启动媒体 - 手动恢复

Install and maintain

NetApp
February 20, 2026

目录

启动媒体 - 手动恢复

启动介质手动恢复工作流程 - AFF A20、 AFF A30 和AFF A50

启动映像的手动恢复涉及使用 USB 驱动器将ONTAP重新安装到AFF A20、 AFF A30 或AFF A50 存储系统的替换启动介质上。您必须从NetApp支持站点下载相应的ONTAP恢复映像并将其复制到 USB 驱动器。然后，使用准备好的 USB 驱动器执行恢复操作，将系统恢复到正常运行状态。

如果您的系统运行的是ONTAP 9.17.1 及更高版本，请使用"自动启动恢复程序" 。

首先，检查恢复要求，关闭控制器，更换启动媒体，使用 USB 驱动器恢复映像，并在必要时重新应用加密设置。

1. "查看启动介质要求"

查看更换启动介质的要求。

2. "检查板载加密密钥"

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"

从受损的控制器中移除故障的启动介质并安装替换的启动介质，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ONTAP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 。

手动启动介质恢复的要求 - AFF A20、 AFF A30 和AFF A50

在更换AFF A20、 AFF A30 或AFF A50 存储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，并验证您是否拥有正确的替换启动设备。

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"。

检查手动启动媒体恢复的加密支持 - AFF A20、 AFF A30 和AFF A50

为确保AFF A20、 AFF A30 或AFF A50 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和状态。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。

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 `10no-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	`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。

下一步是什么？

检查启动介质上的加密密钥支持和状态后，您需要"关闭控制器"。

关闭控制器以进行手动启动介质恢复 - AFF A20、 AFF A30 和AFF A50

关闭AFF A20、 AFF A30 或AFF A50 存储系统中受损的控制器，以防止数据丢失并在手动启动介质恢复过程中保持系统稳定性。

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. 禁用自动交还：

   a. 从健康控制器的控制台输入以下命令：

      ```
      storage failover modify -node impaired_node_name -auto-giveback false
      ```

   b. 进入 `y`当您看到提示“您是否要禁用自动回馈？”时

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控制器： `storage failover takeover -ofnode impaired_node_name -halt true` -halt true参数将进入Loader提示符。

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"。
- 您必须确认已配置MetroCluster配置状态、并且节点处于启用和正常状态：

```
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：

```
system 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. 禁用自动交还：
   a. 从健康控制器的控制台输入以下命令：

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

   b. 进入 `y`当您看到提示“您是否要禁用自动回馈？”时
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	转至下一节。
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控制器： `storage failover takeover -ofnode` *`impaired_node_name`* `-halt` *`true`* -halt true参数将进入Loader提示符。

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 A20、 AFF A30 和AFF A50

AFF A20、 AFF A30 或AFF A50 存储系统中的启动介质存储了必要的固件和配置数据。更换过程包括移除控制器模块、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。

关于此任务

如果需要、您可以打开平台机箱位置(蓝色) LED、以帮助找到受影响的平台。使用SSH登录到BMC并输入`system location-led *on*`命令。

平台机箱有三个定位LED：操作员显示面板上一个、每个控制器上一个。Location LEDs remain illuminated for 30 minutes.

您可以输入命令将其关闭 `system location-led *off*`。如果您不确定LED是亮起还是熄灭、可以输入命令来检查其状态 `system location-led show`。

第 1 步：卸下控制器

在更换控制器或更换控制器内部的组件时、必须从机箱中卸下控制器。

开始之前

确保存储系统中的所有其他组件均正常运行；否则、您必须先联系、 "NetApp 支持"然后再继续此过程。

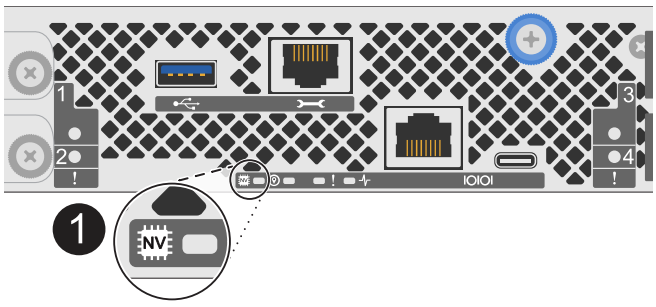
步骤

1. 在受损控制器上、确保NV LED熄灭。

   当NV LED熄灭时、转销已完成、可以安全地卸下受损控制器。

   如果NV LED闪烁(绿色)、则表示正在进行减载。您必须等待NV LED熄灭。但是、如果闪烁持续时间超过五分钟、请先联系、 "NetApp 支持"然后再继续此过程。

   NV LED位于控制器上的NV图标旁边。



1	控制器上的NV图标和LED

在安装和维护过程中，请始终佩戴连接到已验证接地点的接地腕带。未遵循正确的 ESD 预防措施可能会对控制器节点、存储架和网络交换机造成永久性损坏。

1. 断开受损控制器的电源：

   电源(PSU)没有电源开关。

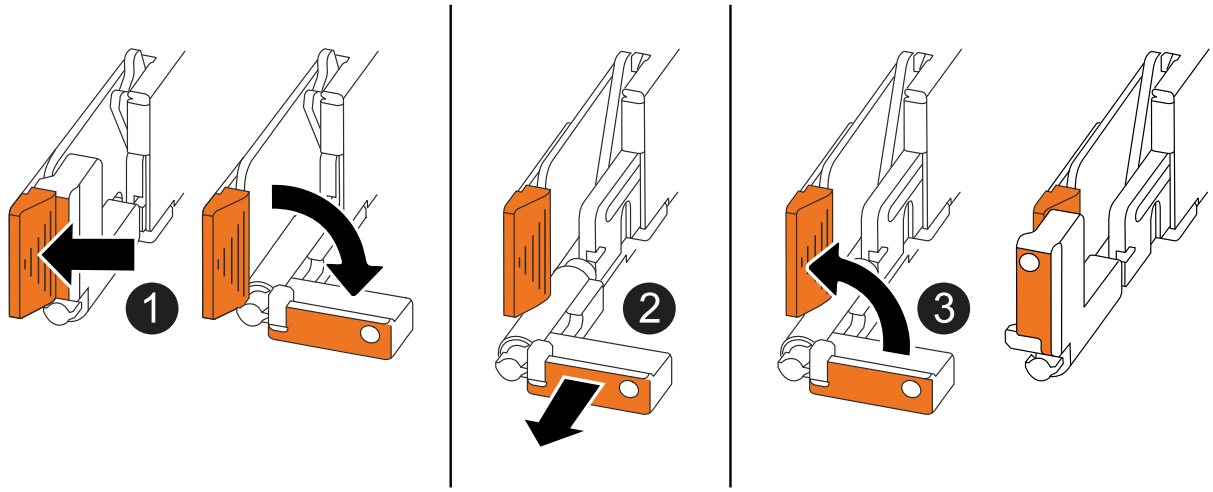
如果您要断开...	那么 ...
交流PSU	a. 打开电源线固定器。 b. 从PSU上拔下电源线、并将其放在一旁。
直流PSU	a. 拧下D-sub直流电源线连接器上的两颗指旋螺钉。 b. 从PSU上拔下电源线、并将其放在一旁。

2. 从受损控制器上拔下所有缆线。

   跟踪电缆的连接位置。

3. 删除受损控制器：

   下图显示了卸下控制器时控制器手柄(从控制器左侧开始)的操作：



1	在控制器的两端、向外推垂直锁定卡舌以释放手柄。
2	• 朝您的方向拉动手柄、将控制器从中间板上取下。 拉动时、手柄会从控制器中伸出、然后您会感觉到一些阻力、请继续拉动。 • 将控制器滑出机箱、同时支撑控制器底部、然后将其放在平稳的表面上。

3	如果需要、竖直旋转手柄(位于卡舌旁边)以将其移开。

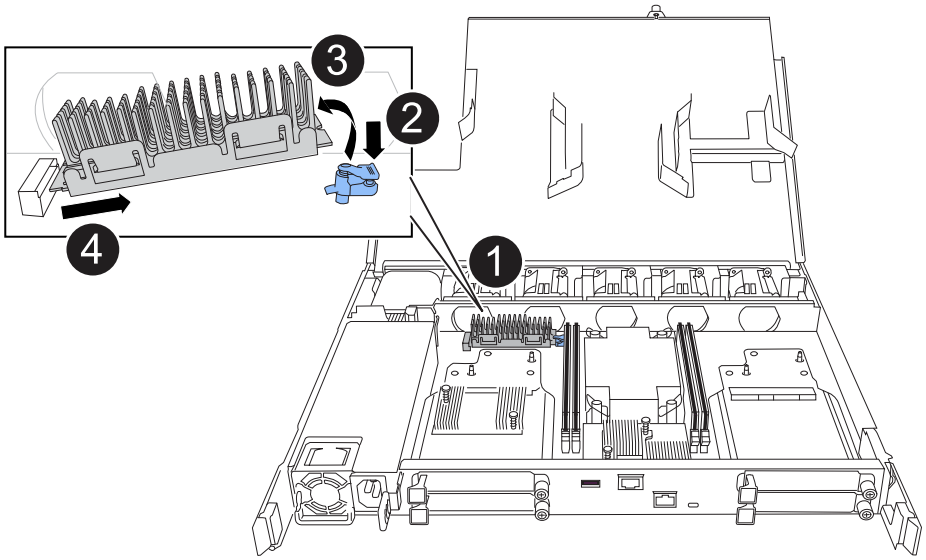
4. 将控制器放在防静电垫上。
5. 逆时针旋转指旋螺钉以打开控制器护盖、然后打开护盖。

第 2 步：更换启动介质

要更换启动介质、请在控制器内找到它、然后按照特定的步骤顺序进行操作。

在安装和维护过程中，请始终佩戴连接到已验证接地点的接地腕带。未遵循正确的 ESD 预防措施可能会对控制器节点、存储架和网络交换机造成永久性损坏。

1. 删除启动介质：



1	启动介质位置
2	按下蓝色卡舌以释放启动介质的右端。
3	轻轻向上提起引导介质的右端，以便沿着引导介质的两侧获得良好的抓持力。
4	轻轻地将引导介质的左端从插槽中拉出。

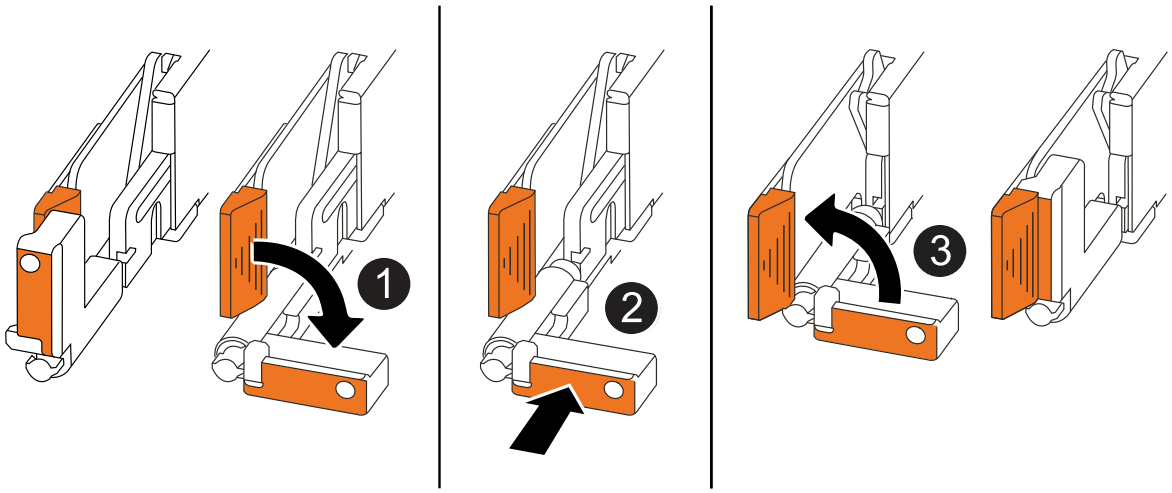
2. 安装替代启动介质：
   a. 从启动介质的软件包中取出启动介质。
   b. 将启动介质的插槽端滑入其插槽。
   c. 在启动介质的另一端、按住蓝色卡舌(处于打开位置)、轻轻向下推启动介质的那一端、直到其停止、然后释放卡舌以将启动介质锁定到位。

Step 3: Reinstall the controller

将控制器重新安装到机箱中、但不要重新启动它。

关于此任务

下图显示了重新安装控制器时控制器手柄(从控制器左侧开始)的操作、可用作其余控制器重新安装步骤的参考。



1	如果在维修控制器时竖直旋转控制器手柄(卡舌旁边)以使其移出、请将其向下旋转至水平位置。
2	将手柄推至一半以将控制器重新插入机箱、然后在系统提示时按、直至控制器完全就位。
3	将手柄旋转至竖直位置、并使用锁定卡舌锁定到位。

步骤

1. 合上控制器护盖、然后顺时针旋转指旋螺钉、直到拧紧为止。
2. 将控制器插入机箱一半。

   将控制器背面与机箱中的开口对齐、然后使用手柄轻轻推动控制器。

   请勿将控制器完全插入机箱、除非此过程稍后指示您这样做。

3. 将缆线重新连接到控制器；但是、此时请勿将电源线插入电源(PSU)。

   确保控制台电缆已连接到控制器、因为您希望稍后在将控制器完全装入机箱并开始启动时、在启动介质更换过程中捕获并记录启动顺序。

Step 4: Transfer the boot image to the boot media

您安装的替代启动介质没有ONTAP映像、因此您需要使用USB闪存驱动器传输ONTAP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 。
- 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。
- 您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闪存驱动器插入受损控制器上的USB-A端口。

   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. 将受损控制器完全装入机箱：
   a. 用力推动手柄、直至控制器与中板接触并完全就位。

      将控制器滑入机箱时、请勿用力过度、否则可能会损坏连接器。

      控制器在完全插入机箱后启动。它从配对控制器获得电源。
   a. 向上旋转控制器手柄、并使用卡舌锁定到位。
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. 将电源线重新连接到受损控制器上的电源(PSU)。

   在PSU恢复供电后、状态LED应为绿色。

如果您要重新连接...	那么 ...
交流PSU	a. 将电源线插入PSU。 b. 使用电源线固定器固定电源线。

如果您要重新连接...	那么 ...
直流PSU	a. 将D-sub直流电源线连接器插入PSU。 b. 拧紧两颗指旋螺钉、将D-sub直流电源线连接器固定至PSU。

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 A20、 AFF A30 和AFF A50

在AFF A20、 AFF A30 或AFF A50 存储系统中安装新的启动介质设备后，您可以从 USB 驱动器手动启动恢复映像以从合作伙伴节点恢复配置。

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"。

手动启动恢复后恢复加密密钥 - AFF A20、 AFF A30 和AFF A50

在AFF A20、 AFF A30 或AFF A50 存储系统中的替换启动介质上恢复加密，以确保持续的数据保护。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。

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	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. 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。

显示示例提示符

```
Enter the backup data:

--------------------------BEGIN
BACKUP--------------------------
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
34567890123456789012345678901234567890123456789012345678901234
56
45678901234567890123456789012345678901234567890123456789012345
67
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
01234567890123456789012345678901234567890123456789012345678901
23
12345678901234567890123456789012345678901234567890123456789012
34
23456789012345678901234567890123456789012345678901234567890123
45
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
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器信息：

   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"。

将故障部件退回给NetApp - AFF A20、AFF A30和AFF A50

如果您的AFF A20、 AFF A30 或AFF A50 存储系统中的某个组件发生故障，请将故障部件退回NetApp。请参阅 "部件退回和更换"页面以获取更多信息。