Boot-Medien

Install and maintain

NetApp
March 24, 2023

Inhaltsverzeichnis

Boot-Medien

Übersicht über den Austausch von Bootmedien - AFF A320

Das Boot-Medium speichert einen primären und sekundären Satz von Systemdateien (Boot-Image), die das System beim Booten verwendet. Je nach Netzwerkkonfiguration können Sie entweder einen unterbrechungsfreien oder störenden Austausch durchführen.

Sie müssen über ein USB-Flash-Laufwerk verfügen, das auf FAT32 formatiert ist, und über die entsprechende Speichermenge, um die zu speichern `image_xxx.tgz` Datei:

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

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

Integrierte Verschlüsselungsschlüssel - AFF A320

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

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

Schritte

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

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 integrierte Passphrase für das Verschlüsselungsmanagement des Kunden ein. Falls die Passphrase nicht angegeben werden kann, wenden Sie sich an den NetApp Support. "mysupport.netapp.com"

   b. Überprüfen Sie die `Restored` In der Spalte wird angezeigt `yes` Für alle Authentifizierungsschlüssel: `security key-manager key-query`
   c. Überprüfen Sie das `Key Manager` Typ zeigt an `onboard`, Und dann manuell sichern Sie die OKM-Informationen.
   d. Wechseln Sie zum erweiterten Berechtigungsebene-Modus, und geben Sie ein `y` Wenn Sie dazu aufgefordert werden, fortzufahren: `set -priv advanced`

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

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

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

h. Sie können den Controller sicher herunterfahren.

Überprüfen der NSE-Konfiguration

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

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

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

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

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

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

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

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

   e. Sie können den Controller sicher herunterfahren.

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

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

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

   "mysupport.netapp.com"

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

b. Sie können den Controller sicher herunterfahren.

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

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

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

   "mysupport.netapp.com"

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

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

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

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

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

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

   g. Sie können den Controller sicher herunterfahren.

Fahren Sie den Knoten herunter – AFF A320

Nach Abschluss der NVE oder NSE-Aufgaben müssen Sie den Shutdown des beeinträchtigten Nodes durchführen. Fahren Sie den Controller mit eingeschränkter Konfiguration herunter oder übernehmen Sie ihn entsprechend.

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.

Wenn der eingeschränkte Controller angezeigt wird…	Dann…
`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: Das System befindet sich in einem MetroCluster

> 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	Wechseln Sie zu Controller-Modul entfernen.
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`.

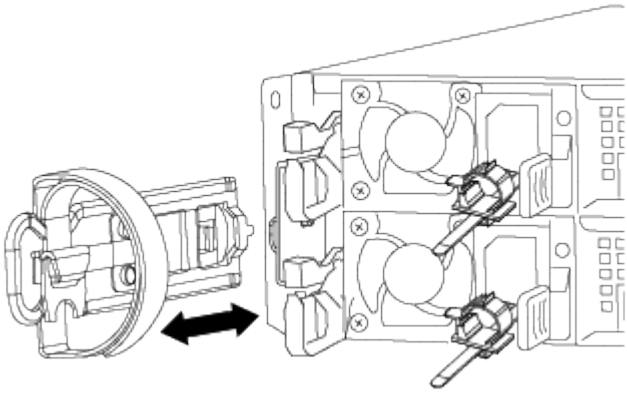
Ersetzen Sie die Startmedien - AFF A320

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

Schritt 1: Entfernen Sie das Controller-Modul

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

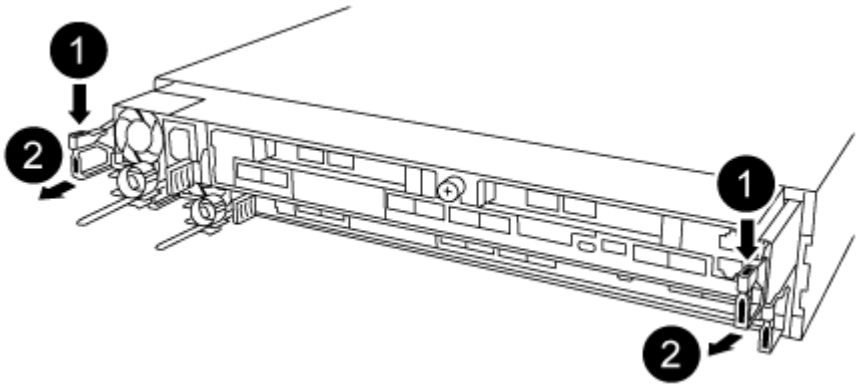
1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
2. Trennen Sie das Netzteil des Controller-Moduls von der Stromversorgung.
3. Lösen Sie den Haken- und Schlaufenriemen, mit dem die Kabel am Kabelführungsgerät befestigt sind, und ziehen Sie dann die Systemkabel und SFPs (falls erforderlich) vom Controller-Modul ab, um zu verfolgen, wo die Kabel angeschlossen waren.



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

4. Entfernen Sie die Kabelführungsgeräte von der linken und rechten Seite des Controller-Moduls und stellen Sie sie zur Seite.

5. Entfernen Sie das Controller-Modul aus dem Chassis:



   a. Setzen Sie den Zeigefinger in den Verriegelungsmechanismus auf beiden Seiten des Controller-Moduls ein.

   b. Drücken Sie auf die orangefarbene Lasche oben am Verriegelungsmechanismus nach unten, bis der Rastbolzen am Gehäuse entfernt wird.

      Der Haken des Verriegelungsmechanismus sollte fast senkrecht sein und sich vom Chassispindel frei sein.

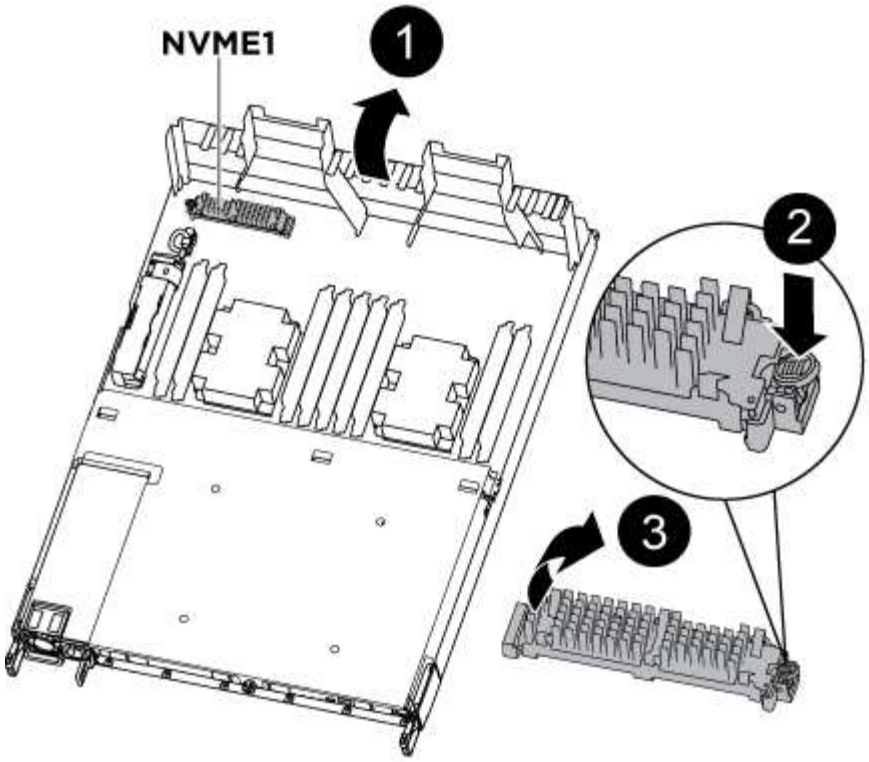
   c. Ziehen Sie das Controller-Modul vorsichtig einige Zentimeter zu Ihnen, damit Sie die Seiten des Controller-Moduls erfassen können.

   d. Ziehen Sie das Controller-Modul vorsichtig mit beiden Händen aus dem Gehäuse und legen Sie es auf eine flache, stabile Oberfläche.

Schritt 2: Ersetzen Sie die Startmedien

Sie müssen das Startmedium im Controller-Modul finden und dann die Anweisungen befolgen, um es auszutauschen.

1. Öffnen Sie den Luftkanal, und suchen Sie das Boot-Medium mithilfe der folgenden Abbildung oder der FRU-Zuordnung auf dem Controller-Modul:
2. Suchen und entfernen Sie die Startmedien aus dem Controller-Modul:



a. Drücken Sie die blaue Taste am Ende des Startmediums, bis der Lip auf dem Boot-Medium die blaue Taste löscht.

b. Drehen Sie das Startmedium nach oben, und ziehen Sie das Startmedium vorsichtig aus dem Sockel.

   i. 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.

3. Sperren Sie das Boot-Medium:

   a. Drehen Sie das Startmedium nach unten zur Hauptplatine.

   b. Platzieren Sie einen Finger am Ende des Startmediums mit der blauen Taste und drücken Sie das Bootmedium-Ende nach unten, um die blaue Verriegelungstaste zu berühren.

   c. Heben Sie beim Drücken auf die Startmedien die blaue Verriegelungstaste an, um die Boot-Medien zu verriegeln.

4. Schließen Sie den Luftkanal.

Schritt 3: Übertragen Sie das Startabbild über ein USB-Flash-Laufwerk auf die Startmedien

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

- 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.
   i. Laden Sie das Service-Image auf Ihren Arbeitsbereich auf Ihrem Laptop herunter.
   ii. Entpacken Sie das Service-Image.

   > Wenn Sie den Inhalt mit Windows extrahieren, verwenden Sie winzip nicht zum Extrahieren des Netzboots-Images. Verwenden Sie ein anderes Extraktionstool, wie 7-Zip oder WinRAR.

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

   - Booten
   - efi

   iii. 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.

   iv. Entfernen Sie das USB-Flash-Laufwerk von Ihrem Laptop.

b. Wenn Sie dies noch nicht getan haben, schließen Sie den Luftkanal.

c. Richten Sie das Ende des Controller-Moduls an der Öffnung im Gehäuse aus, und drücken Sie dann vorsichtig das Controller-Modul zur Hälfte in das System.

d. Installieren Sie das Kabelverwaltungsgerät neu und führen Sie das System nach Bedarf wieder ein.

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

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

f. Stecken Sie das USB-Flash-Laufwerk in den USB-Steckplatz des Controller-Moduls.

   Stellen Sie sicher, dass Sie das USB-Flash-Laufwerk in den für USB-Geräte gekennzeichneten Steckplatz und nicht im USB-Konsolenport installieren.

g. Führen Sie die Neuinstallation des Controller-Moduls durch:
   i. Stellen Sie sicher, dass die Verriegelungsarme in der ausgestreckten Position verriegelt sind.
   ii. Drücken Sie das Controller-Modul mithilfe der Entriegelungshebel in den Chassis-Schacht, bis der Anschlag einrastet.

   > Drücken Sie den Verriegelungsmechanismus nicht oben in den Verriegelungsarmen nach unten. Dabei den Verriegelungsmechanismus anheben und das Einschieben des Controller-Moduls in das Gehäuse untersagen.

iii. Drücken Sie die orangefarbenen Laschen oben am Verriegelungsmechanismus nach unten und halten Sie sie gedrückt.

iv. Schieben Sie das Controller-Modul vorsichtig in den Gehäuseschacht, bis es bündig an den Kanten des Chassis liegt.

Die Arms des Verriegelungsmechanismus lassen sich in das Gehäuse schieben.

Das Controller-Modul beginnt zu booten, sobald es vollständig im Gehäuse sitzt.

i. Lösen Sie die Verriegelungen, um das Controller-Modul einrasten zu lassen.

ii. Wenn Sie dies noch nicht getan haben, installieren Sie das Kabelverwaltungsgerät neu.

a. Unterbrechen Sie den Boot-Vorgang, indem Sie Strg-C drücken, um an der LOADER-Eingabeaufforderung zu stoppen.

Wenn Sie diese Meldung verpassen, drücken Sie Strg-C, wählen Sie die Option zum Booten im Wartungsmodus aus, und halten Sie dann den Node zum Booten in LOADER.

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

Das Bild wird vom USB-Flash-Laufwerk heruntergeladen.

c. 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.

d. Starten Sie nach der Installation des Images den Wiederherstellungsprozess:

iii. Notieren Sie die IP-Adresse des Node, der auf dem Bildschirm angezeigt wird.

iv. Drücken Sie `y` Wenn Sie aufgefordert werden, die Backup-Konfiguration wiederherzustellen.

v. Drücken Sie `y` Bei Aufforderung zum Überschreiben von /etc/ssh/ssh_Host_dsa_Key.

a. Starten Sie vom Partner-Node auf der erweiterten Berechtigungsebene die Konfigurationssynchronisierung mit der im vorherigen Schritt aufgezeichneten IP-Adresse: `system node restore-backup -node local -target-address` *`impaired_node_IP_address`*

b. Wenn die Wiederherstellung erfolgreich ist, drücken Sie `y` Wenn Sie auf dem Knoten mit eingeschränkter Funktion aufgefordert werden, die wiederhergestellte Kopie zu verwenden?

c. Drücken Sie `y` Wenn Sie sehen, dass der Sicherungsvorgang erfolgreich war, und drücken Sie dann `y` Wenn Sie zum Neubooten des Node aufgefordert werden.

d. Vergewissern Sie sich, dass die Umgebungsvariablen wie erwartet festgelegt sind.

vi. Nehmen Sie den Node zur LOADER-Eingabeaufforderung.

Über die ONTAP Eingabeaufforderung können Sie den Befehl System Node stop -skip-lif-Migration -before-shutdown true -ignore-Quorum-Warns TRUE -emmen-Takeover TRUE ausgeben.

vii. Überprüfen Sie die Einstellungen der Umgebungsvariable mit dem `printenv` Befehl.

viii. Wenn eine Umgebungsvariable nicht wie erwartet festgelegt ist, ändern Sie sie mit dem `setenv` *`environment-variable-name changed-value`* Befehl.

ix. Speichern Sie Ihre Änderungen mit dem `savenv` Befehl.

x. Booten Sie den Node neu.

a. Wenn der neu gebootete Knoten angezeigt wird `Waiting for giveback…` Meldung, führen Sie ein Giveback vom gesunden Knoten aus:

Ihr System befindet sich in…	Dann…
Ein HA-Paar	Nachdem der Knoten „beeinträchtigt“ den angezeigt hat `Waiting for giveback…` Meldung, führen Sie ein Giveback vom gesunden Knoten aus: i. Über den gesunden Knoten: `storage failover giveback -ofnode partner_node_name` Der beeinträchtigte Node nimmt seinen Storage zurück, beendet den Booten und startet dann neu und wird erneut vom gesunden Node übernommen. Wenn das Rückübertragung ein Vetorecht ist, können Sie erwägen, das Vetos außer Kraft zu setzen. "ONTAP 9 High-Availability Configuration Guide" ii. Überwachen Sie den Status des Giveback-Vorgangs mithilfe von `storage failover show-giveback` Befehl. iii. Nach Abschluss des Giveback-Vorgangs bestätigen Sie, dass das HA-Paar ordnungsgemäß funktioniert und dass ein Takeover mithilfe des möglich ist `storage failover show` Befehl. iv. Stellen Sie das automatische Giveback wieder her, wenn Sie es mithilfe des Storage Failover modify-Befehls deaktiviert haben.

b. Beenden Sie die erweiterte Berechtigungsebene auf dem gesunden Node.

Starten Sie das Recovery-Image – AFF A320

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 das var-Dateisystem wieder her:

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 Schritte zum Austausch von Medien nach dem Booten für OKM, NSE und NVE
- 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.

Stellen Sie OKM, NSE und NVE nach Bedarf wieder her – AFF A320

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----------------------------------
   TmV0QXBwIETERTABCbGaiAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA . . .
   H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
   AAAAAAAAAAAAAAAAAAAAAAAA

   ---------------------------------- 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` 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` 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 A320

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