Boot-Medien

Install and maintain

NetApp
July 01, 2024

Inhalt

Boot-Medien

Überblick über den Austausch von Boot-Medien – AFF A1K

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

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

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

- 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.

Überprüfen Sie die integrierten Verschlüsselungsschlüssel - AFF A1K

Bevor Sie den beeinträchtigten Controller herunterfahren und den Status der integrierten Verschlüsselungsschlüssel prüfen, müssen Sie den Status des beeinträchtigten Controllers überprüfen, das automatische Giveback deaktivieren und die Version von ONTAP prüfen, die ausgeführt wird.

Wenn Sie über ein Cluster mit mehr als zwei Nodes verfügen, muss es sich im Quorum befinden. Wenn sich das Cluster nicht im Quorum befindet oder ein gesunder Controller FALSE 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".

Prüfen Sie NVE oder NSE auf Systemen mit ONTAP 9.15 und höher

Bevor Sie den beeinträchtigten Controller herunterfahren, müssen Sie überprüfen, ob der Sicherheitsschlüsselmanager aktiviert oder verschlüsselt ist.

Überprüfen Sie die Konfiguration des Sicherheitsschlüsselmanagers

Schritte

1. Determe, wenn Key Manager mit dem Befehl *Security key-Manager keystore show* aktiv ist. Weitere Informationen finden Sie im "Security key-Manager keystore zeigen MAN-Seite"

Möglicherweise haben Sie weitere Schlüsselmanager-Typen. Die Typen sind `KMIP`, `AKV`und `GCP`. Der Prozess zur Bestätigung dieser Typen ist der gleiche wie Bestätigungs `external` - oder `onboard` Schlüsselmanager-Typen.

- Wenn keine Ausgabe angezeigt wird, fahren Sie mit "Schalten Sie den außer Betrieb genommenen Controller aus" fort, um den Knoten „beeinträchtigt“ herunterzufahren.
- Wenn die Ausgabe des Befehls angezeigt wird, verfügt das System über `security key-manager` aktive Ressourcen, und Sie müssen Typ und Status anzeigen `Key Manager` .

2. Zeigen Sie die Informationen für den aktiven `Key Manager` mit dem Befehl *Security key-Manager key query* an.
   - Wenn der `Key Manager` Typ angezeigt wird `external` und die `Restored` Spalte angezeigt `true`wird, ist es sicher, den beeinträchtigten Controller herunterzufahren.
   - Wenn der `Key Manager` Typ angezeigt wird `onboard` und die `Restored` Spalte angezeigt `true`wird, müssen Sie einige zusätzliche Schritte ausführen.
   - Wenn der `Key Manager` Typ angezeigt wird `external` und in der `Restored` Spalte etwas anderes als angezeigt `true`wird, müssen Sie einige zusätzliche Schritte ausführen.
   - Wenn der `Key Manager` Typ angezeigt wird `onboard` und in der `Restored` Spalte etwas anderes als angezeigt `true`wird, müssen Sie einige zusätzliche Schritte ausführen.
3. Wenn der `Key Manager` Typ angezeigt wird `onboard` und die `Restored` Spalte angezeigt `true`wird, sichern Sie die OKM-Informationen manuell:
   a. Geben Sie ein `y` , wenn Sie zum Fortfahren aufgefordert werden: `set -priv advanced`
   b. Geben Sie den Befehl ein, um die Schlüsselverwaltungsinformationen anzuzeigen: *Security key-Manager onboard show-Backup*
   c. Kopieren Sie den Inhalt der Backup-Informationen in eine separate Datei oder eine Protokolldatei. Sie werden es in Disaster-Szenarien benötigen, in denen Sie OKM manuell wiederherstellen müssen.
   d. Sie können den außer Betrieb genommenen Controller sicher herunterfahren.
4. Wenn der `Key Manager` Typ angezeigt wird `onboard` und in der `Restored` Spalte etwas anderes als angezeigt `true`wird:
   a. Geben Sie den Onboard Security Key-Manager Sync-Befehl ein: *Security Key-Manager Onboard Sync*

      Geben Sie an der Eingabeaufforderung die 32-stellige alphanumerische Onboard-Passphrase für die Schlüsselverwaltung ein. Wenn die Passphrase nicht angegeben werden kann, wenden Sie sich an den NetApp-Support. "mysupport.netapp.com"

   b. Überprüfen Sie, ob die `Restored` Spalte für alle Authentifizierungsschlüssel angezeigt wird `true` : `security key-manager key query`
   c. Überprüfen Sie, ob der `Key Manager` Typ , anzeigt `onboard`und sichern Sie die OKM-Informationen manuell.
   d. Geben Sie den Befehl ein, um die Backup-Informationen zum Schlüsselmanagement anzuzeigen: *Security key-Manager onboard show-Backup*
   e. Kopieren Sie den Inhalt der Backup-Informationen in eine separate Datei oder eine Protokolldatei. Sie werden es in Disaster-Szenarien benötigen, in denen Sie OKM manuell wiederherstellen müssen.
   f. Sie können den Controller sicher herunterfahren.

5. Wenn der `Key Manager` Typ angezeigt wird `external` und in der `Restored` Spalte etwas anderes als angezeigt `true`wird:

   a. Stellen Sie die Authentifizierungsschlüssel für das externe Verschlüsselungsmanagement auf allen Nodes im Cluster wieder her: `security key-manager external restore`

      Wenn der Befehl fehlschlägt, wenden Sie sich an den NetApp-Support unter "mysupport.netapp.com".

   b. Vergewissern Sie sich, dass die `Restored` Spalte für alle Authentifizierungsschlüssel angezeigt wird `true` : *Security key-Manager key query*

   c. Sie können den außer Betrieb genommenen Controller sicher herunterfahren.

Schalten Sie den außer Betrieb genommenen Controller - AFF A1K aus

Nach Abschluss der NVE oder NSE-Aufgaben müssen Sie den Shutdown des beeinträchtigten Controllers durchführen. Fahren Sie den Controller mit eingeschränkter Konfiguration herunter oder übernehmen Sie ihn entsprechend.

Option 1: Die meisten Systeme

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 Quorum-Status dieses Node, der Verfügbarkeitsstatus dieses Node und der Betriebsstatus dieses Node angezeigt.

  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 gesunden Controllers: `storage failover modify –node local -auto-giveback false`

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

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

Wenn der eingeschränkte Controller angezeigt wird…	Dann…
Die LOADER-Eingabeaufforderung	Fahren Sie mit dem nächsten Schritt fort.
Warten auf Giveback…	Drücken Sie Strg-C, und antworten Sie dann `y` Wenn Sie dazu aufgefordert werden.

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

Option 2: Controller befindet sich in einem MetroCluster

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

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

Schritte

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

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

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

Wenn der eingeschränkte Controller angezeigt wird…	Dann…
Die LOADER-Eingabeaufforderung	Fahren Sie mit dem nächsten Schritt fort.
Warten auf Giveback…	Drücken Sie Strg-C, und antworten Sie dann `y` Wenn Sie dazu aufgefordert werden.

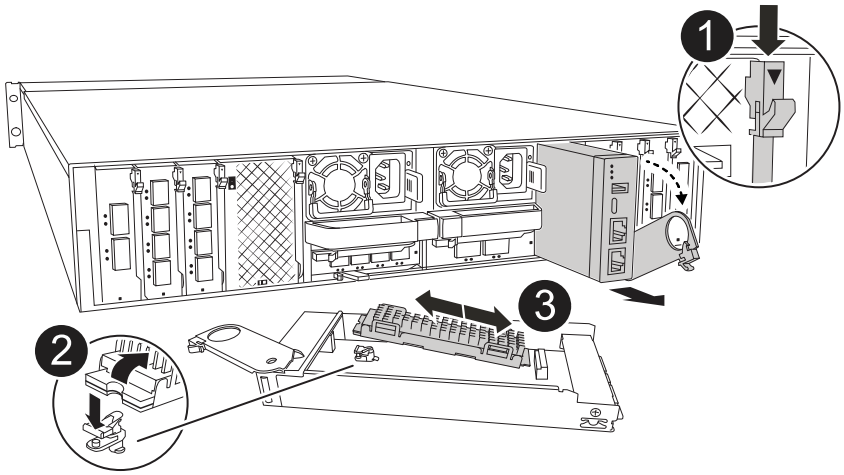
Wenn der eingeschränkte Controller angezeigt wird…	Dann…
Eingabeaufforderung des Systems oder Passwort (Systempasswort eingeben)	Übernehmen oder stoppen Sie den beeinträchtigten Regler von der gesunden Steuerung: `storage failover takeover -ofnode` *`impaired_node_name`* Wenn der Regler „beeinträchtigt“ auf Zurückgeben wartet… anzeigt, drücken Sie Strg-C, und antworten Sie dann `y`.

Ersetzen Sie das Startmedium – AFF A1K

Um das Startmedium zu ersetzen, müssen Sie das Systemverwaltungsmodul von der Rückseite des Systems entfernen, das gestörte Startmedium entfernen, das Ersatzstartmedium in das Systemverwaltungsmodul installieren und das ONTAP-Image von einem USB-Flash-Laufwerk auf das Ersatzstartmedium übertragen.

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. Der Nockenhebel bewegt sich vom Gehäuse weg.

   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, sodass Sie ein ONTAP-Image mithilfe eines USB-Flashlaufwerks übertragen müssen.

Bevor Sie beginnen

- Sie müssen über ein leeres USB-Flash-Laufwerk verfügen, das mit FAT32 formatiert ist und mindestens 4 GB Kapazität hat.
- 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.
- 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.

c. 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 - AFF 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 aus das Wiederherstellungs-Image vom USB-Flashlaufwerk: *Boot_Recovery*

   Das Bild wird vom USB-Flash-Laufwerk heruntergeladen.

2. Wenn Sie dazu aufgefordert werden, geben Sie entweder den Namen des Bilds ein oder akzeptieren Sie das Standardbild, das in den Klammern auf dem Bildschirm angezeigt wird.
3. Stellen Sie das var-Dateisystem wieder her:

Wenn Ihr System…	Dann…
Eine Netzwerkverbindung	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 zum Überschreiben aufgefordert werden `/etc/ssh/ssh_host_ecdsa_key`. c. Setzen Sie auf dem funktionierenden Partner-Controller den beeinträchtigten Controller auf die erweiterte Berechtigungsebene: *Set -Privilege Advanced*. d. Führen Sie auf dem funktionierenden Partner-Controller den Befehl restore Backup aus: *System Node restore-Backup -Node local -target-address Impaired_Node_IP_address*. Wenn Sie eine andere Meldung als eine erfolgreiche Wiederherstellung sehen, wenden Sie sich an "NetApp Support". e. Geben Sie auf dem funktionstüchtigen Partner-Controller den beeinträchtigten Controller auf die Admin-Ebene: *Set -Privilege admin* zurück. f. Drücken Sie auf dem Controller für beeinträchtigte Störungen *y*, wenn angezeigt wird `Was the restore backup procedure successful?`. g. Drücken Sie auf dem Controller für beeinträchtigte Störungen *y*, wenn angezeigt wird `…would you like to use this restored copy now?`. h. Drücken Sie auf dem beeinträchtigten Controller bei Aufforderung *y*, um den beeinträchtigten Controller neu zu starten, und drücken Sie *Ctrl-c* für das Startmenü. i. Wenn das System keine Codierung verwendet, wählen Sie *Option 1 Normal Boot.*, andernfalls gehen Sie zu "Wiederherstellung von Schlüsselmanagern". j. Schließen Sie das Konsolenkabel an den Partner Controller an. k. Geben Sie den Controller mithilfe des Befehls „*Storage Failover Giveback -fromnode local*“ zurück. i. Stellen Sie das automatische Giveback wieder her, wenn Sie es mithilfe des Befehls *Storage Failover modify -Node local -Auto-Giveback true* deaktiviert haben. l. Wenn AutoSupport aktiviert ist, stellen Sie die automatische Fallerstellung mithilfe des Befehls *System Node AutoSupport Invoke -Node * -type all -message MAINT=END* wieder her.
Keine Netzwerkverbindung	Kontakt "NetApp Support".

Wenn Ihr System…	Dann…
Keine Netzwerkverbindung und befindet sich in einer MetroCluster IP-Konfiguration	Kontakt "NetApp Support".

Wiederherstellung der Verschlüsselung – AFF A1K

Die Schritte für Systeme mit aktiviertem Onboard Key Manager (OKM), NetApp Storage Encryption (NSE) oder NetApp Volume Encryption (NVE) müssen über die zu Beginn dieses Verfahrens erfassten Einstellungen ausgeführt werden.

Wenn NSE oder NVE zusammen mit Onboard oder externem Key Manager aktiviert sind, müssen Sie die Einstellungen wiederherstellen, die Sie zu Beginn dieses Verfahrens erfasst haben.

Schritte

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

Option 1: Systeme mit integrierter Key Manager Server-Konfiguration

Stellen Sie die Onboard-Schlüsselmanager-Konfiguration aus dem ONATP-Startmenü wieder her.

Bevor Sie beginnen

Beim Wiederherstellen der OKM-Konfiguration benötigen Sie folgende Informationen:

- 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. Wählen Sie im ONTAP-Startmenü die Option 10:

```
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.
(10) Set Onboard Key Manager recovery secrets.
(11) Configure node for external key management.
Selection (1-11)? _10_
```

2. Bestätigen Sie die Fortsetzung des Prozesses. `This option must be used only in disaster recovery procedures. Are you sure? (y or n): Y`
3. Geben Sie die Cluster-weite Passphrase zweimal ein.

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

```
Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:
```

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

   Drücken Sie am Ende des Eingangs zweimal die Eingabetaste.

```
Enter the backup data:

--------------------------BEGIN BACKUP--------------------------
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
3456789012345678901234567890123456789012345678901234567890123456
4567890123456789012345678901234567890123456789012345678901234567
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
0123456789012345678901234567890123456789012345678901234567890123
1234567890123456789012345678901234567890123456789012345678901234
2345678901234567890123456789012345678901234567890123456789012345
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA

---------------------------END BACKUP---------------------------
```

5. Der Wiederherstellungsprozess wird abgeschlossen.

```
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 ist `Successfully recovered keymanager secrets`. 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.

```
*******************************************************************************
* 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 die Konsole des Controllers angezeigt wird `Waiting for giveback…`

```
(Press Ctrl-C to abort wait)
```

8. Geben Sie vom Partner-Knoten aus die Information zum Partner-Controller ein: *Storage Failover Giveback -fromnode local -only-cfo-Aggregate true*
9. Führen Sie nach dem Start nur mit dem CFO-Aggregat den Befehl *Security Key-Manager onboard sync* aus:
10. Geben Sie die Cluster-weite Passphrase für Onboard Key Manager ein:

```
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.
```

11. Stellen Sie sicher, dass alle Schlüssel synchronisiert sind: *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. GiveBack des Knotens vom Partner: *Storage Failover Giveback -fromnode local*

Option 2: Systeme mit externer Schlüsselmanager-Server-Konfiguration

Stellen Sie die externe Schlüsselmanager-Konfiguration aus dem ONATP-Startmenü wieder her.

Bevor Sie beginnen

Sie benötigen die folgenden Informationen für die Wiederherstellung der Konfiguration des externen Schlüsselmanagers (EKM):

- Sie benötigen 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 Datei /cfcard/kmip/certs/Client.crt von einem anderen Clusterknoten oder dem Clientzertifikat.
- Eine Kopie der Datei /cfcard/kmip/certs/client.key von einem anderen Clusterknoten oder dem Client-Schlüssel.
- Eine Kopie der Datei /cfcard/kmip/certs/CA.pem von einem anderen Clusterknoten oder der KMIP-Server-CA(s).

Schritte

1. Wählen Sie Option 11 aus dem ONTAP-Startmenü.

```
(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
```

2. Wenn Sie dazu aufgefordert werden, bestätigen Sie, dass Sie die erforderlichen Informationen gesammelt haben:
   a. `Do you have a copy of the /cfcard/kmip/certs/client.crt file? {y/n}` *Y*
   b. `Do you have a copy of the /cfcard/kmip/certs/client.key file? {y/n}` *Y*
   c. `Do you have a copy of the /cfcard/kmip/certs/CA.pem file? {y/n}` *Y*
   d. `Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n}` *Y*

      Stattdessen können Sie auch folgende Eingabeaufforderungen ausführen:

   e. `Do you have a copy of the /cfcard/kmip/servers.cfg file? {y/n}` *N*
      i. `Do you know the KMIP server address? {y/n}` *Y*
      ii. `Do you know the KMIP Port? {y/n}` *Y*
3. Geben Sie die Informationen für die folgenden Eingabeaufforderungen an:
   a. `Enter the client certificate (client.crt) file contents:`
   b. `Enter the client key (client.key) file contents:`
   c. `Enter the KMIP server CA(s) (CA.pem) file contents:`
   d. `Enter the server configuration (servers.cfg) file contents:`

```
Example

Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwgY8xCzAJBgNVBAYTAlVT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk5l
MSUbQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxciLJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxpbz3mXF/X/1PC3YOzVNCq5eieek62si
Fp8=
-----END CERTIFICATE-----

Enter the client key (client.key) file contents:
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAoU1eajEG6QC2h2Zih0jEaGVtQUexNeoCFwKPoMSePmjDNtrU
MSB1SlX3VgCuElHk57XPdq6xSbYlbkIb4bAgLztHEmUDOkGmXYAkblQ=
-----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....
kmip_init: configuring ports
Running command '/sbin/ifconfig e0M'
..
..
kmip_init: cmd: ReleaseExtraBSDPort e0M
```

4. Der Wiederherstellungsprozess wird abgeschlossen:

```
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.

```
**********************************************************************
***************
* 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
```

Schließen Sie den Austausch des Startmediums ab

Schließen Sie den Vorgang zum Austauschen von Startmedien nach dem normalen Booten ab, indem Sie die abschließenden Überprüfungen durchführen und den Speicher zurückstellen.

1. Überprüfen Sie die Konsolenausgabe:

Wenn die Konsole angezeigt wird…	**Dann…**
Die Eingabeaufforderung für die Anmeldung	Fahren Sie mit Schritt 6 fort.
Warten auf Giveback…	a. Melden Sie sich beim Partner-Controller an. b. Mit dem Befehl *Storage Failover show* überprüfen Sie, ob der Ziel-Controller für die Rückgabe bereit ist.

2. Verschieben Sie das Konsolenkabel zum Partner-Controller und geben Sie den Ziel-Controller-Storage mit dem Befehl *Storage Failover Giveback -fromnode local -only-cfo-aggregates true* zurück.
   - Wenn der Befehl aufgrund eines ausgefallenen Laufwerks ausfällt, setzen Sie die ausgefallene Festplatte physisch aus, lassen Sie sie aber in den Steckplatz, bis ein Austausch erfolgt.
   - Wenn der Befehl fehlschlägt, weil der Partner „nicht bereit“ ist, warten Sie 5 Minuten, bis das HA-

Subsystem mit den Partnern synchronisiert wird.

- Wenn der Befehl aufgrund eines NDMP-, SnapMirror- oder SnapVault-Prozesses ausfällt, deaktivieren Sie den Prozess. Weitere Informationen finden Sie im entsprechenden Documentation Center.

3. Warten Sie 3 Minuten, und überprüfen Sie den Failover-Status mit dem Befehl *Storage Failover show*.
4. Geben Sie an der Eingabeaufforderung clustershell den Befehl *Network Interface show -is-Home false* ein, um die logischen Schnittstellen aufzulisten, die sich nicht auf ihrem Home-Controller und Port befinden.

   Wenn Schnittstellen als aufgeführt sind `false`, stellen Sie diese Schnittstellen mit dem Befehl *net int revert -vserver Cluster -LIF _nodename* zurück auf ihren Home-Port.

5. Verschieben Sie das Konsolenkabel zum Ziel-Controller und führen Sie den Befehl *Version -V* aus, um die ONTAP-Versionen zu überprüfen.
6. Verwenden Sie die `storage encryption disk show` , um die Ausgabe zu überprüfen.
7. Verwenden Sie den Befehl *Security key-Manager key query*, um die Schlüssel-IDs der Authentifizierungsschlüssel anzuzeigen, die auf den Schlüsselverwaltungs-Servern gespeichert sind.
   - Wenn der `Restored` Spalte = `yes/true`, Sie sind fertig und können den Austauschprozess abschließen.
   - Wenn `Key Manager type` = `external` und die `Restored` Spalte = nichts anderes als `yes/true`, verwenden Sie den Befehl *Security key-Manager external restore*, um die Schlüssel-IDs der Authentifizierungsschlüssel wiederherzustellen.

     Falls der Befehl fehlschlägt, wenden Sie sich an den Kundendienst.

   - Wenn `Key Manager type` = `onboard` und die `Restored` Spalte = eine andere als `yes/true`sind, verwenden Sie den Befehl *Security Key-Manager Onboard Sync*, um die fehlenden Onboard-Schlüssel auf dem reparierten Knoten zu synchronisieren.

     Überprüfen Sie mit dem Befehl *Security key-Manager key query*, ob die `Restored` Spalte für alle Authentifizierungsschlüssel = `yes/true` ist.

8. Schließen Sie das Konsolenkabel an den Partner Controller an.
9. Geben Sie den Controller mithilfe des zurück `storage failover giveback -fromnode local` Befehl.
10. Stellen Sie das automatische Giveback wieder her, wenn Sie es mithilfe des Befehls *Storage Failover modify -Node local -Auto-Giveback true* deaktiviert haben.
11. Wenn AutoSupport aktiviert ist, stellen Sie die automatische Fallerstellung mithilfe des Befehls *System Node AutoSupport Invoke -Node * -type all -message MAINT=END* wieder her.

Senden Sie das fehlerhafte Teil an NetApp - AFF A1K zurück

Senden Sie das fehlerhafte Teil wie in den dem Kit beiliegenden RMA-Anweisungen beschrieben an NetApp zurück. Siehe "Teilerückgabe Austausch" Seite für weitere Informationen.