



Backup-Sicherung mit Cloud-Zielen

ONTAP 9

NetApp
September 12, 2024

Inhalt

- Backup-Sicherung mit Cloud-Zielen 1
 - Anforderungen für Cloud-Zielbeziehungen 1
 - Backup-Beziehung für einen neuen Bucket erstellen (Cloud-Ziel) 1
 - Backup-Beziehung für einen vorhandenen Bucket erstellen (Cloud-Ziel) 6
 - Wiederherstellung eines Buckets aus einem Cloud-Ziel 9

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.

Auf dem Cluster sollten Intercluster-Netzwerkschnittstellen und ein IPspace konfiguriert werden, bevor das Cluster eine Verbindung zu einem Cloud-Objektspeicher herstellen kann. Sie sollten auf jedem Node Cluster-Netzwerkschnittstellen erstellen, um Daten nahtlos vom lokalen Storage in den 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, auf der Admin-Speicher-VM des ONTAP S3-Clusters mit installiert werden `security certificate install` command. 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 (falls verwendet) auf 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**.

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

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.

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

- 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. Erstellung 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. 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 Zertifikat für den StorageGRID CA-Server auf der Admin-SVM des Quell-Clusters:

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

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

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` – Gebrauch `data` Für diesen Workflow. * `-provider-type` – `AWS_S3` Und `SGWS` (StorageGRID) Ziele werden unterstützt. * `-server` – Der FQDN des Zielservers oder die IP-Adresse. * `-is-ssl-enabled` – Die Aktivierung von SSL ist optional, wird jedoch empfohlen. + Siehe `snapmirror object-store config create` Man-Page 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 haben, und der feste Wert `objstore`.

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 sgws-store:/objstore -policy test-policy
```

8. Überprüfen Sie, ob 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.

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

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.
 - **Aktionen** - stellen Sie sicher, dass die folgenden Werte angezeigt werden:
`GetObject, PutObject, DeleteObject, ListBucket, GetBucketAcl, GetObjectAcl, ListBucketMultipartUploads, ListMultipartUploadParts`
 - **Ressourcen** - Verwenden Sie die Standardeinstellungen (`bucketname, bucketname/*`) Oder andere Werte, die Sie benötigen.

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

5. Backup des Buckets mit SnapMirror S3:

- Klicken Sie auf **Storage > Buckets** und wählen Sie dann den Eimer aus, den Sie sichern möchten.
- 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. Vergewissern Sie sich, dass 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
```

Siehe security certificate install Man-Page für Details.

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 – Gebrauch data Für diesen Workflow. * -provider-type – AWS_S3 Und SGWS (StorageGRID) Ziele werden unterstützt. * -server – Der FQDN des Zielservers oder die IP-Adresse. * -is-ssl-enabled –Die Aktivierung von SSL ist optional, wird jedoch empfohlen. + Siehe snapmirror object-store config create Man-Page 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 haben, und der feste Wert objstore.

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

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

6. Überprüfen Sie, ob 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. Siehe ["Storage Service Level"](#) Finden Sie weitere Informationen.
 - 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 eines Restore-Vorgangs 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
```

Copyright-Informationen

Copyright © 2024 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, 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.