Boot-Medien

Install and maintain

NetApp
January 09, 2026

Inhalt

Boot-Medien

Arbeitsablauf zum Ersetzen des Bootmediums – AFX 1K

Beginnen Sie mit dem Ersetzen des Startmediums in Ihrem AFX 1K-Speichersystem, indem Sie die Anforderungen für den Austausch überprüfen, den Verschlüsselungsstatus prüfen, den Controller herunterfahren, das Startmedium ersetzen, das Wiederherstellungsimage starten, die Verschlüsselung wiederherstellen und die Systemfunktionalität überprüfen.

1. **"Überprüfen Sie die Anforderungen der Startmedien"**

Überprüfen Sie die Anforderungen für den Austausch von Boot-Medien.

2. **"Fahren Sie den Controller herunter"**

Fahren Sie den Controller in Ihrem Speichersystem herunter, wenn Sie das Startmedium ersetzen müssen.

3. **"Ersetzen Sie das Startmedium"**

Entfernen Sie das fehlerhafte Startmedium aus dem System Management-Modul, und installieren Sie das Ersatz-Startmedium.

4. **"Stellen Sie das Image auf dem Startmedium wieder her"**

Stellen Sie das ONTAP-Image vom Partner-Controller wieder her.

5. **"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.

Voraussetzungen zum Ersetzen des Bootmediums - AFX 1K

Stellen Sie vor dem Austauschen des Startmediums in Ihrem AFX 1K-Speichersystem sicher, dass Sie die notwendigen Voraussetzungen für einen erfolgreichen Austausch erfüllen. Dazu gehört die Überprüfung, ob Sie über das richtige Ersatz-Bootmedium verfügen, die Bestätigung, dass keine defekten Cluster-Ports auf dem Controller vorhanden sind, und die Feststellung, ob Onboard Key Manager (OKM) oder External Key Manager (EKM) aktiviert ist.

Überprüfen Sie vor dem Austauschen des Startmediums die folgenden Anforderungen.

- 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.
- Es dürfen keine fehlerhaften Cluster-Ports auf dem gestörten Controller vorhanden sein.

Was kommt als Nächstes?

Nachdem Sie die Voraussetzungen für den Austausch des Bootmediums überprüft haben, müssen Sie"Fahren Sie den Controller herunter" .

Fahren Sie den Controller herunter, um das Bootmedium zu ersetzen – AFX 1K

Fahren Sie den beeinträchtigten Controller in Ihrem AFX 1K-Speichersystem herunter, um Datenverlust zu verhindern und die Systemstabilität beim Austausch des Startmediums sicherzustellen.

Um den beeinträchtigten Controller herunterzufahren, müssen Sie den Status des Controllers ermitteln und gegebenenfalls eine Speicher-Failover-Übernahme des Controllers durchführen, damit der fehlerfreie Controller weiterhin Daten aus dem beeinträchtigten Controller-Speicher bereitstellt.

Über diese Aufgabe

- Wenn Sie einen Cluster mit mehr als vier Knoten haben, muss dieser im Quorum sein. Um Clusterinformationen zu Ihren Knoten anzuzeigen, verwenden Sie die `cluster show` Befehl. Weitere Informationen zum `cluster show` Befehl, siehe"Anzeigen von Details auf Knotenebene in einem ONTAP Cluster" .
- Wenn der Cluster nicht im Quorum ist oder wenn der Zustand oder die Berechtigung eines Controllers (mit Ausnahme des beeinträchtigten Controllers) als falsch angezeigt wird, müssen Sie das Problem beheben, bevor Sie den beeinträchtigten Controller herunterfahren. Sehen "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=<# 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 die automatische Rückgabe von der Konsole des beeinträchtigten Controllers:

   ```
   storage failover modify -node impaired-node -auto-giveback-of false
   ```

   Wenn Sie *Möchten Sie die automatische Rückgabe deaktivieren?* sehen, geben Sie ein `y` .

   a. Wenn Sie ONTAP Version 9.17.1 ausführen und der beeinträchtigte Controller nicht hochgefahren werden kann oder bereits übernommen wurde, müssen Sie die HA-Verbindung vom fehlerfreien Controller trennen, bevor Sie den beeinträchtigten Controller hochfahren. Dadurch wird verhindert,

dass der beeinträchtigte Controller eine automatische Rückgabe durchführt.

```
system ha interconnect link off -node healthy-node -link 0
system ha interconnect link off -node healthy-node -link 1
```

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.
Eingabeaufforderung für das System oder Passwort	Übernehmen oder stoppen Sie den beeinträchtigten Controller vom fehlerfreien Controller: `storage failover takeover -ofnode` *`impaired_node_name`* `-halt` *`true`* Der Parameter *-halt true* bringt den beeinträchtigten Knoten zur LOADER-Eingabeaufforderung.

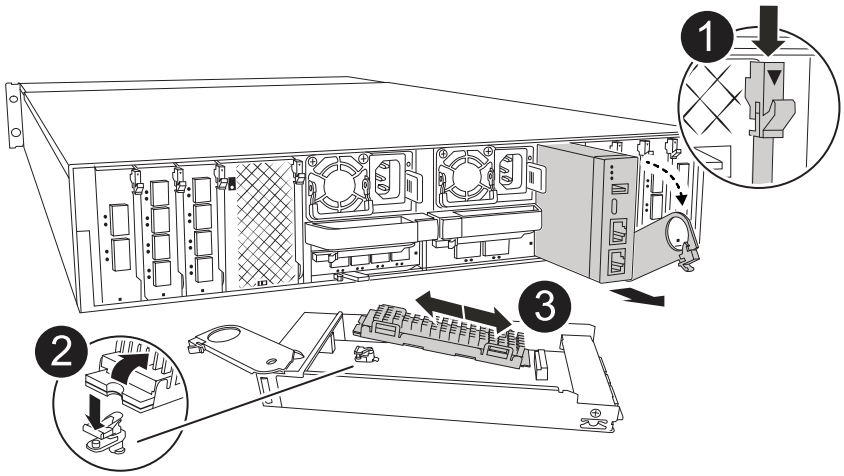
Was kommt als Nächstes?

Nach dem Herunterfahren des Controllers"Ändern Sie das Bootmedium" .

Ersetzen Sie das Bootmedium - AFX 1K

Das Bootmedium in Ihrem AFX 1K-Speichersystem speichert wichtige Firmware- und Konfigurationsdaten. Der Austauschvorgang umfasst das Entfernen des Systemverwaltungsmoduls, das Entfernen des beschädigten Bootmediums, das Installieren des Ersatz-Bootmediums im Systemverwaltungsmodul und die anschließende Neuinstallation des Systemverwaltungsmoduls.

Das Startmedium befindet sich im System Management-Modul und kann durch Entfernen des Moduls aus dem System aufgerufen werden.



1	Nockenverriegelung des Systemmanagementmoduls
2	Verriegelungstaste für Startmedien
3	Boot-Medien

Schritte

1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
2. Ziehen Sie die Stromversorgungskabel von den Netzteilen ab.
3. Entfernen Sie das System Management-Modul:
   a. Entfernen Sie die Kabel vom Systemverwaltungsmodul und beschriften Sie sie, um bei der Neuinstallation einen korrekten Anschluss sicherzustellen.
   b. Drehen Sie das Kabelführungs-Fach nach unten, indem Sie die Tasten an beiden Seiten an der Innenseite des Kabelführungs-Fachs ziehen und das Fach dann nach unten drehen.
   c. Drücken Sie die CAM-Taste für die Systemverwaltung.
   d. Drehen Sie die Nockenverriegelung so weit wie möglich nach unten.
   e. Entfernen Sie das System-Management-Modul aus dem Gehäuse, indem Sie den Finger in die Öffnung des Nockenhebels stecken und das Modul aus dem Gehäuse ziehen.
   f. Platzieren Sie das System-Management-Modul auf einer antistatischen Matte, damit das Startmedium zugänglich ist.
4. Entfernen Sie das Startmedium aus dem Verwaltungsmodul:
   a. Drücken Sie die blaue Verriegelungstaste.
   b. Drehen Sie das Startmedium nach oben, schieben Sie es aus dem Sockel und legen Sie es beiseite.
5. Installieren Sie das Ersatz-Startmedium im System Management-Modul:
   a. Richten Sie die Kanten der Startmedien am Buchsengehäuse aus, und schieben Sie sie vorsichtig in die Buchse.
   b. Drehen Sie das Startmedium nach unten in Richtung Verriegelungstaste.
   c. Drücken Sie die Verriegelungstaste, drehen Sie die Manschettenmedien ganz nach unten, und lassen Sie dann die Verriegelungstaste los.
6. Installieren Sie das System Management-Modul neu:
   a. Richten Sie das Modul an den Kanten der Öffnung des Gehäusesteckplatzes aus.
   b. Schieben Sie das Modul vorsichtig in den Steckplatz bis zum Gehäuse, und drehen Sie dann die Nockenverriegelung ganz nach oben, um das Modul zu verriegeln.
7. Drehen Sie das Kabelführungs-Fach bis in die geschlossene Position.
   a. System-Management-Modul erneut verwenden.
8. Schließen Sie die Netzkabel an die Netzteile an, und setzen Sie die Stromkabelhalterung wieder ein.

   Der Controller beginnt zu starten, sobald die Stromversorgung wieder mit dem System verbunden wird.

Was kommt als Nächstes?

Nach dem Austausch des Bootmediums"Stellen Sie das ONTAP-Image vom Partner-Node wieder her" .

Booten Sie das Wiederherstellungsimage – AFX 1K

Nachdem Sie das neue Boot-Mediengerät in Ihrem AFX 1K-Speichersystem installiert haben, können Sie den automatisierten Boot-Medienwiederherstellungsprozess starten, um die Konfiguration vom Partnerknoten wiederherzustellen.

Über diese Aufgabe

Während des Wiederherstellungsprozesses prüft das System, ob die Verschlüsselung aktiviert ist und identifiziert die Art der verwendeten Schlüsselverschlüsselung. Wenn die Schlüsselverschlüsselung aktiviert ist, führt Sie das System durch die entsprechenden Schritte zur Wiederherstellung.

Bevor Sie beginnen

- Für OKM benötigen Sie die clusterweite Passphrase und die Sicherungsdaten.
- Für EKM benötigen Sie Kopien der folgenden Dateien vom Partnerknoten:
  - Datei /cfcard/kmip/servers.cfg.
  - Datei /cfcard/kmip/certs/Client.crt.
  - Datei /cfcard/kmip/certs/client.key.
  - Datei /cfcard/kmip/certs/CA.pem.

Schritte

1. Geben Sie an der Loader-Eingabeaufforderung den Befehl ein:

   ```
   boot_recovery -partner
   ```

   Auf dem Bildschirm wird die folgende Meldung angezeigt:

   ```
   Starting boot media recovery (BMR) process. Press Ctrl-C to abort…
   ```

2. Überwachen Sie den Wiederherstellungsprozess für die Installation der Startmedien.

   Der Vorgang ist abgeschlossen und zeigt die `Installation complete` Meldung an.

3. Das System prüft nach Verschlüsselung und Verschlüsselungstyp und zeigt eine von zwei Meldungen an. Je nachdem, welche Meldung angezeigt wird, führen Sie eine der folgenden Aktionen durch:

   Gelegentlich kann der Prozess möglicherweise nicht erkennen, ob der Schlüsselmanager auf dem System konfiguriert ist. Es wird eine Fehlermeldung angezeigt, gefragt, ob Key Manager für das System konfiguriert ist, und dann gefragt, welcher Schlüsselmanager konfiguriert ist. Der Vorgang wird fortgesetzt, nachdem Sie das Problem behoben haben.

Beispiel für Eingabeaufforderungen zum Suchen von Konfigurationsfehlern anzeigen

```
Error when fetching key manager config from partner ${partner_ip}:
${status}

Has key manager been configured on this system

Is the key manager onboard
```

Wenn diese Meldung angezeigt wird…	Tun Sie das…
`key manager is not configured. Exiting.`	Auf dem System ist keine Verschlüsselung konfiguriert. Führen Sie die folgenden Schritte aus: a. Drücken Sie <enter>, wenn die Konsolenmeldungen angehalten werden. ◦ Wenn die Anmeldeaufforderung angezeigt wird, fahren Sie mit Schritt 4 fort. ◦ Wenn keine Anmeldeaufforderung angezeigt wird, melden Sie sich beim Partnerknoten an und fahren Sie mit Schritt 4 fort. b. Fahren Sie mit Schritt 6 fort, um die automatische Rückgabe zu aktivieren, falls sie deaktiviert war.
`key manager is configured.`	Fahren Sie mit Schritt 5 fort, um den entsprechenden Schlüsselmanager wiederherzustellen. Der Knoten greift auf das Startmenü zu und führt Folgendes aus: • Option 10 für Systeme mit Onboard Key Manager (OKM). • Option 11 für Systeme mit externem Key Manager (EKM).

4. Wenn auf dem System keine Verschlüsselung installiert ist und die Anmeldeaufforderung nicht angezeigt wird. Führen Sie die folgenden Schritte aus:

   a. Geben Sie nur die Wurzel mit der Option „override-destination-checks“ zurück:

      ```
      storage failover giveback -ofnode impaired-node -only-root true -override
      -destination-checks true
      ```

      Dieser Befehl ist nur im Diagnosemodus verfügbar. Weitere Informationen finden Sie unter "Berechtigungsstufen für ONTAP CLI-Befehle" .

      Wenn Sie auf Fehler stoßen, wenden Sie sich an "NetApp Support".

   b. Warten Sie 5 Minuten, nachdem der Giveback-Bericht abgeschlossen ist, und prüfen Sie den Failover-Status und den Giveback-Status:

`storage failover show`Und `storage failover show-giveback

Der folgende Befehl ist nur auf der Berechtigungsebene „Diagnosemodus“ verfügbar.

c. Wenn Sie ONTAP 9.17.1 ausführen und die HA-Internconnect-Links deaktiviert wurden, aktivieren Sie sie erneut:

```
system ha interconnect link on -node healthy-node -link 0

system ha interconnect link on -node healthy-node -link 1
```

Wenn Sie 9.18.1 oder höher ausführen, überspringen Sie den obigen Schritt und fahren Sie mit dem nächsten Schritt fort.

a. Stellen Sie den funktionsbeeinträchtigten Controller wieder in den Normalbetrieb ein, indem Sie den Speicher zurückgeben:

```
storage failover giveback -ofnode impaired_node_name
```

5. Wählen Sie für Systeme mit konfiguriertem Schlüsselmanager den entsprechenden Schlüsselmanager-Wiederherstellungsprozess aus.

Onboard Key Manager (OKM)

Wenn OKM erkannt wird, zeigt das System die folgende Meldung an und beginnt mit der Ausführung der Startmenüoption 10.

```
key manager is configured.
Entering Bootmenu Option 10...

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

a. Geben Sie an der Eingabeaufforderung ein `Y`, um zu bestätigen, dass Sie den OKM-Wiederherstellungsprozess starten möchten.

b. Geben Sie bei der entsprechenden Aufforderung Folgendes ein:

   i. Die Passphrase

   ii. Die Passphrase erneut, wenn Sie zur Bestätigung aufgefordert werden

   iii. Sicherungsdaten für den integrierten Schlüsselmanager

   Beispiel für Eingabeaufforderungen für Passphrasen und Sicherungsdaten anzeigen

   ```
   Enter the passphrase for onboard key management:
   -----BEGIN PASSPHRASE-----
   <passphrase_value>
   -----END PASSPHRASE-----
   Enter the passphrase again to confirm:
   -----BEGIN PASSPHRASE-----
   <passphrase_value>
   -----END PASSPHRASE-----
   Enter the backup data:
   -----BEGIN BACKUP-----
   <passphrase_value>
   -----END ACKUP-----
   ```

c. Überwachen Sie den Recovery-Prozess weiterhin, wenn die entsprechenden Dateien vom Partner-Node wiederhergestellt werden.

   Nach Abschluss der Wiederherstellung wird der Node neu gebootet. Die folgenden Meldungen weisen auf eine erfolgreiche Wiederherstellung hin:

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

Successfully recovered keymanager secrets.
```

d. Wenn der Node neu gebootet wird, überprüfen Sie, ob die Boot-Medien erfolgreich wiederhergestellt wurden, indem Sie bestätigen, dass das System wieder online und funktionsfähig ist.

e. Stellen Sie den funktionsbeeinträchtigten Controller wieder in den Normalbetrieb ein, indem Sie den Speicher zurückgeben:

`storage failover giveback -ofnode` *`impaired_node_name`*

i. Wenn die HA-Verbindungslinks getrennt wurden, aktivieren Sie sie erneut, um die automatische Rückgabe fortzusetzen:

`system ha interconnect link on -node healthy-node -link 0`

`system ha interconnect link on -node healthy-node -link 1`

f. Nachdem der Partner-Node vollständig eingerichtet ist und Daten bereitstellt, synchronisieren Sie die OKM-Schlüssel über das Cluster hinweg.

`security key-manager onboard sync`

Externer Schlüsselmanager (EKM)

Wenn EKM erkannt wird, zeigt das System die folgende Meldung an und beginnt mit der Ausführung der Startmenüoption 11.

```
key manager is configured.
Entering Bootmenu Option 11...
```

a. Je nachdem, ob der Schlüssel erfolgreich wiederhergestellt wurde, führen Sie eine der folgenden Aktionen durch:

- Wenn Sie sehen `kmip2_client: Successfully imported the keys from external key server: xxx.xxx.xxx.xxx:5696` In der Ausgabe wurde die EKM-Konfiguration erfolgreich wiederhergestellt.

  Der Prozess versucht, die entsprechenden Dateien vom Partnerknoten wiederherzustellen und startet den Knoten neu. Fahren Sie mit dem nächsten Schritt fort.

- Wenn der Schlüssel nicht erfolgreich wiederhergestellt werden kann, wird das System angehalten und zeigt an, dass der Schlüssel nicht wiederhergestellt werden konnte. Die Fehler- und Warnmeldungen werden angezeigt. Sie müssen den Wiederherstellungsprozess erneut ausführen:

```
boot_recovery -partner
```

Zeigt ein Beispiel für Fehler und Warnmeldungen bei der Schlüsselwiederherstellung an

```
ERROR: kmip_init: halting this system with encrypted mroot...
WARNING: kmip_init: authentication keys might not be
available.
*********************************************************
*                 A T T E N T I O N                     *
*                                                       *
*       System cannot connect to key managers.          *
*                                                       *
*********************************************************
ERROR: kmip_init: halting this system with encrypted mroot...
.
Terminated

Uptime: 11m32s
System halting...

LOADER-B>
```

b. Wenn der Node neu gebootet wird, überprüfen Sie, ob die Boot-Medien erfolgreich wiederhergestellt wurden, indem Sie bestätigen, dass das System wieder online und funktionsfähig ist.

c. Wiederherstellung des normalen Betriebs des Controllers durch Zurückgeben des Speichers:

```
storage failover giveback -ofnode impaired_node_name
```

i. Wenn die HA-Verbindungslinks getrennt wurden, aktivieren Sie sie erneut, um die automatische Rückgabe fortzusetzen:

```
system ha interconnect link on -node healthy-node -link 0
```

```
system ha interconnect link on -node healthy-node -link 1
```

6. Wenn die automatische Rückübertragung deaktiviert wurde, aktivieren Sie sie erneut:

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

7. Wenn AutoSupport aktiviert ist, stellen Sie die automatische Fallerstellung wieder her:

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

Was kommt als Nächstes?

Nachdem Sie das ONTAP -Image wiederhergestellt haben und der Knoten aktiv ist und Daten bereitstellt,

müssen Sie"Geben Sie das fehlerhafte Teil an NetApp zurück" .

Senden Sie das ausgefallene Teil an NetApp zurück – AFX 1K

Wenn eine Komponente in Ihrem AFX 1K-Speichersystem ausfällt, senden Sie das ausgefallene Teil an NetApp zurück. Siehe die "Rückgabe und Austausch von Teilen" Seite für weitere Informationen.