NVMe-Protokoll verwalten

ONTAP 9

NetApp
November 10, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/san-admin/start-nvme-fc-service-svm-task.html on November 10, 2026. Always check docs.netapp.com for the latest.

Inhalt

NVMe-Protokoll verwalten . . . 1
- Start des NVMe-Service für eine ONTAP SVM . . . 1
- NVMe-Service von einer ONTAP SVM löschen . . . 1
- Größenänderung eines ONTAP NVMe Namespace . . . 2
  - Die Größe eines Namespace vergrößern . . . 2
  - Die Größe eines Namensraums verringern . . . 2
- Konvertierung eines NVMe-Namespace in eine ONTAP LUN . . . 2
  - Bevor Sie beginnen . . . 2
- Einrichten der In-Band-Authentifizierung über NVMe in ONTAP . . . 3
- Deaktivieren der In-Band-Authentifizierung über NVMe in ONTAP . . . 5
- Einrichten eines TLS-sicheren Kanals für NVMe/TCP in ONTAP . . . 6
- TLS sicheren Kanal für NVMe/TCP in ONTAP deaktivieren . . . 7
- Ändern der NVMe Hostpriorität in ONTAP . . . 7
- Automatische Host-Erkennung von NVMe/TCP-Controllern in ONTAP verwalten . . . 8
  - Automatische Host-Erkennung von NVMe/TCP Controllern ermöglichen . . . 9
  - Automatische Erkennung von NVMe/TCP-Controllern auf Hosts deaktivieren . . . 9
- NVMe-Host-VM-Kennung in ONTAP deaktivieren . . . 9

NVMe-Protokoll verwalten

Start des NVMe-Service für eine ONTAP SVM

Bevor Sie das NVMe-Protokoll auf Ihrer Storage Virtual Machine (SVM) verwenden können, muss der NVMe-Dienst auf der SVM gestartet werden.

Bevor Sie beginnen

NVMe muss als Protokoll auf Ihrem System zugelassen sein.

Folgende NVMe-Protokolle werden unterstützt:

Protokoll	Ab Version …	Erlaubt durch…
TCP	ONTAP 9.10.1	Standard
FCP	ONTAP 9.4	Standard

Schritte

1. Die Berechtigungseinstellung auf „Erweitert“ ändern:

   ```
   set -privilege advanced
   ```

2. Es sollte überprüft werden, ob NVMe als Protokoll zulässig ist:

   ```
   vserver nvme show
   ```

3. Den NVMe-Protokolldienst erstellen:

   ```
   vserver nvme create
   ```

4. Der NVMe-Protokolldienst auf der SVM wird gestartet:

   ```
   vserver nvme modify -status -admin up
   ```

NVMe-Service von einer ONTAP SVM löschen

Bei Bedarf kann der NVMe-Service von Ihrer Storage Virtual Machine (SVM) entfernt werden.

Schritte

1. Die Berechtigungseinstellung auf „Erweitert“ ändern:

   ```
   set -privilege advanced
   ```

2. Den NVMe-Service auf der SVM beenden:

   ```
   vserver nvme modify -status -admin down
   ```

3. Der NVMe-Dienst wird gelöscht:

```
vserver nvme delete
```

Größenänderung eines ONTAP NVMe Namespace

Ab ONTAP 9.10.1 kann die Größe eines NVMe Namespace über die ONTAP Befehlszeile (CLI) erhöht oder verringert werden. Mit dem System Manager kann die Größe eines NVMe Namespace erhöht werden.

Die Größe eines Namespace vergrößern

System Manager

1. **Speicher > NVMe Namespaces** auswählen.
2. Fahren Sie mit dem Mauszeiger über den Namespace, den Sie vergrößern möchten, klicken Sie auf ⋮ und anschließend auf **Bearbeiten**.
3. Unter **CAPACITY** die Größe des Namensraums ändern.

CLI

1. Geben Sie den folgenden Befehl ein: `vserver nvme namespace modify -vserver` *`SVM_name`* `-path` *`path`* `–size` *`new_size_of_namespace`*

Die Größe eines Namensraums verringern

Die ONTAP CLI muss verwendet werden, um die Größe eines NVMe Namespace zu verringern.

1. Die Berechtigungseinstellung auf „Erweitert“ ändern:

   ```
   set –privilege advanced
   ```

2. Die Größe des Namensraums verringern:

   ```
   vserver nvme namespace modify -vserver SVM_name -path namespace_path -size
   new_size_of_namespace
   ```

Konvertierung eines NVMe-Namespace in eine ONTAP LUN

Ab ONTAP 9.11.1 kann die ONTAP CLI verwendet werden, um einen vorhandenen NVMe Namespace direkt in eine LUN zu konvertieren.

Bevor Sie beginnen

- Der angegebene NVMe Namespace sollte keine bestehenden Zuordnungen zu einem Subsystem haben.
- Der Namespace sollte weder Teil eines Snapshots sein noch auf der Zielseite der SnapMirror Beziehung als schreibgeschützter Namespace vorliegen.
- Da NVMe-Namespaces nur von bestimmten Plattformen und Netzwerkkarten unterstützt werden, funktioniert diese Funktion nur mit bestimmter Hardware.

Schritte

1. Geben Sie den folgenden Befehl ein, um einen NVMe Namespace in eine LUN zu konvertieren:

   `lun convert-from-namespace -vserver -namespace-path`

   Weitere Informationen zu `lun convert-from-namespace` finden sich in der "ONTAP-Befehlsreferenz".

Einrichten der In-Band-Authentifizierung über NVMe in ONTAP

Ab ONTAP 9.12.1 kann die ONTAP Befehlszeilenschnittstelle (CLI) verwendet werden, um die In-Band-Authentifizierung (sicher), bidirektionale und unidirektionale Authentifizierung zwischen einem NVMe-Host und einem Controller über die Protokolle NVMe/TCP und NVMe/FC mittels DH-HMAC-CHAP Authentifizierung zu konfigurieren. Ab ONTAP 9.14.1 kann die In-Band-Authentifizierung im System Manager konfiguriert werden.

Um die In-Band-Authentifizierung einzurichten, muss jedem Host oder Controller ein DH-HMAC-CHAP-Schlüssel zugeordnet werden, der eine Kombination aus dem NQN des NVMe-Hosts oder -Controllers und einem vom Administrator konfigurierten Authentifizierungsgeheimnis ist. Damit ein NVMe-Host oder -Controller seinen Peer authentifizieren kann, muss er den dem Peer zugeordneten Schlüssel kennen.

Bei der unidirektionalen Authentifizierung wird ein geheimer Schlüssel für den Host, aber nicht für den Controller konfiguriert. Bei der bidirektionalen Authentifizierung wird ein geheimer Schlüssel sowohl für den Host als auch für den Controller konfiguriert.

SHA-256 ist die Standard-Hashfunktion und 2048-Bit ist die Standard-DH-Gruppe.

System Manager

Ab ONTAP 9.14.1 kann mit dem System Manager die In-Band-Authentifizierung beim Erstellen oder Aktualisieren eines NVMe-Subsystems, beim Erstellen oder Klonen von NVMe-Namespaces oder beim Hinzufügen von Konsistenzgruppen mit neuen NVMe-Namespaces konfiguriert werden.

Schritte

1. Im System Manager auf **Hosts > NVMe Subsystem** und dann auf **Hinzufügen** klicken.
2. Den Namen des NVMe-Subsystems hinzufügen sowie die Storage-VM und das Host-Betriebssystem auswählen.
3. Geben Sie den Host NQN ein.
4. Neben dem Host-NQN ist **In-Band-Authentifizierung verwenden** auszuwählen.
5. Das Host-Geheimnis und das Controller-Geheimnis angeben.

   Der DH-HMAC-CHAP-Schlüssel ist eine Kombination aus dem NQN des NVMe-Hosts oder -Controllers und einem vom Administrator konfigurierten Authentifizierungsgeheimnis.

6. Die bevorzugte Hash-Funktion und DH-Gruppe für jeden Host auswählen.

   Wenn Sie keine Hash-Funktion und keine DH-Gruppe auswählen, wird SHA-256 als Standard-Hash-Funktion und 2048-Bit als Standard-DH-Gruppe festgelegt.

7. Optional auf **Hinzufügen** klicken und die Schritte nach Bedarf wiederholen, um weitere Hosts

hinzuzufügen.

8. Auf **Speichern** klicken.
9. Zur Überprüfung, ob die In-Band Authentifizierung aktiviert ist, **System Manager > Hosts > NVMe Subsystem > Grid > Peek view** auswählen.

   Ein transparentes Schlüsselsymbol neben dem Hostnamen zeigt an, dass der unidirektionale Modus aktiviert ist. Ein undurchsichtiges Schlüsselsymbol neben dem Hostnamen zeigt an, dass der bidirektionale Modus aktiviert ist.

CLI

Schritte

1. DH-HMAC-CHAP-Authentifizierung zum NVMe-Subsystem hinzufügen:

   ```
   vserver nvme subsystem host add -vserver <svm_name> -subsystem
   <subsystem> -host-nqn <host_nqn> -dhchap-host-secret
   <authentication_host_secret> -dhchap-controller-secret
   <authentication_controller_secret> -dhchap-hash-function <sha-
   256|sha-512> -dhchap-group <none|2048-bit|3072-bit|4096-bit|6144-
   bit|8192-bit>
   ```

   Weitere Informationen zu `vserver nvme subsystem host add` finden sich in der "ONTAP-Befehlsreferenz".

2. Es sollte überprüft werden, ob das DH-HMAC CHAP Authentifizierungsprotokoll zu Ihrem Host hinzugefügt wurde:

   ```
   vserver nvme subsystem host show
   ```

   ```
     [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
   Function
     [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
   bit} ]
                                                  Authentication
   Diffie-Hellman
                                                  Group
     [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                  Authentication Mode
   ```

   Weitere Informationen zu `vserver nvme subsystem host show` finden sich in der "ONTAP-Befehlsreferenz".

3. Es sollte überprüft werden, ob die DH-HMAC CHAP Authentifizierung während der Erstellung des NVMe Controllers erfolgt ist:

```
vserver nvme subsystem controller show
```

```
 [ -dhchap-hash-function {sha-256|sha-512} ]  Authentication Hash
Function
 [ -dhchap-dh-group {none|2048-bit|3072-bit|4096-bit|6144-bit|8192-
bit} ]
                                                Authentication
Diffie-Hellman
                                                Group
 [ -dhchap-mode {none|unidirectional|bidirectional} ]
                                                Authentication Mode
```

Verwandte Informationen

- "vserver nvme subsystem controller show"

Deaktivieren der In-Band-Authentifizierung über NVMe in ONTAP

Wenn Sie die In-Band-Authentifizierung über NVMe mit DH-HMAC-CHAP konfiguriert haben, kann sie jederzeit deaktiviert werden.

Wenn Sie von ONTAP 9.12.1 oder höher auf ONTAP 9.12.0 oder früher zurückkehren, müssen Sie die In-Band-Authentifizierung vor dem Zurücksetzen deaktivieren. 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>
```

Einrichten eines TLS-sicheren Kanals für NVMe/TCP in ONTAP

Ab ONTAP 9.16.1 ist die Konfiguration eines sicheren TLS-Kanals für NVMe/TCP-Verbindungen möglich. System Manager oder die ONTAP CLI können verwendet werden, um entweder ein neues NVMe-Subsystem mit aktiviertem TLS hinzuzufügen oder TLS für ein bestehendes NVMe-Subsystem zu aktivieren. Ab ONTAP 9.19.1 wird TLS Hardware Offload unterstützt.

System Manager

Ab ONTAP 9.16.1 kann mit System Manager TLS für NVMe/TCP-Verbindungen konfiguriert werden, wenn ein NVMe-Subsystem erstellt oder aktualisiert, NVMe-Namespaces erstellt oder geklont oder Konsistenzgruppen mit neuen NVMe-Namespaces hinzugefügt werden.

Schritte

1. Im System Manager auf **Hosts > NVMe Subsystem** und dann auf **Hinzufügen** klicken.
2. Den Namen des NVMe-Subsystems hinzufügen sowie die Storage-VM und das Host-Betriebssystem auswählen.
3. Geben Sie den Host NQN ein.
4. Neben dem Host-NQN ist **Transport Layer Security (TLS) erforderlich** auszuwählen.
5. Den vorab geteilten Schlüssel (PSK) angeben.
6. Auf **Speichern** klicken.
7. Zur Überprüfung, ob der sichere TLS-Kanal aktiviert ist, **System Manager > Hosts > NVMe Subsystem > Grid > Peek view** auswählen.

CLI

Schritte

1. Einen NVMe-Subsystem-Host hinzufügen, der TLS Secure Channel unterstützt. Ein vorab geteilter Schlüssel (PSK) kann mit dem `tls-configured-psk` Argument bereitgestellt werden.

```
vserver nvme subsystem host add -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-configured-psk <key_text>
```

2. Es sollte überprüft werden, ob der NVMe-Subsystem-Host für den sicheren TLS-Kanal konfiguriert ist. Optional kann das `tls-key-type` Argument verwendet werden, um nur Hosts anzuzeigen, die diesen Schlüsseltyp verwenden:

```
vserver nvme subsystem host show -vserver <svm_name> -subsystem
<subsystem> -host-nqn <host_nqn> -tls-key-type {none|configured}
```

3. Es sollte überprüft werden, ob der Hostcontroller des NVMe-Subsystems für einen sicheren TLS-Kanal konfiguriert ist. Optional können die Argumente `tls-key-type`, `tls-identity` oder `tls-cipher` verwendet werden, um nur die Controller anzuzeigen, die diese TLS-Attribute aufweisen.

```
vserver nvme subsystem controller show -vserver <svm_name>
-subsystem <subsystem> -host-nqn <host_nqn> -tls-key-type
{none|configured} -tls-identity <text> -tls-cipher
{none|TLS_AES_128_GCM_SHA256|TLS_AES_256_GCM_SHA384}
```

Verwandte Informationen

- "vserver nvme Subsystem"
- "TLS-Hardware-Offload konfigurieren"

TLS sicheren Kanal für NVMe/TCP in ONTAP deaktivieren

Ab ONTAP 9.16.1 kann ein TLS-Sicherheitskanal für NVMe/TCP-Verbindungen konfiguriert werden. Wenn ein TLS-Sicherheitskanal für NVMe/TCP-Verbindungen konfiguriert wurde, besteht jederzeit die Möglichkeit, ihn zu deaktivieren.

Schritte

1. Entfernen Sie den Host aus dem Subsystem, um den sicheren TLS-Kanal zu deaktivieren:

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

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

```
vserver nvme subsystem host show
```

3. Den Host ohne sicheren TLS-Kanal wieder zum Subsystem hinzufügen:

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

Verwandte Informationen

- "vserver nvme subsystem host"

Ändern der NVMe Hostpriorität in ONTAP

Ab ONTAP 9.14.1 kann das NVMe-Subsystem so konfiguriert werden, dass die Ressourcenzuweisung für bestimmte Hosts priorisiert wird. Standardmäßig wird einem Host, der dem Subsystem hinzugefügt wird, eine reguläre Priorität zugewiesen. Hosts mit hoher Priorität werden größere I/O-Warteschlangenzahlen und Warteschlangentiefen zugewiesen.

Die Standardpriorität kann über die ONTAP command line interface (CLI) manuell von Normal auf Hoch geändert werden. Um die einem Host zugewiesene Priorität zu ändern, ist es erforderlich, den Host aus dem Subsystem zu entfernen und anschließend wieder hinzuzufügen.

Schritte

1. Es sollte überprüft werden, ob die Hostpriorität auf „regulär“ gesetzt ist:

   ```
   vserver nvme show-host-priority
   ```

   Weitere Informationen zu `vserver nvme show-host-priority` finden sich in der "ONTAP-Befehlsreferenz".

2. Den Host aus dem Subsystem entfernen:

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

   Weitere Informationen zu `vserver nvme subsystem host remove` finden sich in der "ONTAP-Befehlsreferenz".

3. Es sollte überprüft werden, ob der Host aus dem Subsystem entfernt wurde:

   ```
   vserver nvme subsystem host show
   ```

   Weitere Informationen zu `vserver nvme subsystem host show` finden sich in der "ONTAP-Befehlsreferenz".

4. Den Host mit hoher Priorität wieder dem Subsystem hinzufügen:

   ```
   vserver nvme subsystem host add -vserver <SVM_name> -subsystem
   <subsystem_name> -host-nqn <Host_NQN_:subsystem._subsystem_name>
   -priority high
   ```

   Weitere Informationen zu `vserver nvme subsystem host add` finden sich in der "ONTAP-Befehlsreferenz".

Automatische Host-Erkennung von NVMe/TCP-Controllern in ONTAP verwalten

Ab ONTAP 9.14.1 ist die Host-Erkennung von Controllern über das NVMe/TCP-Protokoll in IP-basierten Fabrics standardmäßig automatisiert.

Automatische Host-Erkennung von NVMe/TCP Controllern ermöglichen

Falls die automatische Host-Erkennung zuvor deaktiviert wurde, sich die Anforderungen jedoch geändert haben, kann sie wieder aktiviert werden.

Schritte

1. Erweiterten Berechtigungsmodus aktivieren:

```
set -privilege advanced
```

2. Automatische Erkennung:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled true
```

3. Es wird überprüft, ob die automatische Erkennung von NVMe/TCP Controllern aktiviert ist.

```
vserver nvme show -fields mdns-service-discovery-enabled
```

Automatische Erkennung von NVMe/TCP-Controllern auf Hosts deaktivieren

Wenn es nicht erforderlich ist, dass NVMe/TCP Controller von Ihrem Host automatisch erkannt werden und unerwünschter Multicast-Verkehr in Ihrem Netzwerk festgestellt wird, empfiehlt sich das Deaktivieren dieser Funktionalität.

Schritte

1. Erweiterten Berechtigungsmodus aktivieren:

```
set -privilege advanced
```

2. Automatische Erkennung deaktivieren:

```
vserver nvme modify -vserver <vserver_name> -mdns-service-discovery
-enabled false
```

3. Es wird überprüft, ob die automatische Erkennung von NVMe/TCP Controllern deaktiviert ist.

```
vserver nvme show -fields mdns-service-discovery-enabled
```

NVMe-Host-VM-Kennung in ONTAP deaktivieren

Ab ONTAP 9.14.1 unterstützt ONTAP standardmäßig die Möglichkeit von NVMe/FC-

Hosts, virtuelle Maschinen anhand einer eindeutigen Kennung zu identifizieren und für NVMe/FC-Hosts, die Ressourcenauslastung virtueller Maschinen zu überwachen. Dies verbessert die Berichterstellung und Fehlerbehebung auf Host-Seite.

Sie können das Bootargument verwenden, um diese Funktionalität zu deaktivieren. Siehe "NetApp Knowledge Base: Wie die NVMe-Host-VM-Kennung in ONTAP deaktiviert wird".

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.