



Boot-Medien

Install and maintain

NetApp
March 24, 2023

Inhaltsverzeichnis

- Boot-Medien 1
 - Ersetzen Sie den Startdatenträger - AFF A900 1
 - Prüfungen vor dem Herunterfahren für integrierte Verschlüsselungsschlüssel - AFF A900 1
 - Schalten Sie den beeinträchtigten Regler AFF A900 aus 5
 - Entfernen Sie den Controller, ersetzen Sie den Startdatenträger, und übertragen Sie das Startabbild – AFF A900 8
 - Starten Sie das Recovery-Image - AFF A900 13
 - Schritte zum Austausch von Medien nach dem Booten für OKM, NSE und NVE – AFF A900 16
 - Das fehlgeschlagene Teil an NetApp - AFF A900 zurückgeben 20

Boot-Medien

Ersetzen Sie den Startdatenträger - AFF A900

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

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

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

- Bei den unterbrechungsfreien und unterbrechungsfreien Methoden zum Austausch von Boot-Medien müssen Sie den wiederherstellen `var` Filesystem:
 - Beim unterbrechungsfreien Austausch benötigt das HA-Paar keine Verbindung zu einem Netzwerk, um den wiederherzustellen `var` File-System. Das HA-Paar in einem einzelnen Chassis hat eine interne EOS-Verbindung, die zum Transfer verwendet wird `var` Konfigurieren zwischen ihnen.
 - Für den störenden Austausch benötigen Sie keine Netzwerkverbindung, um den wiederherzustellen `var` Dateisystem, aber der Prozess erfordert zwei Neustarts.
- Sie müssen die fehlerhafte Komponente durch eine vom Anbieter empfangene Ersatz-FRU-Komponente ersetzen.
- Es ist wichtig, dass Sie die Befehle in diesen Schritten auf dem richtigen Controller anwenden:
 - Der Controller *Impared* ist der Controller, an dem Sie Wartungsarbeiten durchführen.
 - Der *Healthy* Controller ist der HA-Partner des beeinträchtigten Controllers.

Prüfungen vor dem Herunterfahren für integrierte Verschlüsselungsschlüssel - AFF A900

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.

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 irgendeine 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 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)

- 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 Regler AFF A900 aus

Fahren Sie den Controller mit eingeschränkter Konfiguration herunter oder übernehmen Sie ihn entsprechend.

In den meisten Konfigurationen

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

Um den beeinträchtigten Controller herunterzufahren, müssen Sie den Status des Controllers bestimmen und gegebenenfalls den Controller übernehmen, damit der gesunde Controller weiterhin Daten aus dem beeinträchtigten Reglerspeicher bereitstellen kann.

Über diese Aufgabe

- Wenn Sie NetApp Storage Encryption verwenden, müssen Sie die MSID mithilfe der Anweisungen im zurückgesetzt haben ["SEDs werden in den ungeschützten Modus versetzt"](#).
- Wenn Sie über ein SAN-System verfügen, müssen Sie Ereignismeldungen geprüft haben `cluster kernel-service show` Für beeinträchtigte Controller SCSI-Blade. Der `cluster kernel-service show` Der Befehl zeigt den Node-Namen, den Quorum-Status dieses Node, den Verfügbarkeitsstatus dieses Node und den Betriebsstatus dieses Node an.

Jeder Prozess des SCSI-Blades sollte sich im Quorum mit den anderen Nodes im Cluster befinden. Probleme müssen behoben werden, bevor Sie mit dem Austausch fortfahren.

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

Schritte

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

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

2. Deaktivieren Sie das automatische Giveback von der Konsole des gesunden Controllers: `storage failover modify -node local -auto-giveback false`



Wenn Sie sehen *Möchten Sie Auto-Giveback deaktivieren?*, geben Sie ein `y`.

3. Nehmen Sie den beeinträchtigten Controller zur LOADER-Eingabeaufforderung:

Wenn der eingeschränkte Controller angezeigt wird...	Dann...
Die LOADER-Eingabeaufforderung	Wechseln Sie zu Controller-Modul entfernen.
Warten auf Giveback...	Drücken Sie Strg-C, und antworten Sie dann <code>y</code> Wenn Sie dazu aufgefordert werden.

Wenn der eingeschränkte Controller angezeigt wird...	Dann...
Eingabeaufforderung für das System oder Passwort	Übernehmen oder stoppen Sie den beeinträchtigten Regler von der gesunden Steuerung: <code>storage failover takeover -ofnode <i>impaired_node_name</i></code> Wenn der Regler „beeinträchtigt“ auf Zurückgeben wartet... zeigt, drücken Sie Strg-C, und antworten Sie dann <code>y</code> .

Controller befindet sich in einem MetroCluster

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



Verwenden Sie dieses Verfahren nicht, wenn sich Ihr System in einer MetroCluster-Konfiguration mit zwei Knoten befindet.

Um den beeinträchtigten Controller herunterzufahren, müssen Sie den Status des Controllers bestimmen und gegebenenfalls den Controller übernehmen, damit der gesunde Controller weiterhin Daten aus dem beeinträchtigten Reglerspeicher bereitstellen kann.

- Wenn Sie über ein Cluster mit mehr als zwei Nodes verfügen, muss es sich im Quorum befinden. Wenn sich das Cluster nicht im Quorum befindet oder ein gesunder Controller FALSE anzeigt, um die Berechtigung und den Zustand zu erhalten, müssen Sie das Problem korrigieren, bevor Sie den beeinträchtigten Controller herunterfahren; siehe "[Synchronisieren eines Node mit dem Cluster](#)".
- Wenn Sie über eine MetroCluster-Konfiguration verfügen, müssen Sie bestätigt haben, dass der MetroCluster-Konfigurationsstatus konfiguriert ist und dass die Nodes in einem aktivierten und normalen Zustand vorliegen (`metrocluster node show`).

Schritte

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

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

2. Deaktivieren Sie das automatische Giveback von der Konsole des gesunden Controllers: `storage failover modify -node local -auto-giveback false`
3. Nehmen Sie den beeinträchtigten Controller zur LOADER-Eingabeaufforderung:

Wenn der eingeschränkte Controller angezeigt wird...	Dann...
Die LOADER-Eingabeaufforderung	Wechseln Sie zu Controller-Modul entfernen.

Wenn der eingeschränkte Controller angezeigt wird...	Dann...
Warten auf 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 <i>impaired_node_name</i></code> Wenn der Regler „beeinträchtigt“ auf Zurückgeben wartet... anzeigt, drücken Sie Strg-C, und antworten Sie dann <code>y</code> .

Entfernen Sie den Controller, ersetzen Sie den Startdatenträger, und übertragen Sie das Startabbild – AFF A900

Sie müssen das Controller-Modul entfernen und öffnen, die Startmedien im Controller suchen und austauschen und dann das Image auf das Ersatzstartmedium übertragen.

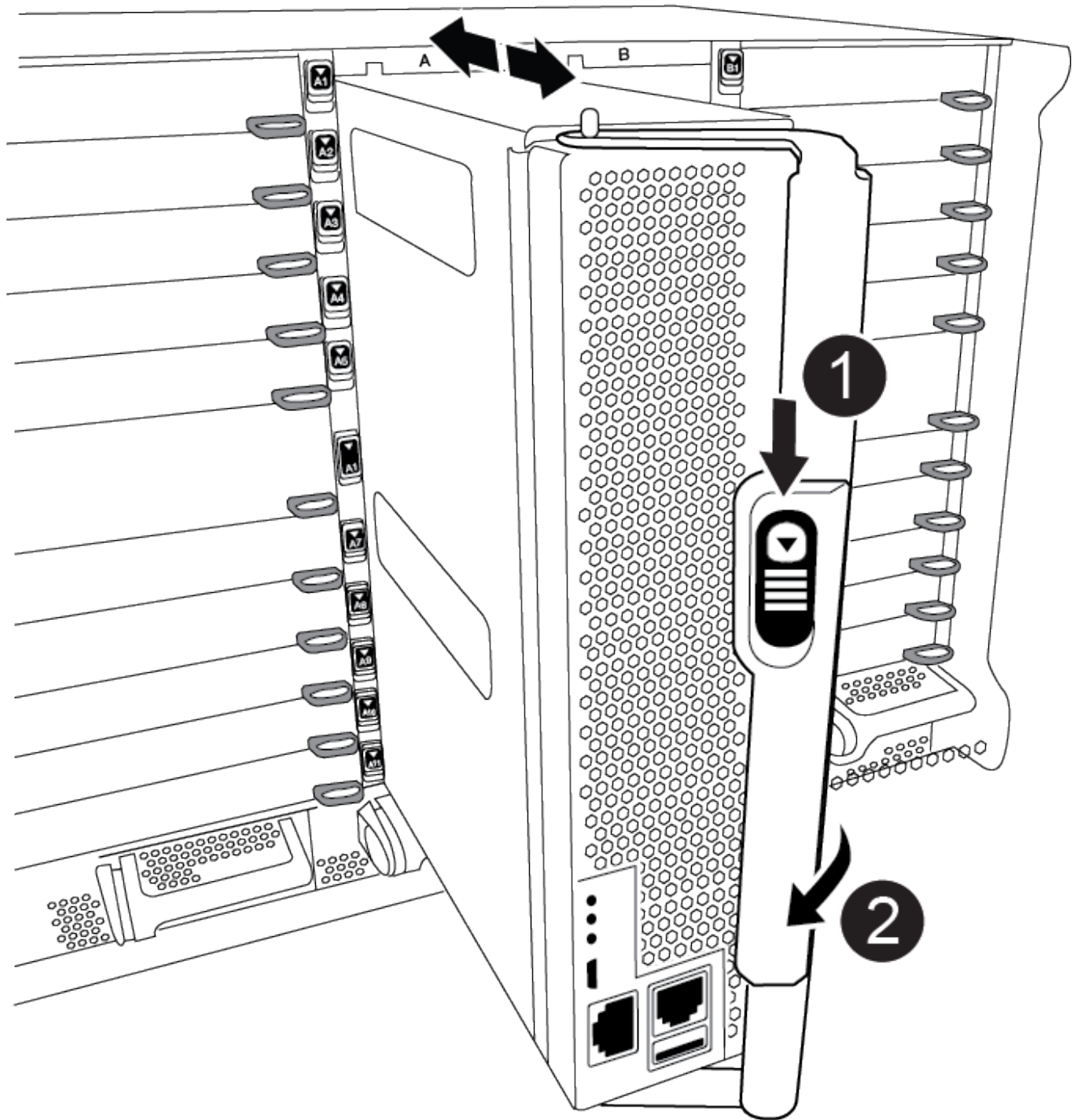
Schritt 1: Entfernen Sie das Controller-Modul

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.

Schritte

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

[Animation - Entfernen Sie den Controller](#)



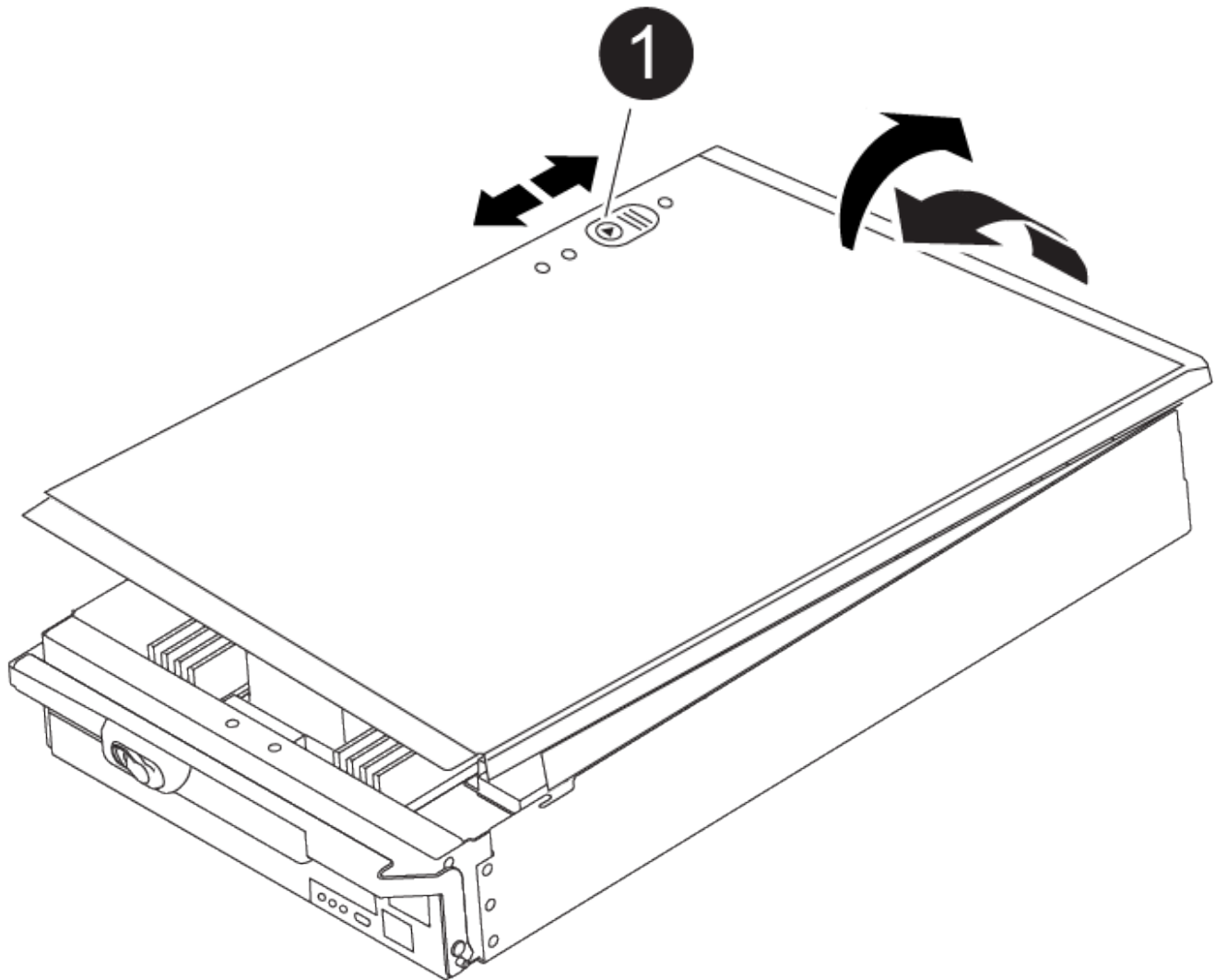
1	Freigabetaste für den CAM-Griff
2	CAM-Griff

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

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

Gehäuse schieben.

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



1

Verriegelungstaste für die Controllermodulabdeckung

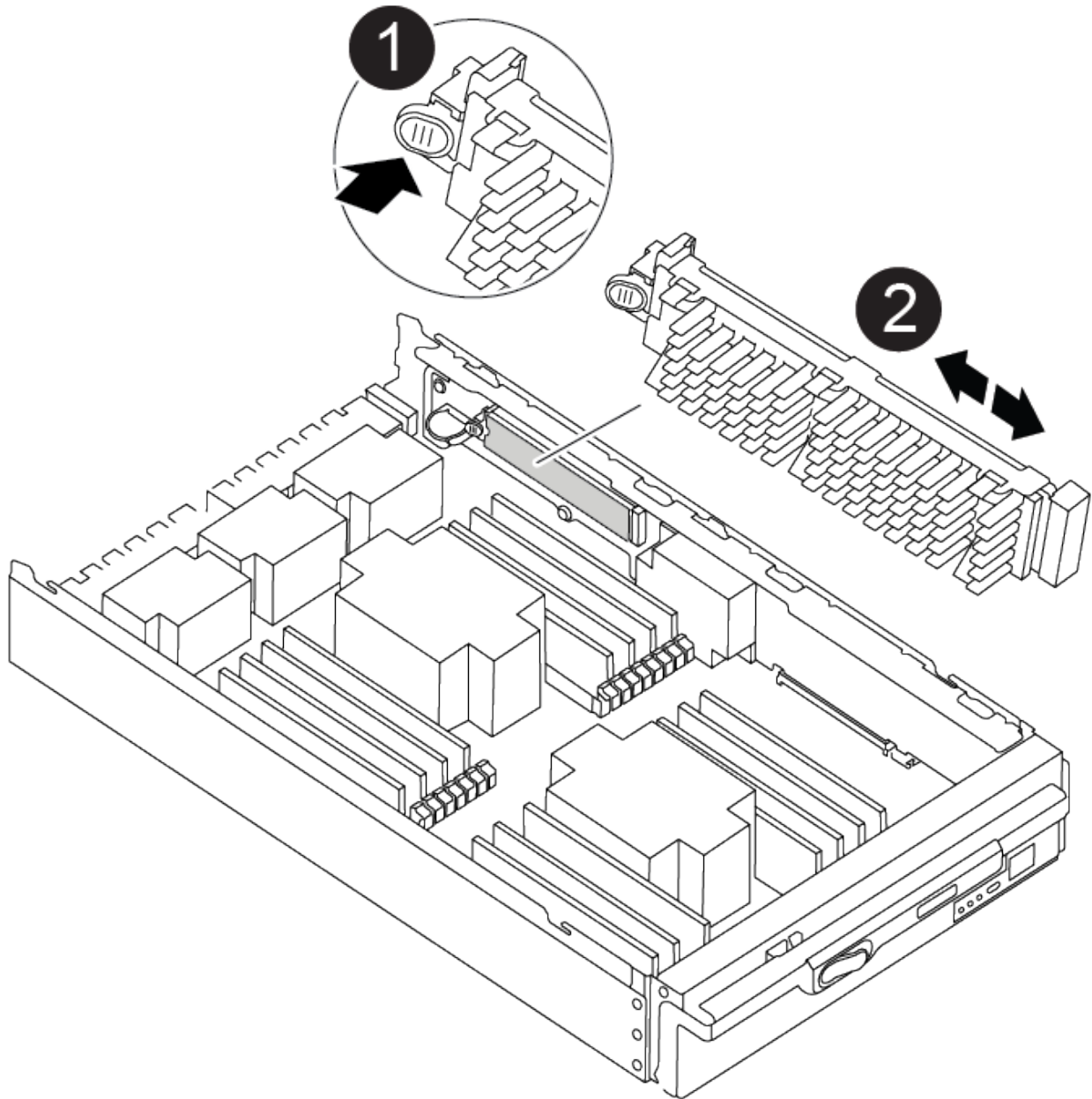
Schritt 2: Ersetzen Sie die Startmedien

Sie müssen das Startmedium im Controller finden und die Anweisungen befolgen, um es zu ersetzen.

Schritte

1. Heben Sie den schwarzen Luftkanal auf der Rückseite des Controller-Moduls an, und suchen Sie dann mithilfe der folgenden Abbildung oder der FRU-Karte am Controller-Modul die Bootmedien:

[Animation - Bootmedium ersetzen](#)



1	Drücken Sie die Freigabelasche
2	Boot-Medien

2. 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.

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

4. 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.

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

Schritt 3: Übertragen Sie das Startabbild auf das Startmedium

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

Bevor Sie beginnen

- Sie müssen über ein USB-Flash-Laufwerk verfügen, das auf FAT32 formatiert ist und eine Kapazität von mindestens 4 GB aufweist.
- Eine Kopie der gleichen Bildversion von ONTAP wie der beeinträchtigte Controller. Das entsprechende Image können Sie im Abschnitt „Downloads“ auf der NetApp Support-Website herunterladen
 - Wenn NVE aktiviert ist, laden Sie das Image mit NetApp Volume Encryption herunter, wie in der Download-Schaltfläche angegeben.
 - Wenn NVE nicht aktiviert ist, laden Sie das Image ohne NetApp Volume Encryption herunter, wie im Download-Button dargestellt.
- Wenn es sich bei Ihrem System um ein eigenständiges System handelt, benötigen Sie keine Netzwerkverbindung, 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. Das Controller-Modul nach Bedarf wieder einschalten.
3. Stecken Sie das USB-Flash-Laufwerk in den USB-Steckplatz des Controller-Moduls.

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

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

Der 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 abzubrechen

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

6. Legen Sie den Verbindungstyp für das Netzwerk an der LOADER-Eingabeaufforderung fest:
 - Wenn Sie DHCP konfigurieren: `ifconfig e0a -auto`



Der von Ihnen konfigurierte Zielport ist der Zielport, über den Sie 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 Domänennamen in der Netzboot-Server-URL. Sie benötigen nur den Hostnamen des Servers.



Andere Parameter können für Ihre Schnittstelle erforderlich sein. Sie können Hilfe `ifconfig` an der Firmware-Eingabeaufforderung für Details eingeben.

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

- a. Start in Wartungsmodus: `boot_ontap maint`
- b. Legen Sie die MetroCluster-Ports als Initiatoren fest: `ucadmin modify -m fc -t initiator adapter_name`
- c. Anhalten, um zum Wartungsmodus zurückzukehren: `halt`

Die Änderungen werden implementiert, wenn das System gestartet wird.

Starten Sie das Recovery-Image - AFF A900

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	<ul style="list-style-type: none"> a. Drücken Sie <code>y</code> Wenn Sie aufgefordert werden, die Backup-Konfiguration wiederherzustellen. b. Drücken Sie <code>y</code> Bei Aufforderung zum Überschreiben <code>/etc/ssh/ssh_host_ecdsa_key</code>. c. Drücken Sie <code>y</code> Wenn Sie aufgefordert werden, zu bestätigen, ob die Wiederherstellung erfolgreich war. d. Drücken Sie <code>Y</code> Wenn Sie zur wiederhergestellten Konfigurationskopie aufgefordert werden. e. Stellen Sie den beeinträchtigten Controller auf die erweiterte Berechtigungsebene ein: <code>set -privilege advanced</code> f. Führen Sie den Befehl <code>Restore Backup</code> aus: <code>system node restore-backup -node local -target-address impaired_node_IP_address</code> g. Geben Sie den beeinträchtigten Controller auf Administratorebene zurück: <code>set -privilege admin</code> h. Drücken Sie <code>y</code> Wenn Sie aufgefordert werden, die wiederhergestellte Konfiguration zu verwenden. i. Drücken Sie <code>y</code> Wenn Sie dazu aufgefordert werden, den beeinträchtigten Controller neu zu starten.
Keine Netzwerkverbindung	<ul style="list-style-type: none"> a. Drücken Sie <code>n</code> 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. <p>Wenn Sie aufgefordert werden, mit der Aktualisierung fortzufahren, drücken Sie <code>y</code>.</p>

Wenn Ihr System...	Dann...
Keine Netzwerkverbindung und befindet sich in einer MetroCluster IP-Konfiguration	<p>a. Drücken Sie n Wenn Sie aufgefordert werden, die Backup-Konfiguration wiederherzustellen.</p> <p>b. Starten Sie das System neu, wenn Sie dazu aufgefordert werden.</p> <p>c. Warten Sie, bis die iSCSI-Speicherverbindungen verbunden sind.</p> <p>Sie können fortfahren, nachdem Sie die folgenden Meldungen angezeigt haben:</p> <div data-bbox="672 464 1484 1325" style="border: 1px solid gray; padding: 10px; margin: 10px 0;"> <pre> date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address). date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address). date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_auxiliary, address: ip-address). date-and-time [node- name:iscsi.session.stateChanged:notice]: iSCSI session state is changed to Connected for the target iSCSI-target (type: dr_partner, address: ip-address). </pre> </div> <p>d. 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 y.</p>

4. Stellen Sie sicher, dass die Umgebungsvariablen wie erwartet festgelegt sind:
 - a. Nehmen Sie den beeinträchtigten Controller zur LOADER-Eingabeaufforderung.
 - b. Überprüfen Sie die Einstellungen der Umgebungsvariablen mit dem Befehl `printenv`.
 - c. Wenn eine Umgebungsvariable nicht wie erwartet festgelegt ist, ändern Sie sie mit dem Befehl `setenvumwelt_variable_Name changed_value`.
 - d. Speichern Sie Ihre Änderungen mit dem Befehl `saveenv`.
5. Das nächste hängt von Ihrer Systemkonfiguration ab:

- Wenn keymanager, NSE oder NVE in Ihrem System integriert sind, finden Sie unter [Schritte zum Austausch von Medien nach dem Booten für OKM, NSE und NVE](#)
- Wenn keymanager, NSE oder NVE auf Ihrem System nicht konfiguriert sind, führen Sie die Schritte in diesem Abschnitt aus.

6. Geben Sie an der LOADER-Eingabeaufforderung den Befehl `Boot_ontap` ein.

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

- Schließen Sie das Konsolenkabel an den Partner Controller an.
- Geben Sie den Controller mit dem lokalen Befehl `Storage Failover Giveback -abnode` zurück.
- Überprüfen Sie an der Cluster-Eingabeaufforderung die logischen Schnittstellen mit dem falsch-Befehl `net int -is-Home`.

Wenn Schnittstellen als „false“ aufgeführt sind, setzen Sie diese Schnittstellen mit dem `net int revert` Befehl zurück auf ihren Home Port zurück.

- Bewegen Sie das Konsolenkabel in den reparierten Herunterfahren oder übernehmen Sie den beeinträchtigten Controller mit dem entsprechenden Verfahren für Ihre Konfiguration. Und führen Sie den Befehl `Version -V` aus, um die ONTAP-Versionen zu überprüfen.
- Stellen Sie das automatische Giveback wieder her, wenn Sie es mithilfe des `Storage Failover modify -Node local -Auto-Giveback true` Befehls deaktiviert haben.

Schritte zum Austausch von Medien nach dem Booten für OKM, NSE und NVE – AFF A900

Sobald Umgebungsvariablen aktiviert sind, müssen Sie bestimmte Schritte zur Wiederherstellung von Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) und NetApp Volume Encryption (NVE) ausführen.

- Bestimmen Sie den Abschnitt, den Sie zum Wiederherstellen Ihrer OKM-, NSE- oder NVE-Konfigurationen verwenden sollten: Wenn NSE oder NVE zusammen mit Onboard Key Manager aktiviert sind, müssen Sie die zu Beginn dieses Verfahrens erfassten Einstellungen wiederherstellen.
 - Wenn NSE oder NVE aktiviert sind und der Onboard Key Manager aktiviert ist, wechseln Sie zu [wenn Onboard Key Manager aktiviert ist](#).
 - Wenn NSE oder NVE für ONTAP 9.6 aktiviert sind, finden Sie unter [Stellen Sie NSE/NVE auf Systemen mit ONTAP 9.6 und höher wieder her](#).

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

- Schließen Sie das Konsolenkabel an den Ziel-Controller an.

2. Verwenden Sie den `boot_ontap`-Befehl an der LOADER-Eingabeaufforderung, um den Controller zu booten.
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 Zurückgeben	<ol style="list-style-type: none"> a. Eingabe <code>Ctrl-C</code> An der Eingabeaufforderung b. Bei der Meldung: Möchten Sie diesen Knoten 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 Backup-Daten aufgefordert werden, fügen Sie die zu Beginn dieses Abschnitts erfassten Backup-Daten bei der Aufforderung ein. 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-Daten eingeben:

```

----- BACKUP-----
TmV0QXBwIETERTABCbGaiAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA . .
H4nPQM0nrDRYRa9SCv8AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
----- END-BACKUP-----

```

7. Wählen Sie im Startmenü die Option Normal Boot aus.
Das System startet zum Warten auf Giveback... Eingabeaufforderung.
8. Verschieben Sie das Konsolenkabel zum Partner Controller 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 zurück `storage failover giveback -fromnode local -only-cfo-aggregates true` Befehl.
 - Wenn der Befehl aufgrund eines ausgefallenen Laufwerks ausfällt, setzen Sie die ausgefallene Festplatte physisch aus, lassen Sie sie aber in den Steckplatz, bis ein Austausch erfolgt.
 - Wenn der Befehl aufgrund einer offenen CIFS-Sitzung nicht erfolgreich ausgeführt wird, informieren Sie sich beim 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 NVRAMs synchronisiert wurden.
 - Wenn der Befehl aufgrund eines NDMP-, SnapMirror- oder SnapVault-Prozesses ausfällt, deaktivieren Sie den Prozess. Weitere Informationen finden Sie in den entsprechenden Inhalten.
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. Wenn Sie ONTAP 9.6 oder höher verwenden, führen Sie die integrierte Synchronisierung des Security Key-Managers aus:
 - 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 `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.
13. Stellen Sie das Konsolenkabel auf den Partner Controller um.
14. Geben Sie den Ziel-Controller mithilfe des zurück `storage failover giveback -fromnode local` Befehl.
15. Überprüfen Sie den Giveback-Status, drei Minuten nachdem Berichte abgeschlossen wurden, mithilfe des `storage failover show` Befehl.

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

16. Geben Sie an der Eingabeaufforderung für `clustershell` den Befehl `net int show -is-Home false` ein, um die logischen Schnittstellen aufzulisten, die sich nicht auf ihrem Home-Controller und Port befinden.

Wenn Schnittstellen als aufgeführt werden `false`, Zurücksetzen dieser Schnittstellen zurück auf ihren Home-Port mit dem `net int revert` Befehl.

17. Bewegen Sie das Konsolenkabel auf den Ziel-Controller, und führen Sie den aus `version -v` Befehl zum Prüfen der ONTAP-Versionen.

18. Stellen Sie die automatische Rückgabe wieder her, wenn Sie die Funktion mithilfe von deaktivieren `storage failover modify -node local -auto-giveback true` Befehl.

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

- Schließen Sie das Konsolenkabel an den Ziel-Controller an.
- Verwenden Sie den `Boot_ontap`-Befehl an der LOADER-Eingabeaufforderung, um den Controller zu booten.
- 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.

- Bewegen Sie das Konsolenkabel auf den Partner Controller und geben Sie den Ziel-Controller-Storage mit dem Storage Failover Giveback `-vNode local -only-cfo-Aggregates` echten lokalen Befehl zurück.
 - 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 synchronisieren.
 - Wenn der Befehl aufgrund eines NDMP-, SnapMirror- oder SnapVault-Prozesses ausfällt, deaktivieren Sie den Prozess. Weitere Informationen finden Sie in den entsprechenden Inhalten.
- Warten Sie 3 Minuten, und überprüfen Sie den Failover-Status mit dem Befehl „Storage Failover show“.
 - 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.

- Bewegen Sie das Konsolenkabel auf den Ziel-Controller, und führen Sie den aus `version -v` Befehl zum Prüfen der ONTAP-Versionen.
- Stellen Sie die automatische Rückgabe wieder her, wenn Sie die Funktion mithilfe von deaktivieren `storage failover modify -node local -auto-giveback true` Befehl.
- 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 Verschlüsselung und Authentifizierungsschlüssel, die auf den Verschlüsselungsmanagement-Servern 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 den Befehl `Security Key-Manager External Restore`, um die Schlüssel-IDs der Authentifizierungsschlüssel wiederherzustellen.



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 den `Onboard Sync`-Befehl des `Security Key-Managers`, um den `Key Manager`-Typ neu zu synchronisieren.

Verwenden Sie die `security key-manager key-query` Befehl zum Überprüfen des `Restored` Spalte = `yes/true` Für alle Authentifizierungsschlüssel.

11. Schließen Sie das Konsolenkabel an den Partner Controller an.
12. Geben Sie den Controller mit dem lokalen Befehl `Storage Failover Giveback -abnode` zurück.
13. Stellen Sie die automatische Rückgabe wieder her, wenn Sie die Funktion mithilfe von `deaktivieren storage failover modify -node local -auto-giveback true` Befehl.

Das fehlgeschlagene Teil an NetApp - AFF A900 zurückgeben

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.