Boot-Medien

Install and maintain

NetApp
April 19, 2024

This PDF was generated from https://docs.netapp.com/de-de/ontap-systems/a250/bootmedia-replace-overview.html on April 19, 2024. Always check docs.netapp.com for the latest.

Inhalt

Boot-Medien . . . 1
Übersicht über den Austausch von Boot-Medien - AFF A250 . . . 1
Integrierte Verschlüsselungsschlüssel - AFF A250 . . . 1
Schalten Sie den Controller aus - AFF A250 . . . 5
Ersetzen Sie die Startmedien - AFF A250 . . . 7
Starten Sie das Wiederherstellungsabbild - AFF A250 . . . 15
Stellen Sie OKM, NSE und NVE nach Bedarf wieder her – AFF A250 . . . 20
Senden Sie das fehlerhafte Teil an NetApp - AFF A250 zurück . . . 24

Boot-Medien

Übersicht über den Austausch von Boot-Medien - AFF A250

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.

Integrierte Verschlüsselungsschlüssel - AFF A250

Bevor Sie den beeinträchtigten Controller herunterfahren und den Status der integrierten Schlüssel überprüfen, müssen Sie den Status des beeinträchtigten Controllers überprüfen, das automatische Giveback deaktivieren und überprüfen, welche Version von ONTAP auf dem System ausgeführt wird.

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

Schritte

1. Den Status des beeinträchtigten Reglers prüfen:
   - Wenn sich der Controller mit eingeschränkter Bedieneinheit an der Anmeldeaufforderung befindet, melden Sie sich als an `admin`.
   - Wenn der Controller mit eingeschränkter Einstellung an der LOADER-Eingabeaufforderung steht und Teil der HA-Konfiguration ist, melden Sie sich als an `admin` Auf dem gesunden Controller.
   - Wenn sich der beeinträchtigte Controller in einer eigenständigen Konfiguration befindet und an DER

LOADER-Eingabeaufforderung angezeigt wird, wenden Sie sich an "mysupport.netapp.com".

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

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

3. Überprüfen Sie die Version von ONTAP, auf der das System auf dem beeinträchtigten Controller ausgeführt wird, wenn er eingeschaltet ist, oder auf dem Partner-Controller, wenn der beeinträchtigte Controller nicht verfügbar ist, über das `version -v` Befehl:
   - Wenn <lno-DARE> oder <1Ono-DARE> in der Befehlsausgabe angezeigt wird, unterstützt das System NVE nicht. Fahren Sie mit dem Herunterfahren des Controllers fort.
   - Wenn <lno-DARE> nicht in der Befehlsausgabe angezeigt wird und auf dem System ONTAP 9.6 oder höher ausgeführt wird, fahren Sie mit dem nächsten Abschnitt fort.
4. Wenn der beeinträchtigte Controller Teil einer HA-Konfiguration ist, deaktivieren Sie das automatische Giveback vom ordnungsgemäßen Controller: `storage failover modify -node local -auto -giveback false` Oder `storage failover modify -node local -auto-giveback-after -panic false`

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

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

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

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

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

Überprüfen der NVE-Konfiguration

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

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

- Wenn der `Key Manager` Typ wird angezeigt `external` Und das `Restored` Spalte wird angezeigt `yes`, Es ist sicher, den beeinträchtigten Regler herunterzufahren.
- Wenn der `Key Manager` Typ wird angezeigt `onboard` Und das `Restored` Spalte wird angezeigt `yes`, Sie müssen einige zusätzliche Schritte.
- Wenn der `Key Manager` Typ wird angezeigt `external` Und das `Restored` Spalte zeigt alle anderen als an `yes`, Sie müssen einige zusätzliche Schritte.
- Wenn der `Key Manager` Typ wird angezeigt `onboard` Und das `Restored` Spalte zeigt alle anderen als an `yes`, Sie müssen einige zusätzliche Schritte.

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

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

   "mysupport.netapp.com"

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

      > Geben Sie an der Eingabeaufforderung die 32-stellige alphanumerische Onboard-Passphrase des Kunden ein. Falls die Passphrase nicht angegeben werden kann, wenden Sie sich an den NetApp Support. "mysupport.netapp.com"

   b. Überprüfen Sie die `Restored` In der Spalte wird angezeigt `yes` Für alle Authentifizierungsschlüssel: `security key-manager key query`
   c. Überprüfen Sie das `Key Manager` Typ zeigt an `onboard`, Und dann manuell sichern Sie die OKM-Informationen.

d. Wechseln Sie zum erweiterten Berechtigungsebene-Modus, und geben Sie ein `y` Wenn Sie dazu aufgefordert werden, fortzufahren: `set -priv advanced`

e. Geben Sie den Befehl ein, um die Backup-Informationen für das Verschlüsselungsmanagement anzuzeigen: `security key-manager onboard show-backup`

f. Kopieren Sie den Inhalt der Backup-Informationen in eine separate Datei oder eine Protokolldatei. Sie werden es in Disaster-Szenarien benötigen, in denen Sie OKM manuell wiederherstellen müssen.

g. Zurück zum Admin-Modus: `set -priv admin`

h. Sie können den Controller sicher herunterfahren.

Überprüfen der NSE-Konfiguration

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

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

   - Wenn der `Key Manager` Typ wird angezeigt `external` Und das `Restored` Spalte wird angezeigt `yes`, Es ist sicher, den beeinträchtigten Regler herunterzufahren.
   - Wenn der `Key Manager` Typ wird angezeigt `onboard` Und das `Restored` Spalte wird angezeigt `yes`, Sie müssen einige zusätzliche Schritte.
   - Wenn der `Key Manager` Typ wird angezeigt `external` Und das `Restored` Spalte zeigt alle anderen als an `yes`, Sie müssen einige zusätzliche Schritte.
   - Wenn der `Key Manager` Typ wird angezeigt `external` Und das `Restored` Spalte zeigt alle anderen als an `yes`, Sie müssen einige zusätzliche Schritte.

2. Wenn der `Key Manager` Typ wird angezeigt `onboard` Und das `Restored` Spalte wird angezeigt `yes`, Manuelle Sicherung der OKM-Informationen:

   a. Wechseln Sie zum erweiterten Berechtigungsebene-Modus, und geben Sie ein `y` Wenn Sie dazu aufgefordert werden, fortzufahren: `set -priv advanced`

   b. Geben Sie den Befehl ein, um die Schlüsselmanagementinformationen anzuzeigen: `security key-manager onboard show-backup`

   c. Kopieren Sie den Inhalt der Backup-Informationen in eine separate Datei oder eine Protokolldatei. Sie werden es in Disaster-Szenarien benötigen, in denen Sie OKM manuell wiederherstellen müssen.

   d. Zurück zum Admin-Modus: `set -priv admin`

   e. Sie können den Controller sicher herunterfahren.

3. Wenn der `Key Manager` Typ wird angezeigt `external` Und das `Restored` Spalte zeigt alle anderen als an `yes`:

   a. Stellen Sie die Authentifizierungsschlüssel für das externe Verschlüsselungsmanagement auf allen Nodes im Cluster wieder her: `security key-manager external restore`

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

   "mysupport.netapp.com"

a. Überprüfen Sie das `Restored` Spalte entspricht `yes` Für alle Authentifizierungsschlüssel: `security key-manager key query`

b. Sie können den Controller sicher herunterfahren.

4. Wenn der `Key Manager` Typ wird angezeigt `onboard` Und das `Restored` Spalte zeigt alle anderen als an `yes`:

   a. Geben Sie den integrierten Sicherheitsschlüssel-Manager Sync-Befehl ein: `security key-manager onboard sync`

      Geben Sie an der Eingabeaufforderung die 32-stellige alphanumerische Onboard-Passphrase des Kunden ein. Falls die Passphrase nicht angegeben werden kann, wenden Sie sich an den NetApp Support.

   "mysupport.netapp.com"

   a. Überprüfen Sie die `Restored` In der Spalte wird angezeigt `yes` Für alle Authentifizierungsschlüssel: `security key-manager key query`

   b. Überprüfen Sie das `Key Manager` Typ zeigt an `onboard`, Und dann manuell sichern Sie die OKM-Informationen.

   c. Wechseln Sie zum erweiterten Berechtigungsebene-Modus, und geben Sie ein `y` Wenn Sie dazu aufgefordert werden, fortzufahren: `set -priv advanced`

   d. Geben Sie den Befehl ein, um die Backup-Informationen für das Verschlüsselungsmanagement anzuzeigen: `security key-manager onboard show-backup`

   e. Kopieren Sie den Inhalt der Backup-Informationen in eine separate Datei oder eine Protokolldatei. Sie werden es in Disaster-Szenarien benötigen, in denen Sie OKM manuell wiederherstellen müssen.

   f. Zurück zum Admin-Modus: `set -priv admin`

   g. Sie können den Controller sicher herunterfahren.

Schalten Sie den Controller aus - AFF A250

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.

Wenn der eingeschränkte Controller angezeigt wird…	Dann…
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 die Startmedien - AFF A250

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

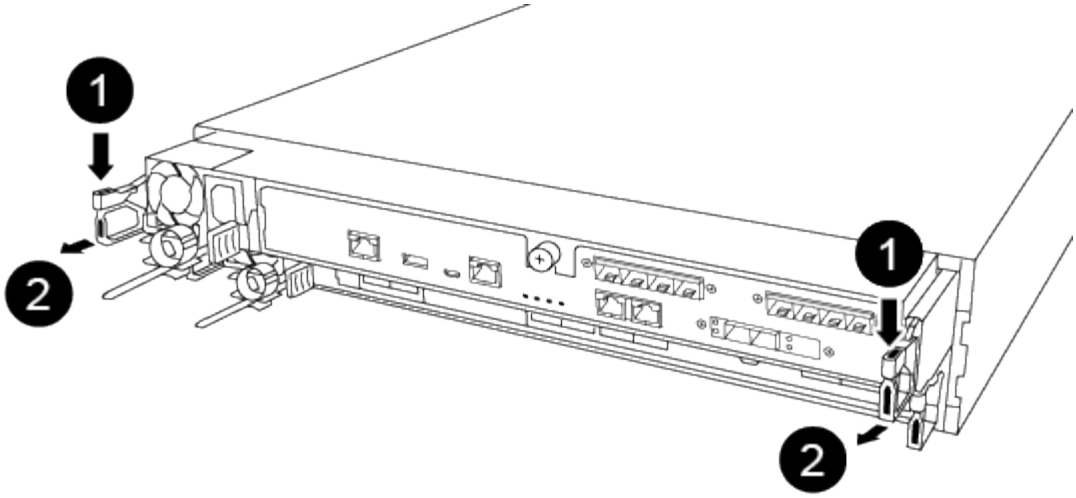
Schritt 1: Entfernen Sie das Controller-Modul

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

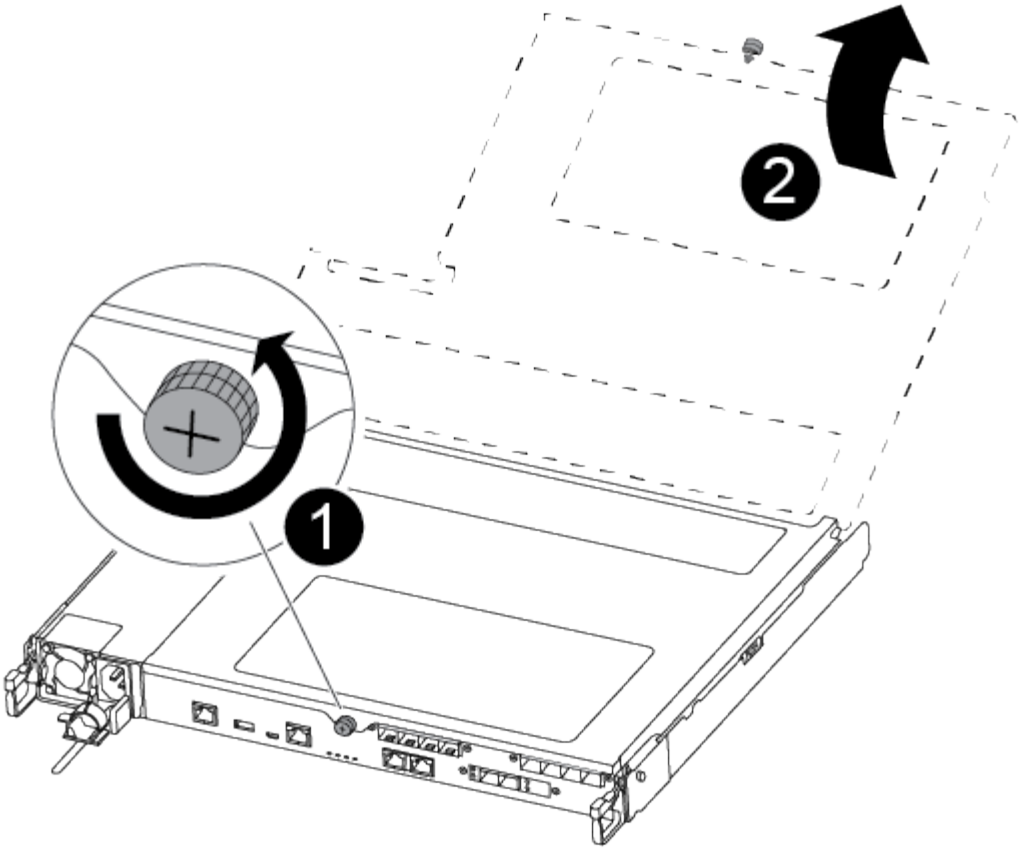
1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
2. Trennen Sie die Netzteile des Controller-Moduls von der Quelle.
3. Lösen Sie die Netzkabelhalter, und ziehen Sie anschließend die Kabel von den Netzteilen ab.
4. Setzen Sie den Zeigefinger in den Verriegelungsmechanismus auf beiden 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).



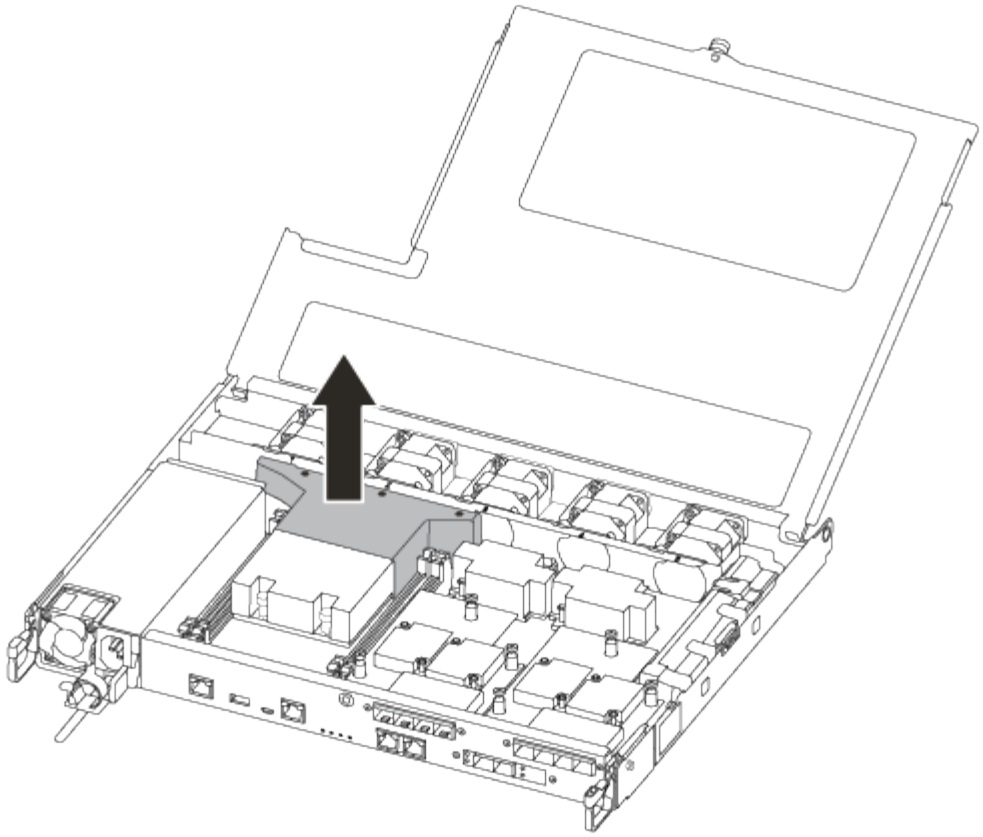
1	
Hebel	
2	
Verriegelungsmechanismus	

5. 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.
6. 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.	

7. Heben Sie die Luftkanalabdeckung heraus.



Schritt 2: Ersetzen Sie die Startmedien

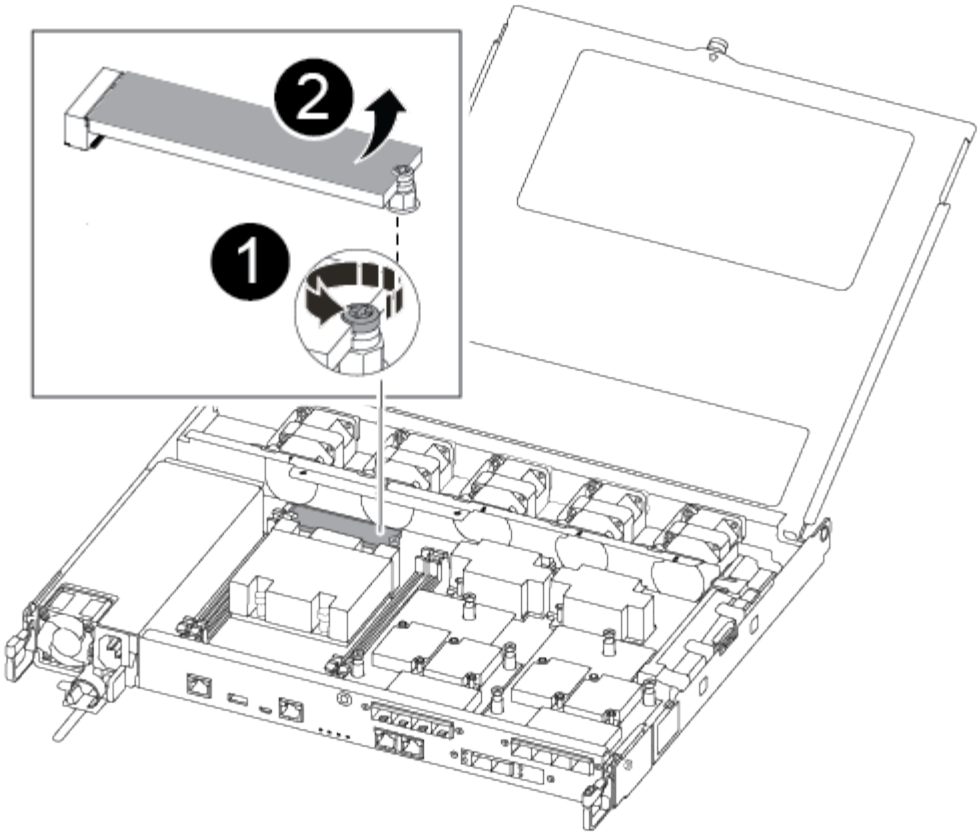
Sie finden das ausgefallene Bootmedium im Controller-Modul, indem Sie den Luftkanal am Controller-Modul entfernen, bevor Sie das Boot-Medium ersetzen können.

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.

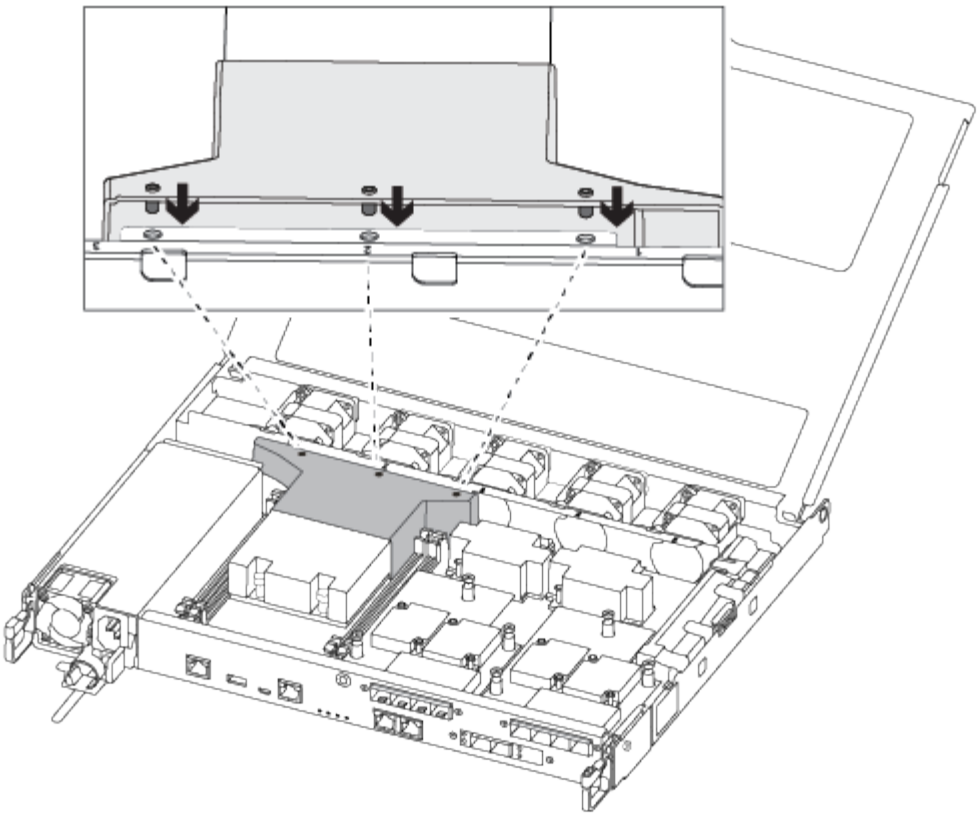
   Die Image-Datei „ungezippte Dienste“ enthält zwei Ordner:

   - Booten
   - efi

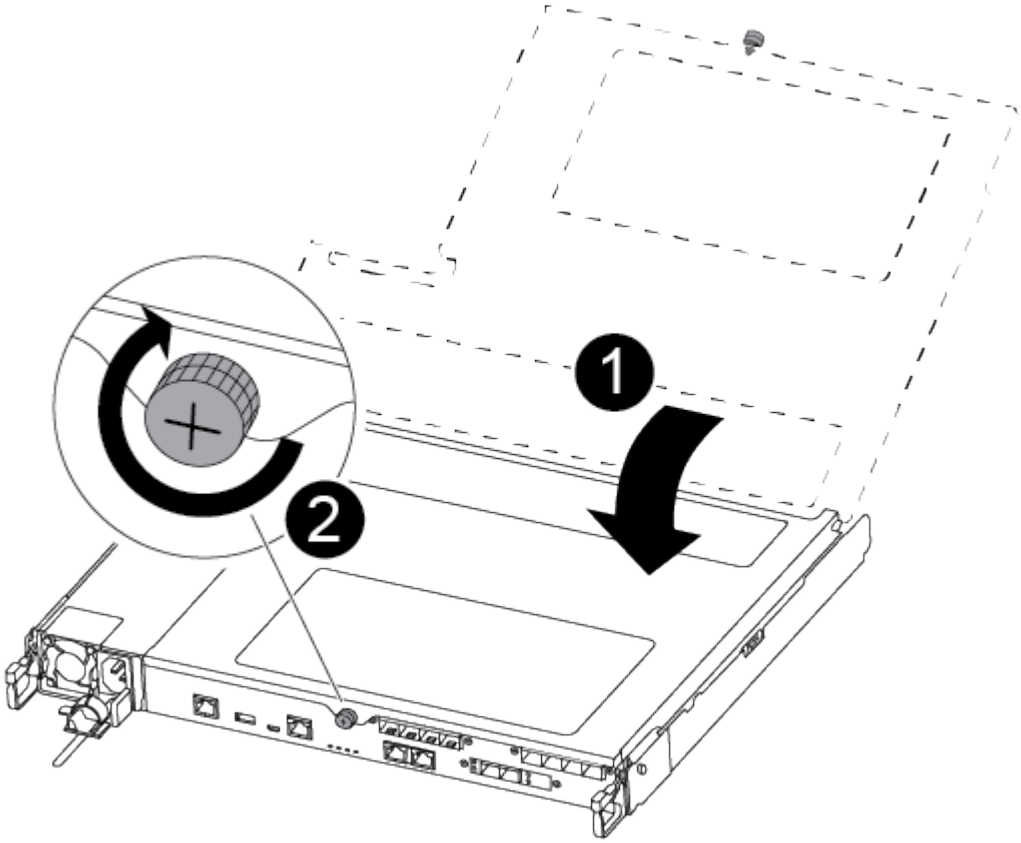
d. kopieren Sie den efi-Ordner in das oberste Verzeichnis auf dem USB-Flash-Laufwerk.

   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.



❶	Controller-Modulabdeckung
❷	Flügelschraube

h. 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.

i. Schließen Sie das Netzkabel an das Netzteil an, und setzen Sie den Netzkabelhalter wieder ein.

j. 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.

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

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

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

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

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

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

o. 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.

p. 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.

q. 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 Storage-Systems.

- `netmask` Ist die Netzwerkmaske des Management-Netzwerks, die mit dem HA-Partner verbunden ist.
- `gateway` Ist das Gateway für das Netzwerk.
- `dns_addr` Ist die IP-Adresse eines Namensservers in Ihrem Netzwerk.
- `dns_domain` Der Domain Name (DNS) ist der Domain-Name.

  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 Wiederherstellungsabbild - AFF A250

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

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. Stellen Sie den gesunden Controller auf die erweiterte Berechtigungsebene ein: `set -privilege advanced` c. Führen Sie den Befehl Restore Backup aus: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Zurückkehren des Controllers zur Administratorebene: `set -privilege admin` e. Drücken Sie `y` Wenn Sie aufgefordert werden, die wiederhergestellte Konfiguration zu verwenden. f. Drücken Sie `y` Wenn Sie dazu aufgefordert werden, den Controller neu zu booten.

Wenn Ihr System…	Dann…
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`.

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 Controller zur LOADER-Eingabeaufforderung.
   b. Überprüfen Sie die Einstellungen der Umgebungsvariable mit dem `printenv` Befehl.
   c. Wenn eine Umgebungsvariable nicht wie erwartet festgelegt ist, ändern Sie sie mit dem `setenvenvironment_variable_name changed_value` Befehl.
   d. Speichern Sie Ihre Änderungen mit dem `saveenv` Befehl.
5. Das nächste hängt von Ihrer Systemkonfiguration ab:
   - Wenn keymanager, NSE oder NVE in Ihrem System integriert sind, finden Sie unter Stellen Sie OKM, NSE und NVE nach Bedarf wieder her
   - Wenn keymanager, NSE oder NVE auf Ihrem System nicht konfiguriert sind, führen Sie die Schritte in diesem Abschnitt aus.
6. Geben Sie an der LOADER-Eingabeaufforderung das ein `boot_ontap` Befehl.

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

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

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

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

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

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. Stellen Sie den gesunden Controller auf die erweiterte Berechtigungsebene ein: `set -privilege advanced` c. Führen Sie den Befehl Restore Backup aus: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`* d. Zurückkehren des Controllers zur Administratorebene: `set -privilege admin` e. Drücken Sie `y` Wenn Sie aufgefordert werden, die wiederhergestellte Konfiguration zu verwenden. f. Drücken Sie `y` Wenn Sie dazu aufgefordert werden, den Controller neu zu booten.
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 Controller zur LOADER-Eingabeaufforderung.
   b. Überprüfen Sie die Einstellungen der Umgebungsvariable mit dem `printenv` Befehl.

c. Wenn eine Umgebungsvariable nicht wie erwartet festgelegt ist, ändern Sie sie mit dem `setenvenvironment_variable_name changed_value` Befehl.

d. Speichern Sie Ihre Änderungen mit dem `saveenv` Befehl.

5. Das nächste hängt von Ihrer Systemkonfiguration ab:
   - Wenn keymanager, NSE oder NVE in Ihrem System integriert sind, finden Sie unter Stellen Sie OKM, NSE und NVE nach Bedarf wieder her
   - Wenn keymanager, NSE oder NVE auf Ihrem System nicht konfiguriert sind, führen Sie die Schritte in diesem Abschnitt aus.
6. Geben Sie an der LOADER-Eingabeaufforderung das ein `boot_ontap` Befehl.

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

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

   Wenn Schnittstellen als „falsch“ aufgeführt sind, stellen Sie diese Schnittstellen mithilfe der zurück auf ihren Home Port `net int revert` Befehl.
10. Bewegen Sie das Konsolenkabel auf den reparierten Controller und führen Sie den aus `version -v` Befehl zum Prüfen der ONTAP-Versionen.
11. Stellen Sie die automatische Rückgabe wieder her, wenn Sie die Funktion mithilfe von deaktivieren `storage failover modify -node local -auto-giveback true` Befehl.

Stellen Sie OKM, NSE und NVE nach Bedarf wieder her – AFF A250

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

1. Bestimmen Sie den Abschnitt, den Sie zum Wiederherstellen Ihrer OKM-, NSE- oder NVE-Konfigurationen verwenden sollten: Wenn NSE oder NVE zusammen mit Onboard Key Manager aktiviert sind, müssen Sie die zu Beginn dieses Verfahrens erfassten Einstellungen wiederherstellen.
   - Wenn NSE oder NVE aktiviert sind und der Onboard Key Manager aktiviert ist, wechseln Sie zu wenn Onboard Key Manager aktiviert ist.

- Wenn NSE oder NVE für ONTAP 9.6 aktiviert sind, finden Sie unter Stellen Sie NSE/NVE auf Systemen mit ONTAP 9.6 und höher wieder her.

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

Schritte

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

Wenn die Konsole angezeigt wird…	Dann…
Die LOADER-Eingabeaufforderung	Starten des Controllers zum Boot-Menü: `boot_ontap menu`
Warten auf Zurückgeben	a. Eingabe `Ctrl-C` An der Eingabeaufforderung b. Bei der Meldung: Möchten Sie diesen Knoten anhalten, anstatt [y/n] zu warten? , Geben Sie ein: `y` c. Geben Sie an der LOADER-Eingabeaufforderung den ein `boot_ontap menu` Befehl.

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

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

Beispiel für Backup-Daten:

```
---------------------------- BACKUP-----------------------------------
TmV0QXBwIETERTABCbGaiAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA . . .
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAA

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

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

   Das System startet zum Warten auf Giveback… Eingabeaufforderung.

8. Stellen Sie das Konsolenkabel auf den Partner Controller um und melden Sie sich als „admin“ an.
9. Überprüfen Sie, ob der Ziel-Controller bereit ist für die Rückgabe an den `storage failover show` Befehl.
10. GiveBack nur der CFO sammelt mit dem `storage failover giveback -fromnode local -only -cfo-aggregates true` Befehl.
    - Wenn der Befehl aufgrund eines ausgefallenen Laufwerks ausfällt, setzen Sie die ausgefallene Festplatte physisch aus, lassen Sie sie aber in den Steckplatz, bis ein Austausch erfolgt.
    - Wenn der Befehl aufgrund von offenen CIFS-Sitzungen ausfällt, wenden Sie sich an den Kunden, wie CIFS-Sitzungen abgeschlossen werden können.

      Die Beendigung von CIFS kann zu Datenverlust führen.

    - Wenn der Befehl fehlschlägt, weil der Partner „nicht bereit“ ist, warten Sie 5 Minuten, bis die NVMEMs synchronisiert werden.
    - Wenn der Befehl aufgrund eines NDMP-, SnapMirror- oder SnapVault-Prozesses ausfällt, deaktivieren Sie den Prozess. Weitere Informationen finden Sie im entsprechenden Documentation Center.
11. Sobald die Rückgabe abgeschlossen ist, überprüfen Sie den Failover- und Giveback-Status mit `storage failover show` Und `storage failover show`-GiveBack`-Befehle.

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

12. Schieben Sie das Konsolenkabel auf den Ziel-Controller.
    a. Wenn Sie ONTAP 9.6 oder höher verwenden, führen Sie die integrierte Synchronisierung des Security Key-Managers aus:
    b. Führen Sie die aus `security key-manager onboard sync` Geben Sie bei der entsprechenden Aufforderung die Passphrase ein.
    c. Geben Sie das ein `security key-manager key query` Befehl zum Anzeigen einer detaillierten Ansicht aller im Onboard-Schlüsselmanager gespeicherten Schlüssel und zur Überprüfung des s `Restored` Spalte = `yes/true` Für alle Authentifizierungsschlüssel.

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

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

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

16. Geben Sie an der Clustershell-Eingabeaufforderung den ein `net int show -is-home false` Befehl

zum Auflistung der logischen Schnittstellen, die sich nicht auf ihrem Home Controller und Port befinden.

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

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

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

Schritte

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

Wenn die Konsole angezeigt wird…	Dann…
Die Eingabeaufforderung für die Anmeldung	Fahren Sie mit Schritt 7 fort.
Warten auf Giveback…	a. Melden Sie sich beim Partner-Controller an. b. Überprüfen Sie, ob der Ziel-Controller bereit ist für die Rückgabe an den `storage failover show` Befehl.

4. Bewegen Sie das Konsolenkabel zum Partner-Controller und geben Sie den Ziel-Controller-Storage mithilfe des zurück `storage failover giveback -fromnode local -only-cfo-aggregates true local` Befehl.
   - Wenn der Befehl aufgrund eines ausgefallenen Laufwerks ausfällt, setzen Sie die ausgefallene Festplatte physisch aus, lassen Sie sie aber in den Steckplatz, bis ein Austausch erfolgt.
   - Wenn der Befehl aufgrund von offenen CIFS-Sitzungen ausfällt, wenden Sie sich an den Kunden, wie CIFS-Sitzungen abgeschlossen werden können.

     Die Beendigung von CIFS kann zu Datenverlust führen.

   - Wenn der Befehl fehlschlägt, weil der Partner „nicht bereit“ ist, warten Sie 5 Minuten, bis die NVMEMs synchronisiert werden.
   - Wenn der Befehl aufgrund eines NDMP-, SnapMirror- oder SnapVault-Prozesses ausfällt, deaktivieren Sie den Prozess. Weitere Informationen finden Sie im entsprechenden Documentation Center.
5. Warten Sie 3 Minuten, und überprüfen Sie den Failover-Status mit `storage failover show` Befehl.
6. Geben Sie an der Clustershell-Eingabeaufforderung den ein `net int show -is-home false` Befehl zum Auflistung der logischen Schnittstellen, die sich nicht auf ihrem Home Controller und Port befinden.

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

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

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

      Verwenden Sie die `security key-manager key query` Befehl zum Überprüfen des `Restored` Spalte = `yes/true` Für alle Authentifizierungsschlüssel.
11. Schließen Sie das Konsolenkabel an den Partner Controller an.
12. Geben Sie den Controller mithilfe des zurück `storage failover giveback -fromnode local` Befehl.
13. Stellen Sie die automatische Rückgabe wieder her, wenn Sie die Funktion mithilfe von deaktivieren `storage failover modify -node local -auto-giveback true` Befehl.

Senden Sie das fehlerhafte Teil an NetApp - AFF A250 zurück

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

Copyright-Informationen

Copyright © 2024 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.