Boot-Medien

Install and maintain

NetApp
December 18, 2024

Inhalt

Boot-Medien

Überblick über den Austausch von Boot-Medien – FAS2820

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.

Prüfen Sie Support und Status der Verschlüsselungsschlüssel - FAS2820

Überprüfen Sie vor dem Herunterfahren des beeinträchtigten Controllers, ob Ihre Version von ONTAP NetApp Volume Encryption (NVE) unterstützt und ob Ihr Verschlüsselungsmanagement-System ordnungsgemäß konfiguriert ist.

Schritt: Prüfen Sie, ob Ihre Version von ONTAP NetApp-Volume-Verschlüsselung unterstützt

Prüfen Sie, ob Ihre ONTAP Version NetApp Volume Encryption (NVE) unterstützt. Diese Informationen sind entscheidend, um das richtige ONTAP-Image herunterzuladen.

1. Stellen Sie fest, ob Ihre ONTAP-Version Verschlüsselung unterstützt, indem Sie den folgenden Befehl ausführen:

   ```
   version -v
   ```

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

2. Je nachdem, ob NVE auf Ihrem System unterstützt wird, führen Sie eine der folgenden Aktionen durch:
   - Falls 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-Verschlüsselung herunter.

Schritt 2: Stellen Sie fest, ob es sicher ist, den Controller herunterzufahren

Um einen Controller sicher herunterzufahren, müssen Sie zuerst ermitteln, ob der External Key Manager (EKM) oder der Onboard Key Manager (OKM) aktiv ist. Überprüfen Sie anschließend den verwendeten Schlüsselmanager, zeigen Sie die entsprechenden Schlüsselinformationen an und ergreifen Sie Maßnahmen, die auf dem Status der Authentifizierungsschlüssel basieren.

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

ONTAP-Version	Führen Sie diesen Befehl aus
ONTAP 9.14.1 oder höher	`security key-manager keystore show` • Wenn EKM aktiviert ist, `EKM` wird in der Befehlsausgabe aufgelistet. • Wenn OKM aktiviert ist, `OKM` wird in der Befehlsausgabe aufgelistet. • Wenn kein Schlüsselmanager aktiviert ist, `No key manager keystores configured` wird in der Befehlsausgabe aufgeführt.
ONTAP 9.13.1 oder früher	`security key-manager show-key-store` • Wenn EKM aktiviert ist, `external` wird in der Befehlsausgabe aufgelistet. • Wenn OKM aktiviert ist, `onboard` wird in der Befehlsausgabe aufgelistet. • Wenn kein Schlüsselmanager aktiviert ist, `No key managers configured` wird in der Befehlsausgabe aufgeführt.

2. Wählen Sie eine der folgenden Optionen, je nachdem, ob ein Key Manager auf Ihrem System konfiguriert ist.

Kein Schlüsselmanager konfiguriert

Sie können den außer Betrieb genommenen Controller sicher herunterfahren. Gehen Sie zu "Schalten Sie den außer Betrieb genommenen Controller aus".

Externer oder integrierter Schlüsselmanager konfiguriert

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 für den Wert in der `Restored` Spalte für Ihren Schlüsselmanager.

Diese Spalte gibt an, ob die Authentifizierungsschlüssel für Ihren Schlüsselmanager (entweder EKM oder OKM) erfolgreich wiederhergestellt wurden.

3. Wählen Sie je nachdem, ob Ihr System den External Key Manager oder den Onboard Key Manager verwendet, eine der folgenden Optionen aus.

Externer Schlüsselmanager

Befolgen Sie je nach dem in der Spalte angezeigten Ausgangswert `Restored` die entsprechenden Schritte.

Ausgabewert in `Restored` Spalte	**Führen Sie die folgenden Schritte aus…**
`true`	Sie können den außer Betrieb genommenen Controller sicher herunterfahren. Gehen Sie zu "Schalten Sie den außer Betrieb genommenen Controller aus".
Alles andere als `true`	a. Stellen Sie die externen Authentifizierungsschlüssel für das Verschlüsselungsmanagement auf allen Nodes im Cluster mit dem folgenden Befehl wieder her: `security key-manager external restore` Wenn der Befehl fehlschlägt, wenden Sie sich an "NetApp Support". b. Überprüfen Sie, ob in der `Restored` Spalte für alle Authentifizierungsschlüssel die angezeigt werden `true`, indem Sie den Befehl eingeben `security key-manager key query`. Wenn alle Authentifizierungsschlüssel vorhanden sind `true`, können Sie den beeinträchtigten Controller sicher herunterfahren. Gehen Sie zu "Schalten Sie den außer Betrieb genommenen Controller aus".

Onboard Key Manager

Befolgen Sie je nach dem in der Spalte angezeigten Ausgangswert `Restored` die entsprechenden Schritte.

Ausgabewert in `Restored` Spalte	**Führen Sie die folgenden Schritte aus…**
`true`	Sichern Sie die OKM-Informationen manuell. a. Wechseln Sie in den erweiterten Modus, indem `set -priv advanced` Sie aufrufen und dann bei Aufforderung eingeben `Y`. b. Geben Sie den folgenden Befehl ein, um die Informationen zum Verschlüsselungsmanagement 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. Sie können den außer Betrieb genommenen Controller sicher herunterfahren. Gehen Sie zu "Schalten Sie den außer Betrieb genommenen Controller aus".

Ausgabewert in `Restored` Spalte	**Führen Sie die folgenden Schritte aus…**

Alles andere als `true`	a. Geben Sie den integrierten Sicherheitsschlüssel-Manager Sync-Befehl ein:
	
	`security key-manager onboard sync`
	
	b. Geben Sie bei Aufforderung die 32-stellige alphanumerische Passphrase für das Onboard-Verschlüsselungsmanagement ein.
	
	Wenn die Passphrase nicht angegeben werden kann, wenden Sie sich an "NetApp Support".
	
	c. Überprüfen Sie, ob die `Restored` Spalte für alle Authentifizierungsschlüssel angezeigt wird `true`:
	
	`security key-manager key query`
	
	d. Überprüfen Sie, ob der `Key Manager` Typ , anzeigt `onboard`und sichern Sie die OKM-Informationen manuell.
	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. Sie können den außer Betrieb genommenen Controller sicher herunterfahren. Gehen Sie zu "Schalten Sie den außer Betrieb genommenen Controller aus".

Fahren Sie den beeinträchtigten Controller herunter - FAS2820

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

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: `storage failover takeover -ofnode impaired_node_name` Wenn der Regler „beeinträchtigt“ auf Zurückgeben wartet… anzeigt, drücken Sie Strg-C, und antworten Sie dann `y`.

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

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

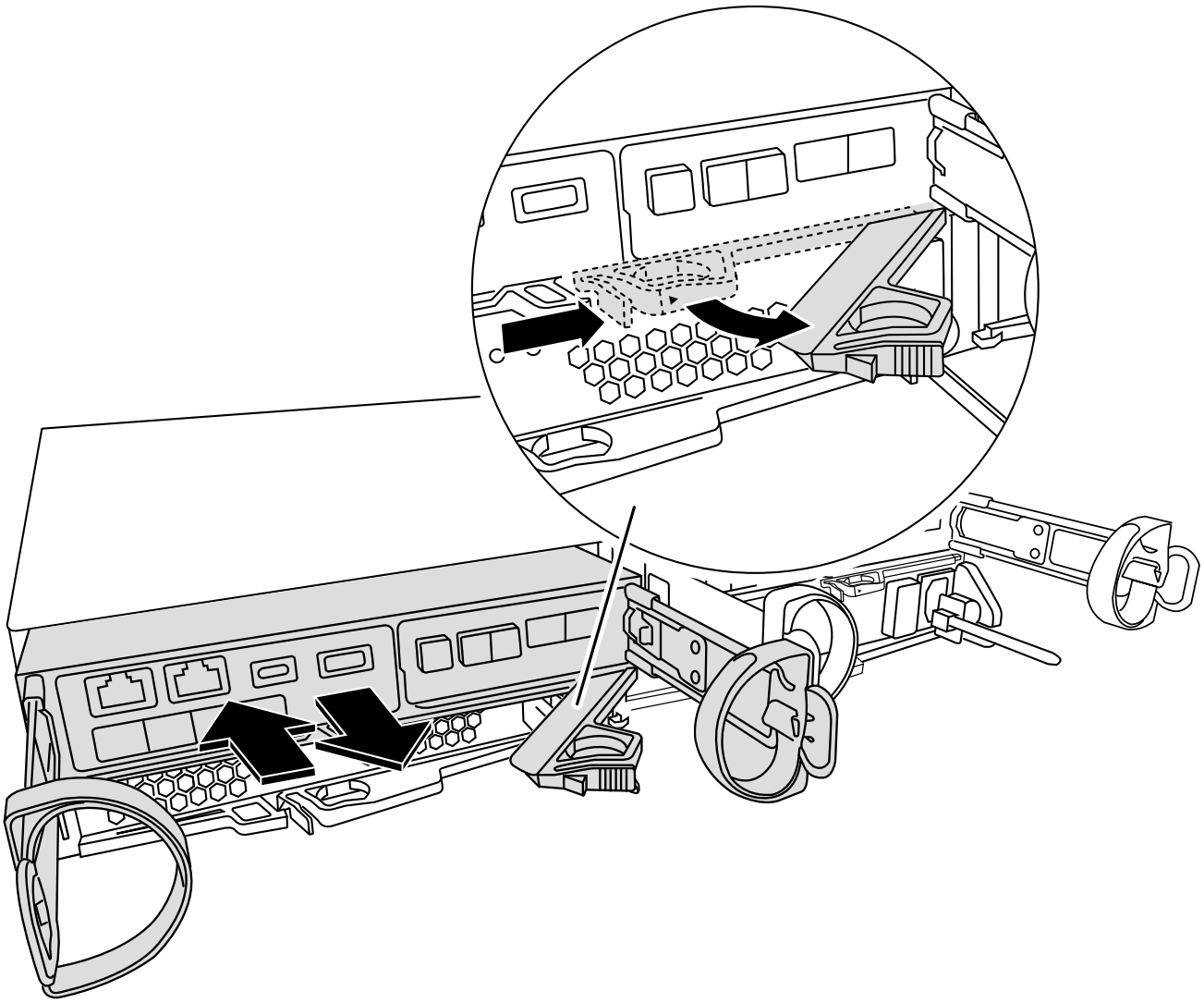
Ersetzen Sie das Boot-Medium - FAS2820

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

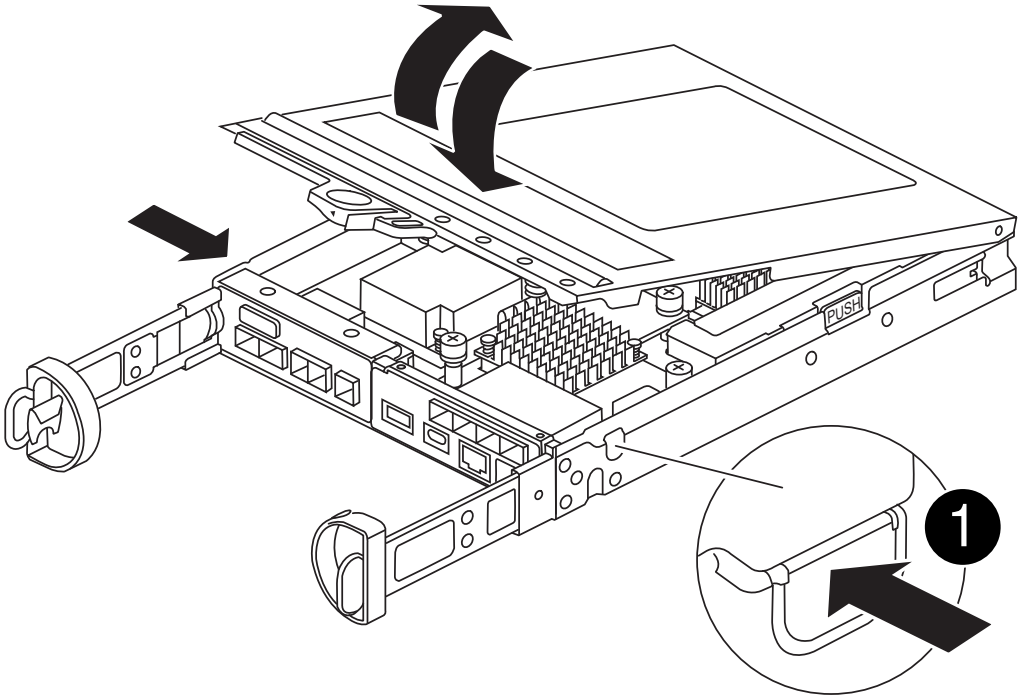
Schritt 1: Entfernen Sie das Controller-Modul

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

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



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

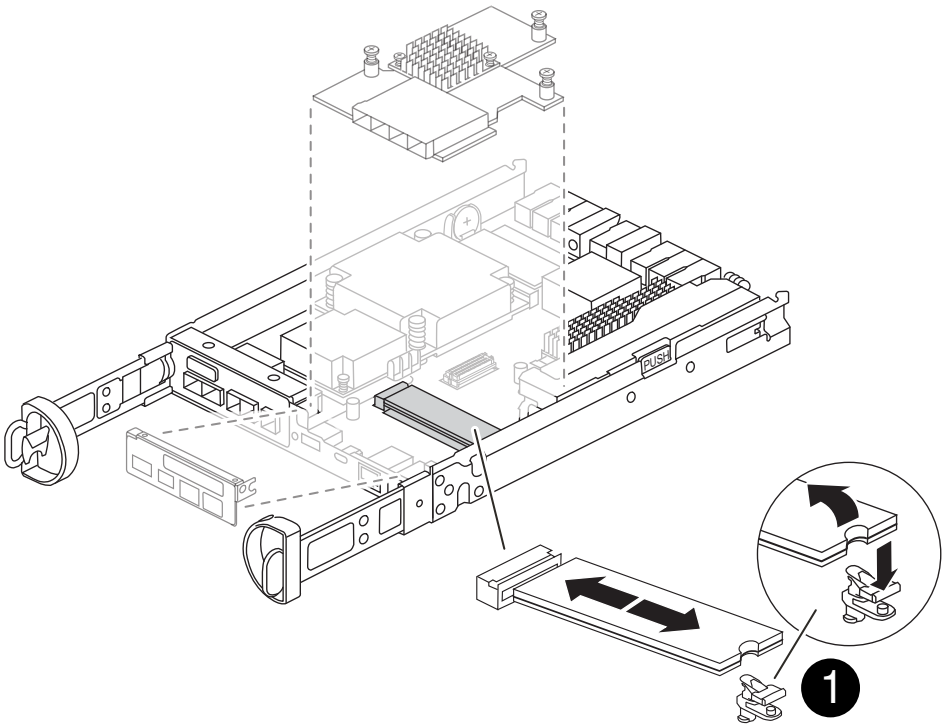


1	Entriegelungstaste der Steuermodulabdeckung

Schritt 2: Ersetzen Sie die Startmedien

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

Animation - Ersetzen Sie das Startmedium



1	Verriegelungslasche für Startmedien

Schritte

1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
2. Entfernen Sie die Mezzanine-Karte mithilfe der folgenden Abbildung oder der FRU-Zuordnung auf dem Controller-Modul:
   a. Entfernen Sie die E/A-Platte, indem Sie sie gerade aus dem Controller-Modul herausschieben.
   b. Lösen Sie die Rändelschrauben auf der Zusatzkarte.

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

   c. Heben Sie die Zusatzkarte gerade nach oben.
3. Ersetzen Sie die Startmedien:
   a. Drücken Sie die blaue Taste am Startmediengehäuse, um die Startmedien aus dem Gehäuse zu lösen, drehen Sie die Startmedien nach oben und ziehen Sie sie dann vorsichtig gerade aus dem Startmediensockel.

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

   b. Richten Sie die Kanten des Ersatzstartmediums an der Buchse des Boot-Mediums aus, und schieben Sie ihn dann vorsichtig in die Buchse. Überprüfen Sie die Startmedien, um sicherzustellen, dass sie korrekt und vollständig in den Sockel eingesetzt sind. Entfernen Sie gegebenenfalls die Startmedien, und setzen Sie sie wieder in den Sockel ein.
   c. Drücken Sie die blaue Verriegelungstaste, drehen Sie das Startmedium ganz nach unten, und lassen Sie dann die Verriegelungstaste los, um das Startmedium zu verriegeln.
4. Setzen Sie die Zusatzkarte wieder ein:
   a. Richten Sie den Sockel auf der Hauptplatine mit dem Sockel auf der Zusatzkarte aus, und setzen Sie die Karte vorsichtig in den Sockel ein.
   b. Ziehen Sie die drei Rändelschrauben auf der Zusatzkarte fest.
   c. Setzen Sie die E/A-Platte wieder ein.
5. Setzen Sie die Abdeckung des Controller-Moduls wieder ein, und verriegeln Sie sie.

Schritt 3: Übertragen Sie das Startabbild auf das Startmedium

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

Bevor Sie beginnen

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

Schritte

1. Laden Sie die entsprechende Bildversion von ONTAP auf das formatierte USB-Flash-Laufwerk herunter:
   a. Nutzung "So stellen Sie fest, ob die laufende ONTAP-Version NetApp Volume Encryption (NVE) unterstützt" Um festzustellen, ob die Volume-Verschlüsselung derzeit unterstützt wird.
      - Wenn NVE auf dem Cluster unterstützt wird, laden Sie das Image mit NetApp Volume Encryption herunter.
      - Wenn NVE nicht auf dem Cluster unterstützt wird, laden Sie das Image ohne NetApp Volume Encryption herunter. Siehe "Welches ONTAP Image sollte ich herunterladen? Mit oder ohne Volume-Verschlüsselung?" Entnehmen.
2. Entpacken Sie das heruntergeladene Bild.

   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`
     i. 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.

     ii. Entfernen Sie das USB-Flash-Laufwerk von Ihrem Laptop.
3. Installieren Sie das Controller-Modul:
   a. Richten Sie das Ende des Controller-Moduls an der Öffnung im Gehäuse aus, und drücken Sie dann vorsichtig das Controller-Modul zur Hälfte in das System.
   b. Controller-Modul wieder einsetzen.

      Denken Sie beim Neuinstallieren der Medienkonverter (SFPs) daran, wenn sie entfernt wurden.
4. Stecken Sie das USB-Flash-Laufwerk in den USB-Steckplatz des Controller-Moduls.

   Stellen Sie sicher, dass Sie das USB-Flash-Laufwerk in den für USB-Geräte gekennzeichneten Steckplatz und nicht im USB-Konsolenport installieren.
5. Drücken Sie das Controller-Modul ganz in das System, vergewissern Sie sich, dass der Nockengriff das USB-Flash-Laufwerk löscht, drücken Sie den Nockengriff fest, um den Sitz des Controller-Moduls zu beenden, schieben Sie den Nockengriff in die geschlossene Position und ziehen Sie die Daumenschraube fest.

   Der Controller beginnt 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 Systeme mit einem Controller im Chassis vorhanden sind, schließen Sie das Netzteil wieder an und

schalten Sie die Netzteile ein.

Das System beginnt mit dem Booten und wird bei DER LOADER-Eingabeaufforderung angehalten.

8. Legen Sie den Verbindungstyp für das Netzwerk an der LOADER-Eingabeaufforderung fest:

   ◦ Wenn Sie DHCP konfigurieren: `ifconfig e0a -auto`

   > Der von Ihnen konfigurierte Zielport ist der Zielport, über den Sie während der Wiederherstellung des var-Dateisystems mit dem beeinträchtigten Controller über den gesunden Controller kommunizieren. Sie können in diesem Befehl auch den Port E0M verwenden.

   ◦ Wenn Sie manuelle Verbindungen konfigurieren: `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`

   - Filer_addr ist die IP-Adresse des Speichersystems.
   - Netmask ist die Netzwerkmaske des Managementnetzwerks, das mit dem HA-Partner verbunden ist.
   - Das Gateway ist das Gateway für das Netzwerk.
   - dns_addr ist die IP-Adresse eines Namensservers in Ihrem Netzwerk.
   - die dns_Domain ist der Domain Name des Domain Name System (DNS).

     Wenn Sie diesen optionalen Parameter verwenden, benötigen Sie keinen vollqualifizierten Domänennamen in der Netzboot-Server-URL. Sie benötigen nur den Hostnamen des Servers.

   > Andere Parameter können für Ihre Schnittstelle erforderlich sein. Sie können eingeben `help ifconfig` Details finden Sie in der Firmware-Eingabeaufforderung.

Starten Sie das Recovery-Image – FAS2820

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

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 das var-Dateisystem wieder her:

Option 1: ONTAP 9.16.0 oder früher

a. Drücken Sie auf der außer Betrieb genommenen Steuerung `Y`, wenn angezeigt wird `Do you want to restore the backup configuration now?`

b. Drücken Sie auf dem Controller für beeinträchtigte Störungen `Y`, wenn Sie dazu aufgefordert werden, */etc/ssh/ssh_Host_ecdsa_Key* zu überschreiben.

c. Setzen Sie auf dem funktionierenden Partner-Controller den beeinträchtigten Controller auf die erweiterte Berechtigungsebene: `set -privilege advanced`.

d. Führen Sie auf dem gesunden Partner-Controller den Wiederherstellungsbefehl aus: `system node restore-backup -node local -target-address impaired_node_IP_address` .

   HINWEIS: Wenn Sie eine andere Nachricht als eine erfolgreiche Wiederherstellung sehen, kontaktieren Sie "NetApp Support".

e. Setzen Sie auf dem gesunden Partner-Controller den beeinträchtigten Controller auf Admin-Ebene zurück: `set -privilege admin`.

f. Drücken Sie auf der außer Betrieb genommenen Steuerung `Y`, wenn angezeigt wird `Was the restore backup procedure successful?`.

g. Drücken Sie auf der außer Betrieb genommenen Steuerung `Y`, wenn angezeigt wird `...would you like to use this restored copy now?`.

h. Drücken Sie auf dem Controller für beeinträchtigte `Y` Störungen, wenn Sie dazu aufgefordert werden, den Controller für beeinträchtigte Störungen neu zu starten, und drücken Sie `ctrl-c` für das Startmenü.

i. Wenn das System keine Verschlüsselung verwendet, wählen Sie *Option 1 Normal Boot.*, andernfalls gehen Sie zu "Wiederherstellung der Verschlüsselung".

Option 2: ONTAP 9.16.1 oder höher

a. Drücken Sie auf dem Controller für beeinträchtigte `Y` Vorgänge, wenn Sie dazu aufgefordert werden, die Sicherungskonfiguration wiederherzustellen.

   Nachdem der Wiederherstellungsvorgang erfolgreich war, wird diese Meldung auf der Konsole - angezeigt `syncflash_partner: Restore from partner complete`.

b. Drücken Sie auf dem Controller für beeinträchtigte `Y` Vorgänge, wenn Sie dazu aufgefordert werden, um zu bestätigen, ob die Wiederherstellung erfolgreich war.

c. Drücken Sie auf dem Controller für beeinträchtigte Störungen `Y`, wenn Sie dazu aufgefordert werden, die wiederhergestellte Konfiguration zu verwenden.

d. Drücken Sie auf dem Controller für beeinträchtigte Störungen `Y` bei der Aufforderung, um den Node neu zu booten.

e. Drücken Sie auf dem Controller für beeinträchtigte `Y` Störungen, wenn Sie dazu aufgefordert werden, den Controller für beeinträchtigte Störungen neu zu starten, und drücken Sie `ctrl-c` für das Startmenü.

f. Wenn das System keine Verschlüsselung verwendet, wählen Sie *Option 1 Normal Boot.*, andernfalls gehen Sie zu "Wiederherstellung der Verschlüsselung".

4. Schließen Sie das Konsolenkabel an den Partner Controller an.
5. Geben Sie den Controller mithilfe des zurück `storage failover giveback -fromnode local` Befehl.
6. Stellen Sie die automatische Rückgabe wieder her, wenn Sie die Funktion mithilfe von deaktivieren `storage failover modify -node local -auto-giveback true` Befehl.
7. Wenn AutoSupport aktiviert ist, können Sie die automatische Fallerstellung mit dem Befehl wiederherstellen/zurücknehmen. `system node autosupport invoke -node * -type all -message MAINT=END`

   HINWEIS: Wenn der Prozess fehlschlägt, kontaktieren Sie "NetApp Support".

Wiederherstellung der Verschlüsselung – FAS2820

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

Sie müssen die Schritte speziell für Systeme mit aktiviertem Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) oder NetApp Volume Encryption (NVE) anhand der Einstellungen abschließen, die Sie zu Beginn des Austauschvorgangs des Boot-Mediums erfasst haben.

Je nachdem, welcher Key Manager auf Ihrem System konfiguriert ist, wählen Sie eine der folgenden Optionen aus, um ihn im Startmenü wiederherzustellen.

- "Option 1: Wiederherstellen der Onboard Key Manager-Konfiguration"
- "Option 2: Wiederherstellung der Konfiguration des externen Schlüsselmanagers"

Option 1: Wiederherstellen der Onboard Key Manager-Konfiguration

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

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie beim Wiederherstellen der OKM-Konfiguration folgende Informationen haben:
  - Cluster-weite Passphrase eingegeben "Und ermöglicht integriertes Verschlüsselungsmanagement".
  - "Backup-Informationen für den Onboard Key Manager".
- Führen Sie das "Verifizierung von Onboard-Verschlüsselungsmanagement-Backup und Cluster-weiter Passphrase" Verfahren durch, bevor Sie fortfahren.

Schritte

1. Schließen Sie das Konsolenkabel an den Ziel-Controller an.
2. Wählen Sie im ONTAP-Startmenü die entsprechende Option aus dem Startmenü aus.

ONTAP-Version	Wählen Sie diese Option aus
ONTAP 9.8 oder höher	Wählen Sie Option 10. **Beispiel für ein Startmenü anzeigen** ``` Please choose one of the following: (1) Normal Boot. (2) Boot without /etc/rc. (3) Change password. (4) Clean configuration and initialize all disks. (5) Maintenance mode boot. (6) Update flash from backup config. (7) Install new software first. (8) Reboot node. (9) Configure Advanced Drive Partitioning. (10) Set Onboard Key Manager recovery secrets. (11) Configure node for external key management. Selection (1-11)? 10 ```

ONTAP-Version	Wählen Sie diese Option aus

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

3. Bestätigen Sie, 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 zeigt die Konsole keine Eingaben an.

   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 aus der Zeile „START BACKUP“ durch die Zeile „END BACKUP“ ein.

Beispiel-Eingabeaufforderung anzeigen

```
Enter the backup data:

--------------------------BEGIN BACKUP--------------------------
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
3456789012345678901234567890123456789012345678901234567890123456
4567890123456789012345678901234567890123456789012345678901234567
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

---------------------------END BACKUP---------------------------
```

b. Drücken Sie am Ende des Eingangs zweimal die Eingabetaste.

Die Wiederherstellung ist abgeschlossen.

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 als ist `Successfully recovered keymanager secrets`. Führen Sie die Fehlerbehebung durch, um den Fehler zu beheben.

6. Wählen Sie Option 1 aus dem Startmenü, um mit dem Booten in ONTAP fortzufahren.

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 an der Konsole des Controllers die folgende Meldung angezeigt wird.

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

8. Geben Sie am Partner-Node den Partner-Controller ein, indem Sie den folgenden Befehl eingeben.

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

9. Führen Sie nach dem Booten nur mit dem CFO-Aggregat den folgenden Befehl aus.

   `security key-manager onboard sync`

10. Geben Sie die Cluster-weite Passphrase für das 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 war, wird die Cluster-Eingabeaufforderung ohne weitere Meldungen zurückgegeben. Wenn die Synchronisierung fehlschlägt, wird eine Fehlermeldung angezeigt, bevor Sie zur Cluster-Eingabeaufforderung zurückkehren. Fahren Sie nicht fort, bis der Fehler behoben ist und die Synchronisierung erfolgreich ausgeführt wird.

11. Stellen Sie sicher, dass alle Schlüssel synchronisiert wurden, indem Sie den folgenden Befehl eingeben.

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

    There are no entries matching your query.
    ```

    Beim Filtern nach FALSE im wiederhergestellten Parameter sollten keine Ergebnisse angezeigt werden.

12. Geben Sie dem Partner ein Giveback des Node durch Eingabe des folgenden Befehls ein.

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

13. Stellen Sie das automatische Giveback wieder her, wenn Sie es deaktiviert haben, indem Sie den folgenden Befehl eingeben.

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

14. Wenn AutoSupport aktiviert ist, stellen Sie die automatische Fallerstellung durch Eingabe des folgenden Befehls wieder her.

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

Option 2: Wiederherstellung der Konfiguration des externen Schlüsselmanagers

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

Bevor Sie beginnen

Sie benötigen die folgenden Informationen für die Wiederherstellung der EKM-Konfiguration (External Key Manager).

- Eine Kopie der Datei /cfcard/kmip/servers.cfg von einem anderen Clusterknoten oder die folgenden Informationen:
  - Die Adresse des KMIP-Servers.
  - Der KMIP-Port.
- Eine Kopie der `/cfcard/kmip/certs/client.crt` Datei von einem anderen Cluster-Node oder dem Client-Zertifikat.
- Eine Kopie der `/cfcard/kmip/certs/client.key` Datei von einem anderen Cluster-Node oder dem Client-Schlüssel.
- Eine Kopie der `/cfcard/kmip/certs/CA.pem` Datei von einem anderen Cluster-Knoten oder der KMIP-Server-CA(s).

Schritte

1. Schließen Sie das Konsolenkabel an den Ziel-Controller an.
2. Wählen Sie Option 11 aus dem ONTAP-Startmenü.

   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, dass Sie die erforderlichen Informationen gesammelt haben, wenn Sie dazu aufgefordert werden.

   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 bei der entsprechenden Aufforderung die Client- und Serverinformationen ein.

Eingabeaufforderung anzeigen

```
Enter the client certificate (client.crt) file contents:
Enter the client key (client.key) file contents:
Enter the KMIP server CA(s) (CA.pem) file contents:
Enter the server configuration (servers.cfg) file contents:
```

Beispiel anzeigen

```
Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwgY8xCzAJBgNVBAYTAlVT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk5l
MSUbQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxciLJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxpbz3mXF/X/1PC3YOzVNCq5eieek62si
Fp8=
-----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-----
MIIEizCCA3OgAwIBAgIBADANBgkqhkiG9w0BAQsFADCBjzELMAkGA1UEBhMCVVMx
7yaumMQETNrpMfP+nQMd34y4AmseWYGM6qG0z37BRnYU0Wf2qDL61cQ3/jkm7Y94
EQBKG1NY8dVyjphmYZv+
-----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
```

Nachdem Sie die Client- und Serverinformationen eingegeben haben, ist der Wiederherstellungsvorgang abgeschlossen.

Beispiel anzeigen

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
[Aug 29 21:06:28]: 0x808806100: 0: DEBUG: kmip2::main:
[initOpenssl]:460: Performing initialization of OpenSSL
Successfully recovered keymanager secrets.
```

5. Wählen Sie Option 1 aus dem Startmenü, um mit dem Booten in ONTAP fortzufahren.

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. Stellen Sie das automatische Giveback wieder her, wenn Sie es deaktiviert haben, indem Sie den folgenden Befehl eingeben.

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

7. Wenn AutoSupport aktiviert ist, stellen Sie die automatische Fallerstellung durch Eingabe des folgenden Befehls wieder her.

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

Senden Sie das fehlerhafte Teil an NetApp - FAS2820 zurück

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