



# 启动介质

## Install and maintain

NetApp  
December 18, 2024

# 目录

启动介质	1
启动介质更换概述—FAS2820	1
检查加密密钥支持和状态- FAS2820	1
关闭受损控制器—FAS2820	4
更换启动介质- FAS2820	5
启动恢复映像—FAS2820	10
还原加密- FAS2820	12
将故障部件退回给NetApp - FAS2820	22

# 启动介质

## 启动介质更换概述—FAS2820

启动介质存储系统在启动时使用的一组主文件和二级系统文件（启动映像）。根据您的网络配置，您可以执行无中断或中断更换。

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。

您还必须将 image\_XXX.tgz 文件复制到 USB 闪存驱动器，以供日后在此操作步骤中使用。

- 更换启动介质的无中断和中断方法都要求您还原 var 文件系统：
  - 要进行无中断更换，必须将 HA 对连接到网络以还原 var 文件系统。
  - 要进行中断更换，您不需要网络连接即可还原 var 文件系统，但此过程需要重新启动两次。
- 您必须将故障组件更换为从提供商处收到的替代 FRU 组件。
- 请务必在正确的节点上应用以下步骤中的命令：
  - 受损节点是指要在其中执行维护的节点。
  - 运行状况良好的节点 \_ 是受损节点的 HA 配对节点。

## 检查加密密钥支持和状态- FAS2820

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 1Ono-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	<pre>security key-manager keystore show</pre> <ul style="list-style-type: none"><li>• 如果启用了EKM、`EKM`则会在命令输出中列出。</li><li>• 如果启用了OKM、`OKM`则会在命令输出中列出。</li><li>• 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。</li></ul>
ONTAP 9.13.1 或更早版本	<pre>security key-manager show-key-store</pre> <ul style="list-style-type: none"><li>• 如果启用了EKM、`external`则会在命令输出中列出。</li><li>• 如果启用了OKM、`onboard`则会在命令输出中列出。</li><li>• 如果未启用密钥管理器、`No key managers configured`则会在命令输出中列出。</li></ul>

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。" <a href="#">关闭受损控制器</a> "
以外的任何内容 true	<p>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：</p> <pre>security key-manager external restore</pre> <p>如果命令失败，请联系 "<a href="#">NetApp 支持</a>"。</p> <p>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。</p> <p>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。"<a href="#">关闭受损控制器</a>"</p>

## 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	<p>手动备份OKM信息。</p> <p>a. 输入进入高级模式、然后 y`在出现提示时输入 `set -priv advanced。</p> <p>b. 输入以下命令以显示密钥管理信息：</p> <pre>security key-manager onboard show-backup</pre> <p>c. Copy the contents of the backup information to a separate file or your log file.</p> <p>You'll need it in disaster scenarios where you might need to manually recover OKM.</p> <p>d. 您可以安全地关闭受损控制器。转到。"<a href="#">关闭受损控制器</a>"</p>

列中的输出值 Restored	请按照以下步骤操作 ...
以外的任何内容 true	<p>a. 输入板载security key-manager sync命令：</p> <pre>security key-manager onboard sync</pre> <p>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。</p> <p>如果无法提供密码短语，请联系 <a href="#">"NetApp 支持"</a>。</p> <p>c. 验证 Restored`所有身份验证密钥的列显示 `true：</p> <pre>security key-manager key query</pre> <p>d. 验证类型是否 Key Manager 显示 onboard，然后手动备份OKM信息。</p> <p>e. 输入命令以显示密钥管理备份信息：</p> <pre>security key-manager onboard show-backup</pre> <p>f. Copy the contents of the backup information to a separate file or your log file.</p> <p>You'll need it in disaster scenarios where you might need to manually recover OKM.</p> <p>g. 您可以安全地关闭受损控制器。转到。 <a href="#">"关闭受损控制器"</a></p>

## 关闭受损控制器—FAS2820

关闭或接管受损控制器。

完成 NVE 或 NSE 任务后，您需要关闭受损控制器。

步骤

1. 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 "Remove controller module" 。
正在等待交还 ...	按 Ctrl-C ，然后在出现提示时回答 y 。

如果受损控制器显示 ...	那么 ...
系统提示符或密码提示符（输入系统密码）	<p>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 impaired_node_name</code></p> <p>当受损控制器显示 <code>Waiting for giveback...</code> 时，按 <code>Ctrl-C</code>，然后回答 <code>y</code>。</p>

2. 在 `LOADER` 提示符处，输入 `printenv` 以捕获所有启动环境变量。将输出保存到日志文件中。



如果启动设备损坏或无法正常运行，则此命令可能不起作用。

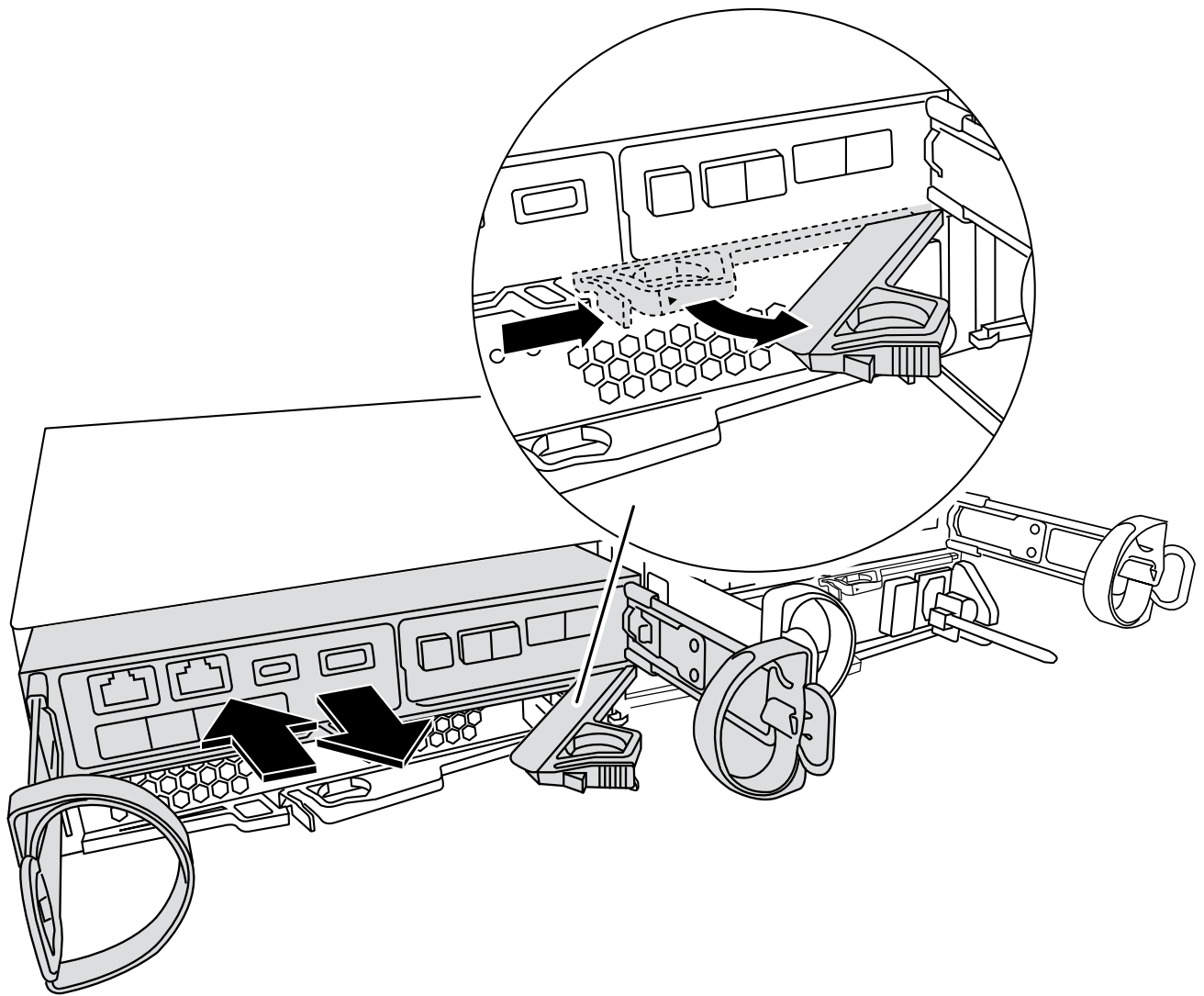
## 更换启动介质- FAS2820

要更换启动介质，您必须卸下受损的控制器模块，安装替代启动介质并将启动映像传输到 USB 闪存驱动器。

### 第 1 步：卸下控制器模块

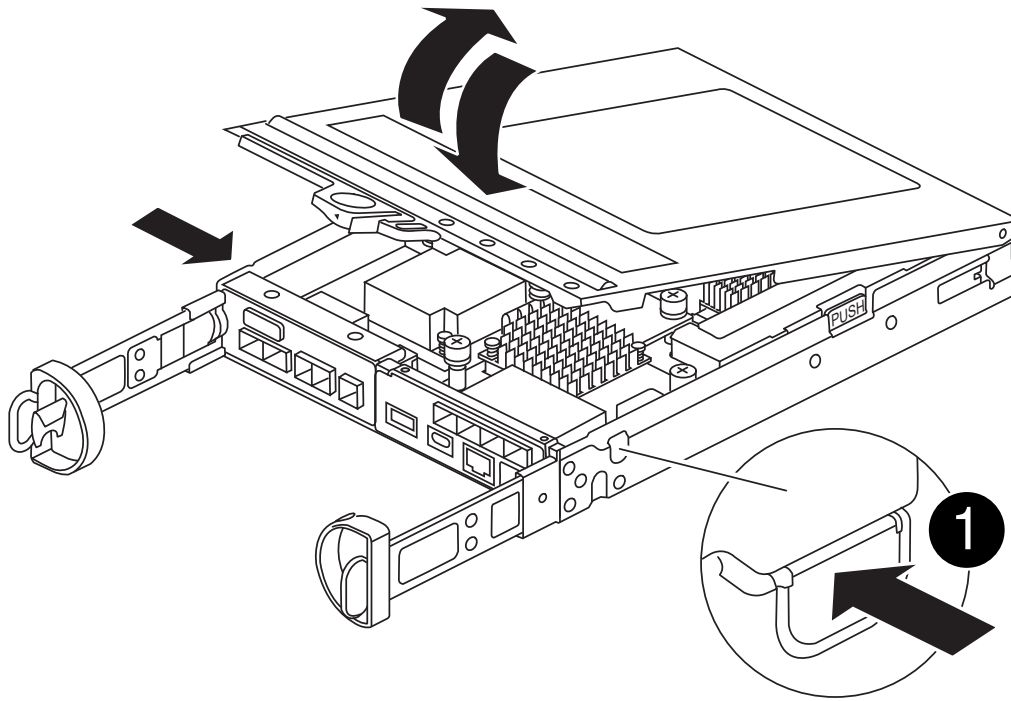
要访问控制器内部的组件，您必须先从系统中卸下控制器模块，然后再卸下控制器模块上的盖板。

1. 如果您尚未接地，请正确接地。
2. 松开将缆线绑在缆线管理设备上的钩环带，然后从控制器模块上拔下系统缆线和 SFP（如果需要），并跟踪缆线的连接位置。
3. 按压凸轮把手上的门锁，直到其释放为止，完全打开凸轮把手以从中板释放控制器模块，然后用两只手将控制器模块拉出机箱。



4. 将控制器模块翻转，将其放在平稳的表面上。
5. 按下控制器模块两侧的蓝色按钮以松开护盖、然后向上旋转护盖、使其脱离控制器模块、从而打开护盖。





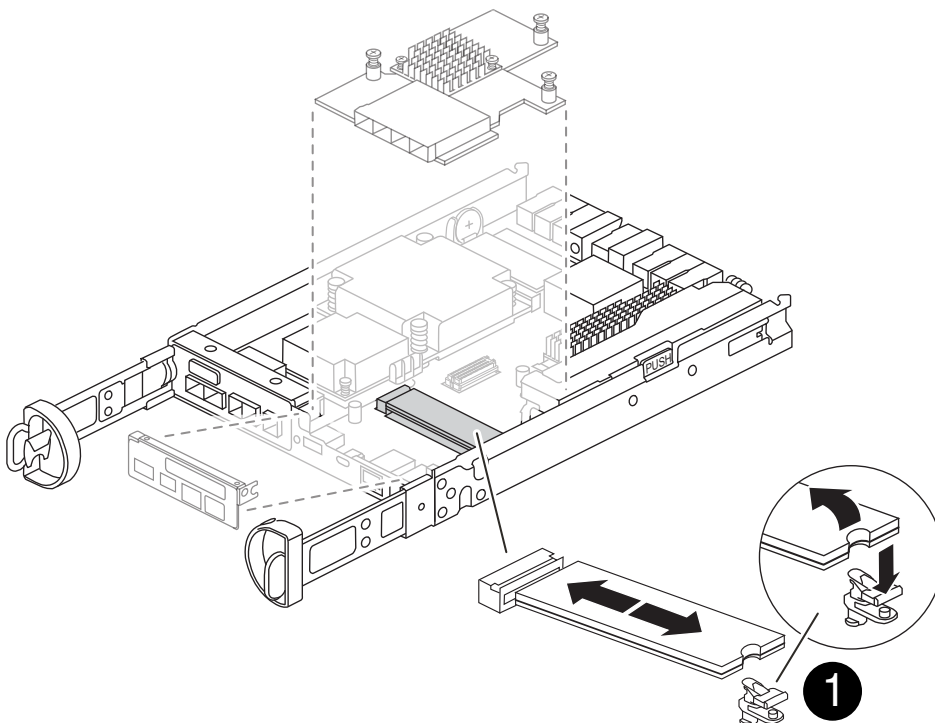
1

控制器模块护盖释放按钮

## 第 2 步：更换启动介质

找到位于夹层卡下方的控制器模块中的启动介质、然后按照说明进行更换。

动画-更换启动介质



## 步骤

1. 如果您尚未接地，请正确接地。
2. 按照下图或控制器模块上的FRU示意图卸下夹层卡：
  - a. 将IO板从控制器模块中直接滑出、以将其卸下。
  - b. 拧松夹层卡上的翼形螺钉。



您可以用手指或螺丝刀拧松翼形螺钉。如果您用手指，则可能需要向上旋转NV电池、以便在其旁边的指旋螺钉上购买更好的手指。

- c. 垂直向上提起夹层卡。
3. 更换启动介质：
    - a. 按下启动介质外壳上的蓝色按钮、将启动介质从其外壳中释放出来、向上旋转启动介质、然后轻轻地将其从启动介质插槽中竖直拉出。



请勿将启动介质竖直向上扭曲或拉，因为这样可能会损坏插槽或启动介质。

- b. Align the edges of the replacement boot media with the boot media socket, and then gently push it into the socket. 检查启动介质以确保其完全正确地固定在插槽中、如有必要、请取出启动介质并将其重新插入插槽。
  - c. 按下蓝色锁定按钮、向下旋转启动介质、然后释放锁定按钮以将启动介质锁定到位。
4. 重新安装夹层卡：
    - a. 将主板上的插槽与夹层卡上的插槽对齐、然后将卡轻轻地插入插槽中。
    - b. 拧紧夹层卡上的三个翼形螺钉。
    - c. 重新安装IO板。
  5. 重新安装控制器模块护盖并将其锁定到位。

### 第 3 步：将启动映像传输到启动介质

使用已安装系统映像的USB闪存驱动器将系统映像安装在替代启动介质上。在此操作步骤期间、您必须还原var文件系统。

## 开始之前

- 您必须具有一个格式化为MBR/FAT32且容量至少为4 GB的USB闪存驱动器。
- 您必须具有网络连接。

## 步骤

1. 将适当的ONTAP映像版本下载到已格式化的USB闪存驱动器：
  - a. 使用 ... ["如何确定正在运行的ONTAP版本是否支持NetApp卷加密\(NVE\)"](#) 以确定当前是否支持卷加密。
    - 如果集群支持NVE、请使用NetApp卷加密下载映像。

- 如果集群不支持NVE、请下载不带NetApp卷加密的映像。请参见 ["我应该下载哪个ONTAP映像？是否使用卷加密？"](#) 有关详细信息：

## 2. 解压缩下载的映像。



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。

解压缩的服务映像文件中有两个文件夹：

- 启动
- EFI
  - i. 将 EFI 文件夹复制到 USB 闪存驱动器上的顶部目录。

USB 闪存驱动器应具有 EFI 文件夹，并且与受损控制器运行的服务映像（BIOS）版本相同。

- ii. 从笔记本电脑中取出 USB 闪存驱动器。

## 3. 安装控制器模块：

- a. 将控制器模块的末端与机箱中的开口对齐，然后将控制器模块轻轻推入系统的一半。
- b. 重新对控制器模块进行配置。

重新布线时，如果已卸下介质转换器（SFP），请务必重新安装它们。

## 4. 将 USB 闪存驱动器插入控制器模块上的 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。

## 5. 将控制器模块完全推入系统中，确保凸轮把手离开 USB 闪存驱动器，用力推动凸轮把手以完成控制器模块的就位，将凸轮把手推至关闭位置，然后拧紧翼形螺钉。

控制器一旦完全安装到机箱中，就会开始启动。

## 6. 按 Ctrl-C 中断启动过程，并在加载程序提示符处停止。如果看到正在启动自动启动，请按 Ctrl-C 中止 ...

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。

## 7. 对于机箱中有一个控制器的系统，重新连接电源并打开电源。

系统开始启动并停留在 LOADER 提示符处。

## 8. 在 LOADER 提示符处设置网络连接类型：

- 如果要配置 DHCP：`ifconfig e0a -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 e0a -addr=filer_addr -mask=netmask -gw=gateway -dns=dns_addr-domain=dns_domain`

- `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。
- `dns_addr` 是网络上名称服务器的 IP 地址。
- `dns_domain` 是域名系统（DNS）域名。

如果使用此可选参数，则无需在网络启动服务器 URL 中使用完全限定域名。您只需要服务器的主机名。



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

## 启动恢复映像—FAS2820

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"](#)。

# 还原加密- FAS2820

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	<p data-bbox="621 159 776 195">选择选项10。</p> <p data-bbox="621 233 834 268">显示启动菜单示例</p> <div data-bbox="654 306 1455 1087" style="border: 1px solid #ccc; padding: 10px;"><p data-bbox="683 344 1292 373">Please choose one of the following:</p><ul data-bbox="683 422 1365 1016" style="list-style-type: none"><li data-bbox="683 422 971 451">(1) Normal Boot.</li><li data-bbox="683 464 1133 493">(2) Boot without /etc/rc.</li><li data-bbox="683 506 1045 535">(3) Change password.</li><li data-bbox="683 548 1365 611">(4) Clean configuration and initialize all disks.</li><li data-bbox="683 623 1149 653">(5) Maintenance mode boot.</li><li data-bbox="683 665 1328 695">(6) Update flash from backup config.</li><li data-bbox="683 707 1240 737">(7) Install new software first.</li><li data-bbox="683 749 971 779">(8) Reboot node.</li><li data-bbox="683 791 1192 854">(9) Configure Advanced Drive Partitioning.</li><li data-bbox="683 867 1333 930">(10) Set Onboard Key Manager recovery secrets.</li><li data-bbox="683 942 1317 1005">(11) Configure node for external key management.</li></ul><p data-bbox="683 1026 1029 1056">Selection (1-11)? 10</p></div>

ONTAP 版本	选择此选项
ONTAP 9.7及更早版本	<p>选择隐藏选项 <code>recover_onboard_keymanager</code></p> <p>显示启动菜单示例</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. 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-----  
01234567890123456789012345678901234567890123456789012345678901234567890123  
12345678901234567890123456789012345678901234567890123456789012345678901234  
23456789012345678901234567890123456789012345678901234567890123456789012345  
34567890123456789012345678901234567890123456789012345678901234567890123456  
45678901234567890123456789012345678901234567890123456789012345678901234567  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
01234567890123456789012345678901234567890123456789012345678901234567890123  
12345678901234567890123456789012345678901234567890123456789012345678901234  
23456789012345678901234567890123456789012345678901234567890123456789012345  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA  
  
-----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-----
MIIDvjCCAqagAwIBAgICN3gwDQYJKoZIhvcNAQELBQAwwY8xCzAJBgNVBAYTA1VT
MRMwEQYDVQQIEwpDYWxpZm9ybmlhMQwwCgYDVQQHEwNTVkwxDzANBgNVBAoTBk5l
MSUubQusvzAFs8G3P54GG32iIRvaCFnj2gQpCxcilJ0qB2foiBGx5XVQ/Mtk+rlap
Pk4ECW/wqSOUXDYtJs1+RB+w0+SHx8mzxpzb3mXF/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
```

输入客户端和服务端信息后、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 - FAS2820

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。