E

SANtricity commands

NetApp
September 08, 2026

This PDF was generated from https://docs.netapp.com/de-de/e-series-cli/commands-a-z/enable-controller-datatransfer.html on September 08, 2026. Always check docs.netapp.com for the latest.

Inhalt

E . . . 1
Controller-Datenübertragung aktivieren – SANtricity CLI . . . 1
Unterstützte Arrays . . . 1
Rollen . . . 1
Syntax . . . 1
Parameter . . . 1
Minimale Firmware-Stufe . . . 1
Datenträgerpool-Sicherheit aktivieren – SANtricity CLI . . . 1
Unterstützte Arrays . . . 1
Rollen . . . 2
Kontext . . . 2
Syntax . . . 2
Parameter . . . 2
Hinweise . . . 2
Minimale Firmware-Stufe . . . 2
AutoSupport aktivieren oder deaktivieren (alle einzelnen Arrays) – SANtricity CLI . . . 2
Unterstützte Arrays . . . 2
Rollen . . . 3
Kontext . . . 3
Syntax . . . 3
Parameter . . . 3
Verifizierung . . . 3
Minimale Firmware-Stufe . . . 3
Externe Sicherheitsschlüsselverwaltung aktivieren – SANtricity CLI . . . 4
Unterstützte Arrays . . . 4
Rollen . . . 4
Kontext . . . 4
Syntax . . . 4
Parameter . . . 4
Hinweise . . . 5
Minimale Firmware-Stufe . . . 5
Speicherarray-Funktion aktivieren – SANtricity CLI . . . 5
Unterstützte Arrays . . . 5
Rollen . . . 5
Kontext . . . 5
Syntax zum Aktivieren eines Feature-Schlüssels . . . 6
Syntax zum Aktivieren eines Funktionspacks . . . 6
Syntax, um eine Funktion für einen Testzeitraum zu aktivieren . . . 6
Minimale Firmware-Stufe . . . 7
Volumegruppensicherheit aktivieren – SANtricity CLI . . . 7
Unterstützte Arrays . . . 7
Rollen . . . 7
Syntax . . . 7

Parameter . . . 7
Hinweise . . . 7
Minimale Firmware-Stufe . . . 8
Asynchrones gespiegeltes Paar erstellen – SANtricity CLI . . . 8
Unterstützte Arrays . . . 8
Rollen . . . 8
Kontext . . . 8
Syntax . . . 8
Parameter . . . 8
Hinweise . . . 9
Minimale Firmware-Stufe . . . 9
Sicherheitsschlüssel für Speicherarrays exportieren – SANtricity CLI . . . 9
Unterstützte Arrays . . . 9
Rollen . . . 10
Kontext . . . 10
Syntax . . . 10
Parameter . . . 10
Hinweise . . . 10
Minimale Firmware-Stufe . . . 11

E

Controller-Datenübertragung aktivieren – SANtricity CLI

Der `enable controller dataTransfer` Befehl gibt einen Controller wieder, der während der Ausführung der Diagnose stillgelegt wurde.

Unterstützte Arrays

Dieser Befehl gilt für jedes einzelne Speichersystem, einschließlich der E4000, E2700, E5600, E2800, E5700, EF600, EF300, EF50 und EF80 Arrays, sofern alle SMcli Pakete installiert sind.

Rollen

Um diesen Befehl auf einem E4000, E2800, E5700, EF600, EF300, EF50 oder EF80 Storage-Array auszuführen, müssen Sie die Storage Admin-Rolle haben.

Syntax

```
enable controller [(a|b)] dataTransfer
```

Parameter

Parameter	Beschreibung
`controller`	Der Controller, den Sie beleben möchten. Gültige Controller-IDs sind `a` Oder `b`, Wo `a` Ist der Controller in Steckplatz A, und `b` Ist der Controller in Steckplatz B. Schließen Sie die Controller-Kennung in eckige Klammern ([ ]). Wenn Sie keinen Controller angeben, gibt die Storage-Managementsoftware einen Syntaxfehler aus.

Minimale Firmware-Stufe

6.10

Datenträgerpool-Sicherheit aktivieren – SANtricity CLI

Der `enable diskPool security` Befehl konvertiert einen nicht sicheren Laufwerk-Pool in einen sicheren Laufwerk-Pool.

Unterstützte Arrays

Dieser Befehl gilt für jedes einzelne Speichersystem, einschließlich der E4000, E2700, E5600, E2800, E5700, EF600, EF300, EF50 und EF80 Arrays, sofern alle SMcli Pakete installiert sind.

Rollen

Um diesen Befehl auf einem E4000, E2800, E5700, EF600, EF300, EF50 oder EF80 Storage-Array auszuführen, müssen Sie die Storage Admin-Rolle haben.

Kontext

Alle Laufwerke aus dem Laufwerk-Pool müssen sicher sein.

Syntax

```
enable diskPool [diskPoolName] security
```

Parameter

Parameter	Beschreibung
`diskPool`	Der Name des Laufwerk-Pools, den Sie in den Status Security Enabled setzen möchten. Schließen Sie die Disk-Pool-Kennung in eckige Klammern ([ ]).

Hinweise

Jeder Disk Pool-Name muss eindeutig sein. Sie können eine beliebige Kombination aus alphanumerischen Zeichen, Unterstrich (_), Bindestrich (-) und Pfund (#) für die Benutzerbezeichnung verwenden. Benutzeretiketten können maximal 30 Zeichen lang sein.

Minimale Firmware-Stufe

7.83

AutoSupport aktivieren oder deaktivieren (alle einzelnen Arrays) – SANtricity CLI

Mit diesem Befehl wird die AutoSupport (ASUP)-Funktion für das Storage Array aktiviert oder deaktiviert und Meldungen können an den technischen Support-Standort übertragen werden. Nach Aktivierung der ASUP Funktion wird das ASUP-fähige Storage-Array automatisch bereit, Support-bezogene Daten zu sammeln und an den technischen Support zu senden. Die Daten können dann für Remote-Fehlerbehebung und Problemanalysen genutzt werden.

Unterstützte Arrays

Dieser Befehl gilt für jedes einzelne Speichersystem, einschließlich der E4000, E2700, E5600, E2800, E5700, EF600, EF300, EF50 und EF80 Arrays, sofern alle SMcli Pakete installiert sind.

Rollen

Um diesen Befehl auf einem E4000, E2800, E5700, EF600, EF300, EF50 oder EF80 Storage-Array auszuführen, müssen Sie die Storage Admin-Rolle haben.

Kontext

Nach der Aktivierung dieser Funktion können Sie die Funktion AutoSupport OnDemand (falls gewünscht) als nächstes aktivieren und anschließend die Funktion AutoSupport Remote Diagnostics (falls gewünscht) aktivieren.

Sie müssen die drei Funktionen in dieser Reihenfolge aktivieren:

1. **AutoSupport aktivieren**
2. **AutoSupport OnDemand aktivieren**
3. **AutoSupport-Ferndiagnose aktivieren**

Syntax

```
set storageArray autoSupport (enable | disable)
```

Parameter

Parameter	Beschreibung
`enable	disable`

Beispiele

```
SMcli -n Array1 -c "set storageArray autoSupport enable;"

SMcli completed successfully.
```

Verifizierung

Verwenden Sie die `show storageArray autoSupport` Befehl, um zu sehen, ob Sie die Funktion aktiviert haben. In der Anfangszeile der angezeigten Ausgabe wird der Status „Aktivieren“ angezeigt:

```
The AutoSupport feature is enabled on this storage array.
```

Minimale Firmware-Stufe

7.86 – zusätzlicher Befehl für alle Storage Arrays bis zum Modell E2700 und E5600

8.40 - Unterstützung für E2800 und E5700 hinzugefügt

Externe Sicherheitsschlüsselverwaltung aktivieren – SANtricity CLI

Der `enable storageArray externalKeyManagement file` Befehl aktiviert die externe Sicherheitsschlüsselverwaltung für ein Speicher-Array mit vollständigen Festplatten-Verschlüsselung und erstellt den ersten Sicherheitsschlüssel des Laufwerks.

Unterstützte Arrays

Dieser Befehl gilt für einzelne E4000, E2800, E5700, EF600, EF300, EF50 und EF80 Speicherarrays. Er funktioniert nicht auf E2700 oder E5600 Speicherarrays.

Rollen

Um diesen Befehl auf einem E4000, E2800, E5700, EF600, EF300, EF50 oder EF80 Storage-Array auszuführen, müssen Sie die Security Admin-Rolle haben.

Kontext

Dieser Befehl gilt nur für externes Verschlüsselungsmanagement.

Syntax

```
enable storageArray externalKeyManagement
file="fileName"
passPhrase="passPhraseString"
saveFile=(TRUE | FALSE)
```

Parameter

Parameter	Beschreibung
`file`	Der Dateipfad und der Dateiname, in dem der neue Sicherheitsschlüssel gespeichert wird. Schließen Sie den Dateipfad und den Dateinamen in doppelte Anführungszeichen (" "). Beispiel: `file="C:\Program Files\CLI\sup\drivesecurity.slk"` Der Dateiname muss über eine Erweiterung von verfügen `.slk`.

Parameter	Beschreibung
`passPhrase`	Eine Zeichenkette, die den Sicherheitsschlüssel verschlüsselt, sodass Sie den Sicherheitsschlüssel in einer externen Datei speichern können. Schließen Sie die Zeichenfolge für den Durchlauf in doppelte Anführungszeichen (" ") ein.
`saveFile`	Überprüft und speichert den Sicherheitsschlüssel in einer Datei. Auf einstellen `FALSE` So speichern und überprüfen Sie den Sicherheitsschlüssel nicht in einer Datei. Der Standardwert ist `TRUE`.

Hinweise

Ihr Passphrase muss folgende Kriterien erfüllen:

- Muss zwischen acht und 32 Zeichen lang sein.
- Muss mindestens einen Großbuchstaben enthalten.
- Muss mindestens einen Kleinbuchstaben enthalten.
- Muss mindestens eine Zahl enthalten.
- Muss mindestens ein nicht-alphanumerisches Zeichen enthalten, z. B. @ +.

Wenn Ihr Passphrase diese Kriterien nicht erfüllt, erhalten Sie eine Fehlermeldung.

Minimale Firmware-Stufe

8.40

8.70 fügt die hinzu *`saveFile`* Parameter.

Speicherarray-Funktion aktivieren – SANtricity CLI

Der `enable storageArray feature file` Mit dem Befehl wird eine Funktion für ein permanentes Upgrade auf das Speicher-Array oder eine Testphase aktiviert.

Unterstützte Arrays

Dieser Befehl gilt für jedes einzelne Speichersystem, einschließlich der E4000, E2700, E5600, E2800, E5700, EF600, EF300, EF50 und EF80 Arrays, sofern alle SMcli Pakete installiert sind.

Rollen

Um diesen Befehl auf einem E4000, E2800, E5700, EF600, EF300, EF50 oder EF80 Speichersystem auszuführen, müssen Sie die Rolle Storage Admin oder Support Admin haben.

Kontext

Dieser Befehl führt eine der folgenden Aktionen aus:

- Aktiviert einen Funktionstaste für ein permanentes Upgrade einer Funktion
- Aktiviert einen Funktionstaste für ein permanentes Upgrade eines Funktionsacks
- Aktiviert eine Funktion für einen Testzeitraum

Ein Funktionspaket ist ein vordefinierter Satz an Funktionen, wie z. B. Storage Partitioning und Synchronous Mirroring. Diese Funktionen werden für den Komfort der Benutzer kombiniert. Wenn Benutzer ein Feature Pack installieren, werden alle Funktionen des Feature Packs gleichzeitig installiert.

Jede Funktion wird von einem Lizenzschlüssel verwaltet, der für eine bestimmte Funktion oder ein bestimmtes Funktionspaket und ein bestimmtes Storage-Array erzeugt wird. Der Lizenzschlüssel wird als Datei ausgeliefert, die Sie ausführen, um die Lizenz für die Funktion anzuwenden.

Um festzustellen, welche Funktionen auf dem Speicher-Array geladen sind, führen Sie den aus `show storageArray features` Befehl. Der `show storageArray features` Der Befehl führt alle auf dem Speicher-Array installierten Funktionen auf, die für einen Testzeitraum ausgewertet werden können, welche Funktionen aktiviert sind und welche Funktionen deaktiviert sind.

Syntax zum Aktivieren eines Feature-Schlüssels

```
enable storageArray feature file="filename"
```

Der `file` Parameter identifiziert den Dateipfad und den Dateinamen einer gültigen Funktionsschlüsseldatei. Schließen Sie den Dateipfad und den Dateinamen in doppelte Anführungszeichen (" "). Beispiel:

```
file="C:\Program Files\CLI\dnld\ftrkey.key"
```

Gültige Dateinamen für Feature-Key-Dateien enden mit einem `.key` Erweiterung.

Für jedes Feature, das Sie aktivieren möchten, benötigen Sie eine Feature Key-Datei.

Syntax zum Aktivieren eines Funktionspacks

```
enable storageArray featurePack file="filename"
```

Der `file` Der Parameter identifiziert den Dateipfad und den Dateinamen einer gültigen Feature Pack-Datei. Schließen Sie den Dateipfad und den Dateinamen in doppelte Anführungszeichen (" "). Beispiel:

```
file="C:\Program Files\CLI\dnld\ftrpk.key"
```

Gültige Dateinamen für Feature-Key-Dateien enden mit einem `.key` Erweiterung.

Syntax, um eine Funktion für einen Testzeitraum zu aktivieren

```
enable storageArray feature=featureAttributeList
```

Um eine Funktion für einen Testzeitraum zu bewerten, können Sie einen oder mehrere der folgenden Attributwerte für das eingeben `featureAttributeList`. Wenn Sie mehr als einen Attributwert eingeben, trennen Sie die Werte mit einem Leerzeichen.

- `driveSecurity`

Minimale Firmware-Stufe

8.25 entfernt alle Attribute, die nicht mehr gültig sind.

Volumegruppensicherheit aktivieren – SANtricity CLI

Der `enable volumeGroup security` Befehl konvertiert eine nicht sichere Volume-Gruppe in eine sichere Volume-Gruppe.

Unterstützte Arrays

Dieser Befehl gilt für jedes einzelne Speichersystem, einschließlich der E4000, E2700, E5600, E2800, E5700, EF600, EF300, EF50 und EF80 Arrays, sofern alle SMcli Pakete installiert sind.

Rollen

Um diesen Befehl auf einem E4000, E2800, E5700, EF600, EF300, EF50 oder EF80 Storage-Array auszuführen, müssen Sie die Storage Admin-Rolle haben.

Syntax

```
enable volumeGroup [volumeGroupName] security
```

Parameter

Parameter	Beschreibung
`volumeGroup`	Der Name der Volume-Gruppe, die Sie in den Status „Security Enabled“ einfügen möchten. Umschließen Sie den Namen der Volume-Gruppe in eckige Klammern ([ ]).

Hinweise

Diese Bedingungen müssen erfüllt sein, damit dieser Befehl erfolgreich ausgeführt wird.

- Bei allen Laufwerken in der Volume-Gruppe müssen es sich um Laufwerke mit vollständiger Festplattenverschlüsselung befinden.
- Die Laufwerkssicherheitsfunktion muss aktiviert sein.

- Der Sicherheitsschlüssel für das Speicher-Array muss festgelegt werden.
- Die Volume-Gruppe ist optimal und verfügt nicht über Repository-Volumes.

Durch die Controller-Firmware wird eine Sperre erstellt, durch die der Zugriff auf FDE-Laufwerke eingeschränkt wird. FDE-Laufwerke weisen einen Zustand auf, der als „Security-fähig“ bezeichnet wird. Wenn Sie einen Sicherheitsschlüssel erstellen, wird der Status auf „aktiviert“ gesetzt, was den Zugriff auf alle im Speicher-Array vorhandenen FDE-Laufwerke einschränkt.

Minimale Firmware-Stufe

7.40

Asynchrones gespiegeltes Paar erstellen – SANtricity CLI

Der `establish asyncMirror volume` Der Befehl schließt ein asynchrones gespiegeltes Paar auf dem Remote-Storage-Array durch Hinzufügen eines sekundären Volumes zu einer vorhandenen asynchronen Spiegelgruppe ab.

Unterstützte Arrays

Dieser Befehl gilt für jedes einzelne Speichersystem, einschließlich der E4000, E2700, E5600, E2800, E5700, EF600 und EF300 Arrays, sofern alle SMcli Pakete installiert sind.

Rollen

Um diesen Befehl auf einem E4000, E2800, E5700, EF600 oder EF300 Storage Array auszuführen, ist die Rolle Storage Admin erforderlich.

Kontext

Bevor Sie diesen Befehl ausführen, muss die asynchrone Spiegelgruppe vorhanden sein und das primäre Volume in der asynchronen Spiegelgruppe vorhanden sein. Wenn dieser Befehl erfolgreich abgeschlossen ist, wird die asynchrone Spiegelung zwischen dem primären Volume und dem sekundären Volume gestartet.

Die beiden Volumes, die ein asynchrones gespiegeltes Paar umfassen, funktionieren als einzelne Einheit. Über ein asynchrones gespiegeltes Paar können Sie Aktionen auf dem gesamten gespiegelten Paar gegenüber den beiden individuellen Volumes durchführen.

Syntax

```
establish asyncMirror volume="secondaryVolumeName"
asyncMirrorGroup="asyncMirrorGroupName"
primaryVolume="primaryVolumeName"
```

Parameter

Parameter	Beschreibung
`volume`	Der Name eines vorhandenen Volumes auf dem Remote-Storage-Array, das Sie für das sekundäre Volume verwenden möchten. Schließen Sie den Volumennamen in doppelte Anführungszeichen (" ").
`asyncMirrorGroup`	Der Name einer vorhandenen asynchronen Spiegelgruppe, die Sie verwenden möchten, um das asynchrone gespiegelte Paar zu enthalten. Schließen Sie den Namen der asynchronen Spiegelgruppe in doppelte Anführungszeichen (" ").
`primaryVolume`	Der Name eines vorhandenen Volumes auf dem lokalen Speicher-Array, das Sie für das primäre Volume verwenden möchten. Schließen Sie den Volumennamen in doppelte Anführungszeichen (" ").

Hinweise

Ein asynchrones gespiegeltes Paar besteht aus zwei Volumes, einem primären Volume und einem sekundären Volume, die identische Kopien derselben Daten enthalten. Das gespiegelte Paar ist Teil einer asynchronen Spiegelgruppe, die es dem gespiegelten Paar ermöglicht, gleichzeitig mit allen anderen gespiegelten Paaren innerhalb der asynchronen Spiegelgruppe zu synchronisieren.

Sie können eine beliebige Kombination aus alphanumerischen Zeichen, Bindestriche und Unterstrichen für die Namen verwenden. Namen können maximal 30 Zeichen lang sein.

Bei Auswahl des primären Volume und des sekundären Volumes muss das sekundäre Volume größer oder gleich dem primären Volume sein. Die RAID-Ebene des sekundären Volumes muss nicht mit dem primären Volume identisch sein.

Minimale Firmware-Stufe

7.84

11.80 bietet Unterstützung für EF600 und EF300 Arrays

Sicherheitsschlüssel für Speicherarrays exportieren – SANtricity CLI

Der `export storageArray securityKey` Befehl speichert einen Laufwerksicherheitsschlüssel in einer Datei.

Unterstützte Arrays

Wenn die externe Schlüsselverwaltung aktiviert ist, gilt dieser Befehl nur für die E4000, E2800, E5700, EF600, EF300, EF50 und EF80 Arrays. Wenn die interne Schlüsselverwaltung aktiviert ist, gilt der Befehl für jedes einzelne Storage-Array, sofern alle SMcli Pakete installiert sind.

Rollen

Um diesen Befehl auf einem E4000, E2800, E5700, EF600, EF300, EF50 oder EF80 Storage-Array auszuführen, müssen Sie die Security Admin-Rolle haben.

Kontext

Wenn die Schlüsseldatei aus einem Speicher-Array exportiert wird, kann dieser Schlüssel in ein anderes Speicher-Array importiert werden. So können Sie sicherheitsfähige Laufwerke zwischen Storage Arrays verschieben.

> Dieser Befehl gilt sowohl für das interne als auch für das externe Verschlüsselungsmanagement.

Syntax

```
export storageArray securityKey
passPhrase="passPhraseString"
file="fileName"
```

Parameter

Parameter	Beschreibung
`passPhrase`	Eine Zeichenkette, die den Sicherheitsschlüssel verschlüsselt, sodass Sie den Sicherheitsschlüssel in einer externen Datei speichern können. Schließen Sie den Passphrase in doppelte Anführungszeichen (" ").
`file`	Der Dateipfad und der Dateiname, in den Sie den Sicherheitsschlüssel speichern möchten. Beispiel: `file="C:\Program Files\CLI\sup\drivesecurity.slk"` Der Dateiname muss über eine Erweiterung von verfügen `.slk`.

Hinweise

Das Speicher-Array, auf das Sie Laufwerke verschieben möchten, muss Laufwerke haben, die eine Kapazität aufweisen, die den Laufwerken entspricht oder größer ist als die Laufwerke, die Sie importieren.

Durch die Controller-Firmware wird eine Sperre erstellt, durch die der Zugriff auf vollständige Festplattenverschlüsselung (Full Disk Encryption, FDE) beschränkt wird. FDE-Laufwerke weisen einen Zustand auf, der als „Security-fähig“ bezeichnet wird. Wenn Sie einen Sicherheitsschlüssel erstellen, wird der Status auf „aktiviert“ gesetzt, was den Zugriff auf alle im Speicher-Array vorhandenen FDE-Laufwerke einschränkt.

Ihr Passphrase muss folgende Kriterien erfüllen:

- Muss zwischen acht und 32 Zeichen lang sein.
- Darf kein Leerzeichen enthalten.
- Muss mindestens einen Großbuchstaben enthalten.
- Muss mindestens einen Kleinbuchstaben enthalten.
- Muss mindestens eine Zahl enthalten.
- Muss mindestens ein nicht-alphanumerisches Zeichen enthalten, z. B. @ +.

Wenn Ihr Passphrase diese Kriterien nicht erfüllt, erhalten Sie eine Fehlermeldung und werden aufgefordert, den Befehl erneut zu versuchen.

Minimale Firmware-Stufe

7.40

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.