



# **Bootmedium – automatisierte Wiederherstellung**

Install and maintain

NetApp

February 13, 2026

# Inhalt

Bootmedium – automatisierte Wiederherstellung . . . . .	1
Automatisierter Wiederherstellungs-Workflow für Bootmedien – ASA A800 . . . . .	1
Voraussetzungen für die automatische Wiederherstellung von Bootmedien – ASA A800 . . . . .	1
Fahren Sie den Controller für die automatische Wiederherstellung des Bootmediums herunter - ASA A800 . . . . .	2
Ersetzen Sie das Bootmedium für die automatische Boot-Wiederherstellung - ASA A800 . . . . .	4
Automatisierte Boot-Medienwiederherstellung vom Partnerknoten - ASA A800 . . . . .	8
Senden Sie das fehlerhafte Bootmedium an NetApp - ASA A800 zurück . . . . .	15

# Bootmedium – automatisierte Wiederherstellung

## Automatisierter Wiederherstellungs-Workflow für Bootmedien – ASA A800

Bei der automatischen Wiederherstellung des Boot-Images erkennt und wählt das System automatisch die entsprechende Boot-Menüoption aus. Es verwendet das Boot-Image auf dem Partnerknoten, um ONTAP auf dem Ersatz-Bootmedium in Ihrem ASA A800 -System neu zu installieren.

Der automatisierte Boot-Medien-Wiederherstellungsprozess wird nur in ONTAP 9.17.1 und höher unterstützt. Wenn Ihr Speichersystem eine frühere Version von ONTAP verwendet, verwenden Sie die "[manuelle Boot-Wiederherstellung](#)" .

Überprüfen Sie zunächst die Anforderungen für den Austausch, fahren Sie den Controller herunter, ersetzen Sie das Startmedium, lassen Sie das System das Image wiederherstellen und überprüfen Sie die Systemfunktionalität.

**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 Storage-System herunter, wenn Sie die Boot-Medien austauschen müssen.

**3**

**"Ersetzen Sie das Startmedium"**

Entfernen Sie das fehlerhafte Startmedium aus dem Controllermodul 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 für die automatische Wiederherstellung von Bootmedien – ASA A800

Stellen Sie vor dem Austausch des Bootmediums in Ihrem ASA A800 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 der e0S-Port (e0M Wrench) am beeinträchtigten Controller nicht fehlerhaft ist, und die Feststellung, ob Onboard Key Manager (OKM) oder External Key Manager (EKM) aktiviert ist.

Der automatisierte Boot-Medien-Wiederherstellungsprozess wird nur in ONTAP 9.17.1 und höher unterstützt. Wenn Ihr Speichersystem eine frühere Version von ONTAP verwendet, verwenden Sie die "[manuelle Boot-Wiederherstellung](#)".

- Sie müssen die ausgefallene Komponente durch eine FRU-Ersatz-Komponente ersetzen, die dieselbe Kapazität hat wie Sie von NetApp erhalten.
- Stellen Sie sicher, dass der e0M-Anschluss (Schraubenschlüssel) am beeinträchtigten Controller angeschlossen und nicht fehlerhaft ist.

Der e0M-Port wird während des automatisierten Boot-Wiederherstellungsprozesses zur Kommunikation zwischen den beiden Controllern verwendet.

- Für OKM benötigen Sie die clusterweite Passphrase und auch 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.
- Es ist wichtig, die Befehle auf den richtigen Controller anzuwenden, wenn Sie das beschädigte Startmedium ersetzen:
  - Der *beschädigte Controller* ist der Controller, an dem Sie Wartungsarbeiten durchführen.
  - Der *gesunde Controller* ist der HA-Partner des beeinträchtigten Controllers.

#### Wie es weiter geht

Nachdem Sie die Anforderungen für die Startmedien überprüft haben, können Sie "[Fahren Sie den Controller herunter](#)".

## Fahren Sie den Controller für die automatische Wiederherstellung des Bootmediums herunter - ASA A800

Fahren Sie den beeinträchtigten Controller in Ihrem ASA A800 Speichersystem herunter, um Datenverlust zu verhindern und die Systemstabilität während des automatischen Wiederherstellungsprozesses des Bootmediums aufrechtzuerhalten.

Der automatisierte Boot-Medien-Wiederherstellungsprozess wird nur in ONTAP 9.17.1 und höher unterstützt. Wenn Ihr Speichersystem eine frühere Version von ONTAP verwendet, verwenden Sie die "[manuelle Boot-Wiederherstellung](#)".

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 überprüfen 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, unterdrücken Sie die automatische Erstellung eines Cases durch Aufrufen einer AutoSupport Meldung:

```
system node autosupport invoke -node * -type all -message MAINT=<# of hours>
```

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. Automatische Rückgabe deaktivieren:

- a. Geben Sie den folgenden Befehl von der Konsole des fehlerfreien Controllers ein:

```
storage failover modify -node impaired_node_name -auto-giveback false
```

- b. Eingeben `y` wenn die Eingabeaufforderung *Möchten Sie die automatische Rückgabe deaktivieren?* angezeigt wird

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 <code>y</code> 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> -halt true</code>  Der Parameter <code>-stop true</code> führt Sie zur Loader-Eingabeaufforderung.

## Wie es weiter geht

Nach dem Herunterfahren des außer Betrieb genommenen Controllers, Sie "["Ersetzen Sie das Startmedium"](#)".

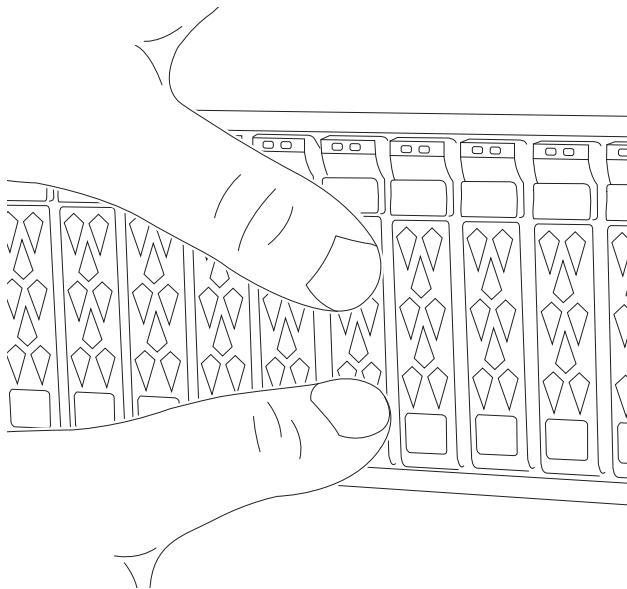
# Ersetzen Sie das Bootmedium für die automatische Boot-Wiederherstellung - ASA A800

Das Bootmedium in Ihrem ASA A800 -System speichert wichtige Firmware- und Konfigurationsdaten. Der Austauschvorgang umfasst das Entfernen und Öffnen des Controllermoduls, das Entfernen des beschädigten Startmediums, das Installieren des Ersatz-Startmediums im Controllermodul und die anschließende Neuinstallation des Controllermoduls.

Der automatisierte Boot-Medien-Wiederherstellungsprozess wird nur in ONTAP 9.17.1 und höher unterstützt. Wenn Ihr Speichersystem eine frühere Version von ONTAP verwendet, verwenden Sie die "[manuelle Boot-Wiederherstellung](#)".

Das Startmedium befindet sich im Controllermodul unter dem Luftkanal und ist zugänglich, indem das Controllermodul aus dem System entfernt wird.

1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
2. Stellen Sie sicher, dass alle Laufwerke im Gehäuse fest auf der Mittelplatine sitzen, indem Sie mit den Daumen auf die einzelnen Laufwerke drücken, bis Sie einen positiven Anschlag spüren.

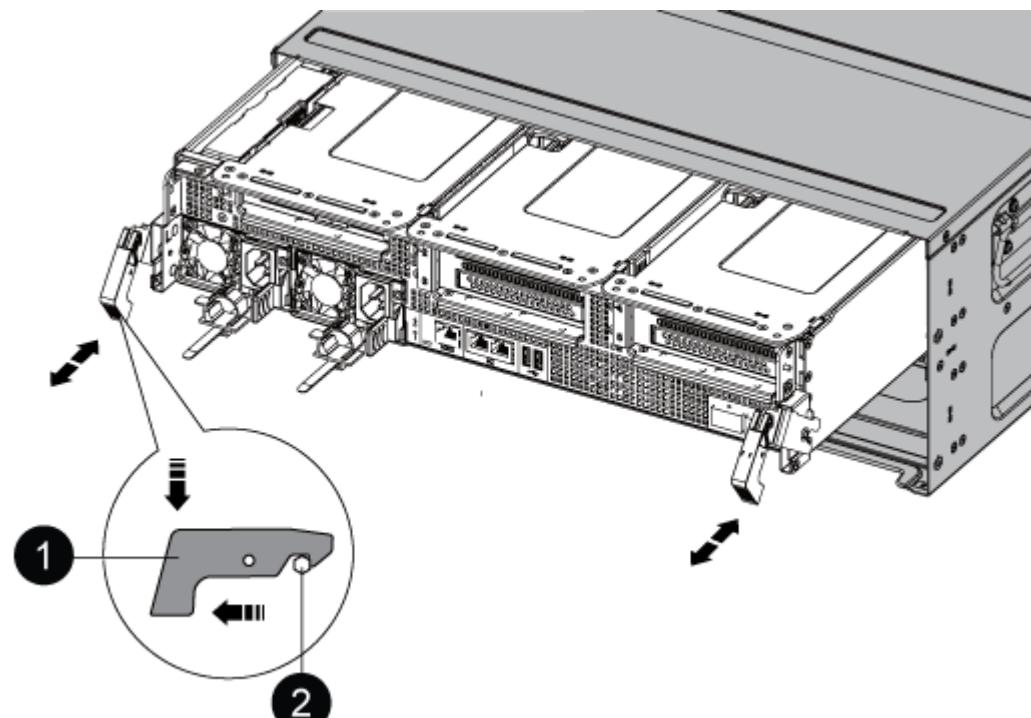


3. Trennen Sie die Netzteile des Controller-Moduls von der Quelle.
4. Lösen Sie die Netzkabelhalter, und ziehen Sie anschließend die Kabel von den Netzteilen ab.
5. Lösen Sie den Haken- und Schlaufenriemen, mit dem die Kabel an das Kabelmanagement-Gerät gebunden sind, und ziehen Sie dann die Systemkabel und SFP- und QSFP-Module (falls erforderlich) vom Controller-Modul ab, um zu verfolgen, wo die Kabel angeschlossen waren.

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

6. Entfernen Sie das Kabelführungs-Gerät aus dem Controller-Modul und legen Sie es beiseite.
7. Drücken Sie beide Verriegelungsriegel nach unten, und drehen Sie dann beide Verriegelungen gleichzeitig nach unten.

Das Controller-Modul wird leicht aus dem Chassis entfernt.



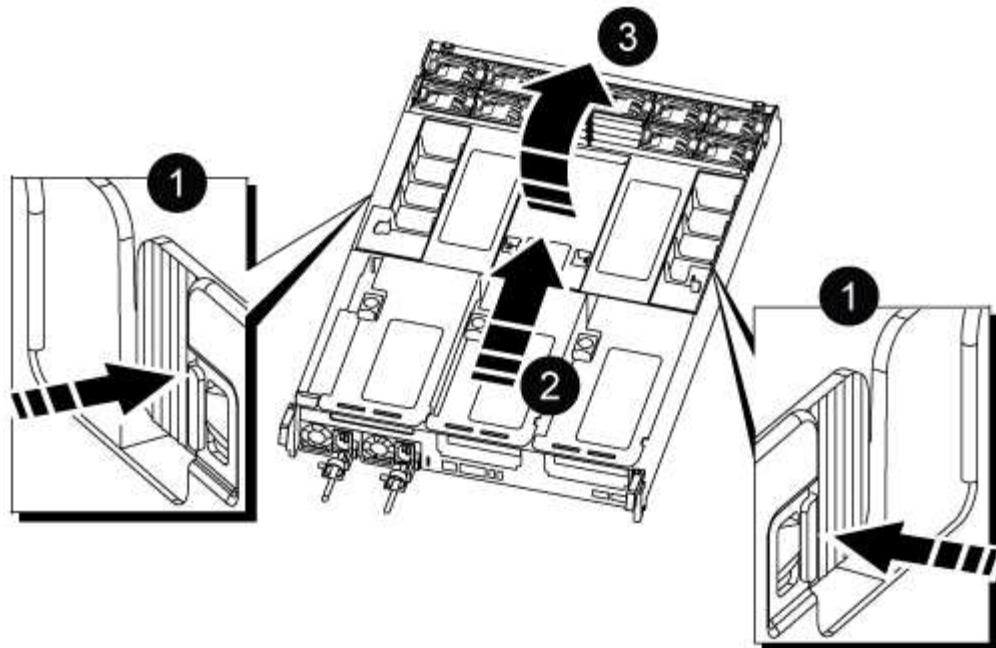
1	Verriegelungsverschluss
2	Sicherungsstift

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

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

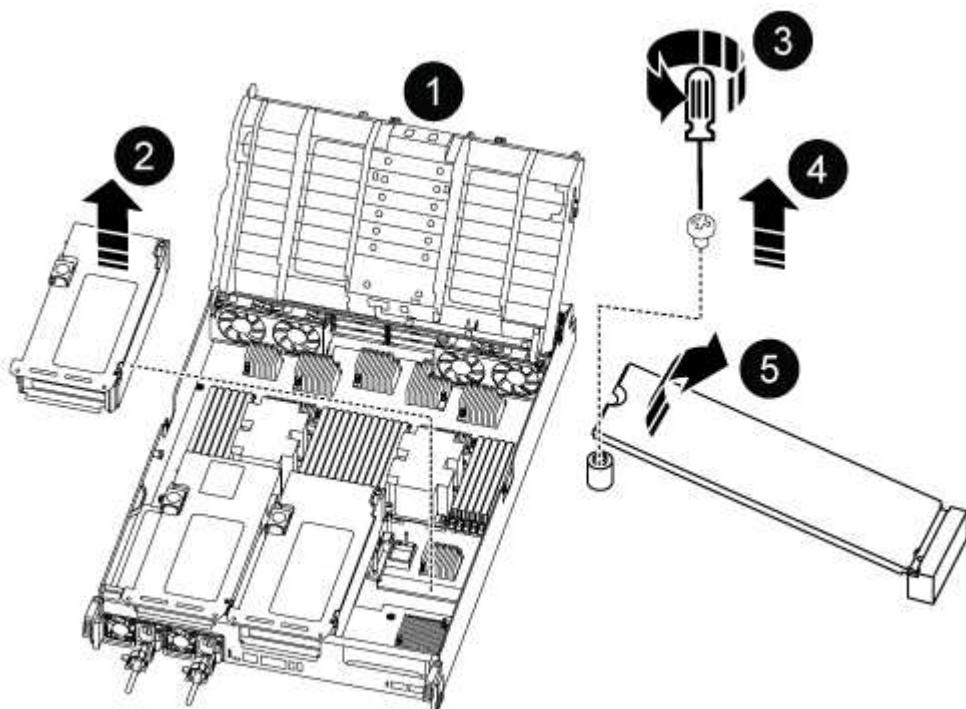
9. Das Steuermodul auf eine stabile, flache Oberfläche legen und den Luftkanal öffnen:

- Drücken Sie die Verriegelungslaschen an den Seiten des Luftkanals in Richtung der Mitte des Controller-Moduls.
- Schieben Sie den Luftkanal in Richtung der Lüftermodule, und drehen Sie ihn dann nach oben in die vollständig geöffnete Position.



1	Verriegelungsklammern für Luftkanäle
2	Schieben Sie den Luftkanal in Richtung Lüftermodule
3	Luftkanal in Richtung Lüftermodule drehen

10. Suchen Sie das Startmedium im Controllermodul und ersetzen Sie es:



1	Luftkanal
2	Riser 3
3	Kreuzschlitzschraubendreher #1
4	Schraube für Boot-Medien
5	Boot-Medien

- Entfernen Sie mit einem #1 Kreuzschlitzschraubendreher die Schraube, mit der das Bootmedium befestigt ist, und setzen Sie die Schraube an einem sicheren Ort beiseite.
- Fassen Sie die Seiten des Startmediums an, drehen Sie die Startmedien vorsichtig nach oben, ziehen Sie dann die Startmedien gerade aus dem Sockel und legen Sie sie beiseite.

11. Installieren Sie die Ersatzstartmedien in das Controller-Modul:

- Richten Sie die Kanten der Startmedien am Buchsengehäuse aus, und schieben Sie sie vorsichtig in die Buchse.
- Drehen Sie das Startmedium nach unten zur Hauptplatine.
- Befestigen Sie das Bootmedium mit der Boot-Medienschraube am Motherboard.

Ziehen Sie die Schraube nicht zu fest, oder beschädigen Sie die Bootsmedien möglicherweise nicht.

12. Setzen Sie den Riser wieder in das Controller-Modul ein.

13. Luftkanal schließen:

- Den Luftkanal nach unten drehen.
- Schieben Sie den Luftkanal in Richtung der Steigleitungen, bis er einrastet.

14. Installieren Sie das Controller-Modul:

- Richten Sie das Ende des Controllermoduls an der Öffnung im Gehäuse aus und schieben Sie das Controllermodul dann vorsichtig zur Hälfte in das System hinein.
- Verkabeln Sie das Controllermodul neu, drücken Sie den Nockengriff fest, um das Controllermodul vollständig einzusetzen, drücken Sie den Nockengriff in die geschlossene Position und ziehen Sie dann die Rändelschraube fest.

Das Controllermodul beginnt mit dem Booten und stoppt bei der LOADER-Eingabeaufforderung.

### Wie es weiter geht

Nach dem physischen Austausch der gestörten Startmedien, ["Stellen Sie das ONTAP-Image vom Partner-Node wieder her"](#).

# Automatisierte Boot-Medienwiederherstellung vom Partnerknoten - ASA A800

Nach der Installation des neuen Bootmediums in Ihrem ASA A800 -System können Sie den automatisierten Bootmedium-Wiederherstellungsprozess starten, um die Konfiguration vom Partnerknoten wiederherzustellen. Während des Wiederherstellungsprozesses prüft das System, ob die Verschlüsselung aktiviert ist und ermittelt den verwendeten Schlüsselverschlüsselungstyp. Wenn die Schlüsselverschlüsselung aktiviert ist, führt Sie das System durch die entsprechenden Schritte zur Wiederherstellung.

Der automatisierte Boot-Medien-Wiederherstellungsprozess wird nur in ONTAP 9.17.1 und höher unterstützt. Wenn Ihr Speichersystem eine frühere Version von ONTAP verwendet, verwenden Sie die "[manuelle Boot-Wiederherstellung](#)".

## Bevor Sie beginnen

- Ermitteln Sie Ihren Schlüsselmanagertyp:
  - Onboard Key Manager (OKM): Erfordert eine clusterweite Passphrase und Sicherungsdaten.
  - Externer Schlüsselmanager (EKM): Benötigt die folgenden Dateien vom Partnerknoten:
    - /cfcard/kmip/servers.cfg
    - /cfcard/kmip/certs/client.crt
    - /cfcard/kmip/certs/client.key
    - /cfcard/kmip/certs/CA.pem

## Schritte

1. Starten Sie an der Eingabeaufforderung LOADER den Wiederherstellungsprozess des Bootmediums:

```
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 die Verschlüsselung und zeigt eine der folgenden Meldungen an:

Wenn diese Meldung angezeigt wird...	Tun Sie das...
key manager is not configured. Exiting.	<p>Auf dem System ist keine Verschlüsselung installiert.</p> <ol style="list-style-type: none"> <li data-bbox="641 259 1383 291">a. Warten Sie, bis die Anmeldeaufforderung angezeigt wird.</li> <li data-bbox="641 312 1473 375">b. Melden Sie sich am Knoten an und geben Sie den Speicherplatz zurück:</li> </ol> <pre data-bbox="674 418 1237 481">storage failover giveback -ofnode impaired_node_name</pre> <ol style="list-style-type: none"> <li data-bbox="641 513 1481 576">c. Gehe zu <a href="#">automatische Rückvergütung wieder aktivieren</a> wenn es deaktiviert war.</li> </ol>
key manager is configured.	Die Verschlüsselung ist installiert. Gehe zu <a href="#">Wiederherstellung des Schlüsselmanagers</a> .



Kann das System die Konfiguration des Schlüsselmanagers nicht identifizieren, wird eine Fehlermeldung angezeigt, und Sie werden aufgefordert zu bestätigen, ob ein Schlüsselmanager konfiguriert ist und um welchen Typ es sich handelt (intern oder extern). Beantworten Sie die Anweisungen, um fortzufahren.

4. Stellen Sie den Schlüsselmanager mithilfe der für Ihre Konfiguration geeigneten Vorgehensweise wieder her:

## Onboard Key Manager (OKM)

Das System zeigt die folgende Meldung an und beginnt mit der Ausführung von BootMenu Option 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. Eingeben **y** Wenn Sie dazu aufgefordert werden, zu bestätigen, dass Sie den OKM-Wiederherstellungsprozess starten möchten, folgen Sie dieser Aufforderung.
- b. Geben Sie bei Aufforderung die Passphrase für die Onboard-Schlüsselverwaltung ein.
- c. Geben Sie die Passphrase bei Aufforderung erneut ein, um sie zu bestätigen.
- d. Geben Sie die Sicherungsdaten für den Onboard Key Manager ein, wenn Sie dazu aufgefordert werden.

### 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 BACKUP-----
```

- e. Überwachen Sie den Wiederherstellungsprozess, während die entsprechenden Dateien vom Partnerknoten wiederhergestellt werden.

Nach Abschluss des Wiederherstellungsprozesses wird der Knoten neu gestartet. Die folgenden Meldungen deuten 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.
```

- f. Nach dem Neustart des Knotens überprüfen Sie, ob das System wieder online und betriebsbereit ist.
- g. Stellen Sie den funktionsbeeinträchtigten Controller wieder in den Normalbetrieb ein, indem Sie den Speicher zurückgeben:

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

- h. Sobald der Partnerknoten vollständig betriebsbereit ist und Daten bereitstellt, synchronisieren Sie die OKM-Schlüssel im gesamten Cluster:

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

Gehe zu [automatische Rückvergütung wieder aktivieren](#) wenn es deaktiviert war.

### Externer Schlüsselmanager (EKM)

Das System zeigt die folgende Meldung an und beginnt mit der Ausführung von BootMenu Option 11:

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

- a. Geben Sie die EKM-Konfigurationseinstellungen ein, wenn Sie dazu aufgefordert werden:
  - i. Geben Sie den Inhalt des Clientzertifikats aus dem /cfcard/kmip/certs/client.crt Datei:

**Zeigt ein Beispiel für den Inhalt des Clientzertifikats an**

```
-----BEGIN CERTIFICATE-----  
<certificate_value>  
-----END CERTIFICATE-----
```

- ii. Geben Sie den Inhalt der Client-Schlüsseldatei aus dem/der /cfcard/kmip/certs/client.key Datei:

### Beispiel für den Inhalt der Schlüsseldatei des Clients anzeigen

```
-----BEGIN RSA PRIVATE KEY-----  
<key_value>  
-----END RSA PRIVATE KEY-----
```

- iii. Geben Sie den Inhalt der CA-Serverdatei(en) des KMIP-Servers ein.

/cfcard/kmip/certs/CA.pem Datei:

### Beispiel für Dateiinhalte des KMIP-Servers anzeigen

```
-----BEGIN CERTIFICATE-----  
<KMIP_certificate_CA_value>  
-----END CERTIFICATE-----
```

- iv. Geben Sie den Inhalt der Serverkonfigurationsdatei aus dem folgenden Verzeichnis ein:

/cfcard/kmip/servers.cfg Datei:

### Beispiel für den Inhalt der Serverkonfigurationsdatei anzeigen

```
xxx.xxx.xxx.xxx:5696.host=xxx.xxx.xxx.xxx  
xxx.xxx.xxx.xxx:5696.port=5696  
xxx.xxx.xxx.xxx:5696.trusted_file=/cfcard/kmip/certs/CA.pem  
xxx.xxx.xxx.xxx:5696.protocol=KMIP1_4  
1xxx.xxx.xxx.xxx:5696.timeout=25  
xxx.xxx.xxx.xxx:5696.nbio=1  
xxx.xxx.xxx.xxx:5696.cert_file=/cfcard/kmip/certs/client.crt  
xxx.xxx.xxx.xxx:5696.key_file=/cfcard/kmip/certs/client.key  
xxx.xxx.xxx.xxx:5696.ciphers="TLSv1.2:kRSA:!CAMELLIA:!IDEA:  
!RC2:!RC4:!SEED:!eNULL:!aNULL"  
xxx.xxx.xxx.xxx:5696.verify=true  
xxx.xxx.xxx.xxx:5696.netapp_keystore_uuid=<id_value>
```

- v. Geben Sie bei Aufforderung die ONTAP Cluster-UUID des Partnerknotens ein. Sie können die Cluster-UUID vom Partnerknoten aus mit folgendem Befehl überprüfen: `cluster identify show` Befehl.

### Beispiel für die ONTAP Cluster UUID-Eingabeaufforderung anzeigen

```
Notice: bootarg.mgwd.cluster_uuid is not set or is empty.  
Do you know the ONTAP Cluster UUID? {y/n} y  
Enter the ONTAP Cluster UUID: <cluster_uuid_value>  
  
System is ready to utilize external key manager(s).
```

- vi. Geben Sie bei Aufforderung die temporäre Netzwerkschnittstelle und die Einstellungen für den Knoten ein:

- Die IP-Adresse für den Port
- Die Netzmaske für den Port
- Die IP-Adresse des Standard-Gateways

### Beispiel für Eingabeaufforderungen für temporäre Netzwerkeinstellungen anzeigen

```
In order to recover key information, a temporary network  
interface needs to be  
configured.  
  
Select the network port you want to use (for example,  
'e0a')  
e0M  
  
Enter the IP address for port : xxx.xxx.xxx.xxx  
Enter the netmask for port : xxx.xxx.xxx.xxx  
Enter IP address of default gateway: xxx.xxx.xxx.xxx  
Trying to recover keys from key servers....  
[discover_versions]  
[status=SUCCESS reason= message=]
```

- b. Überprüfen Sie den Status der Schlüsselwiederherstellung:

- Wenn Sie sehen `kmip2_client: Successfully imported the keys from external key server: xxx.xxx.xxx.xxx:5696` Im Ergebnis wird angezeigt, dass die EKM-Konfiguration erfolgreich wiederhergestellt wurde. Der Prozess stellt die entsprechenden Dateien vom Partnerknoten wieder her und startet den Knoten neu. Fahren Sie mit dem nächsten Schritt fort.
- Wenn der Schlüssel nicht erfolgreich wiederhergestellt werden kann, stoppt das System und zeigt Fehler- und Warnmeldungen an. Führen Sie den Wiederherstellungsprozess über die LOADER-Eingabeaufforderung erneut aus: `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>
```

- c. Nach dem Neustart des Knotens überprüfen Sie, ob das System wieder online und betriebsbereit ist.
- d. Wiederherstellung des normalen Betriebs des Controllers durch Zurückgeben des Speichers:

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

Gehe zu [automatische Rückvergütung wieder aktivieren](#) wenn es deaktiviert war.

5. Falls die automatische Rückgabe deaktiviert war, aktivieren Sie sie wieder:

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

6. Wenn AutoSupport aktiviert ist, stellen Sie die automatische Fehlerstellung wieder her:

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

#### Wie es weiter geht

Nachdem Sie das ONTAP-Image wiederhergestellt haben und der Node ausgeführt wurde und Daten bereitstellt, können Sie ["Geben Sie das fehlerhafte Teil an NetApp zurück"](#).

## **Senden Sie das fehlerhafte Bootmedium an NetApp - ASA A800 zurück**

Wenn eine Komponente in Ihrem ASA A800 System ausfällt, senden Sie das ausgefallene Teil an NetApp zurück. Siehe die "["Rückgabe und Austausch von Teilen"](#)" Seite für weitere Informationen.

## Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers 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 BESCHRÄNKKT 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, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKKT 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 VERTRÄGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER 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.