Volumendaten mit NVE oder NAE verschlüsseln

ONTAP 9

NetApp
November 10, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap/encryption-at-rest/encrypt-volumes-concept.html on November 10, 2026. Always check docs.netapp.com for the latest.

Inhalt

Volumendaten mit NVE oder NAE verschlüsseln . . . 1
- Informationen zur Verschlüsselung von ONTAP Volume-Daten mit NVE . . . 1
- Verschlüsselung auf Aggregatebene mit der VE-Lizenz in ONTAP aktivieren . . . 1
- Verschlüsselung auf einem neuen Volume in ONTAP aktivieren . . . 3
- NAE oder NVE auf einem vorhandenen ONTAP Volume aktivieren . . . 4
  - Die Verschlüsselung eines vorhandenen Volumes kann mit dem Befehl volume encryption conversion start aktiviert werden. . . . 4
  - Die Verschlüsselung auf einem vorhandenen Volume mit dem Befehl „volume move start“ aktivieren . . . 6
- Konfiguration von NVE auf einem ONTAP SVM Root-Volume . . . 8
- Konfiguration von NVE auf einem ONTAP Knoten-Root-Volume . . . 10

Volumendaten mit NVE oder NAE verschlüsseln

Informationen zur Verschlüsselung von ONTAP Volume-Daten mit NVE

Ab ONTAP 9.7 ist die Aggregat- und Volumenverschlüsselung standardmäßig aktiviert, wenn die VE-Lizenz sowie die integrierte oder externe Schlüsselverwaltung vorhanden sind. Für ONTAP 9.6 und frühere Versionen kann die Verschlüsselung auf einem neuen oder einem bestehenden Volume aktiviert werden. Die VE-Lizenz muss installiert und die Schlüsselverwaltung aktiviert sein, bevor die Volumenverschlüsselung aktiviert werden kann. NVE ist FIPS-140-2 Level 1-konform.

Verschlüsselung auf Aggregatebene mit der VE-Lizenz in ONTAP aktivieren

Ab ONTAP 9.7 werden neu erstellte Aggregate und Volumes standardmäßig verschlüsselt, wenn die "VE-Lizenz" sowie eine integrierte oder externe Schlüsselverwaltung vorhanden sind. Ab ONTAP 9.6 kann die Verschlüsselung auf Aggregatebene verwendet werden, um dem übergeordneten Aggregat Schlüssel für die zu verschlüsselnden Volumes zuzuweisen.

Über diese Aufgabe

Eine Verschlüsselung auf Aggregatebene ist erforderlich, wenn eine Inline- oder Hintergrunddeduplizierung auf Aggregatebene vorgesehen ist. Die Deduplizierung auf Aggregatebene wird ansonsten von NVE nicht unterstützt.

Ein für die Verschlüsselung auf Aggregatebene aktiviertes Aggregat wird als *NAE-Aggregat* (für NetApp Aggregate Encryption) bezeichnet. Alle Volumes in einem NAE-Aggregat müssen mit NAE- oder NVE-Verschlüsselung verschlüsselt sein. Bei der Verschlüsselung auf Aggregatebene werden Volumes, die Sie im Aggregat erstellen, standardmäßig mit NAE-Verschlüsselung verschlüsselt. Sie können die Standardeinstellung überschreiben, um stattdessen NVE-Verschlüsselung zu verwenden.

Plain-Text-Volumes werden in NAE Aggregaten nicht unterstützt.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können.

Schritte

1. Verschlüsselung auf Aggregatebene aktivieren oder deaktivieren:

Zu…	Verwenden Sie diesen Befehl…
Ein NAE Aggregat mit ONTAP 9.7 oder höher erstellen	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`*
Ein NAE Aggregat mit ONTAP 9.6 erstellen	`storage aggregate create -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`

Ein Nicht-NAE-Aggregat in ein NAE-Aggregat konvertieren	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key true`
Ein NAE-Aggregat in ein Nicht-NAE-Aggregat konvertieren	`storage aggregate modify -aggregate` *`aggregate_name`* `-node` *`node_name`* `-encrypt-with -aggr-key false`

Weitere Informationen zu `storage aggregate modify` finden sich in der "ONTAP-Befehlsreferenz".

Der folgende Befehl aktiviert die Verschlüsselung auf Aggregatebene für `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
```

Weitere Informationen zu `storage aggregate create` finden sich in der "ONTAP-Befehlsreferenz".

2. Überprüfen, ob das Aggregat für die Verschlüsselung aktiviert ist:

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

Der folgende Befehl überprüft, ob `aggr1` für die 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.
```

Weitere Informationen zu `storage aggregate show` finden sich in der "ONTAP-Befehlsreferenz".

Nachdem Sie fertig sind

Den `volume create` Befehl ausführen, um die verschlüsselten Volumes zu erstellen.

Wenn Sie einen KMIP-Server zum Speichern der Verschlüsselungsschlüssel für einen Knoten verwenden, sendet ONTAP beim Verschlüsseln eines Volumes automatisch einen Verschlüsselungsschlüssel an den Server.

Verschlüsselung auf einem neuen Volume in ONTAP aktivieren

Mit dem `volume create` Befehl lässt sich die Verschlüsselung auf einem neuen Volume aktivieren.

Über diese Aufgabe

Volumes lassen sich mit NetApp Volume Encryption (NVE) und ab ONTAP 9.6 mit NetApp Aggregate Encryption (NAE) verschlüsseln. Weitere Informationen zu NAE und NVE enthält die Übersicht zur Volumenverschlüsselung.

Weitere Informationen zu den in diesem Verfahren beschriebenen Befehlen befinden sich in der "ONTAP-Befehlsreferenz".

Die Vorgehensweise zum Aktivieren der Verschlüsselung auf einem neuen Volume in ONTAP variiert je nach verwendeter ONTAP-Version und Ihrer spezifischen Konfiguration:

- Ab ONTAP 9.4, wenn beim Einrichten des Onboard Key Managers `cc-mode` aktiviert wird, werden Volumes, die mit dem `volume create` Befehl erstellt werden, automatisch verschlüsselt, unabhängig davon, ob `-encrypt true` angegeben wird.
- In ONTAP 9.6 und früheren Versionen muss `-encrypt true` mit `volume create` Befehlen die Verschlüsselung aktiviert werden (sofern `cc-mode` nicht aktiviert wurde).
- Wenn in ONTAP 9.6 ein NAE-Volume erstellt werden soll, muss NAE auf Aggregatebene aktiviert werden. Weitere Details zu dieser Aufgabe sind unter Verschlüsselung auf Aggregatebene mit der VE-Lizenz aktivieren zu finden.
- Ab ONTAP 9.7 werden neu erstellte Volumes standardmäßig verschlüsselt, wenn die "VE-Lizenz" sowie eine integrierte oder externe Schlüsselverwaltung vorhanden sind. Standardmäßig sind neue Volumes, die in einem NAE Aggregat erstellt werden, vom Typ NAE statt NVE.
  - In ONTAP 9.7 und späteren Versionen, wenn `-encrypt true` zum `volume create`-Befehl hinzugefügt wird, um ein Volume in einem NAE-Aggregat zu erstellen, erhält das Volume NVE-Verschlüsselung anstelle von NAE. Alle Volumes in einem NAE-Aggregat müssen entweder mit NVE oder NAE verschlüsselt sein.

Klartext-Volumes werden in NAE Aggregaten nicht unterstützt.

Schritte

1. Ein neues Volume erstellen und angeben, ob die Verschlüsselung für das Volume aktiviert ist. Befindet sich das neue Volume in einem NAE Aggregat, ist das Volume standardmäßig ein NAE Volume:

Zum Erstellen…	Verwenden Sie diesen Befehl…
Ein NAE Volume	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`*

Ein NVE Volume	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt true` In ONTAP 9.6 und früher, wo NAE nicht unterstützt wird, `-encrypt true` gibt an, dass das Volume mit NVE verschlüsselt werden soll. In ONTAP 9.7 und später, wo Volumes in NAE Aggregaten erstellt werden, `-encrypt true` überschreibt den Standardverschlüsselungstyp von NAE, sodass stattdessen ein NVE Volume erstellt wird.
Ein einfaches Text-Volume	`volume create -vserver` *`SVM_name`* `-volume` *`volume_name`* `-aggregate` *`aggregate_name`* `-encrypt false`

Weitere Informationen zu `volume create` finden sich in der "ONTAP-Befehlsreferenz".

2. Überprüfen, ob Volumes für die Verschlüsselung aktiviert sind:

   `volume show -is-encrypted true`

   Weitere Informationen zu `volume show` finden sich in der "ONTAP-Befehlsreferenz".

Ergebnis

Wenn ein KMIP-Server zum Speichern der Verschlüsselungsschlüssel für einen Knoten verwendet wird, überträgt ONTAP automatisch einen Verschlüsselungsschlüssel an den Server, wenn ein Volume verschlüsselt wird.

NAE oder NVE auf einem vorhandenen ONTAP Volume aktivieren

Sie können entweder den `volume move start` oder den `volume encryption conversion start` Befehl verwenden, um die Verschlüsselung auf einem vorhandenen Volume zu aktivieren.

Über diese Aufgabe

Sie können den `volume encryption conversion start`Befehl verwenden, um die Verschlüsselung eines vorhandenen Volumes „an Ort und Stelle“ zu aktivieren, ohne das Volume an einen anderen Speicherort verschieben zu müssen. Alternativ kann der `volume move start` Befehl verwendet werden.

Die Verschlüsselung eines vorhandenen Volumes kann mit dem Befehl volume encryption conversion start aktiviert werden.

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

Nachdem Sie eine Konvertierungsoperation gestartet haben, muss diese abgeschlossen werden. Wenn während des Vorgangs Leistungsprobleme auftreten, kann der Vorgang mit dem `volume encryption conversion pause` Befehl angehalten und mit dem `volume encryption conversion resume` Befehl fortgesetzt werden.

Sie können `volume encryption conversion start`nicht verwenden, um ein SnapLock-Volumen zu konvertieren.

Schritte

1. Verschlüsselung für ein vorhandenes Volume aktivieren:

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

   Weitere Informationen zu `volume encryption conversion start` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl aktiviert die Verschlüsselung auf einem bestehenden Volume `vol1`:

   ```
   cluster1::> volume encryption conversion start -vserver vs1 -volume vol1
   ```

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

2. Status des Konvertierungsvorgangs überprüfen:

   `volume encryption conversion show`

   Weitere Informationen zu `volume encryption conversion show` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt den Status des Konvertierungsvorgangs an:

   ```
   cluster1::> volume encryption conversion show

   Vserver   Volume   Start Time           Status
   -------   ------   ------------------   --------------------------
   vs1       vol1     9/18/2017 17:51:41   Phase 2 of 2 is in progress.
   ```

3. Nach Abschluss der Konvertierung sollte überprüft werden, ob das Volume für die Verschlüsselung aktiviert ist:

   `volume show -is-encrypted true`

   Weitere Informationen zu `volume show` finden sich in der "ONTAP-Befehlsreferenz".

   Der folgende Befehl zeigt die verschlüsselten Volumes auf `cluster1` an:

   ```
   cluster1::> 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 zum Speichern der Verschlüsselungsschlüssel für einen Knoten verwenden, sendet ONTAP beim Verschlüsseln eines Volumes automatisch einen Verschlüsselungsschlüssel an den Server.

Die Verschlüsselung auf einem vorhandenen Volume mit dem Befehl „volume move start“ aktivieren

Sie können den `volume move start` Befehl verwenden, um die Verschlüsselung durch Verschieben eines vorhandenen Volumes zu aktivieren. Sie können dasselbe Aggregat oder ein anderes Aggregat verwenden.

Über diese Aufgabe

- Ab ONTAP 9.8 kann `volume move start` verwendet werden, um die Verschlüsselung auf einem SnapLock- oder FlexGroup-Volume zu aktivieren.
- Ab ONTAP 9.4 werden Volumes, die mit dem `volume move start` Befehl erstellt werden, automatisch verschlüsselt, wenn beim Einrichten des Onboard Key Managers der “cc-mode” aktiviert ist. Eine Angabe von `-encrypt-destination true` ist nicht erforderlich.
- Ab ONTAP 9.6 kann die Verschlüsselung auf Aggregatebene verwendet werden, um dem enthaltenen Aggregat für die zu verschiebenden Volumes Schlüssel zuzuweisen. Ein mit einem eindeutigen Schlüssel verschlüsseltes Volume wird als *NVE Volume* bezeichnet (das bedeutet, es verwendet NetApp Volume Encryption). Ein mit einem Schlüssel auf Aggregatebene verschlüsseltes Volume wird als *NAE Volume* bezeichnet (für NetApp Aggregate Encryption). Klartext-Volumes werden in NAE Aggregaten nicht unterstützt.
- Ab ONTAP 9.14.1 ist es möglich, ein SVM-Root-Volume mit NVE zu verschlüsseln. Weitere Informationen finden sich unter Konfiguration der NetApp Volume Encryption auf einem SVM Root-Volume.

Bevor Sie beginnen

Sie müssen Cluster-Administrator sein, um diese Aufgabe ausführen zu können, oder SVM-Administrator, dem der Cluster-Administrator die entsprechende Berechtigung delegiert hat.

"Delegierung der Berechtigung zum Ausführen des Volume Move-Befehls"

Schritte

1. Ein vorhandenes Volume verschieben und angeben, ob die Verschlüsselung für das Volume aktiviert ist:

Zum Umwandeln…	Verwenden Sie diesen Befehl…
Ein Klartext-Volume zu einem NVE-Volume	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination true`
Ein NVE- oder Klartext-Volume zu einem NAE-Volume (vorausgesetzt, die Verschlüsselung auf Aggregatebene ist auf dem Ziel aktiviert)	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key true`
Ein NAE Volume zu einem NVE Volume	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-with-aggr-key false`

Ein NAE Volume zu einem Klartext Volume	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false -encrypt-with-aggr-key false`
Ein NVE Volume zu einem Klartext Volume	`volume move start -vserver SVM_name -volume volume_name -destination-aggregate aggregate_name -encrypt-destination false`

Weitere Informationen zu `volume move start` finden sich in der "ONTAP-Befehlsreferenz".

Der folgende Befehl konvertiert ein Klartext-Volume mit dem Namen `vol1` zu einem NVE-Volume:

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

Unter der Annahme, dass die Verschlüsselung auf Aggregatebene auf dem Zielsystem aktiviert ist, konvertiert der folgende Befehl ein NVE- oder Klartext-Volume mit dem Namen `vol1` in ein NAE-Volume:

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

Der folgende Befehl konvertiert ein NAE-Volume mit dem Namen `vol2` zu einem NVE-Volume:

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

Der folgende Befehl konvertiert ein NAE-Volume mit dem Namen `vol2` in ein Klartext-Volume:

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

Der folgende Befehl konvertiert ein NVE-Volume mit dem Namen `vol2` in ein Klartext-Volume:

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

2. Den Verschlüsselungstyp der Cluster-Volumes anzeigen:

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

   Das `encryption-type` Feld ist in ONTAP 9.6 und späteren Versionen verfügbar.

Weitere Informationen zu `volume show` finden sich in der "ONTAP-Befehlsreferenz".

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

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

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

3. Überprüfen, ob Volumes für die Verschlüsselung aktiviert sind:

   `volume show -is-encrypted true`

   Weitere Informationen zu `volume show` finden sich in der "ONTAP-Befehlsreferenz".

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

```
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 ein KMIP-Server zum Speichern der Verschlüsselungsschlüssel für einen Knoten verwendet wird, überträgt ONTAP automatisch einen Verschlüsselungsschlüssel an den Server, wenn ein Volume verschlüsselt wird.

Konfiguration von NVE auf einem ONTAP SVM Root-Volume

Ab ONTAP 9.14.1 kann die NetApp Volume Encryption (NVE) auf einem Storage-VM (SVM) Root-Volume aktiviert werden. Mit NVE wird das Root-Volume mit einem eindeutigen Schlüssel verschlüsselt, was eine höhere Sicherheit auf der SVM ermöglicht.

Über diese Aufgabe

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

Bevor Sie beginnen

- Das SVM-Root-Volume darf sich nicht auf einem mit NetApp Aggregate Encryption (NAE) verschlüsselten Aggregat befinden.
- Die Verschlüsselung muss mit dem Onboard Key Manager oder einem externen Key Manager aktiviert sein.

- ONTAP 9.14.1 oder höher muss ausgeführt werden.
- Um eine SVM mit einem mit NVE verschlüsselten Root-Volume zu migrieren, muss das SVM-Root-Volume nach Abschluss der Migration in ein Klartext-Volume konvertiert und anschließend das SVM-Root-Volume erneut verschlüsselt werden.
  - 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:
  - Die Verschlüsselungseinstellungen einer gespiegelten SVM werden nicht auf das Ziel kopiert. Wenn NVE auf dem Quell- oder Zielsystem aktiviert wird, muss NVE separat auf dem Root-Volume der gespiegelten SVM aktiviert werden.
  - Wenn alle Aggregate im Ziel-Cluster NAE verwenden, verwendet das SVM-Root-Volume ebenfalls NAE.

Schritte

NVE kann auf einem SVM-Root-Volume mit der ONTAP CLI oder dem System Manager aktiviert werden.

CLI

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

Das Root-Volume wird direkt verschlüsselt.

1. Das Root-Volume in ein verschlüsseltes Volume umwandeln:

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

2. Bestätigen Sie, dass die Verschlüsselung erfolgreich war. Der `volume show -encryption-type volume`zeigt eine Liste aller Volumes an, die NVE verwenden.

Das SVM-Root-Volume durch Verschieben verschlüsseln

1. Eine Volumenverschiebung initiieren:

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

   Weitere Informationen zu `volume move` finden sich in der "ONTAP-Befehlsreferenz".

2. Der erfolgreiche Abschluss des `volume move`Vorgangs kann mit dem `volume move show`Befehl bestätigt werden. Der `volume show -encryption-type volume`zeigt eine Liste aller Volumes an, die NVE verwenden.

System Manager

1. Zu **Speicher** > **Volumes** navigieren.
2. Neben dem Namen des SVM-Root-Volumes, das Sie verschlüsseln möchten, ⋮ dann **Bearbeiten** auswählen.
3. Unter der Überschrift **Speicherung und Optimierung** die Option **Verschlüsselung aktivieren** auswählen.
4. **Speichern** auswählen.

Konfiguration von NVE auf einem ONTAP Knoten-Root-Volume

Ab ONTAP 9.8 kann die NetApp Volume Encryption verwendet werden, um das Root-Volume eines Knotens zu schützen.

Über diese Aufgabe

Dieses Verfahren gilt für das Knoten-Root-Volume. Es gilt nicht für SVM-Root-Volumes. SVM-Root-Volumes können durch Verschlüsselung auf Aggregatebene geschützt werden und beginnend mit ONTAP 9.14.1, NVE.

Sobald die Verschlüsselung des Root-Volumes beginnt, muss sie abgeschlossen werden. Der Vorgang kann nicht pausiert werden. Nach Abschluss der Verschlüsselung kann dem Root-Volume kein neuer Schlüssel zugewiesen werden und eine sichere Löschung kann nicht durchgeführt werden.

Bevor Sie beginnen

- Ihr System muss eine HA Konfiguration verwenden.
- Ihr Node Root-Volume muss bereits erstellt sein.
- Ihr System muss über einen integrierten Schlüsselmanager oder einen externen Schlüsselverwaltungsserver verfügen, der das Key Management Interoperability Protocol (KMIP) verwendet.

Schritte

1. Das Root-Volume verschlüsseln:

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

2. Status des Konvertierungsvorgangs überprüfen:

   ```
   volume encryption conversion show
   ```

3. Nach Abschluss der Konvertierung kann überprüft werden, ob das Volume verschlüsselt ist:

   ```
   volume show -fields
   ```

   Nachfolgend wird eine Beispielausgabe für ein verschlüsseltes Volume gezeigt.

   ```
   ::> 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 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.