



# 启动介质

## Install and maintain

NetApp  
September 25, 2024

# 目录

启动介质 .....	1
启动介质更换 workflow—FAS70和FAS90 .....	1
启动介质更换要求- FAS70和FAS90 .....	1
检查板载加密密钥- FAS70和FAS90 .....	2
Shut down the impaired controller - FAS70 and FAS90 .....	3
更换启动介质— FAS70 和 FAS90 .....	5
启动恢复映像—FAS70和FAS90 .....	8
恢复加密—FAS70和FAS90 .....	10
将故障部件退回给NetApp—FAS70和FAS90 .....	18

# 启动介质

## 启动介质更换工作流程—FAS70和FAS90

按照以下工作流程步骤更换启动介质。

1

"查看启动介质更换要求"

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- FAS70和FAS90

在更换启动介质之前、请确保查看以下要求。

- You must have a USB flash drive, formatted to FAT32, with the appropriate amount of storage to hold the `image_xxx.tgz`.
- 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。

- 您必须将故障组件更换为从提供商处收到的替代 FRU 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。

## 检查板载加密密钥- FAS70和FAS90

在关闭受损控制器并检查板载加密密钥的状态之前，您必须检查受损控制器的状态，禁用自动交还并检查正在运行的 ONTAP 版本。

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"](#)。

### 检查NVE或NSE

在关闭受损控制器之前、您需要验证系统是否已启用安全密钥管理器或已加密磁盘。

### 验证安全密钥管理器配置

#### 步骤

1. 使用 `_security key-manager keyStore show_` 命令确定密钥管理器是否处于活动状态。有关详细信息、请参见 ["security key-manager keyStore show手册页"](#)



您可能还有其他密钥管理器类型。类型包括 KMIP、AKV 和 GCP。确认这些类型的过程与确认或密钥管理器类型的过程相同 `external onboard`。

- 如果未显示任何输出、请转至 ["关闭受损控制器"](#) 以关闭受损节点。
  - 如果命令显示输出、则表示系统 `security key-manager` 处于活动状态、您需要显示 Key Manager 类型和状态。
2. 使用 `_security key-manager key query_` 命令 显示活动的信息 Key Manager 。
    - 如果 Key Manager 类型显示 `external` 且列显示，`Restored`true`` 则可以安全地关闭受损控制器。
    - 如果 Key Manager 显示类型 `onboard`，并且 `Restored` 列显示 `true`，则需要完成一些附加步骤。
    - 如果 Key Manager 显示类型 `external`，而 `Restored` 列显示除以外的任何内容 `true`，则需要完成一些附加步骤。
    - 如果 Key Manager 显示类型 `onboard`，而 `Restored` 列显示除以外的任何内容 `true`，则需要完成一些附加步骤。
  3. 如果 Key Manager 类型显示 `onboard` 且 `Restored` 列显示 `true`，则手动备份OKM信息：
    - a. 在系统提示您继续时输入 `y: set -priv advanced`
    - b. 输入命令以显示密钥管理信息：`security key-manager onboard show-backup`
    - c. 将备份信息的内容复制到单独的文件或日志文件。在可能需要手动恢复 OKM 的灾难情形下，您将需要它。

- d. 您可以安全地关闭受损控制器。
4. 如果 Key Manager 显示类型 onboard ，并且 Restored 列显示除此以外的任何内容 true：
  - a. 输入板载 security key-manager sync 命令：`security key-manager onboard sync`

 在提示符处输入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支持部门。 "[mysupport.netapp.com](https://mysupport.netapp.com)"
  - b. 验证 Restored 所有身份验证密钥的列显示 true：`security key-manager key query`
  - c. 验证类型是否 Key Manager 显示 onboard，然后手动备份OKM信息。
  - d. 输入命令以显示密钥管理备份信息：`security key-manager onboard show-backup`
  - e. 将备份信息的内容复制到单独的文件或日志文件。在可能需要手动恢复 OKM 的灾难情形下，您将需要它。
  - f. 您可以安全地关闭控制器。
5. 如果 Key Manager 显示类型 external ，并且 Restored 列显示除此以外的任何内容 true：
  - a. 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，请通过联系NetApp支持部门 "[mysupport.netapp.com](https://mysupport.netapp.com)"。
  - b. 验证是否 Restored 为所有身份验证密钥显示列 true：`security key-manager key query`
  - c. 您可以安全地关闭受损控制器。

## Shut down the impaired controller - FAS70 and FAS90

完成 NVE 或 NSE 任务后，您需要关闭受损控制器。使用适用于您的配置的操作步骤 关闭或接管受损控制器。

## 选项 1：大多数系统

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)可显示节点名称、该节点的仲裁状态、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. 从运行正常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 <code>y</code> 。
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： <code>storage failover takeover -ofnode <i>impaired_node_name</i></code>  当受损控制器显示 <code>Waiting for giveback...</code> 时，按 Ctrl-C ，然后回答 <code>y</code> 。

## 选项 2：控制器位于 MetroCluster 中

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。

- 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”。

- 如果您使用的是 MetroCluster 配置，则必须确认已配置 MetroCluster 配置状态，并且节点处于已启用且正常的状态 (MetroCluster node show)。

#### 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：

```
ssystem node  
AutoSupport invoke -node * -type all -message MAINT=number_of_hours_downh
```

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. 从运行正常的控制器的控制台禁用自动交还：

```
storage failover modify - node local  
-auto-giveback false
```
3. 将受损控制器显示为 LOADER 提示符：

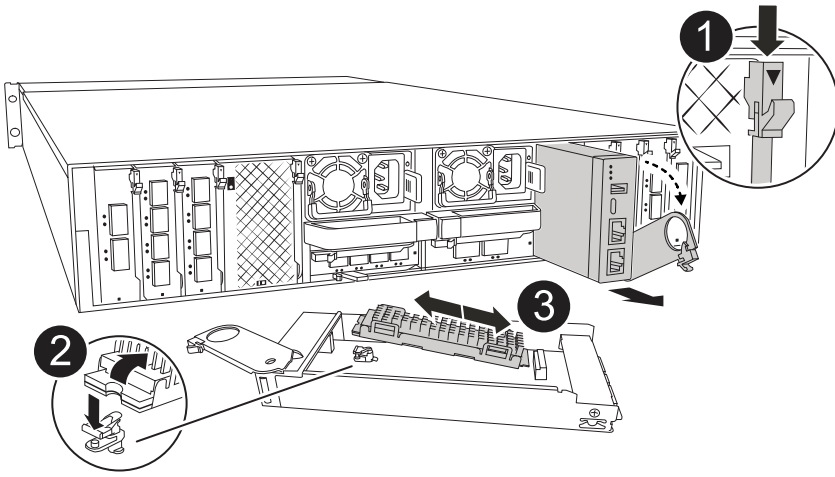
如果受损控制器显示 ...	那么 ...
LOADER 提示符	转至下一步。
正在等待交还	按 Ctrl-C，然后在出现提示时回答 y。
系统提示符或密码提示符（输入系统密码）	从运行正常的控制器接管或暂停受损的控制器： <pre>storage failover takeover -ofnode <i>impaired_node_name</i></pre> 当受损控制器显示 Waiting for giveback... 时，按 Ctrl-C，然后回答 y。

## 更换启动介质— FAS70 和 FAS90

要更换引导介质、您必须从系统背面卸下系统管理模块、卸下受损的引导介质、然后在系统管理模块中安装替代引导介质。

### 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。



	<p>系统管理模块凸轮门锁</p>
	<p>启动介质锁定按钮</p>
	<p>启动介质</p>

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ONTAP映像传输到替代启动介质、方法是从下载相应的ONTAP服务映像到 ["NetApp 支持站点"](#) USB闪存驱动器、然后再下载到替代启动介质。

### 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。
- 您必须拥有与受损控制器正在运行的ONTAP映像版本相同的副本。您可以从NetApp支持站点上的部分下载相应的映像 ["下载"](#)
  - 如果支持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。

- c. 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—FAS70和FAS90

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. 从加载程序提示符处、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：

如果系统正在运行 ...	那么 ...
ONTAP 9.16.0 或更早版本	<p>a. 在受损控制器上、看到时按_Y_ Do you want to restore the backup configuration now?</p> <p>b. 在受损控制器上，当系统提示覆盖时按_Y_ /etc/ssh/ssh_host_ecdsa_key。</p> <p>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：<i>set -PRILEGE advanced</i>。</p> <p>d. 在运行状况良好的配对控制器上、运行restore backup命令：<i>system node reRestore -backup -node local -target-address受损_none_ip_address</i>。</p> <p>*注：*如果您看到除成功还原以外的任何消息，请联系 <a href="#">"NetApp 支持"</a>。</p> <p>e. 在运行正常的配对控制器上、将受损控制器恢复为管理级别：<i>set -PRILEGE ADMIN</i>。</p> <p>f. 在受损控制器上，看到时按_y_ Was the restore backup procedure successful?。</p> <p>g. 在受损控制器上，看到时按_y_ ...would you like to use this restored copy now?。</p> <p>h. 在受损控制器上、在系统提示重新启动受损控制器时按_y_、然后按_Ctrl-c_进入启动菜单。</p> <p>i. 如果系统不使用加密，请选择_Option 1 Normal Boot._，否则转到。<a href="#">"还原密钥管理器"</a></p> <p>j. 将控制台缆线连接到配对控制器。</p> <p>k. 使用_storage故障转移交还-from node local_命令交还控制器。</p> <p>l. 如果已使用_storage故障转移修改-node local -auto-交还true命令禁用自动交还、则还原自动交还。</p> <p>m. 如果启用了AutoSupport、请使用_system node AutoSupport invoke -node *-type all -message Maint=end_命令还原/取消禁止自动创建案例。</p> <p>*注：*如果此过程失败，请联系 <a href="#">"NetApp 支持"</a>。</p>

如果系统正在运行 ...	那么 ...
ONTAP 9. 16. 1或更高版本	<p>a. 在受损控制器上、当系统提示还原备份配置时、按_y_。</p> <p>恢复过程成功后，将在控制台-上显示此消息  <code>syncflash_partner: Restore from partner complete.</code></p> <p>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_。</p> <p>c. 在受损控制器上、当系统提示您使用已还原的配置时、按_y_。</p> <p>d. 在受损控制器上、当系统提示重新启动节点时、按_y_。</p> <p>e. 在受损控制器上、在系统提示重新启动受损控制器时按_y_、然后按_Ctrl-c_进入启动菜单。</p> <p>f. 如果系统不使用加密，请选择_Option 1 Normal Boot._，否则转到。<a href="#">"还原密钥管理器"</a></p> <p>g. 将控制台缆线连接到配对控制器。</p> <p>h. 使用_storage故障转移交还-from node local_命令交还控制器。</p> <p>i. 如果已使用_storage故障转移修改-node local -auto-交还true命令禁用自动交还、则还原自动交还。</p> <p>j. 如果启用了AutoSupport、请使用_system node AutoSupport invoke -node *-type all -message Maint=end_命令还原/取消禁止自动创建案例。</p> <p>*注：*如果此过程失败，请联系 <a href="#">"NetApp 支持"</a>。</p>

## 恢复加密—FAS70和FAS90

恢复替代启动介质上的加密。

### 第1步：还原板载密钥管理器

您必须使用在此过程开始时捕获的设置完成特定于启用了板载密钥管理器(OKM)、NetApp存储加密(NSE)或NetApp卷加密(NVE)的系统的步骤。



如果启用了NSE或NVE以及板载或外部密钥管理器、则必须还原在此过程开始时捕获的设置。

#### 步骤

1. 将控制台缆线连接到目标控制器。
2. 从ONATp启动菜单中选择以下选项之一以还原板载密钥管理器配置。

选项1：具有板载密钥管理器服务器配置的系统  
从ONATp启动菜单还原板载密钥管理器配置。

开始之前

还原OKM配置时、需要以下信息：

- 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. 从ONTAP启动菜单中选择选项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. 确认此过程是否继续。`This option must be used only in disaster recovery procedures. Are you sure? (y or n):`y

3. 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。

```
Enter the passphrase for onboard key management:
```

```
Enter the passphrase again to confirm:
```

4. 输入备份信息。将整个内容从开始备份行粘贴到结束备份行。

在输入末尾按两次回车键。



```
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。

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

8. 从配对节点交还配对控制器： `_storage故障转移交还-frofnode local -only—cfo-Aggregates true _`
9. 仅使用CFO聚合启动后、运行 `_security key-manager onboard sync_` 命令：
10. 输入板载密钥管理器的集群范围密码短语：

```
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. 确保所有密钥均已同步： `security key-manager key query-reRestored false`

```
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. 从配对节点进行节点恢复： `storage故障转移-from node local`

选项2：具有外部密钥管理器服务器配置的系统

从ONATp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(EKM)配置、您需要以下信息：

- 您需要另一个集群节点上的/cfcard/kmip/servers.cfg文件的副本、或者以下信息：
- KMIP服务器地址。
- KMIP端口。
- 另一个集群节点或客户端证书中的/cfcard/kmip/certs/client.crt文件的副本。
- 另一个集群节点或客户端密钥上的/cfcard/kmip/certs client.key文件的副本。
- 另一个集群节点或KMIP服务器CA的/cfcard/kmip/certs /CA.pm文件的副本。

步骤

1. 从ONTAP启动菜单中选择选项11。



```
(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. 出现提示时、确认您已收集所需信息：

- 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*

您也可以使用以下提示：

- 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. 为每个提示提供相关信息：

- 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-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwwY8xCzAJBgNVBAYTA1VT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk5l
MSUybQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxcilJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxp bz3mXF/X/1PC3YOzVNCq5eieek62si
Fp8=
-----END CERTIFICATE-----
```

Enter the client key (client.key) file contents:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpQIBAAKCAQEAOUleaajEG6QC2h2Zih0jEaGVtQUexNeoCFwKPomSePmjDNtrU
MSB1SlX3VgCuElHk57XPdq6xSbYl b kIb4bAgLztHEmUDOkGmXYAkblQ=
-----END RSA PRIVATE KEY-----
```

Enter the KMIP server CA(s) (CA.pem) file contents:

```
-----BEGIN CERTIFICATE-----
MIIEIzCCA3OgAwIBAgIBADANBgkqhkiG9w0BAQsFADCBjzELMAkGA1UEBhMVCVMx
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. 恢复过程将完成:

```
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。

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

## 第2步：完成启动介质更换

在正常启动后、通过完成最终检查并交还存储来完成启动介质更换过程。

1. 检查控制台输出：

如果控制台显示 ...	那么 ...
登录提示符	转至步骤6。
正在等待交还	a. 登录到配对控制器。 b. 使用 <code>_storage故障转移show_</code> 命令确认目标控制器已准备好进行恢复。

2. 使用 `_storage故障转移交还-fronode local -only -cfo-Aggregates true` 命令将控制台缆线移至配对控制器并交还目标控制器存储。

- 如果命令因磁盘发生故障而失败，请物理断开故障磁盘，但将磁盘保留在插槽中，直到收到更换磁盘为止。
- 如果此命令因配对节点“未就绪”而失败、请等待5分钟、以便HA子系统在配对节点之间同步。
- 如果命令因 NDMP ， SnapMirror 或 SnapVault 进程而失败，请禁用此进程。有关详细信息，请参见相应的文档中心。

3. 等待3分钟、然后使用 `_storage故障转移show_` 命令检查故障转移状态。
4. 在 `cluster-shell` 提示符处、输入 `_network interface show -is-home false_` 命令、列出不在其主控制器和端口上的逻辑接口。

如果列出了任何接口 `false`，请使用 `_net int revserver cluster -lif _nokename_` 命令 将这些接口还原回其主端口。

5. 将控制台缆线移至目标控制器、然后运行 `_version -v_` 命令以检查ONTAP版本。
6. 使用 `storage encryption disk show` 查看输出。
7. 使用 `_security key-manager key query_` 命令 显示密钥管理服务器上存储的身份验证密钥的密钥ID。
  - 如果 `restored column = yes/true`，则表示您已完成更换过程，并可继续完成更换过程。
  - 如果 `Key Manager type = external` 和 `Restored` 列=以外的任何内容 `yes/true`，请使用 `_security key-manager External Restore_` 命令 还原身份验证密钥的密钥ID。



如果命令失败，请联系客户支持。

- 如果 `Key Manager type = onboard` 和 `Restored` 列=以外的任何内容 `yes/true`，请使用 `_security key-manager onboard sync_` 命令同步修复后节点上缺少的板载密钥。

使用 `_security key-manager key query_` 命令 验证所有身份验证 `Restored` 密钥的列= `yes/true`。

8. 将控制台缆线连接到配对控制器。
9. 使用 `storage failover giveback -fromnode local` 命令交还控制器。
10. 如果已使用 `_storage故障转移修改-node local -auto-交还true` 命令禁用自动交还、则还原自动交还。
11. 如果启用了AutoSupport、请使用 `_system node AutoSupport invoke -node *-type all -message Maint=end_` 命令还原/取消禁止自动创建案例。

## 将故障部件退回给NetApp—FAS70和FAS90

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。

## 版权信息

版权所有 © 2024 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

## 商标信息

NetApp、NetApp 标识和 <http://www.netapp.com/TM> 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。