# Backup-Schutz mit Cloud-Zielen

ONTAP 9

NetApp
November 05, 2026

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

# Inhalt

Backup-Schutz mit Cloud-Zielen . . . . . 1
Anforderungen für ONTAP SnapMirror S3 Cloud-Zielbeziehungen . . . . . 1
Eine Cloud-Backup-Beziehung für einen neuen ONTAP S3 Bucket erstellen . . . . . 1
Eine Cloud-Backup-Beziehung für einen vorhandenen ONTAP S3 Bucket erstellen . . . . . 5
Wiederherstellung eines ONTAP S3-Buckets aus einem Cloud-Ziel . . . . . 8

# 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,GetOb
jectAcl,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".

**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.