启动介质
Install and maintain

NetApp
February 20, 2026

目录

启动介质

启动介质更换工作流- ASA A20、ASA A30和ASA A50

通过查看更换要求、关闭受损控制器、更换启动介质、还原启动介质上的映像以及验证系统功能、开始更换ASA A30、ASA A20或ASA A50存储系统中的启动介质。

1. "查看启动介质要求"

查看更换启动介质的要求。

2. **"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。

3. "更换启动介质"

从受损控制器中取出故障启动介质、然后安装替代启动介质。

4. "还原启动介质上的映像"

从运行正常的控制器还原ONTAP映像。

5. "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 。

更换启动介质的要求- ASA A20、ASA A30和ASA A50

在更换ASA A20、 ASA A30 或ASA A50 存储系统中的启动介质之前，请确保满足成功更换所需的要求和注意事项。这包括验证您是否拥有正确的替换启动介质、确认受损控制器上的 e0M（扳手）端口是否正常工作，以及确定是否启用了板载密钥管理器 (OKM) 或外部密钥管理器 (EKM)。

查看以下要求。

- 您必须使用与从NetApp收到的容量相同的替代FRU组件来更换故障组件。
- 验证受损控制器上的 e0M（扳手）端口是否已连接且没有故障。

  e0M 端口用于在自动启动恢复过程中在两个控制器之间进行通信。

- 对于 OKM，您需要集群范围的密码以及备份数据。
- 对于EMM、您需要配对节点上以下文件的副本：

- /cfcard/kmip/servers.cfg文件。
- /cfcard/kmip/certs/client.crt文件。
- /cfcard/kmip/certs client.key文件。
- /cfcard/kmip/certs或CA.prom文件。

- 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。

下一步行动

查看引导介质要求后，您可以"关闭受损控制器"。

关闭控制器以更换启动介质- ASA A20、ASA A30和ASA A50

在更换启动介质时、关闭ASA A20、ASA A30或ASA A50存储系统中的受损控制器、以防止数据丢失并确保系统稳定性。

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。

下一步行动

关闭受损控制器后，您可以"更换启动介质"。

更换启动介质- ASA A20、ASA A30和ASA A50

ASA A20、 ASA A30 或ASA 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，然后重新安装控制器模块。

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。

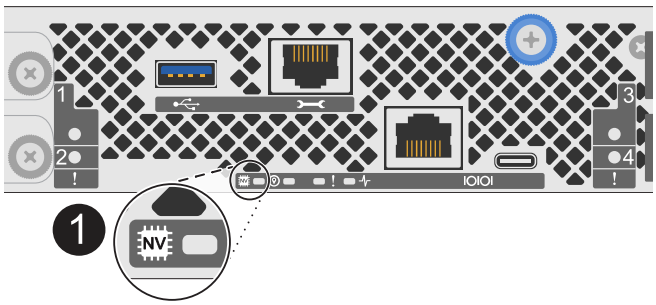
步骤

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。

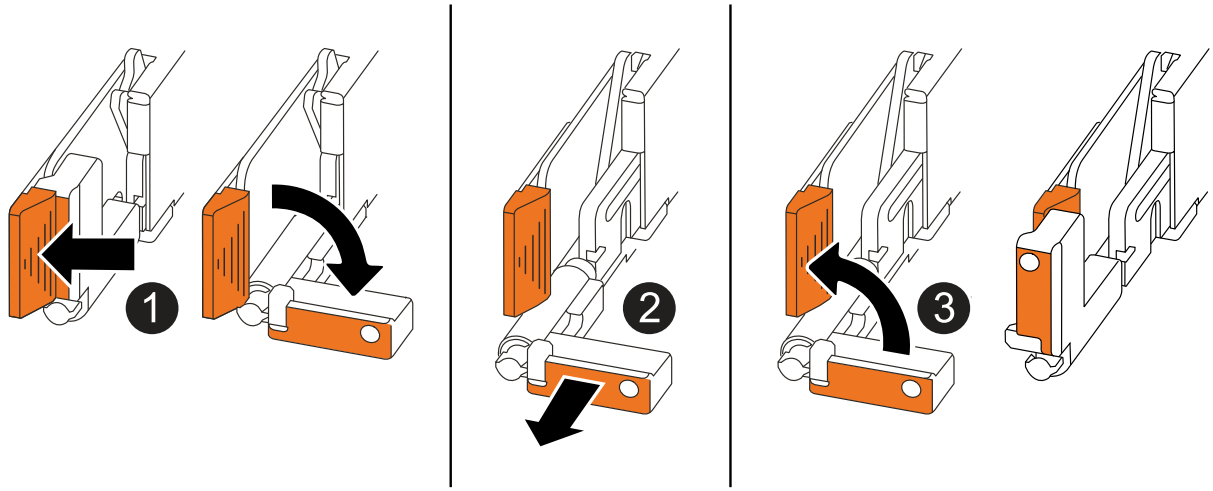
如果您要断开...	那么 ...
交流PSU	a. 打开电源线固定器。 b. 从PSU上拔下电源线、并将其放在一旁。
直流PSU	a. 拧下D-sub直流电源线连接器上的两颗指旋螺钉。 b. 从PSU上拔下电源线、并将其放在一旁。

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。

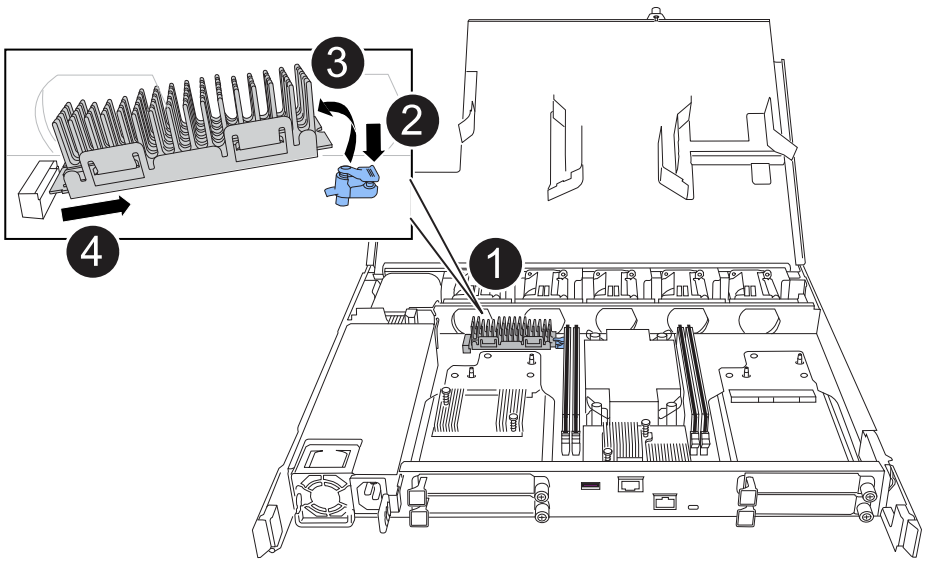
4. 将控制器放在防静电垫上。
5. 逆时针旋转指旋螺钉以打开控制器护盖、然后打开护盖。

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。

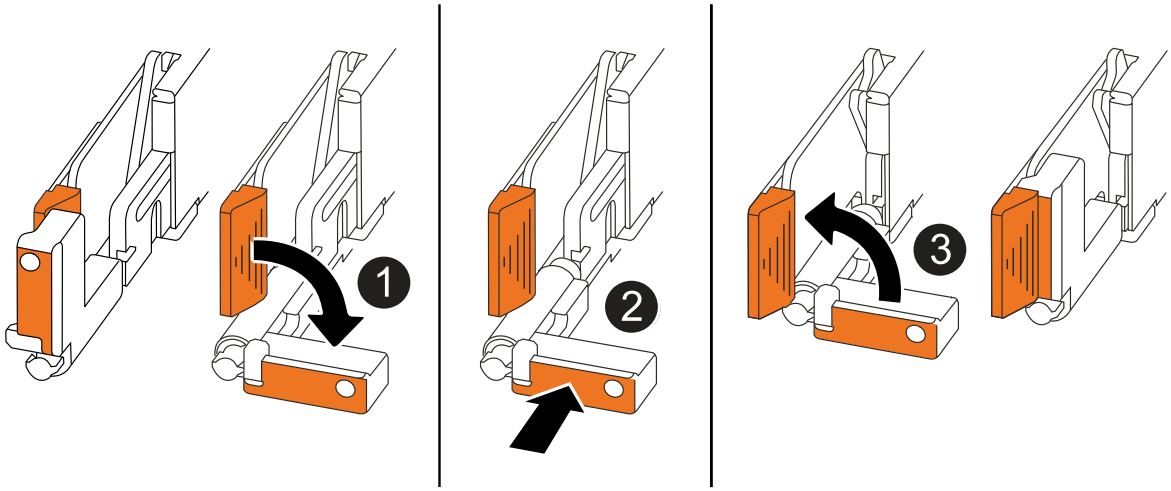
2. 安装替代启动介质：
   a. 从启动介质的软件包中取出启动介质。
   b. 将启动介质的插槽端滑入其插槽。
   c. 在启动介质的另一端、按住蓝色卡舌(处于打开位置)、轻轻向下推启动介质的那一端、直到其停止、然后释放卡舌以将启动介质锁定到位。

Step 3: Reinstall the controller

将控制器重新安装到机箱中并重新启动。

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。

4. 将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。

      完全插入机箱后、控制器将启动至Loader提示符。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。

5. 将电源线重新连接到受损控制器上的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。

下一步行动

在物理更换受损的启动介质后，您"从配对节点还原ONTAP映像" 。

还原启动介质上的ONTAP映像- ASA A20、ASA A30和ASA A50

在ASA A20、ASA A30或ASA A50存储系统中安装新的启动介质设备后、您可以启动自动启动介质恢复过程、以便从运行状况良好的节点还原配置。

在恢复过程中、系统会检查是否已启用加密、并确定所使用的密钥加密类型。如果启用了密钥加密、系统将指导您完成相应的还原步骤。

开始之前

- 确定您的密钥管理器类型：
  - 板载密钥管理器 (OKM)：需要集群范围的密码短语和备份数据
  - 外部密钥管理器 (EKM)：需要来自伙伴节点的以下文件：
    - `/cfcard/kmip/servers.cfg`
    - `/cfcard/kmip/certs/client.crt`
    - `/cfcard/kmip/certs/client.key`
    - `/cfcard/kmip/certs/CA.pem`

步骤

1. 在 LOADER 提示符下，启动启动介质恢复过程：

   ```
   boot_recovery -partner
   ```

   屏幕将显示以下消息：

   ```
   Starting boot media recovery (BMR) process. Press Ctrl-C to abort…
   ```

2. 监控启动介质安装恢复过程。

   此过程完成并显示 `Installation complete`消息。

3. 系统检查加密情况，并显示以下消息之一：

如果您看到此消息...	操作
`key manager is not configured. Exiting.`	系统未安装加密功能。 a. 等待登录提示出现。 b. 登录节点并归还存储空间： `storage failover giveback -ofnode impaired_node_name` c. 前往 重新启用自动返还功能 如果它被禁用了。
`key manager is configured.`	已安装加密功能。前往恢复密钥管理器。

如果系统无法识别密钥管理器配置，则会显示错误消息，并提示您确认是否已配置密钥管理器以及配置类型（板载或外部）。请回答提示以继续。

4. 使用适合您配置的相应过程还原密钥管理器：

板载密钥管理器（**OKM**）

系统显示以下消息并开始运行启动菜单选项 10：

```
key manager is configured.
Entering Bootmenu Option 10...

This option must be used only in disaster recovery procedures. Are
you sure? (y or n):
```

a. 进入 `y`在提示时确认您是否要开始 OKM 恢复过程。

b. 出现提示时，请输入机载密钥管理密码。

c. 出现确认提示时，请再次输入密码。

d. 出现提示时，输入车载密钥管理器的备份数据。

显示密码和备份数据提示的示例

```
Enter the passphrase for onboard key management:
-----BEGIN PASSPHRASE-----
<passphrase_value>
-----END PASSPHRASE-----
Enter the passphrase again to confirm:
-----BEGIN PASSPHRASE-----
<passphrase_value>
-----END PASSPHRASE-----
Enter the backup data:
-----BEGIN BACKUP-----
<passphrase_value>
-----END BACKUP-----
```

e. 监控恢复过程，看它如何从伙伴节点恢复相应的文件。

恢复过程完成后，节点将重新启动。以下信息表明恢复成功：

```
Trying to recover keymanager secrets....
Setting recovery material for the onboard key manager
Recovery secrets set successfully
Trying to delete any existing km_onboard.keydb file.

Successfully recovered keymanager secrets.
```

f. 节点重启后，验证系统是否恢复在线并正常运行。

g. 通过交还存储使受损控制器恢复正常运行：

```
storage failover giveback -ofnode impaired_node_name
```

h. 在伙伴节点完全启动并开始提供数据服务后，同步集群中的 OKM 密钥：

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

前往 重新启用自动返还功能 如果它被禁用了。

外部密钥管理器（ **EKM** ）

系统显示以下消息并开始运行启动菜单选项 11：

```
key manager is configured.
Entering Bootmenu Option 11...
```

a. 出现提示时，请输入EKM配置设置：

i. 请输入客户端证书的内容。 `/cfcard/kmip/certs/client.crt`文件：

显示客户端证书内容示例

```
-----BEGIN CERTIFICATE-----
<certificate_value>
-----END CERTIFICATE-----
```

ii. 请输入客户端密钥文件的内容。 `/cfcard/kmip/certs/client.key`文件：

显示客户端密钥文件内容的示例

```
-----BEGIN RSA PRIVATE KEY-----
<key_value>
-----END RSA PRIVATE KEY-----
```

iii. 从以下位置输入 KMIP 服务器 CA(s) 文件的内容： `/cfcard/kmip/certs/CA.pem`文件：

显示**KMIP**服务器文件内容示例

```
-----BEGIN CERTIFICATE-----
<KMIP_certificate_CA_value>
-----END CERTIFICATE-----
```

iv. 输入服务器配置文件内容 `/cfcard/kmip/servers.cfg`文件：

显示服务器配置文件内容示例

```
xxx.xxx.xxx.xxx:5696.host=xxx.xxx.xxx.xxx
xxx.xxx.xxx.xxx:5696.port=5696
xxx.xxx.xxx.xxx:5696.trusted_file=/cfcard/kmip/certs/CA.pem
xxx.xxx.xxx.xxx:5696.protocol=KMIP1_4
1xxx.xxx.xxx.xxx:5696.timeout=25
xxx.xxx.xxx.xxx:5696.nbio=1
xxx.xxx.xxx.xxx:5696.cert_file=/cfcard/kmip/certs/client.cr
t
xxx.xxx.xxx.xxx:5696.key_file=/cfcard/kmip/certs/client.key
xxx.xxx.xxx.xxx:5696.ciphers="TLSv1.2:kRSA:!CAMELLIA:!IDEA:
!RC2:!RC4:!SEED:!eNULL:!aNULL"
xxx.xxx.xxx.xxx:5696.verify=true
xxx.xxx.xxx.xxx:5696.netapp_keystore_uuid=<id_value>
```

v. 如果出现提示，请输入伙伴节点的ONTAP集群 UUID。您可以使用以下命令从伙伴节点检查集群 UUID： `cluster identify show`命令。

显示**ONTAP**集群 **UUID** 提示示例

```
Notice: bootarg.mgwd.cluster_uuid is not set or is empty.
Do you know the ONTAP Cluster UUID? {y/n} y
Enter the ONTAP Cluster UUID: <cluster_uuid_value>


System is ready to utilize external key manager(s).
```

vi. 如果出现提示，请输入节点的临时网络接口和设置：

- 端口的 IP 地址
- 端口的网络掩码
- 默认网关的 IP 地址

显示临时网络设置提示示例

```
In order to recover key information, a temporary network
interface needs to be
configured.

Select the network port you want to use (for example,
'e0a')
e0M

Enter the IP address for port : xxx.xxx.xxx.xxx
Enter the netmask for port : xxx.xxx.xxx.xxx
Enter IP address of default gateway: xxx.xxx.xxx.xxx
Trying to recover keys from key servers....
[discover_versions]
[status=SUCCESS reason= message=]
```

b. 验证密钥恢复状态：

- 如果你看到 `kmip2_client: Successfully imported the keys from external key server: xxx.xxx.xxx.xxx:5696`输出结果显示，EKM 配置已成功恢复。该过程从伙伴节点恢复相应的文件并重启节点。继续下一步。
- 如果密钥恢复失败，系统将停止运行并显示错误和警告信息。从 LOADER 提示符重新运行恢复过程： `boot_recovery -partner`

显示密钥恢复错误和警告消息的示例

```
ERROR: kmip_init: halting this system with encrypted
mroot...
WARNING: kmip_init: authentication keys might not be
available.
*****************************************************
*                  A T T E N T I O N                  *
*                                                     *
*       System cannot connect to key managers.        *
*                                                     *
*****************************************************
ERROR: kmip_init: halting this system with encrypted
mroot...
.
Terminated

Uptime: 11m32s
System halting...

LOADER-B>
```

c. 节点重启后，验证系统是否恢复在线并正常运行。

d. 通过交还存储使控制器恢复正常运行：

```
storage failover giveback -ofnode impaired_node_name
```

前往 重新启用自动返还功能 如果它被禁用了。

5. 如果已禁用自动交还，请重新启用：

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

6. 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
```

下一步行动

在还原ONTAP映像且节点正常运行并提供数据后，您可以"将故障部件退回给NetApp"。

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

如果ASA A20、ASA A30或ASA A50存储系统中的某个组件发生故障、请将故障部件退回

给NetApp。 "部件退回和更换"有关详细信息、请参见页面。