Boot-Medien

Install and maintain

NetApp
January 09, 2026

This PDF was generated from https://docs.netapp.com/de-de/ontap-systems/a700/bootmedia-replace-overview.html on January 09, 2026. Always check docs.netapp.com for the latest.

Inhalt

Boot-Medien . . . 1
- Übersicht zum Austausch des Bootmediums – AFF A700 . . . 1
- Prüfen Sie die Unterstützung und den Status der Verschlüsselungsschlüssel - AFF A700 . . . 1
  - Schritt 1: NVE-Unterstützung prüfen und das richtige ONTAP Image herunterladen . . . 2
  - Schritt 2: Überprüfen Sie den Status des Schlüsselmanagers und sichern Sie die Konfiguration. . . . 2
- Fahren Sie den gestörten Controller herunter - AFF A700 . . . 5
  - Option 1: Die meisten Systeme . . . 6
  - Option 3: Controller befindet sich in einem MetroCluster mit zwei Nodes . . . 7
- Ersetzen Sie das Startmedium – AFF A700 . . . 8
  - Schritt 1: Entfernen Sie die Steuerung . . . 9
  - Schritt 2: Ersetzen Sie die Startmedien . . . 10
  - Schritt 3: Übertragen Sie das Startabbild auf das Startmedium . . . 11
- Starten Sie das Wiederherstellungs-Image – AFF A700 . . . 13
  - Option 1: Starten Sie das Wiederherstellungs-Image in den meisten Systemen . . . 13
  - Option 2: Booten des Recovery-Images in einer MetroCluster-Konfiguration mit zwei Nodes . . . 16
- Switch-Back-Aggregate in einer Zwei-Knoten MetroCluster -Konfiguration - AFF A700 . . . 17
- Wiederherstellung der Verschlüsselung – AFF A700 . . . 18
- Senden Sie das defekte Teil an NetApp - AFF A700 zurück. . . . 28

Boot-Medien

Übersicht zum Austausch des Bootmediums – AFF A700

Lernen Sie den Austausch des Bootmediums auf einem AFF A700 -System kennen und verstehen Sie die verschiedenen Austauschmethoden. Das Bootmedium speichert primäre und sekundäre Boot-Image-Dateien, die das System beim Start verwendet. Je nach Ihrer Netzwerkkonfiguration können Sie entweder einen unterbrechungsfreien Austausch (über eine interne e0S-Verbindung) oder einen unterbrechenden Austausch (erfordert zwei Neustarts) durchführen.

Das AFF A700 -System unterstützt ausschließlich manuelle Wiederherstellungsverfahren über Bootmedien. Die automatische Wiederherstellung über Bootmedien wird nicht unterstützt.

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`.

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

- Bei den unterbrechungsfreien und unterbrechungsfreien Methoden zum Austausch von Boot-Medien müssen Sie den wiederherstellen `var` Filesystem:
  - Beim unterbrechungsfreien Austausch benötigt das HA-Paar keine Verbindung zu einem Netzwerk, um den wiederherzustellen `var` File-System. Das HA-Paar in einem einzelnen Chassis hat eine interne E0S-Verbindung, die zum Transfer verwendet wird `var` Konfigurieren zwischen ihnen.
  - Für den störenden Austausch benötigen Sie keine Netzwerkverbindung, um den wiederherzustellen `var` Dateisystem, aber der Prozess erfordert zwei Neustarts.
- Sie müssen die 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 die Unterstützung und den Status der Verschlüsselungsschlüssel - AFF A700

Um die Datensicherheit auf Ihrem Speichersystem zu gewährleisten, müssen Sie die Unterstützung und den Status des Verschlüsselungsschlüssels auf Ihrem Bootmedium überprüfen. Das AFF A700 -System unterstützt ausschließlich manuelle Wiederherstellungsverfahren über Bootmedien. Die automatische Wiederherstellung über Bootmedien wird nicht unterstützt.

Prüfen Sie, ob Ihre ONTAP Version NetApp Volume Encryption (NVE) unterstützt, und prüfen Sie vor dem Herunterfahren des Controllers, 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 `10no-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-Version	Führen Sie diesen Befehl aus
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 gestörten Controller herunter - AFF A700

Schalten Sie den beeinträchtigten Controller eines AFF A700 -Systems nach Abschluss der Verschlüsselungsprüfungen ab. Dieses Verfahren beinhaltet das Hochfahren des

Controllers bis zur LOADER-Eingabeaufforderung, das Erfassen von Boot-Umgebungsvariablen zu Referenzzwecken und die Vorbereitung des Controllers auf den Austausch des Bootmediums, wobei die einzelnen Schritte je nach Systemkonfiguration variieren.

Das AFF A700 -System unterstützt ausschließlich manuelle Wiederherstellungsverfahren über Bootmedien. Die automatische Wiederherstellung über Bootmedien wird nicht unterstützt.

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: Controller befindet sich in einem MetroCluster

Nach Abschluss der NVE oder NSE-Aufgaben müssen Sie den Shutdown des beeinträchtigten Nodes durchführen. HINWEIS: Verwenden Sie diese Vorgehensweise 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`.

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

Nach Abschluss der NVE oder NSE-Aufgaben müssen Sie den Shutdown des beeinträchtigten Nodes 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 – AFF A700

Ersetzen Sie das defekte Bootmedium auf einem AFF A700 -Controllermodul. Dieses Verfahren umfasst das Entfernen des Controllermoduls aus dem Gehäuse, das physische Ersetzen der Bootmedienkomponente, das Übertragen des Boot-Images auf das Ersatzmedium mithilfe eines USB-Sticks und die Wiederherstellung des normalen Systembetriebs.

Das AFF A700 -System unterstützt ausschließlich manuelle Wiederherstellungsverfahren über Bootmedien. Die automatische Wiederherstellung über Bootmedien wird nicht unterstützt.

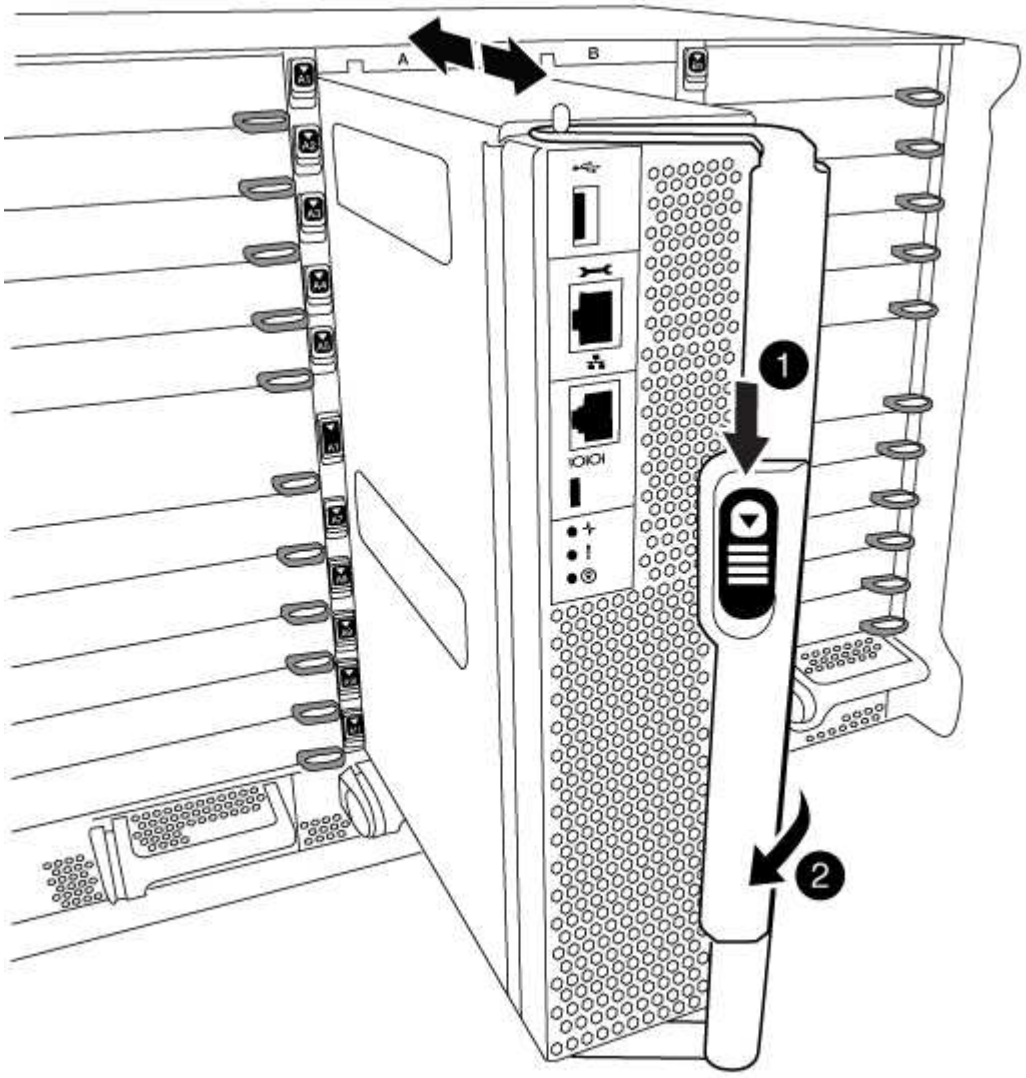
Zum Austauschen des Startmediums müssen Sie das beeinträchtigte Controller-Modul entfernen, das Ersatzstartmedium installieren und das Boot-Image auf ein USB-Flash-Laufwerk übertragen.

Schritt 1: Entfernen Sie die Steuerung

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

Schritte

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



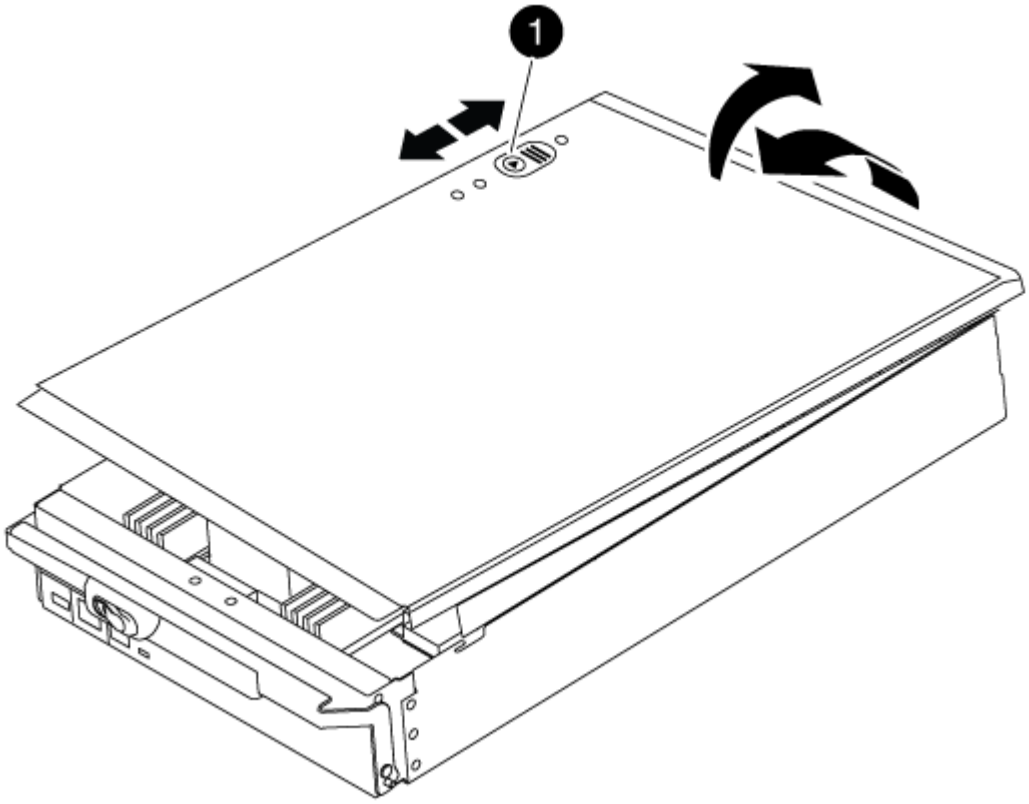
1	
Freigabetaste für den CAM-Griff	
2	

CAM-Griff

4. Drehen Sie den Nockengriff so, dass er das Controller-Modul vollständig aus dem Gehäuse herausrückt, und schieben Sie dann das Controller-Modul aus dem Gehäuse.

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

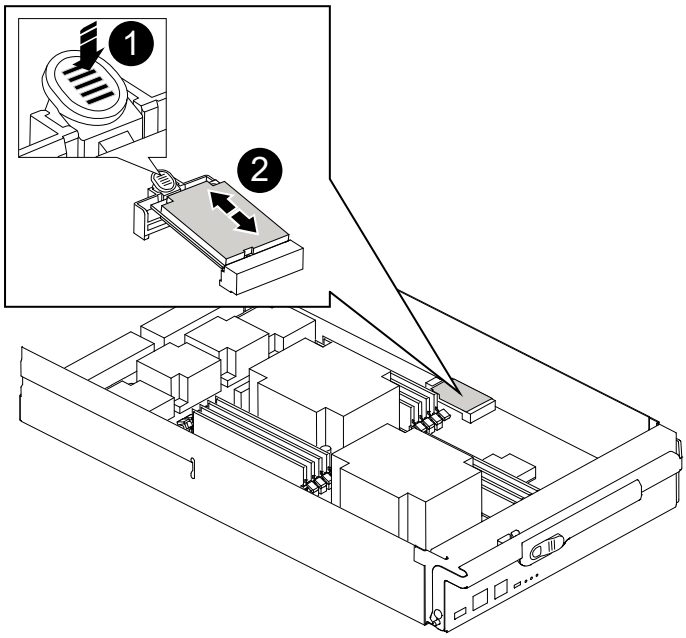
5. Setzen Sie die Abdeckung des Controller-Moduls auf eine stabile, flache Oberfläche, drücken Sie die blaue Taste auf der Abdeckung, schieben Sie die Abdeckung auf die Rückseite des Controller-Moduls, und schwenken Sie sie dann nach oben und heben Sie sie vom Controller-Modul ab.



1
Verriegelungstaste für die Controllermodulabdeckung

Schritt 2: Ersetzen Sie die Startmedien

Suchen Sie das Boot-Medium mithilfe der folgenden Abbildung oder der FRU-Zuordnung auf dem Controller-Modul:



1	
Drücken Sie die Freigabelasche	
2	
Boot-Medien	

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

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

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

4. Drücken Sie die Startmedien nach unten, um die Verriegelungstaste am Startmediengehäuse zu betätigen.
5. Bringen Sie die Abdeckung des Controller-Moduls wieder an, indem Sie die Stifte auf dem Deckel an die Schlitze auf dem Motherboard-Träger ausrichten und den Deckel dann in die richtige Position schieben.

Schritt 3: Übertragen Sie das Startabbild auf das Startmedium

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

- Sie müssen über ein USB-Flash-Laufwerk verfügen, das auf 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 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.

Schritte

1. 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.
2. Das Controller-Modul nach Bedarf wieder einschalten.
3. 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.

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

   Der Node wird gestartet, sobald er vollständig im Chassis installiert ist.

5. 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 Node zum Booten in LOADER.

6. 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 mit dem beeinträchtigten Knoten über den gesunden Knoten während kommunizieren `var` Dateisystemwiederherstellung mit Netzwerkverbindung. 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.

7. Wenn sich der Controller in einem Stretch- oder Fabric-Attached MetroCluster befindet, müssen Sie die FC-Adapterkonfiguration wiederherstellen:

   a. Start in Wartungsmodus: `boot_ontap maint`

   b. Legen Sie die MetroCluster-Ports als Initiatoren fest: `ucadmin modify -m fc -t` *`initiator adapter_name`*

   c. Anhalten, um zum Wartungsmodus zurückzukehren: `halt`

   Die Änderungen werden implementiert, wenn das System gestartet wird.

Starten Sie das Wiederherstellungs-Image – AFF A700

Starten Sie das ONTAP Wiederherstellungsimage vom USB-Laufwerk auf einem AFF A700 -System, um die Startmedien wiederherzustellen. Dieses Verfahren umfasst das Booten vom USB-Flash-Laufwerk, das Wiederherstellen des Dateisystems, das Überprüfen der Umgebungsvariablen und das Zurückführen des Controllers in den Normalbetrieb, wobei die spezifischen Schritte je nach Konfiguration des Systems (Zwei-Knoten MetroCluster) variieren.

Das AFF A700 -System unterstützt ausschließlich manuelle Wiederherstellungsverfahren über Bootmedien. Die automatische Wiederherstellung über Bootmedien wird nicht unterstützt.

Das Verfahren zum Booten des beeinträchtigten Knotens vom Wiederherstellungsabbild hängt davon ab, ob sich das System in einer MetroCluster-Konfiguration mit zwei Knoten befindet.

Option 1: Starten Sie das Wiederherstellungs-Image in den meisten Systemen

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	a. Drücken Sie `y` Wenn Sie aufgefordert werden, die Backup-Konfiguration wiederherzustellen. b. Legen Sie den gesunden Node auf die erweiterte Berechtigungsebene fest: `set -privilege advanced` c. Führen Sie den Befehl Restore Backup aus: `system node restore-backup -node local -target-address impaired_node_IP_address` d. Gibt den Node wieder auf Administratorebene: `set -privilege admin` e. Drücken Sie `y` Wenn Sie aufgefordert werden, die wiederhergestellte Konfiguration zu verwenden. f. Drücken Sie `y` Wenn Sie zum Neubooten des Node aufgefordert werden.
Keine Netzwerkverbindung	a. Drücken Sie `n` Wenn Sie aufgefordert werden, die Backup-Konfiguration wiederherzustellen. b. Starten Sie das System neu, wenn Sie dazu aufgefordert werden. c. Wählen Sie im angezeigten Menü die Option **Flash aktualisieren aus Backup config** (Flash synchronisieren) aus. Wenn Sie aufgefordert werden, mit der Aktualisierung fortzufahren, drücken Sie `y`.

Wenn Ihr System…	Dann…

Keine Netzwerkverbindung und befindet sich in einer MetroCluster IP-Konfiguration	a. Drücken Sie `n` Wenn Sie aufgefordert werden, die Backup-Konfiguration wiederherzustellen.
	b. Starten Sie das System neu, wenn Sie dazu aufgefordert werden.
	c. Warten Sie, bis die iSCSI-Speicherverbindungen verbunden sind.
	Sie können fortfahren, nachdem Sie die folgenden Meldungen angezeigt haben:
	`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address).`
	`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address).`
	`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address).`
	`date-and-time [node-name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address).`
	d. Wählen Sie im angezeigten Menü die Option **Flash aktualisieren aus Backup config** (Flash synchronisieren) aus.
	Wenn Sie aufgefordert werden, mit der Aktualisierung fortzufahren, drücken Sie `y`.

4. Stellen Sie sicher, 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 `savenv` 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…	a. Melden Sie sich beim Partner-Node an. b. Vergewissern Sie sich, dass der Ziel-Node zur Rückgabe mit dem bereit ist `storage failover show` Befehl.

7. Schließen Sie das Konsolenkabel an den Partner-Node an.
8. Geben Sie den Node 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 Node 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: Booten des Recovery-Images in einer MetroCluster-Konfiguration 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 `savenv` Befehl.
   e. Booten Sie den Node neu.

Switch-Back-Aggregate in einer Zwei-Knoten MetroCluster -Konfiguration - AFF A700

Nach Abschluss des Austauschs der Startmedien muss die MetroCluster -Umschaltung durchgeführt werden. Das AFF A700 -System unterstützt ausschließlich manuelle Wiederherstellungsverfahren über Bootmedien. Die automatische Wiederherstellung über Bootmedien wird nicht unterstützt.

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

Wiederherstellung der Verschlüsselung – AFF A700

Die Verschlüsselung auf dem Ersatz-Bootmedium wiederherstellen. Das AFF A700 -System unterstützt ausschließlich manuelle Wiederherstellungsverfahren über Bootmedien. Die automatische Wiederherstellung über Bootmedien wird nicht unterstützt.

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---------------------------
012345678901234567890123456789012345678901234567890123456789012
23
123456789012345678901234567890123456789012345678901234567890123
34
234567890123456789012345678901234567890123456789012345678901234
45
345678901234567890123456789012345678901234567890123456789012345
56
456789012345678901234567890123456789012345678901234567890123456
67
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
```

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

Senden Sie das defekte Teil an NetApp - AFF A700 zurück.

Senden Sie das defekte Teil an NetApp zurück, wie in den mit dem Kit gelieferten RMA-Anweisungen beschrieben. Siehe die "Rückgabe und Austausch von Teilen" Weitere Informationen finden Sie auf der entsprechenden Seite. Das AFF A700 -System unterstützt ausschließlich manuelle Wiederherstellungsverfahren über Bootmedien. Die automatische Wiederherstellung über Bootmedien wird nicht unterstützt.

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.