ONTAP versionsspezifische Prüfungen vor dem Zurücksetzen durchführen

ONTAP 9

NetApp
November 10, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/revert/concept_pre_revert_checks.html on November 10, 2026. Always check docs.netapp.com for the latest.

Inhalt

ONTAP versionsspezifische Prüfungen vor dem Zurücksetzen durchführen . . . 1
Voraussetzungen vor der Rückkehr zu Ihrer ONTAP Version . . . 1
Jede ONTAP 9 Version . . . 3
Bestimmte SMB-Sitzungen müssen beendet werden, bevor ONTAP zurückgesetzt wird . . . 3
Informationen zum Zurücksetzen von ONTAP SMB-Clustern . . . 4
ONTAP Rücksetzanforderungen für SnapMirror und SnapVault Beziehungen . . . 4
Freier Speicherplatz für deduplizierte Volumes sollte vor dem Zurücksetzen von ONTAP überprüft werden . . . 5
Vor dem Zurücksetzen eines ONTAP Cluster ist es ratsam, Snapshot-Kopien zu erstellen. . . . 7
Autocommit-Zeiträume für SnapLock Volumes vor dem Zurücksetzen von ONTAP festlegen . . . 9
Deaktivierung der automatischen ungeplanten Umschaltung vor einem ONTAP MetroCluster Revert . . . 9
Behebung von ARP-Aktivitätswarnungen vor einem ONTAP Revert . . . 10
ONTAP 9.20.1 . . . 10
Deaktivierung von FC-SP-3 auf FC LIFs vor dem Zurücksetzen von ONTAP 9.20.1 . . . 10
Entfernen von Registrierungen für persistente Reservierungen für eine Rücksetzung auf ONTAP 9.20.1 . . . 11
Vor der Rückkehr von ONTAP 9.20.1 sollten SHA-512-SNMPv3-Benutzer entfernt werden. . . . 12
ONTAP 9.19.1 . . . 13
Aktiv/Aktiv SVMs müssen gelöscht werden, bevor von ONTAP 9.19.1 zurückgekehrt wird. . . . 13
Ändern von QoS-Richtliniengruppen vor der Rückkehr von ONTAP 9.19.1 . . . 13
Entfernen Sie die zweiten S3-Zugriffsschlüssel, bevor Sie von ONTAP 9.19.1 zurückkehren. . . . 14
ONTAP 9.18.1 . . . 14
Automatische ARP-Aktivierung vor dem Zurücksetzen von ONTAP 9.18.1 deaktivieren . . . 14
ONTAP 9.17.1 . . . 15
Deaktivierung von ARP auf SAN-Volumes vor dem Revert von ONTAP 9.17.1 . . . 15
ONTAP 9.16.1 . . . 15
TLS auf NVMe-Hosts vor dem Zurücksetzen von ONTAP 9.16.1 deaktivieren . . . 15
Deaktivieren der erweiterten qtree-Performanceüberwachung vor einem ONTAP Revert . . . 16
CORS-Konfiguration vor dem Zurücksetzen von ONTAP 9.16.1 entfernen . . . 16
ONTAP 9.14.1 . . . 16
NFSv4.1 Session Trunking vor dem Zurücksetzen von ONTAP 9.14.1 deaktivieren . . . 16
ONTAP 9.12.1 . . . 17
Die S3 NAS-Bucket-Konfiguration sollte entfernt werden, bevor von ONTAP 9.12.1 zurückgekehrt wird. . . . 17
NVMe In-Band-Authentifizierung vor der Rückkehr von ONTAP 9.12.1 deaktivieren . . . 18
Deaktivierung von IPsec in MetroCluster vor der Rückkehr von ONTAP 9.12.1 . . . 18
ONTAP 9.11.1 . . . 19
Prüfung der ARP-Lizenzierung vor dem Revert von ONTAP 9.11.1 . . . 19
ONTAP 9.6 . . . 19
Vorbereitung synchroner SnapMirror Beziehungen für einen ONTAP 9.6 Revert . . . 19

ONTAP versionsspezifische Prüfungen vor dem Zurücksetzen durchführen

Voraussetzungen vor der Rückkehr zu Ihrer ONTAP Version

Je nach Ihrer ONTAP Version sind möglicherweise zusätzliche vorbereitende Aufgaben erforderlich, bevor der Wiederherstellungsprozess gestartet werden kann.

Wenn Sie von … zurückkehren	Vor Beginn des Wiederherstellungsprozesses ist Folgendes zu beachten…
Jede ONTAP 9 Version	• "SMB-Sitzungen beenden, die nicht durchgehend verfügbar sind". • "Überprüfung der Rückführungsanforderungen für SnapMirror und SnapVault Beziehungen". • "Es sollte sichergestellt werden, dass die deduplizierten Volumes über ausreichend freien Speicherplatz verfügen.". • "Snapshots vorbereiten". • "Legen Sie den Autocommit-Zeitraum für SnapLock Volumes auf Stunden fest". • Wenn Sie eine MetroCluster Konfiguration haben, "Automatische ungeplante Umschaltung deaktivieren". • "Auf Warnungen des autonomen Ransomware-Schutzes bezüglich ungewöhnlicher Aktivität reagieren".
ONTAP 9.20.1	• Wenn für eine LUN in der Vergangenheit mehr als 182 Registrierungen für persistente SCSI-3-Reservierungen vorlagen, "Alle Registrierungen für persistente Reservierungen auf den betroffenen LUNs entfernen". • Wenn Sie über SNMPv3-Benutzer verfügen, die die SHA-512-Authentifizierung verwenden, "löschen und mit einem unterstützten Authentifizierungsprotokoll neu erstellen".

Wenn Sie von … zurückkehren	Vor Beginn des Wiederherstellungsprozesses ist Folgendes zu beachten…
ONTAP 9.19.1	• Wenn Sie SVMs mit Aktiv/Aktiv Multipathing-Konfigurationen haben, ist Folgendes zu beachten "Die SVMs löschen". • Wenn Sie die Standardeinstellungen einer in ONTAP 9.19.1 oder höher erstellten QoS-Richtliniengruppe geändert haben, "zurücksetzen". • Wenn Sie die Volumes auf ONTAP 9.19.1 aktualisiert und einem Benutzer einen zweiten S3-Zugriffsschlüssel hinzugefügt haben, muss "Diese Schlüssel entfernen".
ONTAP 9.18.1	• Wenn die automatische Aktivierung für ARP/AI im Rahmen eines ONTAP 9.18.1 Upgrades eingestellt wurde, ist es erforderlich, "deaktivieren".
ONTAP 9.17.1	• Wenn Sie die ONTAP ARP/AI Funktion für SAN aktiviert haben, "deaktivieren".
ONTAP 9.16.1	• Wenn Sie TLS für NVMe/TCP-Verbindungen konfiguriert haben, "Die TLS-Konfiguration auf den NVMe-Hosts deaktivieren". • Wenn Sie die erweiterte Qtree-Leistungsüberwachung aktiviert haben, "deaktivieren". • Wenn Sie CORS verwenden, um auf Ihre ONTAP s3 Buckets zuzugreifen, "Die CORS-Konfiguration entfernen".
ONTAP 9.14.1	Wenn Sie Trunking für Clientverbindungen aktiviert haben, "Trunking auf allen NFSv4.1 Servern deaktivieren".
ONTAP 9.12.1	• Wenn Sie den S3-Clientzugriff für NAS-Daten konfiguriert haben, "Die S3 NAS-Bucket-Konfiguration wird entfernt." • Wenn Sie das NVMe-Protokoll verwenden und die In-Band Authentifizierung konfiguriert haben, "In-Band Authentifizierung deaktivieren". • Wenn Sie eine MetroCluster Konfiguration haben, "IPsec deaktivieren".
ONTAP 9.11.1	Wenn Sie den autonomen Ransomware-Schutz (ARP) konfiguriert haben, "Die ARP-Lizenzierung prüfen.".
ONTAP 9.6	Wenn Sie SnapMirror synchron Beziehungen haben, "Die Beziehungen für das Zurücksetzen vorbereiten".

Jede ONTAP 9 Version

Bestimmte SMB-Sitzungen müssen beendet werden, bevor ONTAP zurückgesetzt wird

Bevor ein ONTAP Cluster von einer beliebigen Version von ONTAP 9 zurückgesetzt wird, sollten alle SMB-Sitzungen identifiziert und ordnungsgemäß beendet werden, die nicht kontinuierlich verfügbar sind.

Kontinuierlich verfügbare SMB-Freigaben, auf die Hyper-V- oder Microsoft SQL Server Clients über das SMB 3.0-Protokoll zugreifen, müssen vor einem Upgrade oder Downgrade nicht beendet werden.

Schritte

1. Alle bestehenden SMB-Sitzungen, die nicht kontinuierlich verfügbar sind, identifizieren:

```
vserver cifs session show -continuously-available No -instance
```

   Dieser Befehl zeigt detaillierte Informationen zu allen SMB-Sitzungen an, die keine kontinuierliche Verfügbarkeit aufweisen. Diese sollten vor dem Fortfahren mit dem ONTAP Downgrade beendet werden.

```
cluster1::> vserver cifs session show -continuously-available No
-instance

                        Node: node1
                     Vserver: vs1
                  Session ID: 1
                Connection ID: 4160072788
Incoming Data LIF IP Address: 198.51.100.5
      Workstation IP address: 203.0.113.20
    Authentication Mechanism: NTLMv2
                Windows User: CIFSLAB\user1
                   UNIX User: nobody
                 Open Shares: 1
                  Open Files: 2
                  Open Other: 0
              Connected Time: 8m 39s
                   Idle Time: 7m 45s
           Protocol Version: SMB2_1
      Continuously Available: No
1 entry was displayed.
```

2. Ermitteln Sie gegebenenfalls die Dateien, die für jede identifizierte SMB-Sitzung geöffnet sind:

```
vserver cifs session file show -session-id session_ID
```

```
cluster1::> vserver cifs session file show -session-id 1

Node:       node1
Vserver:    vs1
Connection: 4160072788
Session:    1
File    File      Open Hosting
Continuously
ID      Type      Mode Volume          Share                 Available
------- --------- ---- --------------- ---------------------
------------
1       Regular   rw   vol10           homedirshare          No
Path: \TestDocument.docx
2       Regular   rw   vol10           homedirshare          No
Path: \file1.txt
2 entries were displayed.
```

Informationen zum Zurücksetzen von ONTAP SMB-Clustern

Wenn Sie planen, den Cluster auf eine ONTAP Version zurückzusetzen, die keine lokalen Benutzer und Gruppen unterstützt und lokale Benutzer und Gruppen zur Verwaltung von Dateizugriff oder Benutzerrechten verwendet werden, sind bestimmte Aspekte zu beachten.

- Aus Sicherheitsgründen werden Informationen über konfigurierte lokale Benutzer, Gruppen und Berechtigungen nicht gelöscht, wenn ONTAP auf eine Version zurückgesetzt wird, die die Funktionalität lokaler Benutzer und Gruppen nicht unterstützt.
- Bei der Rückkehr zu einer früheren Hauptversion von ONTAP verwendet ONTAP während der Authentifizierung und der Erstellung von Anmeldeinformationen keine lokalen Benutzer und Gruppen.
- Lokale Benutzer und Gruppen werden nicht aus den Datei- und Ordner-ACLs entfernt.
- Dateizugriffsanfragen, die davon abhängen, dass der Zugriff aufgrund von Berechtigungen lokaler Benutzer oder Gruppen gewährt wird, werden abgelehnt.

  Um den Zugriff zu ermöglichen, müssen die Dateiberechtigungen so umkonfiguriert werden, dass der Zugriff auf Domänenobjekten anstatt auf lokalen Benutzer- und Gruppenobjekten basiert.

ONTAP Rücksetzanforderungen für SnapMirror und SnapVault Beziehungen

Der `system node revert-to` Befehl benachrichtigt Sie über alle SnapMirror und SnapVault Beziehungen, die für den Abschluss des Wiederherstellungsprozesses gelöscht oder neu konfiguriert werden müssen. Allerdings sollten diese Anforderungen vor Beginn der Wiederherstellung bekannt sein.

- Alle SnapVault- und Datenschutz-Spiegelbeziehungen müssen stillgelegt und anschließend getrennt werden.

Nach Abschluss der Rücksetzung können Sie diese Beziehungen erneut synchronisieren und fortsetzen, sofern ein gemeinsamer Snapshot vorhanden ist.

- SnapVault-Beziehungen dürfen die folgenden SnapMirror-Richtlinientypen nicht enthalten:
  - async-mirror

    Alle Beziehungen, die diesen Richtlinientyp verwenden, müssen gelöscht werden.

  - MirrorAndVault

    Falls eine dieser Beziehungen besteht, sollte die SnapMirror Richtlinie auf mirror-vault geändert werden.
- Alle Load Sharing Mirror-Beziehungen und Ziel-Volumes müssen gelöscht werden.
- SnapMirror-Beziehungen mit FlexClone-Zielvolumes müssen gelöscht werden.
- Die Netzwerkkomprimierung muss für jede SnapMirror Richtlinie deaktiviert werden.
- Die Regel all_source_snapshot muss aus allen async-mirror Typ SnapMirror Richtlinien entfernt werden.

  Die Einzeldatei SnapRestore (SFSR) und Partial File Snapshot Restore (PFSR) Operationen sind auf dem Root-Volume veraltet.

- Alle aktuell laufenden Wiederherstellungsvorgänge für einzelne Dateien und Snapshots müssen abgeschlossen sein, bevor die Rücksetzung fortgesetzt werden kann.

  Sie können entweder warten, bis der Wiederherstellungsvorgang abgeschlossen ist, oder ihn abbrechen.

- Alle unvollständigen Wiederherstellungsvorgänge einzelner Dateien und Snapshots müssen mit dem `snapmirror restore` Befehl entfernt werden.

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

Freier Speicherplatz für deduplizierte Volumes sollte vor dem Zurücksetzen von ONTAP überprüft werden

Bevor ein ONTAP Cluster von einer beliebigen Version von ONTAP 9 zurückgesetzt wird, muss sichergestellt sein, dass die Volumes über ausreichend freien Speicherplatz für den Rücksetzungsvorgang verfügen.

Das Volumen muss ausreichend Platz bieten, um die durch die Inline-Erkennung von Nullblöcken erzielten Einsparungen aufzunehmen. Siehe "NetApp Knowledge Base: Wie sich Speicherplatzeinsparungen durch Deduplizierung, Komprimierung und Kompaktierung in ONTAP 9 anzeigen lassen".

Wenn sowohl Deduplizierung als auch Datenkomprimierung auf einem Volume aktiviert wurden, dessen Zustand zurückgesetzt werden soll, muss die Datenkomprimierung vor der Deduplizierung zurückgesetzt werden.

Schritte

1. Den Fortschritt der Effizienzmaßnahmen, die auf den Volumes ausgeführt werden, anzeigen:

```
volume efficiency show -fields vserver,volume,progress
```

2. Alle aktiven und in der Warteschlange befindlichen Deduplizierungsvorgänge anhalten:

```
volume efficiency stop -vserver <svm_name> -volume <volume_name> -all
```

3. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

4. Die Effizienzmetadaten eines Volumes auf die Zielversion von ONTAP herabstufen:

```
volume efficiency revert-to -vserver <svm_name> -volume <volume_name>
-version <version>
```

Das folgende Beispiel setzt die Effizienz-Metadaten auf dem Volume VolA auf ONTAP 9.x zurück.

```
volume efficiency revert-to -vserver vs1 -volume VolA -version 9.x
```

> ⓘ Der Befehl „volume efficiency revert-to“ setzt die Volumes zurück, die sich auf dem Knoten befinden, auf dem dieser Befehl ausgeführt wird. Mit diesem Befehl werden keine Volumes über Knoten hinweg zurückgesetzt.

5. Der Fortschritt der Herabstufung kann überwacht werden:

```
volume efficiency show -vserver <svm_name> -op-status Downgrading
```

6. Falls die Rücksetzung fehlschlägt, kann die Instanz angezeigt werden, um den Grund für das Scheitern der Rücksetzung zu ermitteln.

```
volume efficiency show -vserver <svm_name> -volume <volume_name> -
instance
```

7. Nach Abschluss des Rückgängigmachungsvorgangs wird zur Administratorberechtigungsstufe zurückgekehrt:

```
set -privilege admin
```

Weitere Informationen zu "Logische Speicherverwaltung".

Vor dem Zurücksetzen eines ONTAP Cluster ist es ratsam, Snapshot-Kopien zu erstellen.

Bevor ein ONTAP Cluster von einer beliebigen Version von ONTAP 9 zurückgesetzt wird, müssen alle Snapshot-Richtlinien deaktiviert und alle Snapshots gelöscht werden, die nach dem Upgrade auf die aktuelle Version erstellt wurden.

Wenn Sie in einer SnapMirror-Umgebung einen Reset durchführen, müssen zuvor die folgenden Spiegelbeziehungen gelöscht worden sein:

- Alle lastverteilenden Spiegelbeziehungen

  Weitere Informationen zum Löschen von Lastverteilungsbeziehungen sind unter "Entfernen einer Load-Sharing Mirror-Beziehung" zu finden.

Schritte

1. Snapshot-Richtlinien für alle Daten-SVMs deaktivieren:

```
volume snapshot policy modify -vserver * -enabled false
```

2. Snapshot-Richtlinien für die Aggregate jedes Knotens deaktivieren:
   a. Die Aggregate des Knotens identifizieren:

```
run -node <nodename> -command aggr status
```

   b. Die Snapshot-Richtlinie für jedes Aggregat wird deaktiviert:

```
run -node <nodename> -command aggr options aggr_name nosnap on
```

   c. Wiederholen Sie diesen Schritt für jeden verbleibenden Node.
3. Snapshot-Richtlinien für das Root-Volume jedes Knotens deaktivieren:
   a. Das Root-Volume des Node identifizieren:

```
run -node <node_name> -command vol status
```

   Das Root-Volume wird durch das Wort „root“ in der Spalte **Optionen** der `vol status` Befehlsausgabe identifiziert.

```
vs1::> run -node node1 vol status

         Volume State           Status            Options
           vol0 online          raid_dp, flex     root, nvfail=on
```

```
                                    64-bit
```

a. Die Snapshot-Richtlinie auf dem Root-Volume wird deaktiviert:

```
run -node <node_name> vol options root_volume_name nosnap on
```

b. Wiederholen Sie diesen Schritt für jeden verbleibenden Node.

4. Alle Snapshots, die nach dem Upgrade auf die aktuelle Version erstellt wurden, löschen:

a. Stellen Sie die Berechtigungsstufe auf „Erweitert“ ein:

```
set -privilege advanced
```

b. Snapshots deaktivieren:

```
snapshot policy modify -vserver * -enabled false
```

c. Die neueren Snapshots des Knotens löschen:

```
volume snapshot prepare-for-revert -node <node_name>
```

Dieser Befehl löscht die neueren Snapshots auf jedem Datenvolume, Root-Aggregat und Root-Volume.

Falls Snapshots nicht gelöscht werden können, schlägt der Befehl fehl und Sie werden über die erforderlichen Aktionen informiert, die Sie vor dem Löschen der Snapshots durchführen müssen. Die erforderlichen Aktionen müssen abgeschlossen und anschließend der `volume snapshot prepare-for-revert` Befehl erneut ausgeführt werden, bevor mit dem nächsten Schritt fortgefahren wird.

```
cluster1::*> volume snapshot prepare-for-revert -node node1

Warning: This command will delete all snapshots that have the format
used by the current version of ONTAP. It will fail if any snapshot
policies are enabled, or
         if any snapshots have an owner. Continue? {y|n}: y
```

a. Es sollte überprüft werden, ob die Snapshots gelöscht wurden:

```
volume snapshot show -node nodename
```

b. Falls noch neuere Snapshots vorhanden sind, diese zwangsweise löschen:

```
volume snapshot delete {-fs-version 9.0 -node nodename -is
```

```
-constituent true} -ignore-owners -force
```

c. Diese Schritte sind für jeden verbleibenden Knoten zu wiederholen.

d. Zurück zur Administrator-Privilegstufe:

```
set -privilege admin
```

Diese Schritte sind auf beiden Clustern in der MetroCluster Konfiguration durchzuführen.

Autocommit-Zeiträume für SnapLock Volumes vor dem Zurücksetzen von ONTAP festlegen

Bevor ein ONTAP Cluster von einer beliebigen Version von ONTAP 9 zurückgesetzt wird, muss der Wert des Autocommit-Zeitraums für SnapLock Volumes in Stunden und nicht in Tagen festgelegt sein. Es empfiehlt sich, den Autocommit-Wert für die SnapLock Volumes zu überprüfen und ihn gegebenenfalls von Tagen auf Stunden zu ändern.

Schritte

1. Es wird überprüft, ob im Cluster SnapLock Volumes vorhanden sind, die nicht unterstützte Autocommit-Zeiträume haben:

```
volume snaplock show -autocommit-period *days
```

2. Nicht unterstützte Autocommit-Zeiträume auf Stunden ändern

```
volume snaplock modify -vserver <vserver_name> -volume <volume_name>
-autocommit-period value hours
```

Deaktivierung der automatischen ungeplanten Umschaltung vor einem ONTAP MetroCluster Revert

Vor dem Zurücksetzen einer MetroCluster Konfiguration, auf der eine beliebige Version von ONTAP 9 ausgeführt wird, muss die automatische ungeplante Umschaltung (AUSO) deaktiviert werden.

Schritt

1. In beiden Clustern in MetroCluster die automatische ungeplante Umschaltung deaktivieren:

```
metrocluster modify -auto-switchover-failure-domain auso-disabled
```

Verwandte Informationen

"MetroCluster Management und Katastrophenwiederherstellung"

Behebung von ARP-Aktivitätswarnungen vor einem ONTAP Revert

Bevor Sie auf ONTAP 9.17.1 oder eine frühere Version zurückkehren, sollten Sie auf alle von Autonomous Ransomware Protection gemeldeten Warnungen vor ungewöhnlichen Aktivitäten reagieren und alle zugehörigen Autonomous Ransomware Protection Snapshots löschen.

Bevor Sie beginnen

Zum Löschen von Snapshots der Autonomous Ransomware Protection sind „Advanced“-Berechtigungen erforderlich.

Schritte

1. Auf alle von "Autonomous Ransomware Protection" gemeldeten Warnungen zu ungewöhnlichen Aktivitäten reagieren und mögliche Probleme beheben.
2. Bestätigen Sie die Behebung dieser Probleme, bevor Sie die vorherigen Schritte rückgängig machen, indem Sie **Aktualisieren und verdächtige Dateitypen löschen** auswählen, um Ihre Entscheidung zu speichern und die normale Überwachung von Autonomous Ransomware Protection fortzusetzen.
3. Alle mit den Warnungen verknüpften Autonomous Ransomware Protection Snapshots werden durch Ausführen des folgenden Befehls aufgelistet:

   ```
   volume snapshot snapshot show -fs-version 9.18
   ```

4. Alle mit den Warnungen verknüpften Autonomous Ransomware Protection Snapshots löschen:

   ⓘ Dieser Befehl löscht alle Snapshots, die das von der aktuellen Version von ONTAP verwendete Format haben, möglicherweise nicht nur Snapshots von Autonomous Ransomware Protection. Es sollte sichergestellt werden, dass alle erforderlichen Maßnahmen für alle zu entfernenden Snapshots getroffen wurden, bevor dieser Befehl ausgeführt wird.

   ```
   volume snapshot prepare-for-revert -node <node_name>
   ```

ONTAP 9.20.1

Deaktivierung von FC-SP-3 auf FC LIFs vor dem Zurücksetzen von ONTAP 9.20.1

Ab ONTAP 9.20.1 unterstützt ONTAP die Authentifizierung und Verschlüsselung mit Fibre Channel Security Protocol 3 (FC-SP-3) unter Verwendung sicherer Broadcom Host-Bus-Adapter (HBAs) mit AFF und FAS Systemen. Wenn FC- oder NVMe/FC-Netzwerkschnittstellen (LIFs) auf Ihrem ONTAP System für FC-SP-3 aktiviert sind, müssen Sie FC-SP-3 deaktivieren, bevor Sie zu ONTAP 9.19.1 zurückkehren.

Schritte

1. Überprüfung der FC-SP-3 Konfiguration auf Ihren LIFs:

```
network interface show -fields fc-transport-security
```

2. Wenn der Status des Feldes **transport-security-state** nicht verfügbar ist, sind keine weiteren Maßnahmen erforderlich. Wenn der Status **mandatory** oder **preferred** ist, ist er in **disabled** zu ändern:

```
network interface modify -vserver <vserver_name> -lif <lif_name> -fc
-transport-security disabled
```

3. Prüfung, ob FC-SP-3 auf den zuvor aktivierten LIFs deaktiviert ist:

```
network interface show -fields fc-transport-security
```

Entfernen von Registrierungen für persistente Reservierungen für eine Rücksetzung auf ONTAP 9.20.1

ONTAP Versionen vor 9.20.1 unterstützen maximal 182 Registrierungen persistenter Reservierungen pro LUN. Ab ONTAP 9.20.1 erhöht sich dieses Limit auf 256. Wenn eine LUN in der Vergangenheit mehr als 182 Registrierungen aufgewiesen hat, blockiert ONTAP die Revertierung unabhängig von der aktuellen Anzahl der Registrierungen. Vor einer Revertierung von 9.20.1 auf 9.19.1 ist die Identifizierung und Entfernung der Registrierungen persistenter Reservierungen auf den betroffenen LUNs erforderlich.

ⓘ Das Entfernen von Registrierungen für persistente Reservierungen kann in Clusterumgebungen eine Neukonfiguration auf Host-Seite erfordern. Je nach Host-Betriebssystem und Clustering-Software kann es erforderlich sein, Clusterressourcen offline zu nehmen, betroffene LUNs aus der Clusterverwaltung zu entfernen und den Clusterzugriff nach dem Revert erneut herzustellen. Die Dokumentation der Clustering-Lösung sollte überprüft und der Recovery-Workflow vor einem Revert in einer Testumgebung validiert werden.

Schritte

1. Es ist zu prüfen, ob LUNs in der Vergangenheit mehr als 182 Registrierungen für persistente Reservierungen aufwiesen:

```
lun show -field persistent-reservation-scale-tier
```

Ein Wert über 182 im Feld „persistent-reservation-scale-tier“ bedeutet, dass die LUN zusätzliche persistente Reservierungsmetadaten zugewiesen hat. Dies blockiert eine Reversion, unabhängig von der aktuellen Anzahl der Registrierungen.

2. Für jede betroffene LUN folgt die Anzeige der aktuellen Anzahl aktiver Registrierungen:

```
lun persistent-reservation show -vserver <vserver_name> -path <lun_path>
```

3. Die Registrierungen für persistente Reservierungen sind auf allen betroffenen LUNs zu entfernen.

   Die Vorabprüfung für das Revert ausführen. Wenn diese Bedingung erkannt wird, enthält die Ausgabe der Vorabprüfung die erforderlichen spezifischen Bereinigungsbefehle.

Vor der Rückkehr von ONTAP 9.20.1 sollten SHA-512-SNMPv3-Benutzer entfernt werden.

Ab ONTAP 9.20.1 können SNMPv3-Benutzer erstellt werden, die die SHA-512 Authentifizierung verwenden. ONTAP Versionen vor 9.20.1 unterstützen die SHA-512 Authentifizierung nicht, daher blockiert ONTAP das Zurücksetzen, wenn SNMPv3-Benutzer mit SHA-512 Authentifizierung vorhanden sind. Vor dem Zurücksetzen müssen diese Benutzer gelöscht und mit einem unterstützten Authentifizierungsprotokoll neu erstellt werden.

Schritte

1. SNMPv3-Benutzer, die die SHA-512-Authentifizierung verwenden:

   ```
   security snmpusers -authmethod usm -authprotocol sha512
   ```

2. Löschen der einzelnen SHA-512-Benutzer:

   ```
   security login delete -vserver <vserver_name> -user-or-group-name
   <user_name> -application snmp -authentication-method usm
   ```

3. Falls Sie die Benutzer weiterhin benötigen, ist eine Neuerstellung mit einem unterstützten Authentifizierungsprotokoll wie `sha` oder `sha2-256` erforderlich:

   ```
   security login create -vserver <vserver_name> -user-or-group-name
   <user_name> -application snmp -authentication-method usm
   ```

   Wenn der Benutzer einen Switch überwacht, ist der `-remote-switch-ipaddress`Parameter mit der IP-Adresse des Switches anzugeben:

   ```
   security login create -user-or-group-name <user_name> -application snmp
   -authentication-method usm -remote-switch-ipaddress <switch_ip_address>
   ```

   Weitere Informationen zu "Konfigurieren von SNMPv3-Benutzern".

4. Falls Ethernet-Switches die gelöschten SHA-512-Benutzer für die Überwachung verwendet haben, muss jeder Switch so aktualisiert werden, dass er den neu erstellten Benutzer verwendet:

   ```
   system switch ethernet modify -device <switch_name> -snmp-version SNMPv3
   ```

```
-community-or-username <snmp_user_name>
```

Weitere Informationen zu `system switch ethernet modify` finden sich in der "ONTAP-Befehlsreferenz".

Weitere Informationen zu SNMPv3 für den Ethernet Switch Systemstatus Monitor (CSHM), einschließlich Informationen zur Konfiguration der Ethernet Switches, enthält "SNMPv3 für die Zustandsüberwachung von Ethernet-Switches konfigurieren".

ONTAP 9.19.1

Aktiv/Aktiv SVMs müssen gelöscht werden, bevor von ONTAP 9.19.1 zurückgekehrt wird.

SAN Aktiv/Aktiv Multipathing wird in ONTAP 9.18.1 und früher nicht unterstützt. Vor dem Zurücksetzen von ONTAP 9.19.1 müssen alle Storage Virtual Machines (SVMs) mit Aktiv/Aktiv Konfigurationen gelöscht werden.

Schritte

1. Alle SVMs identifizieren, bei denen die Option san-multipathing für Aktiv/Aktiv oder Aktiv/Aktiv-nur-SCSI konfiguriert ist:

```
vserver show
```

2. Alle SVMs, die für Aktiv/Aktiv oder Aktiv/Aktiv-SCSI-Only-Multipathing konfiguriert sind, löschen:

```
vserver delete -vserver <SVM>
```

3. Es wird überprüft, ob die SVMs gelöscht wurden:

```
vserver show
```

Verwandte Informationen

Weitere Informationen zu "SAN Aktiv/Aktiv Multipathing-Unterstützung" in ONTAP 9.19.1 und späteren Versionen.

Ändern von QoS-Richtliniengruppen vor der Rückkehr von ONTAP 9.19.1

Adaptive und nicht-adaptive QoS-Richtliniengruppen werden standardmäßig automatisch aktiviert, um den Durchsatz einer Arbeitslast für eine Dauer von 1 Sekunde um 50 % zu erhöhen, um kurzfristigen Anforderungen nach höherer Leistung zu entsprechen. Ab ONTAP 9.19.1 können Sie diese Standardeinstellungen ändern. In ONTAP 9.18.1 und früher können diese Einstellungen nicht geändert werden. Wenn Sie die Standardeinstellungen einer in ONTAP 9.19.1 oder später erstellten QoS-Policy-Gruppe

geändert haben, müssen Sie diese zurücksetzen, bevor Sie von ONTAP 9.19.1 auf ONTAP 9.18.1 zurückkehren können.

Schritte

1. Prüfen Sie, ob QoS-Richtliniengruppen für die automatische Erhöhung des Durchsatzlimits aktiviert sind:

```
qos policy-group show – instance
```

2. Wenn Richtliniengruppen mit `burst-percent`, `burst-iops` und `burst-duration` konfiguriert sind, setzen Sie diese Optionen auf 0.

```
qos policy-group modify -policy-group <policy-group> -burst-percent 0
-burst-iops 0 -burst-duration 0
```

Entfernen Sie die zweiten S3-Zugriffsschlüssel, bevor Sie von ONTAP 9.19.1 zurückkehren.

Wenn Sie auf ONTAP 9.19.1 aktualisiert und einem Benutzer einen zweiten S3-Zugriffsschlüssel hinzugefügt haben, müssen diese Schlüssel entfernt werden, bevor Sie zu einer früheren ONTAP-Version zurückkehren können.

Schritte

1. "S3-Zugriffsschlüssel anzeigen" um festzustellen, ob für S3-Benutzer zweite Zugriffsschlüssel hinzugefügt wurden.
2. "Entfernen Sie die zweiten Zugriffsschlüssel" für alle S3-Nutzer.

ONTAP 9.18.1

Automatische ARP-Aktivierung vor dem Zurücksetzen von ONTAP 9.18.1 deaktivieren

Wenn Volumes auf ONTAP 9.18.1 oder höher aktualisiert wurden, könnte die automatische Aktivierung von ONTAP ARP/AI nach einer kurzen Karenzzeit (12 Stunden) für Ihre Volumes eingerichtet worden sein. Es wird empfohlen, diese automatische Aktivierungseinstellung auf Volumes, die auf ONTAP 9.18.1 oder höher aktualisiert wurden, zu deaktivieren, bevor auf ONTAP 9.17.1 oder eine frühere Version zurückgekehrt wird.

Schritte

1. Ermitteln Sie, ob die automatische Aktivierungsoption auf Volumes aktiviert wurde, die auf ONTAP 9.18.1 oder höher aktualisiert wurden:

```
security anti-ransomware auto-enable show
```

2. Deaktivieren Sie die automatische Aktivierungsoption für den Ransomware-Schutz auf allen Volumes auf der SVM:

```
security anti-ransomware volume disable -volume * -auto-enabled-volumes
-only true
```

ONTAP 9.17.1

Deaktivierung von ARP auf SAN-Volumes vor dem Revert von ONTAP 9.17.1

Die ONTAP ARP/AI-Funktion für SAN-Volumes wird in ONTAP 9.16.1 und früher nicht unterstützt. Es wird empfohlen, ARP/AI auf SAN-Volumes zu deaktivieren, bevor auf ONTAP 9.16.1 oder eine frühere Version zurückgesetzt wird, um zu verhindern, dass die Funktion aktiv bleibt und CPU- sowie Festplattenressourcen nutzt, ohne in der zurückgesetzten Version eine tatsächliche Erkennung durchzuführen.

Beispiel 1. Schritte

System Manager

1. **Speicher > Volumes** auswählen und dann den Namen des Volumes auswählen.
2. Im Tab **Sicherheit** der **Volumes**-Übersicht **Status** auswählen, um von Aktiviert auf Deaktiviert zu wechseln.

CLI

1. Ransomware-Schutz auf einem Volume deaktivieren:

```
security anti-ransomware volume disable -volume <vol_name> -vserver
<svm_name>
```

ONTAP 9.16.1

TLS auf NVMe-Hosts vor dem Zurücksetzen von ONTAP 9.16.1 deaktivieren

Wenn auf einem NVMe-Host ein sicherer TLS-Kanal für NVMe/TCP-Verbindungen konfiguriert ist, muss dieser deaktiviert werden, bevor der Cluster von ONTAP 9.16.1 zurückgesetzt wird.

Schritte

1. Die TLS-Sicherheitskanalkonfiguration wird vom Host entfernt:

```
vserver nvme subsystem host unconfigure-tls-for-revert -vserver
<svm_name> -subsystem <subsystem> -host-nqn <host_nqn>
```

Dieser Befehl entfernt den Host aus dem Subsystem und erstellt den Host anschließend ohne die TLS-Konfiguration im Subsystem neu.

2. Es sollte überprüft werden, ob der sichere TLS-Kanal vom Host entfernt wurde:

```
vserver nvme subsystem host show
```

Deaktivieren der erweiterten qtree-Performanceüberwachung vor einem ONTAP Revert

Ab ONTAP 9.16.1 kann über die ONTAP REST API auf die erweiterten Qtree-Überwachungsfunktionen zugegriffen werden, die Latenzmetriken und historische Statistiken umfassen. Wenn die erweiterte Qtree-Überwachung auf einem Qtree aktiviert ist, muss `ext_performance_monitoring.enabled` vor dem Zurücksetzen von Version 9.16.1 auf false gesetzt werden.

Sie arbeiten mit der `ext_performance_monitoring.enabled` Einstellung, indem Sie den `/api/storage/qtrees` Endpoint verwenden. Verwenden Sie GET, um den aktuellen Wert abzurufen, POST, um ihn beim Erstellen eines neuen qtree festzulegen, und PATCH, um ihn bei einem bestehenden qtree zu ändern.

Weitere Informationen zu "Wiederherstellung von Clustern mit erweiterter Qtree-Leistungsüberwachung".

CORS-Konfiguration vor dem Zurücksetzen von ONTAP 9.16.1 entfernen

Wenn Sie Cross-Origin Resource Sharing (CORS) für den Zugriff auf ONTAP S3 Buckets verwenden, muss dies entfernt werden, bevor Sie von ONTAP 9.16.1 zurückkehren.

Weitere Informationen zu "Zurücksetzen von ONTAP Clustern mit CORS".

ONTAP 9.14.1

NFSv4.1 Session Trunking vor dem Zurücksetzen von ONTAP 9.14.1 deaktivieren

Wenn Trunking für Clientverbindungen aktiviert wurde, muss Trunking auf allen NFSv4.1-Servern deaktiviert werden, bevor ein Wechsel von ONTAP 9.14.1 erfolgt.

Wenn Sie den `revert-to` Befehl eingeben, erscheint eine Warnmeldung, in der empfohlen wird, Trunking zu deaktivieren, bevor Sie fortfahren.

Nach dem Downgrade auf ONTAP 9.13.1 nutzen Clients mit trunked Verbindungen eine einzelne Verbindung. Ihr Datendurchsatz wird beeinträchtigt, es kommt jedoch zu keiner Unterbrechung. Das Rückkehrverhalten entspricht der Änderung der NFSv4.1 trunking Option für die SVM von aktiviert auf deaktiviert.

Schritte

1. Trunking auf dem NFSv4.1 Server deaktivieren:

```
vserver nfs modify -vserver _svm_name_ -v4.1-trunking disabled
```

2. Es sollte überprüft werden, ob NFS wie gewünscht konfiguriert ist:

```
vserver nfs show -vserver _svm_name_
```

ONTAP 9.12.1

Die S3 NAS-Bucket-Konfiguration sollte entfernt werden, bevor von ONTAP 9.12.1 zurückgekehrt wird.

Wenn der S3-Clientzugriff für NAS-Daten konfiguriert wurde, empfiehlt sich die Verwendung der ONTAP Befehlszeilenschnittstelle (CLI), um die NAS-Bucket-Konfiguration sowie alle Namenszuordnungen (S3-Benutzer zu Windows- oder Unix-Benutzern) zu entfernen, bevor von ONTAP 9.12.1 zurückgekehrt wird.

Über diese Aufgabe

Die folgenden Aufgaben werden während des Rücksetzungsprozesses im Hintergrund abgeschlossen.

- Alle unvollständig erstellten Singleton-Objekte (also alle Einträge in versteckten Verzeichnissen) entfernen.
- Alle versteckten Verzeichnisse entfernen; möglicherweise existiert für jedes Volume, das vom Stammverzeichnis des aus dem S3 NAS-Bucket gemappten Exports aus zugänglich ist, ein solches Verzeichnis.
- Die Upload-Tabelle wird entfernt.
- Alle default-unix-user- und default-windows-user-Werte für alle konfigurierten S3-Server löschen.

Schritte

1. S3 NAS-Bucket-Konfiguration entfernen:

```
vserver object-store-server bucket delete -vserver <svm_name> -bucket
<s3_nas_bucket_name>
```

   Weitere Informationen zu `vserver object-store-server bucket delete` finden sich in der "ONTAP-Befehlsreferenz".

2. Namenszuordnungen für UNIX entfernen:

```
vserver name-mapping delete -vserver <svm_name> -direction s3-unix
```

   Weitere Informationen zu `vserver name-mapping delete` finden sich in der "ONTAP-Befehlsreferenz".

3. Namenszuordnungen für Windows entfernen:

```
vserver name-mapping delete -vserver <svm_name> -direction s3-win
```

4. Die S3-Protokolle aus der SVM entfernen:

```
vserver remove-protocols -vserver <svm_name> -protocols s3
```

Weitere Informationen zu `vserver remove-protocols` finden sich in der "ONTAP-Befehlsreferenz".

NVMe In-Band-Authentifizierung vor der Rückkehr von ONTAP 9.12.1 deaktivieren

Wenn Sie das NVME-Protokoll verwenden, muss die In-Band Authentifizierung deaktiviert werden, bevor Sie Ihren Cluster von ONTAP 9.12.1 zurücksetzen. Wenn die In-Band Authentifizierung mit DH-HMAC-CHAP nicht deaktiviert ist, schlägt das Zurücksetzen fehl.

Schritte

1. Den Host aus dem Subsystem entfernen, um die DH-HMAC-CHAP Authentifizierung zu deaktivieren:

```
vserver nvme subsystem host remove -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

2. Es sollte überprüft werden, ob das DH-HMAC-CHAP Authentifizierungsprotokoll vom Host entfernt ist:

```
vserver nvme subsystem host show
```

3. Den Host ohne Authentifizierung wieder dem Subsystem hinzufügen:

```
vserver nvme subsystem host add vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn>
```

Deaktivierung von IPsec in MetroCluster vor der Rückkehr von ONTAP 9.12.1

Bevor eine MetroCluster Konfiguration von ONTAP 9.12.1 zurückgesetzt wird, muss IPsec deaktiviert werden.

Vor dem Zurücksetzen wird geprüft, ob innerhalb der MetroCluster Konfiguration IPsec-Konfigurationen vorhanden sind. Alle vorhandenen IPsec-Konfigurationen müssen entfernt und IPsec muss deaktiviert werden, bevor mit dem Zurücksetzen fortgefahren werden kann. Das Zurücksetzen von ONTAP ist blockiert, wenn IPsec aktiviert ist, selbst wenn keine Benutzerrichtlinien konfiguriert wurden.

ONTAP 9.11.1

Prüfung der ARP-Lizenzierung vor dem Revert von ONTAP 9.11.1

Wenn Sie Autonomous Ransomware Protection (ARP) konfiguriert haben und von ONTAP 9.11.1 auf ONTAP 9.10.1 zurückkehren, kann es zu Warnmeldungen und einer eingeschränkten ARP-Funktionalität kommen.

In ONTAP 9.11.1 wurde die Anti-ransomware-Lizenz anstelle der Multi-Tenant Key Management (MTKM) Lizenz eingeführt. Wenn Ihr System über die Anti_ransomware-Lizenz, aber nicht über die MT_EK_MGMT-Lizenz verfügt, erscheint beim Zurücksetzen eine Warnung, dass ARP auf neuen Volumes nach dem Zurücksetzen nicht aktiviert werden kann.

Die Volumes mit bestehendem Schutz funktionieren nach dem Zurücksetzen weiterhin normal, und der ARP-Status kann über die ONTAP CLI angezeigt werden. System Manager kann den ARP-Status ohne die MTKM-Lizenz nicht anzeigen.

Wenn ARP nach der Rückkehr zu ONTAP 9.10.1 weiterhin funktionieren soll, muss die MTKM-Lizenz vor der Rückkehr installiert sein."Informationen zur ARP-Lizenzierung."

ONTAP 9.6

Vorbereitung synchroner SnapMirror Beziehungen für einen ONTAP 9.6 Revert

Vor dem Zurücksetzen von ONTAP 9.6 auf ONTAP 9.5 sind die Überlegungen zu SnapMirror synchronen Beziehungen zu beachten.

Vor dem Zurücksetzen sind die folgenden Schritte erforderlich, wenn SnapMirror synchron Beziehungen bestehen:

- Es müssen alle SnapMirror synchronen Beziehungen gelöscht werden, in denen das Quellvolume Daten über NFSv4 oder SMB bereitstellt.

  ONTAP 9.5 unterstützt NFSv4 und SMB nicht.

- Alle SnapMirror synchronen Beziehungen in einer Mirror-Mirror-Kaskadenbereitstellung müssen gelöscht werden.

  Eine Spiegel Spiegel Kaskadenbereitstellung wird für SnapMirror synchron Beziehungen in ONTAP 9.5 nicht unterstützt.

- Wenn die gemeinsamen Snapshots in ONTAP 9.5 während des Rücksetzens nicht verfügbar sind, muss die SnapMirror synchron Beziehung nach dem Rücksetzen initialisiert werden.

  Nach zwei Stunden nach dem Upgrade auf ONTAP 9.6 werden die gemeinsamen Snapshots von ONTAP 9.5 automatisch durch die gemeinsamen Snapshots in ONTAP 9.6 ersetzt. Daher kann die SnapMirror synchron Beziehung nach dem Zurücksetzen nicht erneut synchronisiert werden, wenn die gemeinsamen Snapshots von ONTAP 9.5 nicht verfügbar sind.

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.