



# Sicherung von Buckets mit SnapMirror S3

ONTAP 9

NetApp  
January 17, 2025

# Inhalt

- Sicherung von Buckets mit SnapMirror S3 ..... 1
  - SnapMirror S3 Übersicht ..... 1
  - Spiegelung und Backup-Schutz auf einem Remote-Cluster ..... 3
  - Spiegelung und Backup-Schutz auf dem lokalen Cluster ..... 14
  - Backup-Sicherung mit Cloud-Zielen ..... 25
  - Ändern einer Spiegelrichtlinie ..... 34

# Sicherung von Buckets mit SnapMirror S3

## SnapMirror S3 Übersicht

Ab ONTAP 9.10.1 können Buckets in ONTAP S3 Objektspeichern mithilfe von SnapMirror Spiegelungs- und Backup-Funktion gesichert werden. Im Gegensatz zu Standard-SnapMirror ermöglicht SnapMirror S3 Spiegelung und Backups an nicht-NetApp-Ziele wie AWS S3.

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

Ziel	Unterstützt aktive Spiegelungen und Takeover?	Unterstützung für Backup und Restore?
ONTAP S3 <ul style="list-style-type: none"><li>• Buckets in derselben SVM</li><li>• Buckets in verschiedenen SVMs im selben Cluster</li><li>• Buckets in SVMs auf verschiedenen Clustern</li></ul>	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 vorhandene Buckets auf ONTAP S3 Servern sichern oder neue Buckets erstellen, wobei die Datensicherung sofort aktiviert ist.

## Anforderungen für SnapMirror S3

- ONTAP-Version

ONTAP 9.10.1 oder höher muss auf Quell- und Ziel-Clustern ausgeführt werden.

- Lizenzierung

Die folgenden Lizenzen sind in der **"ONTAP One"** Softwaresuite verfügbar, die auf den Quell- und Zielsystemen von ONTAP erforderlich sind, um Zugriff auf:

- ONTAP S3 Protokoll und Storage
- SnapMirror S3 als Ziel für andere NetApp Objektspeicher-Ziele (ONTAP S3, StorageGRID und Cloud Volumes ONTAP)
- SnapMirror S3 für Objektspeicher von Drittanbietern, einschließlich AWS S3 (verfügbar im **"ONTAP One Kompatibilitätspaket"**)

- ONTAP S3
  - ONTAP S3 Server müssen Quell- und Ziel-SVMs ausführen.
  - Es wird empfohlen, aber nicht erforderlich, dass CA-Zertifikate für TLS-Zugriff auf Systemen installiert werden, die S3-Server hosten.
    - Die Zertifizierungsstellenzertifikate, die zum Signieren der S3-Serverzertifikate verwendet werden, müssen auf der Admin-Speicher-VM der Cluster installiert werden, die S3-Server hosten.
    - Sie können ein selbstsigniertes CA-Zertifikat oder ein Zertifikat verwenden, das von einem externen CA-Anbieter signiert wurde.
    - Wenn die Quell- oder Ziel-Storage-VMs nicht HTTPS zuhören, ist es nicht erforderlich, CA-Zertifikate zu installieren.
- Peering (für ONTAP S3 Ziele)
  - Intercluster LIFs müssen konfiguriert werden (für Remote ONTAP Ziele). Die Intercluster LIFs des Quell- und Ziel-Clusters können mit den S3-Daten-LIFs des Quell- und Ziel-Servers verbunden werden.
  - Quell- und Ziel-Cluster werden (für Remote-ONTAP-Ziele) per Peering durchgeführt.
  - Quell- und Ziel-Storage VMs werden (für alle ONTAP Ziele) Peered.
- SnapMirror-Richtlinie
  - Eine S3-spezifische SnapMirror-Richtlinie ist für alle SnapMirror S3-Beziehungen erforderlich, Sie können jedoch für mehrere Beziehungen dieselbe Richtlinie verwenden.
  - Sie können Ihre eigene Richtlinie erstellen oder die standardmäßige **Continuous**-Richtlinie akzeptieren, die die folgenden Werte enthält:
    - Drosselklappe (oberer Grenzwert für Durchsatz/Bandbreite) – unbegrenzt.
    - Zeit für Recovery-Zeitpunkt: 1 Stunde (3600 Sekunden).



Sie sollten beachten, dass wenn sich zwei S3-Buckets in einer SnapMirror Beziehung befinden und Lifecycle-Richtlinien so konfiguriert sind, dass die aktuelle Version eines Objekts abläuft (gelöscht wird), wird dieselbe Aktion auch in den Partner-Bucket repliziert. Dies gilt selbst dann, wenn der Partner-Bucket schreibgeschützt oder passiv ist.

- Root-Benutzerschlüssel Storage VM Root-Benutzerzugriffsschlüssel sind für SnapMirror S3-Beziehungen erforderlich; ONTAP weist diese standardmäßig nicht zu. Wenn Sie zum ersten Mal eine SnapMirror S3-Beziehung erstellen, müssen Sie überprüfen, ob die Schlüssel sowohl auf Quell- als auch auf den Ziel-Storage-VMs vorhanden sind, und sie erneut erstellen, wenn dies nicht der Fall ist. Wenn Sie sie neu generieren müssen, müssen Sie sicherstellen, dass alle Clients und alle SnapMirror Objektspeicher-Konfigurationen unter Verwendung des Zugriffs- und geheimen Schlüsselpaars mit den neuen Schlüsseln aktualisiert werden.

Informationen zur S3-Serverkonfiguration finden Sie unter den folgenden Themen:

- ["Aktivieren eines S3-Servers auf einer Storage-VM"](#)
- ["Allgemeines zum ONTAP S3-Konfigurationsprozess"](#)

Informationen über Cluster und Storage VM Peering finden Sie unter folgendem Thema:

- ["Vorbereiten auf Spiegelung und Vaulting \(System Manager, Schritte 1–6\)"](#)
- ["Cluster- und SVM-Peering \(CLI\)"](#)

## Unterstützte SnapMirror Beziehungen

SnapMirror S3 unterstützt Fan-out- und Kaskadenbeziehungen. Eine Übersicht finden Sie unter ["Fan-out- und kaskadierende Datensicherungsimplementierungen"](#).

SnapMirror S3 unterstützt keine Fan-in-Implementierungen (Datensicherungsbeziehungen zwischen mehreren Quell-Buckets und einem einzelnen Ziel-Bucket). SnapMirror S3 kann mehrere Bucket-Spiegelungen von mehreren Clustern auf ein einzelnes sekundäres Cluster unterstützen, aber jeder Quell-Bucket muss auf dem sekundären Cluster über einen eigenen Ziel-Bucket verfügen.

## Steuerung des Zugriffs auf S3 Buckets

Beim Erstellen neuer Buckets können Sie den Zugriff durch Erstellen von Benutzern und Gruppen steuern. Weitere Informationen finden Sie in den folgenden Themen:

- ["Hinzufügen von S3-Benutzern und -Gruppen \(System Manager\)"](#)
- ["Erstellen eines S3-Benutzers \(CLI\)"](#)
- ["S3-Gruppen erstellen oder ändern \(CLI\)"](#)

## Spiegelung und Backup-Schutz auf einem Remote-Cluster

### Erstellen einer Spiegelbeziehung für einen neuen Bucket (Remote-Cluster)

Wenn neue S3-Buckets erstellt werden, können sie sofort auf einem SnapMirror S3-Ziel auf einem Remote-Cluster geschützt werden.



#### Über diese Aufgabe


Sie müssen Aufgaben sowohl auf Quell- als auch auf Zielsystemen ausführen.

#### Bevor Sie beginnen


- Die Anforderungen für ONTAP-Versionen, Lizenzierung und S3-Serverkonfiguration wurden erfüllt.
- Zwischen Quell- und Ziel-Clustern ist eine Peering-Beziehung vorhanden, während zwischen Quell- und Ziel-Storage VMs eine Peering-Beziehung besteht.
- 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 SnapMirror S3-Beziehung für diese Storage-VM ist, überprüfen Sie, ob Root-Benutzerschlüssel sowohl für Quell- als auch für Ziel-Storage-VMs vorhanden sind, und regenerieren Sie sie erneut, wenn dies nicht der Fall ist:
  - a. Klicken Sie auf **Storage > Storage VMs** und wählen Sie dann die Speicher-VM aus.
  - b. Klicken Sie im Register **Einstellungen** auf  die Kachel **S3**.
  - c. Überprüfen Sie auf der Registerkarte **Benutzer**, ob für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist.
  - d. Wenn nicht, klicken Sie  neben **root** und dann auf **regenerieren-Schlüssel**. Generieren Sie den Schlüssel nicht neu, wenn er bereits vorhanden ist.
2. Bearbeiten Sie die Storage VM, um Benutzer hinzuzufügen und Benutzern zu Gruppen hinzuzufügen, sowohl im Quell- als auch im Ziel-Storage der VMs:

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

Weitere Informationen finden Sie unter "[Fügen Sie S3-Benutzer und -Gruppen hinzu](#)".

3. Erstellen Sie auf dem Quell-Cluster eine SnapMirror S3-Richtlinie, wenn keine vorhandene Richtlinie vorhanden ist und Sie die Standardrichtlinie nicht verwenden möchten:
  - 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.
    - Wählen Sie den Richtlinienumfang, das Cluster oder die SVM aus
    - Wählen Sie **kontinuierlich** für SnapMirror S3-Beziehungen aus.
    - 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**. Die Überprüfung der Berechtigungen ist optional, wird aber empfohlen.
  - 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**.
    - **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.

["Management des Benutzerzugriffs auf Buckets"](#)Weitere Informationen zu diesen Feldern finden Sie unter.

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 Remote-Cluster aus.
    - **STORAGE VM**: Wählen Sie eine Speicher-VM auf dem Remote-Cluster aus.
    - **S3-SERVER-CA-ZERTIFIKAT**: Kopieren Sie den Inhalt des *source*-Zertifikats.
  - Quelle
    - **S3-SERVER-CA-ZERTIFIKAT**: Kopieren und Einfügen des Inhalts des *Destination*-Zertifikats.
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 Objektsperre für Ziel-Buckets aktivieren, sofern auf den Quell- und Ziel-Clustern ONTAP 9.14.1 oder höher ausgeführt wird und die Objektsperre 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 Objektsperre auf einem Bucket finden Sie unter "[Erstellen eines Buckets](#)".

### CLI

1. Wenn es sich hierbei um die erste SnapMirror S3-Beziehung für diese SVM handelt, überprüfen Sie, ob Root-Benutzerschlüssel für Quell- und Ziel-SVMs vorhanden sind, und regenerieren Sie sie erneut, wenn dies nicht der Fall ist:

```
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]
```

#### 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. Erstellen Sie auf der Quell-SVM eine SnapMirror S3-Richtlinie, wenn keine bereits vorhanden ist 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:

- Typ `continuous`: Die einzige Richtlinienart für SnapMirror S3-Beziehungen (erforderlich).
- `-rpo` - Gibt die Zeit für die Recovery Point Objective 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 von CA-Server-Zertifikaten auf den Administrator-SVMs der Quell- und Ziel-Cluster:

- a. Installieren Sie auf dem Quell-Cluster das CA-Zertifikat, das das *Destination* 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 *Source* S3-Serverzertifikat signiert hat:

```
security certificate install -type server-ca -vserver dest_admin_svm
-cert-name src_server_certificate
```

Wenn Sie ein von einem externen CA-Anbieter signiertes Zertifikat verwenden, installieren Sie dasselbe Zertifikat auf der Quell- und Ziel-Administrator-SVM.



Einzelheiten dazu finden Sie auf der `security certificate install man`-Page.

6. Erstellen Sie auf der Quell-SVM eine 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 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. Vergewissern Sie sich, dass die Spiegelung aktiv ist:

```
snapmirror show -policy-type continuous -fields status
```

## Erstellen einer Spiegelbeziehung für einen vorhandenen Bucket (Remote-Cluster)

Sie können jederzeit damit beginnen, vorhandene S3-Buckets zu schützen. Wenn Sie beispielsweise eine S3-Konfiguration von einer älteren Version als ONTAP 9.10.1 aktualisiert haben.

### Über diese Aufgabe

Sie müssen Aufgaben sowohl auf den Quell- als auch auf den Ziel-Clustern ausführen.

### Bevor Sie beginnen

- Die Anforderungen für ONTAP-Versionen, Lizenzierung und S3-Serverkonfiguration wurden erfüllt.
- Zwischen Quell- und Ziel-Clustern ist eine Peering-Beziehung vorhanden, während zwischen Quell- und Ziel-Storage VMs eine Peering-Beziehung besteht.
- 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.



### Schritte

Sie können eine Spiegelbeziehung mit System Manager oder der ONTAP CLI erstellen.

## System Manager

1. Wenn dies die erste SnapMirror S3-Beziehung für diese Storage-VM ist, überprüfen Sie, ob Root-Benutzerschlüssel sowohl für Quell- als auch für Ziel-Storage-VMs vorhanden sind, und regenerieren Sie sie erneut, wenn dies nicht der Fall ist:
  - a. Wählen Sie **Storage > Storage VMs** aus und wählen Sie dann die Storage VM aus.
  - b. Klicken Sie im Register **Einstellungen** auf  die Kachel **S3**.
  - c. Überprüfen Sie auf der Registerkarte **Benutzer**, ob für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist.
  - d. Wenn nicht, klicken Sie  neben **root** und dann auf **regenerieren-Schlüssel**. Generieren Sie den Schlüssel nicht neu, wenn er bereits vorhanden ist.
2. Überprüfen Sie, ob vorhandene Benutzer und Gruppen vorhanden sind und den richtigen Zugriff auf die Quell- und Zielspeicher-VMs haben: Wählen Sie **Speicher > Speicher-VMs**, wählen Sie dann die Speicher-VM und dann **Einstellungen** Tab. Suchen Sie schließlich die Kachel **S3**, wählen Sie , und wählen Sie die Registerkarte **Benutzer** und dann die Registerkarte **Gruppen**, um die Benutzer- und Gruppenzugriffseinstellungen anzuzeigen.

Weitere Informationen finden Sie unter "[Fügen Sie S3-Benutzer und -Gruppen hinzu](#)".

3. Erstellen Sie auf dem Quell-Cluster eine SnapMirror S3-Richtlinie, wenn keine vorhandene Richtlinie vorhanden ist und Sie die Standardrichtlinie nicht verwenden möchten:
  - a. Wählen Sie **Schutz > Übersicht** und klicken Sie dann auf **Einstellungen für lokale Richtlinien**.
  - b. Wählen Sie neben **Schutzrichtlinien** aus , und klicken Sie dann auf **Hinzufügen**.
  - c. Geben Sie den Namen und die Beschreibung der Richtlinie ein.
  - d. Wählen Sie den Richtlinienumfang aus – entweder Cluster oder SVM.
  - e. Wählen Sie **kontinuierlich** für SnapMirror S3-Beziehungen aus.
  - f. 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 im Register **Berechtigungen** auf  **Bearbeiten** und dann unter **Berechtigungen** auf **Hinzufügen**.
    - **Principal und Effect:** Wählen Sie die Werte, die Ihren Benutzergruppeneinstellungen entsprechen, oder übernehmen Sie die Standardeinstellungen.
    - **Aktionen:** Stellen Sie sicher, dass folgende Werte angezeigt werden:

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

- **Ressourcen:** Verwenden Sie die Standardwerte (*bucketname*, *bucketname/\**) oder andere Werte, die Sie benötigen.

["Management des Benutzerzugriffs auf Buckets"](#)Weitere Informationen zu diesen Feldern finden Sie unter.

5. Schützen Sie einen vorhandenen Bucket mit SnapMirror S3-Sicherung:
  - 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 Remote-Cluster aus.
      - **STORAGE VM:** Wählen Sie eine Speicher-VM auf dem Remote-Cluster aus.
      - **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 Objektsperre für Ziel-Buckets aktivieren, sofern auf den Quell- und Ziel-Clustern ONTAP 9.14.1 oder höher ausgeführt wird und die Objektsperre 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 Objektsperre auf einem Bucket finden Sie unter ["Erstellen eines Buckets"](#).

### CLI

1. Wenn dies die erste SnapMirror S3-Beziehung für diese SVM ist, überprüfen Sie, ob Root-Benutzerschlüssel für Quell- und Ziel-SVMs vorhanden sind, und regenerieren Sie sie, wenn sie `vserver object-store-server user show` dies nicht tun: + Überprüfen Sie, ob es einen Zugriffsschlüssel für den Root-Benutzer gibt. Wenn nicht, geben Sie ein:
 

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

 + Den Schlüssel nicht neu generieren, 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. Überprüfen Sie, ob die Zugriffsregeln der 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

```
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 auf der Quell-SVM eine SnapMirror S3-Richtlinie, wenn Sie keine vorhandene Richtlinie 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` – Die einzige Richtlinienart für SnapMirror S3 Beziehungen (erforderlich).
- `-rpo` – Gibt die Zeit für Recovery Point Objective 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 von CA-Zertifikaten auf den Administrator-SVMs von Quell- und Ziel-Clustern:

- a. Installieren Sie auf dem Quell-Cluster das CA-Zertifikat, das das *Destination* 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 *source* S3-Serverzertifikat signiert hat: + Wenn Sie ein von einem externen CA-Anbieter signiertes Zertifikat verwenden, installieren Sie dasselbe Zertifikat auf der Quell- und Ziel-Admin-SVM.

Einzelheiten dazu finden Sie auf der `security certificate install man`-Page.

6. Erstellen Sie auf der Quell-SVM eine 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 Standardeinstellung übernehmen.

#### Beispiel

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

7. Vergewissern Sie sich, dass die Spiegelung aktiv ist:

```
snapmirror show -policy-type continuous -fields status
```

## Übernahme und Bereitstellung von Daten vom Ziel-Bucket (Remote-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 Quell-Bucket in schreibgeschützt konvertiert und der ursprüngliche Ziel-Bucket in Lese-/Schreibzugriff konvertiert, um die SnapMirror S3-Beziehung rückgängig zu machen.

Wenn der deaktivierte Quell-Bucket wieder verfügbar ist, synchronisiert SnapMirror S3 den Inhalt der beiden Buckets automatisch neu. Es ist nicht erforderlich, die Beziehung explizit neu zu synchronisieren, wie es für Volume SnapMirror Implementierungen erforderlich ist.

Der Takeover-Vorgang muss 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 **SnapMirror S3** aus.
2. Klicken Sie auf , wählen Sie **Failover** und klicken Sie dann auf **Failover**.

### CLI

1. Initiieren Sie einen Failover-Vorgang 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

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

## Wiederherstellung eines Buckets aus der Ziel-Storage-VM (Remote-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 Speicherplatz des Ziel-Buckets.

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 Remote-Cluster initiiert werden.

## System Manager

Gesicherte Daten wiederherstellen:

1. Klicken Sie auf **Schutz > Beziehungen**, und wählen Sie dann **SnapMirror S3** 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.
    - Kopieren Sie den Inhalt des CA-Zertifikats des *Destination* S3-Servers 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 Weitere Informationen finden Sie unter "[Storage Service Level](#)".
    - Der Inhalt des CA-Zertifikats des *Destination* S3-Servers.
4. Kopieren Sie unter **Destination** den Inhalt des CA-Zertifikats *source* S3-Server.
5. 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 Objektsperre aktiviert ist, kann ein Bucket wiederhergestellt werden, indem ein Bucket erstellt wird, für den auch die Objektsperre aktiviert ist. Wenn Sie einen gesperrten Bucket wiederherstellen, werden der Objektsperremodus 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 Objektsperre auf einem Bucket nicht aktiviert ist, können Sie sie in einem Bucket wiederherstellen, der die Objektsperre 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. Erstellen Sie den neuen Ziel-Bucket für die Wiederherstellung. Weitere Informationen finden Sie unter "[Backup-Beziehung für einen neuen Bucket erstellen \(Cloud-Ziel\)](#)".
2. Initiieren Sie einen Wiederherstellungsvorgang für den Ziel-Bucket:

```
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
```

## 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 sofort auf einem SnapMirror S3-Ziel im selben Cluster schützen. 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 SnapMirror S3-Beziehung für diese Storage-VM ist, überprüfen Sie, ob Root-Benutzerschlüssel sowohl für Quell- als auch für Ziel-Storage-VMs vorhanden sind, und regenerieren Sie sie erneut, wenn dies nicht der Fall ist:
  - a. Klicken Sie auf **Storage > Storage VMs** und wählen Sie dann die Speicher-VM aus.
  - b. Klicken Sie im Register **Einstellungen** auf  die Kachel S3.
  - c. Überprüfen Sie auf der Registerkarte **Benutzer**, ob für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist
  - d. Wenn nicht, klicken Sie  neben **root** und dann auf **regenerieren-Schlüssel**. Generieren Sie den Schlüssel nicht neu, wenn er bereits vorhanden ist.
2. Bearbeiten Sie die Speicher-VM zum Hinzufügen von Benutzern und zum Hinzufügen von Benutzern zu Gruppen in den Quell- und Zielspeicher-VMs: Klicken Sie auf **Speicher > Speicher-VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und klicken Sie dann  unter S3.

Weitere Informationen finden Sie unter "[Fügen Sie S3-Benutzer und -Gruppen hinzu](#)".

3. Erstellen Sie eine SnapMirror S3-Richtlinie, wenn Sie keine vorhandene Richtlinie haben und die Standardrichtlinie nicht verwenden möchten:
  - a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Einstellungen für lokale Richtlinien**.
  - b. Klicken Sie  neben **Schutzrichtlinien** und dann auf **Hinzufügen**.
    - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
    - Wählen Sie den Richtlinienumfang, das Cluster oder die SVM aus
    - Wählen Sie **kontinuierlich** für SnapMirror S3-Beziehungen aus.
    - 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

["Management des Benutzerzugriffs auf Buckets"](#) Weitere Informationen zu diesen Feldern finden Sie unter.

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 Objektsperre für Ziel-Buckets aktivieren, sofern auf den Quell- und Ziel-Clustern ONTAP 9.14.1 oder höher ausgeführt wird und die Objektsperre 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 Objektsperre auf einem Bucket finden Sie unter "[Erstellen eines Buckets](#)".

### CLI

1. Wenn es sich hierbei um die erste SnapMirror S3-Beziehung für diese SVM handelt, überprüfen Sie, ob Root-Benutzerschlüssel für Quell- und Ziel-SVMs vorhanden sind, und regenerieren Sie sie erneut, wenn dies nicht der Fall ist:

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

Vergewissern Sie sich, dass für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist. Wenn dies nicht der Fall ist, 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 SnapMirror S3-Richtlinie, wenn Sie keine vorhandene Richtlinie haben und 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* – Die einzige Richtlinienart für SnapMirror S3 Beziehungen (erforderlich).
- *-rpo* – Gibt die Zeit für Recovery Point Objective 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

```
security certificate install -type server-ca -vserver admin_svm -cert
```

-name *dest\_server\_certificate*-Zertifikat, das das *Destination* S3-Serverzertifikat auf der Admin-SVM signiert hat: + Wenn Sie ein Zertifikat verwenden, das von einem externen CA-Anbieter signiert wurde, müssen Sie dieses Zertifikat nur auf der Admin-SVM installieren.

Einzelheiten dazu finden Sie auf der `security certificate install man`-Page.

6. 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 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. Vergewissern Sie sich, dass 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 SnapMirror S3-Beziehung für diese Storage-VM ist, überprüfen Sie, ob Root-Benutzerschlüssel sowohl für Quell- als auch für Ziel-Storage-VMs vorhanden sind, und regenerieren Sie sie erneut, wenn dies nicht der Fall ist:
  - a. Klicken Sie auf **Storage > Storage VMs** und wählen Sie dann die Speicher-VM aus.
  - b. Klicken Sie im Register **Einstellungen** auf  die Kachel **S3**.
  - c. Überprüfen Sie auf der Registerkarte **Benutzer**, ob für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist.
  - d. Wenn nicht, klicken Sie  neben **root** und dann auf **regenerieren-Schlüssel**. Generieren Sie den Schlüssel nicht neu, wenn er bereits vorhanden ist
2. Überprüfen Sie, ob vorhandene Benutzer und Gruppen vorhanden sind und den richtigen Zugriff auf die Quell- und ZielspeicherVMs haben: Wählen Sie **Speicher > Speicher-VMs**, wählen Sie dann die Speicher-VM und dann **Einstellungen** Tab. Suchen Sie schließlich die Kachel **S3**, wählen Sie , und wählen Sie die Registerkarte **Benutzer** und dann die Registerkarte **Gruppen**, um die Benutzer- und Gruppenzugriffseinstellungen anzuzeigen.

Weitere Informationen finden Sie unter "[Fügen Sie S3-Benutzer und -Gruppen hinzu](#)".

3. Erstellen Sie eine SnapMirror S3-Richtlinie, wenn Sie keine vorhandene Richtlinie haben und die Standardrichtlinie nicht verwenden möchten:
  - a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Lokale Richtlinieneinstellung**.
  - b. Klicken Sie  neben **Schutzrichtlinien** und dann auf **Hinzufügen**.
    - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
    - Wählen Sie den Richtlinienumfang, das Cluster oder die SVM aus
    - Wählen Sie **kontinuierlich** für SnapMirror S3-Beziehungen aus.
    - 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 im Register **Berechtigungen** auf  **Bearbeiten** und dann 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.

["Management des Benutzerzugriffs auf Buckets"](#)Weitere Informationen zu diesen Feldern finden Sie unter.

5. Schützen Sie einen vorhandenen Bucket mit SnapMirror S3:

- 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 Objektsperre für Ziel-Buckets aktivieren, sofern auf den Quell- und Ziel-Clustern ONTAP 9.14.1 oder höher ausgeführt wird und die Objektsperre 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 Objektsperre auf einem Bucket finden Sie unter "[Erstellen eines Buckets](#)".

### CLI

1. Wenn es sich hierbei um die erste SnapMirror S3-Beziehung für diese SVM handelt, überprüfen Sie, ob Root-Benutzerschlüssel für Quell- und Ziel-SVMs vorhanden sind, und regenerieren Sie sie erneut, wenn dies nicht der Fall ist:

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

Vergewissern Sie sich, dass für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist. Wenn dies nicht der Fall ist, 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 SnapMirror S3-Richtlinie, wenn Sie keine vorhandene Richtlinie haben und 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` – Die einzige Richtlinienart für SnapMirror S3 Beziehungen (erforderlich).
- `-rpo` – Gibt die Zeit für Recovery Point Objective 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

```
security certificate install -type server-ca -vserver admin_svm -cert
```

`-name dest_server_certificate`-Zertifikat, das das *Destination* S3-Serverzertifikat auf der Admin-SVM signiert hat: + Wenn Sie ein Zertifikat verwenden, das von einem externen CA-Anbieter signiert wurde, müssen Sie dieses Zertifikat nur auf der Admin-SVM installieren.

Einzelheiten dazu finden Sie auf der `security certificate install man-Page`.

6. 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 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. Vergewissern Sie sich, dass 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 Quell-Bucket in schreibgeschützt konvertiert und der ursprüngliche Ziel-Bucket in Lese-/Schreibzugriff konvertiert, um die SnapMirror S3-Beziehung rückgängig zu machen.


Wenn der deaktivierte Quell-Bucket wieder verfügbar ist, synchronisiert SnapMirror S3 den Inhalt der beiden Buckets automatisch neu. 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 **SnapMirror S3** aus.
2. Klicken Sie auf , wählen Sie **Failover** und klicken Sie dann auf **Failover**.

## CLI

1. Initiieren Sie einen Failover-Vorgang 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-Zielsever-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 Weitere Informationen finden Sie unter "[Storage Service Level](#)".
    - 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 Objektsperre aktiviert ist, kann ein Bucket wiederhergestellt werden, indem ein Bucket erstellt wird, für den auch die Objektsperre aktiviert ist. Wenn Sie einen gesperrten Bucket wiederherstellen, werden der Objektsperremodus 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 Objektsperre auf einem Bucket nicht aktiviert ist, können Sie sie in einem Bucket wiederherstellen, der die Objektsperre 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 Sie einen Wiederherstellungsvorgang 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
```

## Backup-Sicherung mit Cloud-Zielen

### Anforderungen für Cloud-Zielbeziehungen

Stellen Sie sicher, dass Ihre Quell- und Zielumgebungen die Anforderungen für die SnapMirror S3-Backup-Sicherung auf Cloud-Ziele erfüllen.

Um auf den Daten-Bucket zuzugreifen, müssen Sie über gültige Kontoanmeldeinformationen beim Objektspeicher-Provider verfügen.

Intercluster LIFs und ein IPspace sollten auf dem Cluster konfiguriert werden, bevor das Cluster eine Verbindung zu einem Cloud-Objektspeicher herstellen kann. Es sollten Intercluster LIFs auf jedem Node erstellt werden, um Daten nahtlos vom lokalen Storage zum Cloud-Objektspeicher zu übertragen.

Für StorageGRID-Ziele müssen Sie die folgenden Informationen kennen:

- Servername, ausgedrückt als vollständig qualifizierter Domain-Name (FQDN) oder IP-Adresse
- Bucket-Name: Der Bucket muss bereits vorhanden sein
- Zugriffsschlüssel
- Geheimer Schlüssel

Darüber hinaus muss das CA-Zertifikat, das zum Signieren des StorageGRID-Serverzertifikats verwendet wird `security certificate install command`, auf der Admin-Storage-VM des ONTAP S3-Clusters mithilfe der installiert werden. Weitere Informationen finden Sie unter "[Installieren eines CA-Zertifikats](#)", wenn Sie StorageGRID verwenden.

Für AWS S3 Ziele sind die folgenden Informationen erforderlich:

- Servername, ausgedrückt als vollständig qualifizierter Domain-Name (FQDN) oder IP-Adresse
- Bucket-Name: Der Bucket muss bereits vorhanden sein
- Zugriffsschlüssel
- Geheimer Schlüssel

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

### Backup-Beziehung für einen neuen Bucket erstellen (Cloud-Ziel)


Wenn neue S3-Buckets erstellt werden, können diese sofort in einem SnapMirror S3-Ziel-Bucket auf einem Objektspeicher-Provider gesichert werden, das ein StorageGRID-

System oder eine Amazon S3-Implementierung sein kann.

**Bevor Sie beginnen**

- Sie haben gültige Anmeldeinformationen und Konfigurationsinformationen für den Objektspeicher-Provider.
- Intercluster-Netzwerkschnittstellen und ein IPspace wurden auf dem Quellsystem konfiguriert.
- Die DNS-Konfiguration für die Quell-Speicher-VM muss in der Lage sein, den FQDN des Ziels aufzulösen.

## System Manager


1. Bearbeiten Sie die Storage-VM, um Benutzer hinzuzufügen und Gruppen Benutzer hinzuzufügen:
  - a. Klicken Sie auf **Speicher > Speicher-VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und klicken Sie dann  unter **S3**.

Weitere Informationen finden Sie unter "[Fügen Sie S3-Benutzer und -Gruppen hinzu](#)".

2. Cloud Object Store auf dem Quellsystem hinzufügen:
  - a. Klicken Sie auf **Schutz > Übersicht** und wählen Sie dann **Cloud Object Stores**.
  - 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 virtuell gehostet)
- Storage-VM (aktiviert für S3)
- Objektspeicherservername (FQDN)
- Objektspeicherzertifikat
- Zugriffsschlüssel
- Geheimer Schlüssel
- Container-Name (Bucket

3. Erstellen Sie eine SnapMirror S3-Richtlinie, wenn Sie keine vorhandene Richtlinie haben und die Standardrichtlinie nicht verwenden möchten:

- 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.
  - Wählen Sie den Richtlinienumfang, das Cluster oder die SVM aus
  - Wählen Sie **kontinuierlich** für SnapMirror S3-Beziehungen aus.
  - 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.

"[Management des Benutzerzugriffs auf Buckets](#)" Weitere Informationen zu diesen Feldern finden Sie unter.

- d. Aktivieren Sie unter **Schutz SnapMirror aktivieren (ONTAP oder Cloud)** die Option **Cloud-Speicher** und wählen Sie dann den **Cloud-Objektspeicher** aus.

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

## CLI

1. Wenn dies die erste SnapMirror S3-Beziehung für diese SVM ist, überprüfen Sie, ob Root-Benutzerschlüssel für Quell- und Ziel-SVMs vorhanden sind, und regenerieren Sie sie, wenn sie `vserver object-store-server user show` dies nicht tun: + Bestätigen Sie, dass es einen Zugriffsschlüssel für den Root-Benutzer gibt. Wenn nicht, geben Sie ein:

```
vserver object-store-server user regenerate-keys -vserver svm_name -user root + Den Schlüssel nicht neu generieren, wenn er bereits vorhanden ist.
```

2. Bucket in der Quell-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. Fügen Sie Zugriffsregeln zur Standard-Bucket-Richtlinie 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]
```

## Beispiel

```
clusterA::> vserver object-store-server bucket policy add-statement -bucket test-bucket -effect allow -action GetObject,PutObject,DeleteObject,ListBucket,GetBucketAcl,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts -principal - -resource test-bucket, test-bucket /*
```

4. Erstellen Sie eine SnapMirror S3-Richtlinie, wenn Sie keine vorhandene Richtlinie haben und 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: \* `type continuous` – Der einzige Richtlinientyp für SnapMirror S3 Beziehungen (erforderlich). \* `-rpo` – Gibt die Zeit für die Recovery Point Objective 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. Wenn es sich bei dem Ziel um ein StorageGRID-System handelt, installieren Sie das StorageGRID CA-Serverzertifikat auf der Admin-SVM des Quell-Clusters:

```
security certificate install -type server-ca -vserver src_admin_svm -cert
-name storage_grid_server_certificate
```

Einzelheiten dazu finden Sie auf der `security certificate install man`-Page.

6. SnapMirror S3-Zielobjektspeicher 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 –SSL` zu aktivieren ist optional, aber empfohlen. + Siehe die `snapmirror object-store config create man`-Seite für Details.

### 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. Eine SnapMirror S3 Beziehung erstellen:

```
snapmirror create -source-path svm_name:/bucket/bucket_name -destination
-path object_store_name:/objstore -policy policy_name
```

Parameter: \* `-destination-path` - Der Name des Objektspeichers, den Sie im vorherigen Schritt erstellt `objstore` haben, und der feste Wert. + Sie können eine Richtlinie verwenden, die Sie erstellt haben, oder die Standardvorgabe akzeptieren.

### Beispiel

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

8. Vergewissern Sie sich, dass die Spiegelung aktiv ist:

```
snapmirror show -policy-type continuous -fields status
```

## **Backup-Beziehung für einen vorhandenen Bucket erstellen (Cloud-Ziel)**


Sie können jederzeit damit beginnen, vorhandene S3-Buckets zu sichern. Wenn Sie beispielsweise eine S3-Konfiguration aus einer älteren Version als ONTAP 9.10.1 aktualisiert haben,

### **Bevor Sie beginnen**



- Sie haben gültige Anmeldeinformationen und Konfigurationsinformationen für den Objektspeicher-Provider.
- Intercluster-Netzwerkschnittstellen und ein IPspace wurden auf dem Quellsystem konfiguriert.
- Die DNS-Konfiguration für die Quell-Speicher-VM muss in der Lage sein, den FQDN des Ziels aufzulösen.



## 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 klicken Sie dann  unter S3.

Weitere Informationen finden Sie unter "[Fügen Sie S3-Benutzer und -Gruppen hinzu](#)".

2. Erstellen Sie eine SnapMirror S3-Richtlinie, wenn Sie keine vorhandene Richtlinie haben und die Standardrichtlinie nicht verwenden möchten:
  - a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Lokale Richtlinieneinstellungen**.
  - b. Klicken Sie  neben **Schutzrichtlinien** und dann auf **Hinzufügen**.
  - c. Geben Sie den Namen und die Beschreibung der Richtlinie ein.
  - d. Wählen Sie den Richtlinienumfang, das Cluster oder die SVM aus
  - e. Wählen Sie **kontinuierlich** für SnapMirror S3-Beziehungen aus.
  - f. Geben Sie Ihre **Throttle-** und **Recovery Point-Zielwerte** ein.
3. Cloud Object Store auf dem Quellsystem hinzufügen:
  - a. Klicken Sie auf **Schutz > Übersicht** und wählen Sie dann **Cloud Object Store**.
  - b. Klicken Sie auf **Hinzufügen** und wählen Sie **Amazon S3** oder **andere** für StorageGRID Webscale.
  - c. Geben Sie die folgenden Werte ein:
    - Name des Cloud-Objektspeichers
    - URL-Stil (Pfad oder virtuell gehostet)
    - Storage-VM (aktiviert für S3)
    - Objektspeicherservername (FQDN)
    - Objektspeicherzertifikat
    - Zugriffsschlüssel
    - Geheimer Schlüssel
    - Container-Name (Bucket
4. Vergewissern Sie sich, dass die Bucket-Zugriffsrichtlinie des vorhandenen Buckets nach wie vor die Anforderungen erfüllt:
  - a. Klicken Sie auf **Storage > Buckets** und wählen Sie dann den Eimer aus, den Sie schützen möchten.
  - b. Klicken Sie im Register **Berechtigungen** auf  **Bearbeiten** und dann unter **Berechtigungen** auf **Hinzufügen**.
    - **Principal** und **Effect** - Wählen Sie Werte aus, die Ihren Benutzergruppeneinstellungen entsprechen, oder übernehmen Sie die Standardeinstellungen.
    - **Actions** - 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.

"[Management des Benutzerzugriffs auf Buckets](#)" Weitere Informationen zu diesen Feldern finden Sie unter.

#### 5. Backup des Buckets mit SnapMirror S3:

- a. Klicken Sie auf **Storage > Buckets** und wählen Sie dann den Eimer aus, den Sie sichern möchten.
- b. Klicken Sie auf **Protect**, wählen Sie **Cloud Storage** unter **Target** und wählen Sie dann den **Cloud Object Store** aus.

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

#### CLI

##### 1. Überprüfen Sie, 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,GetObjectAcl,
ListBucketMultipartUploads,ListMultipartUploadParts -principal -
-resource test-bucket, test-bucket /*
```

##### 2. Erstellen Sie eine SnapMirror S3-Richtlinie, wenn Sie keine vorhandene Richtlinie haben und 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: \* *type* continuous – Der einzige Richtlinientyp für SnapMirror S3 Beziehungen (erforderlich). \* *-rpo* – Gibt die Zeit für die Recovery Point Objective 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
```

##### 3. Wenn es sich bei dem Ziel um ein StorageGRID-System handelt, installieren Sie das StorageGRID CA-Zertifikat auf der Admin-SVM des Quell-Clusters:

```
security certificate install -type server-ca -vserver src_admin_svm -cert
-name storage_grid_server_certificate
```

Einzelheiten dazu finden Sie auf der `security certificate install` man-Page.

##### 4. SnapMirror S3-Zielobjektspeicher 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 -SSL zu aktivieren ist optional, aber empfohlen. + Siehe die snapmirror object-store config create man-Seite für Details.

### 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. Eine SnapMirror S3 Beziehung erstellen:

```
snapmirror create -source-path svm_name:/bucket/bucket_name -destination
-path object_store_name:/objstore -policy policy_name
```

Parameter: \* -destination-path - Der Name des Objektspeichers, den Sie im vorherigen Schritt erstellt objstore haben, und der feste Wert. + Sie können eine Richtlinie verwenden, die Sie erstellt haben, oder die Standardvorgabe akzeptieren.

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

### 6. Vergewissern Sie sich, dass die Spiegelung aktiv ist:

```
snapmirror show -policy-type continuous -fields status
```

## Wiederherstellung eines Buckets aus einem Cloud-Ziel

Wenn Daten in einem Quell-Bucket verloren gehen oder beschädigt sind, können Sie Ihre Daten neu befüllen, indem Sie sie von 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 verwendete Speicherplatz des Ziels.

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.

## System Manager

Wiederherstellen der Backup-Daten:

1. Klicken Sie auf **Schutz > Beziehungen**, und wählen Sie dann **SnapMirror S3** 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.
    - Kopieren Sie den Inhalt des CA-Zertifikats des *Destination* S3-Servers 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.
    - Der Name, die Kapazität und das Performance-Service-Level des neuen Buckets. Weitere Informationen finden Sie unter "[Storage Service Level](#)".
    - Der Inhalt des CA-Zertifikats des Ziel-S3-Servers.
4. Kopieren Sie unter **Destination** den Inhalt des CA-Zertifikats *source* S3-Server.
5. Klicken Sie auf **Schutz > Beziehungen**, um den Wiederherstellungsfortschritt zu überwachen.

## CLI-Verfahren

1. Erstellen Sie den neuen Ziel-Bucket für die Wiederherstellung. Weitere Informationen finden Sie unter "[Backup-Beziehung für einen Bucket erstellen \(Cloud-Ziel\)](#)".
2. Initiieren Sie einen Wiederherstellungsvorgang für den Ziel-Bucket:

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

### Beispiel

Im folgenden Beispiel wird ein Ziel-Bucket in einem vorhandenen Bucket wiederhergestellt.


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

## Ändern einer Spiegelrichtlinie

Vielleicht möchten Sie eine S3-Spiegelrichtlinie ändern, beispielsweise wenn Sie die RPO- und Drosselwerte anpassen möchten.

## System Manager

Wenn Sie diese Werte anpassen möchten, können Sie eine vorhandene Schutzrichtlinie bearbeiten.

1. Klicken Sie auf **Schutz > Beziehungen** und wählen Sie dann die Schutzrichtlinie für die Beziehung aus, die Sie ändern möchten.
2. Klicken Sie neben dem Richtliniennamen auf  und dann auf **Bearbeiten**.

## CLI

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 Recovery Point Objective in Sekunden an.
- `-throttle` – Gibt die obere Grenze für Durchsatz/Bandbreite in Kilobyte/Sekunden an.

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

## Copyright-Informationen

Copyright © 2025 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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, BEISPIELHAFT 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 IRGEND EINER 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.