



# **Boot-Medien – manuelle Wiederherstellung**

## **Install and maintain**

NetApp  
December 18, 2024

# Inhalt

- Boot-Medien – manuelle Wiederherstellung ..... 1
  - Übersicht über die manuelle Wiederherstellung der Startmedien - ASAA1K ..... 1
  - Workflow für den Austausch von Startmedien – ASAA1K ..... 1
  - Voraussetzungen für den Austausch von Startmedien – ASAA1K ..... 2
  - Unterstützung und Status von Verschlüsselungsschlüsseln prüfen – ASAA1K ..... 2
  - Schalten Sie den außer Betrieb genommenen Controller - ASAA1K aus ..... 7
  - Ersetzen Sie das Startmedium – ASAA1K ..... 8
  - Starten Sie das Wiederherstellungs-Image - ASAA1K ..... 11
  - Wiederherstellung der Verschlüsselung – ASAA1K ..... 13
  - Senden Sie das fehlerhafte Teil an NetApp - ASAA1K zurück ..... 23

# Boot-Medien – manuelle Wiederherstellung

## Übersicht über die manuelle Wiederherstellung der Startmedien - ASA A1K

Sie können fehlerhafte Startmedien manuell durch Verwendung eines USB-Moduls für das Startabbild ersetzen.

Beim manuellen Ersetzen von Startmedien wird das ONTAP-Image von der NetApp-Support-Website heruntergeladen, das Image auf ein USB-Laufwerk übertragen, auf das Startmedium heruntergeladen und manuell durch die Optionen des Startmenüs geleitet, um das ONTAP-Image auf dem Ersatz-Startmedium zu installieren.

## Workflow für den Austausch von Startmedien – ASA A1K

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 aktiviert oder 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 aus dem Systemverwaltungsmodul, 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.

## Voraussetzungen für den Austausch von Startmedien – ASA A1K

Überprüfen Sie vor dem Austauschen des Startmediums die folgenden 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` Datei:
- 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-Austauschkomponente ersetzen, die Sie NetApp erhalten haben.
- Es ist wichtig, dass Sie die Befehle in diesen Schritten auf dem richtigen Controller anwenden:
  - Der Controller *Impaired* ist der Controller, an dem Sie Wartungsarbeiten durchführen.
  - Der *Healthy* Controller ist der HA-Partner des beeinträchtigten Controllers.

## Unterstützung und Status von Verschlüsselungsschlüsseln prüfen – ASA A1K

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

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 " <a href="#">Schalten Sie den außer Betrieb genommenen Controller aus</a> ".
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 "<a href="#">NetApp Support</a>".</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 "<a href="#">Schalten Sie den außer Betrieb genommenen Controller aus</a>".</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"><li>Wechseln Sie in den erweiterten Modus, indem <code>set -priv advanced</code> Sie aufrufen und dann bei Aufforderung eingeben <code>Y</code>.</li><li>Geben Sie den folgenden Befehl ein, um die Informationen zum Verschlüsselungsmanagement anzuzeigen:  <pre>security key-manager onboard show-backup</pre></li><li>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.</li><li>Sie können den außer Betrieb genommenen Controller sicher herunterfahren. Gehen Sie zu "<a href="#">Schalten Sie den außer Betrieb genommenen Controller aus</a>".</li></ol>

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 <a href="#">"NetApp Support"</a>.</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 <a href="#">"Schalten Sie den außer Betrieb genommenen Controller aus"</a>.</p>

## Schalten Sie den außer Betrieb genommenen Controller - ASA A1K aus

Sie müssen das Herunterfahren des außer Betrieb genommenen Controllers abschließen. 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:

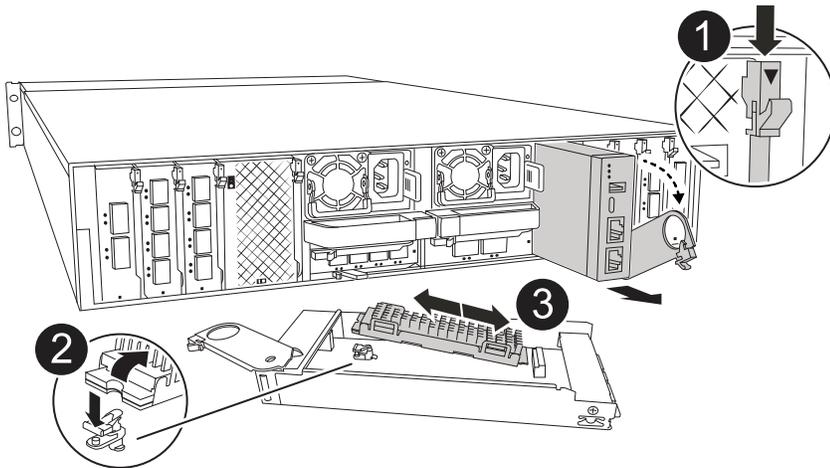
Wenn der eingeschränkte Controller angezeigt wird...	Dann...
Die LOADER-Eingabeaufforderung	Fahren Sie mit dem nächsten Schritt fort.
Warten auf Giveback...	Drücken Sie Strg-C, und antworten Sie dann <code>y</code> Wenn Sie dazu aufgefordert werden.
Eingabeaufforderung für das System oder Passwort	Übernehmen oder stoppen Sie den beeinträchtigten Regler von der gesunden Steuerung: <code>storage failover takeover -ofnode <i>impaired_node_name</i></code>  Wenn der Regler „beeinträchtigt“ auf Zurückgeben wartet... anzeigt, drücken Sie Strg-C, und antworten Sie dann <code>y</code> .

## Ersetzen Sie das Startmedium – ASA A1K

Sie müssen das Controller-Modul trennen, das System-Management-Modul von der Rückseite des Systems entfernen, das gestörte Startmedium entfernen und das Ersatz-Startmedium im System-Management-Modul installieren.

## Schritt 1: Ersetzen Sie die Startmedien

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

1. Wenn Sie nicht bereits geerdet sind, sollten Sie sich richtig Erden.
2. Ziehen Sie die Netzteilkabel von den Netzteilen vom Controller ab.



Wenn Ihr Speichersystem über Gleichstromnetzteile verfügt, trennen Sie den Stromkabelblock von den Netzteilen.

- a. Entfernen Sie alle Kabel, die am System Management-Modul angeschlossen sind. Stellen Sie sicher, dass Sie den Ort kennzeichnen, an dem die Kabel angeschlossen wurden, damit Sie sie bei der Neuinstallation des Moduls an die richtigen Anschlüsse anschließen können.
  - 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.
3. 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.

4. 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.
5. 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.
6. Drehen Sie das Kabelführungs-Fach bis in die geschlossene Position.
  - a. System-Management-Modul erneut verwenden.

## Schritt 2: Übertragen Sie das ONTAP-Image auf das Boot-Medium

Das von Ihnen installierte Ersatzstartmedium ist ohne ein ONTAP-Image. Sie können das ONTAP-Image auf das Ersatz-Startmedium übertragen, indem Sie das entsprechende ONTAP-Service-Image vom auf ein USB-Flash-Laufwerk und anschließend auf das Ersatz-Startmedium herunterladen "[NetApp Support Website](#)".

### Bevor Sie beginnen

- Sie müssen über ein leeres USB-Flash-Laufwerk verfügen, das mit FAT32 formatiert ist und mindestens 4 GB Kapazität hat.
- Laden Sie eine Kopie der gleichen Bildversion von ONTAP herunter, die den Betrieb des beeinträchtigten Controllers enthält. Sie können das entsprechende Bild im Abschnitt „Downloads“ auf der NetApp Support-Website herunterladen. Verwenden Sie den `version -v` Befehl, um anzuzeigen, ob Ihre Version von ONTAP NVE unterstützt. Wenn die Befehlsausgabe angezeigt wird `<10no- DARE>`, unterstützt Ihre Version von ONTAP NVE nicht.
  - Wenn NVE von Ihrer Version von ONTAP 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.
- Wenn es sich bei Ihrem System um ein HA-Paar handelt, müssen Sie über eine Netzwerkverbindung zwischen den Node-Management-Ports der Controller verfügen (normalerweise die E0M Schnittstellen).

### 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. Stecken Sie das USB-Flash-Laufwerk in den USB-Steckplatz des Systemmanagementmoduls.

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

3. 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.

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 Hilfe `ifconfig` an der Firmware-Eingabeaufforderung für Details eingeben.

## Starten Sie das Wiederherstellungs-Image - ASA A1K

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 – ASA A1K

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"><b>Beispiel für ein Startmenü anzeigen</b></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="683 411 971 449">(1) Normal Boot.</li><li data-bbox="683 453 1133 491">(2) Boot without /etc/rc.</li><li data-bbox="683 495 1045 533">(3) Change password.</li><li data-bbox="683 537 1370 606">(4) Clean configuration and initialize all disks.</li><li data-bbox="683 611 1154 648">(5) Maintenance mode boot.</li><li data-bbox="683 653 1328 690">(6) Update flash from backup config.</li><li data-bbox="683 695 1240 732">(7) Install new software first.</li><li data-bbox="683 737 976 774">(8) Reboot node.</li><li data-bbox="683 779 1192 848">(9) Configure Advanced Drive Partitioning.</li><li data-bbox="683 852 1333 921">(10) Set Onboard Key Manager recovery secrets.</li><li data-bbox="683 926 1317 995">(11) Configure node for external key management.</li></ul><p data-bbox="683 1010 1029 1047">Selection (1-11)? 10</p></div>

ONTAP-Version	Wählen Sie diese Option aus
ONTAP 9.7 und frühere Versionen	<p>Wählen Sie die ausgeblendete Option aus recover_onboard_keymanager</p> <p><b>Beispiel für ein Startmenü anzeigen</b></p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <pre> 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

Enter the backup data:

```
-----BEGIN BACKUP-----  
01234567890123456789012345678901234567890123456789012345678901234567890123  
12345678901234567890123456789012345678901234567890123456789012345678901234  
23456789012345678901234567890123456789012345678901234567890123456789012345  
34567890123456789012345678901234567890123456789012345678901234567890123456  
45678901234567890123456789012345678901234567890123456789012345678901234567  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
01234567890123456789012345678901234567890123456789012345678901234567890123  
12345678901234567890123456789012345678901234567890123456789012345678901234  
23456789012345678901234567890123456789012345678901234567890123456789012345  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
-----END BACKUP-----
```

b. Drücken Sie am Ende des Eingangs zweimal die Eingabetaste.

Die Wiederherstellung ist abgeschlossen.

## 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 - ASA A1K 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.