



Bootmedium - manuelle Wiederherstellung

Install and maintain

NetApp
January 09, 2026

Inhalt

Bootmedium - manuelle Wiederherstellung	1
Ersetzen Sie das Startmedium – ASA A900	1
Unterstützung und Status von Verschlüsselungsschlüsseln prüfen – ASA A900	1
Schritt 1: NVE-Unterstützung prüfen und das richtige ONTAP Image herunterladen	1
Schritt 2: Überprüfen Sie den Status des Schlüsselmanagers und sichern Sie die Konfiguration.	2
Fahren Sie den Controller für die manuelle Wiederherstellung des Bootmediums herunter - ASA A900	5
Ersetzen Sie das Startmedium und bereiten Sie die manuelle Startwiederherstellung vor - ASA A900	9
Schritt 1: Entfernen Sie das Controller-Modul	9
Schritt 2: Ersetzen Sie die Startmedien	11
Schritt 3: Übertragen Sie das Startabbild auf das Startmedium	12
Manuelle Wiederherstellung eines Bootmediums von einem USB-Laufwerk – ASA A900	13
Wiederherstellung der Verschlüsselung – ASA A900	16
Senden Sie das fehlerhafte Teil an NetApp - ASA A900 zurück	26

Bootmedium - manuelle Wiederherstellung

Ersetzen Sie das Startmedium – ASA A900

Das Boot-Medium speichert einen primären und sekundären Satz von Systemdateien (Boot-Image), die das System beim Booten verwendet. Je nach Netzwerkkonfiguration können Sie entweder einen unterbrechungsfreien oder störenden Austausch durchführen.

Sie müssen über ein USB-Flash-Laufwerk verfügen, das auf FAT32 formatiert ist, und über die entsprechende Speichermenge, um die zu speichern `image_xxx.tgz` Datei:

Außerdem müssen Sie die kopieren `image_xxx.tgz` Datei auf dem USB-Flash-Laufwerk zur späteren Verwendung in diesem Verfahren.

- Bei den unterbrechungsfreien und unterbrechungsfreien Methoden zum Austausch von Boot-Medien müssen Sie den wiederherstellen `var` Filesystem:
 - Beim unterbrechungsfreien Austausch benötigt das HA-Paar keine Verbindung zu einem Netzwerk, um den wiederherzustellen `var` File-System. Das HA-Paar in einem einzelnen Chassis hat eine interne E0S-Verbindung, die zum Transfer verwendet wird `var` Konfigurieren zwischen ihnen.
 - Für den störenden Austausch benötigen Sie keine Netzwerkverbindung, um den wiederherzustellen `var` Dateisystem, aber der Prozess erfordert zwei Neustarts.
- Sie müssen die ausgefallene Komponente durch eine FRU-Ersatzkomponente ersetzen, die Sie von NetApp erhalten haben.
- Es ist wichtig, dass Sie die Befehle in diesen Schritten auf dem richtigen Controller anwenden:
 - Der Controller *Impaired* ist der Controller, an dem Sie Wartungsarbeiten durchführen.
 - Der *Healthy* Controller ist der HA-Partner des beeinträchtigten Controllers.

Unterstützung und Status von Verschlüsselungsschlüsseln prüfen – ASA A900

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

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“:

- 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.

- Überprüfen Sie, ob alle Authentifizierungsschlüssel wiederhergestellt wurden:

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

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

- 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“:

- Sichern Sie die OKM-Informationen:

- In den erweiterten Berechtigungsmodus wechseln:

```
set -priv advanced
```

Eingeben y wenn er zur Fortsetzung aufgefordert wird.

- Informationen zur Schlüsselverwaltung und Datensicherung anzeigen:

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

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

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

- Zurück zum Administratormodus:

```
set -priv admin
```

- b. 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. 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.

- ii. Informationen zur Schlüsselverwaltung und Datensicherung anzeigen:

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

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

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

- iv. Zurück zum Administratormodus:

```
set -priv admin
```

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

Fahren Sie den Controller für die manuelle Wiederherstellung des Bootmediums herunter - ASA A900

Fahren Sie den Controller mit eingeschränkter Konfiguration herunter oder übernehmen

Sie ihn entsprechend.

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.

In den meisten Konfigurationen

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

Um den beeinträchtigten Controller herunterzufahren, müssen Sie den Status des Controllers bestimmen und gegebenenfalls den Controller übernehmen, damit der gesunde Controller weiterhin Daten aus dem beeinträchtigten Reglerspeicher bereitstellen kann.

Über diese Aufgabe

- Wenn Sie über ein SAN-System verfügen, müssen Sie Event-Meldungen) für den beeinträchtigten Controller SCSI Blade überprüft haben `cluster kernel-service show`. Mit dem `cluster kernel-service show` Befehl (im erweiterten Modus von priv) werden der Knotenname, der Node, der Verfügbarkeitsstatus dieses Node und der Betriebsstatus dieses Node angezeigt "[Quorum-Status](#)".

Jeder Prozess des SCSI-Blades sollte sich im Quorum mit den anderen Nodes im Cluster befinden. Probleme müssen behoben werden, bevor Sie mit dem Austausch fortfahren.

- Wenn Sie über ein Cluster mit mehr als zwei Nodes verfügen, muss es sich im Quorum befinden. Wenn sich das Cluster nicht im Quorum befindet oder ein gesunder Controller FALSE anzeigt, um die Berechtigung und den Zustand zu erhalten, müssen Sie das Problem korrigieren, bevor Sie den beeinträchtigten Controller herunterfahren; siehe "[Synchronisieren eines Node mit dem Cluster](#)".

Schritte

1. Wenn AutoSupport aktiviert ist, unterdrücken Sie die automatische Erstellung eines Cases durch Aufrufen einer AutoSupport Meldung:

```
system node autosupport invoke -node * -type all -message MAINT=<# of hours>h
```

Die folgende AutoSupport Meldung unterdrückt die automatische Erstellung von Cases für zwei Stunden:

```
cluster1:> system node autosupport invoke -node * -type all -message MAINT=2h
```

2. Automatische Rückgabe deaktivieren:

- a. Geben Sie den folgenden Befehl von der Konsole des fehlerfreien Controllers ein:

```
storage failover modify -node impaired_node_name -auto-giveback false
```

- b. Eingeben `y` wenn die Eingabeaufforderung *Möchten Sie die automatische Rückgabe deaktivieren?* angezeigt wird

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

Wenn der eingeschränkte Controller angezeigt wird...	Dann...
Die LOADER-Eingabeaufforderung	Fahren Sie mit dem nächsten Schritt fort.

Wenn der eingeschränkte Controller angezeigt wird...	Dann...
Warten auf Giveback...	Drücken Sie Strg-C, und antworten Sie dann <i>y</i> Wenn Sie dazu aufgefordert werden.
Eingabeaufforderung für das System oder Passwort	Übernehmen oder stoppen Sie den beeinträchtigten Regler von der gesunden Steuerung: <code>storage failover takeover -ofnode impaired_node_name -halt true</code> Der Parameter <i>-stop true</i> führt Sie zur Loader-Eingabeaufforderung.

Controller befindet sich in einem MetroCluster

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



Verwenden Sie dieses Verfahren nicht, wenn sich Ihr System in einer MetroCluster-Konfiguration mit zwei Knoten befindet.

Um den beeinträchtigten Controller herunterzufahren, müssen Sie den Status des Controllers bestimmen und gegebenenfalls den Controller übernehmen, damit der gesunde Controller weiterhin Daten aus dem beeinträchtigten Reglerspeicher bereitstellen kann.

- Wenn Sie über ein Cluster mit mehr als zwei Nodes verfügen, muss es sich im Quorum befinden. Wenn sich das Cluster nicht im Quorum befindet oder ein gesunder Controller FALSE anzeigt, um die Berechtigung und den Zustand zu erhalten, müssen Sie das Problem korrigieren, bevor Sie den beeinträchtigten Controller herunterfahren; siehe "[Synchronisieren eines Node mit dem Cluster](#)".
- Wenn Sie über eine MetroCluster-Konfiguration verfügen, müssen Sie bestätigt haben, dass der MetroCluster-Konfigurationsstatus konfiguriert ist und dass die Nodes in einem aktvierten und normalen Zustand vorliegen (`metrocluster node show`).

Schritte

1. Wenn AutoSupport aktiviert ist, unterdrücken Sie die automatische Erstellung eines Cases durch Aufrufen einer AutoSupport Meldung: `system node autosupport invoke -node * -type all -message MAINT=number_of_hours_downh`

Die folgende AutoSupport Meldung unterdrückt die automatische Erstellung von Cases für zwei Stunden: `cluster1:*> system node autosupport invoke -node * -type all -message MAINT=2h`

2. Deaktivieren Sie das automatische Giveback von der Konsole des gesunden Controllers: `storage failover modify -node local -auto-giveback false`
3. Nehmen Sie den beeinträchtigten Controller zur LOADER-Eingabeaufforderung:

Wenn der eingeschränkte Controller angezeigt wird...	Dann...
Die LOADER-Eingabeaufforderung	Fahren Sie mit dem nächsten Schritt fort.
Warten auf Giveback...	Drücken Sie Strg-C, und antworten Sie dann <i>y</i> 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 <i>impaired_node_name</i></code> Wenn der Regler „beeinträchtigt“ auf Zurückgeben wartet... anzeigt, drücken Sie Strg-C, und antworten Sie dann <i>y</i> .

Ersetzen Sie das Startmedium und bereiten Sie die manuelle Startwiederherstellung vor - ASA A900

Sie müssen das Controller-Modul trennen, das Controller-Modul entfernen und öffnen, das Boot-Medium im Controller suchen und austauschen und dann das Image auf das Ersatz-Boot-Medium übertragen.

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.

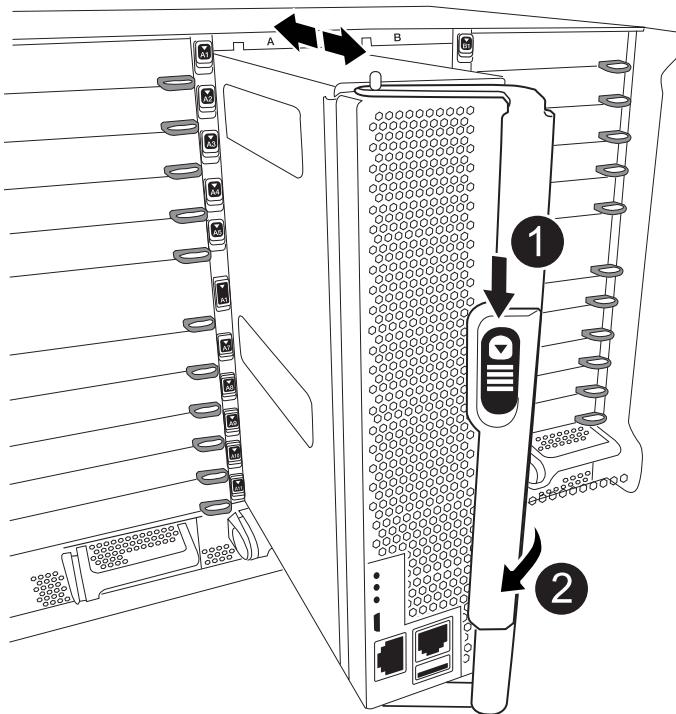
Schritt 1: Entfernen Sie das Controller-Modul

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.

Schritte

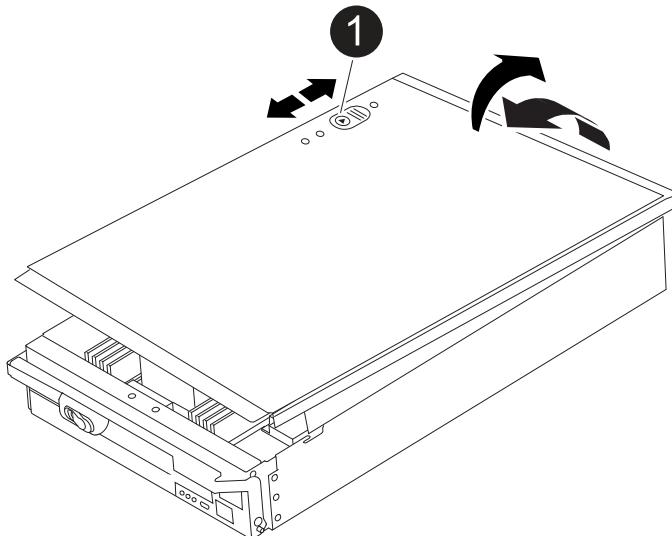
1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
2. Ziehen Sie die Kabel vom beeinträchtigten Controller-Modul ab, und verfolgen Sie, wo die Kabel angeschlossen waren.
3. Schieben Sie die Terrakotta-Taste am Nockengriff nach unten, bis sie entsperrt wird.

[Animation - Entfernen Sie den Controller](#)



1	Freigabetaste für den CAM-Griff
2	CAM-Griff

4. Drehen Sie den Nockengriff so, dass er das Controller-Modul vollständig aus dem Gehäuse herausrückt, und schieben Sie dann das Controller-Modul aus dem Gehäuse.
Stellen Sie sicher, dass Sie die Unterseite des Controller-Moduls unterstützen, während Sie es aus dem Gehäuse schieben.
5. Setzen Sie die Abdeckung des Controller-Moduls auf eine stabile, flache Oberfläche, drücken Sie die blaue Taste auf der Abdeckung, schieben Sie die Abdeckung auf die Rückseite des Controller-Moduls, und schwenken Sie sie dann nach oben und heben Sie sie vom Controller-Modul ab.



1

Verriegelungstaste für die Controllermodulabdeckung

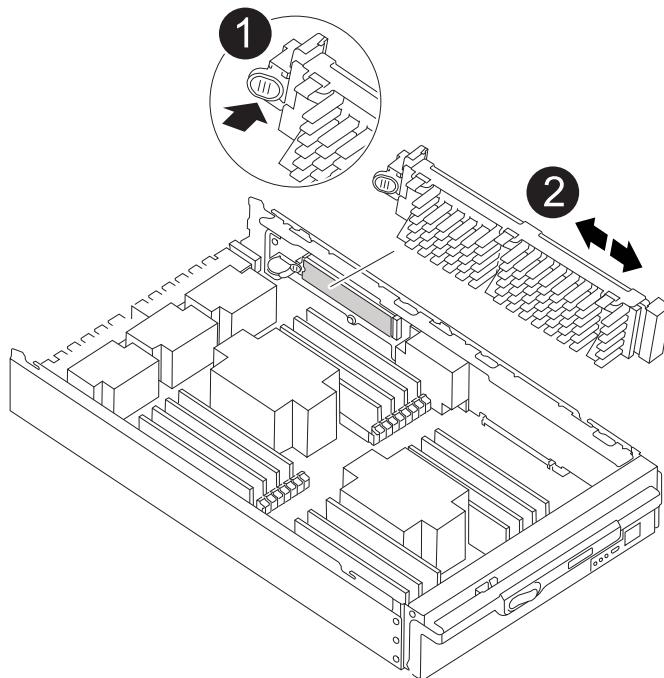
Schritt 2: Ersetzen Sie die Startmedien

Sie müssen das Startmedium im Controller finden und die Anweisungen befolgen, um es zu ersetzen.

Schritte

1. Heben Sie den schwarzen Luftkanal auf der Rückseite des Controller-Moduls an, und suchen Sie dann mithilfe der folgenden Abbildung oder der FRU-Karte am Controller-Modul die Bootmedien:

[Animation - Bootmedium ersetzen](#)



1	Drücken Sie die Freigabelasche
2	Boot-Medien

2. Drücken Sie die blaue Taste am Startmediengehäuse, um die Startmedien aus dem Gehäuse zu lösen, und ziehen Sie sie vorsichtig gerade aus der Buchse des Boot-Mediums heraus.



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

3. Richten Sie die Kanten des Ersatzstartmediums an der Buchse des Boot-Mediums aus, und schieben Sie ihn dann vorsichtig in die Buchse.

4. Überprüfen Sie die Startmedien, um sicherzustellen, dass sie ganz und ganz in der Steckdose sitzt.

Entfernen Sie gegebenenfalls die Startmedien, und setzen Sie sie wieder in den Sockel ein.

5. Drücken Sie die Startmedien nach unten, um die Verriegelungstaste am Startmediengehäuse zu betätigen.

6. Bringen Sie die Abdeckung des Controller-Moduls wieder an, indem Sie die Stifte auf dem Deckel an die Slitze auf dem Motherboard-Träger ausrichten und den Deckel dann in die richtige Position schieben.

Schritt 3: Übertragen Sie das Startabbild auf das Startmedium

Sie können das System-Image über ein USB-Flash-Laufwerk, auf dem das Image installiert ist, auf dem Ersatzstartmedium installieren. Sie müssen das var-Dateisystem jedoch während dieses Vorgangs wiederherstellen.

Bevor Sie beginnen

- Sie müssen über ein USB-Flash-Laufwerk verfügen, das auf FAT32 formatiert ist und eine Kapazität von mindestens 4 GB aufweist.
- Laden Sie eine Kopie der gleichen Bildversion von ONTAP herunter, die den Betrieb des beeinträchtigten Controllers enthält. Sie können das entsprechende Bild im Abschnitt „Downloads“ auf der NetApp Support-Website herunterladen. Verwenden Sie den `version -v` Befehl, um anzuzeigen, ob Ihre Version von ONTAP NVE unterstützt. Wenn die Befehlsausgabe angezeigt wird <10no- DARE>, unterstützt Ihre Version von ONTAP NVE nicht.
 - Wenn NVE von Ihrer Version von ONTAP unterstützt wird, laden Sie das Image mit NetApp Volume Encryption herunter, wie auf der Download-Schaltfläche angegeben.
 - Wenn NVE nicht unterstützt wird, laden Sie das Image ohne NetApp-Volume-Verschlüsselung herunter, wie auf der Download-Schaltfläche angegeben.
- Wenn es sich bei Ihrem System um ein eigenständiges System handelt, benötigen Sie keine Netzwerkverbindung, Sie müssen jedoch beim Wiederherstellen des var-Dateisystems einen zusätzlichen Neustart durchführen.

Schritte

1. Wenn Sie dies nicht getan haben, laden Sie das entsprechende Service-Image vom auf das USB-Flash-Laufwerk herunter, und kopieren ["NetApp Support Website"](#) Sie es.
 - a. Laden Sie das Service-Image über den Link Downloads auf der Seite auf Ihren Arbeitsbereich auf Ihrem Laptop herunter.

b. Entpacken Sie das Service-Image.



Wenn Sie den Inhalt mit Windows extrahieren, verwenden Sie WinZip nicht zum Extrahieren des Netzboots-Images. Verwenden Sie ein anderes Extraktionsstool, wie 7-Zip oder WinRAR.

Das USB-Flash-Laufwerk sollte über das entsprechende ONTAP-Image des ausgeführten Controllers verfügen.

2. 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.
3. Das Controller-Modul nach Bedarf wieder einschalten.
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. Das Controller-Modul ganz in das System schieben, sicherstellen, dass der Nockengriff das USB-Flash-Laufwerk löscht, den Nockengriff fest drücken, um den Sitz des Controller-Moduls zu beenden, und dann den Nockengriff in die geschlossene Position drücken.

Der Controller beginnt zu booten, sobald er vollständig im Chassis installiert ist.

6. Unterbrechen Sie den Boot-Vorgang, um an der LOADER-Eingabeaufforderung zu stoppen, indem Sie Strg-C drücken, wenn Sie sehen Starten VON AUTOBOOT drücken Sie Strg-C, um den Vorgang abzubrechen

Wenn Sie diese Meldung verpassen, drücken Sie Strg-C, wählen Sie die Option zum Booten im Wartungsmodus aus, und halten Sie dann den Controller zum Booten in LOADER an.

7. Wenn sich der Controller in einem Stretch- oder Fabric-Attached MetroCluster befindet, müssen Sie die FC-Adapterkonfiguration wiederherstellen:
 - a. Start in Wartungsmodus: `boot_ontap maint`
 - b. Legen Sie die MetroCluster -Ports als Initiatoren fest: `ucadmin modify -m fc -t initiator adapter_name`
 - c. Anhalten, um zum Wartungsmodus zurückzukehren: `halt`

Die Änderungen werden implementiert, wenn das System gestartet wird.

Manuelle Wiederherstellung eines Bootmediums von einem USB-Laufwerk – ASA A900

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
```

## **Wiederherstellung der Verschlüsselung – ASA A900**

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 style="border: 1px solid #ccc; padding: 10px; border-radius: 10px;"><p>Please choose one of the following:</p><p>(1) Normal Boot.<br/>(2) Boot without /etc/rc.<br/>(3) Change password.<br/>(4) Clean configuration and initialize all disks.<br/>(5) Maintenance mode boot.<br/>(6) Update flash from backup config.<br/>(7) Install new software first.<br/>(8) Reboot node.<br/>(9) Configure Advanced Drive Partitioning.<br/>(10) Set Onboard Key Manager recovery secrets.<br/>(11) Configure node for external key management.<br/>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<br/>recover_onboard_keymanager</p> <p><b>Beispiel für ein Startmenü anzeigen</b></p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <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> </ul> <p>Selection (1-19)?<br/>recover_onboard_keymanager</p> </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:

```
AA
AA
AA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
0123456789012345678901234567890123456789012345678901
23
1234567890123456789012345678901234567890123456789012
34
2345678901234567890123456789012345678901234567890123
45
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
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:

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

## Senden Sie das fehlerhafte Teil an NetApp - ASA A900 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 BESCHRÄNKKT 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 BESCHRÄNKKT 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 VERTRÄGLICH 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.