



启动媒体 - 手动恢复

Install and maintain

NetApp
February 13, 2026

目录

启动媒体 - 手动恢复	1
启动媒体手动恢复工作流程 - AFF C800	1
手动启动媒体恢复的要求 - AFF C800	1
检查加密密钥支持和状态- AFF C800	2
步骤 1: 检查 NVE 支持并下载正确的ONTAP映像	2
步骤 2: 验证密钥管理器状态并备份配置	3
关闭控制器以进行手动启动介质恢复 - AFF C800	5
选项 1: 大多数系统	5
选项 2: 系统位于 MetroCluster 中	6
更换启动介质并准备手动启动恢复 - AFF C800	7
第 1 步: 卸下控制器模块	7
第 2 步: 更换启动介质	9
第 3 步: 将启动映像传输到启动介质	11
从 USB 驱动器手动恢复启动媒体 - AFF C800	13
恢复加密- AFF C800	15
将失败的启动介质返回给NetApp - AFF C800	25

启动媒体 - 手动恢复

启动媒体手动恢复工作流程 - AFF C800

通过查看更换要求、检查加密状态、关闭控制器、更换启动介质、启动恢复映像、恢复加密以及验证系统功能，开始更换AFF C800存储系统中的启动介质。

如果您的存储系统运行的是ONTAP 9.17.1 或更高版本，请使用["自动启动恢复程序"](#)。如果您的系统运行的是早期版本的ONTAP，则必须使用手动启动恢复过程。

1

["查看启动介质要求"](#)

查看更换启动介质的要求。

2

["检查加密密钥支持和状态"](#)

确定系统是启用了安全密钥管理器还是对磁盘进行了加密。

3

["关闭控制器"](#)

需要更换启动介质时、请关闭控制器。

4

["更换启动介质"](#)

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

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启动菜单恢复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 。

手动启动媒体恢复的要求 - AFF C800

在更换AFF C800 系统中的启动介质之前，请确保满足成功更换的必要要求。这包括确保您拥有具有适当存储容量的 USB 闪存驱动器，并验证您拥有正确的替换启动设备。

如果您的存储系统运行的是ONTAP 9.17.1 或更高版本，请使用["自动启动恢复程序"](#)。如果您的系统运行的是早期版本的ONTAP，则必须使用手动启动恢复过程。

USB 闪存盘

- 确保您有一个格式化为 FAT32 的 USB 闪存驱动器。
- USB 必须具有足够的存储容量来容纳 `image_xxx.tgz` 文件。

文件准备

复制 `image_xxx.tgz` 将文件复制到 USB 闪存驱动器。使用 USB 闪存驱动器传输ONTAP映像时将使用此文件。

组件更换

使用NetApp提供的替换组件来更换故障组件。

控制器识别

更换受损的启动介质时，将命令应用到正确的控制器至关重要：

- `_受损控制器_`是您正在执行维护的控制器。
- `_健康控制器_`是受损控制器的 HA 伙伴。

下一步是什么？

查看更换引导介质的要求后，您需要["检查启动介质上的加密密钥支持和状态"](#)。

检查加密密钥支持和状态- AFF C800

为确保AFF C800 存储系统上的数据安全，您需要验证启动介质上的加密密钥支持情况及其状态。检查您的ONTAP版本是否支持NetApp卷加密 (NVE)，并在关闭控制器之前检查密钥管理器是否处于活动状态。

如果您的存储系统运行的是ONTAP 9.17.1 或更高版本，请使用["自动启动恢复程序"](#)。如果您的系统运行的是早期版本的ONTAP，则必须使用手动启动恢复过程。

步骤 1：检查 NVE 支持并下载正确的ONTAP映像

确定您的ONTAP版本是否支持NetApp卷加密 (NVE)，以便您可以下载正确的ONTAP映像来替换启动介质。

步骤

1. 检查您的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. 下载符合 NVE 支持的ONTAP镜像：
 - 如果支持 NVE：下载带有NetApp卷加密的ONTAP映像
 - 如果不支持 NVE：下载不带NetApp卷加密的ONTAP映像



从NetApp支持网站下载ONTAP映像到您的 HTTP 或 FTP 服务器或本地文件夹。在更换启动介质的过程中，您将需要此映像文件。

步骤 2：验证密钥管理器状态并备份配置

在关闭故障控制器之前，请验证密钥管理器配置并备份必要信息。

步骤

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"> • 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	<pre>security key-manager show-key-store</pre> <ul style="list-style-type: none"> • 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. 根据系统中是否配置了密钥管理器，执行以下操作之一：

如果未配置密钥管理器：

您可以安全地关闭故障控制器，并继续执行关机程序。

如果配置了密钥管理器（**EKM** 或 **OKM**）：

- a. 输入以下查询命令，显示密钥管理器中身份验证密钥的状态：

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

- b. 查看输出结果并检查其中的值。`Restored` 柱子。此列指示密钥管理器（EKM 或 OKM）的身份验证密钥是否已成功恢复。

3. 请根据您的密钥管理员类型完成相应的操作步骤：

外部密钥管理器（EKM）

根据数值完成以下步骤。`Restored` 柱子。

如果所有按键都显示 `true` 在“已恢复”列中：

您可以安全地关闭故障控制器，并继续执行关机程序。

如果任何键显示的值不是 `true` 在“已恢复”列中：

- a. 将外部密钥管理认证密钥恢复到集群中的所有节点：

```
security key-manager external restore
```

如果命令执行失败，请联系NetApp支持。

- b. 确认所有身份验证密钥均已恢复：

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

确认 `Restored` 列显示 `true` 适用于所有身份验证密钥。

- c. 如果所有密钥都已恢复，则可以安全地关闭故障控制器并继续执行关机程序。

板载密钥管理器（OKM）

根据数值完成以下步骤。`Restored` 柱子。

如果所有按键都显示 `true` 在“已恢复”列中：

- a. 备份 OKM 信息：

- i. 切换到高级权限模式：

```
set -priv advanced
```

进入 `y` 当提示继续时。

- i. 显示密钥管理备份信息：

```
security key-manager onboard show-backup
```

- ii. 将备份信息复制到单独的文件或日志文件中。

如果在更换过程中需要手动恢复 OKM，您将需要此备份信息。

- iii. 返回管理员模式：

```
set -priv admin
```

- b. 您可以安全地关闭故障控制器，并继续执行关机程序。

如果任何键显示的值不是 `true` 在“已恢复”列中：

a. 同步板载密钥管理器：

```
security key-manager onboard sync
```

出现提示时，请输入 32 个字符的字母数字组合的机载密钥管理密码。



这是您在最初配置车载密钥管理器时创建的集群范围密码短语。如果您没有此密码短语，请联系NetApp支持。

b. 请确认所有身份验证密钥均已恢复：

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

确认 Restored 列显示 `true` 对于所有身份验证密钥和 `Key Manager` 类型展 `onboard`。

c. 备份 OKM 信息：

i. 切换到高级权限模式：

```
set -priv advanced
```

进入 `y` 当提示继续时。

i. 显示密钥管理备份信息：

```
security key-manager onboard show-backup
```

ii. 将备份信息复制到单独的文件或日志文件中。

如果在更换过程中需要手动恢复 OKM，您将需要此备份信息。

iii. 返回管理员模式：

```
set -priv admin
```

d. 您可以安全地关闭故障控制器，并继续执行关机程序。

关闭控制器以进行手动启动介质恢复 - AFF C800

关闭AFF C800 存储系统中受损的控制器，以防止数据丢失并在自动启动介质恢复过程中保持系统稳定性。

如果您的存储系统运行的是ONTAP 9.17.1 或更高版本，请使用["自动启动恢复程序"](#)。如果您的系统运行的是早期版本的ONTAP，则必须使用手动启动恢复过程。

选项 1：大多数系统

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 。
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： <code>storage failover takeover -ofnode impaired_node_name</code> 当受损控制器显示 Waiting for giveback... 时，按 Ctrl-C ，然后回答 y 。

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。

选项 2：系统位于 MetroCluster 中



如果您的系统采用双节点 MetroCluster 配置，请勿使用此操作步骤。

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。

如果受损控制器显示 ...	那么 ...
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 impaired_node_name</pre> <p>当受损控制器显示 Waiting for giveback... 时，按 Ctrl-C ，然后回答 y 。</p>

下一步是什么？

关闭控制器后，您需要["更换启动介质"](#)。

更换启动介质并准备手动启动恢复 - AFF C800

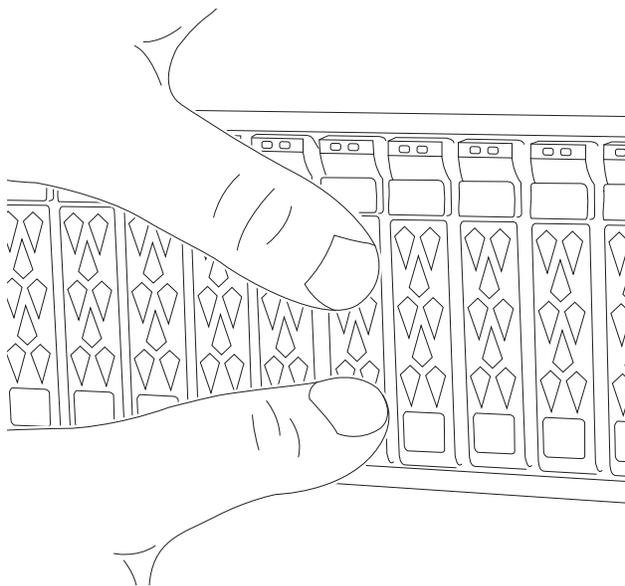
AFF C800 系统中的启动介质存储了重要的固件和配置数据。更换过程包括：移除系统管理模块、移除损坏的启动介质、安装替换启动介质，然后使用 USB 闪存驱动器将ONTAP映像手动传输到替换启动介质。

如果您的存储系统运行的是ONTAP 9.17.1 或更高版本，请使用["自动启动恢复程序"](#)。如果您的系统运行的是早期版本的ONTAP，则必须使用手动启动恢复过程。

第 1 步：卸下控制器模块

在更换控制器模块或更换控制器模块内的组件时，您必须从机箱中卸下控制器模块。

1. 如果您尚未接地，请正确接地。
2. 使用拇指推动每个驱动器、直至感觉到强制停止、以确保机箱中的所有驱动器都牢固地固定在中板上。



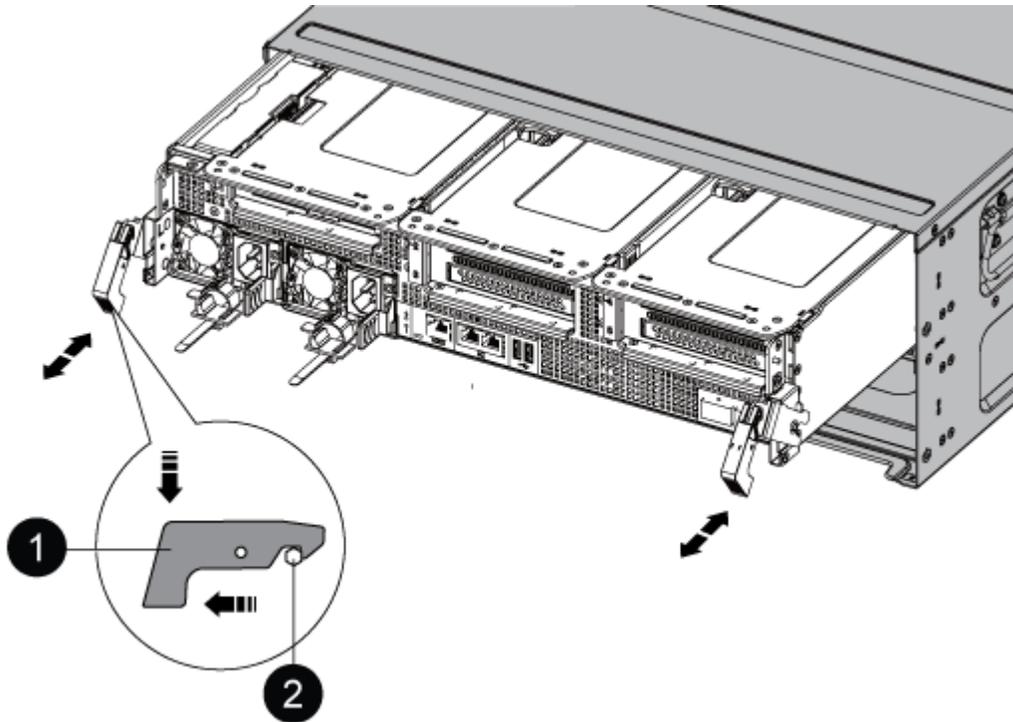
3. 从源拔下控制器模块电源。

4. 释放电源线固定器，然后从电源中拔下缆线。
5. 松开将缆线绑在缆线管理设备上的钩环带，然后从控制器模块中拔下系统缆线以及 SFP 和 QSFP 模块（如果需要），并跟踪缆线的连接位置。

将缆线留在缆线管理设备中，以便在重新安装缆线管理设备时，缆线排列有序。

6. 将缆线管理设备从控制器模块中取出并放在一旁。
7. 向下按两个锁定闩锁，然后同时向下旋转两个闩锁。

此控制器模块会从机箱中略微移出。

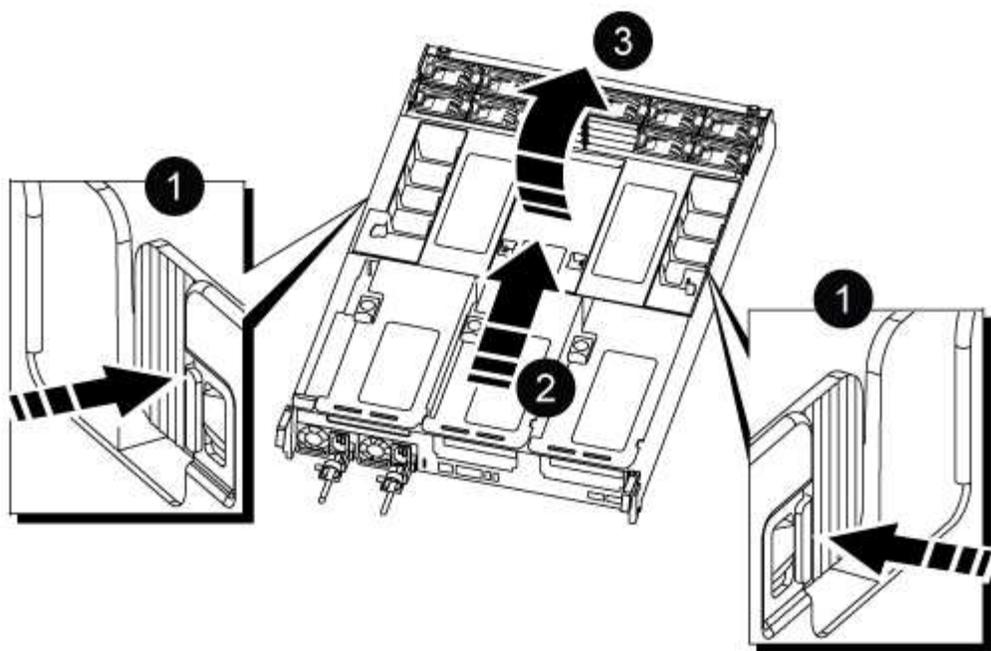


1	锁定闩锁
2	锁定销

8. 将控制器模块滑出机箱。

将控制器模块滑出机箱时，请确保您支持控制器模块的底部。

9. 将控制器模块放在平稳的表面上，然后打开通风管：
 - a. 朝控制器模块中间按下通风管两侧的锁定片。
 - b. 将通风管滑向风扇模块，然后将其向上旋转到完全打开的位置。



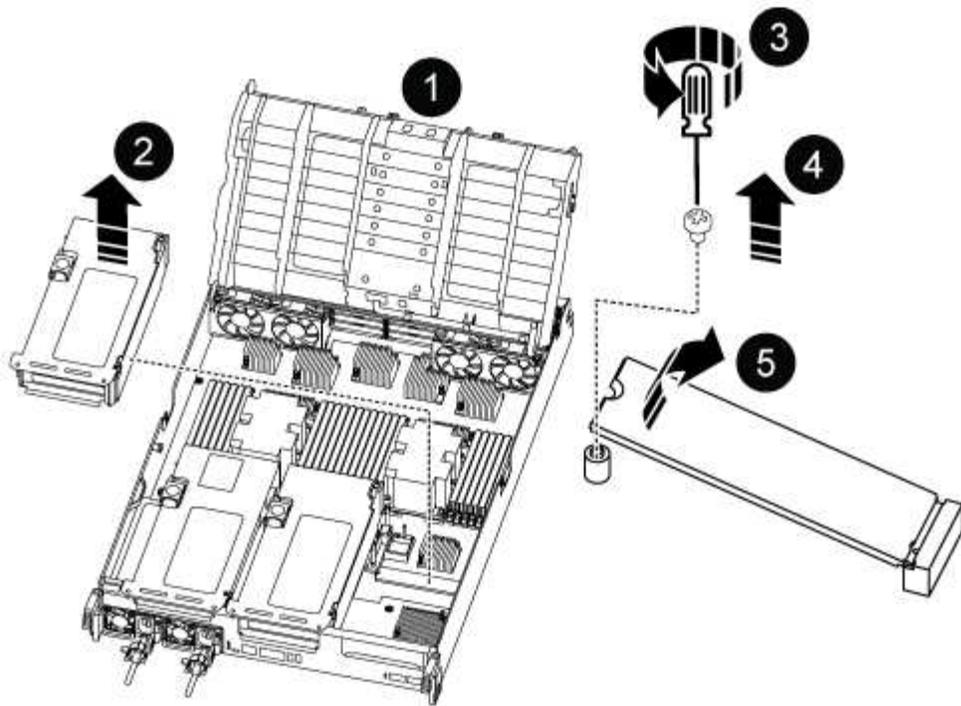
1	通风管锁定卡舌
2	将通风管滑向风扇模块
3	向风扇模块旋转通风管

第 2 步：更换启动介质

在更换启动介质之前，您可以通过删除控制器模块上的提升板 3 来找到控制器模块中发生故障的启动介质。

要卸下用于固定启动介质的螺钉，您需要使用十字螺丝刀。

1. 找到启动介质：



1	通风管
2	提升板 3
3	1 号十字螺丝刀
4	启动介质螺钉
5	启动介质

2. 从控制器模块中取出启动介质：

- a. 使用 1 号十字螺丝刀卸下固定启动介质的螺钉，并将螺钉放在安全位置。
- b. 抓住启动介质的两侧，将启动介质轻轻向上旋转，然后将启动介质竖直拉出插槽并放在一旁。

3. 将替代启动介质安装到控制器模块中：

- 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. 将启动介质向下旋转到主板。
- c. 使用启动介质螺钉将启动介质固定到主板。

请勿过度拧紧螺钉，否则可能会损坏启动介质。

4. 将此提升板重新安装到控制器模块中。

5. 关闭通风管：

- a. 向下旋转通风管。
- b. 将通风管滑向升降器，直到其卡入到位。

第 3 步：将启动映像传输到启动介质

您安装的替代启动介质没有启动映像，因此您需要使用 USB 闪存驱动器传输启动映像。

开始之前

- 您必须具有一个已格式化为 32 位的 USB 闪存驱动器，并且容量至少为 4 GB。
- 与受损控制器运行的 ONTAP 映像版本相同的副本。您可以从 NetApp 支持站点上的 "Downloads" 部分下载相应的映像
 - 如果启用了 NVE，请按照下载按钮中的指示，使用 NetApp 卷加密下载映像。
 - 如果未启用 NVE，请按照下载按钮中的指示，在不使用 NetApp 卷加密的情况下下载映像。
- 如果您的系统是 HA 对，则必须具有网络连接。
- 如果您的系统是独立系统，则不需要网络连接，但在还原 var 文件系统时，您必须执行额外的重新启动。

步骤

1. 将相应的服务映像从 NetApp 支持站点下载并复制到 USB 闪存驱动器。
 - a. 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。

解压缩的服务映像文件中有两个文件夹：

- /boot
- EFI

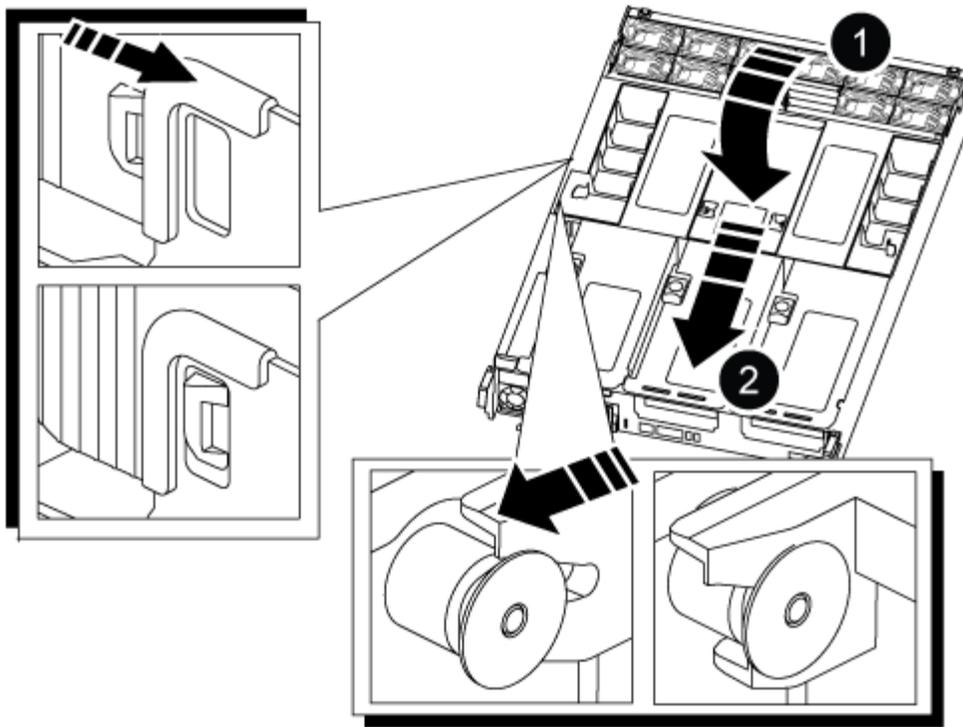
- c. 将 EFI 文件夹复制到 USB 闪存驱动器上的顶部目录。



如果服务映像没有EFI文件夹，请参阅["用于FAS和AFF型号的启动设备恢复的服务映像下载文件缺少EFI文件夹"](#)。

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。

- d. 从笔记本电脑中取出 USB 闪存驱动器。
2. 如果尚未关闭通风管：
 - a. 将通风管一直旋转至控制器模块。
 - b. 向提升板滑动通风管，直到锁定卡舌卡入到位。
 - c. 检查通风管，确保其正确就位并锁定到位。



1	通风管
2	提升板

3. 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。
4. 重新安装缆线管理设备，并根据需要重新对系统进行布线。

重新布线时，如果已卸下介质转换器（SFP 或 QSFP），请务必重新安装它们。

5. 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。

6. 将控制器模块一直轻轻推入系统中，直到控制器模块锁定挂钩开始上升，用力推动锁定挂钩以完成控制器模块的就位，然后将锁定挂钩旋转到控制器模块上插脚上方的锁定位置。
7. 将电源线插入电源、重新安装电源线锁环、然后将电源连接到电源。

电源恢复后、控制器模块将立即启动。Be prepared to interrupt the boot process.

8. 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。

下一步是什么？

更换启动介质后，您需要["启动恢复映像"](#)。

从 USB 驱动器手动恢复启动媒体 - AFF C800

在AFF C800系统中安装新的启动介质设备后，您可以从 USB 驱动器启动恢复映像，并从伙伴节点恢复配置。

如果您的存储系统运行的是ONTAP 9.17.1 或更高版本，请使用["自动启动恢复程序"](#)。如果您的系统运行的是早期版本的ONTAP，则必须使用手动启动恢复过程。

开始之前

- 请确保您的游戏机已连接到故障控制器。
- 请确认您拥有包含恢复映像的U盘。
- 确定您的系统是否使用加密。在步骤 3 中，您需要根据是否启用加密来选择相应的选项。

步骤

1. 在故障控制器的 LOADER 提示符下，从 USB 闪存驱动器启动恢复映像：

```
boot_recovery
```

恢复镜像文件是从U盘下载的。

2. 出现提示时，输入图像名称或按 **Enter** 键接受括号中显示的默认图像。
3. 请使用适用于您的ONTAP版本的步骤恢复 var 文件系统：

ONTAP 9.16.0 或更早版本

对受损控制人和合作控制人完成以下步骤：

- a. 在故障控制器上：按下 `y` 当你看到 `\Do you want to restore the backup configuration now?`
- b. 在故障控制器上：如果出现提示，请按 `Y` 覆盖 `/etc/ssh/ssh_host_ecdsa_key`。
- c. *在伙伴控制器上：*将故障控制器的权限级别设置为高级：

```
set -privilege advanced
```

- d. *在伙伴控制器上：*运行恢复备份命令：

```
system node restore-backup -node local -target-address  
impaired_node_IP_address
```



如果看到的不是恢复成功的消息，请联系NetApp支持。

- e. 在合作伙伴控制器上：返回管理员级别：

```
set -privilege admin
```

- f. 在故障控制器上：按下 `y` 当你看到 `\Was the restore backup procedure successful?`
- g. 在故障控制器上：按下 `y` 当你看到 `\...would you like to use this restored copy now?`
- h. 在故障控制器上：按下 `Y` 当提示重启时，按 `Ctrl-C` 当您看到启动菜单时。
- i. *对于故障控制器：*执行以下操作之一：
 - 如果系统不使用加密，请从启动菜单中选择_选项 1 正常启动_。
 - 如果系统使用加密，请转到["恢复加密"](#)。

ONTAP 9.16.1 或更高版本

对受损控制器完成以下步骤：

- a. 在系统提示还原备份配置时、按 `y`。

```
恢复过程成功后，将显示以下消息： syncflash_partner: Restore from partner  
complete
```

- b. 按 `Y` 当提示确认恢复备份成功时。
- c. 按 `Y` 当系统提示使用恢复的配置时。
- d. 按 `Y` 当系统提示重启节点时。
- e. 按 `Y` 当系统提示再次重启时，请按 `Ctrl-C` 当您看到启动菜单时。
- f. 执行以下操作之一：
 - 如果系统不使用加密，请从启动菜单中选择_选项 1 正常启动_。

- 如果系统使用加密，请转到["恢复加密"](#)。

4. 将控制台缆线连接到配对控制器。
5. 通过交还存储使控制器恢复正常运行：

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

6. 如果您禁用了自动返还功能，请重新启用它：

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

7. 如果启用了AutoSupport、则还原自动创建案例：

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

下一步是什么？

启动恢复映像后，您需要["恢复启动介质上的加密"](#)。

恢复加密- AFF C800

在AFF C800系统中，恢复替换启动介质上的加密，以确保数据持续受到保护。替换过程包括验证密钥可用性、重新应用加密设置以及确认对数据的安全访问。

如果您的存储系统运行的是ONTAP 9.17.1 或更高版本，请使用["自动启动恢复程序"](#)。如果您的系统运行的是早期版本的ONTAP，则必须使用手动启动恢复过程。

根据您的密钥管理器类型，完成相应的步骤以恢复系统加密。如果您不确定您的系统使用哪个密钥管理器，请检查您在启动介质更换过程开始时捕获的设置。

板载密钥管理器 (OKM)

从ONTAP启动菜单还原板载密钥管理器(OKM)配置。

开始之前

请确保您已准备好以下信息：

- 在输入集群范围的密码短语时 "启用车载密钥管理"
- "板载密钥管理器的备份信息"
- 使用以下方式验证您是否拥有正确的密码短语和备份数据： "如何验证板载密钥管理备份和集群范围的密码短语"程序

步骤

关于受损控制器：

1. 将游戏机连接线连接到故障控制器上。
2. 从ONTAP启动菜单中，选择相应的选项：

ONTAP 版本	选择此选项
ONTAP 9.8 或更高版本	<p>选择选项10。</p> <p>显示启动菜单示例</p> <div data-bbox="662 1024 1425 1810" style="border: 1px solid #ccc; padding: 10px;"><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. (10) Set Onboard Key Manager recovery secrets. (11) Configure node for external key management. Selection (1-11)? 10</pre></div>

ONTAP 版本	选择此选项
ONTAP 9.7及更早版本	选择隐藏选项 <code>recover_onboard_keymanager</code> 显示启动菜单示例 <div style="border: 1px solid #ccc; padding: 10px; background-color: #f9f9f9;"> <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. 出现提示时，请确认您是否要继续恢复过程：

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。

输入密码时，控制台不显示任何输入内容。

显示示例提示符

```
Enter the passphrase for onboard key management:

Enter the passphrase again to confirm:
```

5. 请输入备份信息：

- a. 粘贴从 BEGIN BACKUP 行到 END BACKUP 行的所有内容，包括破折号。


```
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
-----END
BACKUP-----
```

b. 输入内容结束后，按两次回车键。

恢复过程完成，并显示以下消息：

Successfully recovered keymanager secrets.

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

+



如果显示的输出结果不是以下内容，请勿继续操作：Successfully recovered keymanager secrets。进行故障排除以纠正错误。

6. 选择选项 `1` 从启动菜单继续启动进入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. 确认控制器控制台显示以下信息：

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

关于合作伙伴控制器：

8. 归还受损控制器：

```
storage failover giveback -fromnode local -only-cfo-aggregates true
```

关于受损控制器：

9. 仅使用 CFO 聚合启动后，同步密钥管理器：

```
security key-manager onboard sync
```

10. 出现提示时，输入集群范围内的板载密钥管理器密码短语。

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，则返回集群提示符，不包含其他消息。如果同步失败，则会在返回集群提示符之前显示错误消息。请勿继续操作，直到错误得到纠正且同步成功为止。

11. 确认所有密钥均已同步：

```
security key-manager key query -restored false
```

该命令不应返回任何结果。如果出现任何结果，请重复同步命令，直到没有结果返回为止。

关于合作伙伴控制器：

12. 归还受损控制器：

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

13. 如果禁用了自动交还、则还原它：

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

14. 如果启用了AutoSupport、则还原自动创建案例：

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

外部密钥管理器（EKM）

从ONTAP启动菜单还原外部密钥管理器配置。

开始之前

从另一个集群节点或备份中收集以下文件：

- ``/cfcard/kmip/servers.cfg`` 文件或 KMIP 服务器地址和端口
- ``/cfcard/kmip/certs/client.crt`` 文件（客户端证书）
- ``/cfcard/kmip/certs/client.key`` 文件（客户端密钥）
- ``/cfcard/kmip/certs/CA.pem`` 文件（KMIP 服务器 CA 证书）

步骤

关于受损控制器：

1. 将游戏机连接线连接到故障控制器上。
2. 选择选项 `11` 从ONTAP启动菜单。

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，请确认您已收集到所需信息：

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，请输入客户端和服务信息：
 - a. 输入客户端证书 (client.crt) 文件的内容，包括 BEGIN 行和 END 行。
 - b. 输入客户端密钥 (client.key) 文件的内容，包括 BEGIN 和 END 行。
 - c. 输入 KMIP 服务器 CA(s) (CA.pem) 文件内容，包括 BEGIN 和 END 行。
 - d. 请输入KMIP服务器IP地址。
 - e. 输入 KMIP 服务器端口（按 Enter 键使用默认端口 5696）。

显示示例

```
Enter the client certificate (client.crt) file contents:
-----BEGIN CERTIFICATE-----
<certificate_value>
-----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-----
<certificate_value>
-----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
```

恢复过程完成，并显示以下消息：

```
Successfully recovered keymanager secrets.
```

显示示例

```
System is ready to utilize external key manager(s).
Trying to recover keys from key servers....
Performing initialization of OpenSSL
Successfully recovered keymanager secrets.
```

5. 选择选项 `1` 从启动菜单继续启动进入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. 如果禁用了自动交还、则还原它：

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

7. 如果启用了AutoSupport、则还原自动创建案例：

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

下一步是什么？

在启动介质上恢复加密后，您需要["将故障部件退回给NetApp"](#)。

将失败的启动介质返回给NetApp - AFF C800

如果您的AFF C800 存储系统中的某个组件发生故障，请将故障部件退回给NetApp。参见["部件退回和更换"](#)更多信息请参见页面。

版权信息

版权所有 © 2026 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。