Boot-Medien

Install and maintain

NetApp
March 24, 2023

Inhaltsverzeichnis

Boot-Medien . . . 1
- Überblick über den Austausch von Boot-Medien - AFF A700s . . . 1
- Integrierte Verschlüsselungsschlüssel - AFF A700s . . . 1
- Herunterfahren des Controllers - AFF A700s . . . 8
- Setzen Sie das Boot-Medium AFF A700s wieder ein . . . 9
- Übertragen Sie das Boot-Image auf das Boot-Medium AFF A700s . . . 13
- Starten des Recovery-Images – AFF A700s . . . 19
- Stellen Sie OKM, NSE und NVE nach Bedarf wieder her – AFF A700s . . . 21
- Senden Sie das fehlgeschlagene Teil an NetApp - AFF A700s zurück . . . 27

Boot-Medien

Überblick über den Austausch von Boot-Medien - AFF A700s

Das primäre Boot-Medium speichert das ONTAP Boot-Image, das das System beim Booten verwendet. Sie können das primäre Startmedienabbild wiederherstellen, indem Sie das ONTAP-Image auf dem sekundären Startmedium oder falls erforderlich über ein USB-Flash-Laufwerk verwenden.

Wenn das sekundäre Startmedium ausgefallen ist oder die Datei image.tgz fehlt, müssen Sie das primäre Startmedium über ein USB-Flash-Laufwerk wiederherstellen. Das Laufwerk muss in FAT32 formatiert sein und über die entsprechende Menge Speicherplatz verfügen, um die Datei image_xxx.tgz zu speichern.

- Der Ersatzprozess stellt das var-Dateisystem vom sekundären Bootmedium oder USB-Flash-Laufwerk auf den primären Bootmedium wieder her.
- 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 Controller *Impared* ist der Controller, an dem Sie Wartungsarbeiten durchführen.
  - Der *Healthy* Controller ist der HA-Partner des beeinträchtigten Controllers.

Integrierte Verschlüsselungsschlüssel - AFF A700s

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 9.5 ausgeführt wird, fahren Sie mit fort [Option 1: Prüfen von NVE oder NSE auf Systemen mit ONTAP 9.5 und früher].
   - Wenn <lno-DARE> nicht in der Befehlsausgabe angezeigt wird und auf dem System ONTAP 9.6 oder höher ausgeführt wird, fahren Sie mit fort [Option 2: Prüfen von NVE oder NSE auf Systemen mit ONTAP 9.6 und höher].
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`

Option 1: Prüfen Sie NVE oder NSE auf Systemen mit ONTAP 9.5 und früher

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

Schritte

1. Schließen Sie das Konsolenkabel an den beeinträchtigten Controller an.
2. Überprüfen Sie, ob NVE für alle Volumes im Cluster konfiguriert ist: `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 ist.
3. Überprüfen Sie, ob NSE konfiguriert 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 überprüfen.
   - Wenn NVE und NSE nicht konfiguriert sind, kann der beeinträchtigte Controller sicher heruntergefahren werden.

Überprüfen der NVE-Konfiguration

Schritte

1. Anzeigen der Schlüssel-IDs der Authentifizierungsschlüssel, die auf den Schlüsselverwaltungsservern gespeichert sind: `security key-manager query`
   - Wenn der `Restored` Spalte wird angezeigt `yes` Außerdem werden alle Schlüsselmanager angezeigt `available`, Es ist sicher, den beeinträchtigten Regler herunterzufahren.
   - Wenn der `Restored` Spalte zeigt alle anderen als an `yes`, Oder wenn ein Schlüsselmanager angezeigt wird `unavailable`, Sie müssen einige zusätzliche Schritte.

◦ Wenn die Meldung angezeigt wird dieser Befehl wird nicht unterstützt, wenn die integrierte Schlüsselverwaltung aktiviert ist, müssen Sie einige weitere Schritte durchführen.

2. Wenn der `Restored` Spalte hat andere als angezeigt `yes`, Oder wenn ein Schlüsselmanager angezeigt `unavailable`:

   a. Abrufen und Wiederherstellen aller Authentifizierungsschlüssel und der zugehörigen Schlüssel-IDs: `security key-manager restore -address *`

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

   "mysupport.netapp.com"

   a. Überprüfen Sie das `Restored` Spalte wird angezeigt `yes` Für alle Authentifizierungsschlüssel und dass alle Schlüsselmanager angezeigt werden `available`: `security key-manager query`

   b. Schalten Sie den beeinträchtigten Regler aus.

3. Wenn Sie die Meldung gesehen haben dieser Befehl wird nicht unterstützt, wenn die integrierte Schlüsselverwaltung aktiviert ist, zeigen Sie die im Onboard-Schlüsselmanager gespeicherten Schlüssel an: `security key-manager key show -detail`

   a. Wenn der `Restored` Spalte wird angezeigt `yes` Manuelle Sicherung der Informationen zum Onboard-Verschlüsselungsmanagement:

      - Wechseln Sie zum erweiterten Berechtigungsebene-Modus, und geben Sie ein `y` Wenn Sie dazu aufgefordert werden, fortzufahren: `set -priv advanced`
      - Geben Sie den Befehl ein, um die OKM Backup-Informationen anzuzeigen: `security key-manager backup show`
      - 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.
      - Zurück zum Admin-Modus: `set -priv admin`
      - Schalten Sie den beeinträchtigten Regler aus.

   b. Wenn der `Restored` Spalte zeigt alle anderen als an `yes`:

      - Führen Sie den Setup-Assistenten für den Schlüsselmanager aus: `security key-manager setup -node target/impaired node name`

        Geben Sie an der Eingabeaufforderung die integrierte Passphrase für das Verschlüsselungsmanagement des Kunden ein. Wenn die Passphrase nicht angegeben werden kann, wenden Sie sich an "mysupport.netapp.com"

      - Überprüfen Sie das `Restored` Spalte wird angezeigt `yes` Für alle Authentifizierungsschlüssel: `security key-manager key show -detail`
      - Wechseln Sie zum erweiterten Berechtigungsebene-Modus, und geben Sie ein `y` Wenn Sie dazu aufgefordert werden, fortzufahren: `set -priv advanced`
      - Geben Sie den Befehl ein, um die OKM Backup-Informationen anzuzeigen: `security key-manager backup show`
      - 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.

- Zurück zum Admin-Modus: `set -priv admin`
- Sie können den Controller sicher herunterfahren.

Überprüfen der NSE-Konfiguration

Schritte

1. Anzeigen der Schlüssel-IDs der Authentifizierungsschlüssel, die auf den Schlüsselverwaltungsservern gespeichert sind: `security key-manager query`
   - Wenn der `Restored` Spalte wird angezeigt `yes` Außerdem werden alle Schlüsselmanager angezeigt `available`, Es ist sicher, den beeinträchtigten Regler herunterzufahren.
   - Wenn der `Restored` Spalte zeigt alle anderen als an `yes`, Oder wenn ein Schlüsselmanager angezeigt wird `unavailable`, Sie müssen einige zusätzliche Schritte.
   - Wenn die Meldung angezeigt wird dieser Befehl wird nicht unterstützt, wenn die integrierte Schlüsselverwaltung aktiviert ist, müssen Sie einige weitere Schritte durchführen
2. Wenn der `Restored` Spalte hat andere als angezeigt `yes`, Oder wenn ein Schlüsselmanager angezeigt `unavailable`:
   a. Abrufen und Wiederherstellen aller Authentifizierungsschlüssel und der zugehörigen Schlüssel-IDs: `security key-manager restore -address *`

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

   "mysupport.netapp.com"

   a. Überprüfen Sie das `Restored` Spalte wird angezeigt `yes` Für alle Authentifizierungsschlüssel und dass alle Schlüsselmanager angezeigt werden `available`: `security key-manager query`
   b. Schalten Sie den beeinträchtigten Regler aus.
3. Wenn Sie die Meldung gesehen haben dieser Befehl wird nicht unterstützt, wenn die integrierte Schlüsselverwaltung aktiviert ist, zeigen Sie die im Onboard-Schlüsselmanager gespeicherten Schlüssel an: `security key-manager key show -detail`
   a. Wenn der `Restored` Spalte wird angezeigt `yes`, Manuelle Sicherung der Informationen zum Onboard-Verschlüsselungsmanagement:
      - Wechseln Sie zum erweiterten Berechtigungsebene-Modus, und geben Sie ein `y` Wenn Sie dazu aufgefordert werden, fortzufahren: `set -priv advanced`
      - Geben Sie den Befehl ein, um die OKM Backup-Informationen anzuzeigen: `security key-manager backup show`
      - 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.
      - Zurück zum Admin-Modus: `set -priv admin`
      - Schalten Sie den beeinträchtigten Regler aus.
   b. Wenn der `Restored` Spalte zeigt alle anderen als an `yes`:
      - Führen Sie den Setup-Assistenten für den Schlüsselmanager aus: `security key-manager setup -node target/impaired node name`

Geben Sie die OKM-Passphrase des Kunden an der Eingabeaufforderung ein. Wenn die Passphrase nicht angegeben werden kann, wenden Sie sich an "mysupport.netapp.com"

- Überprüfen Sie das `Restored` In der Spalte wird angezeigt `yes` Für alle Authentifizierungsschlüssel: `security key-manager key show -detail`
- Wechseln Sie zum erweiterten Berechtigungsebene-Modus, und geben Sie ein `y` Wenn Sie dazu aufgefordert werden, fortzufahren: `set -priv advanced`
- Geben Sie den Befehl ein, um die OKM-Informationen zu sichern: `security key-manager backup show`

Stellen Sie sicher, dass OKM-Informationen in Ihrer Protokolldatei gespeichert werden. Diese Informationen werden in Disaster-Szenarien benötigt, in denen OKM möglicherweise manuell wiederhergestellt werden muss.

- Kopieren Sie den Inhalt der Sicherungsinformationen in eine separate Datei oder Ihr Protokoll. Sie werden es in Disaster-Szenarien benötigen, in denen Sie OKM manuell wiederherstellen müssen.
- Zurück zum Admin-Modus: `set -priv admin`
- Sie können den Controller sicher herunterfahren.

Option 2: 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.

Herunterfahren des Controllers - AFF A700s

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.

Setzen Sie das Boot-Medium AFF A700s wieder ein

Sie müssen das Controller-Modul aus dem Chassis entfernen, öffnen und dann das ausgefallene Boot-Medium ersetzen.

Schritt 1: Entfernen Sie das Controller-Modul

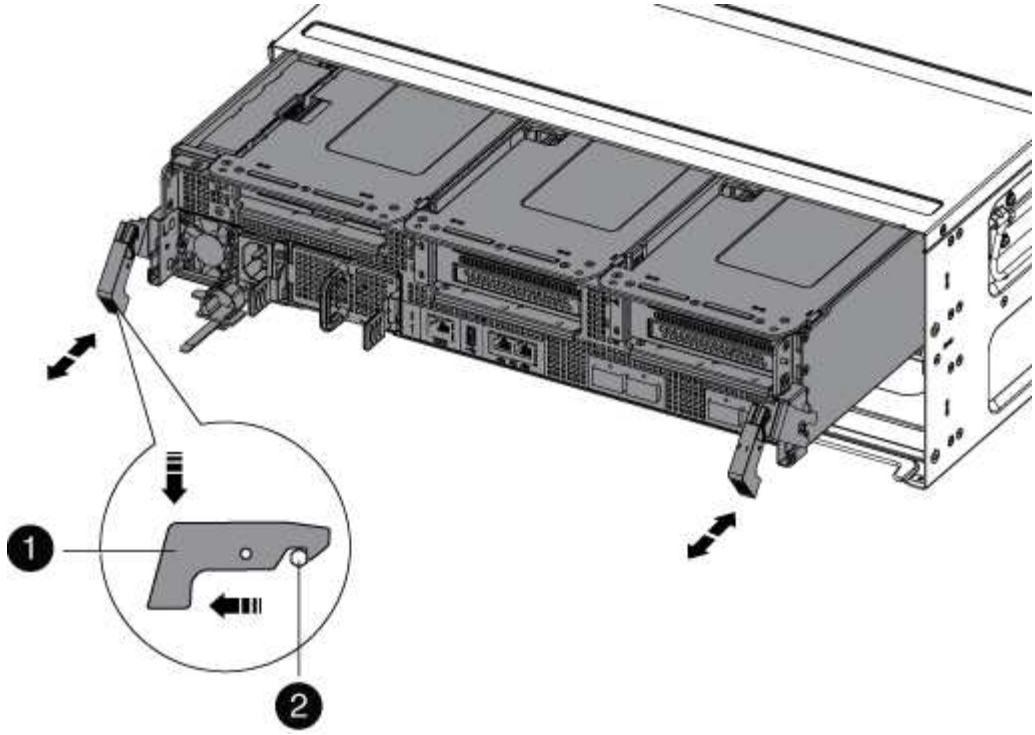
Sie müssen das Controller-Modul aus dem Chassis entfernen, wenn Sie das Controller-Modul ersetzen oder eine Komponente im Controller-Modul ersetzen.

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

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

3. Trennen Sie das Netzteil des Controller-Moduls von der Quelle, und ziehen Sie dann das Kabel vom Netzteil ab.
4. Entfernen Sie das Kabelführungs-Gerät aus dem Controller-Modul und legen Sie es beiseite.
5. Drücken Sie beide Verriegelungsriegel nach unten, und drehen Sie dann beide Verriegelungen gleichzeitig nach unten.

   Das Controller-Modul wird leicht aus dem Chassis entfernt.

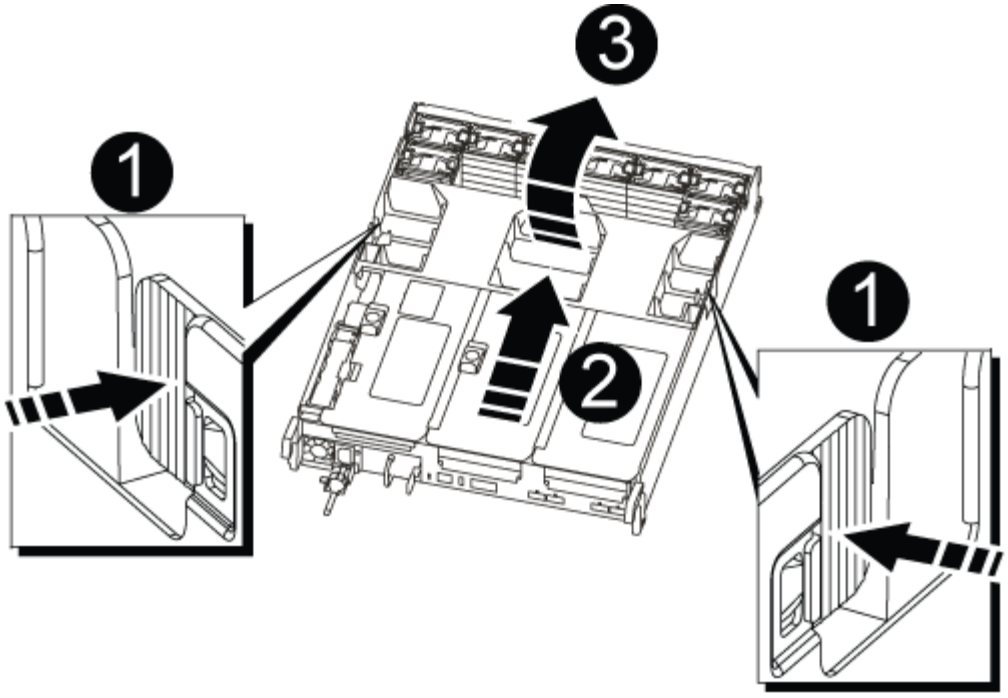


1	
Verriegelungsverschluss	
2	
Sicherungsstift	

1. Schieben Sie das Controller-Modul aus dem Gehäuse.

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

2. Das Steuermodul auf eine stabile, flache Oberfläche legen und den Luftkanal öffnen:
   a. Drücken Sie die Verriegelungslaschen an den Seiten des Luftkanals in Richtung der Mitte des Controller-Moduls.
   b. Schieben Sie den Luftkanal in Richtung der Lüftermodule, und drehen Sie ihn dann nach oben in die vollständig geöffnete Position.



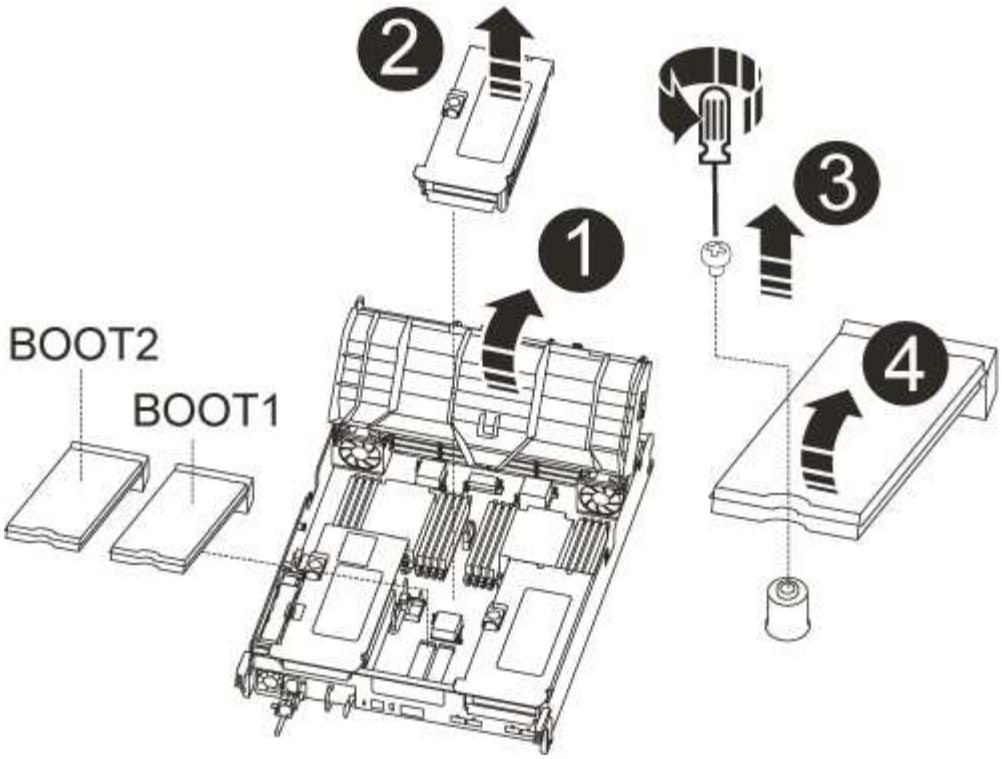
1	Verriegelungsklammern für Luftkanäle
2	Riser
3	Luftkanal

Schritt 2: Ersetzen Sie die Startmedien - AFF A700s

Sie müssen das ausgefallene Startmedium im Controller-Modul finden, indem Sie das mittlere PCIe-Modul am Controller-Modul entfernen, das ausgefallene Startmedium suchen und dann das Boot-Medium ersetzen.

Sie benötigen einen Kreuzschlitzschraubendreher, um die Schraube zu entfernen, mit der die Bootmedien befestigt sind.

1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
2. Suchen Sie das Startmedium:
    a. Öffnen Sie den Luftkanal, falls erforderlich.
    b. Entfernen Sie bei Bedarf die Riserkarte 2, das mittlere PCIe-Modul, indem Sie die Sperrklinke entriegeln und dann den Riser aus dem Controller-Modul entfernen.



1	
Luftkanal	
2	
Riser 2 (mittleres PCIe-Modul)	
3	
Schraube für Boot-Medien	
4	
Boot-Medien	

3. Suchen Sie das ausgefallene Startmedium.
4. Entfernen Sie die Boot-Medien aus dem Controller-Modul:
   a. Entfernen Sie mit einem #1 Kreuzschlitzschraubendreher die Schraube, mit der das Bootmedium befestigt ist, und setzen Sie die Schraube an einem sicheren Ort beiseite.
   b. Fassen Sie die Seiten des Startmediums an, drehen Sie die Startmedien vorsichtig nach oben, ziehen Sie dann die Startmedien gerade aus dem Sockel und legen Sie sie beiseite.
5. Richten Sie die Kanten des Ersatzstartmediums an der Buchse des Boot-Mediums aus, und schieben Sie

ihn dann vorsichtig in die Buchse.

6. 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.

7. Drehen Sie das Boot-Medium nach unten, bis es mit der Hauptplatine bündig ist.
8. Befestigen Sie die Boot-Medien mit der Schraube.

   Ziehen Sie die Schraube nicht zu fest. Dadurch kann die Boot-Media-Leiterplatte knacken.

9. Setzen Sie den Riser wieder in das Controller-Modul ein.
10. Luftkanal schließen:
    a. Den Luftkanal nach unten drehen.
    b. Schieben Sie den Luftkanal in Richtung der Steigleitungen, bis er einrastet.

Übertragen Sie das Boot-Image auf das Boot-Medium AFF A700s

Sie können das System-Image auf dem Ersatzstartmedium installieren. Verwenden Sie dazu entweder das Image auf dem zweiten Boot-Medium, das im Controller-Modul installiert ist, die primäre Methode zur Wiederherstellung des System-Images. Oder indem Sie das Boot-Image über ein USB-Flash-Laufwerk auf das Boot-Medium übertragen, wenn die Wiederherstellung des sekundären Startmediums fehlgeschlagen ist oder wenn die Datei image.tgz nicht auf dem sekundären Startmedium gefunden wurde.

Option 1: Übertragen Sie Dateien auf das Boot-Medium mit Backup Recovery von dem zweiten Boot-Medium

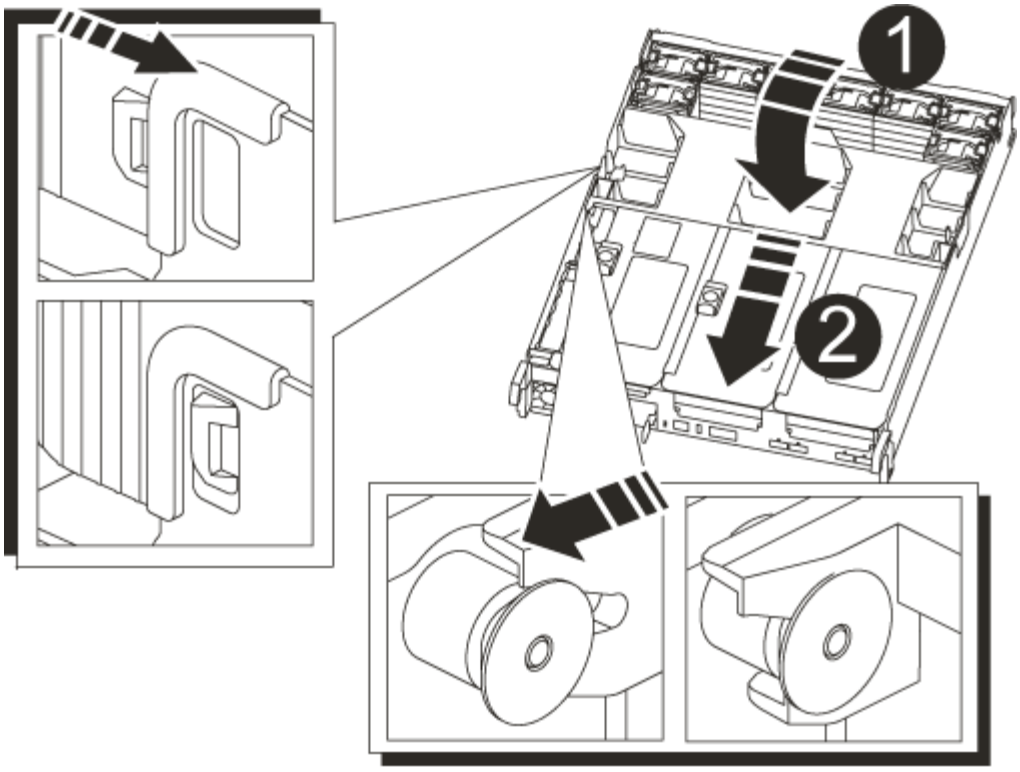
Sie können das System-Image mithilfe des Images auf dem zweiten Boot-Medium installieren, das im Controller-Modul installiert ist. Dies ist die primäre Methode zur Übertragung der Boot-Mediendateien auf die Ersatz-Boot-Medien in Systemen mit zwei Boot-Medien im Controller-Modul.

Das Image auf dem sekundären Startmedium muss einen enthalten `image.tgz` Datei und darf keine Fehler melden. Wenn die Datei image.tgz fehlt oder das Boot-Medium Fehler meldet, können Sie dieses Verfahren nicht verwenden. Sie müssen das Startabbild mithilfe des Austauschvorgangs für das USB-Flash-Laufwerk auf das Ersatzmedium übertragen.

Schritte

1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
2. Wenn Sie dies noch nicht getan haben, schließen Sie den Luftkanal:

   a. Schwenken Sie den Luftkanal bis nach unten zum Controller-Modul.
   b. Schieben Sie den Luftkanal in Richtung der Steigleitungen, bis die Verriegelungslaschen einrasten.
   c. Überprüfen Sie den Luftkanal, um sicherzustellen, dass er richtig sitzt und fest sitzt.



1	
Luftkanal	
2	
Riser	

3. 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.
4. Installieren Sie das Kabelverwaltungsgerät neu und führen Sie das System nach Bedarf wieder ein.

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

5. Schließen Sie das Netzteil wieder an, und schließen Sie es an die Stromquelle an.

   Vergewissern Sie sich, dass Sie den Sicherungsring des Netzkabels wieder am Netzkabel anbringen.

6. Schieben Sie das Controller-Modul vorsichtig ganz in das System, bis sich die Verriegelungshaken des Controller-Moduls erheben, drücken Sie fest auf die Verriegelungshaken, um den Sitz des Controller-Moduls zu beenden, und schwenken Sie dann die Verriegelungshaken in die verriegelte Position über den Stiften des Controller-Moduls.

   Der Controller beginnt zu booten, sobald er vollständig im Chassis installiert ist.

7. 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 Controller zum Booten in LOADER an.

8. Booten Sie an der LOADER-Eingabeaufforderung das Recovery-Image von dem sekundären Boot-Medium: `boot_recovery`

   Das Image wird von dem sekundären Boot-Medium heruntergeladen.

9. 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.
10. Starten Sie nach der Installation des Images den Wiederherstellungsprozess:
    a. Notieren Sie die IP-Adresse des auf dem Bildschirm angezeigten beeinträchtigten Controllers.
    b. Drücken Sie `y` Wenn Sie aufgefordert werden, die Backup-Konfiguration wiederherzustellen.
    c. Drücken Sie `y` Wenn Sie aufgefordert werden, zu bestätigen, dass der Sicherungsvorgang erfolgreich war.
11. Starten Sie vom Partner-Controller 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`*
12. Nachdem die Konfigurationssynchronisation fehlerfrei abgeschlossen ist, drücken Sie `y` Wenn Sie aufgefordert werden, zu bestätigen, dass der Sicherungsvorgang erfolgreich war.
13. Drücken Sie `y` Wenn Sie gefragt werden, ob Sie die wiederhergestellte Kopie verwenden möchten, drücken Sie dann `y` Wenn Sie dazu aufgefordert werden, den Controller neu zu booten.
14. Beenden Sie die erweiterte Berechtigungsebene auf dem gesunden Controller.

Option 2: Übertragen Sie das Startabbild über ein USB-Flash-Laufwerk auf das Startmedium

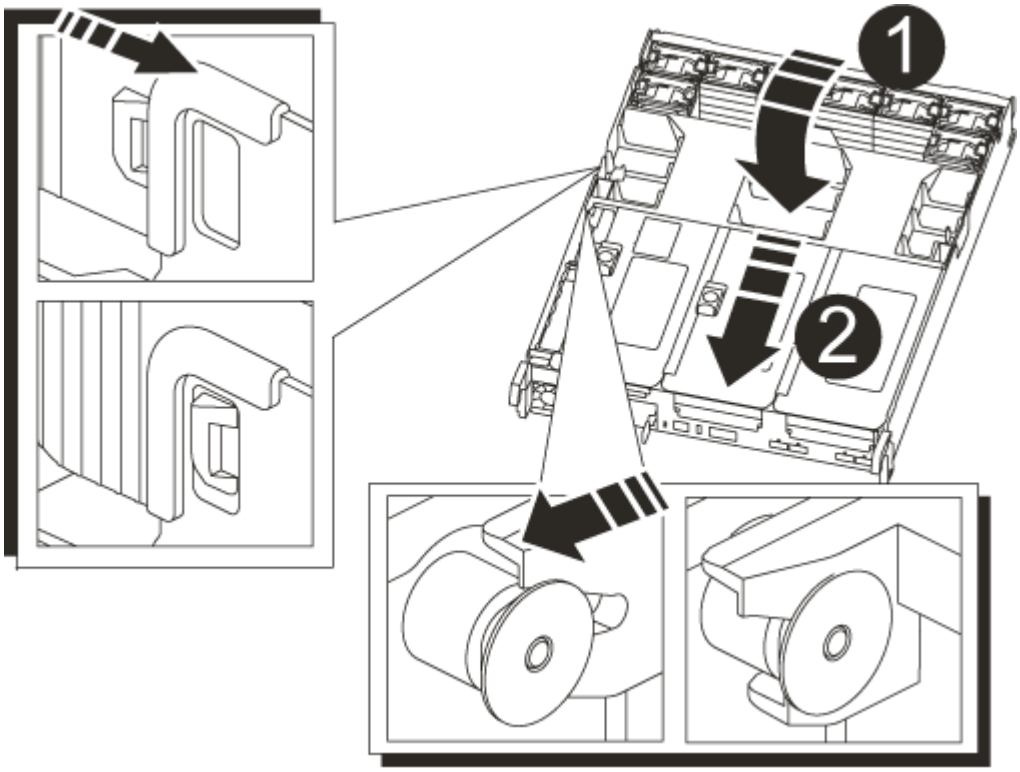
Dieses Verfahren sollte nur verwendet werden, wenn die Wiederherstellung des sekundären Startmediums fehlgeschlagen ist oder wenn die Datei image.tgz auf dem sekundären Startmedium nicht gefunden wird.

- 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 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.

Schritte

1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
2. Wenn Sie dies noch nicht getan haben, schließen Sie den Luftkanal:

a. Schwenken Sie den Luftkanal bis nach unten zum Controller-Modul.
b. Schieben Sie den Luftkanal in Richtung der Steigleitungen, bis die Verriegelungslaschen einrasten.
c. Überprüfen Sie den Luftkanal, um sicherzustellen, dass er richtig sitzt und fest sitzt.



1	
Luftkanal	
2	
Riser	

3. 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.
4. Installieren Sie das Kabelverwaltungsgerät neu und führen Sie das System nach Bedarf wieder ein.

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

5. Schließen Sie das Netzteil wieder an, und schließen Sie es an die Stromquelle an.

   Vergewissern Sie sich, dass Sie den Sicherungsring des Netzkabels wieder am Netzkabel anbringen.

6. 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.

7. Schieben Sie das Controller-Modul vorsichtig ganz in das System, bis sich die Verriegelungshaken des Controller-Moduls erheben, drücken Sie fest auf die Verriegelungshaken, um den Sitz des Controller-Moduls zu beenden, und schwenken Sie dann die Verriegelungshaken in die verriegelte Position über den Stiften des Controller-Moduls.

   Der Controller beginnt zu booten, sobald er vollständig im Chassis installiert ist.

8. 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 Controller zum Booten in LOADER an.

9. Obwohl die Umgebungsvariablen und Bootargs beibehalten werden, sollten Sie überprüfen, ob alle erforderlichen Boot-Umgebungsvariablen und Bootargs für Ihren Systemtyp und die Konfiguration über den richtig eingestellt sind `printenv bootarg name` Führen Sie den Befehl und korrigieren Sie alle Fehler mit dem `setenv variable-name <value>` Befehl.
   a. Überprüfen Sie die Boot-Umgebungsvariablen:
      - `bootarg.init.boot_clustered`
      - `partner-sysid`
      - `bootarg.init.flash_optimized` Für AFF C190/AFF A220 (All-Flash FAS)
      - `bootarg.init.san_optimized` Für AFF A220 und All-SAN-Array
      - `bootarg.init.switchless_cluster.enable`
   b. Wenn der External Key Manager aktiviert ist, überprüfen Sie die Bootarg-Werte, die im aufgeführt sind `kenv` ASUP-Ausgabe:
      - `bootarg.storageencryption.support <value>`
      - `bootarg.keymanager.support <value>`
      - `kmip.init.interface <value>`
      - `kmip.init.ipaddr <value>`
      - `kmip.init.netmask <value>`
      - `kmip.init.gateway <value>`
   c. Wenn der Onboard Key Manager aktiviert ist, überprüfen Sie die Bootarg-Werte, die im aufgeführt sind `kenv` ASUP-Ausgabe:
      - `bootarg.storageencryption.support <value>`
      - `bootarg.keymanager.support <value>`
      - `bootarg.onboard_keymanager <value>`
   d. Speichern Sie die Umgebungsvariablen, die Sie mit dem geändert haben `savenv` Befehl
   e. Bestätigen Sie Ihre Änderungen mit der `printenv *variable-name*` Befehl.
10. Starten Sie von der LOADER-Eingabeaufforderung das Recovery-Image vom USB-Flash-Laufwerk: `boot_recovery`

    Das Bild wird vom USB-Flash-Laufwerk heruntergeladen.

11. 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.
12. Starten Sie nach der Installation des Images den Wiederherstellungsprozess:
    a. Notieren Sie die IP-Adresse des auf dem Bildschirm angezeigten beeinträchtigten Controllers.
    b. Drücken Sie `y` Wenn Sie aufgefordert werden, die Backup-Konfiguration wiederherzustellen.
    c. Drücken Sie `y` Wenn Sie aufgefordert werden, zu bestätigen, dass der Sicherungsvorgang erfolgreich war.
13. Drücken Sie `y` Wenn Sie gefragt werden, ob Sie die wiederhergestellte Kopie verwenden möchten, drücken Sie dann `y` Wenn Sie dazu aufgefordert werden, den Controller neu zu booten.
14. Starten Sie vom Partner-Controller 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`
15. Nachdem die Konfigurationssynchronisation fehlerfrei abgeschlossen ist, drücken Sie `y` Wenn Sie aufgefordert werden, zu bestätigen, dass der Sicherungsvorgang erfolgreich war.
16. Drücken Sie `y` Wenn Sie gefragt werden, ob Sie die wiederhergestellte Kopie verwenden möchten, drücken Sie dann `y` Wenn Sie dazu aufgefordert werden, den Controller neu zu booten.
17. Vergewissern Sie sich, dass die Umgebungsvariablen wie erwartet festgelegt sind.
    a. Nehmen Sie den Controller zur LOADER-Eingabeaufforderung.

       In der ONTAP-Eingabeaufforderung können Sie den Befehl „System Node halt -skip-lif-Migration -before-shutdown true -ignore-Quorum-Warns true -emmen-Takeover TRUE“ eingeben.

    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 Controller neu.
18. Wenn der neu gestörte Controller den anzeigt `Waiting for giveback…` Meldung, führen Sie eine Rückgabe vom ordnungsgemäßen Controller durch:

Ihr System befindet sich in…	Dann…
Ein HA-Paar	Nachdem der Regler „beeinträchtigt“ den angezeigt hat `Waiting for giveback…` Meldung, führen Sie eine Rückgabe vom ordnungsgemäßen Controller durch: a. Von der gesunden Steuerung: `storage failover giveback -ofnode partner_node_name` Der beeinträchtigte Controller nimmt seine Lagerung zurück, beendet den Bootvorgang und startet dann neu und wird wieder vom gesunden Controller übernommen. Wenn das Rückübertragung ein Vetorecht ist, können Sie erwägen, das Vetos außer Kraft zu setzen. "ONTAP 9 High-Availability Configuration Guide" b. Überwachen Sie den Status des Giveback-Vorgangs mithilfe von `storage failover show-giveback` Befehl. c. 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. d. Stellen Sie die automatische Rückgabe wieder her, wenn Sie die Funktion mithilfe des deaktivieren `storage failover modify` Befehl.

19. Beenden Sie die erweiterte Berechtigungsebene auf dem gesunden Controller.

Starten des Recovery-Images – AFF A700s

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. 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`.

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 `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.

Wenn Sie sehen…	Dann…
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 A700s

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.

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 die zu Beginn dieses Verfahrens erfassten Einstellungen wiederhergestellt werden.

- Wenn NSE oder NVE aktiviert sind und der Onboard Key Manager aktiviert ist, wechseln Sie zu Option 1: Wiederherstellung von NVE oder NSE bei aktiviertem Onboard Key Manager.
- Wenn NSE oder NVE für ONATP 9.5 aktiviert sind, finden Sie unter Option 2: Stellen Sie NSE/NVE auf Systemen mit ONTAP 9.5 und früher wieder her.
- Wenn NSE oder NVE für ONTAP 9.6 aktiviert sind, finden Sie unter Option 3: Stellen Sie NSE/NVE auf Systemen mit ONTAP 9.6 und höher wieder her.

Option 1: Wiederherstellung von NVE oder NSE bei aktiviertem Onboard Key Manager

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 Giveback…	a. Eingabe `Ctrl-C` An der Eingabeaufforderung b. Bei der Nachricht: Möchten Sie den Controller 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----------------------------------
TmV0QXBwIETERTABCbGaiAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA . . .
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAA

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

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

   Das System wird mit gebootet `Waiting for giveback…` Eingabeaufforderung:

8. Stellen Sie das Konsolenkabel auf den Partner-Controller um und melden Sie sich als Administrator an.
9. Überprüfen Sie, ob der Ziel-Controller bereit ist für die Rückgabe an den `storage failover show` Befehl.
10. Geben Sie nur die CFO-Aggregate mit dem Storage Failover Giveback zurück `-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 einer offenen CIFS-Sitzung nicht erfolgreich ausgeführt wird, informieren Sie sich beim Kunden darüber, 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 synchronisieren.
- 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.
13. Wenn Sie ONTAP 9.5 und früher ausführen, führen Sie den Key-Manager Setup-Assistenten aus:
    a. Starten Sie den Assistenten mit `security key-manager setup -nodenodename` Geben Sie dann bei der entsprechenden Aufforderung die Passphrase für das Onboard-Verschlüsselungsmanagement ein.
    b. Geben Sie das ein `key-manager key show -detail` Befehl zum Anzeigen einer detaillierten Ansicht aller im Onboard-Schlüsselmanager gespeicherten Schlüssel und zur Überprüfung des s `Restored` Spalte = `yes` Für alle Authentifizierungsschlüssel.

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

    c. Warten Sie 10 Minuten, bis der Schlüssel über das Cluster synchronisiert wird.
14. Wenn Sie ONTAP 9.6 oder höher verwenden:
    a. Führen Sie die aus `security key-manager onboard sync` Geben Sie bei der entsprechenden Aufforderung die Passphrase ein.
    b. 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.

    c. Warten Sie 10 Minuten, bis der Schlüssel über das Cluster synchronisiert wird.
15. Stellen Sie das Konsolenkabel auf den Partner Controller um.
16. Geben Sie den Ziel-Controller mithilfe des zurück `storage failover giveback -fromnode local` Befehl.
17. 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.

18. 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.

19. Bewegen Sie das Konsolenkabel auf den Ziel-Controller, und führen Sie den aus `version -v` Befehl zum Prüfen der ONTAP-Versionen.
20. 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: Stellen Sie NSE/NVE auf Systemen mit ONTAP 9.5 und früher 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. Verschieben Sie das Konsolenkabel auf den Ziel-Controller und führen Sie die Version aus `-v command` Um die ONTAP-Versionen zu prüfen.
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.

   Dieser Befehl funktioniert nicht, wenn NVE (NetApp Volume Encryption) konfiguriert wird

10. Verwenden Sie die Abfrage des Security Key-Managers, um die Schlüssel-IDs der Authentifizierungsschlüssel anzuzeigen, die auf den Schlüsselverwaltungsservern gespeichert sind.
    - Wenn der `Restored` Spalte = `yes` Und alle Schlüsselmanager melden sich in einem verfügbaren Zustand, gehen Sie zu *Complete the Replacement Process*.
    - Wenn der `Restored` Spalte = nichts anderes als `yes`, Und/oder ein oder mehrere Schlüsselmanager sind nicht verfügbar, verwenden Sie die `security key-manager restore -address` Befehl zum Abrufen und Wiederherstellen aller mit allen Knoten verknüpften Authentifizierungsschlüssel (AKS) und Schlüssel-IDs von allen verfügbaren Key Management-Servern.

      Überprüfen Sie die Ausgabe der Sicherheitsschlüssel-Manager-Abfrage erneut, um sicherzustellen, dass der `Restored` Spalte = `yes` Und alle wichtigen Manager sind in einem verfügbaren Zustand unterstellt

11. Wenn das Onboard-Verschlüsselungsmanagement aktiviert ist:
    a. Verwenden Sie die `security key-manager key show -detail` Eine detaillierte Ansicht aller im Onboard Key Manager gespeicherten Schlüssel anzeigen.
    b. Verwenden Sie die `security key-manager key show -detail` Führen Sie den Befehl aus und überprüfen Sie das `Restored` Spalte = `yes` Für alle Authentifizierungsschlüssel.

       Wenn der `Restored` Spalte = nichts anderes als `yes`, Verwenden Sie die `security key-manager setup -node` *`Repaired`*`(Target)`*`node`* Befehl zum Wiederherstellen der Onboard Key Management-Einstellungen. Führen Sie den erneut aus `security key-manager key show -detail` Befehl zur Überprüfung `Restored` Spalte = `yes` Für alle Authentifizierungsschlüssel.

12. Schließen Sie das Konsolenkabel an den Partner Controller an.
13. Geben Sie den Controller mithilfe des zurück `storage failover giveback -fromnode local` Befehl.
14. Stellen Sie die automatische Rückgabe wieder her, wenn Sie die Funktion mithilfe von deaktivieren `storage failover modify -node local -auto-giveback true` Befehl.

Option 3: 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 einer offenen CIFS-Sitzung nicht erfolgreich ausgeführt wird, informieren Sie sich beim Kunden darüber, 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 synchronisieren.
   - 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.

  Überprüfen Sie mithilfe der Schlüsselabfrage für den Sicherheitsschlüssel-Manager, ob der `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 fehlgeschlagene Teil an NetApp - AFF A700s 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.