



Spiegelung und Backup-Schutz auf einem Remote-Cluster

ONTAP 9

NetApp
March 22, 2023

Inhaltsverzeichnis

- Spiegelung und Backup-Schutz auf einem Remote-Cluster 1
 - Erstellen einer Spiegelbeziehung für einen neuen Bucket (Remote-Cluster) 1
 - Erstellen einer Spiegelbeziehung für einen vorhandenen Bucket (Remote-Cluster)..... 4
 - Übernahme und Bereitstellung von Daten vom Ziel-Bucket (Remote-Cluster) 7
 - Wiederherstellung eines Buckets aus der Ziel-Storage-VM (Remote-Cluster) 8

Spiegelung und Backup-Schutz auf einem Remote-Cluster

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

Wenn Sie neue S3-Buckets erstellen, können Sie sie unmittelbar in einem S3-SnapMirror-Ziel in einem Remote-Cluster sichern.



Was Sie benötigen


- 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.

Über diese Aufgabe


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

System Manager Verfahren

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

Siehe "[Fügen Sie S3-Benutzer und -Gruppen hinzu](#)" Finden Sie weitere Informationen.

3. Auf dem Quell-Cluster, erstellen Sie eine S3 SnapMirror Politik wenn Sie nicht haben eine bestehende und Sie wollen nicht die Standard-Policy verwenden:
 - a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Lokale Richtlinieneinstellungen**.
 - b. Klicken Sie Auf  Klicken Sie neben **Schutzrichtlinien** auf **Hinzufügen**.
 - Geben Sie den Namen und die Beschreibung der Richtlinie ein.
 - Wählen Sie den Richtlinienumfang, das Cluster oder die SVM aus
 - Wählen Sie * Continuous* für S3 SnapMirror Beziehungen.

- Geben Sie Ihre **Throttle-** und **Recovery Point Objective**-Werte ein.

4. Erstellung eines Buckets mit SnapMirror Sicherung:

- Klicken Sie auf **Storage > Buckets** und dann auf **Hinzufügen**. Die Überprüfung der Berechtigungen ist optional, wird aber empfohlen.
- 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.

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

d. Aktivieren Sie unter **Schutz Enable SnapMirror (ONTAP oder Cloud)**. Geben Sie anschließend die folgenden Werte ein:

- Ziel
 - **ZIEL: ONTAP-System**
 - **CLUSTER**: Wählen Sie den 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.

Überprüfen Sie **Verwenden Sie dasselbe Zertifikat auf dem Ziel**, wenn Sie ein Zertifikat verwenden, das von einem externen CA-Anbieter signiert wurde.

Wenn Sie auf **Zieleinstellungen** klicken, können Sie Ihre eigenen Werte anstelle der Standardeinstellungen für Bucket-Name, -Kapazität und -Service-Level eingeben.

Wenn Sie auf **Speichern** klicken, wird in der Quell-Storage-VM ein neuer Bucket erstellt und in einem neuen Bucket gespiegelt, der die Ziel-Storage-VM erstellt.

CLI-Verfahren

- Wenn dies die erste S3 SnapMirror Beziehung für diese SVM ist, überprüfen Sie, ob die Root-Benutzerschlüssel für Quell- und Ziel-SVMs vorhanden sind, und generieren Sie sie erneut, wenn sie dies nicht tun:

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

Vergewissern Sie sich, dass für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist. Falls nicht, geben Sie Folgendes ein:

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

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

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

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

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

```
vserver object-store-server bucket policy add-statement -vserver svm_name
-bucket bucket_name -effect {allow|deny} -action object_store_actions
-principal user_and_group_names -resource object_store_resources [-sid text]
[-index integer]
```

Beispiel

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

4. Auf der Quell-SVM, erstellen Sie eine S3 SnapMirror- Politik wenn Sie keine bestehende haben und Sie nicht die Default-Richtlinie 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` – Der einzige Richtlinientyp für S3 SnapMirror Beziehungen (erforderlich).
- `-rpo` – Gibt die Zeit für den Wiederherstellungspunkt in Sekunden an (optional).
- `-throttle` – Gibt die obere Grenze für Durchsatz/Bandbreite in Kilobyte/Sekunden an (optional).

Beispiel

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

5. Installieren von CA-Server-Zertifikaten auf den Administrator-SVMs der Quell- und Ziel-Cluster:

a. Installieren Sie auf dem Quellcluster das CA-Zertifikat, das das *Destination* S3-Serverzertifikat unterzeichnet 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.

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

6. Erstellen Sie auf der Quell-SVM eine S3-SnapMirror Beziehung:

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination  
-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy policy_name]
```

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

Beispiel

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

7. Überprüfen Sie, ob die Spiegelung aktiv ist:

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

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.


Was Sie benötigen

- 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.



Über diese Aufgabe

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



System Manager Verfahren

1. Wenn dies die erste S3 SnapMirror Beziehung für diese Storage-VM ist, überprüfen Sie, ob die Root-Benutzerschlüssel für Quell- und Ziel-Storage VMs vorhanden sind, und generieren Sie sie erneut, wenn sie nicht:
 - a. Klicken Sie auf **Storage > Storage VMs** und wählen Sie dann die Speicher-VM aus.
 - b. Klicken Sie auf der Registerkarte **Einstellungen** auf  In der Kachel **S3**.
 - c. Überprüfen Sie auf der Registerkarte **Benutzer**, ob für den Root-Benutzer ein Zugriffsschlüssel

vorhanden ist.

- d. Falls nicht, klicken Sie auf  Klicken Sie neben **root** dann auf **Schlüssel erneut generieren**. Generieren Sie den Schlüssel nicht neu, wenn er bereits existiert.
2. Überprüfen Sie, ob Benutzer- und Gruppenzugriff sowohl auf den Quell- als auch auf den Ziel-Storage-VMs korrekt ist: Klicken Sie auf **Storage > Storage VMs**, klicken Sie auf die Speicher-VM, klicken Sie auf **Einstellungen** und dann auf  Unter **S3**.

Siehe "[Fügen Sie S3-Benutzer und -Gruppen hinzu](#)" Finden Sie weitere Informationen.

3. Auf dem Quell-Cluster, erstellen Sie eine S3 SnapMirror Politik wenn Sie nicht haben eine bestehende und Sie wollen nicht die Standard-Policy verwenden:
 - a. Klicken Sie auf **Schutz > Übersicht** und dann auf **Lokale Richtlinienereinstellungen**.
 - b. Klicken Sie Auf  Klicken Sie neben **Schutzrichtlinien** 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 * Continuous* für S3 SnapMirror Beziehungen.
 - 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 auf der Registerkarte **Berechtigungen** auf  **Bearbeiten**, dann klicken Sie 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 Standardeinstellungen (`bucketname, bucketname/*`) Oder andere Werte, die Sie benötigen.

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

5. Schutz eines vorhandenen Buckets durch S3 SnapMirror 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.

Überprüfen Sie **Verwenden Sie dasselbe Zertifikat auf dem Ziel**, wenn Sie ein Zertifikat verwenden, das von

einem externen CA-Anbieter signiert wurde.

Wenn Sie auf **Zieleinstellungen** klicken, können Sie Ihre eigenen Werte anstelle der Standardeinstellungen für Bucket-Name, -Kapazität und -Service-Level eingeben.

Wenn Sie auf **Speichern** klicken, wird der vorhandene Bucket auf einem neuen Bucket in der Ziel-Storage-VM gespiegelt.

CLI-Verfahren

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

```
vserver object-store-server user show+ Überprüfen Sie, dass für den Root-Benutzer ein Zugriffsschlüssel vorhanden ist. Falls nicht, geben Sie Folgendes ein:
```

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

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

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

3. Vergewissern Sie sich, dass die Zugriffsregeln der Standard-Bucket-Richtlinien sowohl in den Quell- als auch in den Ziel-SVMs korrigiert werden:

```
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,GetObjectAcl,ListBucketMultipartUploads,ListMultipartUploadParts -principal - -resource test-bucket, test-bucket /*
```

4. Auf der Quell-SVM, erstellen Sie eine S3 SnapMirror- Politik wenn Sie keine bestehende haben und Sie nicht die Default-Richtlinie verwenden möchten:

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

Parameter:

- `continuous` – Der einzige Richtlinientyp für S3 SnapMirror Beziehungen (erforderlich).
- `-rpo` – Gibt die Zeit für den Wiederherstellungspunkt in Sekunden an (optional).

- `-throttle` – Gibt die obere Grenze für Durchsatz/Bandbreite in Kilobyte/Sekunden an (optional).

Beispiel

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

5. Installieren von CA-Zertifikaten auf den Administrator-SVMs von Quell- und Ziel-Clustern:

- Installieren Sie auf dem Quellcluster das CA-Zertifikat, das das *Destination* S3-Serverzertifikat unterzeichnet hat:

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

- 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 Zertifikat verwenden, das von einem externen CA-Anbieter signiert wurde, installieren Sie dasselbe Zertifikat auf der Quell- und Ziel-Administrator-SVM.

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

6. Erstellen Sie auf der Quell-SVM eine S3-SnapMirror Beziehung:

```
snapmirror create -source-path src_svm_name:/bucket/bucket_name -destination
-path dest_peer_svm_name:/bucket/bucket_name, ...} [-policy policy_name]
```

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

Beispiel

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

7. Überprüfen Sie, ob die Spiegelung aktiv ist:

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

Übernahme und Bereitstellung von Daten 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 der Quell-Bucket in schreibgeschützt umgewandelt und der ursprüngliche Ziel-Bucket in Lese-/Schreibzugriff umgewandelt, sodass die S3 SnapMirror Beziehung rückgängig gemacht wird.


Wenn der deaktivierte Quell-Bucket wieder verfügbar ist, werden die Inhalte der beiden Buckets von S3

SnapMirror automatisch neu synchronisiert. 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 Verfahren

Failover aus dem nicht verfügbaren Bucket und Beginn der Datenbereitstellung:

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

CLI-Verfahren

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

Beispiel

```
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 werden, füllen Sie die Daten durch die Wiederherstellung aus einem Ziel-Bucket neu aus.

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.

Der Wiederherstellungsvorgang muss vom Remote-Cluster initiiert werden.

System Manager Verfahren

Wiederherstellen der Backup-Daten:

1. Klicken Sie auf **Schutz > Beziehungen** und wählen Sie dann **S3 SnapMirror**.
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. Siehe "[Storage Service Level](#)" Finden Sie weitere Informationen.
 - 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.

CLI-Verfahren

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


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

Beispiel

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

Copyright-Informationen

Copyright © 2023 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.