



Boot-Medien

Install and maintain

NetApp
December 18, 2024

Inhalt

- Boot-Medien 1
 - Workflow zum Austausch von Boot-Medien – AFF C30 und AFF C60 1
 - Anforderungen und Überlegungen - AFF C30 und AFF C60 1
 - Prüfen Sie die integrierten Verschlüsselungsschlüssel – AFF C30 und AFF C60 2
 - Schalten Sie den Controller für beeinträchtigten Betrieb aus - AFF C30 und AFF C60 7
 - Ersetzen Sie das Startmedium – AFF C30 und AFF C60 8
 - Starten Sie das Wiederherstellungs-Image - AFF C30 und AFF C60 14
 - Wiederherstellung der Verschlüsselung – AFF C30 und AFF C60 17
 - Senden Sie das fehlerhafte Teil an NetApp - AFF C30 und AFF C60 zurück 27

Boot-Medien

Workflow zum Austausch von Boot-Medien – AFF C30 und AFF C60

Führen Sie die folgenden Workflow-Schritte aus, um die Startmedien zu ersetzen.

1

"Überprüfen Sie die Anforderungen der Startmedien"

Um das Boot-Medium zu ersetzen, müssen Sie bestimmte Anforderungen erfüllen.

2

"Integrierte Verschlüsselungsschlüssel überprüfen"

Überprüfen Sie, ob der Sicherheitsschlüsselmanager auf Ihrem Speichersystem aktiviert ist oder ob die Laufwerke verschlüsselt sind.

3

"Schalten Sie den beeinträchtigten Regler aus"

Fahren Sie den beeinträchtigten Controller herunter oder übernehmen Sie ihn, damit der funktionsunzuverlässige Controller weiterhin Daten aus dem Speicher für den beeinträchtigten Controller bereitstellen kann.

4

"Ersetzen Sie das Startmedium"

Entfernen Sie das fehlerhafte Startmedium vom gestörten Controller, installieren Sie das Ersatz-Startmedium, und übertragen Sie dann ein ONTAP-Image mithilfe eines USB-Flashlaufwerks auf das Ersatz-Startmedium.

5

"Starten Sie das Recovery-Image"

Starten Sie das ONTAP-Image vom USB-Laufwerk, stellen Sie das Dateisystem wieder her und überprüfen Sie die Umgebungsvariablen.

6

"Wiederherstellung der Verschlüsselung"

Wiederherstellung der Onboard-Schlüsselmanager-Konfiguration oder des externen Schlüsselmanagers aus dem ONATP-Startmenü.

7

"Senden Sie das fehlerhafte Teil an NetApp zurück"

Senden Sie das fehlerhafte Teil wie in den dem Kit beiliegenden RMA-Anweisungen beschrieben an NetApp zurück.

Anforderungen und Überlegungen - AFF C30 und AFF C60

Bevor Sie die Startmedien austauschen, müssen Sie die folgenden Anforderungen und

Überlegungen beachten.

Anforderungen

- 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`.
- Sie müssen die Datei zur späteren Verwendung in diesem Verfahren auf das USB-Flash-Laufwerk kopieren `image_xxx.tgz`.
- Sie müssen die fehlerhafte Komponente durch eine FRU-Ersatz-Komponente mit derselben Kapazität ersetzen, die Sie von Ihrem Anbieter erhalten haben.

Überlegungen

- 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.
- Bei Bedarf können Sie die (blauen) LEDs für die Position des Plattformgehäuses einschalten, um die physische Lokalisierung der betroffenen Plattform zu erleichtern. Melden Sie sich über SSH bei der BMC an und geben Sie den Befehl ein `system location-led on`.

Ein Plattformgehäuse verfügt über drei Standort-LEDs: Eine auf dem Bedienfeld und eine auf jedem Controller. Die Standort-LEDs leuchten 30 Minuten lang.

Sie können sie deaktivieren, indem Sie den Befehl eingeben `system location-led off`. Wenn Sie sich nicht sicher sind, ob die LEDs leuchten oder nicht, können Sie ihren Status überprüfen, indem Sie den Befehl eingeben `system location-led show`.

Prüfen Sie die integrierten Verschlüsselungsschlüssel – AFF C30 und AFF C60

Überprüfen Sie vor dem Herunterfahren des beeinträchtigten Controllers, ob Ihre Version von ONTAP NetApp Volume Encryption (NVE) unterstützt und ob Ihr Verschlüsselungsmanagement-System ordnungsgemäß konfiguriert ist.

Schritt: Prüfen Sie, ob Ihre Version von ONTAP NetApp-Volume-Verschlüsselung unterstützt

Prüfen Sie, ob Ihre ONTAP Version NetApp Volume Encryption (NVE) unterstützt. Diese Informationen sind entscheidend, um das richtige ONTAP-Image herunterzuladen.

1. Stellen Sie fest, ob Ihre ONTAP-Version Verschlüsselung unterstützt, indem Sie den folgenden Befehl ausführen:

```
version -v
```

Wenn die Ausgabe enthält `1Ono-DARE`, wird NVE auf Ihrer Cluster-Version nicht unterstützt.

2. Je nachdem, ob NVE auf Ihrem System unterstützt wird, führen Sie eine der folgenden Aktionen durch:

- Falls NVE unterstützt wird, laden Sie das ONTAP Image mit NetApp Volume Encryption herunter.
- Falls NVE nicht unterstützt wird, laden Sie das ONTAP Image **ohne** NetApp-Volume-Verschlüsselung herunter.

Schritt 2: Stellen Sie fest, ob es sicher ist, den Controller herunterzufahren

Um einen Controller sicher herunterzufahren, müssen Sie zuerst ermitteln, ob der External Key Manager (EKM) oder der Onboard Key Manager (OKM) aktiv ist. Überprüfen Sie anschließend den verwendeten Schlüsselmanager, zeigen Sie die entsprechenden Schlüsselinformationen an und ergreifen Sie Maßnahmen, die auf dem Status der Authentifizierungsschlüssel basieren.

1. Bestimmen Sie, welcher Schlüsselmanager auf Ihrem System aktiviert ist:

ONTAP-Version	Führen Sie diesen Befehl aus
ONTAP 9.14.1 oder höher	<pre>security key-manager keystore show</pre> <ul style="list-style-type: none"> • Wenn EKM aktiviert ist, <code>EKM</code> wird in der Befehlsausgabe aufgelistet. • Wenn OKM aktiviert ist, <code>OKM</code> wird in der Befehlsausgabe aufgelistet. • Wenn kein Schlüsselmanager aktiviert ist, <code>No key manager keystores configured</code> wird in der Befehlsausgabe aufgeführt.
ONTAP 9.13.1 oder früher	<pre>security key-manager show-key-store</pre> <ul style="list-style-type: none"> • Wenn EKM aktiviert ist, <code>external</code> wird in der Befehlsausgabe aufgelistet. • Wenn OKM aktiviert ist, <code>onboard</code> wird in der Befehlsausgabe aufgelistet. • Wenn kein Schlüsselmanager aktiviert ist, <code>No key managers configured</code> wird in der Befehlsausgabe aufgeführt.

2. Wählen Sie eine der folgenden Optionen, je nachdem, ob ein Key Manager auf Ihrem System konfiguriert ist.

Kein Schlüsselmanager konfiguriert

Sie können den außer Betrieb genommenen Controller sicher herunterfahren. Gehen Sie zu ["Schalten Sie den außer Betrieb genommenen Controller aus"](#).

Externer oder integrierter Schlüsselmanager konfiguriert

- a. Geben Sie den folgenden Abfragebefehl ein, um den Status der Authentifizierungsschlüssel in Ihrem Schlüsselmanager anzuzeigen.

```
security key-manager key query
```

- b. Überprüfen Sie die Ausgabe für den Wert in der `Restored` Spalte für Ihren Schlüsselmanager.

Diese Spalte gibt an, ob die Authentifizierungsschlüssel für Ihren Schlüsselmanager (entweder EKM oder OKM) erfolgreich wiederhergestellt wurden.

3. Wählen Sie je nachdem, ob Ihr System den External Key Manager oder den Onboard Key Manager verwendet, eine der folgenden Optionen aus.

Externer Schlüsselmanager

Befolgen Sie je nach dem in der Spalte angezeigten Ausgangswert `Restored` die entsprechenden Schritte.

Ausgabewert in <code>Restored</code> Spalte	Führen Sie die folgenden Schritte aus...
<code>true</code>	Sie können den außer Betrieb genommenen Controller sicher herunterfahren. Gehen Sie zu "Schalten Sie den außer Betrieb genommenen Controller aus" .
Alles andere als <code>true</code>	<p>a. Stellen Sie die externen Authentifizierungsschlüssel für das Verschlüsselungsmanagement auf allen Nodes im Cluster mit dem folgenden Befehl wieder her:</p> <pre>security key-manager external restore</pre> <p>Wenn der Befehl fehlschlägt, wenden Sie sich an "NetApp Support".</p> <p>b. Überprüfen Sie, ob in der <code>Restored</code> Spalte für alle Authentifizierungsschlüssel die angezeigt werden <code>true</code>, indem Sie den Befehl eingeben <code>security key-manager key query</code>.</p> <p>Wenn alle Authentifizierungsschlüssel vorhanden sind <code>true</code>, können Sie den beeinträchtigten Controller sicher herunterfahren. Gehen Sie zu "Schalten Sie den außer Betrieb genommenen Controller aus".</p>

Onboard Key Manager

Befolgen Sie je nach dem in der Spalte angezeigten Ausgangswert `Restored` die entsprechenden Schritte.

Ausgabewert in Restored Spalte	Führen Sie die folgenden Schritte aus...
true	<p>Sichern Sie die OKM-Informationen manuell.</p> <ol style="list-style-type: none">Wechseln Sie in den erweiterten Modus, indem <code>set -priv advanced</code> Sie aufrufen und dann bei Aufforderung eingeben <code>Y</code>.Geben Sie den folgenden Befehl ein, um die Informationen zum Verschlüsselungsmanagement anzuzeigen: <pre>security key-manager onboard show-backup</pre>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.Sie können den außer Betrieb genommenen Controller sicher herunterfahren. Gehen Sie zu "Schalten Sie den außer Betrieb genommenen Controller aus".

Ausgabewert in Restored Spalte	Führen Sie die folgenden Schritte aus...
Alles andere als true	<p>a. Geben Sie den integrierten Sicherheitsschlüssel-Manager Sync-Befehl ein:</p> <pre>security key-manager onboard sync</pre> <p>b. Geben Sie bei Aufforderung die 32-stellige alphanumerische Passphrase für das Onboard-Verschlüsselungsmanagement ein.</p> <p>Wenn die Passphrase nicht angegeben werden kann, wenden Sie sich an "NetApp Support".</p> <p>c. Überprüfen Sie, ob die Restored Spalte für alle Authentifizierungsschlüssel angezeigt wird true:</p> <pre>security key-manager key query</pre> <p>d. Überprüfen Sie, ob der Key Manager Typ , anzeigt `onboard` und sichern Sie die OKM-Informationen manuell.</p> <p>e. Geben Sie den Befehl ein, um die Backup-Informationen für das Verschlüsselungsmanagement anzuzeigen:</p> <pre>security key-manager onboard show-backup</pre> <p>f. Kopieren Sie den Inhalt der Backup-Informationen in eine separate Datei oder eine Protokolldatei.</p> <p>Sie werden es in Disaster-Szenarien benötigen, in denen Sie OKM manuell wiederherstellen müssen.</p> <p>g. Sie können den außer Betrieb genommenen Controller sicher herunterfahren. Gehen Sie zu "Schalten Sie den außer Betrieb genommenen Controller aus".</p>

Schalten Sie den Controller für beeinträchtigten Betrieb aus - AFF C30 und AFF C60

Schalten Sie den außer Betrieb genommenen Controller aus oder übernehmen Sie ihn.

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 über ein SAN-System verfügen, müssen Sie Event-Meldungen) für den beeinträchtigten Controller SCSI Blade überprüft haben `cluster kernel-service show`. Mit dem `cluster kernel-service show` Befehl (im erweiterten Modus von `priv`) werden der Knotenname, der Node, der

Verfügbarkeitsstatus dieses Node und der Betriebsstatus dieses Node angezeigt "[Quorum-Status](#)".

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, können Sie die automatische Case-Erstellung durch Aufrufen einer AutoSupport Meldung unterdrücken: `system node autosupport invoke -node * -type all -message MAINT=<# of hours>h`

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 Controller mit dem ordnungsgemäßen Zustand: `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	Fahren Sie mit dem nächsten Schritt fort.
Warten auf Giveback...	Drücken Sie Strg-C, und antworten Sie dann <i>y</i> Wenn Sie dazu aufgefordert werden.
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... anzeigt, drücken Sie Strg-C, und antworten Sie dann <i>y</i> .

Ersetzen Sie das Startmedium – AFF C30 und AFF C60

Um das Startmedium zu ersetzen, müssen Sie den Controller für beeinträchtigte Geräte entfernen, das Startmedium entfernen, das neue Startmedium installieren und das Startabbild auf ein USB-Flash-Laufwerk übertragen.

Schritt 1: Entfernen Sie die Steuerung

Sie müssen den Controller aus dem Chassis entfernen, wenn Sie den Controller austauschen oder eine Komponente im Controller austauschen.

Bevor Sie beginnen

Alle anderen Komponenten des Speichersystems müssen ordnungsgemäß funktionieren. Andernfalls müssen Sie sich an Sie wenden, bevor Sie mit "NetApp Support" diesem Verfahren fortfahren.

Schritte

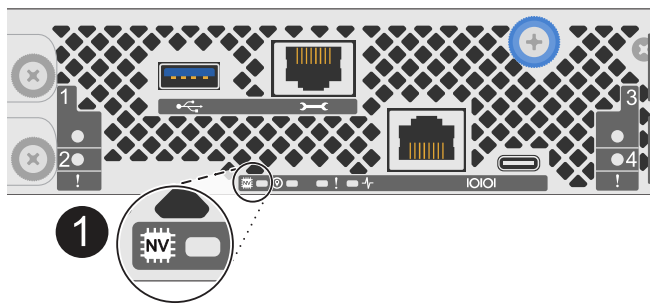
1. Stellen Sie am Controller für beeinträchtigte Störungen sicher, dass die NV-LED nicht leuchtet.

Wenn die NV-LED ausgeschaltet ist, ist die Entrampung abgeschlossen, und es ist sicher, den außer Betrieb genommenen Controller zu entfernen.



Wenn die NV-LED blinkt (grün), wird die Auslagerung ausgeführt. Sie müssen warten, bis die NV-LED erlischt. Wenn das Blinken jedoch länger als fünf Minuten andauert, wenden Sie sich an "NetApp Support", bevor Sie mit diesem Verfahren fortfahren.

Die NV-LED befindet sich neben dem NV-Symbol auf dem Controller.



1	NV-Symbol und LED am Controller
----------	---------------------------------

1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
2. Trennen Sie die Stromversorgung des außer Betrieb genommenen Controllers:



Netzteile (PSUs) verfügen über keinen Netzschalter.

Wenn Sie eine Verbindung trennen...	Dann...
NETZTEILEINHEIT	<ol style="list-style-type: none">a. Öffnen Sie die Netzkabelhalterung.b. Ziehen Sie das Netzkabel vom Netzteil ab, und legen Sie es beiseite.

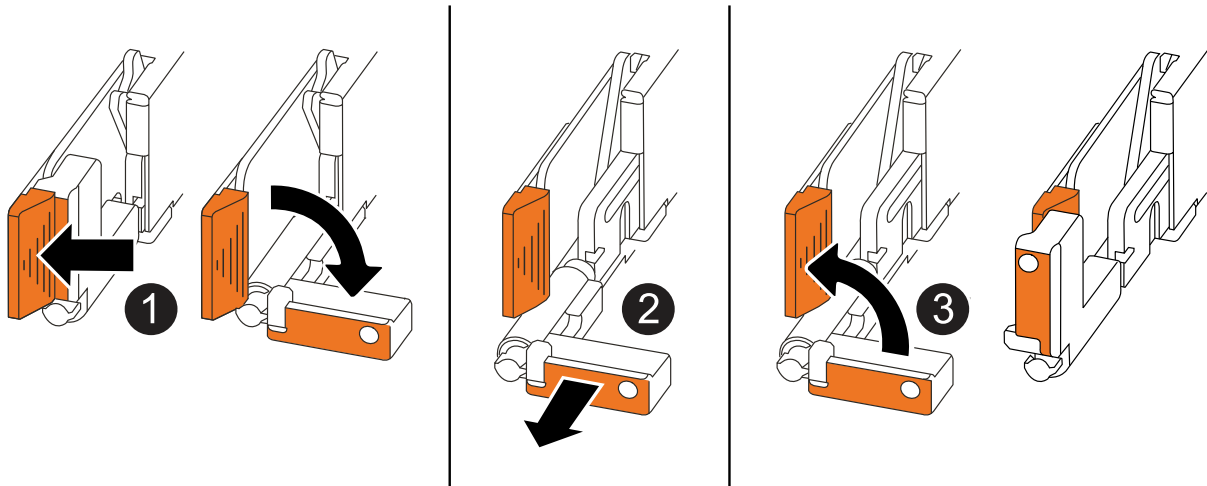
Wenn Sie eine Verbindung trennen...	Dann...
DC-NETZTEIL	<p>a. Lösen Sie die beiden Flügelschrauben am D-SUB-DC-Netzanschluss.</p> <p>b. Ziehen Sie das Netzkabel vom Netzteil ab, und legen Sie es beiseite.</p>

3. Ziehen Sie alle Kabel vom Controller für beeinträchtigte Verbindung ab.

Verfolgen Sie, wo die Kabel angeschlossen wurden.

4. Entfernen Sie die Steuerung für den beeinträchtigten Betrieb:

Die folgende Abbildung zeigt den Betrieb der Controller-Griffe (von der linken Seite des Controllers) beim Entfernen eines Controllers:



1	Drücken Sie an beiden Enden der Steuerung die vertikalen Verriegelungslaschen nach außen, um die Griffe zu lösen.
2	<ul style="list-style-type: none"> • Ziehen Sie die Griffe zu sich, um den Controller von der Mittelplatine zu lösen. <p>Wenn Sie ziehen, die Griffe aus dem Controller und dann fühlen Sie einen gewissen Widerstand, ziehen Sie weiter.</p> <ul style="list-style-type: none"> • Schieben Sie den Controller aus dem Chassis heraus, während Sie die Unterseite des Controllers stützen, und platzieren Sie ihn auf einer ebenen, stabilen Oberfläche.
3	Drehen Sie die Griffe bei Bedarf aufrecht (neben den Laschen), um sie aus dem Weg zu bewegen.

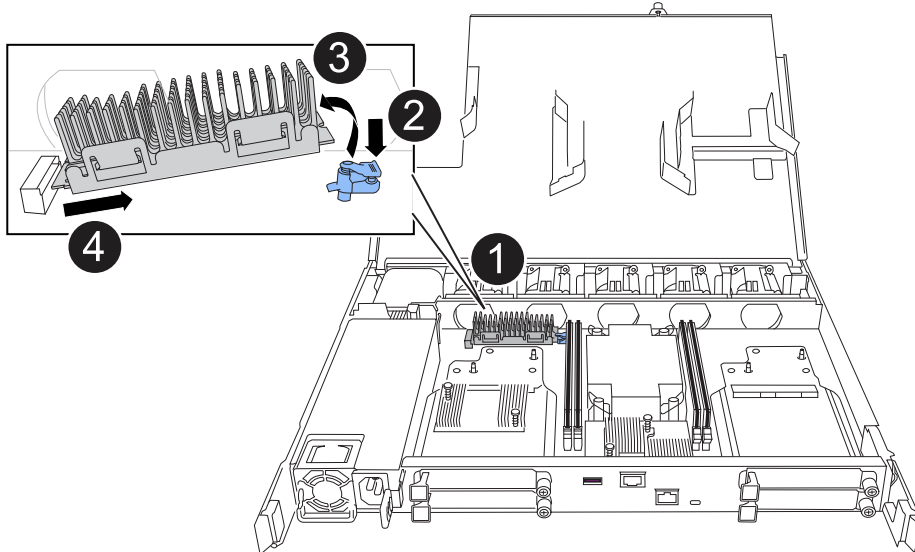
5. Setzen Sie die Steuerung auf eine antistatische Matte.

6. Öffnen Sie die Controllerabdeckung, indem Sie die Flügelschraube gegen den Uhrzeigersinn drehen, um sie zu lösen, und öffnen Sie dann die Abdeckung.

Schritt 2: Ersetzen Sie die Startmedien

Um das Boot-Medium auszutauschen, suchen Sie es im Controller, und befolgen Sie die Schritte in der entsprechenden Reihenfolge.

1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
2. Entfernen Sie das Startmedium:



1	Speicherort des Startmediums
2	Drücken Sie auf die blaue Lasche, um das rechte Ende des Startmediums freizugeben.
3	Heben Sie das rechte Ende des Kofferraummediums in einem leichten Winkel an, um einen guten Halt an den Seiten des Kofferraummediums zu erhalten.
4	Ziehen Sie das linke Ende des Trägermediums vorsichtig aus dem Sockel.

3. Installieren Sie das Ersatz-Startmedium:

- a. Entfernen Sie das Startmedium aus seinem Paket.
- b. Schieben Sie das Buchsenende des Startmediums in den entsprechenden Sockel.
- c. Drücken Sie am gegenüberliegenden Ende des Startmediums die blaue Lasche (in geöffneter Position) nach unten und halten Sie sie gedrückt, drücken Sie das Ende des Startmediums vorsichtig nach unten, bis es stoppt, und lassen Sie dann die Lasche los, um das Startmedium zu fixieren.

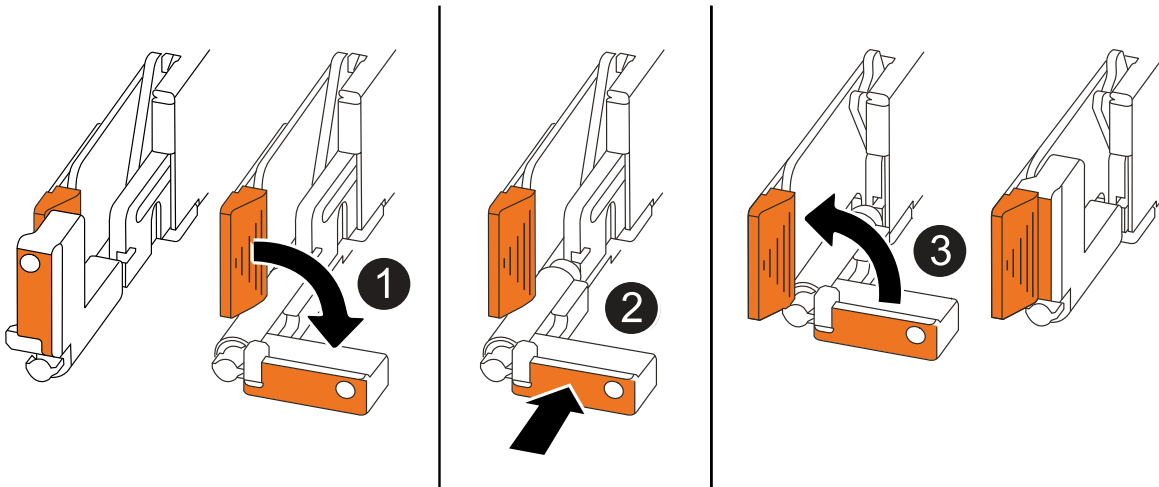
Schritt 3: Installieren Sie den Controller neu

Setzen Sie den Controller wieder in das Gehäuse ein, aber führen Sie keinen Neustart durch.

Über diese Aufgabe

Die folgende Abbildung zeigt den Betrieb der Controller-Griffe (von der linken Seite eines Controllers) beim Wiedereinbau des Controllers und kann als Referenz für die weiteren Schritte zur Neuinstallation des

Controllers verwendet werden.



1	Wenn Sie die Controller-Griffe senkrecht (neben den Laschen) gedreht haben, um sie während der Wartung des Controllers aus dem Weg zu bewegen, drehen Sie sie nach unten in die horizontale Position.
2	Drücken Sie die Griffe, um den Controller wieder in das Gehäuse einzusetzen, und drücken Sie dann, wenn Sie dazu aufgefordert werden, bis der Controller vollständig eingesetzt ist.
3	Drehen Sie die Griffe in die aufrechte Position und sichern Sie sie mit den Verriegelungslaschen.

Schritte

1. Schließen Sie die Controllerabdeckung, und drehen Sie die Flügelschraube im Uhrzeigersinn, bis sie festgezogen ist.
2. Setzen Sie den Controller zur Hälfte in das Chassis ein.

Richten Sie die Rückseite des Controllers an der Öffnung im Chassis aus, und drücken Sie dann den Controller vorsichtig mit den Griffen.



Setzen Sie den Controller erst dann vollständig in das Chassis ein, wenn Sie dazu später in diesem Verfahren aufgefordert werden.

3. Schließen Sie die Kabel wieder an den Controller an. Schließen Sie das Netzkabel jedoch derzeit nicht an das Netzteil an.



Stellen Sie sicher, dass das Konsolenkabel mit dem Controller verbunden ist, da Sie die Boot-Sequenz später beim Austausch der Boot-Medien fangen und protokollieren möchten, wenn Sie den Controller vollständig im Chassis eingesetzt haben und er mit dem Booten beginnt.

Schritt 4: Übertragen Sie das Startabbild auf das Startmedium

Das von Ihnen installierte Ersatzstartmedium ist ohne ein ONTAP-Image, sodass Sie ein ONTAP-Image mithilfe eines USB-Flashlaufwerks übertragen müssen.

Bevor Sie beginnen

- Sie müssen über ein USB-Flash-Laufwerk verfügen, das auf FAT32 formatiert ist und eine Kapazität von mindestens 4 GB aufweist.
- Sie müssen über eine Kopie derselben Image-Version von ONTAP verfügen, wie der beeinträchtigte Controller ausgeführt wurde. Sie können das entsprechende Image im Abschnitt auf der NetApp Support-Website herunterladen "[Downloads](#)"
 - Wenn NVE unterstützt wird, laden Sie das Image mit NetApp Volume Encryption herunter, wie auf der Download-Schaltfläche angegeben.
 - Wenn NVE nicht unterstützt wird, laden Sie das Image ohne NetApp-Volume-Verschlüsselung herunter, wie auf der Download-Schaltfläche angegeben.
- Sie müssen über eine Netzwerkverbindung zwischen den Node-Management-Ports der Controller (in der Regel die E0M Schnittstellen) verfügen.

Schritte

1. Laden Sie das entsprechende Service-Image vom auf das USB-Flash-Laufwerk herunter, und kopieren "[NetApp Support Website](#)" Sie es.
 - a. Laden Sie das Service-Image über den Link Downloads auf der Seite auf Ihren Arbeitsbereich auf Ihrem Laptop herunter.
 - b. Entpacken Sie das Service-Image.



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

Das USB-Flash-Laufwerk sollte über das entsprechende ONTAP-Image des ausgeführten Controllers verfügen.

- a. Entfernen Sie das USB-Flash-Laufwerk von Ihrem Laptop.
2. Schließen Sie das USB-Flash-Laufwerk an den USB-A-Anschluss des außer Betrieb genommenen Controllers an.

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

3. Setzen Sie den außer Betrieb genommenen Controller vollständig in das Gehäuse ein:
 - a. Drücken Sie die Griffe fest, bis der Controller auf die Mittelplatte trifft und vollständig sitzt.



Schieben Sie den Controller nicht zu stark in das Gehäuse, da dadurch die Anschlüsse beschädigt werden können.



Der Controller bootet, wenn er vollständig im Chassis eingesetzt ist. Er bezieht seine Leistung vom Partner-Controller.

- a. Drehen Sie die Controller-Griffe nach oben und fixieren Sie sie mit den Laschen.
- 4. Unterbrechen Sie den Boot-Vorgang, indem Sie Strg-C drücken, um an der LOADER-Eingabeaufforderung zu stoppen.

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

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

- Wenn Sie DHCP konfigurieren:

```
ifconfig e0M -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 e0M -addr=filer_addr -mask=netmask -gw=gateway
```

- 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.



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

- 6. Schließen Sie das Netzkabel wieder an das Netzteil (PSU) des außer Betrieb genommenen Controllers an.

Sobald das Netzteil wieder mit Strom versorgt wird, sollte die Status-LED grün leuchten.

Wenn Sie eine Verbindung...	Dann...
NETZTEILEINHEIT	<ul style="list-style-type: none"> a. Schließen Sie das Netzkabel an das Netzteil an. b. Befestigen Sie das Netzkabel mit der Netzkabelhalterung.
DC-NETZTEIL	<ul style="list-style-type: none"> a. Schließen Sie den D-SUB-DC-Netzkabelanschluss an das Netzteil an. b. Ziehen Sie die beiden Flügelschrauben fest, um den D-SUB DC-Netzkabelanschluss am Netzteil zu befestigen.

Starten Sie das Wiederherstellungs-Image - AFF C30 und AFF C60

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:

Option 1: ONTAP 9.16.0 oder früher

- a. Drücken Sie auf der außer Betrieb genommenen Steuerung Y, wenn angezeigt wird `Do you want to restore the backup configuration now?`
- b. Drücken Sie auf dem Controller für beeinträchtigte Störungen Y, wenn Sie dazu aufgefordert werden, `/etc/ssh/ssh_Host_ecdsa_Key` zu überschreiben.
- c. Setzen Sie auf dem funktionierenden Partner-Controller den beeinträchtigten Controller auf die erweiterte Berechtigungsebene: `set -privilege advanced`.
- d. Führen Sie auf dem gesunden Partner-Controller den Wiederherstellungsbefehl aus: `system node restore-backup -node local -target-address impaired_node_IP_address`.

HINWEIS: Wenn Sie eine andere Nachricht als eine erfolgreiche Wiederherstellung sehen, kontaktieren Sie ["NetApp Support"](#).

- e. Setzen Sie auf dem gesunden Partner-Controller den beeinträchtigten Controller auf Admin-Ebene zurück: `set -privilege admin`.
- f. Drücken Sie auf der außer Betrieb genommenen Steuerung Y, wenn angezeigt wird `Was the restore backup procedure successful?.`
- g. Drücken Sie auf der außer Betrieb genommenen Steuerung Y, wenn angezeigt wird `...would you like to use this restored copy now?.`
- h. Drücken Sie auf dem Controller für beeinträchtigte Y Störungen, wenn Sie dazu aufgefordert werden, den Controller für beeinträchtigte Störungen neu zu starten, und drücken Sie `ctrl-c` für das Startmenü.
- i. Wenn das System keine Verschlüsselung verwendet, wählen Sie *Option 1 Normal Boot.*, andernfalls gehen Sie zu ["Wiederherstellung der Verschlüsselung"](#).

Option 2: ONTAP 9.16.1 oder höher

- a. Drücken Sie auf dem Controller für beeinträchtigte Y Vorgänge, wenn Sie dazu aufgefordert werden, die Sicherungskonfiguration wiederherzustellen.

Nachdem der Wiederherstellungsvorgang erfolgreich war, wird diese Meldung auf der Konsole - angezeigt `syncflash_partner: Restore from partner complete`.

- b. Drücken Sie auf dem Controller für beeinträchtigte Y Vorgänge, wenn Sie dazu aufgefordert werden, um zu bestätigen, ob die Wiederherstellung erfolgreich war.
- c. Drücken Sie auf dem Controller für beeinträchtigte Störungen Y, wenn Sie dazu aufgefordert werden, die wiederhergestellte Konfiguration zu verwenden.
- d. Drücken Sie auf dem Controller für beeinträchtigte Störungen Y bei der Aufforderung, um den Node neu zu booten.
- e. Drücken Sie auf dem Controller für beeinträchtigte Y Störungen, wenn Sie dazu aufgefordert werden, den Controller für beeinträchtigte Störungen neu zu starten, und drücken Sie `ctrl-c` für das Startmenü.
- f. Wenn das System keine Verschlüsselung verwendet, wählen Sie *Option 1 Normal Boot.*, andernfalls gehen Sie zu ["Wiederherstellung der Verschlüsselung"](#).

4. Schließen Sie das Konsolenkabel an den Partner Controller an.
5. Geben Sie den Controller mithilfe des zurück `storage failover giveback -fromnode local` Befehl.
6. Stellen Sie die automatische Rückgabe wieder her, wenn Sie die Funktion mithilfe von deaktivieren `storage failover modify -node local -auto-giveback true` Befehl.
7. Wenn AutoSupport aktiviert ist, können Sie die automatische Fehlerstellung mit dem Befehl wiederherstellen/zurücknehmen. `system node autosupport invoke -node * -type all -message MAINT=END`

HINWEIS: Wenn der Prozess fehlschlägt, kontaktieren Sie ["NetApp Support"](#).

Wiederherstellung der Verschlüsselung – AFF C30 und AFF C60

Stellen Sie die Verschlüsselung auf dem Ersatz-Startmedium wieder her.

Sie müssen die Schritte speziell für Systeme mit aktiviertem Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) oder NetApp Volume Encryption (NVE) anhand der Einstellungen abschließen, die Sie zu Beginn des Austauschvorgangs des Boot-Mediums erfasst haben.

Je nachdem, welcher Key Manager auf Ihrem System konfiguriert ist, wählen Sie eine der folgenden Optionen aus, um ihn im Startmenü wiederherzustellen.

- ["Option 1: Wiederherstellen der Onboard Key Manager-Konfiguration"](#)
- ["Option 2: Wiederherstellung der Konfiguration des externen Schlüsselmanagers"](#)

Option 1: Wiederherstellen der Onboard Key Manager-Konfiguration

Stellen Sie die OKM-Konfiguration (Onboard Key Manager) über das ONTAP-Startmenü wieder her.

Bevor Sie beginnen

- Stellen Sie sicher, dass Sie beim Wiederherstellen der OKM-Konfiguration folgende Informationen haben:
 - Cluster-weite Passphrase eingegeben ["Und ermöglicht integriertes Verschlüsselungsmanagement"](#).
 - ["Backup-Informationen für den Onboard Key Manager"](#).
- Führen Sie das ["Verifizierung von Onboard-Verschlüsselungsmanagement-Backup und Cluster-weiter Passphrase"](#) Verfahren durch, bevor Sie fortfahren.

Schritte

1. Schließen Sie das Konsolenkabel an den Ziel-Controller an.
2. Wählen Sie im ONTAP-Startmenü die entsprechende Option aus dem Startmenü aus.

ONTAP-Version	Wählen Sie diese Option aus
ONTAP 9.8 oder höher	<p data-bbox="621 153 906 191">Wählen Sie Option 10.</p> <p data-bbox="621 222 1073 260">Beispiel für ein Startmenü anzeigen</p> <div data-bbox="654 296 1455 1079" style="border: 1px solid #ccc; padding: 10px;"><p data-bbox="683 331 1295 369">Please choose one of the following:</p><ul data-bbox="683 411 1370 1010" style="list-style-type: none"><li data-bbox="683 411 980 449">(1) Normal Boot.<li data-bbox="683 453 1138 491">(2) Boot without /etc/rc.<li data-bbox="683 495 1049 533">(3) Change password.<li data-bbox="683 537 1370 606">(4) Clean configuration and initialize all disks.<li data-bbox="683 611 1154 648">(5) Maintenance mode boot.<li data-bbox="683 653 1330 690">(6) Update flash from backup config.<li data-bbox="683 695 1243 732">(7) Install new software first.<li data-bbox="683 737 980 774">(8) Reboot node.<li data-bbox="683 779 1192 848">(9) Configure Advanced Drive Partitioning.<li data-bbox="683 852 1333 921">(10) Set Onboard Key Manager recovery secrets.<li data-bbox="683 926 1317 995">(11) Configure node for external key management.<p data-bbox="683 1010 1032 1047">Selection (1-11)? 10</p></div>

ONTAP-Version	Wählen Sie diese Option aus
ONTAP 9.7 und frühere Versionen	<p data-bbox="626 159 1146 226">Wählen Sie die ausgeblendete Option aus <code>recover_onboard_keymanager</code></p> <p data-bbox="626 260 1073 289">Beispiel für ein Startmenü anzeigen</p> <div data-bbox="656 331 1455 999" style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <pre data-bbox="682 373 1370 961">Please choose one of the following: (1) Normal Boot. (2) Boot without /etc/rc. (3) Change password. (4) Clean configuration and initialize all disks. (5) Maintenance mode boot. (6) Update flash from backup config. (7) Install new software first. (8) Reboot node. (9) Configure Advanced Drive Partitioning. Selection (1-19)? recover_onboard_keymanager</pre> </div>

3. Bestätigen Sie, dass Sie den Wiederherstellungsprozess fortsetzen möchten.

Beispiel-Eingabeaufforderung anzeigen

```
This option must be used only in disaster recovery procedures. Are you
sure? (y or n):
```

4. Geben Sie die Cluster-weite Passphrase zweimal ein.

Während der Eingabe der Passphrase zeigt die Konsole keine Eingaben an.

Beispiel-Eingabeaufforderung anzeigen

```
Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:
```

5. Geben Sie die Sicherungsinformationen ein.

a. Fügen Sie den gesamten Inhalt aus der Zeile „START BACKUP“ durch die Zeile „END BACKUP“ ein.

Beispiel-Eingabeaufforderung anzeigen

```
Trying to recover keymanager secrets....
Setting recovery material for the onboard key manager
Recovery secrets set successfully
Trying to delete any existing km_onboard.wkeydb file.

Successfully recovered keymanager secrets.

*****
*****
* Select option "(1) Normal Boot." to complete recovery process.
*
* Run the "security key-manager onboard sync" command to
synchronize the key database after the node reboots.
*****
*****
```



Fahren Sie nicht fort, wenn die angezeigte Ausgabe etwas anderes als `Successfully recovered keymanager secrets` ist. Führen Sie die Fehlerbehebung durch, um den Fehler zu beheben.

6. Wählen Sie Option 1 aus dem Startmenü, um mit dem Booten in ONTAP fortzufahren.

Beispiel-Eingabeaufforderung anzeigen

```
*****
*****
* Select option "(1) Normal Boot." to complete the recovery process.
*
*****
*****

(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 1
```

7. Vergewissern Sie sich, dass an der Konsole des Controllers die folgende Meldung angezeigt wird.

```
Waiting for giveback...(Press Ctrl-C to abort wait)
```

8. Geben Sie am Partner-Node den Partner-Controller ein, indem Sie den folgenden Befehl eingeben.

```
storage failover giveback -fromnode local -only-cfo-aggregates true.
```

9. Führen Sie nach dem Booten nur mit dem CFO-Aggregat den folgenden Befehl aus.

```
security key-manager onboard sync
```

10. Geben Sie die Cluster-weite Passphrase für das Onboard Key Manager ein.

Beispiel-Eingabeaufforderung anzeigen

```
Enter the cluster-wide passphrase for the Onboard Key Manager:
```

```
All offline encrypted volumes will be brought online and the corresponding volume encryption keys (VEKs) will be restored automatically within 10 minutes. If any offline encrypted volumes are not brought online automatically, they can be brought online manually using the "volume online -vserver <vserver> -volume <volume_name>" command.
```



Wenn die Synchronisierung erfolgreich war, wird die Cluster-Eingabeaufforderung ohne weitere Meldungen zurückgegeben. Wenn die Synchronisierung fehlschlägt, wird eine Fehlermeldung angezeigt, bevor Sie zur Cluster-Eingabeaufforderung zurückkehren. Fahren Sie nicht fort, bis der Fehler behoben ist und die Synchronisierung erfolgreich ausgeführt wird.

11. Stellen Sie sicher, dass alle Schlüssel synchronisiert wurden, indem Sie den folgenden Befehl eingeben.

```
security key-manager key query -restored false.
```

```
There are no entries matching your query.
```



Beim Filtern nach FALSE im wiederhergestellten Parameter sollten keine Ergebnisse angezeigt werden.

12. Geben Sie dem Partner ein Giveback des Node durch Eingabe des folgenden Befehls ein.

```
storage failover giveback -fromnode local
```

13. Stellen Sie das automatische Giveback wieder her, wenn Sie es deaktiviert haben, indem Sie den folgenden Befehl eingeben.

```
storage failover modify -node local -auto-giveback true
```

14. Wenn AutoSupport aktiviert ist, stellen Sie die automatische Fallerstellung durch Eingabe des folgenden Befehls wieder her.

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Option 2: Wiederherstellung der Konfiguration des externen Schlüsselmanagers

Stellen Sie die Konfiguration des externen Schlüsselmanagers über das ONTAP-Startmenü wieder her.

Bevor Sie beginnen

Sie benötigen die folgenden Informationen für die Wiederherstellung der EKM-Konfiguration (External Key Manager).

- Eine Kopie der Datei `/cfcard/kmip/servers.cfg` von einem anderen Clusterknoten oder die folgenden Informationen:
 - Die Adresse des KMIP-Servers.
 - Der KMIP-Port.
- Eine Kopie der `/cfcard/kmip/certs/client.crt` Datei von einem anderen Cluster-Node oder dem Client-Zertifikat.
- Eine Kopie der `/cfcard/kmip/certs/client.key` Datei von einem anderen Cluster-Node oder dem Client-Schlüssel.
- Eine Kopie der `/cfcard/kmip/certs/CA.pem` Datei von einem anderen Cluster-Knoten oder der KMIP-Server-CA(s).

Schritte

1. Schließen Sie das Konsolenkabel an den Ziel-Controller an.
2. Wählen Sie Option 11 aus dem ONTAP-Startmenü.

Beispiel für ein Startmenü anzeigen

```
(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 11
```

3. Bestätigen Sie, dass Sie die erforderlichen Informationen gesammelt haben, wenn Sie dazu aufgefordert werden.

Beispiel-Eingabeaufforderung anzeigen

```
Do you have a copy of the /cfcard/kmip/certs/client.crt file? {y/n}
Do you have a copy of the /cfcard/kmip/certs/client.key file? {y/n}
Do you have a copy of the /cfcard/kmip/certs/CA.pem file? {y/n}
Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n}
```

4. Geben Sie bei der entsprechenden Aufforderung die Client- und Serverinformationen ein.

Eingabeaufforderung anzeigen

```
Enter the client certificate (client.crt) file contents:
Enter the client key (client.key) file contents:
Enter the KMIP server CA(s) (CA.pem) file contents:
Enter the server configuration (servers.cfg) file contents:
```

Beispiel anzeigen

```
Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwY8xCzAJBgNVBAYTA1VT
MRMwEQYDVQQIEWpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk51
MSUubQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxcilJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxpbz3mXF/X/1PC3YOzVNCq5eieek62si
Fp8=
-----END CERTIFICATE-----

Enter the client key (client.key) file contents:
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----

Enter the KMIP server CA(s) (CA.pem) file contents:
-----BEGIN CERTIFICATE-----
MIIEizCCA3OgAwIBAgIBADANBgkqhkiG9w0BAQsFADCBjzELMAkGA1UEBhMCVVMx
7yaumMQETNrpMfP+nQMd34y4AmseWYGM6qG0z37BRnYU0Wf2qDL61cQ3/jkm7Y94
EQBKG1NY8dVyjphmYZv+
-----END CERTIFICATE-----

Enter the IP address for the KMIP server: 10.10.10.10
Enter the port for the KMIP server [5696]:

System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
kmp_init: configuring ports
Running command '/sbin/ifconfig e0M'
..
..
kmp_init: cmd: ReleaseExtraBSDPort e0M
```

Nachdem Sie die Client- und Serverinformationen eingegeben haben, ist der Wiederherstellungsvorgang abgeschlossen.

Beispiel anzeigen

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
[Aug 29 21:06:28]: 0x808806100: 0: DEBUG: kmip2::main:
[initOpenssl]:460: Performing initialization of OpenSSL
Successfully recovered keymanager secrets.
```

5. Wählen Sie Option 1 aus dem Startmenü, um mit dem Booten in ONTAP fortzufahren.

Beispiel-Eingabeaufforderung anzeigen

```
*****
*****
* Select option "(1) Normal Boot." to complete the recovery process.
*
*****
*****

(1) Normal Boot.
(2) Boot without /etc/rc.
(3) Change password.
(4) Clean configuration and initialize all disks.
(5) Maintenance mode boot.
(6) Update flash from backup config.
(7) Install new software first.
(8) Reboot node.
(9) Configure Advanced Drive Partitioning.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? 1
```

6. Stellen Sie das automatische Giveback wieder her, wenn Sie es deaktiviert haben, indem Sie den folgenden Befehl eingeben.

```
storage failover modify -node local -auto-giveback true
```

7. Wenn AutoSupport aktiviert ist, stellen Sie die automatische Fallerstellung durch Eingabe des folgenden Befehls wieder her.

```
system node autosupport invoke -node * -type all -message MAINT=END
```

Senden Sie das fehlerhafte Teil an NetApp - AFF C30 und AFF C60 zurück

Senden Sie das fehlerhafte Teil wie in den dem Kit beiliegenden RMA-Anweisungen beschrieben an NetApp zurück. ["Rückgabe und Austausch von Teilen"](#) Weitere Informationen finden Sie auf der Seite.

Copyright-Informationen

Copyright © 2024 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.