Boot-Medien

Install and maintain

NetApp
January 09, 2026

Inhalt

Boot-Medien

Übersicht über den Austausch von Startmedien - ASA C250

Das Boot-Medium speichert einen primären und sekundären Satz von Systemdateien (Boot-Image), die das System beim Booten verwendet.

Bevor Sie beginnen

- Sie müssen über ein USB-Flash-Laufwerk verfügen, das auf MBR/FAT32 formatiert ist und über die entsprechende Speichermenge verfügt, 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.

Über diese Aufgabe

- 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 Controller anwenden:
  - Der Node *gestörter* ist der Controller, an dem Sie Wartungsarbeiten durchführen.
  - Der *Healthy*-Knoten ist der HA-Partner des beeinträchtigten Controllers.

Unterstützung und Status von Verschlüsselungsschlüsseln prüfen – ASA C250

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.

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

   Falls kein Schlüsselmanager konfiguriert ist:

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

Wenn ein Schlüsselmanager (EKM oder OKM) konfiguriert ist:

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

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

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

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

Externer Schlüsselmanager (EKM)

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

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

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

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

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

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

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

b. Überprüfen Sie, ob alle Authentifizierungsschlüssel wiederhergestellt wurden:

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

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

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

Onboard Key Manager (OKM)

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

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

a. Sichern Sie die OKM-Informationen:

   i. In den erweiterten Berechtigungsmodus wechseln:

      ```
      set -priv advanced
      ```

   Eingeben `y` wenn er zur Fortsetzung aufgefordert wird.

   i. Informationen zur Schlüsselverwaltung und Datensicherung anzeigen:

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

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

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

   iii. Zurück zum Administratormodus:

      ```
      set -priv admin
      ```

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

i. Informationen zur Schlüsselverwaltung und Datensicherung anzeigen:

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

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

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

iii. Zurück zum Administratormodus:

```
set -priv admin
```

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

Fahren Sie den Controller - ASA C250 herunter

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: `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.

Option 2: Systeme 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

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 `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`.

Ersetzen Sie das Startmedium – ASA C250

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

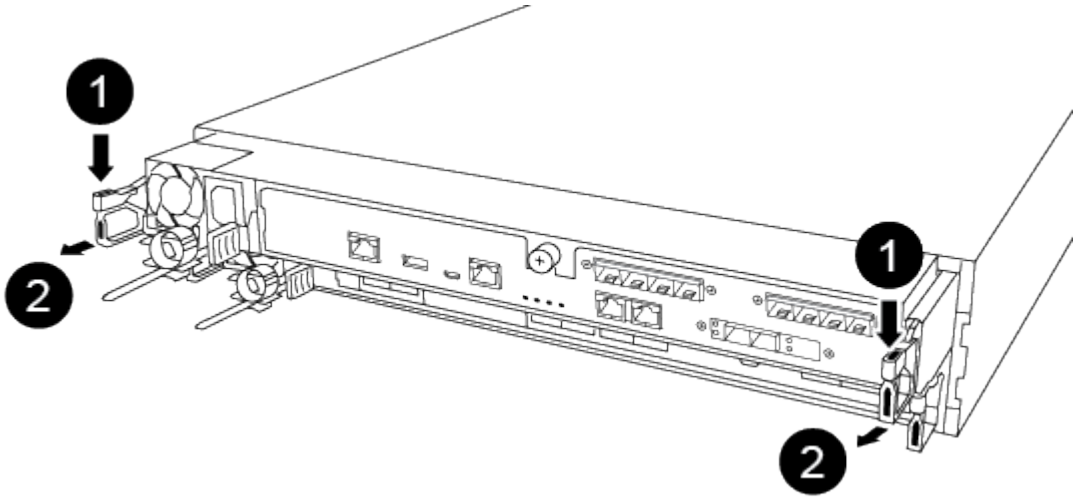
Schritt 1: Entfernen Sie das Controller-Modul

Um auf Komponenten im Controller-Modul zuzugreifen, müssen Sie zunächst das Controller-Modul aus dem System entfernen und dann die Abdeckung am Controller-Modul entfernen.

Schritte

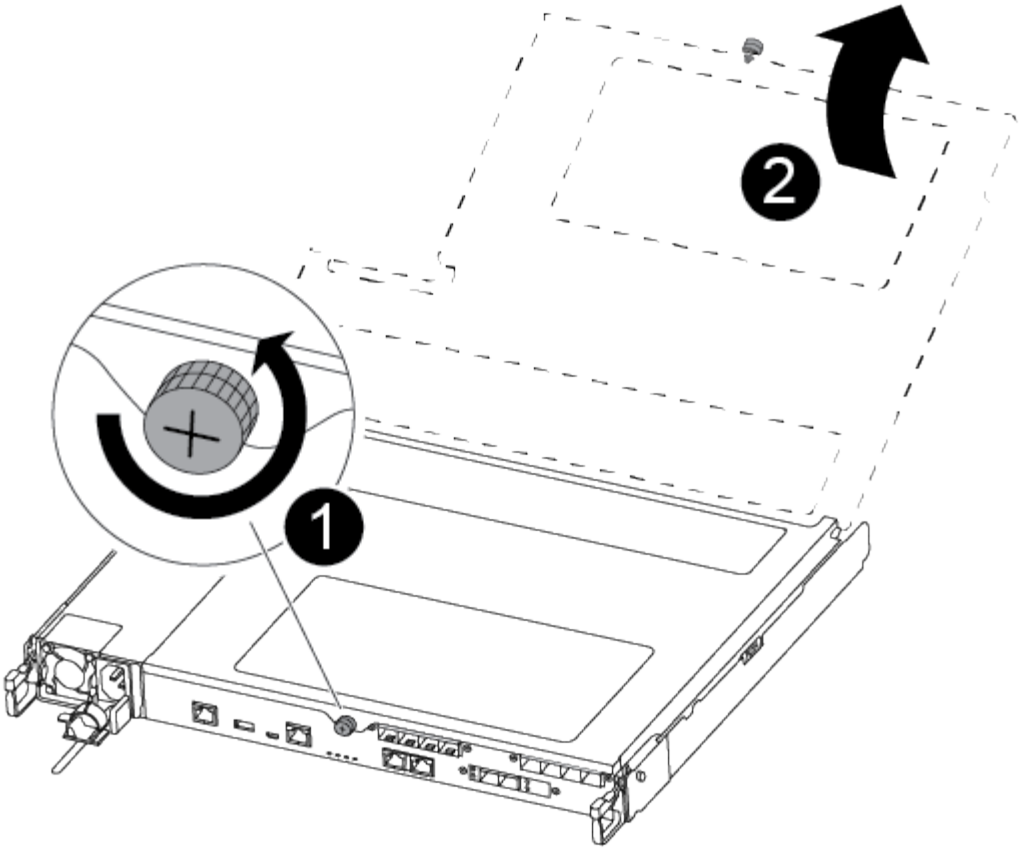
1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
2. Trennen Sie die Netzteile des Controller-Moduls von der Quelle.
3. Lösen Sie die Netzkabelhalter, und ziehen Sie anschließend die Kabel von den Netzteilen ab.
4. Ziehen Sie die E/A-Kabel vom Controller-Modul ab.
5. Setzen Sie den Zeigefinger in den Verriegelungsmechanismus auf beiden Seiten des Controller-Moduls ein, drücken Sie den Hebel mit dem Daumen, und ziehen Sie den Controller vorsichtig einige Zentimeter aus dem Gehäuse.

Wenn Sie Schwierigkeiten beim Entfernen des Controller-Moduls haben, setzen Sie Ihre Zeigefinger durch die Fingerlöcher von innen (durch Überqueren der Arme).



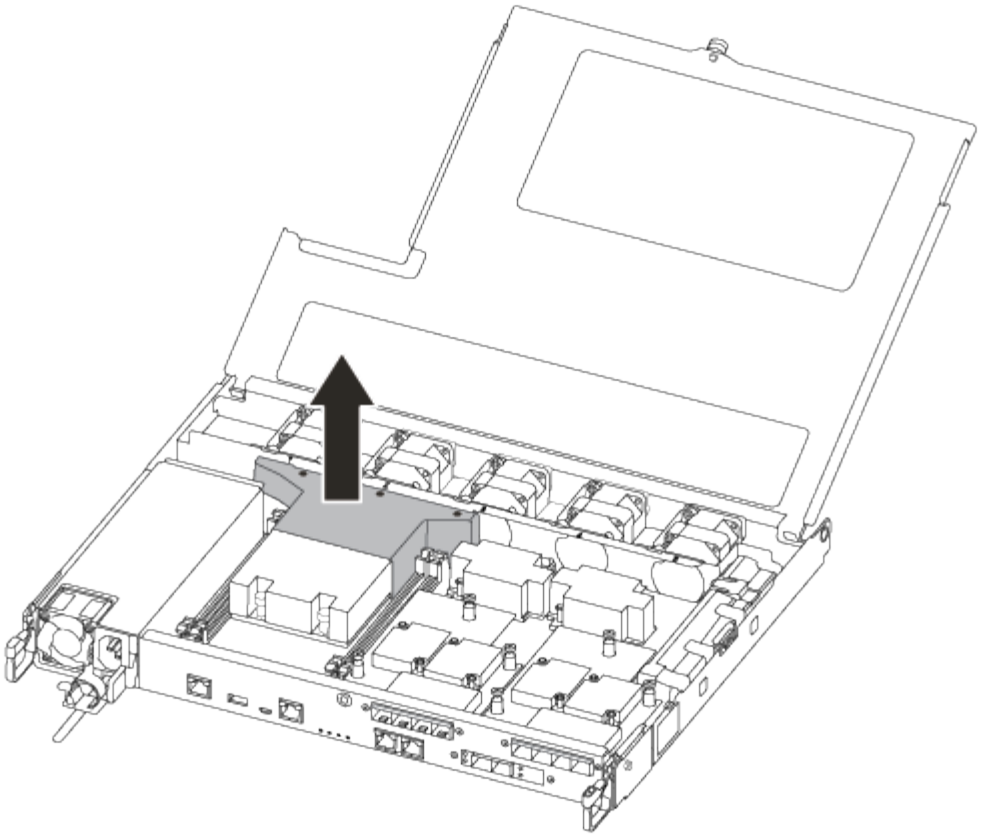
1	Hebel
2	Verriegelungsmechanismus

6. Fassen Sie die Seiten des Controller-Moduls mit beiden Händen an, ziehen Sie es vorsichtig aus dem Gehäuse heraus und legen Sie es auf eine flache, stabile Oberfläche.
7. Drehen Sie die Daumenschraube auf der Vorderseite des Controller-Moduls gegen den Uhrzeigersinn, und öffnen Sie die Abdeckung des Controller-Moduls.



1	Flügelschraube
2	Controller-Modulabdeckung.

8. Heben Sie die Luftkanalabdeckung heraus.



Schritt 2: Ersetzen Sie die Startmedien

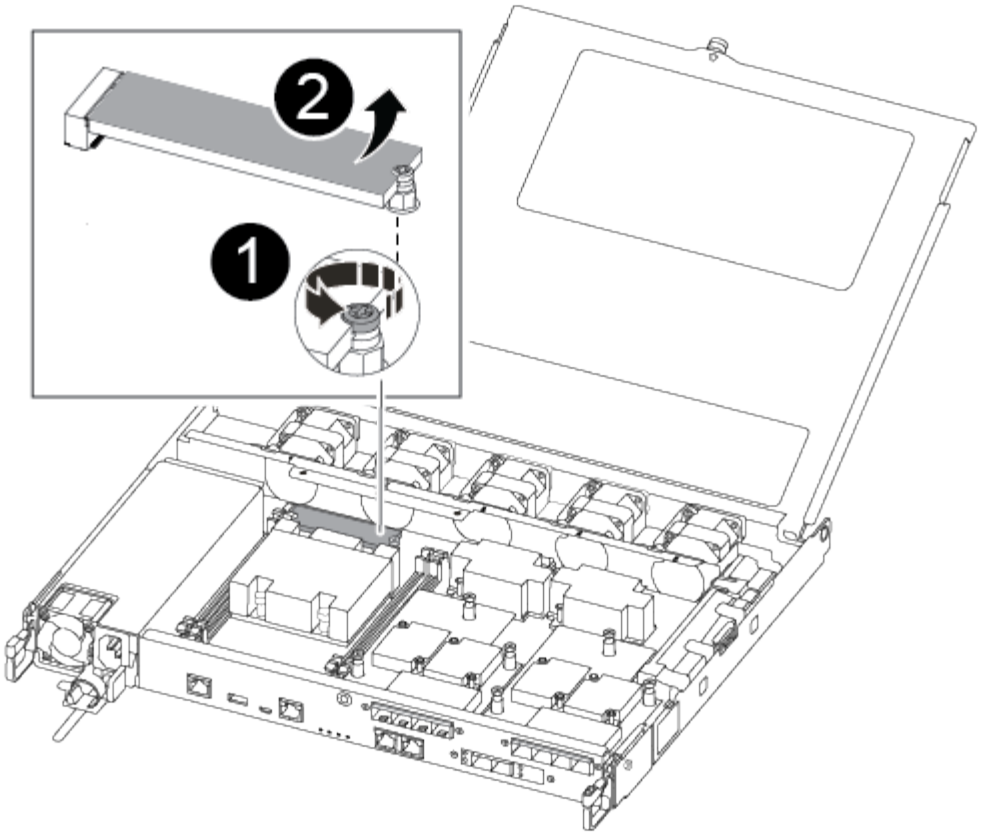
Sie finden das ausgefallene Bootmedium im Controller-Modul, indem Sie den Luftkanal am Controller-Modul entfernen, bevor Sie das Boot-Medium ersetzen können.

Um die Schraube zu entfernen, mit der die Bootsmedien befestigt sind, benötigen Sie einen #1 Magnetschraubendreher. Aufgrund der Platzbeschränkungen im Controller-Modul sollten Sie auch einen Magneten haben, um die Schraube darauf zu übertragen, damit Sie sie nicht verlieren.

Sie können das Bootmedium mit dem folgenden Video oder den tabellarischen Schritten ersetzen:

Animation - Ersetzen Sie das Startmedium

1. Suchen und ersetzen Sie die gestörten Startmedien vom Controller-Modul.



1	Entfernen Sie die Schraube, mit der das Boot-Medium am Motherboard im Controller-Modul befestigt ist.
2	Heben Sie die Boot-Medien aus dem Controller-Modul.

2. Entfernen Sie die Schraube mit dem #1-Magnetschraubendreher aus dem gestörten Boot-Medium und legen Sie sie sicher auf den Magneten.
3. Heben Sie die gestörten Startmedien vorsichtig direkt aus dem Sockel und legen Sie sie beiseite.
4. Entfernen Sie die Ersatzstartmedien aus dem antistatischen Versandbeutel, und richten Sie sie am Controller-Modul aus.
5. Setzen Sie die Schraube mit dem #1-Magnetschraubendreher ein und ziehen Sie sie fest.

> Beim Anziehen der Schraube auf dem Boot-Medium keine Kraft auftragen, da sie möglicherweise knacken kann.

Schritt 3: Übertragen Sie das Startabbild auf das Startmedium

Der installierte Ersatz-Startdatenträger ist ohne Startabbild, sodass Sie ein Startabbild über ein USB-Flash-Laufwerk übertragen müssen.

- 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, Sie müssen jedoch beim Wiederherstellen des var-Dateisystems einen zusätzlichen Neustart durchführen.

a. Laden Sie das entsprechende Service-Image von der NetApp Support Site auf das USB-Flash-Laufwerk herunter und kopieren Sie es.
b. Laden Sie das Service-Image auf Ihren Arbeitsbereich auf Ihrem Laptop herunter.
c. 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:

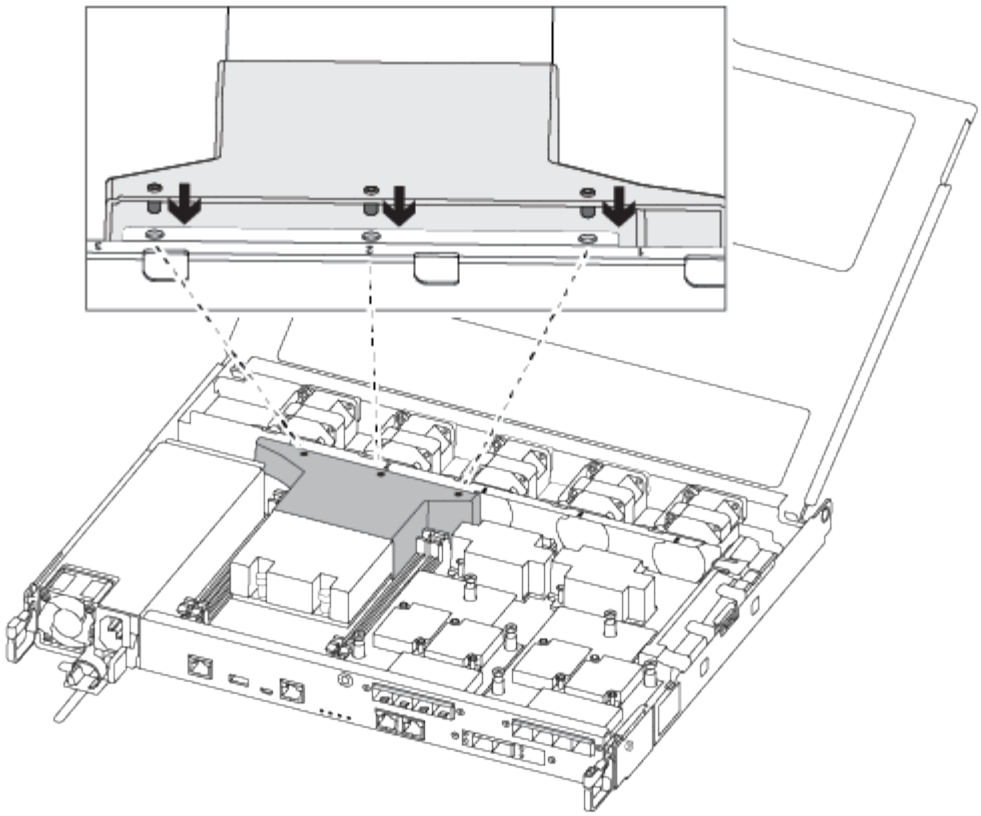
  - Booten
  - efi

d. kopieren Sie den efi-Ordner in das oberste Verzeichnis auf dem USB-Flash-Laufwerk.

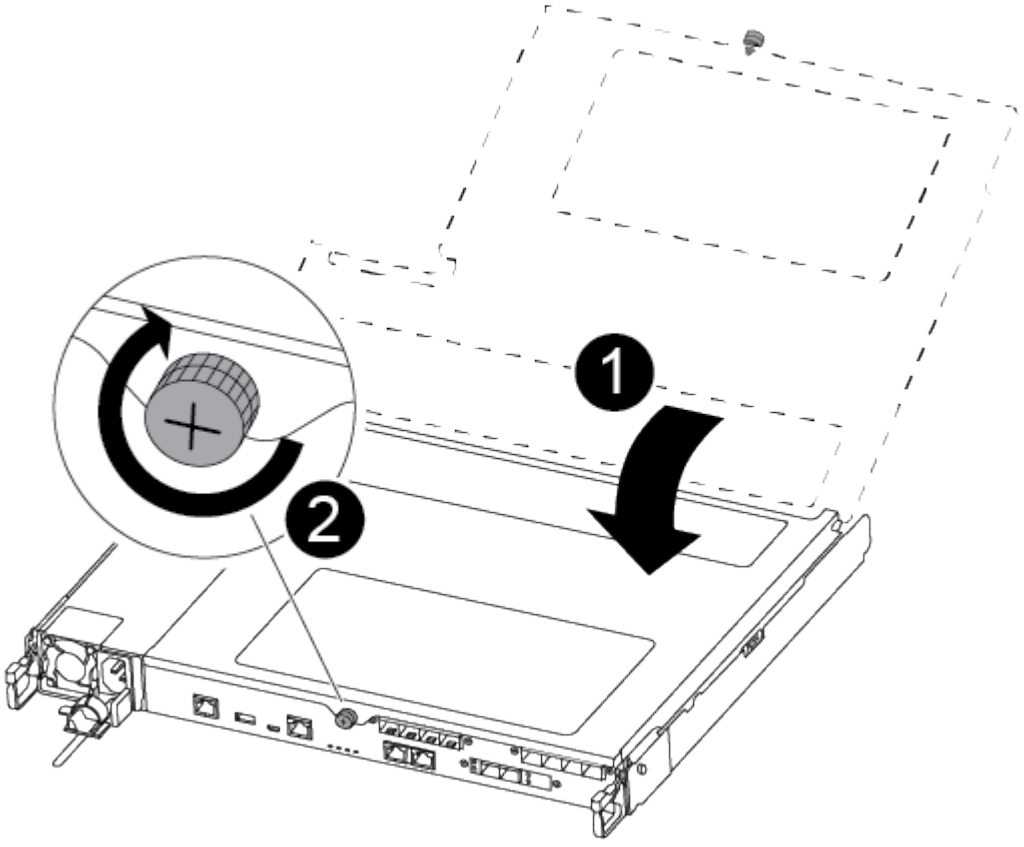
> Wenn das Service-Image keinen efi-Ordner hat, siehe "EFI-Ordner fehlt in Service-Image-Download-Datei verwendet für Boot-Gerät Recovery für FAS-und AFF-Modelle^".

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

e. Entfernen Sie das USB-Flash-Laufwerk von Ihrem Laptop.
f. Wenn Sie dies noch nicht getan haben, den Luftkanal einbauen.



g. Schließen Sie die Abdeckung des Controller-Moduls, und ziehen Sie die Daumenschraube fest.



1	Controller-Modulabdeckung
2	Flügelschraube

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. 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.

c. Drücken Sie das Controller-Modul ganz in das Chassis:

d. Platzieren Sie Ihre Zeigefinger durch die Fingerlöcher von der Innenseite des Verriegelungsmechanismus.

e. Drücken Sie die Daumen auf den orangefarbenen Laschen oben am Verriegelungsmechanismus nach unten, und schieben Sie das Controller-Modul vorsichtig über den Anschlag.

f. Lösen Sie Ihre Daumen von oben auf den Verriegelungs-Mechanismen und drücken Sie weiter, bis die Verriegelungen einrasten.

   Das Controller-Modul sollte vollständig eingesetzt und mit den Kanten des Gehäuses bündig sein.

g. Schließen Sie die E/A-Kabel des Controller-Moduls wieder an.

h. Schließen Sie die Netzkabel an die Netzteile an, setzen Sie die Sicherungsmanschette des Netzkabels wieder ein, und schließen Sie dann die Netzteile an die Stromquelle an.

   Das Controller-Modul startet, sobald die Stromversorgung wiederhergestellt ist. Bereiten Sie sich darauf vor, den Bootvorgang zu unterbrechen.

i. 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.

j. 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.

Starten Sie das Wiederherstellungs-Image - ASA C250

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

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 C250

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

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	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 auf Aufforderung, dass Sie den Wiederherstellungsprozess fortsetzen möchten:

   Beispiel-Eingabeaufforderung anzeigen

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

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

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

   Beispiel-Eingabeaufforderung anzeigen

   ```
   Enter the passphrase for onboard key management:

   Enter the passphrase again to confirm:
   ```

5. Geben Sie die Sicherungsinformationen ein:

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

Beispiel-Eingabeaufforderung anzeigen

```
Enter the backup data:

--------------------------BEGIN
BACKUP--------------------------
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
34567890123456789012345678901234567890123456789012345678901234
56
45678901234567890123456789012345678901234567890123456789012345
67
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
```

```
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA

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

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

   Der Wiederherstellungsprozess ist abgeschlossen und die folgende Meldung wird angezeigt:

   ```
   Successfully recovered keymanager secrets.
   ```

Beispiel-Eingabeaufforderung anzeigen

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

Successfully recovered keymanager secrets.

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

+

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

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

Beispiel-Eingabeaufforderung anzeigen

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


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

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

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

   Auf dem Partner-Controller:

8. Geben Sie den beeinträchtigten Controller zurück:

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

   Zum beeinträchtigten Regler:

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

   `security key-manager onboard sync`

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

Beispiel-Eingabeaufforderung anzeigen

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

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

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

11. Überprüfen Sie, ob alle Schlüssel synchronisiert sind:

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

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

    Auf dem Partner-Controller:

12. Geben Sie den beeinträchtigten Controller zurück:

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

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

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

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

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

Externer Schlüsselmanager (EKM)

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

Bevor Sie beginnen

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

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

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

Schritte

Zum beeinträchtigten Regler:

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

   Beispiel für ein Startmenü anzeigen

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

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

   Beispiel-Eingabeaufforderung anzeigen

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

4. Geben Sie die Client- und Serverinformationen ein, wenn Sie dazu aufgefordert werden:

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

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

Beispiel anzeigen

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

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

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

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

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

Der Wiederherstellungsprozess ist abgeschlossen und die folgende Meldung wird angezeigt:

```
Successfully recovered keymanager secrets.
```

Beispiel anzeigen

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

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

Beispiel-Eingabeaufforderung anzeigen

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

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

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

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

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

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

Geben Sie das fehlerhafte Teil an NetApp - ASA C250 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.