第6阶段。使用替代系统模块启动node2

Upgrade controllers

NetApp
January 09, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/ontap-systems-upgrade/upgrade-arl-auto-in-chassis/cable-node2-for-shared-cluster-HA-storage.html on January 09, 2026. Always check docs.netapp.com for the latest.

目录

第6阶段。使用替代系统模块启动node2 . . . 1
为共享集群HA和存储连接node2 . . . 1
连接e0M和BMC端口 . . . 1
连接到双节点无交换机集群 . . . 1
连接到交换机连接的集群 . . . 2
使用替代系统模块启动node2 . . . 3
验证 node2 安装 . . . 8
还原 node2 上的网络配置 . . . 11
还原 node2 上的 key-manager 配置 . . . 13
验证集群交换机上的 RCF 配置 . . . 14
将非根聚合和 NAS 数据 LIF 移回 node2 . . . 15

第6阶段。使用替代系统模块启动node2

为共享集群HA和存储连接node2

如果您正在执行以下升级之一，则需要将先前连接到现有系统上的 node2 的集群、HA、存储、数据和管理连接连接到替换系统上新安装的 node2。

现有系统	更换系统
AFF A250	AFF A30、AFF A50
AFF C250	AFF C30、AFF C60
AFF A800	AFF A70、AFF A90
AFF C800	AFF C80

连接e0M和BMC端口

如果现有系统具有管理端口(e0M)和BMC端口、则e0M和BMC端口会组合在一起、并通过替代系统上的"扳手"端口进行访问。在连接到替代系统之前、必须确保e0M和BMC端口已连接到现有系统上的同一交换机和子网。

如果...	那么 ...
e0M和BMC IP地址位于同一IP子网上	将现有系统上的e0M或BMC端口连接到更换系统上的"扳手"端口。
e0M和BMC IP地址位于不同子网上	1. 将e0M和BMC IP地址合并到一个IP子网中。 2. 将现有系统上的e0M或BMC端口连接到更换系统上的"扳手"端口。

连接到双节点无交换机集群

下表显示了双节点无交换机集群配置中的交换机端口使用情况。

端口类型	AFF A800、AFF C800	AFF A90	AFF A70、AFF C80
集群	e0a	e1a	e1a
集群	e1a	e7a (如果没有e7a、请使用e1b)	e1b
HA	e0b	不连接	不连接
HA	e1b	不连接	不连接
SAS存储端口(如果存在并使用)	任何可用端口	任何可用端口	任何可用端口
NS224磁盘架的以太网存储端口	任何可用端口	请参见以太网存储连接映射	请参见以太网存储连接映射

端口类型	AFF A250、AFF C250	AFF A30、AFF C60	AFF A50
集群	e0c	e1a（使用 e1a 进行临时集群互连）	e1a（使用 e1a 进行临时集群互连）
集群	e0d	e1b（使用 e1b 进行临时集群互连）	e1b（使用 e1b 进行临时集群互连）
HA	e0c HA 端口与 Cluster 端口共享	节点 1 上的 e4a 使用 100 GbE 电缆直接连接到节点 2 上的 e4a	节点 1 上的 e4a 使用 100 GbE 电缆直接连接到节点 2 上的 e4a
HA	e0d HA 端口与 Cluster 端口共享	节点 1 上的 e2a 使用 100 GbE 电缆直接连接到节点 2 上的 e2a 如果 e2a 不存在或不支持 100 GbE，则使用 100 GbE 电缆直接将节点 1 上的 e4b 连接到节点 2 上的 e4b。	节点 1 上的 e2a 使用 100 GbE 电缆直接连接到节点 2 上的 e2a 如果 e2a 不存在或不支持 100 GbE，则使用 100 GbE 电缆直接将节点 1 上的 e4b 连接到节点 2 上的 e4b。
以太网存储端口	任何可用端口	e3a、e3b	e3a、e3b
SAS存储端口	任何可用端口	3a、3b	3a、3b

连接到交换机连接的集群

对于交换机连接的集群、请检查AFF A30、AFF A50、AFF A70、AFF A90、AFF C30、AFF C60或AFF C80 (替代)节点是否满足以下要求：

- 替代节点上的相同集群端口位于同一交换机上。例如、升级完成后、应将node1上的e1a和node2上的e1a连接到一个集群交换机。同样、两个节点的第二个集群端口应连接到第二个集群交换机。如果交叉连接共享集群HA端口(其中、node1中的e1a连接到SwitchA、而node2中的e1a连接到SwitchB)、则会导致HA通信失败。
- 替代节点使用共享的集群HA以太网端口。
- 验证是否已使用支持共享集群HA端口的参考配置文件(RCF)安装集群交换机：
  a. 删除交换机上的现有配置：

交换机型号	转至 ...
Cisco Nexus	知识库文章"如何在保持远程连接的同时清除Cisco互连交换机上的配置"
Broadcom BES-53248	知识库文章"如何在保持远程连接的同时清除Broadcom互连交换机上的配置"

  b. 配置并验证交换机设置：

交换机型号	转至 ...
Cisco Nexus 9336C-x2	"升级参考配置文件(RCF)"
Broadcom BES-53248	"升级参考配置文件(RCF)"
NVIDIA SN2100	"安装或升级参考配置文件(Reference Configuration File、RCF)脚本"

如果集群交换机仅支持 10/25 GbE 速度，则必须在替换系统的插槽 1 或插槽 2 中使用 X60130A、4 端口 10/25GbE 卡进行集群互连。

使用替代系统模块启动node2

安装了替换模块的 Node2 现在可以启动了。支持的替换模块列表如下："支持的系统列表"。

只有在通过交换系统模块进行升级时、才能移动控制台和管理连接。

步骤

1. 如果您安装了 NetApp 存储加密 (NSE) 驱动器，请执行以下步骤：

   如果您之前尚未在操作步骤 中执行此操作、请参见知识库文章 "如何判断驱动器是否已通过FIPS认证" 确定正在使用的自加密驱动器的类型。

   a. 设置 `bootarg.storageencryption.support` to `true` 或 `false`：

如果正在使用以下驱动器、请使用 ...	然后选择...
符合FIPS 140-2 2级自加密要求的NSE驱动器	`setenv bootarg.storageencryption.support` **`true`**
NetApp非FIPS SED	`setenv bootarg.storageencryption.support` **`false`**

   不能在同一节点或HA对上混用FIPS驱动器和其他类型的驱动器。您可以在同一节点或HA对上混用SED和非加密驱动器。

   b. 转到专用启动菜单并选择选项 `(10) Set Onboard Key Manager recovery secrets`。

   输入先前记录的操作步骤 密码短语和备份信息。请参见 "使用板载密钥管理器管理存储加密"。

2. 将节点启动至启动菜单：

   `boot_ontap` 菜单

3. 当节点在启动菜单处停止时，通过在 node2 上运行以下命令将旧的 node2 磁盘重新分配给替换 node2：

   `boot_after_controller_replacement`

   经过短暂延迟后、系统将提示您输入要替换的节点的名称。如果存在共享磁盘(也称为高级磁盘分区(Advanced Disk Partitioning、ADP)或分区磁盘)、系统将提示您输入HA配对节点的节点名称。

   这些提示可能会被埋在控制台消息中。如果未输入节点名称或输入的名称不正确、系统将提示您重新输入此名称。

如果` localhost：disk.encryptNoSupport：aler]：检测到FIPS认证的加密驱动器`和、或`、则执行以下步骤：localhost：diskown.errorDuringIO：error]：disk` error 3 (disk failed) on disk error occur、则执行以下步骤：

a. 在LOADER提示符处暂停节点。
b. 检查并重置中所述的存储加密启动目标 第 1 步。
c. 在加载程序提示符处、启动：

```
boot_ontap
```

您可以使用以下示例作为参考：

展开控制台输出示例

```
LOADER-A> boot_ontap menu
.
.
<output truncated>
.
All rights reserved.
*******************************
*                             *
* Press Ctrl-C for Boot Menu. *
*                             *
*******************************
.
<output truncated>
.
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)? 22/7

(22/7)                          Print this secret List
(25/6)                          Force boot with multiple filesystem
disks missing.
(25/7)                          Boot w/ disk labels forced to clean.
(29/7)                          Bypass media errors.
(44/4a)                         Zero disks if needed and create new
flexible root volume.
(44/7)                          Assign all disks, Initialize all
disks as SPARE, write DDR labels
.
.
<output truncated>
.
.
(wipeconfig)                        Clean all configuration on boot
```

```
device
(boot_after_controller_replacement) Boot after controller upgrade
(boot_after_mcc_transition)         Boot after MCC transition
(9a)                                Unpartition all disks and remove
their ownership information.
(9b)                                Clean configuration and
initialize node with partitioned disks.
(9c)                                Clean configuration and
initialize node with whole disks.
(9d)                                Reboot the node.
(9e)                                Return to main boot menu.



The boot device has changed. System configuration information could
be lost. Use option (6) to restore the system configuration, or
option (4) to initialize all disks and setup a new system.
Normal Boot is prohibited.

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)? boot_after_controller_replacement

This will replace all flash-based configuration with the last backup
to disks. Are you sure you want to continue?: yes

.
.
<output truncated>
.
.
Controller Replacement: Provide name of the node you would like to
replace:<nodename of the node being replaced>
Controller Replacement: Provide High Availability partner of node1:
<nodename of the partner of the node being replaced>
```

```
Changing sysid of node node1 disks.
Fetched sanown old_owner_sysid = 536940063 and calculated old sys id
= 536940063
Partner sysid = 4294967295, owner sysid = 536940063
.
.
<output truncated>
.
.
varfs_backup_restore: restore using /mroot/etc/varfs.tgz
varfs_backup_restore: attempting to restore /var/kmip to the boot
device
varfs_backup_restore: failed to restore /var/kmip to the boot device
varfs_backup_restore: attempting to restore env file to the boot
device
varfs_backup_restore: successfully restored env file to the boot
device wrote key file "/tmp/rndc.key"
varfs_backup_restore: timeout waiting for login
varfs_backup_restore: Rebooting to load the new varfs
Terminated
<node reboots>

System rebooting...

.
.
Restoring env file from boot media...
copy_env_file:scenario = head upgrade
Successfully restored env file from boot media...
Rebooting to load the restored env file...
.
System rebooting...
.
.
.
<output truncated>
.
.
.
.
WARNING: System ID mismatch. This usually occurs when replacing a
boot device or NVRAM cards!
Override system ID? {y|n} y
.
.
.
```

```
.
Login:
```

上述示例中显示的系统 ID 是示例 ID 。要升级的节点的实际系统 ID 将不同。

在提示符和登录提示符处输入节点名称之间，节点会重新启动几次以还原环境变量，更新系统中卡上的固件以及进行其他 ONTAP 更新。

验证 node2 安装

您必须使用替代系统模块验证node2安装。由于物理端口不变、您无需将物理端口从旧节点2映射到替换节点2。

关于此任务

使用替代系统模块启动node1后、您需要验证其是否已正确安装。您必须等待node2加入仲裁、然后恢复控制器更换操作。

此时，在操作步骤中，操作将暂停，而 node2 加入仲裁。

步骤

1. 验证 node2 是否已加入仲裁：

   `cluster show -node node2 -fields health`

   `health` 字段的输出应为 `true` 。

2. 此步骤适用于以下升级配置。对于所有其他系统升级，请跳过此步骤并转至第 3 步 ：

   - 双节点无交换机集群
   - 将连接的 AFF A250 或 AFF C250 系统升级到 AFF A50、AFF A30、AFF C30 或 AFF C60 系统。

   如果 node2 没有自动加入仲裁：

   a. 检查端口 e1a 和 e1b 的 IP 空间：

      `network port show`

   b. 如果 IP 空间不是“集群”，请在 e1a 和 e1b 上将 IP 空间更改为“集群”：

      `network port modify -node <node_name> -port <port> -ipspace Cluster`

   c. 验证端口 e1a 和 e1b 的 IP 空间是否为“集群”：

      `network port show`

   d. 将节点 2 集群 LIF 迁移到 e1a 和 e1b：

      `network interface migrate -vserver Cluster -lif <cluster_lif1> -destination`

```
-node <node2_name> -destination-port <port_name
```

3. 验证 node2 和 node1 是否属于同一个集群，以及该集群是否健康：

```
cluster show
```

4. 切换到高级权限模式：

```
set advanced
```

5. 此步骤仅适用于从 AFF A250 或 AFF C250 升级到 AFF A50、AFF A30、AFF C60 或 AFF C30 的双节点无交换机配置升级。对于所有其他系统升级，请跳过此步骤并转至第 6 步 ：

   验证 e4a、e2a、e1a、e1b 端口或 e4a、e4b、e1a、e1b 端口是否为“集群”广播域中的集群端口。

   AFF A50、AFF A30、AFF C30 和 AFF C60 系统共享集群和 HA 端口。您可以安全地将所有集群 LIF 迁移到节点 1 和节点 2 上的 e4a、e4b 或 e4a、e2a：

   a. 列出所有集群 LIF 的主端口和当前端口：

   ```
   network interface show -role Cluster -fields home-port,curr-port
   ```

   b. 在节点 1 和节点 2 上，将使用 e1a 作为主端口的集群 LIF 迁移到 e4a：

   ```
   network interface migrate -vserver Cluster -lif <cluster_lif1> -destination
   -node <node> -destination-port e4a
   ```

   c. 在节点 1 和节点 2 上，修改迁移到的集群 LIF 子步骤 b使用 e4a 作为主端口：

   ```
   network interface modify -vserver Cluster -lif <cluster_lif> -home-port e4a
   ```

   d. 验证群集是否符合仲裁：

   ```
   cluster show
   ```

   e. 重复子步骤 b 和子步骤 c将每个节点上的第二个集群 LIF 迁移并修改为 e2a 或 e4b：

   如果存在 e2a 且其为 100GbE 网络端口，则这是默认的第二个集群端口。如果 e2a 不是 100GbE 网络端口，则 ONTAP 使用 e4b 作为第二个集群和 HA 端口。

   f. 从“集群”广播域中删除 e1a 和 e1b：

   ```
   broadcast-domain remove-ports -broadcast-domain Cluster -ipspace Cluster
   -ports <node_name>:e1a
   ```

   g. 验证只有集群端口 e4a、e2a 或 e4a、e4b 位于“集群”广播域中

   ```
   broadcast domain show
   ```

   h. 移除 e1a 节点 1 和 e1a 节点 2 以及 e1b 节点 1 和 e1b 节点 2 之间的电缆连接，以确保仅使用有效的集群 HA 连接并且没有冗余连接。

6. 检查控制器更换操作的状态，并验证它处于暂停状态，并且与 node2 暂停执行安装新控制器和移动电缆的

物理任务之前的状态相同：

```
ssystem controller replace show
```

s系统控制器更换 `show-details`

7. 恢复控制器更换操作：

   s系统控制器更换恢复

8. 控制器更换操作将暂停以进行干预，并显示以下消息：

```
Cluster::*> system controller replace show
Node          Status                        Error-Action
------------  ------------------------
-------------------------------------
Node2         Paused-for-intervention       Follow the instructions given
in
                                            Step Details
Node1         None

Step Details:
--------------------------------------------
To complete the Network Reachability task, the ONTAP network
configuration must be manually adjusted to match the new physical
network configuration of the hardware. This includes:


1. Re-create the interface group, if needed, before restoring VLANs. For
detailed commands and instructions, refer to the "Re-creating VLANs,
ifgrps, and broadcast domains" section of the upgrade controller
hardware guide for the ONTAP version running on the new controllers.
2. Run the command "cluster controller-replacement network displaced-
vlans show" to check if any VLAN is displaced.
3. If any VLAN is displaced, run the command "cluster controller-
replacement network displaced-vlans restore" to restore the VLAN on the
desired port.
2 entries were displayed.
```

> 在此操作步骤 中， *re-creating VLANs* ， *ifgrp* 和 *broadcast domains_section* 已重命名为 *_Restore node2* 上的网络配置。

9. 在控制器更换处于暂停状态的情况下，继续执行 还原 node2 上的网络配置。

还原 **node2** 上的网络配置

确认 node2 处于仲裁状态并可与 node1 通信后，请确认 node2 上显示了 node1 的 VLAN ，接口组和广播域。此外，验证是否已在其正确的广播域中配置所有 node2 网络端口。

关于此任务

有关创建和重新创建 VLAN ，接口组和广播域的详细信息，请参见 "参考资料" 链接到 *Network Management* 内容。

步骤

1. 列出已升级的节点 2 上的所有物理端口：

   ```
   network port show -node node2
   ```

   此时将显示节点上的所有物理网络端口， VLAN 端口和接口组端口。在此输出中，您可以看到 ONTAP 已将任何物理端口移至 **集群** 广播域。您可以使用此输出来帮助确定应将哪些端口用作接口组成员端口， VLAN 基本端口或用于托管 LIF 的独立物理端口。

2. 列出集群上的广播域：

   ```
   network port broadcast-domain show
   ```

3. 列出节点 2 上所有端口的网络端口可访问性：

   ```
   network port reachability show -node node2
   ```

   您应看到类似于以下示例的输出。端口和广播名称会有所不同。

```
Cluster::> reachability show -node node1
  (network port reachability show)
Node      Port     Expected Reachability                Reachability
Status
--------- -------- ------------------------------------
---------------------
Node1
          a0a      Default:Default                      ok
          a0a-822  Default:822                          ok
          a0a-823  Default:823                          ok
          e0M      Default:Mgmt                         ok
          e1a      Cluster:Cluster                      ok
          e1b      -                                    no-reachability
          e2a      -                                    no-reachability
          e2b      -                                    no-reachability
          e3a      -                                    no-reachability
          e3b      -                                    no-reachability
          e7a      Cluster:Cluster                      ok
          e7b      -                                    no-reachability
          e9a      Default:Default                      ok
          e9a-822  Default:822                          ok
          e9a-823  Default:823                          ok
          e9b      Default:Default                      ok
          e9b-822  Default:822                          ok
          e9b-823  Default:823                          ok
          e9c      Default:Default                      ok
          e9d      Default:Default                      ok
20 entries were displayed.
```

在上述示例中， node2 已在更换控制器后启动并加入仲裁。它具有多个不可访问的端口，并且正在等待可访问性扫描。

4. 使用以下命令按以下顺序修复 node2 上每个端口的可访问性状态不是 `ok` 的可访问性：

`network port reachability repair -node` *node_name*`-port` *port_name*

   a. 物理端口
   b. VLAN 端口

您应看到类似于以下示例的输出：

```
Cluster ::> reachability repair -node node2 -port e9d
```

```
Warning: Repairing port "node2:e9d" may cause it to move into a
different broadcast domain, which can cause LIFs to be re-homed away
from the port. Are you sure you want to continue? {y|n}:
```

对于可访问性状态可能与当前所在广播域的可访问性状态不同的端口，应显示警告消息，如上例所示。根据需要查看端口和问题解答 `y` 或 `n` 的连接。

验证所有物理端口是否具有预期可访问性：

网络端口可访问性显示

在执行可访问性修复时， ONTAP 会尝试将端口放置在正确的广播域中。但是，如果无法确定某个端口的可访问性，并且该端口不属于任何现有广播域，则 ONTAP 将为这些端口创建新的广播域。

5. 验证端口可访问性：

   网络端口可访问性显示

   如果所有端口均已正确配置并添加到正确的广播域中，则 `network port reachability show` 命令应将所有已连接端口的可访问性状态报告为 `ok` ，对于无物理连接的端口，此状态报告为 `no-reachability` 。如果任何端口报告的状态不是这两个端口，请按照中的说明执行可访问性修复并在其广播域中添加或删除端口 第 4 步。

6. 验证所有端口是否均已置于广播域中：

   ```
   network port show
   ```

7. 验证广播域中的所有端口是否配置了正确的最大传输单元（ MTU ）：

   ```
   network port broadcast-domain show
   ```

8. 使用以下步骤还原 LIF 主端口，指定需要还原的 Vserver 和 LIF 主端口（如果有）：

   a. 列出所有已替换的 LIF ：

      ```
      displaced interface show
      ```

   b. 还原 LIF 主节点和主端口：

      ```
      displaced interface restore-home-node -node node_name-vserver vserver_name
      -lif-name LIF_name
      ```

9. 验证所有 LIF 是否都具有主端口且已由管理员启动：

   ```
   network interface show -fields home-port ， status-admin
   ```

还原 node2 上的 key-manager 配置

如果使用NetApp聚合加密(NAE)或NetApp卷加密(NVE)对要升级的系统上的卷进行加密、

则加密配置必须同步到新节点。如果不重新同步key-manager、则在使用ARL将node2聚合从已升级的node1重新定位到已升级的node2时、可能会发生故障、因为node2没有使加密卷和聚合联机所需的加密密钥。

关于此任务

执行以下步骤，将加密配置同步到新节点：

步骤

1. 从node2运行以下命令：

   ```
   sSecurity key-manager 板载同步
   ```

2. 在重新定位数据聚合之前、请验证node2上的SVM-KEK密钥是否已还原为"true"：

   ```
   ::> security key-manager key query -node node2 -fields restored -key
   -type SVM-KEK
   ```

   示例

   ```
   ::> security key-manager key query -node node2 -fields restored -key
   -type SVM-KEK

   node     vserver   key-server   key-id
   restored
   -------- --------- -----------  ----------------------------------------
   --------
   node2    svm1      ""           000000000000000002000000000000a008a81976
   true
                                   2190178f9350e071fbb90f00000000000000000
   ```

验证集群交换机上的 RCF 配置

在升级过程的这个阶段，所有数据聚合都应位于节点 1 上。如果您要升级具有交换机连接集群的配置，则需要验证集群交换机参考配置文件 (RCF) 是否支持新控制器的共享集群/HA 端口。

如果您要升级到双节点无交换机集群配置，则可以跳过本节并转至"将非根聚合和 NAS 数据 LIF 移回 node2"。

步骤

1. 切换到高级权限模式：

   ```
   set advanced
   ```

2. 检查“IC RDMA”的状态：

```
ha interconnect status show
```

在输出中，“IC RDMA 连接”应具有状态 `Up`。

如果“IC RDMA 连接”状态为…	然后选择…
`Up`	前往"将非根聚合和 NAS 数据 LIF 移回 node2"。
`Down`	前往第 3 步。

3. 检查集群端口并切换 RCF。

   有关详细信息，请参见 "连接到交换机连接的集群"。

4. 验证“IC RDMA 连接”状态是否已更改为 `Up`：

   ```
   ha interconnect status show
   ```

下一步

"将非根聚合和 NAS 数据 LIF 移回 node2"

将非根聚合和 NAS 数据 LIF 移回 node2

在验证节点 2 上的网络配置后，需要将节点 2 拥有的 NAS 数据 LIF 从节点 1 迁移到节点 2，并确认 SAN LIF 存在于节点 2 上。

关于此任务

远程 LIF 在升级过程中处理到 SAN LUN 的流量。升级过程中，迁移 SAN LIF 对集群或服务运行状况并非必要。除非需要将 SAN LIF 映射到新端口，否则不会移动它们。

在节点 2 上线后，您需要验证 LIF 是否健康以及是否位于正确的端口上。

步骤

1. 恢复重新定位操作：

   ```
   system controller replace resume
   ```

   系统将执行以下任务：

   - 集群仲裁检查
   - 系统 ID 检查
   - 映像版本检查
   - 目标平台检查
   - 网络可访问性检查

   系统在网络可达性检查的此阶段暂停操作。

2. 恢复重新定位操作：

```
system controller replace resume
```

系统将执行以下检查：

- 集群运行状况检查
- 集群 LIF 状态检查

执行这些检查后、系统会将非根聚合和NAS数据RIFs重新定位回node2、而node2现在正在替代控制器上运行。

资源重新定位完成后，控制器更换操作将暂停。

3. 检查聚合重新定位和 NAS 数据 LIF 移动操作的状态：

```
system controller replace show-details
```

如果控制器更换操作步骤已暂停，请检查并更正错误（如果有），然后选择问题描述 `reume` 继续操作。

4. 如有必要，恢复和还原已移位的 LIF，或者手动迁移和修改未能自动迁移到 node2 的 node2 LIF。

恢复和还原移位的 **LIF**

a. 列出所有已移位的 LIF：

```
cluster controller-replacement network displaced-interface show
```

b. 如果已替换任何 LIF ，请将主节点还原回 node2 ：

```
cluster controller-replacement network displaced-interface
restore-home-node -node <node2_nodename> -vserver <vserver name>
-lif-name <lif_name>
```

手动迁移和修改 **LIF** 文件

a. 将未能自动迁移到节点2的LIF迁移出去：

```
network interface migrate -vserver <vserver name> -lif <lif_name>
-destination-node <node2_nodename> -destination-port
<port_on_node2>
```

b. 修改已迁移 LIF 的源节点和源端口：

```
network interface modify -vserver <vserver_name> -lif
<data_lif_name> -home-node <node2_nodename> -home-port
<home_port>
```

5. 恢复此操作以提示系统执行所需的后检查：

```
system controller replace resume
```

系统将执行以下后检查：

- 集群仲裁检查
- 集群运行状况检查
- 聚合重建检查
- 聚合状态检查
- 磁盘状态检查
- 集群 LIF 状态检查
- 卷检查

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。