



# **Volumedaten mit NVE oder NAE verschlüsseln**

**ONTAP 9**

NetApp  
February 12, 2026

# Inhalt

- Volumedaten mit NVE oder NAE verschlüsseln. . . . . 1
  - Erfahren Sie mehr über die Verschlüsselung von ONTAP Volume-Daten mit NVE. . . . . 1
  - Aktivieren Sie die Verschlüsselung auf Aggregatebene mit VE-Lizenz in ONTAP. . . . . 1
  - Aktivieren Sie die Verschlüsselung auf einem neuen Volume in ONTAP . . . . . 3
  - Aktivieren Sie NAE oder NVE auf einem vorhandenen ONTAP -Volume . . . . . 4
    - Aktivieren Sie die Verschlüsselung auf einem vorhandenen Volume mit dem Befehl zur Konvertierung der Volume-Verschlüsselung . . . . . 4
    - Aktivieren Sie die Verschlüsselung auf einem vorhandenen Volume mit dem Befehl Volume move Start . . . . . 6
  - Konfigurieren Sie NVE auf einem ONTAP SVM-Root-Volume . . . . . 8
  - Konfigurieren Sie NVE auf einem ONTAP -Knoten-Root-Volume . . . . . 10

# Volumedaten mit NVE oder NAE verschlüsseln

## Erfahren Sie mehr über die Verschlüsselung von ONTAP Volume-Daten mit NVE

Ab ONTAP 9.7 ist die Aggregat- und Volume-Verschlüsselung standardmäßig aktiviert, wenn Sie über die VE-Lizenz und die integrierte oder externe Schlüsselverwaltung verfügen. Für ONTAP 9.6 und eine frühere Version können Sie die Verschlüsselung auf einem neuen Volume oder auf einem vorhandenen Volume aktivieren. Bevor Sie die Volume-Verschlüsselung aktivieren können, müssen Sie die VE-Lizenz und die aktivierte Schlüsselverwaltung installiert haben. NVE entspricht FIPS-140-2 Level 1.

## Aktivieren Sie die Verschlüsselung auf Aggregatebene mit VE-Lizenz in ONTAP

Ab ONTAP 9.7 sind neu erstellte Aggregate und Volumes standardmäßig verschlüsselt, wenn Sie über ["VE-Lizenz"](#) ein integriertes oder externes Verschlüsselungsmanagement verfügen. Ab ONTAP 9.6 können Sie mithilfe der Verschlüsselung auf Aggregatebene dem enthaltenden Aggregat Schlüssel zuweisen, damit die Volumes verschlüsselt werden können.

### Über diese Aufgabe

Wenn Sie eine Inline- oder eine Hintergrund-Deduplizierung auf Aggregatebene durchführen möchten, muss die Verschlüsselung auf Aggregatebene verwendet werden. Deduplizierung auf Aggregatebene wird ansonsten von NVE nicht unterstützt.

Ein Aggregat, das für die Verschlüsselung auf Aggregatebene aktiviert ist, wird als *NAE Aggregat* (für NetApp Aggregatverschlüsselung) bezeichnet. Alle Volumes in einem NAE-Aggregat müssen mit NAE- oder NVE-Verschlüsselung verschlüsselt sein. Bei der Verschlüsselung auf Aggregatebene werden die im Aggregat erstellten Volumes standardmäßig mit NAE-Verschlüsselung verschlüsselt. Sie können die Standardeinstellung für die Verwendung von NVE-Verschlüsselung überschreiben.

Klartextvolumen werden in NAE-Aggregaten nicht unterstützt.

### Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe auszuführen.

### Schritte

1. Aktivieren oder Deaktivieren der Verschlüsselung auf Aggregatebene:

An...	Befehl
Erstellen Sie ein NAE Aggregat mit ONTAP 9.7 oder höher	<pre>storage aggregate create -aggregate aggregate_name -node node_name</pre>

Erstellen Sie ein NAE-Aggregat mit ONTAP 9.6	<code>storage aggregate create -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true</code>
Konvertieren Sie ein nicht-NAE Aggregat in ein NAE Aggregat	<code>storage aggregate modify -aggregate aggregate_name -node node_name -encrypt-with -aggr-key true</code>
Konvertieren Sie ein NAE Aggregat in ein nicht-NAE Aggregat	<code>storage aggregate modify -aggregate aggregate_name -node node_name -encrypt-with -aggr-key false</code>

Erfahren Sie mehr über `storage aggregate modify` im ["ONTAP-Befehlsreferenz"](#).

Mit dem folgenden Befehl wird die Verschlüsselung auf Aggregatebene aktiviert `aggr1`:

- ONTAP 9.7 oder höher:

```
cluster1::> storage aggregate create -aggregate aggr1
```

- ONTAP 9.6 oder früher:

```
cluster1::> storage aggregate create -aggregate aggr1 -encrypt-with -aggr-key true
```

Erfahren Sie mehr über `storage aggregate create` in der ["ONTAP-Befehlsreferenz"](#).

## 2. Vergewissern Sie sich, dass das Aggregat für die Verschlüsselung aktiviert ist:

```
storage aggregate show -fields encrypt-with-aggr-key
```

Mit dem folgenden Befehl wird überprüft, ob die `aggr1` Verschlüsselung aktiviert ist:

```
cluster1::> storage aggregate show -fields encrypt-with-aggr-key
aggregate          encrypt-aggr-key
-----
aggr0_vsim4        false
aggr1               true
2 entries were displayed.
```

Erfahren Sie mehr über `storage aggregate show` in der ["ONTAP-Befehlsreferenz"](#).

## Nachdem Sie fertig sind

Führen Sie den `volume create` Befehl aus, um die verschlüsselten Volumes zu erstellen.

Wenn Sie einen KMIP-Server zum Speichern der Schlüssel für einen Node verwenden, sendet ONTAP bei der Verschlüsselung eines Volumes automatisch „schiebt“ einen Verschlüsselungsschlüssel an den Server.

## Aktivieren Sie die Verschlüsselung auf einem neuen Volume in ONTAP

Sie können die `volume create` Verschlüsselung für ein neues Volume mit dem Befehl aktivieren.

### Über diese Aufgabe

Sie können Volumes mit NetApp Volume Encryption (NVE) und ab ONTAP 9.6 mit NetApp Aggregate Encryption (NAE) verschlüsseln. Weitere Informationen zu NAE und NVE finden Sie im [Übersicht über Volume-Verschlüsselung](#).

Erfahren Sie mehr über die in diesem Verfahren beschriebenen Befehle im ["ONTAP-Befehlsreferenz"](#).

Das Verfahren zur Aktivierung der Verschlüsselung auf einem neuen Volume in ONTAP variiert abhängig von der verwendeten ONTAP Version und der spezifischen Konfiguration:

- Wenn Sie ab ONTAP 9.4 `cc-mode` beim Einrichten des integrierten Schlüsselmanagers aktivieren, `volume create` werden Volumes, die Sie mit dem Befehl erstellen, automatisch verschlüsselt, unabhängig davon, ob Sie angeben `-encrypt true`.
- In ONTAP 9.6 und früheren Versionen müssen Sie `-encrypt true` mit `volume create` Befehlen verwenden, um die Verschlüsselung zu aktivieren (vorausgesetzt, Sie haben nicht aktiviert `cc-mode`).
- Wenn Sie ein NAE-Volume in ONTAP 9.6 erstellen möchten, müssen Sie NAE auf Aggregatebene aktivieren. [Aktivieren Sie die Verschlüsselung auf Aggregatebene mit der VE-Lizenz](#) Weitere Informationen zu dieser Aufgabe finden Sie unter.
- Ab ONTAP 9.7 werden neu erstellte Volumes standardmäßig verschlüsselt, wenn Sie über das ["VE-Lizenz"](#) integrierte oder externe Verschlüsselungsmanagement verfügen. Standardmäßig sind neue Volumes, die in einem NAE-Aggregat erstellt werden, vom Typ NAE anstatt von NVE aus.
  - Wenn Sie in ONTAP 9.7 und neueren Versionen `-encrypt true` dem `volume create` Befehl hinzufügen, um ein Volume in einem NAE-Aggregat zu erstellen, erhält das Volume anstelle von NAE eine NVE-Verschlüsselung. Alle Volumes in einem NAE-Aggregat müssen entweder mit NVE oder NAE verschlüsselt sein.




Klartext-Volumes werden in NAE-Aggregaten nicht unterstützt.

### Schritte

1. Erstellen Sie ein neues Volume, und geben Sie an, ob die Verschlüsselung auf dem Volume aktiviert ist. Wenn das neue Volume sich in einem NAE-Aggregat befindet, ist das Volume standardmäßig ein NAE-Volume:

Zu erstellen...	Befehl
Ein NAE Volume	<pre>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name</pre>

Ein NVE Volume	<pre>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt true</pre> <div>  <p>In ONTAP 9.6 und früher, wo NAE nicht unterstützt wird, <code>-encrypt true</code> gibt an, dass das Volume mit NVE verschlüsselt werden soll. In ONTAP 9.7 und höher, wo Volumes in NAE-Aggregaten erstellt werden, <code>-encrypt true</code> setzt den Standardverschlüsselungstyp von NAE außer Kraft, um stattdessen ein NVE-Volume zu erstellen.</p> </div>
Nur-Text-Lautstärke	<pre>volume create -vserver SVM_name -volume volume_name -aggregate aggregate_name -encrypt false</pre>

Erfahren Sie mehr über `volume create` in der ["ONTAP-Befehlsreferenz"](#).

2. Vergewissern Sie sich, dass Volumes für die Verschlüsselung aktiviert sind:

```
volume show -is-encrypted true
```

Erfahren Sie mehr über `volume show` in der ["ONTAP-Befehlsreferenz"](#).

### Ergebnis

Wenn Sie einen KMIP-Server zum Speichern der Schlüssel für einen Node verwenden, „sendet“ ONTAP bei der Verschlüsselung eines Volumes automatisch einen Verschlüsselungsschlüssel an den Server.

## Aktivieren Sie NAE oder NVE auf einem vorhandenen ONTAP -Volume

Sie können die `volume move start volume encryption conversion start` Verschlüsselung für ein vorhandenes Volume mit dem Befehl oder mit dem Befehl aktivieren.

### Über diese Aufgabe

Sie können die `volume encryption conversion start` Befehl, um die Verschlüsselung eines vorhandenen Volumes direkt zu aktivieren, ohne das Volume an einen anderen Ort verschieben zu müssen. `volume move start` Befehl.

## Aktivieren Sie die Verschlüsselung auf einem vorhandenen Volume mit dem Befehl zur Konvertierung der Volume-Verschlüsselung

Sie können die `volume encryption conversion start` Befehl, um die Verschlüsselung eines vorhandenen Volumes „vor Ort“ zu aktivieren, ohne das Volume an einen anderen Speicherort verschieben zu müssen.

Nachdem Sie eine Konvertierung gestartet haben, muss diese abgeschlossen sein. Falls während des Vorgangs ein Performance-Problem auftritt, können Sie den `volume encryption conversion pause` Befehl ausführen, um den Vorgang anzuhalten, und den `volume encryption conversion resume` Befehl, um den Vorgang fortzusetzen.



Sie können nicht volume encryption conversion start zum Konvertieren eines SnapLock-Volumes verwenden.

## Schritte

1. Verschlüsselung auf einem vorhandenen Volume aktivieren:

```
volume encryption conversion start -vserver SVM_name -volume volume_name
```

Erfahren Sie mehr über volume encryption conversion start in der ["ONTAP-Befehlsreferenz"](#).

Mit dem folgenden Befehl wird die Verschlüsselung auf einem vorhandenen Volume aktiviert voll1:

```
cluster1::> volume encryption conversion start -vserver vs1 -volume voll1
```

Das System erstellt einen Verschlüsselungsschlüssel für das Volume. Die Daten auf dem Volume werden verschlüsselt.

2. Überprüfen Sie den Status des Konvertierungsvorgangs:

```
volume encryption conversion show
```

Erfahren Sie mehr über volume encryption conversion show in der ["ONTAP-Befehlsreferenz"](#).

Mit dem folgenden Befehl wird der Status des Konvertierungsvorgangs angezeigt:

```
cluster1::> volume encryption conversion show
```

Vserver	Volume	Start Time	Status
-----	-----	-----	-----
vs1	voll1	9/18/2017 17:51:41	Phase 2 of 2 is in progress.

3. Wenn der Konvertierungsvorgang abgeschlossen ist, überprüfen Sie, ob das Volume für die Verschlüsselung aktiviert ist:

```
volume show -is-encrypted true
```

Erfahren Sie mehr über volume show in der ["ONTAP-Befehlsreferenz"](#).

Der folgende Befehl zeigt die verschlüsselten Volumes an cluster1:

```
cluster1::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
-----	-----	-----	-----	-----	-----	-----	-----
vs1	voll1	aggr2	online	RW	200GB	160.0GB	20%

## Ergebnis

Wenn Sie einen KMIP-Server zum Speichern der Schlüssel für einen Node verwenden, sendet ONTAP bei der Verschlüsselung eines Volumes automatisch „schiebt“ einen Verschlüsselungsschlüssel an den Server.

## Aktivieren Sie die Verschlüsselung auf einem vorhandenen Volume mit dem Befehl `Volume move start`

Sie können die `volume move start` Verschlüsselung mit dem Befehl durch das Verschieben eines vorhandenen Volumes aktivieren. Sie können dasselbe oder ein anderes Aggregat verwenden.

### Über diese Aufgabe

- Ab ONTAP 9.8 können Sie `volume move start` die Verschlüsselung auf einem SnapLock oder FlexGroup Volume aktivieren.
- Wenn Sie ab ONTAP 9.4 „cc-Mode“ aktivieren, wenn Sie den integrierten Schlüsselmanager einrichten, `volume move start` werden die mit dem Befehl erstellten Volumes automatisch verschlüsselt. Sie müssen nicht angeben `-encrypt-destination true`.
- Ab ONTAP 9.6 können Sie mithilfe der Verschlüsselung auf Aggregatebene dem enthaltenden Aggregat Schlüssel zuweisen, damit die Volumes verschoben werden können. Ein mit einem eindeutigen Schlüssel verschlüsseltes Volume wird als „NVE Volume“ bezeichnet (d. h., es verwendet NetApp Volume Encryption). Ein mit einem Aggregatschlüssel verschlüsseltes Volume wird als NAE Volume (für NetApp Aggregate Encryption) bezeichnet. Klartext-Volumes werden in NAE-Aggregaten nicht unterstützt.
- Ab ONTAP 9.14.1 können Sie ein SVM Root-Volume mit NVE verschlüsseln. Weitere Informationen finden Sie unter [Konfiguration der NetApp-Volume-Verschlüsselung auf einem SVM-Root-Volume](#).

### Bevor Sie beginnen

Sie müssen ein Cluster-Administrator sein, um diese Aufgabe durchzuführen, oder ein SVM-Administrator, an den der Cluster-Administrator die Berechtigungen delegiert hat.

### ["Delegieren von Berechtigungen zum Ausführen des Befehls zum Verschieben von Volumes"](#)

### Schritte

1. Verschieben Sie ein vorhandenes Volume und geben Sie an, ob die Verschlüsselung auf dem Volume aktiviert ist:

Konvertieren...	Befehl
Ein Klartext-Volume auf ein NVE Volume	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true</code>
Ein NVE oder Klartext Volume auf ein NAE Volume (vorausgesetzt, die Verschlüsselung auf Aggregatebene ist auf dem Zielsystem aktiviert)	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true</code>
Ein NAE-Volume auf ein NVE Volume	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false</code>

Ein NAE Volume auf ein Klartext-Volume	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false</code>
Ein NVE Volume auf ein Klartext-Volume	<code>volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false</code>

Erfahren Sie mehr über `volume move start` in der ["ONTAP-Befehlsreferenz"](#).

Mit dem folgenden Befehl wird ein Klartext-Volume `vol1` mit dem Namen in ein NVE Volume konvertiert:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-destination true
```

Wenn die Verschlüsselung auf Aggregatebene auf dem Ziel aktiviert ist, konvertiert der folgende Befehl ein NVE- oder nur-Text- `vol1` Volume mit dem Namen in ein NAE-Volume:

```
cluster1::> volume move start -vserver vs1 -volume vol1 -destination
-aggregate aggr2 -encrypt-with-aggr-key true
```

Mit dem folgenden Befehl wird ein NAE-Volume `vol2` mit dem Namen in ein NVE Volume konvertiert:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-with-aggr-key false
```

Mit dem folgenden Befehl wird ein NAE-Volume `vol2` mit dem Namen in ein Klartext-Volume konvertiert:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false -encrypt-with-aggr-key false
```

Mit dem folgenden Befehl wird ein NVE Volume mit dem Namen `vol2` in ein Klartext-Volume konvertiert:

```
cluster1::> volume move start -vserver vs1 -volume vol2 -destination
-aggregate aggr2 -encrypt-destination false
```

## 2. Zeigen Sie den Verschlüsselungstyp von Cluster Volumes an:

```
volume show -fields encryption-type none|volume|aggregate
```

Das `encryption-type` Feld ist ab ONTAP 9.6 verfügbar.

Erfahren Sie mehr über `volume show` in der ["ONTAP-Befehlsreferenz"](#).

Der folgende Befehl zeigt den Verschlüsselungstyp von Volumes in an `cluster2`:

```
cluster2::> volume show -fields encryption-type
```

vserver	volume	encryption-type
-----	-----	-----
vs1	vol1	none
vs2	vol2	volume
vs3	vol3	aggregate

3. Vergewissern Sie sich, dass Volumes für die Verschlüsselung aktiviert sind:

```
volume show -is-encrypted true
```

Erfahren Sie mehr über `volume show` in der ["ONTAP-Befehlsreferenz"](#).

Der folgende Befehl zeigt die verschlüsselten Volumes an `cluster2`:

```
cluster2::> volume show -is-encrypted true
```

Vserver	Volume	Aggregate	State	Type	Size	Available	Used
-----	-----	-----	-----	-----	-----	-----	-----
vs1	vol1	aggr2	online	RW	200GB	160.0GB	20%

## Ergebnis

Wenn Sie einen KMIP-Server zur Speicherung der Verschlüsselungsschlüssel für einen Node verwenden, überträgt ONTAP bei der Verschlüsselung eines Volumes automatisch einen Verschlüsselungsschlüssel an den Server.

# Konfigurieren Sie NVE auf einem ONTAP SVM-Root-Volume

Ab ONTAP 9.14.1 können Sie die NetApp Volume Encryption (NVE) auf einem Storage VM (SVM) Root-Volume aktivieren. Mit NVE wird das Root-Volume mit einem eindeutigen Schlüssel verschlüsselt, was für mehr Sicherheit auf der SVM sorgt.

## Über diese Aufgabe

NVE auf einem SVM-Root-Volume kann nur aktiviert werden, nachdem die SVM erstellt wurde.

## Bevor Sie beginnen

- Das SVM-Root-Volume darf sich nicht auf einem mit der NetApp-Aggregatverschlüsselung (NAE) verschlüsselten Aggregat befinden.
- Sie müssen die Verschlüsselung mit dem Onboard Key Manager oder einem externen Schlüsselmanager aktiviert haben.

- Sie müssen ONTAP 9.14.1 oder höher ausführen.
- Um eine SVM, die ein mit NVE verschlüsseltes Root-Volume enthält, zu migrieren, müssen Sie das SVM-Root-Volume nach Abschluss der Migration in ein Klartextvolume konvertieren und anschließend das SVM-Root-Volume neu verschlüsseln.
  - Wenn das Zielaggregat der SVM Migration NAE verwendet, übernimmt das Root-Volume standardmäßig NAE.
- Wenn sich die SVM in einer SVM-Disaster-Recovery-Beziehung befindet:
  - Verschlüsselungseinstellungen auf einer gespiegelten SVM werden nicht an das Ziel kopiert. Wenn Sie NVE auf dem Quell- oder Zielsystem aktivieren, müssen Sie NVE auf dem gespiegelten SVM Root-Volume separat aktivieren.
  - Wenn alle Aggregate im Ziel-Cluster NAE verwenden, verwendet das SVM Root-Volume NAE.

## Schritte

Sie können NVE auf einem SVM Root-Volume mit der ONTAP CLI oder mit System Manager aktivieren.

### CLI

Sie können NVE auf dem Root-Volume der SVM aktivieren oder das Volume zwischen den Aggregaten verschieben.

#### Verschlüsseln Sie das Root-Volume

1. Konvertieren Sie das Root-Volume in ein verschlüsseltes Volume:

```
volume encryption conversion start -vserver svm_name -volume volume
```

2. Bestätigen Sie, dass die Verschlüsselung erfolgreich war. In `volume show -encryption-type volume` wird eine Liste aller Volumes mit NVE angezeigt.

#### Verschlüsseln Sie das SVM-Root-Volume durch Verschieben


1. Volume-Verschiebung initiieren:

```
volume move start -vserver svm_name -volume volume -destination-aggregate aggregate -encrypt-with-aggr-key false -encrypt-destination true
```

Erfahren Sie mehr über `volume move` in der ["ONTAP-Befehlsreferenz"](#).

2. Bestätigen Sie den `volume move` erfolgreichen Vorgang mit dem `volume move show` Befehl. In `volume show -encryption-type volume` wird eine Liste aller Volumes mit NVE angezeigt.

### System Manager

1. Navigieren Sie zu **Storage > Volumes**.
2. Wählen Sie neben dem Namen des SVM-Root-Volumes, das Sie verschlüsseln möchten,  dann **Bearbeiten**.
3. Wählen Sie unter der Überschrift **Speicherung und Optimierung** die Option **Verschlüsselung aktivieren**.
4. Wählen Sie **Speichern**.

# Konfigurieren Sie NVE auf einem ONTAP -Knoten-Root-Volume

Ab ONTAP 9.8 können Sie NetApp Volume Encryption zum Schutz des Root-Volumes des Nodes verwenden.



## Über diese Aufgabe

Dieses Verfahren gilt für das Root-Volume des Nodes. Sie gilt nicht für SVM-Root-Volumes. Root-Volumes der SVM können durch Verschlüsselung auf Aggregatebene gesichert werden, und [Ab ONTAP 9.14.1 ist NVE der Fall](#)

Sobald die Verschlüsselung des Root-Volumes beginnt, muss sie abgeschlossen sein. Sie können den Vorgang nicht unterbrechen. Nach Abschluss der Verschlüsselung können Sie dem Root-Volume keinen neuen Schlüssel zuweisen und keine sichere Löschung durchführen.

## Bevor Sie beginnen

- Ihr System muss eine HA-Konfiguration verwenden.
- Das Root-Volume des Nodes muss bereits erstellt werden.
- Ihr System muss über einen integrierten Schlüsselmanager oder einen externen Verschlüsselungsmanagement-Server mit dem Key Management Interoperability Protocol (KMIP) verfügen.

## Schritte

1. Verschlüsseln Sie das Root-Volume:

```
volume encryption conversion start -vserver SVM_name -volume root_vol_name
```

2. Überprüfen Sie den Status des Konvertierungsvorgangs:

```
volume encryption conversion show
```

3. Nach Abschluss des Konvertierungsvorgangs muss überprüft werden, ob das Volume verschlüsselt ist:

```
volume show -fields
```

Das folgende zeigt eine Beispielausgabe für ein verschlüsseltes Volume.

```
::> volume show -vserver xyz -volume vol0 -fields is-encrypted
vserver      volume is-encrypted
-----
xyz          vol0    true
```

## 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 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.