启动介质-手动恢复

Install and maintain

NetApp
December 18, 2024

目录

启动介质-手动恢复

手动启动介质恢复概述- ASA A1K

您可以使用USB模块作为启动映像来手动更换发生故障的启动介质。

手动启动介质更换使用传统方法：从NetApp支持站点下载ONTAP映像、将映像传输到USB驱动器、将其下载到目标替代启动介质、以及手动浏览启动菜单选项以在替代启动介质上安装ONTAP映像。

启动介质更换工作流- ASA A1K

按照以下工作流步骤更换启动介质。

1. "查看启动介质要求"

要更换启动介质、您必须满足特定要求。

2. "检查板载加密密钥"

验证系统是否已启用安全密钥管理器或已加密磁盘。

3. **"Shut down the impaired controller"**

关闭或接管受损控制器、以使运行正常的控制器继续从受损控制器存储提供数据。

4. "更换启动介质"

从系统管理模块中取出故障启动介质并安装替代启动介质、然后使用USB闪存驱动器将ONTAP映像传输到替代启动介质。

5. "启动恢复映像"

从USB驱动器启动ONTAP映像、还原文件系统并验证环境变量。

6. "恢复加密"

从ONATp启动菜单还原板载密钥管理器配置或外部密钥管理器。

7. "将故障部件退回 **NetApp**"

按照套件随附的 RMA 说明将故障部件退回 NetApp 。

启动介质更换要求- ASA A1K

在更换启动介质之前、请确保查看以下要求。

- 您必须使用格式化为 fat32 的 USB 闪存驱动器，并具有适当的存储容量来存放 `image_xxx.tgz` 文件。
- 您必须将文件复制 `image_xxx.tgz` 到USB闪存驱动器、以供日后在此过程中使用。
- 您必须使用收到的NetApp更换FRU组件来更换故障组件。
- 请务必在正确的控制器上应用以下步骤中的命令：
  - 受损 _ 控制器是要在其中执行维护的控制器。
  - *health* 控制器是受损控制器的 HA 配对控制器。

检查加密密钥支持和状态- ASA A1K

在关闭受损控制器之前、请检查您的ONTAP版本是否支持NetApp卷加密(NVE)以及是否已正确配置密钥管理系统。

第1步：检查您的ONTAP版本是否支持NetApp卷加密

检查您的ONTAP版本是否支持NetApp卷加密(NVE)。此信息对于下载正确的ONTAP映像至关重要。

1. 运行以下命令、确定您的ONTAP版本是否支持加密：

   ```
   version -v
   ```

   如果输出包括 `10no-DARE`，则您的集群版本不支持NVE。

2. 根据您的系统是否支持NVE、执行以下操作之一：
   - 如果支持NVE、请下载采用NetApp卷加密的ONTAP映像。
   - 如果不支持NVE、请下载ONTAP映像*不使用* NetApp卷加密。

第2步：确定关闭控制器是否安全

要安全关闭控制器、请首先确定外部密钥管理器(External Key Manager、EKM)还是板载密钥管理器(Onboard Key Manager、OKM)处于活动状态。然后、验证正在使用的密钥管理器、显示相应的密钥信息、并根据身份验证密钥的状态采取措施。

1. 确定您的系统上启用了哪个密钥管理器：

ONTAP 版本	运行此命令
ONTAP 9．14．1或更高版本	`security key-manager keystore show` • 如果启用了EKM、 `EKM`则会在命令输出中列出。 • 如果启用了OKM、 `OKM`则会在命令输出中列出。 • 如果未启用密钥管理器、 `No key manager keystores configured`则会在命令输出中列出。
ONTAP 9.13.1 或更早版本	`security key-manager show-key-store` • 如果启用了EKM、 `external`则会在命令输出中列出。 • 如果启用了OKM、 `onboard`则会在命令输出中列出。 • 如果未启用密钥管理器、 `No key managers configured`则会在命令输出中列出。

2. 根据系统上是否配置了密钥管理器、选择以下选项之一。

未配置密钥管理器

您可以安全地关闭受损控制器。转到。 "关闭受损控制器"

已配置外部或板载密钥管理器

a. 输入以下查询命令以显示密钥管理器中的身份验证密钥状态。

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

b. 检查密钥管理器列中的值输出 `Restored`。

此列指示您的密钥管理器(EKM或OKM)的身份验证密钥是否已成功还原。

3. 根据您的系统使用的是外部密钥管理器还是板载密钥管理器、选择以下选项之一。

外部密钥管理器

根据列中显示的输出值 `Restored`、执行相应的步骤。

列中的输出值 `Restored`	请按照以下步骤操作 ...
`true`	您可以安全地关闭受损控制器。转到。 "关闭受损控制器"
以外的任何内容 `true`	a. 使用以下命令将外部密钥管理身份验证密钥还原到集群中的所有节点： `security key-manager external restore` 如果命令失败，请联系 "NetApp 支持"。 b. 输入命令以验证所有身份验证密钥的 `security key-manager key query`列是否 `Restored`显示 `true`。 如果所有身份验证密钥均为 `true`，则可以安全地关闭受损控制器。转到。 "关闭受损控制器"

板载密钥管理器

根据列中显示的输出值 `Restored`、执行相应的步骤。

列中的输出值 `Restored`	请按照以下步骤操作 ...
`true`	手动备份OKM信息。 a. 输入进入高级模式、然后 `Y`在出现提示时输入 `set -priv advanced`。 b. 输入以下命令以显示密钥管理信息： `security key-manager onboard show-backup` c. Copy the contents of the backup information to a separate file or your log file. You'll need it in disaster scenarios where you might need to manually recover OKM. d. 您可以安全地关闭受损控制器。转到。 "关闭受损控制器"

列中的输出值 `Restored`	请按照以下步骤操作 ...

以外的任何内容 `true`	a. 输入板载security key-manager sync命令：
	
	`security key-manager onboard sync`
	
	b. 出现提示时、输入32个字符的字母数字板载密钥管理密码短语。
	
	如果无法提供密码短语，请联系 "NetApp 支持"。
	
	c. 验证 `Restored`所有身份验证密钥的列显示 `true`：
	
	`security key-manager key query`
	
	d. 验证类型是否 `Key Manager` 显示 `onboard`，然后手动备份OKM信息。
	e. 输入命令以显示密钥管理备份信息：
	
	`security key-manager onboard show-backup`
	
	f. Copy the contents of the backup information to a separate file or your log file.
	
	You'll need it in disaster scenarios where you might need to manually recover OKM.
	
	g. 您可以安全地关闭受损控制器。转到。 "关闭受损控制器"

关闭受损控制器- ASA A1K

您需要完成受损控制器的关闭。关闭或接管受损控制器。

要关闭受损控制器，您必须确定控制器的状态，并在必要时接管控制器，以便运行正常的控制器继续从受损控制器存储提供数据。

关于此任务

- 如果您使用的是SAN系统，则必须已检查受损控制器SCSI刀片的事件消息 `cluster kernel-service show`。 `cluster kernel-service show`命令(在priv高级模式下)可显示该节点的节点名称"仲裁状态"、该节点的可用性状态以及该节点的运行状态。

  每个 SCSI 刀片式服务器进程应与集群中的其他节点保持仲裁关系。在继续更换之前，必须先解决所有问题。

- If you have a cluster with more than two nodes, it must be in quorum.如果集群未达到仲裁或运行状况良好的控制器在资格和运行状况方面显示false、则必须在关闭受损控制器之前更正问题描述；请参见 "将节点与集群同步"。

步骤

1. 如果启用了AutoSupport、则通过调用AutoSupport消息禁止自动创建案例： `system node autosupport invoke -node * -type all -message MAINT=<# of hours>h`

   以下AutoSupport 消息禁止自动创建案例两小时： `cluster1:> system node autosupport invoke -node * -type all -message MAINT=2h`

2. 从运行状况良好的控制器的控制台禁用自动交还： `storage failover modify -node local -auto -giveback false`

   当您看到_Do you want to disable auto-giveback？_时、输入`y`。

3. 将受损控制器显示为 LOADER 提示符：

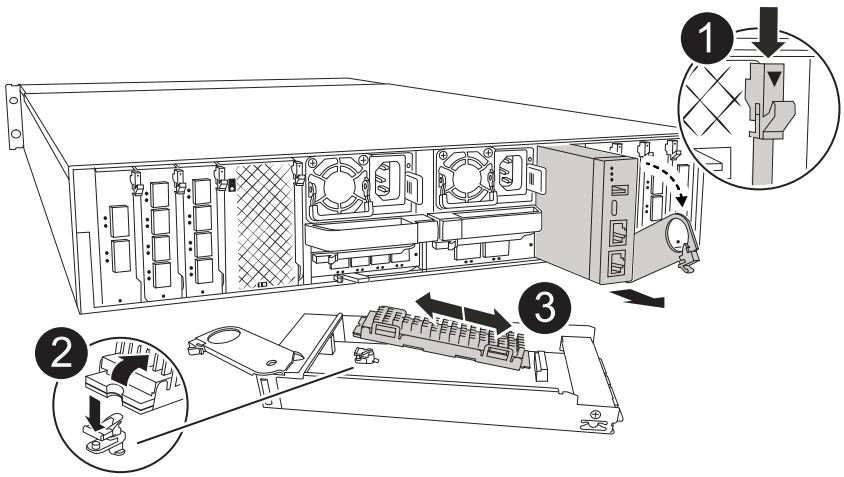
如果受损控制器显示 ...	那么 ...
LOADER 提示符	转至下一步。
正在等待交还	按 Ctrl-C ，然后在出现提示时回答 `y` 。
系统提示符或密码提示符	从运行正常的控制器接管或暂停受损的控制器： `storage failover takeover -ofnode impaired_node_name` 当受损控制器显示 Waiting for giveback… 时，按 Ctrl-C ，然后回答 `y` 。

更换启动介质- ASA A1K

您必须拔下控制器模块、从系统背面卸下系统管理模块、卸下受损启动介质、然后在系统管理模块中安装替代启动介质。

Step 1: Replace the boot media

启动介质位于系统管理模块内部、可通过从系统中卸下模块来访问。



1	系统管理模块凸轮闩锁
2	启动介质锁定按钮
3	启动介质

1. 如果您尚未接地，请正确接地。
2. 从控制器的PSU上拔下电源线。

   如果存储系统具有直流电源、请断开电源电缆块与电源设备(PSU)的连接。

   a. 拔下连接到系统管理模块的所有电缆。请务必在电缆的连接位置贴上标签、以便在重新安装模块时将其连接到正确的端口。
   b. 向下旋转缆线管理托架、方法是拉动缆线管理托架内侧两侧的按钮、然后向下旋转托架。
   c. 按下System Management (系统管理)凸轮按钮。
   d. 将凸轮闩锁向下旋转到最远位置。
   e. 通过将手指插入凸轮拉杆开口并将系统管理模块拉出机柜、从机柜中卸下系统管理模块。
   f. 将系统管理模块放在防静电垫上、以便可以访问启动介质。
3. 从管理模块中删除启动介质：
   a. 按下蓝色锁定按钮。
   b. 向上旋转启动介质、将其从插槽中滑出、然后放在一旁。
4. 将替代启动介质安装到系统管理模块中：
   a. 将启动介质的边缘与插槽外壳对齐，然后将其轻轻直推入插槽。
   b. 朝锁定按钮方向向下旋转启动介质。
   c. 按下锁定按钮、向下旋转行李箱介质、然后松开锁定按钮。
5. 重新安装系统管理模块。
   a. 将模块与机柜插槽开口的边缘对齐。
   b. 将模块轻轻地滑入插槽，直至完全滑入机箱，然后将凸轮闩锁一直向上旋转，以将模块锁定到位。
6. 将缆线管理托架向上旋转到关闭位置。
   a. 重新对系统管理模块进行配置。

第2步：将ONTAP映像传输到启动介质

您安装的替代启动介质没有ONTAP映像。您可以将相应的ONTAP服务映像从下载到USB闪存驱动器、然后再下载到替代启动介质、从而将ONTAP映像传输到 "NetApp 支持站点"替代启动介质。

开始之前

- 您必须有一个空的USB闪存驱动器、格式化为FAT32、容量至少为4 GB。

- 下载与受损控制器正在运行的映像版本相同的ONTAP的副本。您可以从NetApp支持站点上的"Downloads"部分下载相应的映像。使用 `version -v`命令显示您的ONTAP版本是否支持NVE。如果命令输出显示 `<10no- DARE>`，则您的ONTAP版本不支持NVE。
  - 如果您的ONTAP版本支持NVE、请按照下载按钮中的说明、使用NetApp卷加密下载映像。
  - 如果不支持NVE、请按照下载按钮中的说明下载不带NetApp卷加密的映像。
- 如果您的系统是HA对、则必须在控制器的节点管理端口(通常为e0M接口)之间建立网络连接。

步骤

1. 从下载相应的服务映像并将其复制 "NetApp 支持站点" 到USB闪存驱动器。
   a. 从页面上的"Downloads"(下载)链接将服务映像下载到笔记本电脑上的工作空间。
   b. 解压缩服务映像。

   > 如果要使用 Windows 提取内容，请勿使用 WinZip 提取网络启动映像。使用其他提取工具，例如 7-Zip 或 WinRAR 。

   USB闪存驱动器应具有受损控制器正在运行的相应ONTAP映像。

   a. 从笔记本电脑中取出 USB 闪存驱动器。
2. 将USB闪存驱动器插入系统管理模块上的USB插槽。

   确保将 USB 闪存驱动器安装在标有 USB 设备的插槽中，而不是 USB 控制台端口中。
3. 将电源线插入电源设备、然后重新安装电源线固定器。

   将电源重新连接到系统后、控制器将立即启动。
4. 按 Ctrl-C 在 LOADER 提示符处停止，以中断启动过程。

   如果未显示此消息，请按 Ctrl-C ，选择选项以启动到维护模式，然后暂停控制器以启动到加载程序。
5. 在 LOADER 提示符处设置网络连接类型：
   - 如果要配置DHCP： `ifconfig e0M -auto`

     > 您配置的目标端口是在通过网络连接还原 var 文件系统期间，用于与运行正常的控制器中受损的控制器进行通信的目标端口。You can also use the e0M port in this command.

   - 如果要配置手动连接： `ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway`
     - filer_addr 是存储系统的 IP 地址。
     - netmask 是连接到 HA 配对节点的管理网络的网络掩码。
     - gateway 是网络的网关。

   > 您的接口可能需要其他参数。有关详细信息，您可以在固件提示符处输入 help ifconfig 。

启动恢复映像- ASA A1K

您必须从 USB 驱动器启动 ONTAP 映像，还原文件系统并验证环境变量。

步骤

1. 从 LOADER 提示符处，从 USB 闪存驱动器启动恢复映像： `boot_recovery`

   此映像将从 USB 闪存驱动器下载。

2. 出现提示时，请输入映像名称或接受屏幕上括号内显示的默认映像。
3. 还原 var 文件系统：

选项1：**ONTAP 9 16.0**或更早版本

a. 在受损控制器上、看到时 `Do you want to restore the backup configuration now?` 按 `Y`

b. 在受损控制器上、当系统提示覆盖_/etc/ssh/ssh_host_Ossa_key_时、按 `Y`。

c. 在运行状况良好的配对控制器上，将受损控制器设置为高级权限级别： `set -privilege advanced`。

d. 在运行状况良好的配对控制器上，运行restore backup命令： `system node restore-backup -node local -target-address impaired_node_IP_address`。

*注：*如果您看到除成功还原以外的任何消息，请联系 "NetApp 支持"。

e. 在运行状况良好的配对控制器上，将受损控制器恢复为管理级别： `set -privilege admin`。

f. 在受损控制器上，当您看到时 `Was the restore backup procedure successful?`按 `Y`。

g. 在受损控制器上，当您看到时 `...would you like to use this restored copy now?`按 `Y`。

h. 在受损控制器上、当系统提示您重新启动受损控制器时按键 `Y`、然后按键 `ctrl-c`进入Boot Menu (启动菜单)。

i. 如果系统不使用加密，请选择_Option 1 Normal Boot._，否则转到。"恢复加密"

选项2：**ONTAP 9．16．1**或更高版本

a. 在受损控制器上、当系统提示还原备份配置时按 `Y`。

恢复过程成功后，将在控制台-上显示此消息 `syncflash_partner: Restore from partner complete`。

b. 在受损控制器上、当系统提示确认还原备份是否成功时按 `Y`。

c. 在受损控制器上、当系统提示使用还原的配置时、按 `Y`。

d. 在受损控制器上、当系统提示重新启动节点时按 `Y`。

e. 在受损控制器上、当系统提示您重新启动受损控制器时按键 `Y`、然后按键 `ctrl-c`进入Boot Menu (启动菜单)。

f. 如果系统不使用加密，请选择_Option 1 Normal Boot._，否则转到。"恢复加密"

4. 将控制台缆线连接到配对控制器。
5. 使用 `storage failover giveback -fromnode local` 命令交还控制器。
6. 使用 `storage failover modify -node local -auto-giveback true` 命令禁用自动交还后，可将其还原。
7. 如果启用了AutoSupport、请使用命令还原/取消禁止自动创建案例 `system node autosupport invoke -node * -type all -message MAINT=END`。

*注：*如果此过程失败，请联系 "NetApp 支持"。

恢复加密- ASA A1K

恢复替代启动介质上的加密。

您必须使用在启动介质更换过程开始时捕获的设置完成特定于已启用板载密钥管理器(OKM)、NetApp存储加密(NSE)或NetApp卷加密(NVE)的系统的步骤。

根据系统上配置的密钥管理器、选择以下选项之一、从启动菜单中将其还原。

- "选项1：还原板载密钥管理器配置"
- "选项2：还原外部密钥管理器配置"

选项1：还原板载密钥管理器配置

从ONTAP启动菜单还原板载密钥管理器(OKM)配置。

开始之前

- 还原OKM配置时、请确保您具有以下信息：
  - 已输入集群范围的密码短语 "同时启用板载密钥管理"。
  - "板载密钥管理器的备份信息"(英文)
- 请先执行此 "如何验证板载密钥管理备份和集群范围的密码短语" 过程、然后再继续。

步骤

1. 将控制台缆线连接到目标控制器。
2. 从ONTAP启动菜单中、从启动菜单中选择适当的选项。

ONTAP 版本	选择此选项
ONTAP 9.8 或更高版本	选择选项10。 显示启动菜单示例 ``` 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 ```

ONTAP 版本	选择此选项
ONTAP 9 7及更早版本	选择隐藏选项 `recover_onboard_keymanager` 显示启动菜单示例 ``` 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 ```

3. 确认您要继续恢复过程。

   显示示例提示符

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

4. 输入集群范围的密码短语两次。

   输入密码短语时、控制台不会显示任何输入。

   显示示例提示符

   ```
   Enter the passphrase for onboard key management:

   Enter the passphrase again to confirm:
   ```

5. 输入备份信息。

   a. 将整个内容从开始备份行粘贴到结束备份行。

显示示例提示符

```
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---------------------------
```

b. 在输入末尾按两次回车键。

恢复过程完成。

显示示例提示符

```
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.
*******************************************************************
******************
```

如果显示的输出不是，请勿继续 `Successfully recovered keymanager secrets`。执行故障排除以更正错误。

6. 从启动菜单中选择选项1以继续启动至ONTAP。

显示示例提示符

```
**********************************************************************
***************
* 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. 确认控制器的控制台显示以下消息。

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

8. 在配对节点上、输入以下命令以对配对控制器进行回指。

   `storage failover giveback -fromnode local -only-cfo-aggregates true`(英文)

9. 在仅使用CFO聚合启动后、运行以下命令。

   `security key-manager onboard sync`

10. 输入板载密钥管理器的集群范围密码短语。

显示示例提示符

```
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.
```

如果同步成功、则会返回集群提示符、而不会显示任何其他消息。如果同步失败、则会在返回集群提示符之前显示一条错误消息。更正错误并成功运行同步之前、请勿继续。

11. 输入以下命令、确保所有密钥均已同步。

    ```
    security key-manager key query -restored false(英文)

    There are no entries matching your query.
    ```

    在reved参数中筛选false时、不应显示任何结果。

12. 输入以下命令、从配对节点进行节点回给。

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

13. 如果已禁用自动交还、请输入以下命令来还原自动交还。

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

14. 如果启用了AutoSupport、请输入以下命令来恢复自动创建案例。

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

选项2：还原外部密钥管理器配置

从ONTAP启动菜单还原外部密钥管理器配置。

开始之前

要还原外部密钥管理器(External Key Manager、EKM)配置、您需要以下信息。

- 另一个集群节点上的/cfcard/kmip/servers.cfg文件的副本或以下信息：
  - KMIP服务器地址。
  - KMIP端口。
- 另一个集群节点或客户端证书中的文件副本 `/cfcard/kmip/certs/client.crt`。

- 从其他集群节点或客户端密钥获取的文件副本 `/cfcard/kmip/certs/client.key`。
- 另一个集群节点或KMIP服务器CA中的文件副本 `/cfcard/kmip/certs/CA.pem`。

步骤

1. 将控制台缆线连接到目标控制器。
2. 从ONTAP启动菜单中选择选项11。

   显示启动菜单示例

   ```
   (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. 出现提示时、确认您已收集所需信息。

   显示示例提示符

   ```
   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. 出现提示时、输入客户端和服务器信息。

   显示提示符

   ```
   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:
   ```

显示示例

```
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-----
<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....
kmip_init: configuring ports
Running command '/sbin/ifconfig e0M'
..
..
kmip_init: cmd: ReleaseExtraBSDPort e0M
```

输入客户端和服务器信息后、恢复过程将完成。

显示示例

```
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. 从启动菜单中选择选项1以继续启动至ONTAP。

显示示例提示符

```
*****************************************************************
***************
* 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. 如果已禁用自动交还、请输入以下命令来还原自动交还。

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

7. 如果启用了AutoSupport、请输入以下命令来恢复自动创建案例。

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

将故障部件退回给NetApp - ASA A1K

按照套件随附的 RMA 说明将故障部件退回 NetApp 。 "部件退回和更换"有关详细信息、请参见页面。