Ziel-Bucket für die Wiederherstellung erstellen. Weitere Informationen finden sich unter "Erstellen einer Backup-Beziehung für einen Bucket (Cloud-Ziel)".
2. Einen Wiederherstellungsvorgang für den Ziel-Bucket initiieren:
   `snapmirror restore -source-path` *`object_store_name`*`:/objstore -destination -path` *`svm_name`*`:/bucket/`*`bucket_name`*

Beispiel

Das folgende Beispiel stellt einen Ziel-Bucket in einem bestehenden Bucket wieder her.

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

Weitere Informationen zu `snapmirror restore` finden sich in der "ONTAP-Befehlsreferenz".

Eine ONTAP SnapMirror S3-Richtlinie ändern

Möglicherweise wird eine S3 SnapMirror Richtlinie geändert, wenn eine Anpassung der RPO- und Drosselungswerte erforderlich ist.

System Manager

1. Klicken Sie auf **Schutz > Beziehungen** und wählen Sie dann die Datensicherungsstrategie für die Beziehung aus, die Sie ändern möchten.
2. Klicken Sie ⋮ neben dem Namen der Policy und dann auf **Bearbeiten**.

CLI

Eine SnapMirror S3-Richtlinie ändern:

```
snapmirror policy modify -vserver <svm_name> -policy <policy_name> [-rpo
<integer>] [-throttle <throttle_type>] [-comment <text>]
```

Parameter:

- `-rpo`: Gibt die Zeit für das Recovery Point Objective in Sekunden an.
- `-throttle`: Gibt die Obergrenze für Durchsatz/Bandbreite in Kilobyte/Sekunde an.

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

Verwandte Informationen

- "snapmirror policy modify"

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.