



# **Bootmedium – manuelle Wiederherstellung**

Install and maintain

NetApp

January 09, 2026

# Inhalt

Bootmedium – manuelle Wiederherstellung .....	1
Workflow zur manuellen Wiederherstellung des Bootmediums – FAS2800 .....	1
Voraussetzungen für die manuelle Wiederherstellung von Bootmedien – AFF A800 .....	2
Prüfen Sie Support und Status der Verschlüsselungsschlüssel - FAS2820 .....	2
Schritt 1: NVE-Unterstützung prüfen und das richtige ONTAP Image herunterladen .....	3
Schritt 2: Überprüfen Sie den Status des Schlüsselmanagers und sichern Sie die Konfiguration.....	3
Fahren Sie den Controller für die manuelle Wiederherstellung des Startmediums herunter – FAS2820 .....	7
Ersetzen Sie das Startmedium und bereiten Sie die manuelle Startwiederherstellung vor – FAS2820 .....	7
Schritt 1: Entfernen Sie das Controller-Modul .....	8
Schritt 2: Ersetzen Sie die Startmedien .....	9
Schritt 3: Übertragen Sie das Startabbild auf das Startmedium .....	10
Manuelle Wiederherstellung eines Bootmediums von einem USB-Laufwerk – FAS2820 .....	11
Wiederherstellung der Verschlüsselung – FAS2820 .....	14
Senden Sie das fehlerhafte Bootmedium an NetApp - FAS2820 zurück.....	24

# Bootmedium – manuelle Wiederherstellung

## Workflow zur manuellen Wiederherstellung des Bootmediums – FAS2800

Beginnen Sie mit dem Ersetzen des Startmediums in Ihrem FAS2800-Speichersystem, indem Sie die Anforderungen für den Austausch überprüfen, den Verschlüsselungsstatus prüfen, den Controller herunterfahren, das Startmedium ersetzen, das Wiederherstellungsimage starten, die Verschlüsselung wiederherstellen und die Systemfunktionalität überprüfen.

Wenn Ihr Speichersystem ONTAP 9.17.1 oder höher ausführt, verwenden Sie die ["automatisiertes Boot-Wiederherstellungsverfahren"](#). Wenn auf Ihrem System eine frühere Version von ONTAP ausgeführt wird, müssen Sie das manuelle Boot-Wiederherstellungsverfahren verwenden.

1

### "Überprüfen Sie die Anforderungen der Startmedien"

Überprüfen Sie die Anforderungen für den Austausch des Startmediums.

2

### "Prüfen Sie die Unterstützung und den Status der Verschlüsselungsschlüssel"

Prüfen Sie, ob der Sicherheitsschlüsselmanager aktiviert oder die Laufwerke verschlüsselt sind.

3

### "Fahren Sie den Controller herunter"

Fahren Sie den Controller herunter, wenn Sie die Boot-Medien austauschen müssen.

4

### "Ersetzen Sie das Startmedium"

Entfernen Sie das fehlerhafte Startmedium aus dem Systemverwaltungsmodul, installieren Sie das Ersatz-Startmedium, und übertragen Sie dann ein ONTAP-Image mithilfe eines USB-Flashlaufwerks.

5

### "Starten Sie das Recovery-Image"

Starten Sie das ONTAP-Image vom USB-Laufwerk, stellen Sie das Dateisystem wieder her und überprüfen Sie die Umgebungsvariablen.

6

### "Wiederherstellung der Verschlüsselung"

Stellen Sie die Konfiguration des integrierten Schlüsselmanagers oder des externen Schlüsselmanagers über das ONATP Startmenü wieder her.

7

### "Senden Sie das fehlerhafte Teil an NetApp zurück"

Senden Sie das fehlerhafte Teil wie in den dem Kit beiliegenden RMA-Anweisungen beschrieben an NetApp

zurück.

## Voraussetzungen für die manuelle Wiederherstellung von Bootmedien – AFF A800

Stellen Sie vor dem Austausch des Bootmediums in Ihrem AFF A800 System sicher, dass Sie die notwendigen Voraussetzungen für einen erfolgreichen Austausch erfüllen. Stellen Sie dazu sicher, dass Sie über einen USB-Stick mit ausreichend Speicherplatz verfügen und dass Sie das richtige Ersatz-Bootmedium verwenden.

Wenn Ihr Speichersystem ONTAP 9.17.1 oder höher ausführt, verwenden Sie die ["automatisiertes Boot-Wiederherstellungsverfahren"](#). Wenn auf Ihrem System eine frühere Version von ONTAP ausgeführt wird, müssen Sie das manuelle Boot-Wiederherstellungsverfahren verwenden.

### USB-Speicherstick

- Stellen Sie sicher, dass Sie einen USB-Stick haben, der auf FAT32 formatiert ist.
- Der USB-Stick muss über ausreichend Speicherkapazität verfügen, um die `image_XXX.tgz` Datei.

### Dateivorbereitung

Kopieren Sie die `image_XXX.tgz` Datei auf den USB-Stick. Diese Datei wird verwendet, wenn Sie das ONTAP Image mit dem USB-Stick übertragen.

### Komponentenaustausch

Ersetzen Sie die ausgefallene Komponente durch die von NetApp bereitgestellte Ersatzkomponente.

### Controller-Identifikation

Es ist wichtig, die Befehle auf den richtigen Controller anzuwenden, wenn Sie das beschädigte Startmedium ersetzen:

- Der *beschädigte Controller* ist der Controller, an dem Sie Wartungsarbeiten durchführen.
- Der *gesunde Controller* ist der HA-Partner des beeinträchtigten Controllers.

### Was kommt als Nächstes?

Nachdem Sie die Anforderungen für den Austausch des Boot-Mediums überprüft haben, müssen Sie ["Prüfen Sie die Unterstützung und den Status der Verschlüsselungsschlüssel auf dem Startmedium"](#).

## Prüfen Sie Support und Status der Verschlüsselungsschlüssel - FAS2820

Um die Datensicherheit auf Ihrem Speichersystem zu gewährleisten, müssen Sie die Unterstützung und den Status des Verschlüsselungsschlüssels auf Ihrem Boot-Medium überprüfen. Überprüfen Sie, ob Ihre ONTAP Version NetApp Volume Encryption (NVE) unterstützt und bevor Sie den Controller herunterfahren, ob der Schlüsselmanager aktiv ist.

Wenn Ihr Speichersystem ONTAP 9.17.1 oder höher ausführt, verwenden Sie die ["automatisiertes Boot-Wiederherstellungsverfahren"](#). Wenn auf Ihrem System eine frühere Version von ONTAP ausgeführt wird, müssen Sie den manuellen Boot-Wiederherstellungsprozess verwenden.

## Schritt 1: NVE-Unterstützung prüfen und das richtige ONTAP Image herunterladen

Prüfen Sie, ob Ihre ONTAP Version NetApp Volume Encryption (NVE) unterstützt, damit Sie das richtige ONTAP Image für den Austausch des Bootmediums herunterladen können.

### Schritte

1. Prüfen Sie, ob Ihre ONTAP Version Verschlüsselung unterstützt:

```
version -v
```

Wenn die Ausgabe enthält `1Ono-DARE`, wird NVE auf Ihrer Cluster-Version nicht unterstützt.

2. Laden Sie das passende ONTAP Image basierend auf der NVE-Unterstützung herunter:
  - Wenn NVE unterstützt wird: Laden Sie das ONTAP Image mit NetApp Volume Encryption herunter.
  - Falls NVE nicht unterstützt wird: Laden Sie das ONTAP Image ohne NetApp Volume Encryption herunter.



Laden Sie das ONTAP Image von der NetApp -Support-Website auf Ihren HTTP- oder FTP-Server oder in einen lokalen Ordner herunter. Sie benötigen diese Image-Datei während des Austauschs des Startmediums.

## Schritt 2: Überprüfen Sie den Status des Schlüsselmanagers und sichern Sie die Konfiguration.

Bevor Sie den betroffenen Controller herunterfahren, überprüfen Sie die Konfiguration des Schlüsselmanagers und sichern Sie die notwendigen Informationen.

### Schritte

1. Bestimmen Sie, welcher Schlüsselmanager auf Ihrem System aktiviert ist:

ONTAP-Version	Führen Sie diesen Befehl aus
ONTAP 9.14.1 oder höher	<pre>security key-manager keystore show</pre> <ul style="list-style-type: none"><li>• Wenn EKM aktiviert ist, EKM wird in der Befehlsausgabe aufgelistet.</li><li>• Wenn OKM aktiviert ist, OKM wird in der Befehlsausgabe aufgelistet.</li><li>• Wenn kein Schlüsselmanager aktiviert ist, <code>No key manager keystores configured</code> wird in der Befehlsausgabe aufgeführt.</li></ul>

ONTAP-Version	Führen Sie diesen Befehl aus
ONTAP 9.13.1 oder früher	<pre>security key-manager show-key-store</pre> <ul style="list-style-type: none"> <li>• Wenn EKM aktiviert ist, <code>external</code> wird in der Befehlsausgabe aufgelistet.</li> <li>• Wenn OKM aktiviert ist, <code>onboard</code> wird in der Befehlsausgabe aufgelistet.</li> <li>• Wenn kein Schlüsselmanager aktiviert ist, <code>No key managers configured</code> wird in der Befehlsausgabe aufgeführt.</li> </ul>

2. Je nachdem, ob auf Ihrem System ein Schlüsselmanager konfiguriert ist, führen Sie einen der folgenden Schritte aus:

**Falls kein Schlüsselmanager konfiguriert ist:**

Sie können den defekten Controller gefahrlos herunterfahren und mit dem Herunterfahrvorgang fortfahren.

**Wenn ein Schlüsselmanager (EKM oder OKM) konfiguriert ist:**

- a. Geben Sie den folgenden Abfragebefehl ein, um den Status der Authentifizierungsschlüssel in Ihrem Schlüsselmanager anzuzeigen:

```
security key-manager key query
```

- b. Überprüfen Sie die Ausgabe und den Wert im `Restored` Spalte. Diese Spalte zeigt an, ob die Authentifizierungsschlüssel für Ihren Schlüsselmanager (entweder EKM oder OKM) erfolgreich wiederhergestellt wurden.

3. Führen Sie das entsprechende Verfahren entsprechend Ihrem Schlüsselmanagertyp durch:

### Externer Schlüsselmanager (EKM)

Führen Sie diese Schritte anhand des Wertes im `Restored` Spalte.

#### Wenn alle Tasten angezeigt werden `true` in der Spalte „Wiederhergestellt“:

Sie können den defekten Controller gefahrlos herunterfahren und mit dem Herunterfahrvorgang fortfahren.

#### Wenn ein Schlüssel einen anderen Wert als `true` in der Spalte „Wiederhergestellt“:

- a. Stellen Sie die Authentifizierungsschlüssel für die externe Schlüsselverwaltung auf allen Knoten im Cluster wieder her:

```
security key-manager external restore
```

Falls der Befehl fehlschlägt, wenden Sie sich an den NetApp -Support.

- b. Überprüfen Sie, ob alle Authentifizierungsschlüssel wiederhergestellt wurden:

```
security key-manager key query
```

Bestätigen Sie, dass die `Restored` Spaltenanzeigen `true` für alle Authentifizierungsschlüssel.

- c. Sind alle Schlüssel wiederhergestellt, können Sie den betroffenen Controller sicher herunterfahren und mit dem Herunterfahrvorgang fortfahren.

### Onboard Key Manager (OKM)

Führen Sie diese Schritte anhand des Wertes im `Restored` Spalte.

#### Wenn alle Tasten angezeigt werden `true` in der Spalte „Wiederhergestellt“:

- a. Sichern Sie die OKM-Informationen:

- i. In den erweiterten Berechtigungsmodus wechseln:

```
set -priv advanced
```

Eingeben `y` wenn er zur Fortsetzung aufgefordert wird.

- i. Informationen zur Schlüsselverwaltung und Datensicherung anzeigen:

```
security key-manager onboard show-backup
```

- ii. Kopieren Sie die Sicherungsinformationen in eine separate Datei oder Ihre Protokolldatei.

Sie benötigen diese Sicherungsinformationen, falls Sie OKM während des Austauschvorgangs manuell wiederherstellen müssen.

- iii. Zurück zum Administratormodus:

```
set -priv admin
```

- b. Sie können den defekten Controller gefahrlos herunterfahren und mit dem Herunterfahrenvorgang fortfahren.

**Wenn ein Schlüssel einen anderen Wert als `true` in der Spalte „Wiederhergestellt“:**

- a. Synchronisieren Sie den integrierten Schlüsselmanager:

```
security key-manager onboard sync
```

Geben Sie bei Aufforderung die 32-stellige alphanumerische Passphrase für die Onboard-Schlüsselverwaltung ein.



Dies ist die clusterweite Passphrase, die Sie bei der Erstkonfiguration des Onboard Key Managers erstellt haben. Falls Sie diese Passphrase nicht haben, wenden Sie sich bitte an den NetApp -Support.

- b. Überprüfen Sie, ob alle Authentifizierungsschlüssel wiederhergestellt wurden:

```
security key-manager key query
```

Bestätigen Sie, dass die `Restored` Spaltenanzeigen `true` für alle Authentifizierungsschlüssel und die `Key Manager Typ` zeigt `onboard` Die

- c. Sichern Sie die OKM-Informationen:

- i. In den erweiterten Berechtigungsmodus wechseln:

```
set -priv advanced
```

Eingeben `y` wenn er zur Fortsetzung aufgefordert wird.

- i. Informationen zur Schlüsselverwaltung und Datensicherung anzeigen:

```
security key-manager onboard show-backup
```

- ii. Kopieren Sie die Sicherungsinformationen in eine separate Datei oder Ihre Protokolldatei.

Sie benötigen diese Sicherungsinformationen, falls Sie OKM während des Austauschvorgangs manuell wiederherstellen müssen.

- iii. Zurück zum Administratormodus:

```
set -priv admin
```

- d. Sie können den defekten Controller gefahrlos herunterfahren und mit dem Herunterfahrenvorgang fortfahren.

**Was kommt als Nächstes?**

Nachdem Sie die Unterstützung und den Status der Verschlüsselungsschlüssel auf dem Boot-Medium überprüft haben, müssen Sie ["Fahren Sie den Controller herunter"](#).



# Fahren Sie den Controller für die manuelle Wiederherstellung des Startmediums herunter – FAS2820

Schalten Sie den außer Betrieb genommenen Controller aus oder übernehmen Sie ihn.

Wenn Ihr Speichersystem ONTAP 9.17.1 oder höher ausführt, verwenden Sie die ["automatisiertes Boot-Wiederherstellungsverfahren"](#). Wenn auf Ihrem System eine frühere Version von ONTAP ausgeführt wird, müssen Sie das manuelle Boot-Wiederherstellungsverfahren verwenden.

Nach Abschluss der NVE oder NSE-Aufgaben müssen Sie den Shutdown des beeinträchtigten Controllers durchführen.

## Schritte

1. Nehmen Sie den beeinträchtigten Controller zur LOADER-Eingabeaufforderung:

Wenn der eingeschränkte Controller angezeigt wird...	Dann...
Die LOADER-Eingabeaufforderung	Wechseln Sie zu Controller-Modul entfernen.
Waiting for giveback...	Drücken Sie Strg-C, und antworten Sie dann <code>y</code> Wenn Sie dazu aufgefordert werden.
Eingabeaufforderung des Systems oder Passwort (Systempasswort eingeben)	Übernehmen oder stoppen Sie den beeinträchtigten Regler von der gesunden Steuerung: <code>storage failover takeover -ofnode impaired_node_name</code>  Wenn der Regler „beeinträchtigt“ auf Zurückgeben wartet... anzeigt, drücken Sie Strg-C, und antworten Sie dann <code>y</code> .

2. Geben Sie an der LOADER-Eingabeaufforderung Folgendes ein: `printenv` Um alle Boot-Umgebungsvariablen zu erfassen. Speichern Sie die Ausgabe in Ihrer Protokolldatei.



Dieser Befehl funktioniert möglicherweise nicht, wenn das Startgerät beschädigt oder nicht funktionsfähig ist.

## Was kommt als Nächstes?

Nach dem Herunterfahren des Controllers müssen Sie ["Ersetzen Sie das Startmedium"](#).

# Ersetzen Sie das Startmedium und bereiten Sie die manuelle Startwiederherstellung vor – FAS2820

Sie müssen das beschädigte Controllermodul entfernen und öffnen, das Bootmedium im Controller suchen und ersetzen, das Boot-Image auf ein USB-Laufwerk übertragen, das USB-Laufwerk in den Controller einstecken und dann den Controller booten.

Wenn Ihr Speichersystem ONTAP 9.17.1 oder höher ausführt, verwenden Sie die ["automatisiertes Boot-](#)

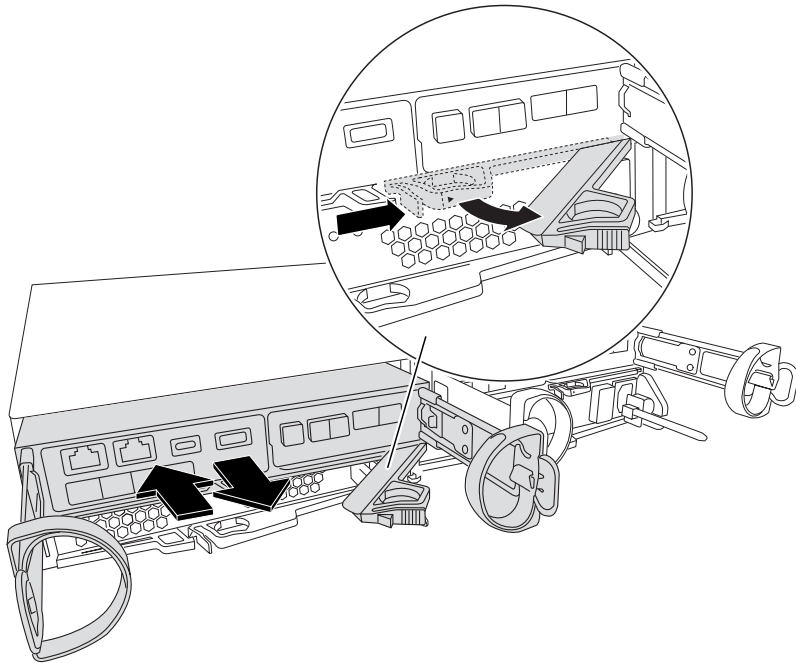
[Wiederherstellungsverfahren](#)" . Wenn auf Ihrem System eine frühere Version von ONTAP ausgeführt wird, müssen Sie das manuelle Boot-Wiederherstellungsverfahren verwenden.

## Schritt 1: Entfernen Sie das Controller-Modul

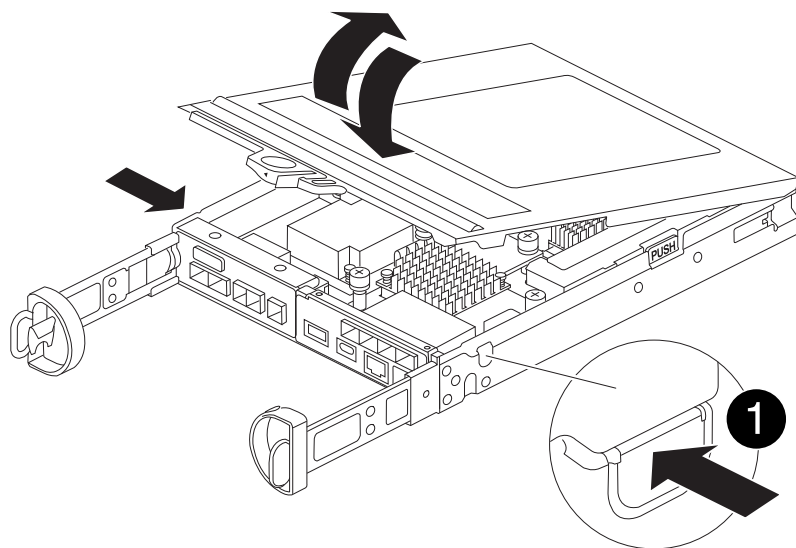
### Schritte

Um auf Komponenten innerhalb des Controllers zuzugreifen, müssen Sie zuerst das Controller-Modul aus dem System entfernen und dann die Abdeckung am Controller-Modul entfernen.

1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
2. Lösen Sie den Haken- und Schlaufenriemen, mit dem die Kabel am Kabelführungsgerät befestigt sind, und ziehen Sie dann die Systemkabel und SFPs (falls erforderlich) vom Controller-Modul ab, um zu verfolgen, wo die Kabel angeschlossen waren.
3. Drücken Sie die Verriegelung am Nockengriff, bis sie loslässt, öffnen Sie den Nockengriff vollständig, um das Controller-Modul aus der Mittelplatine zu lösen, und ziehen Sie das Controller-Modul anschließend mit zwei Händen aus dem Gehäuse heraus.



4. Drehen Sie das Controller-Modul um und legen Sie es auf eine flache, stabile Oberfläche.
5. Öffnen Sie die Abdeckung, indem Sie die blauen Tasten an den Seiten des Controller-Moduls drücken, um die Abdeckung zu lösen, und drehen Sie dann die Abdeckung nach oben und von dem Controller-Modul.

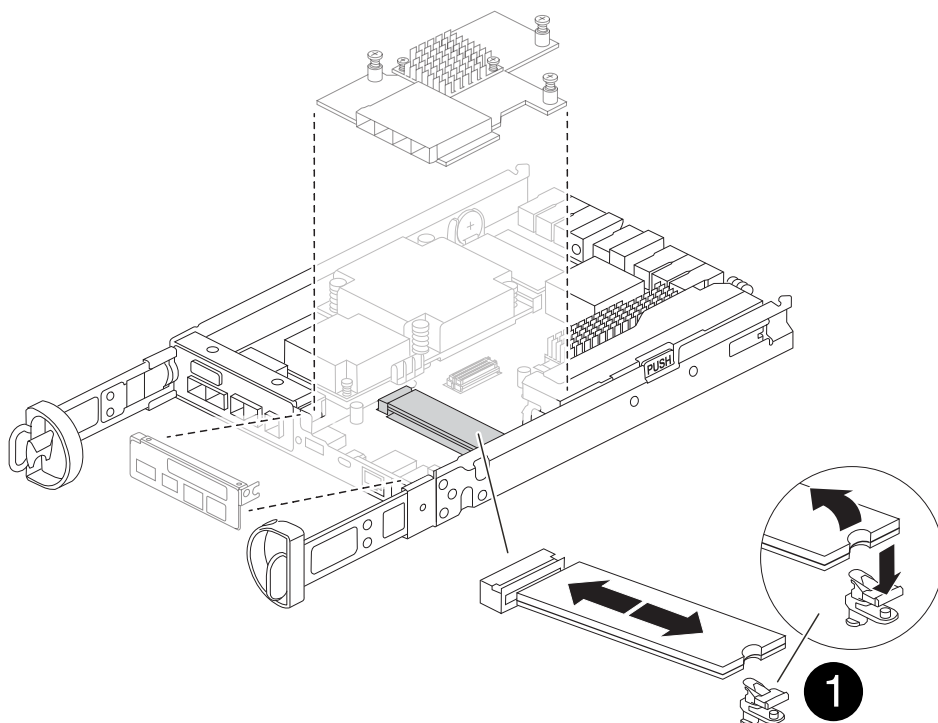


1

Entriegelungstaste der Steuermodulabdeckung

## Schritt 2: Ersetzen Sie die Startmedien

Suchen Sie die Startmedien im Controller-Modul unter der Zusatzkarte, und befolgen Sie die Anweisungen zum Austauschen.



1

Verriegelungslasche für Startmedien

### Schritte

1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.

2. Entfernen Sie die Mezzanine-Karte mithilfe der folgenden Abbildung oder der FRU-Zuordnung auf dem Controller-Modul:

- a. Entfernen Sie die E/A-Platte, indem Sie sie gerade aus dem Controller-Modul herauschieben.
- b. Lösen Sie die Rändelschrauben auf der Zusatzkarte.



Sie können die Rändelschrauben mit den Fingern oder einem Schraubendreher lösen. Wenn Sie Ihre Finger verwenden, müssen Sie den NV-Akku möglicherweise nach oben drehen, um den Finger besser an der Daumenschraube daneben zu kaufen.

- c. Heben Sie die Zusatzkarte gerade nach oben.

3. Ersetzen Sie die Startmedien:

- a. Drücken Sie die blaue Taste am Startmediengehäuse, um die Startmedien aus dem Gehäuse zu lösen, drehen Sie die Startmedien nach oben und ziehen Sie sie dann vorsichtig gerade aus dem Startmediensockel.



Drehen oder ziehen Sie die Boot-Medien nicht gerade nach oben, da dadurch der Sockel oder das Boot-Medium beschädigt werden kann.

- b. Richten Sie die Kanten des Ersatzstartmediums an der Buchse des Boot-Mediums aus, und schieben Sie ihn dann vorsichtig in die Buchse. Überprüfen Sie die Startmedien, um sicherzustellen, dass sie korrekt und vollständig in den Sockel eingesetzt sind. Entfernen Sie gegebenenfalls die Startmedien, und setzen Sie sie wieder in den Sockel ein.

- c. Drücken Sie die blaue Verriegelungstaste, drehen Sie das Startmedium ganz nach unten, und lassen Sie dann die Verriegelungstaste los, um das Startmedium zu verriegeln.

4. Setzen Sie die Zusatzkarte wieder ein:

- a. Richten Sie den Sockel auf der Hauptplatine mit dem Sockel auf der Zusatzkarte aus, und setzen Sie die Karte vorsichtig in den Sockel ein.
- b. Ziehen Sie die drei Rändelschrauben auf der Zusatzkarte fest.
- c. Setzen Sie die E/A-Platte wieder ein.

5. Setzen Sie die Abdeckung des Controller-Moduls wieder ein, und verriegeln Sie sie.

### Schritt 3: Übertragen Sie das Startabbild auf das Startmedium

Installieren Sie das System-Image auf dem Ersatz-Startmedium mit einem USB-Flash-Laufwerk, auf dem das Image installiert ist. Während dieses Vorgangs müssen Sie das var-Dateisystem wiederherstellen.

#### Bevor Sie beginnen

- Sie benötigen ein USB-Flash-Laufwerk, das mit MBR/FAT32 formatiert ist, mit mindestens 4 GB Kapazität.
- Sie müssen über eine Netzwerkverbindung verfügen.

#### Schritte

1. Laden Sie die entsprechende Bildversion von ONTAP auf das formatierte USB-Flash-Laufwerk herunter:

- a. Nutzung "[So stellen Sie fest, ob die laufende ONTAP-Version NetApp Volume Encryption \(NVE\) unterstützt](#)" Um festzustellen, ob die Volume-Verschlüsselung derzeit unterstützt wird.

- Wenn NVE auf dem Cluster unterstützt wird, laden Sie das Image mit NetApp Volume Encryption herunter.

- Wenn NVE nicht auf dem Cluster unterstützt wird, laden Sie das Image ohne NetApp Volume Encryption herunter. Siehe ["Welches ONTAP Image sollte ich herunterladen? Mit oder ohne Volume-Verschlüsselung?"](#) Entnehmen.

2. Entfernen Sie das USB-Flash-Laufwerk von Ihrem Laptop.

3. Installieren Sie das Controller-Modul:

- a. Richten Sie das Ende des Controller-Moduls an der Öffnung im Gehäuse aus, und drücken Sie dann vorsichtig das Controller-Modul zur Hälfte in das System.
- b. Controller-Modul wieder einsetzen.

Denken Sie beim Neuinstallieren der Medienkonverter (SFPs) daran, wenn sie entfernt wurden.

4. Stecken Sie das USB-Flash-Laufwerk in den USB-Steckplatz des Controller-Moduls.

Stellen Sie sicher, dass Sie das USB-Flash-Laufwerk in den für USB-Geräte gekennzeichneten Steckplatz und nicht im USB-Konsolenport installieren.

5. Drücken Sie das Controller-Modul ganz in das System, vergewissern Sie sich, dass der Nockengriff das USB-Flash-Laufwerk löscht, drücken Sie den Nockengriff fest, um den Sitz des Controller-Moduls zu beenden, schieben Sie den Nockengriff in die geschlossene Position und ziehen Sie die Daumenschraube fest.

Der Controller beginnt mit dem Booten, sobald er vollständig im Gehäuse installiert ist, und stoppt bei der LOADER-Eingabeaufforderung.

#### Was kommt als Nächstes?

Nach dem Ersetzen des Boot-Mediums müssen Sie ["Starten Sie das Wiederherstellungs-Image"](#).

## Manuelle Wiederherstellung eines Bootmediums von einem USB-Laufwerk – FAS2820

Nach der Installation des neuen Startmediengeräts im System können Sie das Wiederherstellungsabbild von einem USB-Laufwerk starten und die Konfiguration vom Partnerknoten wiederherstellen.

Wenn Ihr Speichersystem ONTAP 9.17.1 oder höher ausführt, verwenden Sie die ["automatisiertes Boot-Wiederherstellungsverfahren"](#). Wenn auf Ihrem System eine frühere Version von ONTAP ausgeführt wird, müssen Sie das manuelle Boot-Wiederherstellungsverfahren verwenden.

#### Bevor Sie beginnen

- Stellen Sie sicher, dass Ihre Konsole mit dem defekten Controller verbunden ist.
- Vergewissern Sie sich, dass Sie einen USB-Stick mit dem Wiederherstellungsabbild besitzen.
- Prüfen Sie, ob Ihr System Verschlüsselung verwendet. Je nachdem, ob die Verschlüsselung aktiviert ist, müssen Sie in Schritt 3 die entsprechende Option auswählen.

#### Schritte

1. Starten Sie vom LOADER-Eingabeaufforderung des betroffenen Controllers aus das Wiederherstellungsabbild vom USB-Stick:

```
boot_recovery
```

Das Wiederherstellungsabbild wird vom USB-Stick heruntergeladen.

2. Geben Sie bei Aufforderung den Namen des Bildes ein oder drücken Sie die **Eingabetaste**, um das in Klammern angezeigte Standardbild zu übernehmen.
3. Stellen Sie das var-Dateisystem gemäß der für Ihre ONTAP Version geltenden Vorgehensweise wieder her:

### ONTAP 9.16.0 oder früher

Führen Sie die folgenden Schritte sowohl für den beeinträchtigten Steuermann als auch für den Partnersteuermann durch:

- a. **Auf dem beeinträchtigten Controller:** Drücken Sie `Y` wenn du siehst `Do you want to restore the backup configuration now?`
- b. **Auf dem beeinträchtigten Controller:** Drücken Sie bei Aufforderung die Taste `Y` um `/etc/ssh/ssh_host_ecdsa_key` zu überschreiben.
- c. **Auf dem Partnercontroller:** Legen Sie für den beeinträchtigten Controller die erweiterte Berechtigungsstufe fest:

```
set -privilege advanced
```

- d. **Auf dem Partner-Controller:** Führen Sie den Befehl zum Wiederherstellen der Sicherung aus:

```
system node restore-backup -node local -target-address  
impaired_node_IP_address
```



Sollten Sie eine andere Meldung als eine erfolgreiche Wiederherstellung erhalten, wenden Sie sich bitte an den NetApp Support.

- e. **Auf dem Partner-Controller:** Zurück zur Administratorebene:

```
set -privilege admin
```

- f. **Auf dem beeinträchtigten Controller:** Drücken Sie `Y` wenn du siehst `Was the restore backup procedure successful?`
- g. **Auf dem beeinträchtigten Controller:** Drücken Sie `Y` wenn du siehst `...would you like to use this restored copy now?`
- h. **Auf dem beeinträchtigten Controller:** Drücken Sie `Y` Wenn Sie zum Neustart aufgefordert werden, drücken Sie `Ctrl-C` wenn das Bootmenü erscheint.
- i. **Bei beeinträchtigter Steuerung:** Führen Sie einen der folgenden Schritte aus:
  - Wenn das System keine Verschlüsselung verwendet, wählen Sie im Bootmenü *Option 1 Normal Boot* aus.
  - Wenn das System Verschlüsselung verwendet, gehen Sie zu "[Wiederherstellung der Verschlüsselung](#)". Die

### ONTAP 9.16.1 oder höher

Führen Sie die folgenden Schritte auf dem beeinträchtigten Steuergerät durch:

- a. Drücken Sie auf `Y`, wenn Sie dazu aufgefordert werden, die Sicherungskonfiguration wiederherzustellen.

Nach erfolgreichem Wiederherstellungsvorgang wird folgende Meldung angezeigt:

```
syncflash_partner: Restore from partner complete
```

- b. Drücken `Y` wenn man dazu aufgefordert wird, zu bestätigen, dass die Wiederherstellung des Backups erfolgreich war.

- c. Drücken **Y** wenn Sie aufgefordert werden, die wiederhergestellte Konfiguration zu verwenden.
- d. Drücken **Y** wenn zum Neustart des Knotens aufgefordert wird.
- e. Drücken **Y** Wenn Sie zum erneuten Neustart aufgefordert werden, drücken Sie **Ctrl-C** wenn das Bootmenü erscheint.
- f. Führen Sie einen der folgenden Schritte aus:
  - Wenn das System keine Verschlüsselung verwendet, wählen Sie im Bootmenü *Option 1 Normal Boot* aus.
  - Wenn das System Verschlüsselung verwendet, gehen Sie zu "[Wiederherstellung der Verschlüsselung](#)" Die

4. Schließen Sie das Konsolenkabel an den Partner Controller an.

5. Wiederherstellung des normalen Betriebs des Controllers durch Zurückgeben des Speichers:

```
storage failover giveback -fromnode local
```

6. Falls Sie die automatische Rückvergütung deaktiviert haben, aktivieren Sie sie bitte wieder:

```
storage failover modify -node local -auto-giveback true
```

7. Wenn AutoSupport aktiviert ist, stellen Sie die automatische Fallerstellung wieder her:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

### Was kommt als Nächstes?

Nach dem Booten des Wiederherstellungs-Images müssen Sie "[Stellen Sie die Verschlüsselung auf dem Startmedium wieder her](#)".

## Wiederherstellung der Verschlüsselung – FAS2820

Stellen Sie die Verschlüsselung auf dem Ersatz-Startmedium wieder her.

Wenn Ihr Speichersystem ONTAP 9.17.1 oder höher ausführt, verwenden Sie die "[automatisiertes Boot-Wiederherstellungsverfahren](#)". Wenn auf Ihrem System eine frühere Version von ONTAP ausgeführt wird, müssen Sie das manuelle Boot-Wiederherstellungsverfahren verwenden.

Führen Sie die entsprechenden Schritte zur Wiederherstellung der Verschlüsselung auf Ihrem System durch, abhängig von Ihrem Schlüsselverwaltungstyp. Wenn Sie sich nicht sicher sind, welchen Key-Manager Ihr System verwendet, überprüfen Sie die Einstellungen, die Sie zu Beginn des Vorgangs zum Austausch des Startmediums erfasst haben.



## Onboard Key Manager (OKM)

Stellen Sie die OKM-Konfiguration (Onboard Key Manager) über das ONTAP-Startmenü wieder her.

### Bevor Sie beginnen

Stellen Sie sicher, dass Ihnen folgende Informationen zur Verfügung stehen:

- Clusterweite Passphrase eingegeben während "[Aktivierung der Onboard-Schlüsselverwaltung](#)"
- "[Backup-Informationen für den Onboard Key Manager](#)"
- Überprüfen Sie mithilfe der "[Verifizierung von Onboard-Verschlüsselungsmanagement-Backup und Cluster-weiter Passphrase](#)" Verfahren

### Schritte

#### Zum beeinträchtigten Regler:

1. Schließen Sie das Konsolenkabel an den defekten Controller an.
2. Wählen Sie im ONTAP Bootmenü die entsprechende Option aus:

ONTAP-Version	Wählen Sie diese Option aus
ONTAP 9.8 oder höher	<p>Wählen Sie Option 10.</p> <p><b>Beispiel für ein Startmenü anzeigen</b></p> <div><p>Please choose one of the following:</p><ul style="list-style-type: none"><li>(1) Normal Boot.</li><li>(2) Boot without /etc/rc.</li><li>(3) Change password.</li><li>(4) Clean configuration and initialize all disks.</li><li>(5) Maintenance mode boot.</li><li>(6) Update flash from backup config.</li><li>(7) Install new software first.</li><li>(8) Reboot node.</li><li>(9) Configure Advanced Drive Partitioning.</li><li>(10) Set Onboard Key Manager recovery secrets.</li><li>(11) Configure node for external key management.</li></ul><p>Selection (1-11)? 10</p></div>

ONTAP-Version	Wählen Sie diese Option aus
ONTAP 9.7 und frühere Versionen	<p>Wählen Sie die ausgeblendete Option aus recover_onboard_keymanager</p> <p><b>Beispiel für ein Startmenü anzeigen</b></p> <div> <pre>Please choose one of the following:  (1)  Normal Boot. (2)  Boot without /etc/rc. (3)  Change password. (4)  Clean configuration and initialize all disks. (5)  Maintenance mode boot. (6)  Update flash from backup config. (7)  Install new software first. (8)  Reboot node. (9)  Configure Advanced Drive Partitioning. Selection (1-19)? recover_onboard_keymanager</pre> </div>

3. Bestätigen Sie auf Aufforderung, dass Sie den Wiederherstellungsprozess fortsetzen möchten:

**Beispiel-Eingabeaufforderung anzeigen**

```
This option must be used only in disaster recovery procedures. Are you
sure? (y or n):
```

4. Geben Sie die Cluster-weite Passphrase zweimal ein.

Während der Eingabe der Passphrase wird in der Konsole keine Eingabe angezeigt.

**Beispiel-Eingabeaufforderung anzeigen**

```
Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:
```

5. Geben Sie die Sicherungsinformationen ein:

- a. Fügen Sie den gesamten Inhalt von der Zeile BEGIN BACKUP bis zur Zeile END BACKUP einschließlich der Bindestriche ein.

## Beispiel-Eingabeaufforderung anzeigen

Enter the backup data:

-----BEGIN

BACKUP-----

01234567890123456789012345678901234567890123456789012345678901  
23

12345678901234567890123456789012345678901234567890123456789012  
34

23456789012345678901234567890123456789012345678901234567890123  
45

34567890123456789012345678901234567890123456789012345678901234  
56

45678901234567890123456789012345678901234567890123456789012345  
67

[illegible]

A  
A

[illegible][illegible][illegible][illegible][illegible][illegible][illegible][illegible][illegible][illegible][illegible][illegible][illegible]

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
-----END
BACKUP-----
```

b. Drücken Sie am Ende der Eingabe zweimal die Eingabetaste.

Der Wiederherstellungsprozess ist abgeschlossen und die folgende Meldung wird angezeigt:

Successfully recovered keymanager secrets.

### Beispiel-Eingabeaufforderung anzeigen

```
Trying to recover keymanager secrets....
Setting recovery material for the onboard key manager
Recovery secrets set successfully
Trying to delete any existing km_onboard.wkeydb file.

Successfully recovered keymanager secrets.

*****
*****
* Select option "(1) Normal Boot." to complete recovery process.
*
* Run the "security key-manager onboard sync" command to
synchronize the key database after the node reboots.
*****
*****
```

+



Fahren Sie nicht fort, wenn die angezeigte Ausgabe etwas anderes ist als  
Successfully recovered keymanager secrets Die Führen Sie eine  
Fehlerbehebung durch, um den Fehler zu beheben.

6. Option auswählen 1 vom Bootmenü zum Fortfahren des Bootvorgangs in ONTAP.

### Beispiel-Eingabeaufforderung anzeigen

```
*****
*****
* Select option "(1) Normal Boot." to complete the recovery
process.
*
*****
*****

(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 1
```

7. Vergewissern Sie sich, dass auf der Konsole des Controllers die folgende Meldung angezeigt wird:

```
Waiting for giveback...(Press Ctrl-C to abort wait)
```

#### Auf dem Partner-Controller:

8. Geben Sie den beeinträchtigten Controller zurück:

```
storage failover giveback -fromnode local -only-cfo-aggregates true
```

#### Zum beeinträchtigten Regler:

9. Nach dem Booten nur mit dem CFO-Aggregat synchronisieren Sie den Schlüsselmanager:

```
security key-manager onboard sync
```

10. Geben Sie bei Aufforderung die clusterweite Passphrase für den Onboard Key Manager ein.

## Beispiel-Eingabeaufforderung anzeigen

Enter the cluster-wide passphrase for the Onboard Key Manager:

All offline encrypted volumes will be brought online and the corresponding volume encryption keys (VEKs) will be restored automatically within 10 minutes. If any offline encrypted volumes are not brought online automatically, they can be brought online manually using the "volume online -vserver <vserver> -volume <volume\_name>" command.



Wenn die Synchronisierung erfolgreich ist, wird die Cluster-Eingabeaufforderung ohne weitere Meldungen zurückgegeben. Wenn die Synchronisierung fehlschlägt, wird eine Fehlermeldung angezeigt, bevor zur Cluster-Eingabeaufforderung zurückgekehrt wird. Fahren Sie erst fort, wenn der Fehler behoben ist und die Synchronisierung erfolgreich abgeschlossen wurde.

11. Überprüfen Sie, ob alle Schlüssel synchronisiert sind:

```
security key-manager key query -restored false
```

Der Befehl sollte keine Ergebnisse liefern. Falls Ergebnisse angezeigt werden, wiederholen Sie den Synchronisierungsbefehl, bis keine Ergebnisse mehr zurückgegeben werden.

### Auf dem Partner-Controller:

12. Geben Sie den beeinträchtigten Controller zurück:

```
storage failover giveback -fromnode local
```

13. Automatisches Giveback wiederherstellen, wenn Sie es deaktiviert haben:

```
storage failover modify -node local -auto-giveback true
```

14. Wenn AutoSupport aktiviert ist, stellen Sie die automatische Fallerstellung wieder her:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

## Externer Schlüsselmanager (EKM)

Stellen Sie die Konfiguration des externen Schlüsselmanagers über das ONTAP-Startmenü wieder her.

### Bevor Sie beginnen

Sammeln Sie die folgenden Dateien von einem anderen Clusterknoten oder aus Ihrer Sicherung:

- `/cfcard/kmip/servers.cfg` Datei oder die KMIP-Serveradresse und Port
- `/cfcard/kmip/certs/client.crt` Datei (Clientzertifikat)
- `/cfcard/kmip/certs/client.key` Datei (Client-Schlüssel)

- `/cfcard/kmip/certs/CA.pem`Datei (KMIP-Server-CA-Zertifikate)`

## Schritte

### Zum beeinträchtigten Regler:

1. Schließen Sie das Konsolenkabel an den defekten Controller an.
2. Option auswählen 11 aus dem ONTAP Bootmenü.

#### Beispiel für ein Startmenü anzeigen

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 11
```

3. Bestätigen Sie auf Aufforderung, dass Sie die erforderlichen Informationen gesammelt haben:

#### Beispiel-Eingabeaufforderung anzeigen

```
Do you have a copy of the /cfcard/kmip/certs/client.crt file?
{y/n}
Do you have a copy of the /cfcard/kmip/certs/client.key file?
{y/n}
Do you have a copy of the /cfcard/kmip/certs/CA.pem file? {y/n}
Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n}
```

4. Geben Sie die Client- und Serverinformationen ein, wenn Sie dazu aufgefordert werden:
  - a. Geben Sie den Inhalt der Clientzertifikatsdatei (client.crt) einschließlich der BEGIN- und END-Zeilen ein.
  - b. Geben Sie den Inhalt der Client-Schlüsseldatei (client.key) einschließlich der BEGIN- und END-Zeilen ein.
  - c. Geben Sie den Inhalt der KMIP-Server-CA(s)-Datei (CA.pem) ein, einschließlich der BEGIN- und END-Zeilen.
  - d. Geben Sie die IP-Adresse des KMIP-Servers ein.



- e. Geben Sie den KMIP-Server-Port ein (drücken Sie Enter, um den Standardport 5696 zu verwenden).

#### Beispiel anzeigen

```
Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

Enter the client key (client.key) file contents:
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

Enter the KMIP server CA(s) (CA.pem) file contents:
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----

Enter the IP address for the KMIP server: 10.10.10.10
Enter the port for the KMIP server [5696]:

System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
kmip_init: configuring ports
Running command '/sbin/ifconfig e0M'
..
..
kmip_init: cmd: ReleaseExtraBSDPort e0M
```

Der Wiederherstellungsprozess ist abgeschlossen und die folgende Meldung wird angezeigt:

```
Successfully recovered keymanager secrets.
```

#### Beispiel anzeigen

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
Performing initialization of OpenSSL
Successfully recovered keymanager secrets.
```

5. Option auswählen 1 vom Bootmenü zum Fortfahren des Bootvorgangs in ONTAP.

### Beispiel-Eingabeaufforderung anzeigen

```
*****
*****
* Select option "(1) Normal Boot." to complete the recovery
process.
*
*****
*****

(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 1
```

6. Automatisches Giveback wiederherstellen, wenn Sie es deaktiviert haben:

```
storage failover modify -node local -auto-giveback true
```

7. Wenn AutoSupport aktiviert ist, stellen Sie die automatische Fallerstellung wieder her:

```
system node autosupport invoke -node * -type all -message MAINT=END
```

### Was kommt als Nächstes?

Nach dem Wiederherstellen der Verschlüsselung auf dem Boot-Medium müssen Sie ["Geben Sie das fehlerhafte Teil an NetApp zurück"](#).

## Senden Sie das fehlerhafte Bootmedium an NetApp - FAS2820 zurück

Senden Sie das fehlerhafte Teil wie in den dem Kit beiliegenden RMA-Anweisungen beschrieben an NetApp zurück. ["Rückgabe und Austausch von Teilen"](#) Weitere Informationen finden Sie auf der Seite.

## 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.