



# Boot-Medien

Install and maintain

NetApp  
March 17, 2023

# Inhaltsverzeichnis

- Boot-Medien ..... 1
  - Überblick über den Austausch von Boot-Medien – AFF FAS8300 und FAS8700 ..... 1
  - Überprüfen Sie die integrierten Verschlüsselungsschlüssel für die AFF fas8300 und FAS8700 ..... 1
  - Fahren Sie den beeinträchtigten Controller herunter – AFF FAS8300 und FAS8700 ..... 5
  - Ersetzen Sie die Boot-Medien FAS8300 und FAS8700 ..... 9
  - Booten des Recovery-Images – AFF FAS8300 und FAS8700 ..... 15
  - Schalten Sie Aggregate in einer MetroCluster Konfiguration mit zwei Nodes zurück – AFF fas8300 und FAS8700 ..... 17
  - Stellen Sie OKM, NSE und NVE nach Bedarf wieder her – AFF fas8300 und FAS8700 ..... 19
  - Das ausgefallene Teil an NetApp – AFF fas8300 und FAS8700 – zurücksenden ..... 23

# Boot-Medien

## Überblick über den Austausch von Boot-Medien – AFF FAS8300 und FAS8700

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 muss das HA-Paar mit einem Netzwerk verbunden sein, um den wiederherzustellen `var` File-System.
  - Für den störenden Austausch benötigen Sie keine Netzwerkverbindung, um den wiederherzustellen `var` Dateisystem, aber der Prozess erfordert zwei Neustarts.
- Sie müssen die fehlerhafte Komponente durch eine vom Anbieter empfangene Ersatz-FRU-Komponente ersetzen.
- Es ist wichtig, dass Sie die Befehle in diesen Schritten auf dem richtigen Node anwenden:
  - Der Node *Impared* ist der Knoten, auf dem Sie Wartungsarbeiten durchführen.
  - Der *Healthy Node* ist der HA-Partner des beeinträchtigten Knotens.

## Überprüfen Sie die integrierten Verschlüsselungsschlüssel für die AFF fas8300 und FAS8700

Bevor Sie den beeinträchtigten Controller herunterfahren und den Status der integrierten Verschlüsselungsschlüssel prüfen, müssen Sie den Status des beeinträchtigten Controllers überprüfen, das automatische Giveback deaktivieren und die Version von ONTAP prüfen, die ausgeführt wird.

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 für die Berechtigung und den Zustand anzeigt, müssen Sie das Problem korrigieren, bevor Sie den beeinträchtigten Controller herunterfahren; siehe "[Synchronisieren eines Node mit dem Cluster](#)".

### Schritte

1. Den Status des beeinträchtigten Reglers prüfen:
  - Wenn sich der Controller mit eingeschränkter Bedieneinheit an der Anmeldeaufforderung befindet, melden Sie sich als `admin`.

- Wenn der Controller mit eingeschränkter Einstellung an der LOADER-Eingabeaufforderung steht und Teil der HA-Konfiguration ist, melden Sie sich als `admin` Auf dem gesunden Controller.
  - Wenn sich der beeinträchtigte Controller in einer eigenständigen Konfiguration befindet und an DER LOADER-Eingabeaufforderung angezeigt wird, wenden Sie sich an "[mysupport.netapp.com](https://mysupport.netapp.com)".
2. 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`
3. Überprüfen Sie die Version von ONTAP, auf der das System auf dem beeinträchtigten Controller ausgeführt wird, wenn er eingeschaltet ist, oder auf dem Partner-Controller, wenn der beeinträchtigte Controller nicht verfügbar ist, über das `version -v` Befehl:
- Wenn `<Ino-DARE>` oder `<1Ono-DARE>` in der Befehlsausgabe angezeigt wird, unterstützt das System NVE nicht. Fahren Sie mit dem Herunterfahren des Controllers fort.
  - Wenn `<Ino-DARE>` nicht in der Befehlsausgabe angezeigt wird und auf dem System ONTAP 9.6 oder höher ausgeführt wird, fahren Sie mit dem nächsten Abschnitt fort.
4. Wenn der beeinträchtigte Controller Teil einer HA-Konfiguration ist, deaktivieren Sie das automatische Giveback vom ordnungsgemäßen Controller: `storage failover modify -node local -auto-giveback false` Oder `storage failover modify -node local -auto-giveback-after-panic false`

## Prüfen Sie NVE oder NSE auf Systemen mit ONTAP 9.6 und höher

Vor dem Herunterfahren des beeinträchtigten Controllers müssen Sie überprüfen, ob im System NetApp Volume Encryption (NVE) oder NetApp Storage Encryption (NSE) aktiviert ist. In diesem Fall müssen Sie die Konfiguration überprüfen.

1. Überprüfen Sie, ob NVE für alle Volumes im Cluster verwendet wird: `volume show -is-encrypted true`

Wenn im Output irgendwelche Volumes aufgelistet werden, wird NVE konfiguriert, und Sie müssen die NVE-Konfiguration überprüfen. Wenn keine Volumes aufgeführt sind, prüfen Sie, ob NSE konfiguriert und verwendet wird.

2. Überprüfen Sie, ob NSE konfiguriert und in Verwendung ist: `storage encryption disk show`
- Wenn in der Befehlsausgabe die Laufwerkdetails mit Informationen zu Modus und Schlüssel-ID aufgeführt werden, wird NSE konfiguriert und Sie müssen die NSE-Konfiguration und die darin verwendeten Informationen überprüfen.
  - Wenn keine Festplatten angezeigt werden, ist NSE nicht konfiguriert.
  - Wenn NVE und NSE nicht konfiguriert sind, sind keine Laufwerke mit NSE-Schlüsseln geschützt, sodass sich der beeinträchtigte Controller nicht herunterfahren lässt.

## Überprüfen der NVE-Konfiguration

1. Anzeigen der Schlüssel-IDs der Authentifizierungsschlüssel, die auf den Schlüsselverwaltungsservern gespeichert sind: `security key-manager key-query`



Nach der ONTAP 9.6 Version verfügen Sie eventuell über weitere wichtige Manager-Typen. Diese Typen sind KMIP, AKV, und GCP. Der Prozess zur Bestätigung dieser Typen entspricht der Bestätigung `external` Oder `onboard` Wichtige Manager-Typen.

- Wenn der `Key Manager Typ` wird angezeigt `external` Und das `Restored` Spalte wird angezeigt `yes`, Es ist sicher, den beeinträchtigten Regler herunterzufahren.
  - Wenn der `Key Manager Typ` wird angezeigt `onboard` Und das `Restored` Spalte wird angezeigt `yes`, Sie müssen einige zusätzliche Schritte.
  - Wenn der `Key Manager Typ` wird angezeigt `external` Und das `Restored` Spalte zeigt alle anderen als `an yes`, Sie müssen einige zusätzliche Schritte.
  - Wenn der `Key Manager Typ` wird angezeigt `onboard` Und das `Restored` Spalte zeigt alle anderen als `an yes`, Sie müssen einige zusätzliche Schritte.
2. Wenn der `Key Manager Typ` wird angezeigt `onboard` Und das `Restored` Spalte wird angezeigt `yes`, Manuelle Sicherung der OKM-Informationen:
    - a. Wechseln Sie zum erweiterten Berechtigungsebene-Modus, und geben Sie ein `y` Wenn Sie dazu aufgefordert werden, fortzufahren: `set -priv advanced`
    - b. Geben Sie den Befehl ein, um die Schlüsselmanagementinformationen anzuzeigen: `security key-manager onboard show-backup`
    - c. Kopieren Sie den Inhalt der Backup-Informationen in eine separate Datei oder eine Protokolldatei. Sie werden es in Disaster-Szenarien benötigen, in denen Sie OKM manuell wiederherstellen müssen.
    - d. Zurück zum Admin-Modus: `set -priv admin`
    - e. Schalten Sie den beeinträchtigten Regler aus.
  3. Wenn der `Key Manager Typ` wird angezeigt `external` Und das `Restored` Spalte zeigt alle anderen als `an yes`:
    - a. Stellen Sie die Authentifizierungsschlüssel für das externe Verschlüsselungsmanagement auf allen Nodes im Cluster wieder her: `security key-manager external restore`

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

["mysupport.netapp.com"](https://mysupport.netapp.com)

- a. Überprüfen Sie das `Restored` Spalte entspricht `yes` Für alle Authentifizierungsschlüssel: `security key-manager key-query`
  - b. Schalten Sie den beeinträchtigten Regler aus.
4. Wenn der `Key Manager Typ` wird angezeigt `onboard` Und das `Restored` Spalte zeigt alle anderen als `an yes`:
  - a. Geben Sie den integrierten Sicherheitsschlüssel-Manager Sync-Befehl ein: `security key-manager onboard sync`



Geben Sie an der Eingabeaufforderung die integrierte Passphrase für das Verschlüsselungsmanagement des Kunden ein. Falls die Passphrase nicht angegeben werden kann, wenden Sie sich an den NetApp Support. ["mysupport.netapp.com"](https://mysupport.netapp.com)

- b. Überprüfen Sie die `Restored` In der Spalte wird angezeigt `yes` Für alle Authentifizierungsschlüssel:

`security key-manager key-query`

- c. Überprüfen Sie das `Key Manager Typ` zeigt an `onboard`, Und dann manuell sichern Sie die OKM-Informationen.
- d. Wechseln Sie zum erweiterten Berechtigungsebene-Modus, und geben Sie ein `y` Wenn Sie dazu aufgefordert werden, fortzufahren: `set -priv advanced`
- e. Geben Sie den Befehl ein, um die Backup-Informationen für das Verschlüsselungsmanagement anzuzeigen: `security key-manager onboard show-backup`
- f. Kopieren Sie den Inhalt der Backup-Informationen in eine separate Datei oder eine Protokolldatei. Sie werden es in Disaster-Szenarien benötigen, in denen Sie OKM manuell wiederherstellen müssen.
- g. Zurück zum Admin-Modus: `set -priv admin`
- h. Sie können den Controller sicher herunterfahren.

## Überprüfen der NSE-Konfiguration

1. Anzeigen der Schlüssel-IDs der Authentifizierungsschlüssel, die auf den Schlüsselverwaltungsservern gespeichert sind: `security key-manager key-query -key-type NSE-AK`



Nach der ONTAP 9.6 Version verfügen Sie eventuell über weitere wichtige Manager-Typen. Diese Typen sind KMIP, AKV, und GCP. Der Prozess zur Bestätigung dieser Typen entspricht der Bestätigung `external` Oder `onboard` Wichtige Manager-Typen.

- Wenn der `Key Manager Typ` wird angezeigt `external` Und das `Restored` Spalte wird angezeigt `yes`, Es ist sicher, den beeinträchtigten Regler herunterzufahren.
  - Wenn der `Key Manager Typ` wird angezeigt `onboard` Und das `Restored` Spalte wird angezeigt `yes`, Sie müssen einige zusätzliche Schritte.
  - Wenn der `Key Manager Typ` wird angezeigt `external` Und das `Restored` Spalte zeigt alle anderen als `an yes`, Sie müssen einige zusätzliche Schritte.
  - Wenn der `Key Manager Typ` wird angezeigt `external` Und das `Restored` Spalte zeigt alle anderen als `an yes`, Sie müssen einige zusätzliche Schritte.
2. Wenn der `Key Manager Typ` wird angezeigt `onboard` Und das `Restored` Spalte wird angezeigt `yes`, Manuelle Sicherung der OKM-Informationen:
    - a. Wechseln Sie zum erweiterten Berechtigungsebene-Modus, und geben Sie ein `y` Wenn Sie dazu aufgefordert werden, fortzufahren: `set -priv advanced`
    - b. Geben Sie den Befehl ein, um die Schlüsselmanagementinformationen anzuzeigen: `security key-manager onboard show-backup`
    - c. Kopieren Sie den Inhalt der Backup-Informationen in eine separate Datei oder eine Protokolldatei. Sie werden es in Disaster-Szenarien benötigen, in denen Sie OKM manuell wiederherstellen müssen.
    - d. Zurück zum Admin-Modus: `set -priv admin`
    - e. Sie können den Controller sicher herunterfahren.
  3. Wenn der `Key Manager Typ` wird angezeigt `external` Und das `Restored` Spalte zeigt alle anderen als `an yes`:
    - a. Geben Sie den integrierten Sicherheitsschlüssel-Manager Sync-Befehl ein: `security key-manager external sync`

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

["mysupport.netapp.com"](https://mysupport.netapp.com)

- a. Überprüfen Sie das `Restored` Spalte entspricht `yes` Für alle Authentifizierungsschlüssel: `security key-manager key-query`
  - b. Sie können den Controller sicher herunterfahren.
4. Wenn der `Key Manager Typ` wird angezeigt `onboard` Und das `Restored` Spalte zeigt alle anderen als `an yes`:
- a. Geben Sie den integrierten Sicherheitsschlüssel-Manager Sync-Befehl ein: `security key-manager onboard sync`

Geben Sie an der Eingabeaufforderung die integrierte Passphrase für das Verschlüsselungsmanagement des Kunden ein. Falls die Passphrase nicht angegeben werden kann, wenden Sie sich an den NetApp Support.

["mysupport.netapp.com"](https://mysupport.netapp.com)

- a. Überprüfen Sie die `Restored` In der Spalte wird angezeigt `yes` Für alle Authentifizierungsschlüssel: `security key-manager key-query`
- b. Überprüfen Sie das `Key Manager Typ` zeigt an `onboard`, Und dann manuell sichern Sie die OKM-Informationen.
- c. Wechseln Sie zum erweiterten Berechtigungsebene-Modus, und geben Sie ein `y` Wenn Sie dazu aufgefordert werden, fortzufahren: `set -priv advanced`
- d. Geben Sie den Befehl ein, um die Backup-Informationen für das Verschlüsselungsmanagement anzuzeigen: `security key-manager onboard show-backup`
- e. Kopieren Sie den Inhalt der Backup-Informationen in eine separate Datei oder eine Protokolldatei. Sie werden es in Disaster-Szenarien benötigen, in denen Sie OKM manuell wiederherstellen müssen.
- f. Zurück zum Admin-Modus: `set -priv admin`
- g. Sie können den Controller sicher herunterfahren.

## Fahren Sie den beeinträchtigten Controller herunter – AFF FAS8300 und FAS8700

### Option 1: Die meisten Systeme

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 y 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 y.

- 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.

## Option 2: 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 aktivierten und normalen Zustand vorliegen (`metrocluster node show`).

### Schritte

- 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	Wechseln Sie zu Controller-Modul entfernen.
Warten auf 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 <i>impaired_node_name</i></code>  Wenn der Regler „beeinträchtigt“ auf Zurückgeben wartet... anzeigt, drücken Sie Strg-C, und antworten Sie dann <code>y</code> .

### Option 3: Controller befindet sich in einem MetroCluster mit zwei Nodes

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 umschalten, damit der gesunde Controller weiterhin Daten aus dem beeinträchtigten Reglerspeicher bereitstellen kann.

#### Über diese Aufgabe

- Wenn Sie NetApp Storage Encryption verwenden, müssen Sie die MSID mithilfe der Anweisungen im Abschnitt „ein FIPS-Laufwerk oder SED in ungeschützten Modus zurückgeben“ von zurücksetzen "[NetApp Encryption: Übersicht mit CLI](#)".
- Sie müssen die Netzteile am Ende dieses Verfahrens einschalten, um den gesunden Controller mit Strom zu versorgen.

#### Schritte

1. Überprüfen Sie den MetroCluster-Status, um festzustellen, ob der beeinträchtigte Controller automatisch auf den gesunden Controller umgeschaltet wurde: `metrocluster show`
2. Je nachdem, ob eine automatische Umschaltung stattgefunden hat, fahren Sie mit der folgenden Tabelle fort:

Wenn die eingeschränkte Steuerung...	Dann...
Ist automatisch umgeschaltet	Fahren Sie mit dem nächsten Schritt fort.

Wenn die eingeschränkte Steuerung...	Dann...
Nicht automatisch umgeschaltet	Einen geplanten Umschaltvorgang vom gesunden Controller durchführen: <code>metrocluster switchover</code>
Hat nicht automatisch umgeschaltet, haben Sie versucht, mit dem zu wechseln <code>metrocluster switchover</code> Befehl und Switchover wurde vetoed	Überprüfen Sie die Veto-Meldungen, und beheben Sie das Problem, wenn möglich, und versuchen Sie es erneut. Wenn das Problem nicht behoben werden kann, wenden Sie sich an den technischen Support.

- Synchronisieren Sie die Datenaggregate neu, indem Sie das ausführen `metrocluster heal -phase aggregates` Befehl aus dem verbleibenden Cluster.

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

Wenn die Heilung ein Vetorecht ist, haben Sie die Möglichkeit, das zurückzugeben `metrocluster heal` Befehl mit dem `-override-vetoes` Parameter. Wenn Sie diesen optionalen Parameter verwenden, überschreibt das System alle weichen Vetos, die die Heilung verhindern.

- Überprüfen Sie, ob der Vorgang mit dem befehl „MetroCluster Operation show“ abgeschlossen wurde.

```
controller_A_1::> metrocluster operation show
Operation: heal-aggregates
State: successful
Start Time: 7/25/2016 18:45:55
End Time: 7/25/2016 18:45:56
Errors: -
```

- Überprüfen Sie den Status der Aggregate mit `storage aggregate show` Befehl.

```
controller_A_1::> storage aggregate show
Aggregate      Size Available Used% State   #Vols  Nodes           RAID
Status
-----
...
aggr_b2       227.1GB   227.1GB   0% online    0  mcc1-a2
raid_dp, mirrored, normal...
```

- Heilen Sie die Root-Aggregate mit dem `metrocluster heal -phase root-aggregates` Befehl.

```
mccl1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

Wenn die Heilung ein Vetorecht ist, haben Sie die Möglichkeit, das zurückzugeben `metrocluster heal` Befehl mit dem Parameter `-override-vetoes`. Wenn Sie diesen optionalen Parameter verwenden, überschreibt das System alle weichen Vetos, die die Heilung verhindern.

7. Stellen Sie sicher, dass der Heilungsvorgang abgeschlossen ist, indem Sie den verwenden `metrocluster operation show` Befehl auf dem Ziel-Cluster:

```
mccl1A::> metrocluster operation show
Operation: heal-root-aggregates
State: successful
Start Time: 7/29/2016 20:54:41
End Time: 7/29/2016 20:54:42
Errors: -
```

8. Trennen Sie am Controller-Modul mit eingeschränkter Betriebsstörung die Netzteile.

## Ersetzen Sie die Boot-Medien FAS8300 und FAS8700

Zum Austauschen des Startmediums müssen Sie das beeinträchtigte Controller-Modul entfernen, das Ersatzstartmedium installieren und das Boot-Image auf ein USB-Flash-Laufwerk übertragen.

### Schritt 1: Entfernen Sie das Controller-Modul

Um auf Komponenten im Controller-Modul zuzugreifen, müssen Sie das Controller-Modul aus dem Gehäuse entfernen.

Sie können das Controller-Modul mithilfe der folgenden Animation, Illustration oder der geschriebenen Schritte aus dem Gehäuse entfernen.

#### [Animation - Entfernen Sie das Controller-Modul](#)

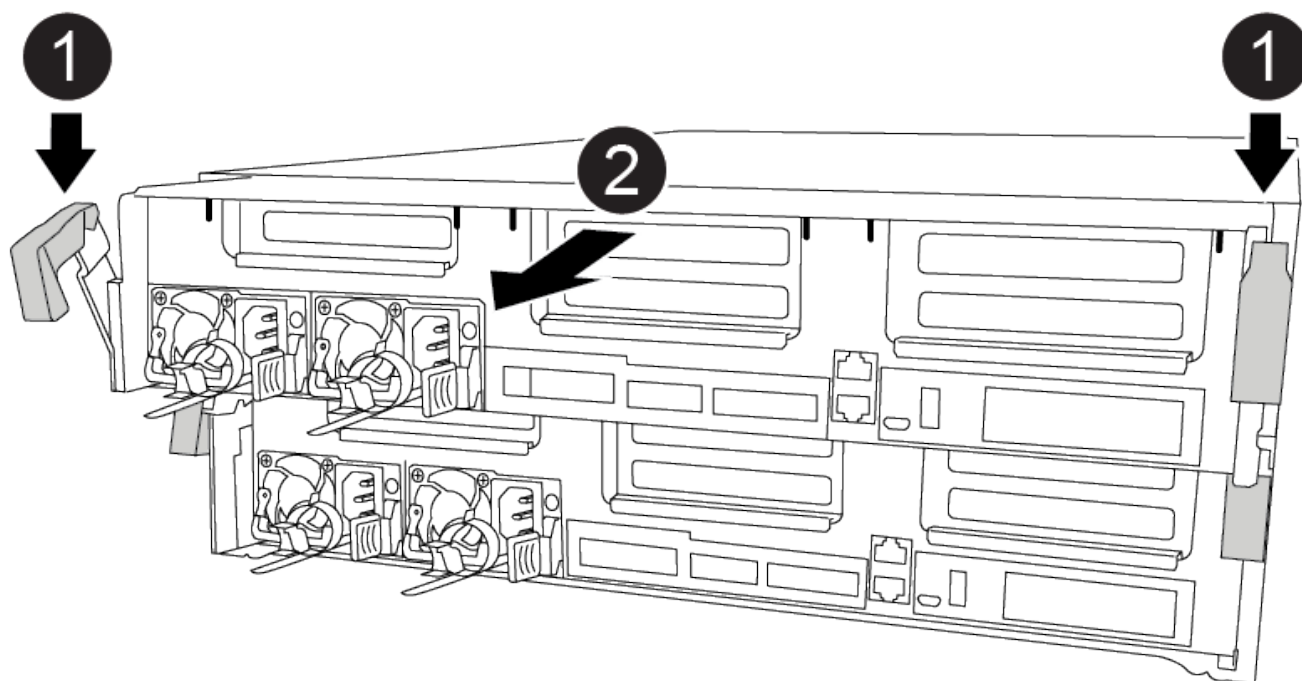
##### Schritte

1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
2. Lösen Sie die Netzkabelhalter, und ziehen Sie anschließend die Kabel von den Netzteilen ab.
3. 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.

Lassen Sie die Kabel im Kabelverwaltungs-Gerät so, dass bei der Neuinstallation des Kabelverwaltungsgeräts die Kabel organisiert sind.

4. Entfernen Sie das Kabelführungs-Gerät aus dem Controller-Modul und legen Sie es beiseite.
5. Drücken Sie beide Verriegelungsriegel nach unten, und drehen Sie dann beide Verriegelungen gleichzeitig nach unten.

Das Controller-Modul wird leicht aus dem Chassis entfernt.



1
Verriegelungsriegel
2
Schieben Sie den Controller aus dem Chassis heraus

6. Schieben Sie das Controller-Modul aus dem Gehäuse.

Stellen Sie sicher, dass Sie die Unterseite des Controller-Moduls unterstützen, während Sie es aus dem Gehäuse schieben.

7. Stellen Sie das Controller-Modul auf eine stabile, flache Oberfläche.

## Schritt 2: Ersetzen Sie die Startmedien

Suchen Sie das Boot-Medium im Controller-Modul (siehe FRU-Zuordnung am Controller-Modul) und befolgen Sie dann die Anweisungen, um es zu ersetzen.

### Bevor Sie beginnen

Obwohl der Inhalt des Startmediums verschlüsselt ist, empfiehlt es sich, den Inhalt der Startmedien zu löschen, bevor sie ersetzt werden. Weitere Informationen finden Sie im ["Angaben zu flüchtigem Speicher"](#) Für Ihr System auf der NetApp Support Site.



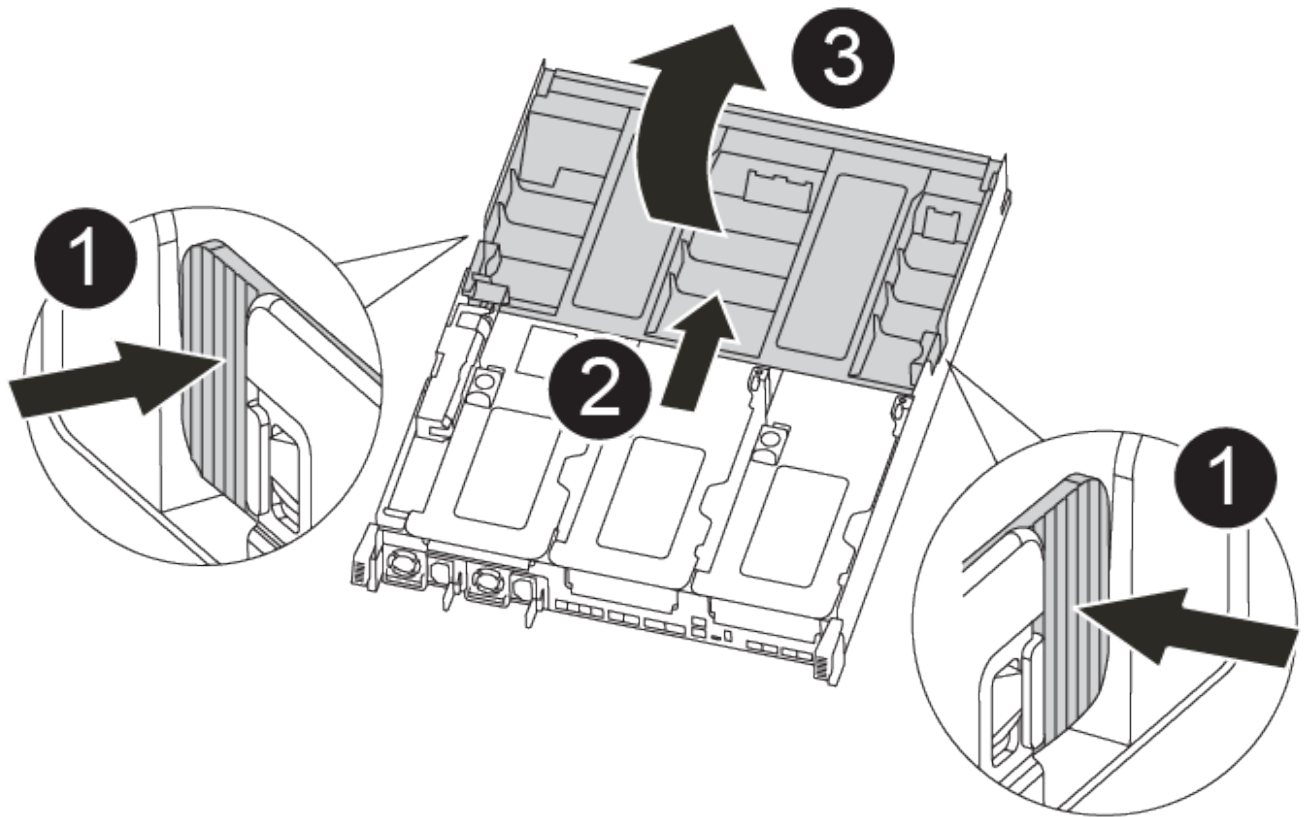
Sie müssen sich auf der NetApp Support Site anmelden, um das *Statement of Volatility* für Ihr System anzuzeigen.

Sie können die Bootmedien mit der folgenden Animation, den Abbildungen oder den schriftlichen Schritten ersetzen.

#### Animation - Ersetzen Sie das Startmedium

##### Schritte

1. Öffnen Sie den Luftkanal:



1

Verriegelungslaschen

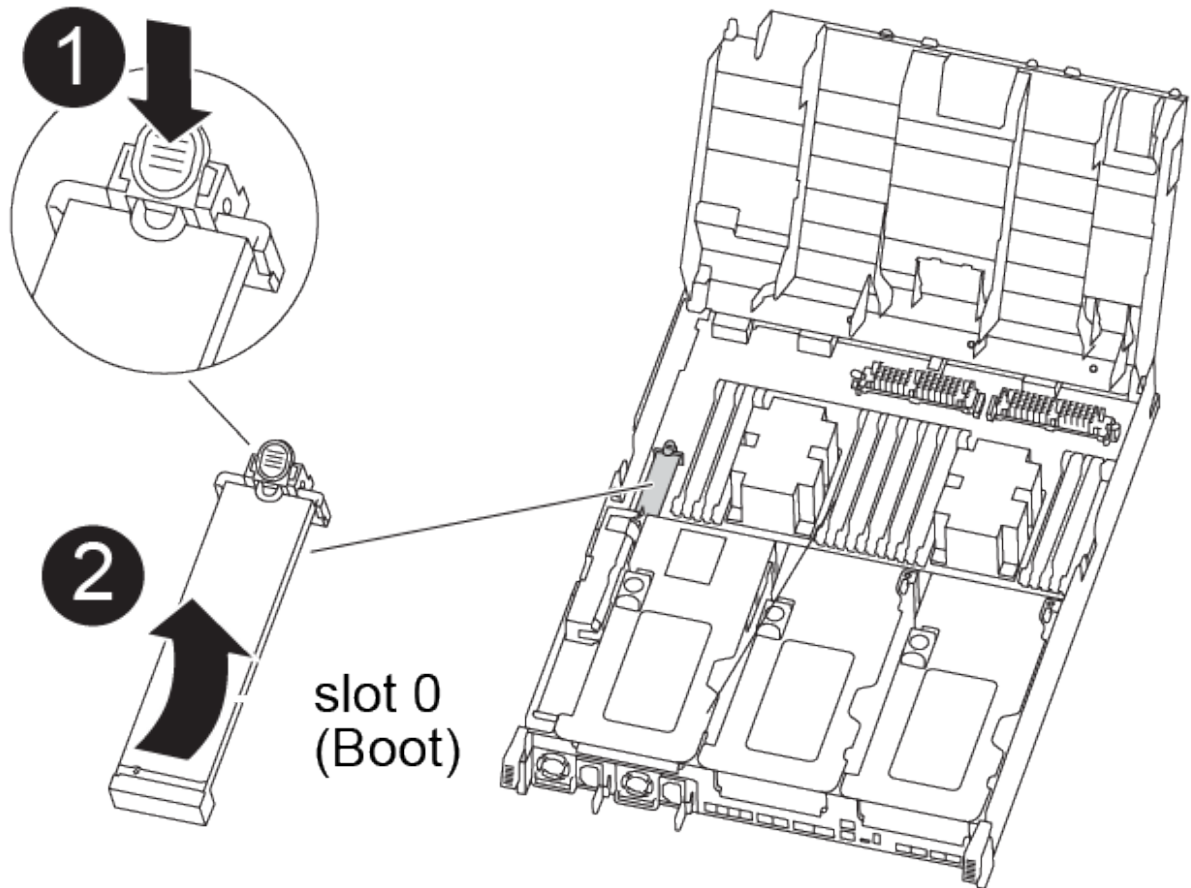
2

Schieben Sie den Luftkanal zur Rückseite der Steuerung

3

Luftkanal nach oben drehen

- a. Drücken Sie die Verriegelungslaschen an den Seiten des Luftkanals in Richtung der Mitte des Controller-Moduls.
  - b. Schieben Sie den Luftkanal zur Rückseite des Controller-Moduls, und drehen Sie ihn dann nach oben in seine vollständig geöffnete Position.
2. Suchen und entfernen Sie die Startmedien aus dem Controller-Modul:



1

Drücken Sie die blaue Taste

2

Startmedien nach oben drehen und aus dem Sockel entfernen

- a. Drücken Sie die blaue Taste am Ende des Startmediums, bis der Lip auf dem Boot-Medium die blaue Taste löscht.
  - b. Drehen Sie das Startmedium nach oben, und ziehen Sie das Startmedium vorsichtig aus dem Sockel.
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. Sperren Sie das Boot-Medium:

- a. Drehen Sie das Startmedium nach unten zur Hauptplatine.
- b. Platzieren Sie einen Finger am Ende des Startmediums mit der blauen Taste und drücken Sie das Bootmedium-Ende nach unten, um die blaue Verriegelungstaste zu berühren.
- c. Heben Sie beim Drücken auf die Startmedien die blaue Verriegelungstaste an, um die Boot-Medien zu verriegeln.

6. Schließen Sie den Luftkanal.

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

Das installierte Ersatzstartmedium verfügt nicht über ein Startabbild. Sie müssen also ein Startabbild über ein USB-Flash-Laufwerk übertragen.

#### Bevor Sie beginnen

- Sie müssen über ein USB-Flash-Laufwerk verfügen, das auf MBR/FAT32 formatiert ist und eine Kapazität von mindestens 4 GB aufweist
- Eine Kopie der gleichen Bildversion von ONTAP wie der beeinträchtigte Controller. Das entsprechende Image können Sie im Abschnitt „Downloads“ auf der NetApp Support-Website herunterladen
  - Wenn NVE aktiviert ist, laden Sie das Image mit NetApp Volume Encryption herunter, wie in der Download-Schaltfläche angegeben.
  - Wenn NVE nicht aktiviert ist, laden Sie das Image ohne NetApp Volume Encryption herunter, wie im Download-Button dargestellt.
- Wenn Ihr System ein HA-Paar ist, müssen Sie eine Netzwerkverbindung haben.
- Wenn es sich bei Ihrem System um ein eigenständiges System handelt, benötigen Sie keine Netzwerkverbindung, sondern Sie müssen beim Wiederherstellen des einen zusätzlichen Neustart durchführen `var` File-System.
  - a. Laden Sie das entsprechende Service-Image von der NetApp Support Site auf das USB-Flash-Laufwerk herunter und kopieren Sie es.
    - i. Laden Sie das Service-Image auf Ihren Arbeitsbereich auf Ihrem Laptop herunter.
    - ii. 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 Extraktionstool, wie 7-Zip oder WinRAR.

Die Image-Datei „ungezippte Dienste“ enthält zwei Ordner:

- `boot`
- `efi`

iii. Kopieren Sie die `efi` Ordner zum obersten Verzeichnis auf dem USB-Flash-Laufwerk.

Das USB-Flash-Laufwerk sollte den `efi`-Ordner und die gleiche Service Image (BIOS)-Version des beeinträchtigten Controllers haben.

- iv. Entfernen Sie das USB-Flash-Laufwerk von Ihrem Laptop.
- b. Wenn Sie dies noch nicht getan haben, schließen Sie den Luftkanal.
- c. 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.
- d. Installieren Sie das Kabelverwaltungsgerät neu und führen Sie das System nach Bedarf wieder ein.

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

- e. Schließen Sie das Netzkabel an das Netzteil an, und setzen Sie den Netzkabelhalter wieder ein.
- f. 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.

- g. Schließen Sie die Installation des Controller-Moduls ab:
  - i. Schließen Sie das Netzkabel an das Netzteil an, setzen Sie die Sicherungshülse des Netzkabels wieder ein, und schließen Sie dann das Netzteil an die Stromquelle an.
  - ii. Drücken Sie das Controller-Modul fest in das Gehäuse, bis es auf die Mittelebene trifft und vollständig sitzt.

Die Verriegelungen steigen, wenn das Controller-Modul voll eingesetzt ist.



Beim Einschieben des Controller-Moduls in das Gehäuse keine übermäßige Kraft verwenden, um Schäden an den Anschlüssen zu vermeiden.

Das Controller-Modul beginnt zu booten, sobald es vollständig im Gehäuse sitzt. Bereiten Sie sich darauf vor, den Bootvorgang zu unterbrechen.

- i. Drehen Sie die Verriegelungsriegel nach oben, und kippen Sie sie so, dass sie die Sicherungsstifte entfernen und dann in die verriegelte Position absenken.
  - ii. Wenn Sie dies noch nicht getan haben, installieren Sie das Kabelverwaltungsgerät neu.
- h. Unterbrechen Sie den Boot-Vorgang, indem Sie Strg-C drücken, um an der LOADER-Eingabeaufforderung zu stoppen.

Wenn Sie diese Meldung verpassen, drücken Sie Strg-C, wählen Sie die Option, um in den Wartungsmodus zu booten, und dann `halt` Der Controller zum Booten zu LOADER.

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

Die Änderungen werden implementiert, wenn das System gestartet wird.



# Booten des Recovery-Images – AFF FAS8300 und FAS8700

Das Verfahren zum Booten des beeinträchtigten Controllers über das Recovery-Image hängt davon ab, ob sich das System in einer MetroCluster-Konfiguration mit zwei Knoten befindet.

## Option 1: Die meisten Systeme

Sie müssen das ONTAP-Image vom USB-Laufwerk starten, das Dateisystem wiederherstellen und die Umgebungsvariablen überprüfen.

Dieses Verfahren gilt für Systeme, die sich nicht in einer MetroCluster Konfiguration mit zwei Nodes befinden.

### Schritte

1. Starten Sie von der LOADER-Eingabeaufforderung das Recovery-Image vom USB-Flash-Laufwerk:  
`boot_recovery`

Das Bild wird vom USB-Flash-Laufwerk heruntergeladen.

2. Wenn Sie dazu aufgefordert werden, geben Sie entweder den Namen des Bilds ein oder akzeptieren Sie das Standardbild, das in den Klammern auf dem Bildschirm angezeigt wird.
3. Stellen Sie die wieder her `var` Filesystem:

Wenn Ihr System...	Dann...
Eine Netzwerkverbindung	<ol style="list-style-type: none"><li>a. Drücken Sie <code>y</code> Wenn Sie aufgefordert werden, die Backup-Konfiguration wiederherzustellen.</li><li>b. Stellen Sie den gesunden Controller auf die erweiterte Berechtigungsebene ein: <code>set -privilege advanced</code></li><li>c. Führen Sie den Befehl Restore Backup aus: <code>system node restore-backup -node local -target-address <i>impaired_node_IP_address</i></code></li><li>d. Zurückkehren des Controllers zur Administratorebene: <code>set -privilege admin</code></li><li>e. Drücken Sie <code>y</code> Wenn Sie aufgefordert werden, die wiederhergestellte Konfiguration zu verwenden.</li><li>f. Drücken Sie <code>y</code> Wenn Sie dazu aufgefordert werden, den Controller neu zu booten.</li></ol>

Wenn Ihr System...	Dann...
Keine Netzwerkverbindung	<p>a. Drücken Sie <code>n</code> Wenn Sie aufgefordert werden, die Backup-Konfiguration wiederherzustellen.</p> <p>b. Starten Sie das System neu, wenn Sie dazu aufgefordert werden.</p> <p>c. Wählen Sie im angezeigten Menü die Option <b>Flash aktualisieren aus Backup config</b> (Flash synchronisieren) aus.</p> <p>Wenn Sie aufgefordert werden, mit der Aktualisierung fortzufahren, drücken Sie <code>y</code>.</p>

4. Stellen Sie sicher, dass die Umgebungsvariablen wie erwartet festgelegt sind:
  - a. Nehmen Sie den Controller zur LOADER-Eingabeaufforderung.
  - b. Überprüfen Sie die Einstellungen der Umgebungsvariable mit dem `printenv` Befehl.
  - c. Wenn eine Umgebungsvariable nicht wie erwartet festgelegt ist, ändern Sie sie mit dem `setenv environment-variable-name changed-value` Befehl.
  - d. Speichern Sie Ihre Änderungen mit dem `saveenv` Befehl.
5. Das nächste hängt von Ihrer Systemkonfiguration ab:
  - Wenn `keymanager`, `NSE` oder `NVE` in Ihrem System integriert sind, finden Sie unter [Stellen Sie OKM, NSE und NVE nach Bedarf wieder her](#)
  - Wenn `keymanager`, `NSE` oder `NVE` auf Ihrem System nicht konfiguriert sind, führen Sie die Schritte in diesem Abschnitt aus.
6. Geben Sie an der LOADER-Eingabeaufforderung das ein `boot_ontap` Befehl.

*Wenn Sie sehen...	Dann...*
Die Eingabeaufforderung für die Anmeldung	Fahren Sie mit dem nächsten Schritt fort.
Warten auf Giveback...	<p>a. Melden Sie sich beim Partner-Controller an.</p> <p>b. Überprüfen Sie, ob der Ziel-Controller bereit ist für die Rückgabe an den <code>storage failover show</code> Befehl.</p>

7. Schließen Sie das Konsolenkabel an den Partner Controller an.
8. Geben Sie den Controller mithilfe des `zurück storage failover giveback -fromnode local` Befehl.
9. Überprüfen Sie an der Cluster-Eingabeaufforderung die logischen Schnittstellen mit dem `net int -is -home false` Befehl.

Wenn Schnittstellen als „falsch“ aufgeführt sind, stellen Sie diese Schnittstellen mithilfe der `zurück auf ihren Home Port net int revert` Befehl.

10. Bewegen Sie das Konsolenkabel auf den reparierten Controller und führen Sie den `aus version -v` Befehl zum Prüfen der ONTAP-Versionen.

11. Stellen Sie die automatische Rückgabe wieder her, wenn Sie die Funktion mithilfe von deaktivieren `storage failover modify -node local -auto-giveback true` Befehl.

## Option 2: Controller befindet sich in einem MetroCluster mit zwei Nodes

Sie müssen das ONTAP-Image vom USB-Laufwerk booten und die Umgebungsvariablen überprüfen.

Dieses Verfahren gilt für Systeme in einer MetroCluster-Konfiguration mit zwei Nodes.

### Schritte

1. Starten Sie von der LOADER-Eingabeaufforderung das Recovery-Image vom USB-Flash-Laufwerk:  
`boot_recovery`

Das Bild wird vom USB-Flash-Laufwerk heruntergeladen.

2. Wenn Sie dazu aufgefordert werden, geben Sie entweder den Namen des Bilds ein oder akzeptieren Sie das Standardbild, das in den Klammern auf dem Bildschirm angezeigt wird.
3. Starten Sie nach der Installation des Images den Wiederherstellungsprozess:
  - a. Drücken Sie `n` Wenn Sie aufgefordert werden, die Backup-Konfiguration wiederherzustellen.
  - b. Drücken Sie `y` Wenn Sie aufgefordert werden, einen Neustart durchzuführen, um die neu installierte Software zu verwenden.

Sie sollten darauf vorbereitet sein, den Bootvorgang zu unterbrechen, wenn Sie dazu aufgefordert werden.

4. Drücken Sie beim Systemstart auf `Ctrl-C` Nachdem Sie den gesehen haben `Press Ctrl-C for Boot Menu` Meldung. Und wenn das Startmenü angezeigt wird, wählen Sie Option 6.
5. Vergewissern Sie sich, dass die Umgebungsvariablen wie erwartet festgelegt sind.
  - a. Nehmen Sie den Node zur LOADER-Eingabeaufforderung.
  - b. Überprüfen Sie die Einstellungen der Umgebungsvariable mit dem `printenv` Befehl.
  - c. Wenn eine Umgebungsvariable nicht wie erwartet festgelegt ist, ändern Sie sie mit dem `setenv environment-variable-name changed-value` Befehl.
  - d. Speichern Sie Ihre Änderungen mit dem `saveenv` Befehl.
  - e. Booten Sie den Node neu.

## Schalten Sie Aggregate in einer MetroCluster Konfiguration mit zwei Nodes zurück – AFF fas8300 und FAS8700

Nachdem Sie in einer MetroCluster Konfiguration mit zwei Nodes den FRU-Austausch abgeschlossen haben, können Sie den MetroCluster SwitchBack-Vorgang durchführen. Damit wird die Konfiguration in ihren normalen Betriebszustand zurückversetzt, wobei die Synchronisations-Storage Virtual Machines (SVMs) auf dem ehemals beeinträchtigten Standort jetzt aktiv sind und Daten aus den lokalen Festplattenpools bereitstellen.

Dieser Task gilt nur für MetroCluster-Konfigurationen mit zwei Nodes.

## Schritte

1. Vergewissern Sie sich, dass sich alle Nodes im befinden enabled Bundesland: `metrocluster node show`

```
cluster_B::> metrocluster node show

DR                               Configuration  DR
Group Cluster Node              State          Mirroring Mode
-----
1      cluster_A
      controller_A_1 configured      enabled    heal roots
completed
      cluster_B
      controller_B_1 configured      enabled    waiting for
switchback recovery
2 entries were displayed.
```

2. Überprüfen Sie, ob die Neusynchronisierung auf allen SVMs abgeschlossen ist: `metrocluster vserver show`
3. Überprüfen Sie, ob die automatischen LIF-Migrationen durch die heilenden Vorgänge erfolgreich abgeschlossen wurden: `metrocluster check lif show`
4. Führen Sie den Wechsel zurück mit dem aus `metrocluster switchback` Befehl von einem beliebigen Node im verbleibenden Cluster
5. Stellen Sie sicher, dass der Umkehrvorgang abgeschlossen ist: `metrocluster show`

Der Vorgang zum zurückwechseln wird weiterhin ausgeführt, wenn sich ein Cluster im befindet `waiting-for-switchback` Bundesland:

```
cluster_B::> metrocluster show
Cluster              Configuration State      Mode
-----
Local: cluster_B configured      switchover
Remote: cluster_A configured      waiting-for-switchback
```

Der Vorgang zum zurückwechseln ist abgeschlossen, wenn sich die Cluster im befinden `normal` Bundesland:

```
cluster_B::> metrocluster show
Cluster              Configuration State      Mode
-----
Local: cluster_B configured      normal
Remote: cluster_A configured      normal
```

Wenn ein Wechsel eine lange Zeit in Anspruch nimmt, können Sie den Status der in-progress-Basispläne über die überprüfen `metrocluster config-replication resync-status show` Befehl.

6. Wiederherstellung beliebiger SnapMirror oder SnapVault Konfigurationen

## Stellen Sie OKM, NSE und NVE nach Bedarf wieder her – AFF fas8300 und FAS8700

Sobald Umgebungsvariablen geprüft werden, müssen Sie spezifische Schritte für Systeme mit aktiviertem Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) oder NetApp Volume Encryption (NVE) durchführen.

1. Bestimmen Sie den Abschnitt, den Sie zum Wiederherstellen Ihrer OKM-, NSE- oder NVE-Konfigurationen verwenden sollten: Wenn NSE oder NVE zusammen mit Onboard Key Manager aktiviert sind, müssen Sie die zu Beginn dieses Verfahrens erfassten Einstellungen wiederherstellen.
  - Wenn NSE oder NVE aktiviert sind und der Onboard Key Manager aktiviert ist, wechseln Sie zu [wenn Onboard Key Manager aktiviert ist](#).
  - Wenn NSE oder NVE für ONTAP 9.6 aktiviert sind, finden Sie unter [Stellen Sie NSE/NVE auf Systemen mit ONTAP 9.6 und höher wieder her](#).

### Stellen Sie NVE oder NSE wieder her, wenn Onboard Key Manager aktiviert ist

#### Schritte

1. Schließen Sie das Konsolenkabel an den Ziel-Controller an.
2. Verwenden Sie die `boot_ontap` Befehl an der LOADER-Eingabeaufforderung zum Booten des Controllers.
3. Überprüfen Sie die Konsolenausgabe:

Wenn die Konsole angezeigt wird...	Dann...
Die LOADER-Eingabeaufforderung	Starten des Controllers zum Boot-Menü: <code>boot_ontap menu</code>
Warten auf Zurückgeben	<ol style="list-style-type: none"> <li>a. Eingabe <code>Ctrl-C</code> An der Eingabeaufforderung</li> <li>b. Bei der Meldung: <code>Möchten Sie diesen Knoten anhalten, anstatt [y/n] zu warten?</code> , Geben Sie ein: <code>y</code></li> <li>c. Geben Sie an der LOADER-Eingabeaufforderung den ein <code>boot_ontap menu</code> Befehl.</li> </ol>

4. Geben Sie im Startmenü den verborgenen Befehl ein. `recover_onboard_keymanager` Und antworten `y` An der Eingabeaufforderung
5. Geben Sie die Passphrase für das Onboard-Schlüsselmanagement ein, das Sie zu Beginn dieses Verfahrens vom Kunden erhalten haben.
6. Wenn Sie zur Eingabe der Sicherungsdaten aufgefordert werden, fügen Sie die zu Beginn dieses Verfahrens erfassten Sicherungsdaten ein, wenn Sie dazu aufgefordert werden. Fügen Sie die Ausgabe

von ein security key-manager backup show ODER security key-manager onboard show-backup Befehl



Die Daten werden von beiden ausgegeben security key-manager backup show Oder security key-manager onboard show-backup Befehl.

Beispiel für Backup-Daten:

```
----- BACKUP-----  
TmV0QXBwIETERTABCbGaiAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA . .  
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
  
----- END-BACKUP-----
```

7. Wählen Sie im Startmenü die Option Normal Boot aus.

Das System startet zum Warten auf Giveback... Eingabeaufforderung.

8. Stellen Sie das Konsolenkabel auf den Partner Controller um und melden Sie sich als „admin“ an.

9. Überprüfen Sie, ob der Ziel-Controller bereit ist für die Rückgabe an den storage failover show Befehl.

10. GiveBack nur der CFO sammelt mit dem storage failover giveback -fromnode local -only -cfo-aggregates true Befehl.

- Wenn der Befehl aufgrund eines ausgefallenen Laufwerks ausfällt, setzen Sie die ausgefallene Festplatte physisch aus, lassen Sie sie aber in den Steckplatz, bis ein Austausch erfolgt.
- Wenn der Befehl aufgrund von offenen CIFS-Sitzungen ausfällt, wenden Sie sich an den Kunden, wie CIFS-Sitzungen abgeschlossen werden können.



Die Beendigung von CIFS kann zu Datenverlust führen.

- Wenn der Befehl fehlschlägt, weil der Partner „nicht bereit“ ist, warten Sie 5 Minuten, bis die NVMEMs synchronisiert werden.
- Wenn der Befehl aufgrund eines NDMP-, SnapMirror- oder SnapVault-Prozesses ausfällt, deaktivieren Sie den Prozess. Weitere Informationen finden Sie im entsprechenden Documentation Center.

11. Sobald die Rückgabe abgeschlossen ist, überprüfen Sie den Failover- und Giveback-Status mit storage failover show Und `storage failover show-GiveBack`-Befehle.

Es werden nur die CFO-Aggregate (Root-Aggregate und Daten-Aggregate im CFO-Stil) angezeigt.

12. Schieben Sie das Konsolenkabel auf den Ziel-Controller.

- a. Wenn Sie ONTAP 9.6 oder höher verwenden, führen Sie die integrierte Synchronisierung des Security Key-Managers aus:

- b. Führen Sie die aus `security key-manager onboard sync` Geben Sie bei der entsprechenden Aufforderung die Passphrase ein.
- c. Geben Sie das ein `security key-manager key query` Befehl zum Anzeigen einer detaillierten Ansicht aller im Onboard-Schlüsselmanager gespeicherten Schlüssel und zur Überprüfung des `Restored` Spalte = `yes/true` Für alle Authentifizierungsschlüssel.



Wenn der `Restored` Spalte = nichts anderes als `yes/true`, Wenden Sie sich an den Kundendienst.

- d. Warten Sie 10 Minuten, bis der Schlüssel über das Cluster synchronisiert wird.
- 13. Stellen Sie das Konsolenkabel auf den Partner Controller um.
- 14. Geben Sie den Ziel-Controller mithilfe des zurück `storage failover giveback -fromnode local` Befehl.
- 15. Überprüfen Sie den Giveback-Status, 3 Minuten nachdem Berichte abgeschlossen wurden, mithilfe von `storage failover show` Befehl.

Falls das Giveback nach 20 Minuten nicht abgeschlossen ist, wenden Sie sich an den Kundendienst.

- 16. Geben Sie an der Clustershell-Eingabeaufforderung den ein `net int show -is-home false` Befehl zum Auflistung der logischen Schnittstellen, die sich nicht auf ihrem Home Controller und Port befinden.

Wenn Schnittstellen als aufgeführt werden `false`, Zurücksetzen dieser Schnittstellen zurück zu ihrem Home-Port mit dem `net int revert` Befehl.

- 17. Bewegen Sie das Konsolenkabel auf den Ziel-Controller, und führen Sie den aus `version -v` Befehl zum Prüfen der ONTAP-Versionen.
- 18. Stellen Sie die automatische Rückgabe wieder her, wenn Sie die Funktion mithilfe von deaktivieren `storage failover modify -node local -auto-giveback true` Befehl.

## Stellen Sie NSE/NVE auf Systemen mit ONTAP 9.6 und höher wieder her

### Schritte

- 1. Schließen Sie das Konsolenkabel an den Ziel-Controller an.
- 2. Verwenden Sie die `boot_ontap` Befehl an der LOADER-Eingabeaufforderung zum Booten des Controllers.
- 3. Überprüfen Sie die Konsolenausgabe:

Wenn die Konsole angezeigt wird...	Dann...
Die Eingabeaufforderung für die Anmeldung	Fahren Sie mit Schritt 7 fort.
Warten auf Giveback...	<ul style="list-style-type: none"> <li>a. Melden Sie sich beim Partner-Controller an.</li> <li>b. Überprüfen Sie, ob der Ziel-Controller bereit ist für die Rückgabe an den <code>storage failover show</code> Befehl.</li> </ul>

- 4. Bewegen Sie das Konsolenkabel zum Partner-Controller und geben Sie den Ziel-Controller-Storage

mithilfe des zurück `storage failover giveback -fromnode local -only-cfo-aggregates true local` Befehl.

- Wenn der Befehl aufgrund eines ausgefallenen Laufwerks ausfällt, setzen Sie die ausgefallene Festplatte physisch aus, lassen Sie sie aber in den Steckplatz, bis ein Austausch erfolgt.
- Wenn der Befehl aufgrund von offenen CIFS-Sitzungen ausfällt, wenden Sie sich an den Kunden, wie CIFS-Sitzungen abgeschlossen werden können.



Die Beendigung von CIFS kann zu Datenverlust führen.

- Wenn der Befehl fehlschlägt, weil der Partner „nicht bereit“ ist, warten Sie 5 Minuten, bis die NVMEMs synchronisiert werden.
- Wenn der Befehl aufgrund eines NDMP-, SnapMirror- oder SnapVault-Prozesses ausfällt, deaktivieren Sie den Prozess. Weitere Informationen finden Sie im entsprechenden Documentation Center.

5. Warten Sie 3 Minuten, und überprüfen Sie den Failover-Status mit `storage failover show` Befehl.
6. Geben Sie an der Clustershell-Eingabeaufforderung den ein `net int show -is-home false` Befehl zum Auflistung der logischen Schnittstellen, die sich nicht auf ihrem Home Controller und Port befinden.

Wenn Schnittstellen als aufgeführt werden `false`, Zurücksetzen dieser Schnittstellen zurück zu ihrem Home-Port mit dem `net int revert` Befehl.

7. Bewegen Sie das Konsolenkabel auf den Ziel-Controller, und führen Sie den aus `version -v` Befehl zum Prüfen der ONTAP-Versionen.
8. Stellen Sie die automatische Rückgabe wieder her, wenn Sie die Funktion mithilfe von deaktivieren `storage failover modify -node local -auto-giveback true` Befehl.
9. Verwenden Sie die `storage encryption disk show` An der clustershell-Eingabeaufforderung zur Überprüfung der Ausgabe.
10. Verwenden Sie die `security key-manager key query` Befehl zum Anzeigen der Schlüssel-IDs der Authentifizierungsschlüssel, die auf den Schlüsselverwaltungsservern gespeichert sind.
  - Wenn der `Restored` Spalte = `yes/true`, Sie sind fertig und können den Austauschprozess abschließen.
  - Wenn der `Key Manager type` = `external` Und das `Restored` Spalte = nichts anderes als `yes/true`, Verwenden Sie die `security key-manager external restore` Befehl zum Wiederherstellen der Schlüssel-IDs der Authentifizierungsschlüssel.



Falls der Befehl fehlschlägt, wenden Sie sich an den Kundendienst.

- Wenn der `Key Manager type` = `onboard` Und das `Restored` Spalte = nichts anderes als `yes/true`, Verwenden Sie die `security key-manager onboard sync` Befehl zum erneuten Synchronisieren des Key Manager-Typs.

Verwenden Sie die `security key-manager key query` Befehl zum Überprüfen des `Restored` Spalte = `yes/true` Für alle Authentifizierungsschlüssel.

11. Schließen Sie das Konsolenkabel an den Partner Controller an.
12. Geben Sie den Controller mithilfe des zurück `storage failover giveback -fromnode local` Befehl.



13. Stellen Sie die automatische Rückgabe wieder her, wenn Sie die Funktion mithilfe von deaktivieren `storage failover modify -node local -auto-giveback true` Befehl.

## **Das ausgefallene Teil an NetApp – AFF fas8300 und FAS8700 – zurücksenden**

Senden Sie das fehlerhafte Teil wie in den dem Kit beiliegenden RMA-Anweisungen beschrieben an NetApp zurück. Siehe "[Teilerückgabe Austausch](#)" Seite für weitere Informationen.

## Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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, BEISPIELHAFT 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.