启动介质
Install and maintain

NetApp
February 13, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/ontap-systems/fas8200/bootmedia-replace-overview.html on February 13, 2026. Always check docs.netapp.com for the latest.

目录

启动介质 . . . 1
启动介质更换概述— FAS8200 . . . 1
检查加密密钥支持和状态- FAS8200 . . . 1
步骤 1：检查 NVE 支持并下载正确的ONTAP映像 . . . 1
步骤 2：验证密钥管理器状态并备份配置 . . . 2
关闭受损控制器— FAS8200 . . . 4
选项 1： 大多数系统 . . . 4
选项 1： 大多数系统 . . . 5
选项 2： 控制器采用 MetroCluster 配置 . . . 5
选项 3： 控制器位于双节点 MetroCluster 中 . . . 6
更换启动介质— FAS8200 . . . 7
第 1 步：卸下控制器 . . . 8
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 . . . 10
启动恢复映像— FAS8200 . . . 11
选项 1： 大多数系统 . . . 11
选项 2： 控制器位于双节点 MetroCluster 中 . . . 13
切回双节点 MetroCluster 配置中的聚合— FAS8200 . . . 13
还原加密- FAS8200 . . . 15
将故障部件退回给 NetApp - FAS8200 . . . 25

启动介质

启动介质更换概述— FAS8200

了解FAS8200系统上的启动介质更换，并了解不同的更换方法。启动介质存储系统启动时使用的主启动映像文件和辅助启动映像文件。根据您的网络配置，您可以执行非中断式更换（HA 对连接到网络）或中断式更换（需要重启两次）。

FAS8200系统仅支持手动启动介质恢复程序。不支持自动启动介质恢复。

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- FAS8200

在关闭FAS8200系统上出现故障的控制器之前，请验证加密密钥支持和状态。此过程包括检查ONTAP版本与NetApp卷加密 (NVE) 的兼容性、验证密钥管理器配置以及备份加密信息，以确保在启动介质恢复期间的数据安全。

FAS8200系统仅支持手动启动介质恢复程序。不支持自动启动介质恢复。

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	`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。

关闭受损控制器— FAS8200

选项 1 ： 大多数系统

完成加密检查后，关闭FAS8200系统上出现故障的控制器。此过程包括将控制器带到 LOADER 提示符，捕获启动环境变量以供参考，以及准备控制器以更换启动介质，具体步骤因系统配置而异。

FAS8200系统仅支持手动启动介质恢复程序。不支持自动启动介质恢复。

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： `storage failover takeover -ofnode impaired_node_name` 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： 控制器采用 MetroCluster 配置

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。
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： `storage failover takeover -ofnode` *`impaired_node_name`* 当受损控制器显示 Waiting for giveback… 时，按 Ctrl-C ，然后回答 `y` 。

选项 3： 控制器位于双节点 MetroCluster 中

要关闭受损控制器，您必须确定控制器的状态，并在必要时切换控制器，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

- 您必须在此操作步骤 末尾保持电源处于打开状态，以便为运行正常的控制器供电。

步骤

1. 检查 MetroCluster 状态以确定受损控制器是否已自动切换到运行正常的控制器： `MetroCluster show`
2. 根据是否发生了自动切换，按照下表继续操作：

如果控制器受损 ...	那么 ...
已自动切换	继续执行下一步。
未自动切换	从运行正常的控制器执行计划内切换操作： `MetroCluster switchover`
未自动切换，您尝试使用 `MetroCluster switchover` 命令进行切换，并且切换已被否决	查看否决消息，如果可能，请解决问题描述并重试。如果无法解决问题描述问题，请联系技术支持。

3. 在运行正常的集群中运行 `MetroCluster heal -phase aggregates` 命令，以重新同步数据聚合。

```
controller_A_1::> metrocluster heal -phase aggregates
[Job 130] Job succeeded: Heal Aggregates is successful.
```

如果修复被否决，您可以使用 ` override-vetoes` 参数重新发出 `MetroCluster heal` 命令。如果使用此可选参数，则系统将覆盖任何阻止修复操作的软否决。

4. 使用 MetroCluster operation show 命令验证操作是否已完成。

```
controller_A_1::> metrocluster operation show
    Operation: heal-aggregates
      State: successful
Start Time: 7/25/2016 18:45:55
   End Time: 7/25/2016 18:45:56
     Errors: -
```

5. 使用 `storage aggregate show` 命令检查聚合的状态。

```
controller_A_1::> storage aggregate show
Aggregate     Size Available Used% State   #Vols  Nodes            RAID
Status
--------- -------- --------- ----- ------- ------ ----------------
------------
...
aggr_b2    227.1GB   227.1GB    0% online       0 mcc1-a2
raid_dp, mirrored, normal...
```

6. 使用 `MetroCluster heal -phase root-aggregates` 命令修复根聚合。

```
mcc1A::> metrocluster heal -phase root-aggregates
[Job 137] Job succeeded: Heal Root Aggregates is successful
```

如果修复被否决，您可以使用 -override-vetoes 参数重新发出 `MetroCluster heal` 命令。如果使用此可选参数，则系统将覆盖任何阻止修复操作的软否决。

7. 在目标集群上使用 `MetroCluster operation show` 命令验证修复操作是否已完成：

```
mcc1A::> metrocluster operation show
  Operation: heal-root-aggregates
      State: successful
 Start Time: 7/29/2016 20:54:41
   End Time: 7/29/2016 20:54:42
     Errors: -
```

8. 在受损控制器模块上，断开电源。

更换启动介质— FAS8200

更换FAS8200控制器模块上故障的启动介质。此过程包括从机箱中取出控制器模块，物理更换启动介质组件，使用 USB 闪存驱动器将启动映像传输到更换的介质，以及将系统恢复到正常运行状态。

FAS8200系统仅支持手动启动介质恢复程序。不支持自动启动介质恢复。

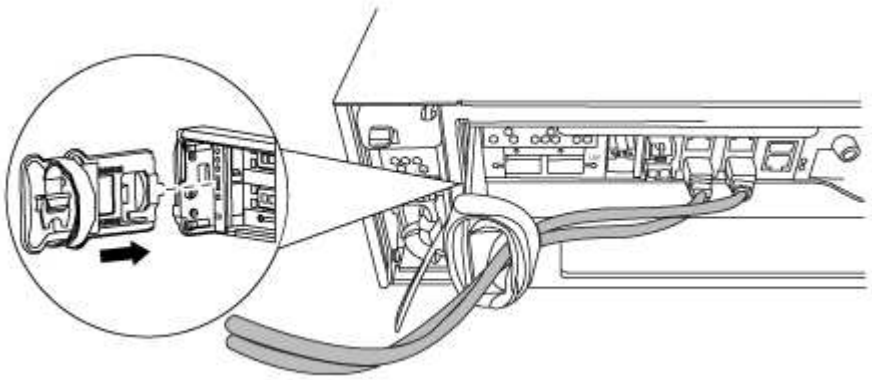
第 1 步：卸下控制器

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。

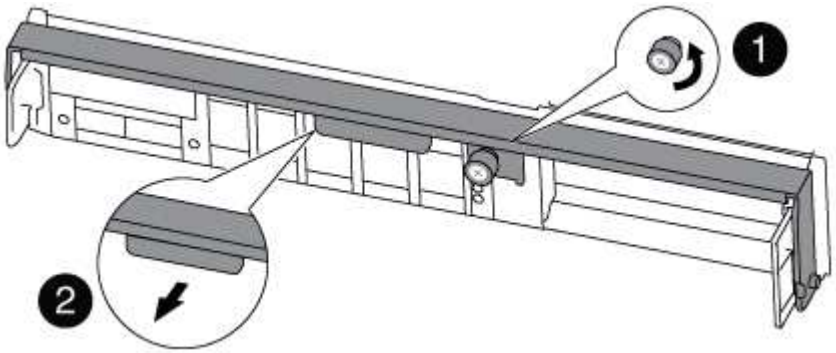
1. 如果您尚未接地，请正确接地。
2. 松开将缆线绑在缆线管理设备上的钩环带，然后从控制器模块上拔下系统缆线和 SFP （如果需要），并跟踪缆线的连接位置。

   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。

3. 从控制器模块的左右两侧卸下缆线管理设备并将其放在一旁。



4. 松开控制器模块凸轮把手上的翼形螺钉。



1	
翼形螺钉	
2	
凸轮把手	

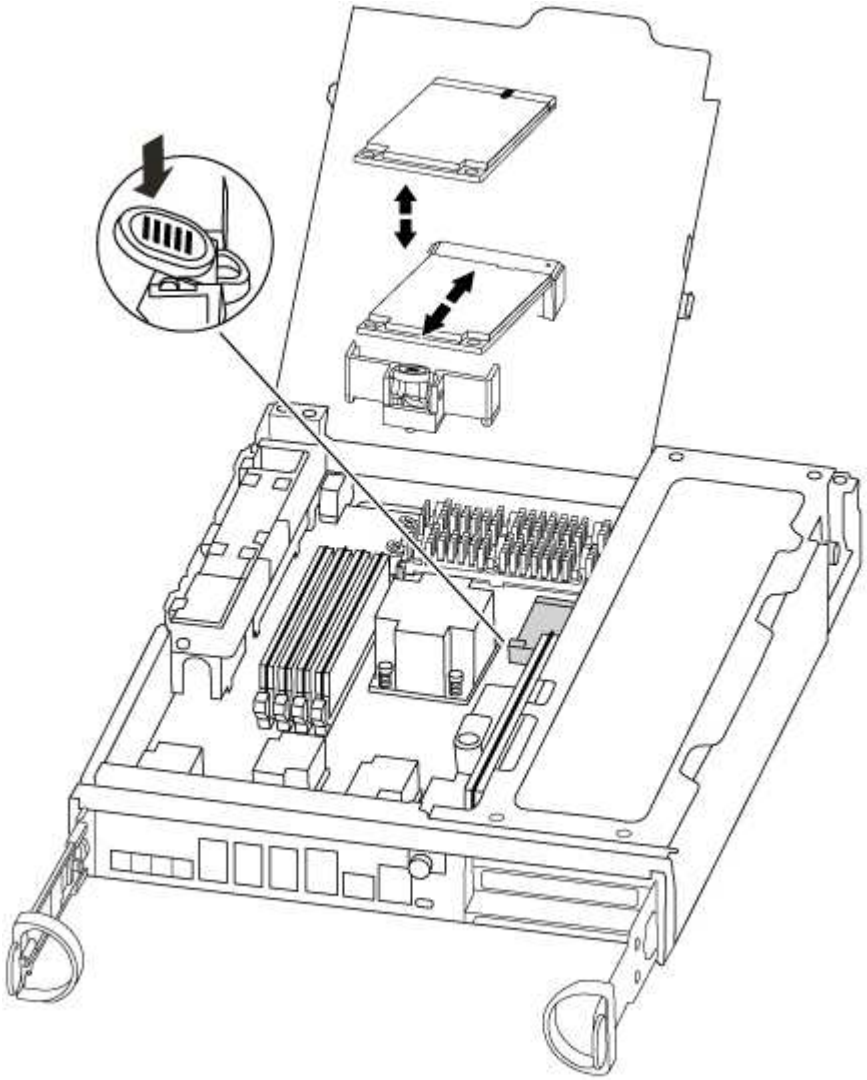
5. 向下拉凸轮把手，开始将控制器模块滑出机箱。

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。

第 2 步：更换启动介质

您必须在控制器中找到启动介质并按照说明进行更换。

1. 如果您尚未接地，请正确接地。
2. 使用下图或控制器模块上的 FRU 映射找到启动介质：



3. 按启动介质外壳上的蓝色按钮，将启动介质从其外壳中释放，然后将其竖直拉出启动介质插槽。

   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。

4. 将替代启动介质的边缘与启动介质插槽对齐，然后将其轻轻推入插槽。
5. 检查启动介质，确保其完全固定在插槽中。

   如有必要，请取出启动介质并将其重新插入插槽。

6. 向下推启动介质以接合启动介质外壳上的锁定按钮。

7. 合上控制器模块外盖。

第 3 步：将启动映像传输到启动介质

您可以使用已安装映像的 USB 闪存驱动器将系统映像安装到替代启动介质。但是，您必须在此操作步骤期间还原 var 文件系统。

- 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 。

> tar.gz文件必须放置在至少4 GB的32位格式化分区上。虽然32 TB分区的大小可以达到2 TB、但Windows内置工具(例如diskpart)无法格式化32 GB以上的32 GB分区。

- 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。

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 ），请务必重新安装它们。

c. 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。

d. 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。

e. 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。

f. 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。

g. 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` 。

h. 如果控制器位于延伸型或光纤连接的 MetroCluster 中，则必须还原 FC 适配器配置：
   i. 启动到维护模式： `boot_ontap maint`
   ii. 将 MetroCluster 端口设置为启动程序： `ucadmin modify -m fc -t initiator adapter_name`
   iii. halt 返回维护模式： `halt`

这些更改将在系统启动时实施。

启动恢复映像— FAS8200

在FAS8200系统上，从 USB 驱动器启动ONTAP恢复映像，以恢复启动介质。该过程包括从 USB 闪存驱动器启动、恢复文件系统、验证环境变量以及使控制器恢复正常运行，具体步骤取决于系统是否处于双节点MetroCluster配置中。

FAS8200系统仅支持手动启动介质恢复程序。不支持自动启动介质恢复。

选项 1： 大多数系统

：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。

此操作步骤适用场景系统不采用双节点 MetroCluster 配置。

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：

如果您的系统 ...	那么 ...
网络连接	a. 当系统提示您还原备份配置时，按 `y` 。 b. 将运行状况良好的控制器设置为高级权限级别： `set -privilege advanced` c. 运行 restore backup 命令： `ssystem node restore-backup -node local -target-address` *`impaired_node_ip_address`* d. 将控制器恢复为管理员级别： `set -privilege admin` e. 当系统提示您使用已还原的配置时，按 `y` 。 f. 在系统提示重新启动控制器时，按 `y` 。
无网络连接	a. 当系统提示您还原备份配置时，按 `n` 。 b. 系统提示时重新启动系统。 c. 从显示的菜单中选择 * 从备份配置更新闪存 * （同步闪存）选项。 如果系统提示您继续更新，请按 `y` 。

4. 确保环境变量按预期设置：
   a. 将控制器显示 LOADER 提示符。
   b. 使用 `printenv` 命令检查环境变量设置。
   c. 如果环境变量未按预期设置，请使用 `setenv` *`environment-variable-name____changed-value`* 命令对其进行修改。
   d. 使用 `savenv` 命令保存所做的更改。
5. 下一个取决于您的系统配置：
   - 如果您的系统配置了板载密钥管理器， NSE 或 NVE ，请转至 根据需要还原 OKM ， NSE 和 NVE
   - 如果您的系统未配置板载密钥管理器， NSE 或 NVE ，请完成本节中的步骤。
6. 在 LOADER 提示符处，输入 `boot_ontap` 命令。

如果您看到 ...	那么 ...
登录提示符	转至下一步。
正在等待交还	a. 登录到配对控制器。 b. 使用 `storage failover show` 命令确认目标控制器已准备好进行交还。

7. 将控制台缆线连接到配对控制器。
8. 使用 `storage failover giveback -fromnode local` 命令交还控制器。

9. 在集群提示符处，使用 `net int -is-home false` 命令检查逻辑接口。

   如果任何接口列为 "false" ，请使用 `net int revert` 命令将这些接口还原回其主端口。

10. 将控制台缆线移至已修复的控制器，然后运行 `version -v` 命令以检查 ONTAP 版本。
11. 使用 `storage failover modify -node local -auto-giveback true` 命令禁用自动交还后，可将其还原。

选项 2： 控制器位于双节点 MetroCluster 中

您必须从 USB 驱动器启动 ONTAP 映像并验证环境变量。

此操作步骤适用场景系统采用双节点 MetroCluster 配置。

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. 安装映像后，启动还原过程：
   a. 当系统提示您还原备份配置时，按 `n` 。
   b. 当系统提示您重新启动时，按 `y` 开始使用新安装的软件。

      系统提示时，您应准备好中断启动过程。

4. 在系统启动时，在看到 `Press Ctrl-C for Boot Menu` 消息后按 `Ctrl-C` ，并在显示 Boot Menu 时选择选项 6 。
5. 验证环境变量是否按预期设置。
   a. 使节点显示 LOADER 提示符。
   b. 使用 `printenv` 命令检查环境变量设置。
   c. 如果环境变量未按预期设置，请使用 `setenv` *`environment-variable-name____changed-value`* 命令对其进行修改。
   d. 使用 `savenv` 命令保存所做的更改。
   e. 重新启动节点。

切回双节点 MetroCluster 配置中的聚合— FAS8200

在双节点MetroCluster配置中完成启动介质更换后，对FAS8200系统执行MetroCluster切换回操作。此过程包括验证节点和存储虚拟机 (SVM) 的状态，执行回退命令，并确认配置恢复到正常运行状态，同步源 SVM 从本地磁盘池提供数据。

FAS8200系统仅支持手动启动介质恢复程序。不支持自动启动介质恢复。

此任务仅限适用场景双节点 MetroCluster 配置。

步骤

1. 验证所有节点是否处于 enabled 状态： MetroCluster node show

```
cluster_B::>  metrocluster node show

DR                           Configuration  DR
Group Cluster Node           State          Mirroring Mode
----- ------- -------------- -------------- ---------
--------------------
1     cluster_A
              controller_A_1 configured     enabled   heal roots
completed
      cluster_B
              controller_B_1 configured     enabled   waiting for
switchback recovery
2 entries were displayed.
```

2. 验证所有 SVM 上的重新同步是否已完成： MetroCluster SVM show
3. 验证修复操作正在执行的任何自动 LIF 迁移是否已成功完成： MetroCluster check lif show
4. 在运行正常的集群中的任何节点上使用 MetroCluster switchback 命令执行切回。
5. 验证切回操作是否已完成： MetroCluster show

   当集群处于 waiting for-switchback 状态时，切回操作仍在运行：

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured        switchover
Remote: cluster_A configured        waiting-for-switchback
```

   当集群处于 normal 状态时，切回操作完成。：

```
cluster_B::> metrocluster show
Cluster              Configuration State    Mode
--------------------    -------------------     ---------
 Local: cluster_B configured            normal
Remote: cluster_A configured            normal
```

   如果切回需要很长时间才能完成，您可以使用 MetroCluster config-replication resync-status show 命令检查正在进行的基线的状态。

6. 重新建立任何 SnapMirror 或 SnapVault 配置。

还原加密- FAS8200

在FAS8200系统的替换启动介质上恢复加密配置。此流程包括完成已启用板载密钥管理器(OKM)、 NetApp存储加密 (NSE) 或NetApp卷加密 (NVE) 的系统更换后的步骤，以确保安全的数据访问和系统的正常运行。

FAS8200系统仅支持手动启动介质恢复程序。不支持自动启动介质恢复。

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
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
```

```
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
   ```

将故障部件退回给 NetApp - FAS8200

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。

FAS8200系统仅支持手动启动介质恢复程序。不支持自动启动介质恢复。

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，本文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。