



Boot-Medien

Install and maintain

NetApp
March 24, 2023

Inhaltsverzeichnis

- Boot-Medien 1
 - Überblick über den Austausch von Boot-Medien – FAS2600 1
 - Integrierte Verschlüsselungsschlüssel - FAS2600 1
 - Schalten Sie den beeinträchtigten Controller aus - FAS2600 8
 - Ersetzen Sie das Boot-Medium FAS2600 9
 - Starten des Recovery-Images – FAS2600 13
 - Stellen Sie OKM, NSE und NVE nach Bedarf wieder her – FAS2600 15
 - Senden Sie das fehlerhafte Teil an NetApp - FAS2600 21

Boot-Medien

Überblick über den Austausch von Boot-Medien – FAS2600

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 *Impaired* ist der Knoten, auf dem Sie Wartungsarbeiten durchführen.
 - Der *Healthy Node* ist der HA-Partner des beeinträchtigten Knotens.

Integrierte Verschlüsselungsschlüssel - FAS2600

Bevor Sie den beeinträchtigten Controller herunterfahren und den Status der integrierten Verschlüsselungsschlüssel prüfen, müssen Sie den Status des beeinträchtigten Controllers überprüfen, die automatische Rückgabe deaktivieren und überprüfen, welche Version von ONTAP das System ausführt.

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 `admin`.

- Wenn der Controller mit eingeschränkter Einstellung an der LOADER-Eingabeaufforderung steht und Teil der HA-Konfiguration ist, melden Sie sich als `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 `<Ino-DARE>` oder `<1Ono-DARE>` in der Befehlsausgabe angezeigt wird, unterstützt das System NVE nicht. Fahren Sie mit dem Herunterfahren des Controllers fort.
 - Wenn `<Ino-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 `<Ino-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"](https://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"](https://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 `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"](https://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 `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"](https://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`



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"](https://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"](https://mysupport.netapp.com)

- a. Überprüfen Sie die `Restored In der Spalte` wird angezeigt `yes` Für alle Authentifizierungsschlüssel: `security key-manager key-query`
- b. Überprüfen Sie das `Key Manager Typ` zeigt an `onboard`, Und dann manuell sichern Sie die OKM-Informationen.
- c. Wechseln Sie zum erweiterten Berechtigungsebene-Modus, und geben Sie ein `y` Wenn Sie dazu aufgefordert werden, fortzufahren: `set -priv advanced`
- d. Geben Sie den Befehl ein, um die Backup-Informationen für das Verschlüsselungsmanagement anzuzeigen: `security key-manager onboard show-backup`
- e. Kopieren Sie den Inhalt der Backup-Informationen in eine separate Datei oder eine Protokolldatei. Sie werden es in Disaster-Szenarien benötigen, in denen Sie OKM manuell wiederherstellen müssen.
- f. Zurück zum Admin-Modus: `set -priv admin`
- g. Sie können den Controller sicher herunterfahren.

Schalten Sie den beeinträchtigten Controller aus - FAS2600

Nach Abschluss der NVE oder NSE-Aufgaben müssen Sie den Shutdown des beeinträchtigten Controllers durchführen.

Schritte

1. Nehmen Sie den beeinträchtigten Controller zur `LOADER`-Eingabeaufforderung:

Wenn der eingeschränkte Controller angezeigt wird...	Dann...
Die LOADER-Eingabeaufforderung	Wechseln Sie zu Controller-Modul entfernen.
Waiting for giveback...	Drücken Sie Strg-C, und antworten Sie dann <code>y</code> Wenn Sie dazu aufgefordert werden.
Eingabeaufforderung des Systems oder Passwort (Systempasswort eingeben)	Übernehmen oder stoppen Sie den beeinträchtigten Regler von der gesunden Steuerung: <code>storage failover takeover -ofnode impaired_node_name</code> Wenn der Regler „beeinträchtigt“ auf Zurückgeben wartet... anzeigt, drücken Sie Strg-C, und antworten Sie dann <code>y</code> .

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.

Ersetzen Sie das Boot-Medium FAS2600

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

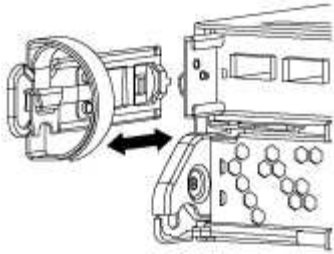
Schritt 1: Entfernen Sie das Controller-Modul

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

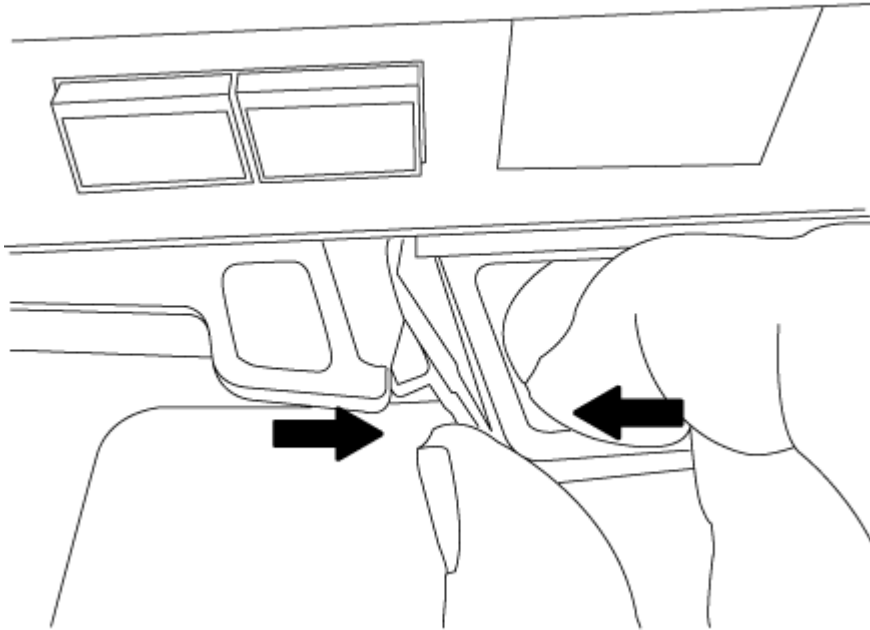
1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
2. Lösen Sie den Haken- und Schlaufenriemen, mit dem die Kabel am Kabelführungsgerät befestigt sind, und ziehen Sie dann die Systemkabel und SFPs (falls erforderlich) vom Controller-Modul ab, um zu verfolgen, wo die Kabel angeschlossen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

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

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



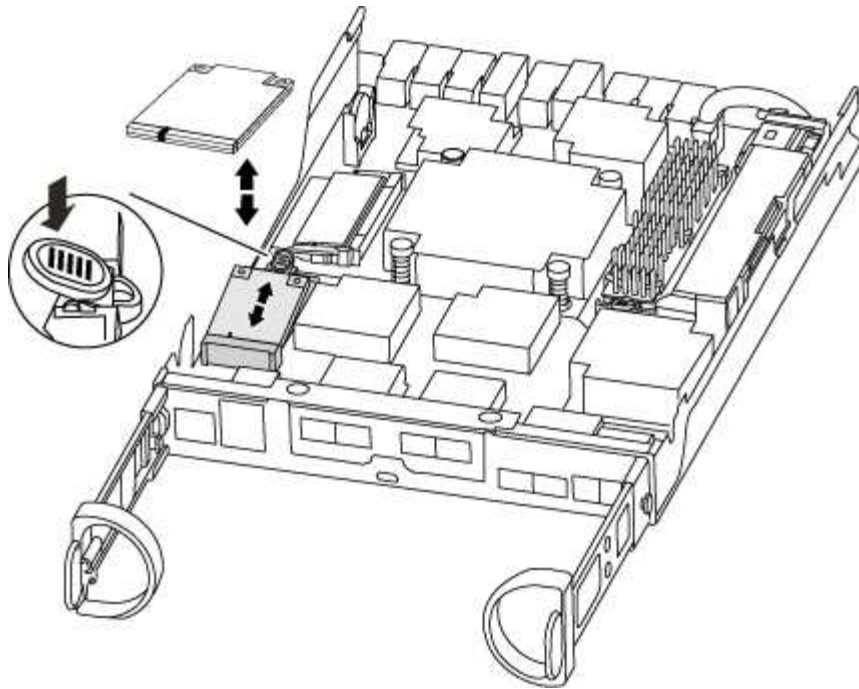
4. Drücken Sie die Verriegelung am Nockengriff, bis sie loslässt, öffnen Sie den Nockengriff vollständig, um das Controller-Modul aus der Mittelplatine zu lösen, und ziehen Sie das Controller-Modul anschließend mit zwei Händen aus dem Gehäuse heraus.



5. Drehen Sie das Controller-Modul um und legen Sie es auf eine flache, stabile Oberfläche.
6. Öffnen Sie die Abdeckung, indem Sie die blauen Laschen einschieben, um die Abdeckung zu lösen, und schwenken Sie dann die Abdeckung nach oben und öffnen Sie sie.

Schritt 2: Ersetzen Sie die Startmedien

1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
2. Suchen Sie das Boot-Medium mithilfe der folgenden Abbildung oder der FRU-Zuordnung auf dem Controller-Modul:



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



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

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

- Drücken Sie die Startmedien nach unten, um die Verriegelungstaste am Startmediengehäuse zu betätigen.
- Schließen Sie die Abdeckung des Controller-Moduls.

Schritt 3: Übertragen Sie das Startabbild auf das Startmedium

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

- 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. Richten Sie das Ende des Controller-Moduls an der Öffnung im Gehäuse aus, und drücken Sie dann vorsichtig das Controller-Modul zur Hälfte in das System.
2. 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.

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

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

4. Drücken Sie das Controller-Modul ganz in das System, vergewissern Sie sich, dass der Nockengriff das USB-Flash-Laufwerk löscht, drücken Sie den Nockengriff fest, um den Sitz des Controller-Moduls zu beenden, schieben Sie den Nockengriff in die geschlossene Position und ziehen Sie die Daumenschraube fest.

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

5. Unterbrechen Sie den Boot-Vorgang, um an der LOADER-Eingabeaufforderung zu stoppen, indem Sie Strg-C drücken, wenn Sie sehen Starten VON AUTOBOOT drücken Sie Strg-C, um den Vorgang abubrechen

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.

6. Wenn Systeme mit einem Controller im Chassis vorhanden sind, schließen Sie das Netzteil wieder an und schalten Sie die Netzteile ein.

Das System beginnt mit dem Booten und wird bei DER LOADER-Eingabeaufforderung angehalten.

7. Legen Sie den Verbindungstyp für das Netzwerk an der LOADER-Eingabeaufforderung fest:

- Wenn Sie DHCP konfigurieren: `ifconfig e0a -auto`



Der von Ihnen konfigurierte Zielport ist der Zielport, über den Sie während der Wiederherstellung des var-Dateisystems mit dem beeinträchtigten Controller über den gesunden Controller kommunizieren. Sie können in diesem Befehl auch den Port E0M verwenden.

- Wenn Sie manuelle Verbindungen konfigurieren: `ifconfig e0a -addr=filer_addr -mask=netmask -gw=gateway-dns=dns_addr-domain=dns_domain`

- Filer_addr ist die IP-Adresse des Speichersystems.
- Netmask ist die Netzwerkmaske des Managementnetzwerks, das mit dem HA-Partner verbunden ist.
- Das Gateway ist das Gateway für das Netzwerk.
- dns_addr ist die IP-Adresse eines Namensservers in Ihrem Netzwerk.

- die `dns_Domain` ist der Domain Name des Domain Name System (DNS).

Wenn Sie diesen optionalen Parameter verwenden, benötigen Sie keinen vollqualifizierten Domännennamen in der Netzboot-Server-URL. Sie benötigen nur den Hostnamen des Servers.



Andere Parameter können für Ihre Schnittstelle erforderlich sein. Sie können eingeben `help ifconfig` Details finden Sie in der Firmware-Eingabeaufforderung.

Starten des Recovery-Images – FAS2600

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

Schritte

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

Das Bild wird vom USB-Flash-Laufwerk heruntergeladen.

2. Wenn Sie dazu aufgefordert werden, geben Sie entweder den Namen des Bilds ein oder akzeptieren Sie das Standardbild, das in den Klammern auf dem Bildschirm angezeigt wird.
3. Stellen Sie das var-Dateisystem wieder her:

Wenn Ihr System...	Dann...
Eine Netzwerkverbindung	<ol style="list-style-type: none"> a. Drücken Sie <code>y</code> Wenn Sie aufgefordert werden, die Backup-Konfiguration wiederherzustellen. b. Stellen Sie den gesunden Controller auf die erweiterte Berechtigungsebene ein: <code>set -privilege advanced</code> c. Führen Sie den Befehl Restore Backup aus: <code>system node restore-backup -node local -target-address <i>impaired_node_IP_address</i></code> d. Zurückkehren des Controllers zur Administratorebene: <code>set -privilege admin</code> e. Drücken Sie <code>y</code> Wenn Sie aufgefordert werden, die wiederhergestellte Konfiguration zu verwenden. f. Drücken Sie <code>y</code> Wenn Sie dazu aufgefordert werden, den Controller neu zu booten.

Wenn Ihr System...	Dann...
Keine Netzwerkverbindung	<p>a. Drücken Sie <code>n</code>. Wenn Sie aufgefordert werden, die Backup-Konfiguration wiederherzustellen.</p> <p>b. Starten Sie das System neu, wenn Sie dazu aufgefordert werden.</p> <p>c. Wählen Sie im angezeigten Menü die Option Flash aktualisieren aus Backup config (Flash synchronisieren) aus.</p> <p>Wenn Sie aufgefordert werden, mit der Aktualisierung fortzufahren, drücken Sie <code>y</code>.</p>

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

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

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 – FAS2600

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: <code>boot_ontap menu</code>
Warten auf Giveback...	<ol style="list-style-type: none"> a. Eingabe <code>Ctrl-C</code> An der Eingabeaufforderung b. Bei der Nachricht: Möchten Sie den Controller anhalten, anstatt [y/n] zu warten? , Geben Sie ein: <code>y</code> c. Geben Sie an der LOADER-Eingabeaufforderung den ein <code>boot_ontap menu</code> 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-----  
TmV0QXBwIETERTABCbGaiAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA . .  
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
----- 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:
- Starten Sie den Assistenten mit `security key-manager setup -nodenodename` Geben Sie dann bei der entsprechenden Aufforderung die Passphrase für das Onboard-Verschlüsselungsmanagement ein.
 - 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.

- Warten Sie 10 Minuten, bis der Schlüssel über das Cluster synchronisiert wird.

14. Wenn Sie ONTAP 9.6 oder höher verwenden:

- Führen Sie die aus `security key-manager onboard sync` Geben Sie bei der entsprechenden Aufforderung die Passphrase ein.
- 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.

- 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

- Schließen Sie das Konsolenkabel an den Ziel-Controller an.
- 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 <code>storage failover show</code> 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:

- Verwenden Sie die `security key-manager key show -detail` Eine detaillierte Ansicht aller im Onboard Key Manager gespeicherten Schlüssel anzeigen.
- 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

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

Wenn die Konsole angezeigt wird...	Dann...
Die Eingabeaufforderung für die Anmeldung	Fahren Sie mit Schritt 7 fort.
Warten auf Giveback...	<ol style="list-style-type: none"> Melden Sie sich beim Partner-Controller an. Überprüfen Sie, ob der Ziel-Controller bereit ist für die Rückgabe an den <code>storage failover show</code> 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 fehlerhafte Teil an NetApp - FAS2600

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

Copyright-Informationen

Copyright © 2023 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

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

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

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

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

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

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

Markeninformationen

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