



启动介质

Install and maintain

NetApp
February 19, 2025

目录

启动介质	1
启动介质更换 workflow- AFF A20、AFF A30和AFF A50	1
启动介质更换要求- AFF A20、AFF A30和AFF A50	1
检查板载加密密钥- AFF A20、AFF A30和AFF A50	2
关闭受损控制器- AFF A20、AFF A30和AFF A50	5
更换启动介质- AFF A20、AFF A30和AFF A50	6
启动恢复映像- AFF A20、AFF A30和AFF A50	11
恢复加密- AFF A20、AFF A30和AFF A50	13
将故障部件退回给NetApp - AFF A20、AFF A30和AFF A50	22

启动介质

启动介质更换工作流程- AFF A20、AFF A30和AFF A50

按照以下工作流程步骤更换启动介质。

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"

验证存储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"

从受损控制器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- AFF A20、AFF A30和AFF A50

在更换启动介质之前、请务必查看以下要求和注意事项。

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。
- 您必须使用与提供商提供的容量相同的替代FRU组件来更换故障组件。

注意事项

- 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。
- 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`。

检查板载加密密钥- **AFF A20**、**AFF A30**和**AFF A50**

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"> • 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	<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 "NetApp 支持"。</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。"关闭受损控制器"</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。"关闭受损控制器"</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 "NetApp 支持"。</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。 "关闭受损控制器"</p>

关闭受损控制器- AFF A20、AFF A30和AFF A50

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 <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> 。

更换启动介质- AFF A20、AFF A30和AFF A50

要更换启动介质、您必须卸下受损控制器、卸下启动介质、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

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

存储系统中的所有其他组件都必须正常运行；否则、您必须先联系、["NetApp 支持"](#)然后再继续此过程。

步骤

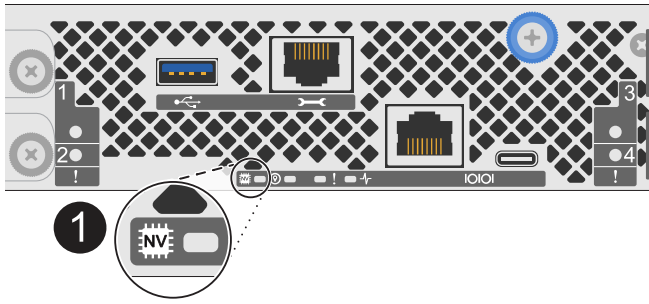
1. 在受损控制器上、确保NV LED熄灭。

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

1. 如果您尚未接地，请正确接地。
2. 断开受损控制器的电源：

i 电源(PSU)没有电源开关。

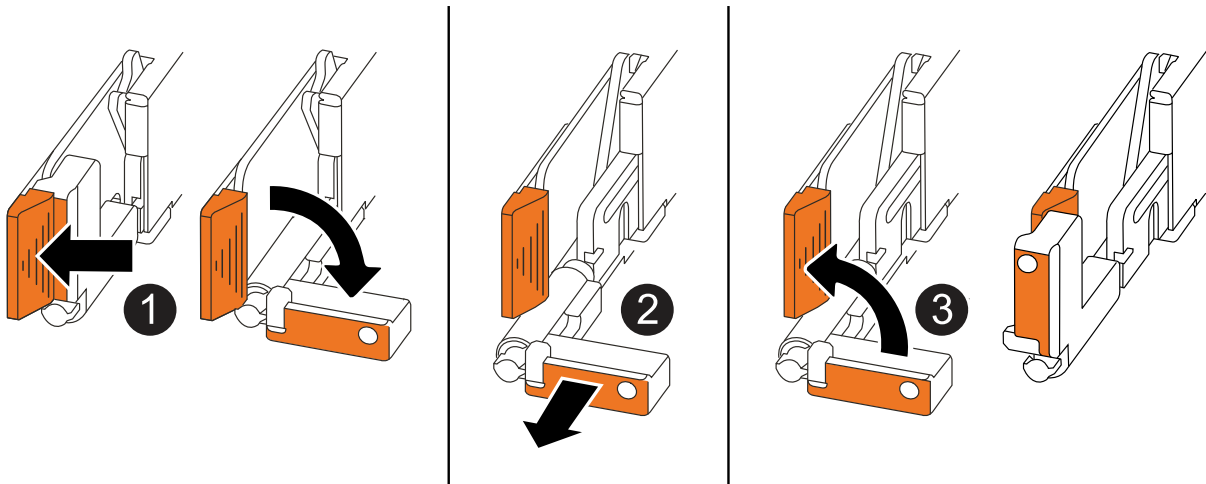
如果您要断开...	那么 ...
交流PSU	<ol style="list-style-type: none"> a. 打开电源线固定器。 b. 从PSU上拔下电源线、并将其放在一旁。
直流PSU	<ol style="list-style-type: none"> a. 拧下D-sub直流电源线连接器上的两颗指旋螺钉。 b. 从PSU上拔下电源线、并将其放在一旁。

3. 从受损控制器上拔下所有缆线。

跟踪电缆的连接位置。

4. 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：



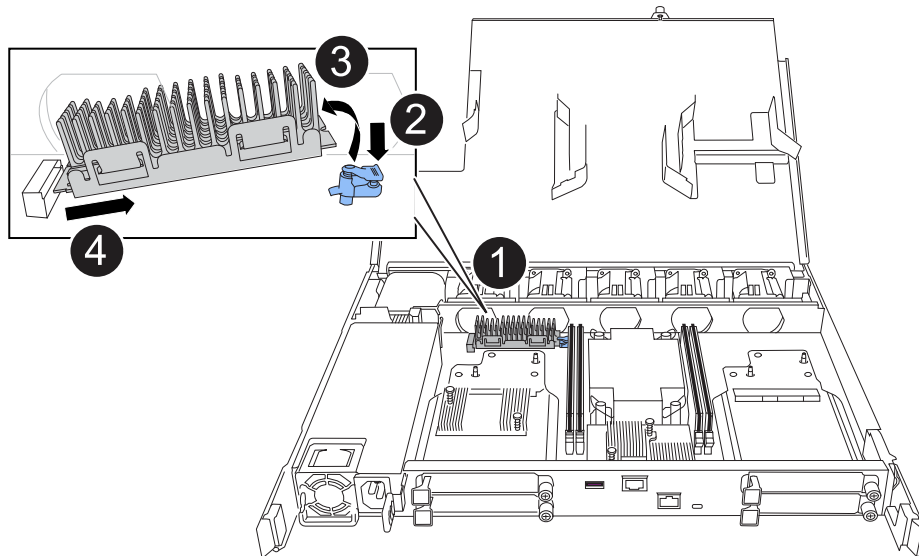
<p>1</p>	<p>在控制器的两端、向外推垂直锁定卡舌以释放手柄。</p>
<p>2</p>	<ul style="list-style-type: none"> 朝您的方向拉动手柄、将控制器从中间板上取下。 <p>拉动时、手柄会从控制器中伸出、然后您会感觉到一些阻力、请继续拉动。</p> <ul style="list-style-type: none"> 将控制器滑出机箱、同时支撑控制器底部、然后将其放在平稳的表面上。
<p>3</p>	<p>如果需要、竖直旋转手柄(位于卡舌旁边)以将其移开。</p>

5. 将控制器放在防静电垫上。
6. 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。

1. 如果您尚未接地，请正确接地。
2. 删除启动介质：



<p>1</p>	<p>启动介质位置</p>
<p>2</p>	<p>按下蓝色卡舌以释放启动介质的右端。</p>
<p>3</p>	<p>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。</p>
<p>4</p>	<p>轻轻地将引导介质的左端从插槽中拉出。</p>

3. 安装替代启动介质：

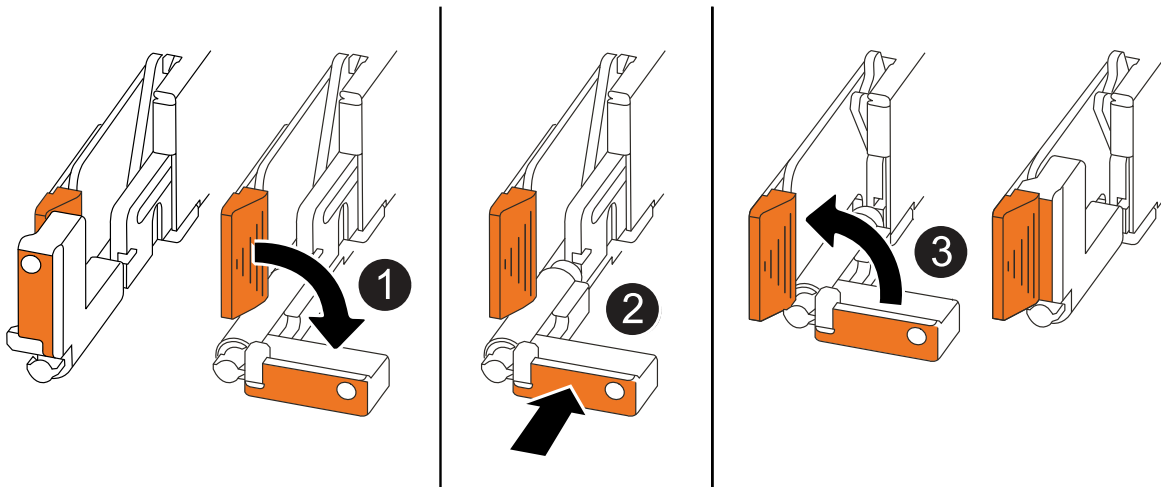
- a. 从启动介质的软件包中取出启动介质。
- b. 将启动介质的插槽端滑入其插槽。
- c. 在启动介质的另一端、按住蓝色卡舌(处于打开位置)、轻轻向下推启动介质的那一端、直到其停止、然后释放卡舌以将启动介质锁定到位。

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. 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, 可以在固件提示符处输入 `help ifconfig`。

6. 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。
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。

启动恢复映像- AFF A20、AFF A30和AFF A50

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- AFF A20、AFF A30和AFF A50

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 data-bbox="683 464 1133 493">(2) Boot without /etc/rc.<li data-bbox="683 506 1045 535">(3) Change password.<li data-bbox="683 548 1365 611">(4) Clean configuration and initialize all disks.<li data-bbox="683 623 1149 653">(5) Maintenance mode boot.<li data-bbox="683 665 1328 695">(6) Update flash from backup config.<li data-bbox="683 707 1240 737">(7) Install new software first.<li data-bbox="683 749 976 779">(8) Reboot node.<li data-bbox="683 791 1192 854">(9) Configure Advanced Drive Partitioning.<li data-bbox="683 867 1333 930">(10) Set Onboard Key Manager recovery secrets.<li data-bbox="683 942 1317 1005">(11) Configure node for external key management.<p data-bbox="683 1026 1032 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 data-bbox="656 310 1455 970" 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

```
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、输入客户端和服务端信息。

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-----
<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....
kmp_init: configuring ports
Running command '/sbin/ifconfig e0M'
..
..
kmp_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....
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
```

6. 如果禁用了自动交还、请还原它。

```
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 - AFF A20、AFF A30和AFF A50

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 © 2025 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。