



# 启动媒体 - 自动恢复

## Install and maintain

NetApp  
February 13, 2026

# 目录

启动媒体 - 自动恢复 .....	1
启动媒体自动恢复工作流程 - ASA A400 .....	1
自动启动介质恢复的要求 - ASA A400 .....	1
关闭控制器以进行自动启动介质恢复 - ASA A400 .....	2
更换启动介质以实现自动启动恢复 - ASA A400 .....	3
从合作伙伴节点自动恢复启动介质 - ASA A400 .....	6
将失败的启动介质返回给NetApp - ASA A400 .....	12

# 启动媒体 - 自动恢复

## 启动媒体自动恢复工作流程 - ASA A400

启动映像的自动恢复涉及系统自动识别并选择适当的启动菜单选项。它使用合作伙伴节点上的启动映像，在ASA A400系统中的替换启动介质上重新安装ONTAP。

自动启动介质恢复过程仅在ONTAP 9.17.1 及更高版本中受支持。如果您的存储系统运行的是早期版本的ONTAP，请使用["手动启动恢复程序"](#)。

首先，检查更换要求，关闭控制器，更换启动介质，允许系统恢复映像，并验证系统功能。

1

["查看启动介质要求"](#)

查看更换启动介质的要求。

2

["关闭控制器"](#)

需要更换启动介质时、关闭存储系统中的控制器。

3

["更换启动介质"](#)

从控制器模块中移除故障的启动介质并安装替换的启动介质。

4

["还原启动介质上的映像"](#)

从配对控制器还原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。

## 自动启动介质恢复的要求 - ASA A400

在更换ASA A400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 e0S (e0M 扳手) 端口没有故障，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)。

自动启动介质恢复过程仅在ONTAP 9.17.1 及更高版本中受支持。如果您的存储系统运行的是早期版本的ONTAP，请使用["手动启动恢复程序"](#)。

- 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["关闭控制器"](#)。

## 关闭控制器以进行自动启动介质恢复 - ASA A400

关闭 ASA A400 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。

自动启动介质恢复过程仅在 ONTAP 9.17.1 及更高版本中受支持。如果您的存储系统运行的是早期版本的 ONTAP，请使用["手动启动恢复程序"](#)。

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：  <pre>storage failover takeover -ofnode <i>impaired_node_name</i> -halt true</pre> -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"](#)。

## 更换启动介质以实现自动启动恢复 - ASA A400

ASA A400 系统中的启动介质存储了重要的固件和配置数据。更换过程包括移除并打开控制器模块、移除受损的启动介质、在控制器模块中安装替换启动介质，然后重新安装控制器模块。

自动启动介质恢复过程仅在 ONTAP 9.17.1 及更高版本中受支持。如果您的存储系统运行的是早期版本的 ONTAP，请使用["手动启动恢复程序"](#)。

启动介质位于风管下方的控制器模块内，通过从系统中移除控制器模块即可访问。

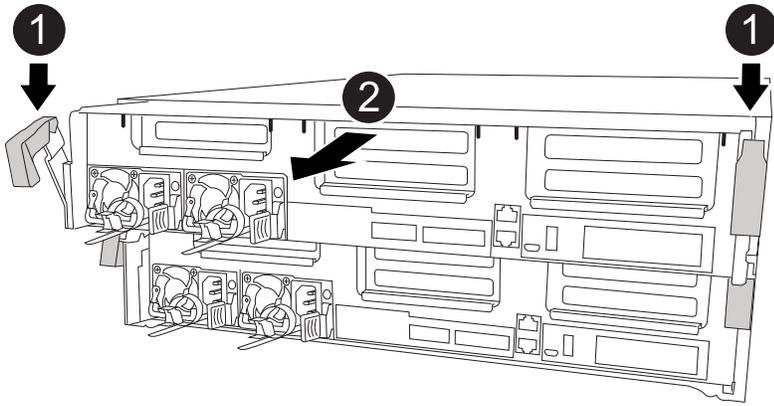
### 步骤

1. 如果您尚未接地，请正确接地。
2. 释放电源线固定器，然后从电源中拔下缆线。
3. 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。

4. 将缆线管理设备从控制器模块中取出并放在一旁。
5. 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。



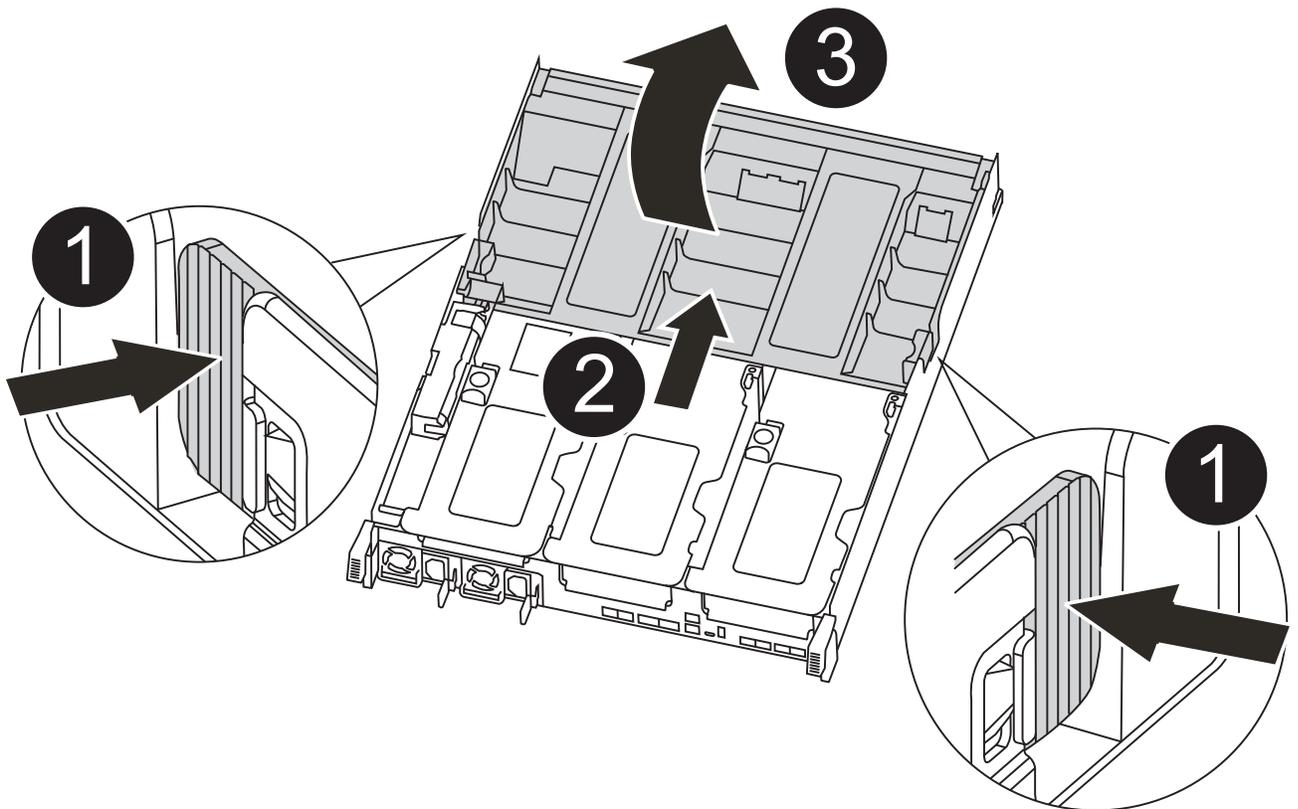
1	锁定门锁
2	控制器从机箱中略微移出

6. 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。

7. 将控制器模块放在平稳的表面上。

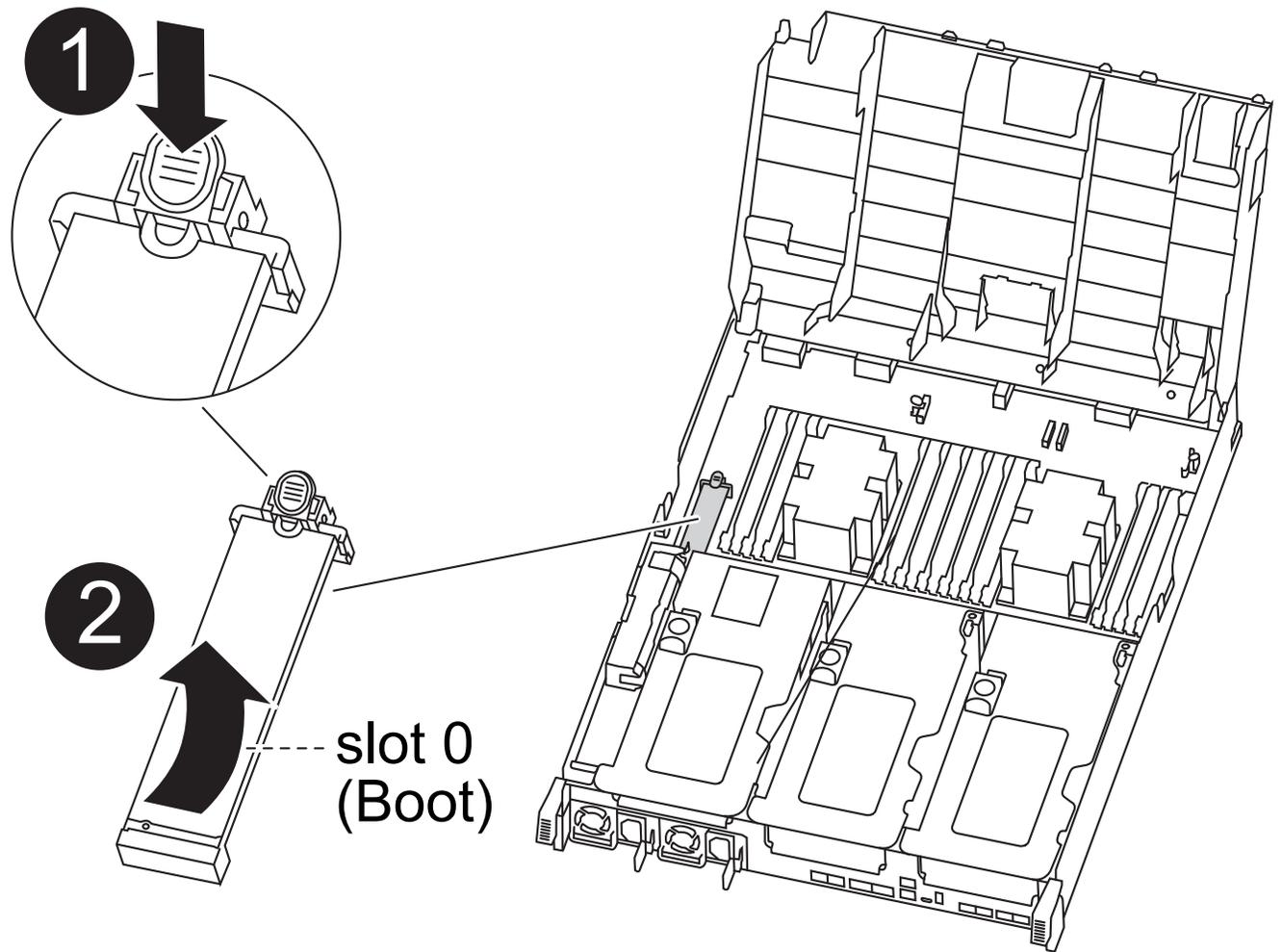
8. 打开通风管：



1	锁定卡舌
2	将通风管滑向控制器背面
3	向上旋转通风管

- a. 将通风管两侧的锁定片朝控制器模块中间按压。
- b. 将通风管滑向控制器模块的背面，然后将其向上旋转至完全打开的位置。

9. 从控制器模块中找到并取出启动介质：



1	按蓝色按钮
2	向上旋转启动介质并从插槽中取出

- a. 按启动介质末端的蓝色按钮，直到启动介质上的边缘清除蓝色按钮。

- b. 将启动介质向上旋转，然后将启动介质从插槽中轻轻拉出。
10. 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。
11. 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。

12. 将启动介质锁定到位：
  - a. 将启动介质向下旋转到主板。
  - b. 将一根手指放在启动介质的末端，然后按下启动介质的一端，以接合蓝色锁定按钮。
  - c. 向下推启动介质时，提起蓝色锁定按钮以将启动介质锁定到位。
13. 关闭通风管。

下一步行动

物理更换受损启动介质后，"[从配对节点还原ONTAP映像](#)"。

## 从合作伙伴节点自动恢复启动介质 - ASA A400

在ASA A400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，以从配对节点恢复配置。在恢复过程中，系统会检查是否已启用加密，并确定正在使用的密钥加密类型。如果已启用密钥加密，系统将引导您完成相应的恢复步骤。

自动启动介质恢复过程仅在ONTAP 9.17.1 及更高版本中受支持。如果您的存储系统运行的是早期版本的ONTAP，请使用"[手动启动恢复程序](#)"。

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：  <code>storage failover giveback -ofnode impaired_node_name</code>  c. 前往 <a href="#">重新启用自动返还功能</a> 如果它被禁用了。
key manager is configured.	已安装加密功能。前往 <a href="#">恢复密钥管理器</a> 。



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.crt
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 `kmp2\_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"](#)。

## 将失败的启动介质返回给NetApp - ASA A400

如果您的ASA A400系统中的某个组件出现故障，请将故障部件退回给NetApp。请参阅 ["部](#)

件退回和更换"页面以获取更多信息。

## 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。