



使用**system controller Replace**
命令升级**9.15.1**
9.15.1及更高版本中引入的控制器硬件
Upgrade controllers

NetApp
January 17, 2025

目录

使用system controller Replace命令升级9.15.1 9.151及更高版本中引入的控制器硬件	1
概述	1
自动执行控制器升级过程	2
确定是否使用聚合重新定位操作步骤	2
所需的工具和文档	3
使用 ARL 升级控制器的准则	4
ARL 升级概述	5
第 1 阶段。准备升级	6
第 2 阶段。重新定位和停用节点 1	11
第 3 阶段。安装并启动 node3	14
第 4 阶段。重新定位和停用节点 2	33
第 5 阶段。安装并启动节点 4.	35
第 6 阶段。完成升级	53
故障排除	59
参考资料	66

使用system controller Replace命令升级9.15.1 9.151及更高版本中引入的控制器硬件

概述

此操作步骤介绍了如何在以下系统配置中使用聚合重新定位（Aggregate Relocation，ARL）升级控制器硬件：

方法	ONTAP 版本	支持的系统
使用 <code>ssystem controller replace</code> 命令	9.151或更高版本	"链接到支持的系统列表"



您不能使用此过程升级MetroCluster FC或IP配置。要升级MetroCluster配置、请参见 ["参考资料"](#) 以链接到 [_ MetroCluster升级和扩展文档_](#)。

在操作步骤期间，您可以使用替代控制器硬件升级原始控制器硬件，从而重新定位非根聚合的所有权。您可以在节点之间多次迁移聚合，以确认在整个升级操作步骤中至少有一个节点正在从聚合提供数据。您还可以迁移数据逻辑接口（LIF），并在继续操作时将新控制器上的网络端口分配给接口组。

此信息中使用的术语

在此信息中，原始节点称为 "node1" 和 "node2"，新节点称为 "node3" 和 "node4"。在所述的操作步骤期间，node1 将替换为 node3，node2 将替换为 node4。

术语 "node1"，"node2"，"node3" 和 "node4" 仅用于区分原始节点和新节点。在操作步骤之后，必须替换原始节点和新节点的实际名称。但是，实际上，节点名称不会更改：在升级控制器硬件后，node3 的名称为 node1，node4 的名称为 node2。

重要信息：

- 此操作步骤非常复杂，假定您具备高级 ONTAP 管理技能。您还必须阅读并了解 ["使用 ARL 升级控制器的准则"](#) 和 ["ARL 升级概述"](#) 开始升级前的章节。
- 此操作步骤假定更换用的控制器硬件是新的，尚未使用。此过程不包括使用命令准备使用过的控制器所需的步骤 `wipeconfig`。如果之前使用了替代控制器硬件、则必须联系技术支持。
- 您可以使用此操作步骤升级具有两个以上节点的集群中的控制器硬件；但是，您需要为集群中的每个高可用性（HA）对单独执行操作步骤。
- 升级到9.15.1 9.151或更高版本中推出的系统时、ONTAP会转换现有卷的存储效率、并应用新的存储效率功能来利用硬件卸载功能。这是一个自动后台进程、不会对系统性能造成明显影响。
 - 对于AFF A20、AFF A30、AFF A50、AFF A70、AFF A90、AFF A1K、AFF C30、AFF C60和AFF C80系统、ONTAP可转换所有现有精简配置卷的存储效率、包括未使用存储效率的卷。
 - 对于FAS70和FAS90系统、ONTAP仅转换在升级之前已启用存储效率的现有精简配置卷的存储效率。

["详细了解存储效率"](#)(英文)

- AFF A20、AFF A50、AFF A70、AFF A90、AFF A1K、FAS70和FAS90系统为集群和HA连接共享100GbE网络端口。这些系统可以支持与传统集群交换机建立10GbE或25GbE集群连接；但是、当不再需要10GbE和25GbE交换机时、NetApp建议更新到100GbE集群速度。有关详细信息，请参见以下知识库文章：

- "如何在新的集群设置中配置10G或25G集群端口"
- "如何将现有10 G或25 G集群端口转换为40 G或100 G集群端口"

对于集群和HA连接、AFF 2020系统会共享10GbE和25GbE网络端口。这些是AFF A20系统支持的唯一网络端口集群连接。

如果无法将现有节点上的e0a或e0b集群端口链接到新节点上的集群端口，请参见 "[NetApp错误在线中的错误ID COBTP-166978](#)"。

自动执行控制器升级过程

在控制器升级期间，此控制器将被替换为另一个运行更新或功能更强大的平台的控制器。本内容介绍了部分自动化过程的步骤、该过程利用自动网络端口可访问性检查进一步简化了控制器升级体验。

确定是否使用聚合重新定位操作步骤

此过程介绍如何在保留现有数据和磁盘的同时、使用新控制器升级HA对中的存储控制器。这是一个复杂的操作步骤，只能由经验丰富的管理员使用。

支持 ARL 升级

在以下情况下、您可以升级一对节点：

- 您运行的是9.15.1 9.151或更高版本。
- 您不希望将新控制器作为新HA对添加到集群中、也不希望使用卷移动过程迁移数据。
- 您在管理ONTAP方面经验丰富、并且可以承受在诊断权限模式下工作的风险。



您可以对此操作步骤 使用NetApp存储加密(NSE)、NetApp卷加密(NVE)和NetApp聚合加密(NAE)。

下表显示了控制器升级支持的型号表。

现有控制器	更换控制器	从ONTAP开始支持...
AFF A400	AFF A50 ²	9.16.1
AFF A300	AFF A50 ²	9.16.1
AFF A220、AFF A150	AFF 2020 ²	9.16.1 ¹
FAS8200 , FAS8300 , FAS8700 , FAS9000	FAS70、FAS90	9.15.1P3
FAS9500	FAS90	9.15.1P3
AFF A300、AFF A400、AFF A700	AFF A70 ² , AFF A90 ² , AFF A1K	9.15.1
AFF A900	AFF A90 ² 、AFF A1K	9.15.1

¹要升级到AFF A20、必须先将AFF A150或AFF A220转换为DS224C磁盘架、方法是将控制器模块更换为IOM12模块。请参阅。"[将原始节点转换为驱动器架](#)"

² AFF A20、AFF A50、AFF A70和AFF A90是集成系统、在HA配置中具有两个控制器、在一个机箱中具有板载磁盘：

- 如果您要升级到具有内部驱动器的AFF A20、AFF A70或AFF A90、则必须在升级之前删除这些内部驱动器的所有权。完成升级后、您可以将内部驱动器分配给AFF A20、AFF A70或AFF A90节点、并使用它们创建数据聚合。您不必将根聚合或数据聚合迁移到内部驱动器。
- 如果要升级到不带内部驱动器的AFF A20、AFF A70或AFF A90、则在完成升级后无需分配内部驱动器。

如果上表不包含您的控制器升级型号组合，请联系技术支持。

ARL 不支持升级

在以下情况下、您不能使用ARL执行升级：

- 您正在执行以下升级之一：

现有控制器	更换控制器
AFF A250	AFF A50、AFF A30
AFF A800	AFF A70、AFF A90
AFF C250	AFF C30、AFF C60
AFF C800	AFF C80

要执行上表中列出的升级、请参见"[参考资料](#)"以链接到 `_use "system controller Replace "`命令升级同一机箱中的控制器型号。

- 您正在升级使用外部阵列作为后端存储的V系列系统或FlexArray虚拟化存储系统。有关V系列或FlexArray系统的升级选项、请联系技术支持。
- 您正在升级MetroCluster FC或IP配置。要升级MetroCluster配置、请参见 "[参考资料](#)" 以链接到 `_MetroCluster升级和扩展文档_`。

如果您希望使用其他方法升级控制器硬件并愿意执行卷移动，请参见 "[参考资料](#)" 通过移动卷或存储链接到 `_Upgrade`。

相关信息

请参见 "[参考资料](#)" 可链接到 `_ONTAP 9 文档中心_`，在此可以访问 ONTAP 9 产品文档。

所需的工具和文档

要安装新硬件，您必须使用特定工具，并且在升级过程中需要参考其他文档。

要执行升级，您需要使用以下工具：

- 接地线
- 2号十字螺丝刀

转至 ["参考资料"](#) 第节以访问此升级所需的参考文档和参考站点列表

使用 ARL 升级控制器的准则

要了解是否可以使用ARL升级一对运行ONTAP 9.151或更高版本的控制器、具体取决于原始控制器和替代控制器的平台和配置。

支持 ARL 升级

在使用此ARL过程升级一对节点之前、请查看以下要求以确保您的配置受支持：

- 验证是否可以对原始控制器和更换用的控制器执行ARL。
- 检查所有已定义聚合的大小以及原始系统支持的磁盘数。然后、将聚合大小和支持的磁盘数与新系统支持的聚合大小和磁盘数进行比较。请参阅 ["参考资料"](#) 以链接至可提供此信息的 [_ Hardware Universe _](#)。新系统支持的聚合大小和磁盘数必须等于或大于原始系统支持的聚合大小和磁盘数。
- 在集群混用规则中验证更换原始控制器后、新节点是否可以与现有节点一起加入集群。有关集群混用规则的详细信息、请参见 ["参考资料"](#) 链接到 [_Data Hardware Universe _](#)。
- 如果您的系统(例如AFF 700)具有以下配置、请将集群LUN迁移并重新归位到每个节点的两个集群端口：
 - 每个节点两个以上的集群端口
 - 以分支模式在插槽4中创建集群互连卡、用于创建端口e4a、e4b、e4c和e4D以及端口e4e、e4f、e4g和e4h



如果执行控制器升级时每个节点的集群端口数超过两个、则可能会导致升级后新控制器上的集群丢失。

有关详细信息，请参阅知识库文章 ["如何删除不需要或不必要的集群LUN"](#)。

配置了 SnapLock 企业版和 SnapLock 合规性卷的系统支持使用 ARL 升级控制器。

双节点无交换机集群

如果要升级双节点无交换机集群中的节点，则可以在执行升级时将这些节点保留在无交换机集群中。您无需将其转换为交换集群。

ARL 不支持升级

您不能升级不支持连接到原始控制器的磁盘架的替代控制器。

请参见 ["参考资料"](#) 链接到 [disk Hardware Universe](#) 以获取磁盘支持信息。

如果要升级具有内部驱动器的入门级控制器、请参见 ["参考资料"](#) 链接到 [_Upgrade by Moving volumes_](#)、然后转到过程 [_Upgrading a pair of running 集群模式Data ONTAP by Moving volumes_](#)。

故障排除

如果在升级控制器时出现任何问题、请参见 ["故障排除"](#) 以了解更多信息和可能的解决方案。

如果您未找到与遇到的问题相关的解决方案，请联系技术支持。

ARL 升级概述

在使用 ARL 升级节点之前，您应了解操作步骤的工作原理。在此内容中，操作步骤将分为多个阶段。

升级节点对

要升级节点对，您需要准备原始节点，然后对原始节点和新节点执行一系列步骤。然后，您可以停用原始节点。

ARL 升级顺序概述

在操作步骤期间，您可以使用替代控制器硬件升级原始控制器硬件，一次升级一个控制器，从而利用 HA 对配置重新定位非根聚合的所有权。所有非根聚合都必须进行两次重新定位，才能到达其最终目标，即正确的升级节点。

每个聚合都有一个主所有者和当前所有者。主所有者是聚合的实际所有者，当前所有者是临时所有者。

下表介绍了您在每个阶段执行的高级任务以及此阶段结束时的聚合所有权状态。操作步骤稍后将提供详细步骤：

阶段	Description
"第 1 阶段。准备升级"	<p>在阶段1中、您可以运行预检、如果需要、还可以更正聚合所有权。如果您要使用OKM管理存储加密、并且可以选择将SnapMirror关系静用、则必须记录某些信息。</p> <p>阶段 1 结束时的聚合所有权：</p> <ul style="list-style-type: none">• node1 是 node1 聚合的主所有者和当前所有者。• node2 是 node2 聚合的主所有者和当前所有者。
"第 2 阶段。重新定位和停用节点 1"	<p>在阶段2中、您会将node1非根聚合和NAS数据LIF重新定位到node2。此过程大部分是自动完成的；操作将暂停，以便您可以检查其状态。您必须手动恢复此操作。如果需要、您可以重新定位失败或被否决的聚合。在停用node1之前、您需要记录node1信息以供稍后在操作步骤 中使用。您也可以稍后在操作步骤 中准备网络启动node3和node4。</p> <p>阶段 2 结束时的聚合所有权：</p> <ul style="list-style-type: none">• node2 是 node1 聚合的当前所有者。• node2 是 node2 聚合的主所有者和当前所有者。

阶段	Description
"第 3 阶段。安装并启动 node3"	<p>在第 3 阶段，您安装并启动 node3，检查 node1 中的集群和节点管理端口是否在 node3 上联机，并验证 node3 安装。如果您使用的是 NetApp 卷加密 (NVE)，则需要还原密钥管理器配置。您还可以将 node1 NAS 数据 LIF 和非根聚合从 node2 重新定位到 node3，并验证 node3 上是否存在 SAN LIF。</p> <p>第 3 阶段结束时的聚合所有权：</p> <ul style="list-style-type: none"> • node3 是 node1 聚合的主所有者和当前所有者。 • node2 是 node2 聚合的主所有者和当前所有者。
"第 4 阶段。重新定位和停用节点 2"	<p>在阶段 4 中，您会将非根聚合和 NAS 数据 LIF 从 node2 重新定位到 node3。您还可以记录 node2 信息，以便在停用 node2 之前在操作步骤中稍后使用。</p> <p>第 4 阶段结束时的聚合所有权：</p> <ul style="list-style-type: none"> • node3 是最初属于 node1 的聚合的主所有者和当前所有者。 • node2 是 node2 聚合的主所有者。 • node3 是 node2 聚合的当前所有者。
"第 5 阶段。安装并启动节点 4."	<p>在第 5 阶段，您安装并启动 node4，检查 node2 中的集群和节点管理端口是否在 node4 上联机，并验证 node4 安装。如果您使用的是 NVE，则需要还原密钥管理器配置。您还可以将 node2 NAS 数据 LIF 和非根聚合从 node3 重新定位到 node4，并验证 node4 上是否存在 SAN LIF。</p> <p>第 5 阶段结束时的聚合所有权：</p> <ul style="list-style-type: none"> • node3 是最初属于 node1 的聚合的主所有者和当前所有者。 • Node4 是最初属于 Node2 的聚合的主所有者和当前所有者。
"第 6 阶段。完成升级"	<p>在第 6 阶段，您需要确认新节点设置正确，如果新节点启用了加密，则需要配置和设置存储加密或 NVE。您还应停用旧节点并恢复 SnapMirror 操作。</p>

第 1 阶段。准备升级

第 1 阶段概述

在阶段 1 中，您可以运行预检，如果需要，还可以更正聚合所有权。如果您要使用板载密钥管理器管理存储加密，并且可以选择将 SnapMirror 关系静置，则还需要记录某些信息。

步骤

1. "准备要升级的节点"

2. "使用板载密钥管理器管理存储加密"

准备要升级的节点

更换控制器的过程从一系列预检开始。此外，您还会收集有关原始节点的信息、以供稍后在操作步骤中使用、并根据需要确定正在使用的自加密驱动器的类型。

步骤

1. 在 ONTAP 命令行中输入以下命令，开始控制器更换过程：

```
system controller replace start -nodes <node_names>
```



您只能在高级权限级别执行system controller Replace start命令：set -privilege advanced

您将看到类似于以下示例的输出。输出将显示集群上运行的ONTAP版本：

```
Warning: 1. Current ONTAP version is 9.15.1

2. Verify that NVMEM or NVRAM batteries of the new nodes are charged,
and charge them if they are not. You need to physically check the new
nodes to see if the NVMEM or NVRAM batteries are charged. You can check
the battery status either by connecting to a serial console or using
SSH, logging into the Service Processor (SP) or Baseboard Management
Controller (BMC) for your system, and use the system sensors to see if
the battery has a sufficient charge.

Attention: Do not try to clear the NVRAM contents. If there is a need to
clear the contents of NVRAM, contact NetApp technical support.

3. If a controller was previously part of a different cluster, run
wipeconfig before using it as the replacement controller.

4. Note: This is not a MetroCluster configuration. Controller
replacement supports only ARL based procedure.
Do you want to continue? {y|n}: y
```

2. 按 y，您将看到以下输出：

```
Controller replacement operation: Prechecks in progress.
Controller replacement operation has been paused for user intervention.
```

系统将运行以下预检；记下每个预检的输出，以便稍后在操作步骤中使用：

预检查	Description
集群运行状况检查	检查集群中的所有节点以确认其运行状况良好。
聚合重新定位状态检查	检查聚合重新定位是否已在进行中。如果正在进行另一个聚合重新定位，则检查将失败。
型号名称检查	检查此操作步骤是否支持这些控制器型号。如果不支持这些型号，则此任务将失败。
集群仲裁检查	检查要更换的节点是否处于仲裁状态。如果节点未处于仲裁状态，则此任务将失败。
映像版本检查	检查要更换的节点是否运行相同版本的 ONTAP 。如果 ONTAP 映像版本不同，则此任务将失败。新节点上安装的 ONTAP 9.x 版本必须与原始节点上安装的版本相同。如果新节点安装的 ONTAP 版本不同，则在安装新控制器后，需要通过网络启动这些控制器。有关如何升级 ONTAP 的说明，请参见 "参考资料" 链接到 _Upgrade ONTAP 。
HA 状态检查	检查要更换的两个节点是否采用高可用性（HA）对配置。如果未为控制器启用存储故障转移，则任务将失败。
聚合状态检查	如果要更换的节点自身的聚合不是主所有者，则此任务将失败。节点不应拥有任何非本地聚合。
磁盘状态检查	如果要更换的任何节点缺少磁盘或磁盘出现故障，则此任务将失败。如果缺少任何磁盘、请参见 "参考资料" 链接到 _Disk and 聚合管理(使用命令行界面_) 、 _逻辑存储管理(使用命令行界面_) 和 _HA 对管理_ 、以便为 HA 对配置存储。
数据 LIF 状态检查	检查要更换的任何节点是否具有非本地数据 LIF 。节点不应包含其不是主所有者的任何数据 LIF 。如果其中一个节点包含非本地数据 LIF ，则任务将失败。
集群 LIF 状态	检查两个节点的集群 LIF 是否均已启动。如果集群 LIF 已关闭，则此任务将失败。
ASUP 状态检查	如果未配置 ASUP 通知，则任务将失败。在开始更换控制器操作步骤之前，必须启用 ASUP 。
CPU 利用率检查	检查要更换的任何节点的 CPU 利用率是否超过 50% 。如果 CPU 使用率在相当长的一段时间内超过 50% ，则此任务将失败。
聚合重建检查	检查是否正在任何数据聚合上进行重建。如果正在进行聚合重建，则此任务将失败。
节点关联性作业检查	检查是否正在运行任何节点关联作业。如果节点关联性作业正在运行，则检查将失败。

- 启动控制器更换操作并完成预检后，此操作将暂停，以便您稍后在配置 node3 时收集可能需要的输出信息。

如果您的系统(例如700)具有以下配置、则在开始升级之前、您可以将集群AFF迁移并将其重新归位到每个节点的两个集群端口：



- 每个节点两个以上的集群端口
- 以分支模式在插槽4中创建集群互连卡、用于创建端口e4a、e4b、e4c和e4D以及端口e4e、e4f、e4g和e4h

如果执行控制器升级时每个节点的集群端口数超过两个、则可能会导致升级后新控制器上的集群丢失。

有关详细信息，请参阅知识库文章 ["如何删除不需要或不必要的集群LUN"](#)。

4. 按照系统控制台上控制器更换操作步骤的指示运行以下一组命令。

从连接到每个节点的串行端口中、分别运行并保存以下命令的输出：

- `vserver services name-service dns show`
- `network interface show -curr-node <local> -role <cluster,intercluster,node-mgmt,cluster-mgmt,data>`
- `network port show -node <local> -type physical`
- `service-processor show -node <local> -instance`
- `network fcp adapter show -node <local>`
- `network port ifgrp show -node <local>`
- `system node show -instance -node <local>`
- `run -node <local> sysconfig`
- `storage aggregate show -r`
- `storage aggregate show -node <local>`
- `volume show -node <local>`
- `system license show -owner <local>`
- `s存储加密磁盘 show`
- `s安全密钥管理器板载 show-backup`
- `security key-manager external show`
- `s安全密钥管理器外部 show-status`
- `network port reachability show -detail -node <local>`



如果正在使用使用板载密钥管理器(OKM)的NetApp卷加密(NVE)或NetApp聚合加密(NAE)、请准备好密钥管理器密码短语、以便稍后在操作步骤中完成密钥管理器重新同步。

5. 如果您的系统使用自加密驱动器、请参见知识库文章 ["如何判断驱动器是否已通过FIPS认证"](#) 确定要升级的HA对上使用的自加密驱动器的类型。ONTAP 软件支持两种类型的自加密驱动器：

- 经FIPS认证的NetApp存储加密(NSE) SAS或NVMe驱动器

- 非FIPS自加密NVMe驱动器(SED)

["了解有关支持的自加密驱动器的更多信息"](#)。

如果 **ARL** 预检失败，请更正聚合所有权

如果聚合状态检查失败，您必须将配对节点拥有的聚合返回到主所有者节点，然后重新启动预检过程。

步骤

1. 将配对节点当前拥有的聚合返回到主所有者节点：

```
s存储聚合重新定位 start -node source_node-destination destination-node-aggregate  
-list *
```

2. 验证 node1 和 node2 均不拥有其当前所有者（而不是主所有者）的聚合：

```
storage aggregate show -nodes node_name-is-home false -fields owner-name, home-  
name, state
```

以下示例显示了当节点同时是聚合的当前所有者和主所有者时命令的输出：

```
cluster::> storage aggregate show -nodes node1 -is-home true -fields  
owner-name,home-name,state  
aggregate    home-name    owner-name    state  
-----  
aggr1        node1        node1         online  
aggr2        node1        node1         online  
aggr3        node1        node1         online  
aggr4        node1        node1         online  
  
4 entries were displayed.
```

完成后

您必须重新启动控制器更换过程：

```
ssystem controller replace start -nodes node_names
```

许可证

有关ONTAP许可的详细信息，请参见 ["许可证管理"](#)。



在控制器上使用未经许可的功能可能会使您无法遵守许可协议。

使用板载密钥管理器管理存储加密

您可以使用板载密钥管理器(OKM)管理加密密钥。如果您已设置OKM、则必须先记录密码

短语和备份材料、然后再开始升级。

步骤

1. 记录集群范围的密码短语。

这是在使用命令行界面或REST API配置或更新OKM时输入的密码短语。

2. 运行以备份密钥管理器信息 `security key-manager onboard show-backup` 命令：

暂停 **SnapMirror** 关系（可选）。

在继续使用操作步骤之前，您必须确认所有 SnapMirror 关系均已暂停。暂停 SnapMirror 关系后，它会在重新启动和故障转移后保持静默状态。

步骤

1. 验证目标集群上的 SnapMirror 关系状态：

```
snapmirror show
```



如果状态为"Transferring"、则必须中止这些传输：`snapmirror abort -destination -vserver vservers_name`

如果 SnapMirror 关系未处于 "正在传输" 状态，则中止将失败。

2. 暂停集群之间的所有关系：

```
snapmirror quiesce -destination-vserver *
```

第 2 阶段。重新定位和停用节点 1

第2阶段概述

在阶段2中、您会将node1非根聚合和NAS数据LIF重新定位到node2。此过程大部分是自动完成的；操作将暂停，以便您可以检查其状态。您必须手动恢复此操作。如果需要、您可以重新定位失败或被否决的聚合。此外、您还会记录必要的node1信息、停用node1、并准备稍后在操作步骤中启动node3和node4。

步骤

1. "将节点 1 拥有的非根聚合和 NAS 数据 LIF 重新定位到节点 2"
2. "重新定位失败或被否决的聚合"
3. "停用 node1"
4. "准备网络启动"

将节点 1 拥有的非根聚合和 **NAS** 数据 **LIF** 重新定位到节点 2

在将 node1 替换为 node3 之前，必须先将非根聚合和 NAS 数据 LIF 从 node1 移动到

node2，然后再最终将 node1 的资源移动到 node3。

开始之前

开始任务时，此操作应已暂停；您必须手动恢复此操作。

关于此任务

迁移聚合和 LIF 后，此操作将暂停以进行验证。在此阶段，您必须验证是否所有非根聚合和非 SAN 数据 LIF 都已迁移到 node3。



不会修改聚合和 LIF 的主所有者；只会修改当前所有者。

步骤

1. 恢复聚合重新定位和 NAS 数据 LIF 移动操作：

`s`系统控制器更换恢复

所有非根聚合和 NAS 数据 LIF 都会从 node1 迁移到 node2。

此操作将暂停，以便验证是否已将所有 node1 非根聚合和非 SAN 数据 LIF 迁移到 node2。

2. 检查聚合重新定位和 NAS 数据 LIF 移动操作的状态：

`s`系统控制器更换 `show-details`

3. 在操作仍处于暂停状态的情况下，验证所有非根聚合在 node2 上的状态是否均处于联机状态：

```
storage aggregate show -node node2-state online -root false
```

以下示例显示 node2 上的非根聚合处于联机状态：

```
cluster::> storage aggregate show -node node2 state online -root false

Aggregate  Size      Available  Used%  State  #Vols  Nodes  RAID  Status
-----
-----
aggr_1     744.9GB  744.8GB   0%     online  5     node2
raid_dp,normal
aggr_2     825.0GB  825.0GB   0%     online  1     node2
raid_dp,normal
2 entries were displayed.
```

如果 node2 上的聚合脱机或变为外部聚合，请在 node2 上使用以下命令将其联机，每个聚合一次：

```
storage aggregate online -aggregate aggr_name
```

4. 在 node2 上使用以下命令并检查其输出，以验证 node2 上的所有卷是否联机：

```
volume show -node node2-state offline
```

如果 node2 上的任何卷脱机，请在 node2 上使用以下命令将其联机，每个卷一次：

```
volume online -vserver vserver_name-volume volume_name
```

要与此命令结合使用的 `vserver_name` 可在上一个 `volume show` 命令的输出中找到。

5. 步骤 5]] 如果任何 LIF 已关闭，请使用以下命令将 LIF 的管理状态设置为 up，每个 LIF 一次：

```
network interface modify -vserver vserver_name-lif LIF_name-home-node nodename  
-status-admin up
```

重新定位失败或被否决的聚合

如果任何聚合无法重新定位或被否决，您必须手动重新定位聚合，或者在必要时覆盖否决或目标检查。

关于此任务

由于此错误，重新定位操作将暂停。

步骤

1. 检查事件管理系统（EMS）日志以确定聚合无法重新定位或被否决的原因。
2. 重新定位任何出现故障或被否决的聚合：

```
s存储聚合重新定位start -node node1-destination node2-aggregate-list aggr_name-no  
-controller-upgrade true
```

3. 出现提示时，输入 y。
4. 您可以使用以下方法之一强制重新定位：

选项	Description
覆盖否决检查	使用以下命令：storage aggregate relocation start -node node1 -destination node2 -aggregate-list aggr_list-no-controller-upgrade true -override -vetoes true
覆盖目标检查	使用以下命令：storage aggregate relocation start -node node1 -destination node2 -aggregate-list aggr_list-no-controller-upgrade true -override -vetoes true -override-destination-checks true

停用 node1

要停用 node1，您需要恢复自动操作，以便使用 node2 禁用 HA 对并正确关闭 node1。稍后在操作步骤中，您将 node1 从机架或机箱中卸下。

步骤

1. 恢复操作：

s 系统控制器更换恢复

2. 验证 node1 是否已暂停：

```
s 系统控制器更换 show-details
```

完成后

升级完成后，您可以停用 node1。请参见 ["停用旧系统"](#)。

准备网络启动

在操作步骤中物理装入 node3 和 node4 后，您可能需要通过网络启动它们。术语 netboot 表示从远程服务器上存储的 ONTAP 映像启动。准备网络启动时，您会将 ONTAP 9 启动映像的副本放置到系统可以访问的 Web 服务器上。

您也可以使用 USB 启动选项执行网络启动。请参见知识库文章 ["如何使用 boot_recovery loader 命令安装 ONTAP 以进行系统初始设置"](#)。

开始之前

- 确认您可以使用系统访问 HTTP 服务器。
- 请参见 ["参考资料"](#) 链接到 [_NetApp 支持站点_](#) 并下载适用于您的平台和正确版本的 ONTAP 的必要系统文件。

关于此任务

如果新控制器上安装的 ONTAP 9 版本与原始控制器上安装的版本不同，则必须通过网络启动这些控制器。安装每个新控制器后，您可以从 Web 服务器上存储的 ONTAP 9 映像启动系统。然后，您可以将正确的文件下载到启动介质设备，以供后续系统启动。

步骤

1. 访问 NetApp 支持站点以下载用于执行系统网络启动的文件。
2. 从 NetApp 支持站点的软件下载部分下载相应的 ONTAP 软件，并将 ``<ontap_version>_image.tgz`` 文件存储在可通过 Web 访问的目录中。
3. 切换到可通过 Web 访问的目录，并验证所需文件是否可用。

您的目录列表应包含以下文件：

```
<ontap_version>_image.tgz
```



您不需要提取 `ontap_version_image.tgz` 文件的内容。

您将使用中目录中的信息 ["第 3 阶段"](#)。

第 3 阶段。安装并启动 node3

第3阶段概述

在第 3 阶段，您安装并启动 node3，检查 node1 中的集群和节点管理端口是否在 node3

上联机，并验证 node3 安装。如果您使用的是NetApp卷加密(NVE)、则需要还原密钥管理器配置。您还可以将node1 NAS数据LIF和非根聚合从node2重新定位到node3、并验证node3上是否存在SAN LIF。

步骤

1. "安装并启动 node3"
2. "验证 node3 安装"
3. "还原 node3 上的 key-manager 配置"
4. "将 node1 拥有的非根聚合和 NAS 数据 LIF 从 node2 移动到 node3"

安装并启动 node3

您可以在机架中安装node3、将node1的连接传输到node3、启动node3并安装ONTAP。然后、如本节所述、重新分配node1的任何备用磁盘、属于根卷的任何磁盘以及此过程之前未重新定位到node2的任何非根聚合。

关于此任务

重新定位操作在此阶段开始时暂停。此过程大部分是自动完成的；操作将暂停，以便您可以检查其状态。您必须手动恢复此操作。此外、您还必须验证SAN LIFs是否已成功联机并分配给node3上的正确FC物理端口。

如果 node3 与 node1 上安装的 ONTAP 9 版本不同，则需要对其进行网络启动。安装 node3 后，从 Web 服务器上存储的 ONTAP 9 映像启动它。然后，您可以按照中的说明将正确的文件下载到启动介质设备，以供后续系统启动 "准备网络启动"。

步骤

1. 【 auto_install3_step1】请确保为 node3 预留机架空间。

新节点的空间和高度要求可能与现有节点不同。规划升级场景的空间要求。
2. 【 auto_install3_step2】按照适用于您的节点型号的 *Installation and Setup Instructions* 在机架中安装 node3。
3. 【 auto_install3_step3】为节点 3 布线，将连接从节点 1 移动到节点 3。

从ONTAP 9.15.1开始、新控制器型号只有一个"扳手"端口用于底板管理控制器(BMC)和管理连接。相应地规划布线更改。

- 控制台（远程管理端口）
- 集群和HA端口
- 数据端口
- 集群和节点管理端口
- 串行连接SCSI (SAS)和以太网存储端口
- SAN配置：iSCSI以太网、FC和NVMe/FC交换机端口

您可能需要更改新旧控制器之间的互连缆线、以便在不同控制器和卡型号之间实现互操作。有关适用于您的系统的以太网存储架的布线图、请参见 ["系统安装过程"](#)。



对于ONTAP 9.151及更高版本中引入的控制器、集群和HA互连使用相同的端口。对于连接交换机的配置、需要将类似端口连接到同一集群交换机。例如、从现有控制器升级到AFF A1K时、您应将两个节点上的e1a端口连接到一个交换机、并将两个节点上的e7a端口连接到第二个交换机。

4. 【auto_install3_step4】打开 node3 的电源，然后在控制台终端按 Ctrl-C 访问启动环境提示符，以中断启动过程。



启动 node3 时，您可能会看到以下警告消息：

```
WARNING: The battery is unfit to retain data during a power outage. This
is likely because the battery is discharged but could be due to other
temporary conditions.
When the battery is ready, the boot process will complete and services
will be engaged.
To override this delay, press 'c' followed by 'Enter'
```

5. 如果您在中看到警告消息，则需要执行以下操作 [第 4 步](#)，执行以下操作：
 - a. 检查是否存在任何可能指示 NVRAM 电池电量低以外问题的控制台消息，如有必要，请采取任何必要的更正措施。
 - b. 让电池充电并完成启动过程。



* 注意：请勿覆盖延迟；如果不允许电池充电，可能会导致数据丢失。 *




请参见 ["准备网络启动"](#)。

6. 【第 6 步】选择以下操作之一，配置网络启动连接。



您必须使用管理端口和 IP 作为网络启动连接。请勿使用数据 LIF IP，否则在执行升级期间可能会发生数据中断。

动态主机配置协议（DHCP）	那么 ...
正在运行	在启动环境提示符处使用以下命令自动配置连接： <code>ifconfig e0M -auto</code>

动态主机配置协议 (DHCP)	那么 ...
未运行	<p>在启动环境提示符处使用以下命令手动配置连接：</p> <pre>ifconfig e0M -addr=filer_addr -mask=netmask -gw=gateway -dns=dns_addr -domain=dns_domain</pre> <p><i>filer_addr</i> 是存储系统的IP地址(必填)。 <i>netmask</i> 是存储系统的网络掩码(必需)。 <i>gateway</i> 是存储系统的网关(必需)。 <i>dns_addr</i> 是网络上名称服务器的IP地址(可选)。 <i>dns_domain</i> 是域名服务(DNS)域名(可选)。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;">  您的接口可能需要其他参数。有关详细信息，请在固件提示符处输入 <code>help ifconfig</code>。 </div>

7. 【第 7 步】对 node3 执行网络启动：

```
netboot http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz
```

`<path_to_the_web-accessible_directory>` 应指向您在部分中下载 `<ontap_version>_image.tgz` 的位置 "[准备网络启动](#)"。



请勿中断启动。

8. 【第 8 步】从启动菜单中选择选项 `(7) 首先安装新软件`。

此菜单选项可下载新的 ONTAP 映像并将其安装到启动设备中。

请忽略以下消息：

```
This procedure is not supported for Non-Disruptive Upgrade on an HA pair
```

注意适用场景可无中断升级 ONTAP，而不是升级控制器。



请始终使用 netboot 将新节点更新为所需映像。如果您使用其他方法在新控制器上安装映像，则可能会安装不正确的映像。此问题描述适用场景所有 ONTAP 版本。netboot 操作步骤与选项结合使用 (7) Install new software 擦除启动介质并将相同的 ONTAP 版本放置在两个映像分区上。

9. 【第 9 步】如果系统提示您继续运行操作步骤，请输入 `y`，当系统提示您输入软件包时，请输入 URL：

```
`http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz`
```

10. 【第 10 步】完成以下子步骤以重新启动控制器模块：

a. 出现以下提示时，输入 `n` 以跳过备份恢复：

```
d要立即还原备份配置? { y|n }
```

b. 出现以下提示时，输入 `y` 以重新启动：

要开始使用新安装的软件，必须重新启动节点。是否要立即重新启动？ { `y|n` }

控制器模块重新启动，但停留在启动菜单处，因为启动设备已重新格式化，并且必须还原配置数据。

11. 【第 11 步】从启动菜单中选择维护模式 5，并在系统提示您继续启动时输入 `y`。

12. 【第 12 步】验证控制器和机箱是否配置为 `ha`：

```
ha-config show
```

以下示例显示了 `ha-config show` 命令的输出：

```
Chassis HA configuration: ha
Controller HA configuration: ha
```



系统会在 PROM 中记录它们是采用 HA 对还是独立配置。独立系统或 HA 对中的所有组件的状态都必须相同。

13. 如果控制器和机箱未配置为 `ha`，请使用以下命令更正配置：

```
ha-config modify controller ha
```

```
ha-config modify chassis ha
```

14. 确认用于连接到以太网磁盘架的所有以太网端口均已配置为存储：

```
storage port show
```

显示的输出取决于系统配置。以下输出示例适用于插槽 11 中具有单个存储卡的节点。您的系统输出可能有所不同：

```
*> storage port show
Port Type Mode      Speed (Gb/s) State      Status  VLAN ID
---- ---- -
e11a ENET storage 100 Gb/s   enabled   online  30
e11b ENET storage 100 Gb/s   enabled   online  30
```

15. 修改未设置为 `storage` 的端口：

```
storage port modify -p <port> -m storage
```

连接到存储架的所有以太网端口都必须配置为存储、才能访问磁盘和磁盘架。

16. 退出维护模式：

```
halt
```

在启动环境提示符处按 `Ctrl-C` 以中断自动启动。

17. 在 node2 上，检查系统日期，时间和时区：

```
date
```

18. 在 node3 上，在启动环境提示符处使用以下命令检查日期：

```
s如何选择日期
```

19. 如有必要，请在 node3 上设置日期：

```
set date <mm/dd/yyyy>
```

20. 在 node3 上，在启动环境提示符处使用以下命令检查时间：

```
s时间
```

21. 如有必要，请在 node3 上设置时间：

```
set time <hh:mm:ss>
```

22. 在启动加载程序中、设置node3上的配对系统ID：

```
setenv partner-sysid <node2_sysid>
```

对于node3、 partner-sysid 必须为node2的。

- a. 保存设置：

```
saveenv
```

23. 【auto_install3_step21】验证 partner-sysid 对于node3：

```
printenv partner-sysid
```

24. 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	<code>setenv bootarg.storageencryption.support true</code>
NetApp非FIPS SED	<code>setenv bootarg.storageencryption.support false</code>

- 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"](#)。

25. 启动节点进入启动菜单：

`boot_ontap` 菜单

26. 在node3上，转到启动菜单，然后使用22/7选择隐藏选项 `boot_after_controller_replacement`。在提示符处，输入 `node1` 以将 `node1` 的磁盘重新分配给 `node3`，如以下示例所示。

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>
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:

```



在上述控制台输出示例中，如果系统使用高级磁盘分区（ADP）磁盘，ONTAP 将提示您输入配对节点名称。

27. 如果系统进入重新启动循环并显示消息 `no disks found`，则表示磁盘重新分配出现问题。要解决此问题、请参见 ["故障排除"](#)。
28. 在自动启动期间、按 `Ctrl-C` 以在提示符处停止节点 `LOADER>`。
29. 在加载程序提示符处、进入维护模式：

```
boot_ontap maint
```

30. 验证磁盘连接、控制器型号字符串、HA配置以及其他硬件连接相关详细信息。
31. 退出维护模式：

```
halt
```

32. 在加载程序提示符处、启动：

```
boot_ontap 菜单
```

现在，在启动时，节点可以检测到先前分配给它的所有磁盘，并可按预期启动。

如果要更换的集群节点使用根卷加密、则ONTAP无法从磁盘中读取卷信息。还原根卷的密钥。



只有当根卷使用NetApp卷加密时、此操作才适用。

- a. 返回到特殊的启动菜单：

```
LOADER> boot_ontap menu
```

```
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
```

b. 选择*(10)设置板载密钥管理器恢复密钥*

c. 输入 ... y 在以下提示符处:

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

d. 在提示符处、输入密钥管理器密码短语。

e. 出现提示时、输入备份数据。



您必须已在中获取密码短语和备份数据 "[准备要升级的节点](#)" section of this procedure.

f. 系统重新启动到特殊启动菜单后、运行选项*(1) Normal Boot*



您可能会在此阶段遇到错误。如果出现错误、请重复中的子步骤、[步骤32](#)。直到系统正常启动为止。

验证 node3 安装

您必须验证 node1 中的物理端口是否正确映射到 node3 上的物理端口。这样，node3 便可在升级后与集群中的其他节点以及网络进行通信。

关于此任务

请参见 "[参考资料](#)" 链接到 *Node Hardware Universe* 以捕获有关新节点上端口的信息。您将在本节稍后部分使用此信息。

物理端口布局可能因节点型号而异。当新节点启动时，ONTAP 将尝试确定应托管集群 LIF 的端口，以便自动达到仲裁。

如果 node1 上的物理端口未直接映射到 node3 上的物理端口，请执行下一节 [还原 node3 上的网络配置](#) 必须用于修复网络连接。

安装并启动 node3 后，您必须验证是否已正确安装它。您必须等待 node3 加入仲裁，然后恢复重新定位操作。

此时，在操作步骤中，操作将暂停，因为 node3 加入仲裁。

步骤

1. 验证 node3 是否已加入仲裁：

```
cluster show -node node3 -fields health
```

health 字段的输出应为 true。

2. 确认 node3 与 node2 属于同一集群，并且运行状况良好：

```
cluster show
```

3. 切换到高级权限模式：

```
set advanced
```

4. 检查控制器更换操作的状态，并验证其是否处于暂停状态，以及是否处于 node1 暂停之前的状态，以便执行安装新控制器和移动缆线的物理任务：

```
ssystem controller replace show
```

```
s系统控制器更换 show-details
```

5. 恢复控制器更换操作：

```
s系统控制器更换恢复
```

6. 控制器更换将暂停以进行干预，并显示以下消息：

```

Cluster::*> system controller replace show
Node                Status                Error-Action
-----
Node1(now node3) Paused-for-intervention  Follow the instructions
given in
Step Details
Node2                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 VLAN*，*ifgrp* 和 *broadcast domains* 一节已重命名为 *_Restore node3* 上的网络配置。

7. 在控制器更换处于暂停状态的情况下，继续执行本文档的下一节以还原节点上的网络配置。

还原 node3 上的网络配置

确认 node3 处于仲裁状态并可与 node2 通信后，请确认 node3 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 node3 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*。

步骤

1. 列出已升级的 node1（称为 node3）上的所有物理端口：

```
network port show -node node3
```

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哪些端口必须用作接口组成员端口，VLAN 基本端口或独立物理端口来托管 LIF。

2. 列出集群上的广播域：

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

3. 列出node3上所有端口的网络端口可访问情况：

网络端口可访问性显示

您应看到类似于以下示例的输出：

```
ClusterA::*> network port reachability show
Node      Port      Expected Reachability      Reachability
Status
-----
node1_node3
      e0M      Default:Mgmt      ok
      e10a      Default:Default      ok
      e10b      -      no-reachability
      e10c      Default:Default      ok
      e10d      -      no-reachability
      e1a      Cluster:Cluster      ok
      e1b      -      no-reachability
      e7a      Cluster:Cluster      ok
      e7b      -      no-reachability
node2_node4
      e0M      Default:Mgmt      ok
      e4a      Default:Default      ok
      e4b      -      no-reachability
      e4c      Default:Default      ok
      e4d      -      no-reachability
      e3a      Cluster:Cluster      ok
      e3b      Cluster:Cluster      ok
18 entries were displayed.
```

在上面的示例中，node1_node3 是在更换控制器后刚刚启动的。某些端口无法访问其预期广播域，必须进行修复。

4. **【 auto_verify_3_step4】** 修复 node3 上每个端口的可访问性状态不是 ok 的可访问性。首先对任何物理端口运行以下命令，然后对任何 VLAN 端口运行以下命令，一次运行一个：

```
network port reachability repair -node <node_name> -port <port_name>
```

您应看到类似于以下示例的输出：

```
Cluster ::> reachability repair -node nodel_node3 -port e4a
```

```
Warning: Repairing port "nodel_node3: e4a" 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，应显示一条警告消息，如上所示。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. 如果接口组配置与新控制器物理端口布局不匹配，请按照以下步骤进行修改。

- a. 您必须先从其广播域成员资格中删除接口组成员端口的物理端口。您可以使用以下命令执行此操作：

```
network port broadcast-domain remove-ports -broadcast-domain <broadcast-
domain_name> -ports <node_name:port_name>
```

- b. 将成员端口添加到接口组：

```
network port ifgrp add-port -node <node_name> -ifgrp <ifgrp> -port
<port_name>
```

- c. 在添加第一个成员端口后大约一分钟，接口组会自动添加到广播域中。

- d. 验证接口组是否已添加到相应的广播域：

```
network port reachability show -node <node_name> -port <ifgrp>
```

如果接口组的可访问性状态为 NOT ok，请将其分配给相应的广播域：

```
network port broadcast-domain add-ports -broadcast-domain
<broadcast_domain_name> -ports <node:port>
```

6. 按照以下步骤将适当的物理端口分配给 Cluster 广播域：

- a. 确定哪些端口可访问 集群 广播域：

```
network port reachability show -reachable-broadcast-domains cluster : 集群
```

- b. 如果可访问性状态不是 正常，请修复可访问 集群 广播域的任何端口：

```
network port reachability repair -node <node_name> -port <port_name>
```

7. 使用以下命令之一将其余物理端口移动到其正确的广播域中：

```
network port reachability repair -node <node_name> -port <port_name>
```

```
network port broadcast-domain remove-port
```

```
网络端口 broadcast-domain add-port
```

确认不存在不可访问或意外的端口。使用以下命令并检查输出以确认状态为 `ok`，以检查所有物理端口的可访问性状态：

```
网络端口可访问性 show -detail
```

8. 使用以下步骤还原可能已被替换的任何 VLAN：

- a. 列出已替换的 VLAN：

```
cluster controller-replacement network placed-vlans show
```

此时应显示如下输出：

```
Cluster::*> displaced-vlans show
(cluster controller-replacement network displaced-vlans show)
      Original
Node   Base Port   VLANs
-----
Node1  a0a         822, 823
      e4a         822, 823
2 entries were displayed.
```

- b. 还原从先前的基本端口中替换的 VLAN：

```
cluster controller-replacement network placed-vlans restore
```

以下示例显示了将已从接口组 `a0a` 中移出的 VLAN 还原到同一接口组的过程：

```
Cluster::*> displaced-vlans restore -node node1_node3 -port a0a
-destination-port a0a
```

以下是将端口 `"e9a"` 上的已替换 VLAN 还原到 `e9d` 的示例：

```
Cluster::*> displaced-vlans restore -node node1_node3 -port e9a
-destination-port e9d
```

成功还原 VLAN 后，将在指定的目标端口上创建已替换的 VLAN。如果目标端口是接口组的成员或目标端口已关闭，则 VLAN 还原将失败。

等待大约一分钟，以便将新还原的 VLAN 放置到其相应的广播域中。

- a. 根据需要为不在`cluster controller-replacement network placed-vlans show`输出中但应在其他物理端口上配置的VLAN端口创建新的VLAN端口。

9. 完成所有端口修复后，删除任何空广播域：

```
network port broadcast-domain delete -broadcast-domain <broadcast_domain_name>
```

10. 【第 10 步】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](#)。

11. 验证所有端口是否均已置于广播域中：

```
network port show
```

12. 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
```

13. 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：

```
cluster controller-replacement network displaced-interface restore-home-node  
-node <node_name> -vserver <vserver_name> -lif-name <LIF_name>
```

14. 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 node3 上的 key-manager 配置

如果要使用NetApp卷加密(NVE)和NetApp聚合加密(NAE)对要升级的系统上的卷进行加密、则必须将加密配置同步到新节点。如果不同步密钥管理器、则在使用ARL将node1聚合从node2重新定位到node3时、可能会发生故障、因为node3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node3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node3上的SVM-KEK密钥是否已还原为"true":

```
::> security key-manager key query -node node3 -fields restored -key  
-type SVM-KEK
```

示例

```
::> security key-manager key query -node node3 -fields restored -key  
-type SVM-KEK
```

node	vserver	key-server	key-id
restored			
-----	-----	-----	-----
node3	svml	""	0000000000000000020000000000a008a81976
true			2190178f9350e071fbb90f000000000000000

将 node1 拥有的非根聚合和 NAS 数据 LIF 从 node2 移动到 node3

在验证 node3 上的网络配置以及将聚合从 node2 重新定位到 node3 之前，您必须验证当前位于 node2 上的 node1 所属的 NAS 数据 LIF 是否已从 node2 重新定位到 node3。您还必须验证 node3 上是否存在 SAN LIF。

关于此任务

在升级操作步骤期间，远程 LIF 处理 SAN LUN 的流量。升级期间，集群或服务运行状况无需移动 SAN LIF。除非需要将 SAN LIF 映射到新端口，否则不会移动这些 LIF。使 node3 联机后，您将验证 LIF 是否运行正常并位于相应的端口上。

步骤

1. iSCSI LUN会通过可访问的扫描自动查找正确的主端口。FC和NVMe/FC SAN LUN不会自动移动。升级之前、它们仍会显示其所在的主端口。

检查node3上的SAN Sifs:

- a. 修改向新数据端口报告"已关闭"操作状态的任何iSCSI SAN LUN:

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif> admin down  
  
network interface modify -vserver <vserver> -lif <iscsi_san_lif> port  
<new_port> node <node>
```

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif>
```

- b. 修改新控制器的主端口并向新控制器上的FCP端口报告"已关闭"运行状态的任何FC和NVMe/FC SAN LIFs:

```
network interface modify -vserver <vserver> -lif <fc_san_lif> admin down
```

```
network interface modify -vserver <vserver> -lif <fc_san_lif> port  
<new_port> node <node>
```

```
network interface modify -vserver <vserver> -lif <fc_san_lif>
```

2. 恢复重新定位操作:

s系统控制器更换恢复

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

此操作将在网络可访问性检查的此阶段暂停。

3. 恢复重新定位操作:

s系统控制器更换恢复

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 node1 拥有的非根聚合和 NAS 数据 LIF 重新定位到新控制器 node3。资源重新定位完成后, 控制器更换操作将暂停。

4. 检查聚合重新定位和 NAS 数据 LIF 移动操作的状态:

```
s系统控制器更换 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。

5. 如有必要, 还原和还原任何已替换的 LIF。列出所有已替换的 LIF:

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

如果已替换任何 LIF, 请将主节点还原回 node3:

```
cluster controller-replacement network placed-interface restore-home-node
```

6. 恢复此操作以提示系统执行所需的后检查：

s 系统控制器更换恢复

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

第 4 阶段。重新定位和停用节点 2

第4阶段概述

在阶段4中、您会将非根聚合和NAS数据LIF从node2重新定位到node3。此外、您还会记录必要的node2信息、以供稍后在操作步骤中使用、然后停用node2。

步骤

1. "将非根聚合和 NAS 数据 LIF 从 node2 重新定位到 node3"
2. "停用 node2"

将非根聚合和 NAS 数据 LIF 从 node2 重新定位到 node3

在将node2替换为node4之前、您需要将node2所拥有的非根聚合和NAS数据生命周期重新定位到node3。

开始之前

上一阶段的后处理检查完成后，node2 的资源释放将自动启动。非根聚合和非 SAN 数据 LIF 将从 node2 迁移到 node3。

关于此任务

在升级操作步骤期间，远程 LIF 处理 SAN LUN 的流量。升级期间，集群或服务运行状况无需移动 SAN LIF。

迁移聚合和 LIF 后，此操作将暂停以进行验证。在此阶段，您必须验证是否所有非根聚合和非 SAN 数据 LIF 都已迁移到 node3。



不会修改聚合和 LIF 的主所有者；只会修改当前所有者。

步骤

1. 验证所有非根聚合是否均已联机及其在 node3 上的状态：

```
storage aggregate show -node node3-state online -root false
```

以下示例显示 node2 上的非根聚合处于联机状态：

```
cluster::> storage aggregate show -node node3 state online -root false

Aggregate      Size      Available  Used%  State  #Vols  Nodes
RAID          Status
-----
-----
aggr_1         744.9GB   744.8GB    0%     online  5      node2
raid_dp normal
aggr_2         825.0GB   825.0GB    0%     online  1      node2
raid_dp normal
2 entries were displayed.
```

如果 node3 上的聚合脱机或变为外部聚合，请在 node3 上使用以下命令将其联机，每个聚合一次：

```
storage aggregate online -aggregate aggr_name
```

2. 在 node3 上使用以下命令并检查输出，以验证 node3 上的所有卷是否联机：

```
volume show -node node3-state offline
```

如果 node3 上的任何卷脱机，请在 node3 上使用以下命令将其联机，每个卷一次：

```
volume online -vserver vservice_name-volume volume_name
```

要与此命令结合使用的 `vserver_name` 可在上一个 `volume show` 命令的输出中找到。

3. 验证 LIF 是否已移至正确的端口且状态为 up。如果任何 LIF 已关闭，请为每个 LIF 输入以下命令，将 LIF 的管理状态设置为 up：

```
network interface modify -vserver vservice_name-lif LIF_name-home-node
node_name-status-admin up
```

4. 如果新硬件上不存在当前托管数据 LIF 的端口，请将其从广播域中删除：

```
network port broadcast-domain remove-ports
```

5. 【第 5 步】输入以下命令并检查输出，验证 node2 上是否没有剩余数据 LIF：

```
network interface show -curr-node node2-role data
```

停用 node2

要停用 node2、首先应正确关闭 node2、然后将其从机架或机箱中卸下。

步骤

1. 恢复操作：

s系统控制器更换恢复

节点会自动暂停。

完成后

升级完成后，您可以停用 node2。请参见 ["停用旧系统"](#)。

第 5 阶段。安装并启动节点 4.

第5阶段概述

在第 5 阶段，您安装并启动 node4，检查 node2 中的集群和节点管理端口是否在 node4 上联机，并验证 node4 安装。如果您使用的是NVE、则需要还原密钥管理器配置。您还可以将node2 NAS数据LIF和非根聚合从node3重新定位到node4、并验证node4上是否存在SAN LIF。

步骤

1. ["安装并启动节点 4."](#)
2. ["验证 node4 安装"](#)
3. ["还原 node4 上的 key-manager 配置"](#)
4. ["将 node2 拥有的非根聚合和 NAS 数据 LIF 从 node3 移动到 node4"](#)

安装并启动节点 4.

您可以在机架中安装node4、将node2的连接传输到node4、启动node4并安装ONTAP。然后、如本节所述、重新分配node2的任何备用磁盘、属于根卷的任何磁盘以及此过程之前未重新定位到node3的任何非根聚合。

关于此任务

重新定位操作在此阶段开始时暂停。此过程大部分是自动完成的；此操作将暂停以使您能够检查其状态。您必须手动恢复此操作。

如果 node4 的 ONTAP 9 版本与 node2 上安装的版本不同，则需要对其进行网络启动。安装 node4 后，从 Web 服务器上存储的 ONTAP 9 映像启动它。然后，您可以按照中的说明将正确的文件下载到启动介质设备，以供后续系统启动 ["准备网络启动"](#)。

步骤

1. `【 auto_install4_step1】` 确保 node4 具有足够的机架空间。

如果 node4 与 node2 位于不同的机箱中，则可以将 node4 与 node3 放在同一位置。如果 node2 和 node4 位于同一机箱中，则 node4 已位于其相应的机架位置。

2. 按照节点型号的 `_Installation and Setup Instructions_` 中的说明，在机架中安装 node4。

3. 为节点 4 布线，将连接从节点 2 移至节点 4。

按照node4平台的_安装和设置说明_或_FlexArray虚拟化安装要求和参考_中的说明、相应的磁盘架文档和_HA对管理_为以下连接布线。

请参见"参考资料"、以链接到_FlexArray虚拟化安装要求和参考_和_HA对管理_。

- 控制台（远程管理端口）
- 集群和HA端口
- 数据端口
- 集群和节点管理端口
- 串行连接SCSI (SAS)和以太网存储端口
- SAN配置：iSCSI以太网、FC和NVMe/FC交换机端口

您可能需要更改新旧控制器之间的互连缆线、以便在不同控制器和卡型号之间实现互操作。有关适用于您的系统的以太网存储架的布线图、请参见 "系统安装过程"。



对于ONTAP 9.151及更高版本中引入的控制器、集群和HA互连使用相同的端口。对于连接交换机的配置、需要将类似端口连接到同一集群交换机。例如、从现有控制器升级到AFF A1K时、您应将两个节点上的e1a端口连接到一个交换机、并将两个节点上的e7a端口连接到第二个交换机。

4. 打开 node4 的电源，然后在控制台终端按 Ctrl-C 以访问启动环境提示符，从而中断启动过程。



启动 node4 时，您可能会看到以下警告消息：

```
WARNING: The battery is unfit to retain data during a power outage. This
is likely
    because the battery is discharged but could be due to other
temporary
    conditions.
When the battery is ready, the boot process will complete
and services will be engaged. To override this delay, press 'c'
followed
    by 'Enter'
```

5. 如果您在步骤 4 中看到警告消息，请执行以下操作：

- a. 检查是否存在任何可能指示 NVRAM 电池电量低以外问题的控制台消息，如有必要，请采取任何必要的更正措施。
- b. 让电池充电并完成启动过程。



* 注意：请勿覆盖延迟；如果不允许电池充电，可能会导致数据丢失。 *



请参见 "准备网络启动"。

6. 通过选择以下操作之一来配置网络启动连接。



您必须使用管理端口和 IP 作为网络启动连接。请勿使用数据 LIF IP，否则在执行升级期间可能会发生数据中断。

动态主机配置协议 (DHCP)	那么 ...
正在运行	在启动环境提示符处使用以下命令自动配置连接： <code>ifconfig e0M -auto</code>
未运行	<p>在启动环境提示符处输入以下命令、以手动配置连接： <code>ifconfig e0M -addr=<i>filer_addr</i> -mask=<i>netmask</i> -gw=<i>gateway</i> -dns=<i>dns_addr</i> -domain=<i>dns_domain</i></code></p> <p><i>filer_addr</i> 是存储系统的IP地址(必填)。 <i>netmask</i> 是存储系统的网络掩码(必需)。 <i>gateway</i> 是存储系统的网关(必需)。 <i>dns_addr</i> 是网络上名称服务器的IP地址(可选)。 <i>dns_domain</i> 是DNS域名(可选)。</p> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 10px;"> <p>您的接口可能需要其他参数。有关详细信息，请在固件提示符处输入 <code>help ifconfig</code>。</p> </div>

7. 对 node4 执行网络启动：

```
netboot http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz
```

`<path_to_the_web-accessible_directory>` 应指向您在本节第 1 步中下载 `<ontap_version>_image.tgz` 的位置 "准备网络启动"。



请勿中断启动。

8. 从启动菜单中，选择选项 `(7) Install new software first` 。

此菜单选项可下载新的 ONTAP 映像并将其安装到启动设备中。

请忽略以下消息：

```
This procedure is not supported for Non-Disruptive Upgrade on an HA pair
```

注意适用场景可无中断升级 ONTAP，而不是升级控制器。



请始终使用 netboot 将新节点更新为所需映像。如果您使用其他方法在新控制器上安装映像，则可能会安装不正确的映像。此问题描述适用场景所有 ONTAP 版本。netboot 操作步骤 与选项结合使用 (7) Install new software 擦除启动介质并将相同的 ONTAP 版本放置在两个映像分区上。

9. 如果系统提示您继续运行操作步骤，请输入 `y`，并在系统提示您输入软件包时，输入 URL：

```
` http://<web_server_ip/path_to_web-accessible_directory>/<ontap_version>_image.tgz`
```

10. 完成以下子步骤以重新启动控制器模块：

a. 出现以下提示时，输入 `n` 以跳过备份恢复：

```
Do you want to restore the backup configuration now? {y|n}
```

b. 出现以下提示时，输入 `y` 以重新启动：

```
The node must be rebooted to start using the newly installed software. Do you want to reboot now? {y|n}
```

控制器模块重新启动，但停留在启动菜单处，因为启动设备已重新格式化，并且必须还原配置数据。

11. 从启动菜单中选择维护模式 `5`，并在系统提示您继续启动时输入 `y`。

12. 验证控制器和机箱是否已配置为 HA：

```
ha-config show
```

以下示例显示了 `ha-config show` 命令的输出：

```
Chassis HA configuration: ha
Controller HA configuration: ha
```



系统会在 PROM 中记录它们是采用 HA 对还是独立配置。独立系统或 HA 对中的所有组件的状态都必须相同。

13. 如果控制器和机箱未配置为 HA，请使用以下命令更正配置：

```
ha-config modify controller ha
```

```
ha-config modify chassis ha
```

14. 确认用于连接到以太网磁盘架的所有以太网端口均已配置为存储：

```
storage port show
```

显示的输出取决于系统配置。以下输出示例适用于插槽 11 中具有单个存储卡的节点。您的系统输出可能有所不同：


```
*> storage port show
Port Type Mode      Speed (Gb/s) State      Status  VLAN ID
-----
e11a ENET storage 100 Gb/s    enabled   online   30
e11b ENET storage 100 Gb/s    enabled   online   30
```

15. 修改未设置为storage的端口:

```
storage port modify -p <port> -m storage
```

连接到存储架的所有以太网端口都必须配置为存储、才能访问磁盘和磁盘架。

16. 退出维护模式:

```
halt
```

在启动环境提示符处按 Ctrl-C 中断自动启动。

17. 在 node3 上, 检查系统日期, 时间和时区:

```
date
```

18. 在 node4 上, 在启动环境提示符处使用以下命令检查日期:

```
s如何选择日期
```

19. 如有必要, 请在 node4 上设置日期:

```
set date <mm/dd/yyyy>
```

20. 在 node4 上, 在启动环境提示符处使用以下命令检查时间:

```
s时间
```

21. 如有必要, 请在 node4 上设置时间:

```
set time <hh:mm:ss>
```

22. 在启动加载程序中、设置node4上的配对系统ID:

```
setenv partner-sysid <node3_sysid>
```

对于node4、 partner-sysid 必须为node3的。

保存设置:

```
saveenv
```

23. 验证 partner-sysid 对于node4:

```
printenv partner-sysid
```

24. 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	<code>setenv bootarg.storageencryption.support true</code>
NetApp非FIPS SED	<code>setenv bootarg.storageencryption.support false</code>

- 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"](#)。

25. 启动节点进入启动菜单：

```
boot_ontap 菜单
```

26. 在node4上，转到启动菜单，然后使用22/7选择隐藏选项 `boot_after_controller_replacement`。在提示符处，输入 `node2` 以将 `node2` 的磁盘重新分配给 `node4`，如以下示例所示。

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>

Changing sysid of node node2 disks.

Fetches 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:

```



在上述控制台输出示例中，如果系统使用高级磁盘分区（ADP）磁盘，ONTAP 将提示您输入配对节点名称。

27. 在加载程序提示符处、启动：

boot_ontap 菜单

现在，在启动时，节点可以检测到先前分配给它的所有磁盘，并可按预期启动。

如果要更换的集群节点使用根卷加密、则ONTAP无法从磁盘中读取卷信息。还原根卷的密钥：

如果根卷已加密、请恢复板载密钥管理密钥、以便系统可以找到根卷。

a. 返回到特殊的启动菜单：

```
LOADER> boot_ontap menu
```

```
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
```

b. 选择*(10)设置板载密钥管理器恢复密钥*

c. 输入 ... y 在以下提示符处：

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

d. 在提示符处、输入密钥管理器密码短语。

e. 出现提示时、输入备份数据。



您必须已在中获取密码短语和备份数据 ["准备要升级的节点"](#) section of this procedure.

f. 系统重新启动到特殊启动菜单后、运行选项*(1) Normal Boot*



您可能会在此阶段遇到错误。如果出现错误、请重复中的子步骤、 [第27步](#) 直到系统正常启动为止。

验证 node4 安装

您必须验证 node2 中的物理端口是否正确映射到 node4 上的物理端口。这样， node4 便

可在升级后与集群中的其他节点以及网络进行通信。

关于此任务

请参见 ["参考资料"](#) 链接到 *Node Hardware Universe* 以捕获有关新节点上端口的信息。您将在本节稍后部分使用此信息。

物理端口布局可能因节点型号而异。当新节点启动时，ONTAP 将尝试确定应托管集群 LIF 的端口，以便自动达到仲裁。

如果 node2 上的物理端口未直接映射到 node4 上的物理端口，请执行下一节 [还原 node4 上的网络配置](#) 必须用于修复网络连接。

安装并启动 node4 后，您必须验证是否已正确安装它。您必须等待 node4 加入仲裁，然后恢复重新定位操作。

此时，在操作步骤中，操作将暂停，因为 node4 加入仲裁。

步骤

1. 验证 node4 是否已加入仲裁：

```
cluster show -node node4 -fields health
```

health 字段的输出应为 true。

2. 确认 node4 与 node3 属于同一集群，并且运行状况良好：

```
cluster show
```

3. 切换到高级权限模式：

```
set advanced
```

4. 检查控制器更换操作的状态，并验证它是否处于暂停状态以及 node2 暂停之前的相同状态，以便执行安装新控制器和移动缆线的物理任务：

```
ssystem controller replace show
```

```
s系统控制器更换 show-details
```

5. 恢复控制器更换操作：

```
s系统控制器更换恢复
```

6. 控制器更换将暂停以进行干预，并显示以下消息：

```

Cluster::*> system controller replace show
Node                Status                Error-Action
-----
Node2(now node4) Paused-for-intervention  Follow the instructions
given in
Node2                Step Details
Node2
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 *_restoring network configuration on node4*。

7. 在控制器更换处于暂停状态的情况下，继续执行本文档的下一节以还原节点上的网络配置。

还原 node4 上的网络配置

确认 node4 处于仲裁状态并可与 node3 通信后，请确认 node4 上显示了 node2 的 VLAN，接口组和广播域。此外，验证所有 node4 网络端口是否均已配置在其正确的广播域中。

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*。

步骤

1. 列出已升级的 node2（称为 node4）上的所有物理端口：

```
network port show -node node4
```

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 基本端口或独立物理端口来托管 LIF。

2. 列出集群上的广播域：

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

3. 列出节点 4 上所有端口的网络端口可访问性：

网络端口可访问性显示

命令的输出类似于以下示例：

```
ClusterA::*> network port reachability show
Node      Port      Expected Reachability      Reachability
Status
-----
node1_node3
          e0M      Default:Mgmt                ok
          e10a     Default:Default             ok
          e10b     -                            no-reachability
          e10c     Default:Default             ok
          e10d     -                            no-reachability
          e1a      Cluster:Cluster             ok
          e1b     -                            no-reachability
          e7a      Cluster:Cluster             ok
          e7b     -                            no-reachability
node2_node4
          e0M      Default:Mgmt                ok
          e10a     Default:Default             ok
          e10b     -                            no-reachability
          e10c     Default:Default             ok
          e10d     -                            no-reachability
          e1a      Cluster:Cluster             ok
          e1b     -                            no-reachability
          e7a      Cluster:Cluster             ok
          e7b     -                            no-reachability
18 entries were displayed.
```

在上面的示例中，node2_node4 是在更换控制器后刚刚启动的。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. 【auto_restore_4_Step4】修复 node4 上每个端口的可访问性状态不是 ok 的可访问性。首先对任何物理端口运行以下命令，然后对任何 VLAN 端口运行以下命令，一次运行一个：

```
network port reachability repair -node <node_name> -port <port_name>
```

输出如下所示：

```
Cluster ::> reachability repair -node node2_node4 -port e10a
```

```
Warning: Repairing port "node2_node4: e10a" 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，应显示一条警告消息，如上所示。

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. 如果接口组配置与新控制器物理端口布局不匹配，请按照以下步骤进行修改。
 - a. 您必须先从其广播域成员资格中删除接口组成员端口的物理端口。您可以使用以下命令执行此操作：

```
network port broadcast-domain remove-ports -broadcast-domain  
<broadcast_domain_name> -ports <node_name:port_name>
```

- b. 将成员端口添加到接口组：

```
network port ifgrp add-port -node <node_name> -ifgrp <ifgrp> -port  
<port_name>
```

- c. 在添加第一个成员端口后大约一分钟，接口组会自动添加到广播域中。
- d. 验证接口组是否已添加到相应的广播域：

```
network port reachability show -node <node_name> -port <ifgrp>
```

如果接口组的可访问性状态为 NOT ok，请将其分配给相应的广播域：

```
network port broadcast-domain add-ports -broadcast-domain  
<broadcast_domain_name> -ports <node:port>
```

6. 为 集群 广播域分配适当的物理端口:

a. 确定哪些端口可访问 集群 广播域:

```
network port reachability show -reachable-broadcast-domains cluster : 集群
```

b. 如果可访问性状态不是 正常 , 请修复可访问 集群 广播域的任何端口:

```
network port reachability repair -node <node_name> -port <port_name>
```

7. 使用以下命令之一将其余物理端口移动到你正确的广播域中:

```
network port reachability repair -node <node_name> -port <port_name>
```

```
network port broadcast-domain remove-port
```

```
网络端口 broadcast-domain add-port
```

确认不存在不可访问或意外的端口。使用以下命令并检查输出以确认状态为 ok , 以检查所有物理端口的可访问性状态:

```
网络端口可访问性 show -detail
```

8. 使用以下步骤还原可能已被替换的任何 VLAN :

a. 列出已替换的 VLAN :

```
cluster controller-replacement network placed-vlans show
```

此时应显示如下输出:

```
Cluster::*> displaced-vlans show
(cluster controller-replacement network displaced-vlans show)
      Original
Node   Base Port   VLANs
-----
Node1  a0a         822, 823
      e10a         822, 823
```

b. 还原从先前的基本端口中替换的 VLAN :

```
cluster controller-replacement network placed-vlans restore
```

以下示例显示了将已从接口组 a0a 中移出的 VLAN 还原到同一接口组的过程:

```
Cluster::*> displaced-vlans restore -node node2_node4 -port a0a
-destination-port a0a
```

以下是将端口 "e10a" 上的已替换 VLAN 还原到 "e10b" 的示例：

```
Cluster::*> displaced-vlans restore -node node2_node4 -port e10a
-destination-port e10b
```

成功还原 VLAN 后，将在指定的目标端口上创建已替换的 VLAN。如果目标端口是接口组的成员或目标端口已关闭，则 VLAN 还原将失败。

等待大约一分钟，以便将新还原的 VLAN 放置到其相应的广播域中。

- a. 根据需要为不在 `cluster controller-replacement network placed-vlans show` 输出中但应在其他物理端口上配置的 VLAN 端口创建新的 VLAN 端口。

9. 完成所有端口修复后，删除任何空广播域：

```
network port broadcast-domain delete -broadcast-domain <broadcast_domain_name>
```

10. 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](#)。

11. 验证所有端口是否均已置于广播域中：

```
network port show
```

12. 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
```

13. 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 主端口：

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

14. 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 node4 上的 key-manager 配置

如果要使用NetApp卷加密(NVE)和NetApp聚合加密(NAE)对要升级的系统上的卷进行加密、则必须将加密配置同步到新节点。如果不同步密钥管理器、则在使用ARL将node2聚合从node3重新定位到node4时、可能会发生故障、因为node4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node4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node4上的SVM-KEK密钥是否已还原为"true"：

```
::> security key-manager key query -node node4 -fields restored -key  
-type SVM-KEK
```

示例

```
::> security key-manager key query -node node4 -fields restored -key  
-type SVM-KEK
```

node	vserver	key-server	key-id
restored			
-----	-----	-----	-----
node4	svml	""	0000000000000000020000000000a008a81976
true			2190178f9350e071fbb90f000000000000000

将 node2 拥有的非根聚合和 NAS 数据 LIF 从 node3 移动到 node4

在验证 node4 上的网络配置以及将聚合从 node3 重新定位到 node4 之前，您必须验证当前位于 node3 上的 node2 所属的 NAS 数据 LIF 是否已从 node3 重新定位到 node4。您还必须验证 node4 上是否存在 SAN LIF。

关于此任务

在升级操作步骤期间，远程 LIF 处理 SAN LUN 的流量。升级期间，集群或服务运行状况无需移动 SAN LIF。除非需要将 SAN LIF 映射到新端口，否则不会移动这些 LIF。使 node4 联机后，您将验证 LIF 是否运行正常并位于相应的端口上。

步骤

1. iSCSI LUN会通过可访问的扫描自动查找正确的主端口。FC和NVMe/FC SAN LUN不会自动移动。升级之前、它们仍会显示其所在的主端口。

检查node4上的SAN Sifs:

- a. 修改向新数据端口报告"已关闭"操作状态的任何iSCSI SAN LUN:

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif> admin down
```

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif> port  
<new_port> node <node>
```

```
network interface modify -vserver <vserver> -lif <iscsi_san_lif>
```

- b. 修改新控制器的主端口并向新控制器上的FCP端口报告"已关闭"运行状态的任何FC和NVMe/FC SAN LIFs:

```
network interface modify -vserver <vserver> -lif <fc_san_lif> admin down
```

```
network interface modify -vserver <vserver> -lif <fc_san_lif> port  
<new_port> node <node>
```

```
network interface modify -vserver <vserver> -lif <fc_san_lif>
```

2. 恢复重新定位操作:

s系统控制器更换恢复

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

此操作将在网络可访问性检查的此阶段暂停。

3. 恢复重新定位操作:

s系统控制器更换恢复

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 node2 拥有的非根聚合和 NAS 数据 LIF 重新定位到新控制器 node4。资源重新定位完成后,控制器更换操作将暂停。

4. 检查聚合重新定位和 NAS 数据 LIF 移动操作的状态:

s系统控制器更换 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。

5. 如有必要，还原和还原任何已替换的 LIF 。列出所有已替换的 LIF ：

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

如果已替换任何 LIF ， 请将主节点还原回 node4 ：

```
cluster controller-replacement network placed-interface restore-home-node
```

6. 恢复此操作以提示系统执行所需的后检查：

s系统控制器更换恢复

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

第 6 阶段。完成升级

第6阶段概述

在第6阶段、您需要确认新节点设置正确、如果新节点启用了加密、则需要配置和设置存储加密或NetApp卷加密。您还应停用旧节点并恢复SnapMirror操作。

步骤

1. "使用 [KMIP 服务器管理身份验证](#)"
2. "确认新控制器设置正确"
3. "在新控制器模块上设置存储加密"
4. "在新控制器模块上设置NetApp卷或聚合加密"
5. "停用旧系统"
6. "恢复 [SnapMirror 操作](#)"

AFF A20、AFF A50、AFF A70、AFF A90、AFF A1K、FAS70和FAS90系统为集群和HA连接共享10GbE网络端口。这些系统可以支持与传统集群交换机建立10GbE或25GbE集群连接；但是、当不再需要10GbE和25GbE交换机时、NetApp建议更新到100GbE集群速度。有关详细信息，请参见以下知识库文章：



- ["如何在新的集群设置中配置10G或25G集群端口"](#)
- ["如何将现有10 G或25 G集群端口转换为40 G或100 G集群端口"](#)

对于集群和HA连接、AFF 2020系统会共享10GbE和25GbE网络端口。这些是AFF A20系统支持的唯一网络端口集群连接。

如果无法将现有节点上的e0a或e0b集群端口链接到新节点上的集群端口，请参见 ["NetApp错误在线中的错误ID COBTP-166978"](#)。

使用 KMIP 服务器管理身份验证

您可以使用密钥管理互操作性协议（Key Management Interoperability Protocol，KMIP）服务器管理身份验证密钥。

步骤

1. 添加新控制器：

```
s安全密钥管理器外部启用
```

2. 添加密钥管理器：

```
security key-manager external add-servers -key-servers  
key_management_server_ip_address
```

3. 验证密钥管理服务器是否已配置且可供集群中的所有节点使用：

```
s安全密钥管理器外部 show-status
```

4. 将所有链接的密钥管理服务器中的身份验证密钥还原到新节点：

```
sSecurity key-manager external restore -node new_controller_name
```

确认新控制器设置正确

要确认设置正确，必须启用 HA 对。此外，还必须验证 node3 和 node4 是否可以访问彼此的存储，并且它们都不拥有属于集群上其他节点的数据 LIF。此外，您还必须确认 node3 拥有 node1 的聚合，node4 拥有 node2 的聚合，并且两个节点的卷均联机。

步骤

1. 在对 node2 执行后检之后，将为 node2 集群启用存储故障转移和集群 HA 对。操作完成后，两个节点均显示为已完成，系统将执行一些清理操作。
2. 验证是否已启用存储故障转移：

s 存储故障转移显示

以下示例显示了启用存储故障转移时命令的输出：

```
cluster::> storage failover show
                Takeover
Node      Partner  Possible  State Description
-----  -
node3     node4    true      Connected to node4
node4     node3    true      Connected to node3
```

3. 使用以下命令并检查输出，验证 node3 和 node4 是否属于同一集群：

```
cluster show
```

4. 使用以下命令并检查输出，验证 node3 和 node4 是否可以访问彼此的存储：

```
storage failover show -fields local-missing-disks、partner-missing-disks
```

5. 使用以下命令并检查输出，验证 node3 和 node4 均不拥有集群中其他节点拥有的主数据 LIF：

```
network interface show
```

如果 node3 或 node4 都不拥有集群中其他节点拥有的主数据 LIF，请将数据 LIF 还原到其主所有者：

网络接口还原

6. 确认 node3 拥有 node1 中的聚合，而 node4 拥有 node2 中的聚合：

```
storage aggregate show -owner-name <node3>
```

```
storage aggregate show -owner-name <node4>
```

7. 确定是否有任何卷脱机：

```
volume show -node <node3> -state offline
```

```
volume show -node <node4> -state offline
```

8. 如果任何卷处于脱机状态，请将其与您在部分中捕获的脱机卷列表进行比较 ["准备要升级的节点"](#)，并根据需要使用以下命令使每个卷的任何脱机卷联机一次：

```
volume online -vserver <vserver_name> -volume <volume_name>
```

9. 对每个节点使用以下命令，为新节点安装新许可证：

```
system license add -license-code <license_code,license_code,license_code...>
```

license-code 参数接受一个包含 28 个大写字母字符密钥的列表。您可以一次添加一个许可证，也可以一次添加多个许可证，并以逗号分隔每个许可证密钥。

10. 使用以下命令之一从原始节点中删除所有旧许可证：

```
ssystem license clean-up -unused -expired
```

```
system license delete -serial-number <node_serial_number> -package  
<licensable_package>
```

- 删除所有已过期的许可证：

```
ssystem license clean-up -expired
```

- 删除所有未使用的许可证：

```
ssystem license clean-up -unused
```

- 在节点上使用以下命令从集群中删除特定许可证：

```
system license delete -serial-number <node1_serial_number> -package *
```

```
system license delete -serial-number <node2_serial_number> -package *
```

此时将显示以下输出：

```
Warning: The following licenses will be removed:  
<list of each installed package>  
Do you want to continue? {y|n}: y
```

输入 `y` 删除所有软件包。

11. 使用以下命令并检查输出，以验证是否已正确安装许可证：

s系统许可证显示

您可以将输出与在部分中捕获的输出进行比较 ["准备要升级的节点"](#)。

12. 如果在配置中使用自加密驱动器，并且您已将变量设置 `kmip.init.maxwait` 为 `off` (例如中的 ["安装并启动 node4 步骤 24"](#))，则必须取消设置变量：

```
set diag; systemshell -node <node_name> -command sudo kenv -u -p  
kmip.init.maxwait
```

13. 在两个节点上使用以下命令配置 SP：

```
system service-processor network modify -node <node_name>
```

请参见 ["参考资料"](#) 链接到 ONTAP s管理参考 _ 以了解 SP 的相关信息，以及 `_SP 9.8 命令：手册页参考 _` 以了解有关 `system service-processor network modify` 命令的详细信息。

14. 如果要在新节点上设置无交换机集群，请参见 ["参考资料"](#) 要链接到 *NetApp 支持站点* _ 并按照 `_switchover to a two-node switchless cluster` 中的说明进行操作。

完成后

如果在 node3 和 node4 上启用了存储加密，请完成此部分 "[在新控制器模块上设置存储加密](#)"。否则，请完成部分 "[停用旧系统](#)"。

在新控制器模块上设置存储加密

如果更换的控制器或新控制器的 HA 配对项使用存储加密，则必须为新控制器模块配置存储加密，包括安装 SSL 证书和设置密钥管理服务器。

关于此任务

此操作步骤包含对新控制器模块执行的步骤。您必须在正确的节点上输入命令。

步骤

1. 验证密钥管理服务器是否仍可用，其状态及其身份验证密钥信息：

```
s安全密钥管理器外部 show-status
```

```
s安全密钥管理器板载 show-backup
```

2. 将上一步中列出的密钥管理服务器添加到新控制器的密钥管理服务器列表中。

- a. 添加密钥管理服务器：

```
security key-manager external add-servers -key-servers  
key_management_server_ip_address
```

- b. 对列出的每个密钥管理服务器重复上述步骤。您最多可以链接四个密钥管理服务器。

- c. 验证是否已成功添加密钥管理服务器：

```
security key-manager external show
```

3. 在新控制器模块上，运行密钥管理设置向导以设置和安装密钥管理服务器。

您必须安装与现有控制器模块上安装的密钥管理服务器相同的密钥管理服务器。

- a. 在新节点上启动密钥管理服务器设置向导：

```
s安全密钥管理器外部启用
```

- b. 完成向导中的步骤以配置密钥管理服务器。

4. 将所有链接的密钥管理服务器中的身份验证密钥还原到新节点：

```
sSecurity key-manager external restore -node new_controller_name
```

在新控制器模块上设置NetApp卷或聚合加密

如果新控制器的已更换控制器或高可用性(HA)配对系统使用NetApp卷加密(NVE)或NetApp聚合加密(NAE)、则必须为NVE或NAE配置新控制器模块。

关于此任务

此操作步骤包含对新控制器模块执行的步骤。您必须在正确的节点上输入命令。

板载密钥管理器

使用板载密钥管理器配置NVE或NAE。

步骤

1. 将所有链接的密钥管理服务器中的身份验证密钥还原到新节点：

```
sSecurity key-manager 板载同步
```

外部密钥管理

使用外部密钥管理配置NVE或NAE。

步骤

1. 验证密钥管理服务器是否仍可用，其状态及其身份验证密钥信息：

```
sSecurity key-manager key query -node node
```

2. 将上一步中列出的密钥管理服务器添加到新控制器的密钥管理服务器列表中：

- a. 添加密钥管理服务器：

```
security key-manager external add-servers -key-servers  
key_management_server_ip_address
```

- b. 对列出的每个密钥管理服务器重复上述步骤。您最多可以链接四个密钥管理服务器。
- c. 验证是否已成功添加密钥管理服务器：

```
security key-manager external show
```

3. 在新控制器模块上，运行密钥管理设置向导以设置和安装密钥管理服务器。

您必须安装与现有控制器模块上安装的密钥管理服务器相同的密钥管理服务器。

- a. 在新节点上启动密钥管理服务器设置向导：

```
s安全密钥管理器外部启用
```

- b. 完成向导中的步骤以配置密钥管理服务器。

4. 将所有链接的密钥管理服务器中的身份验证密钥还原到新节点：

```
s安全密钥管理器外部还原
```

此命令需要OKM密码短语

有关详细信息，请参见知识库文章 ["如何从ONTAP 启动菜单还原外部密钥管理器服务器配置"](#)。

完成后

检查是否有任何卷因身份验证密钥不可用或无法访问 EKM 服务器而脱机。使用 `volume online` 命令将这些卷恢复联机。

停用旧系统

升级后，您可以通过 NetApp 支持站点停用旧系统。停用系统会告知 NetApp 系统不再运行，并将其从支持数据库中删除。

步骤

1. 请参见 ["参考资料"](#) 链接到 `_NetApp 支持站点_` 并登录。
2. 从菜单中选择 `* 产品 > 我的产品 *`。
3. 在 `* 查看已安装系统 *` 页面上，选择要用于显示系统信息的 `* 选择条件 *`。

您可以选择以下选项之一来查找您的系统：

- 序列号（位于设备背面）
- "我的位置" 的序列号

4. 选择 `* 执行! *`

下表显示了集群信息，包括序列号。

5. 在表中找到集群，然后从产品工具集下拉菜单中选择 `* 停用此系统 *`。

恢复 SnapMirror 操作

您可以恢复升级前暂停的 SnapMirror 传输，并恢复 SnapMirror 关系。升级完成后，更新将按计划进行。

步骤

1. 验证目标上的 SnapMirror 状态：

```
snapmirror show
```

2. 恢复 SnapMirror 关系：

```
snapmirror resume -destination-vserver vserver_name
```

故障排除

故障排除

升级节点对时可能会遇到故障。节点可能会崩溃，聚合可能无法重新定位或 LIF 可能无法迁移。故障的发生原因及其解决方案取决于升级操作步骤期间发生故障的时间。

请参见一节中描述操作步骤不同阶段的表 ["ARL 升级概述"](#)。有关可能发生的故障的信息按操作步骤的阶段列

出。

聚合重新定位失败

在升级期间，聚合重新定位（ARL）可能会在不同点失败。

检查聚合重新定位失败

在操作步骤期间，ARL 可能会在第 2 阶段，第 3 阶段或第 5 阶段失败。

步骤

1. 输入以下命令并检查输出：

s 存储聚合重新定位显示

`storage aggregate relocation show` 命令可显示哪些聚合已成功重新定位，哪些聚合未成功重新定位以及故障原因。

2. 检查控制台是否存在任何 EMS 消息。

3. 执行以下操作之一：

- 根据 `storage aggregate relocation show` 命令的输出以及 EMS 消息的输出，采取适当的更正操作。
- 使用 `storage aggregate relocation start` 命令的 `override-vetoes` 选项或 `override-destination-checks` 选项强制重新定位聚合。

有关 `storage aggregate relocation start`，`override-vetoes` 和 `override-destination-checks` 选项的详细信息，请参见 ["参考资料"](#) 链接到 `_Microsoft ONTAP 9.8 命令：手册页参考 _`。

升级完成后，node1 上的聚合属于 node4

升级操作步骤结束时，node3 应为聚合的新主节点，而这些聚合最初将 node1 作为主节点。您可以在升级后重新定位它们。

关于此任务

在以下情况下，聚合可能无法正确重新定位，将 node1 作为其主节点，而不是 node3：

- 在第 3 阶段，聚合从 node2 重新定位到 node3。要重新定位的某些聚合的主节点为 node1。例如，此类聚合可以称为 `aggr_node_1`。如果 `aggr_node_1` 的重新定位在第 3 阶段失败，并且无法强制重新定位，则聚合将留在 node2 上。
- 在第 4 阶段之后，将 node2 替换为 node4。更换 node2 后，`aggr_node_1` 将联机，并将 node4 作为其主节点，而不是 node3。

启用存储故障转移后，您可以通过完成以下步骤在第 6 阶段后修复不正确的所有权问题：

步骤

1. 输入以下命令以获取聚合列表：

```
storage aggregate show -nodes node4-is-home true
```

要确定未正确重新定位的聚合，请参阅在一节中获取的主所有者为 node1 的聚合列表 ["准备要升级的节点"](#) 并将其与上述命令的输出进行比较。

2. 将步骤 1 的输出与您在一节中为 node1 捕获的输出进行比较 ["准备要升级的节点"](#) 并记下未正确重新定位的所有聚合。
3. [【 auto_aggr_relocate_fail_Step3】](#) 重新定位节点 4 上遗留的聚合：

```
s存储聚合重新定位start -node node4-aggr aggr_node_1-destination node3
```

在此重新定位期间，请勿使用 `-nt-controller-upgrade`` 参数。

4. 验证 node3 现在是否为聚合的主所有者：

```
storage aggregate show -aggregate aggr1、 aggr2、 aggr3...-fields home-name
```

``aggr1、 aggr2、 aggr3...``是将node1作为原始主所有者的聚合列表。

如果聚合的主所有者不是 node3 ，则可以在中使用相同的重新定位命令将其重新定位到 node3 [第 3 步](#)。

重新启动，崩溃或重新启动

在升级的不同阶段，系统可能会崩溃—重新启动，崩溃或重新启动。

这些问题的解决方案取决于它们发生的时间。

在预检查阶段重新启动，崩溃或重新启动

在 HA 对的预检查阶段仍处于启用状态之前，节点 1 或节点 2 崩溃

如果 node1 或 node2 在预检查阶段之前崩溃，则尚未重新定位任何聚合，并且 HA 对配置仍处于启用状态。

关于此任务

接管和交还可以正常进行。

步骤

1. 检查控制台是否存在系统可能已发出的 EMS 消息，并采取建议的更正操作。
2. 继续执行节点对升级操作步骤。

在第一个资源释放阶段重新启动，崩溃或重新启动

在 HA 对仍处于启用状态的情况下，节点 1 在第一个资源释放阶段崩溃

部分或所有聚合已从 node1 重新定位到 node2 ，并且 HA 对仍处于启用状态。node2 接管 node1 的根卷以及未重新定位的任何非根聚合。

关于此任务

重新定位的聚合的所有权与因主所有者未发生更改而被接管的非根聚合的所有权相同。

当 node1 进入 Waiting for giveback 状态时，node2 将交还所有 node1 非根聚合。

步骤

1. 启动 node1 后，node1 的所有非根聚合均已移回 node1。您必须手动将聚合从 node1 重新定位到 node2：
storage aggregate relocation start -node node1 -destination node2 -aggregate -list *-ndocontroller-upgrade true
2. 继续执行节点对升级操作步骤。

在禁用 HA 对的情况下，Node1 在第一个资源释放阶段崩溃

Node2 不会接管，但它仍在从所有非根聚合提供数据。

步骤

1. 启动 node1。
2. 继续执行节点对升级操作步骤。

在 HA 对仍处于启用状态的情况下，节点 2 在第一个资源释放阶段失败

node1 已将其部分或全部聚合重新定位到 node2。已启用 HA 对。

关于此任务

node1 接管 node2 的所有聚合以及它已重新定位到 node2 的任何自身聚合。node2 启动时，聚合重新定位将自动完成。

步骤

1. 启动 node2。
2. 继续执行节点对升级操作步骤。

在第一个资源释放阶段以及禁用 HA 对之后，Node2 会崩溃

Node1 不接管。

步骤

1. 启动 node2。

在 node2 启动期间，所有聚合都会发生客户端中断。

2. 继续执行节点对升级操作步骤的其余部分。

在第一个验证阶段重新启动，崩溃或重新启动

在禁用 HA 对的情况下，节点 2 在第一个验证阶段崩溃

Node2 崩溃后 Node3 不会接管，因为 HA 对已禁用。

步骤

1. 启动 node2。

在 node2 启动期间，所有聚合都会发生客户端中断。

2. 继续执行节点对升级操作步骤。

在禁用 HA 对的情况下，节点 3 在第一个验证阶段崩溃

Node2 不会接管，但它仍在从所有非根聚合提供数据。

步骤

1. 启动 node3 。
2. 继续执行节点对升级操作步骤。

在第一个资源重新获取阶段重新启动，崩溃或重新启动

在聚合重新定位期间，节点 2 在第一个资源重新获取阶段崩溃

node2 已将其部分或全部聚合从 node1 重新定位到 node3 。node3 用于从已重新定位的聚合提供数据。HA 对已禁用，因此不存在接管。

关于此任务

未重新定位的聚合发生客户端中断。启动 node2 时， node1 的聚合将重新定位到 node3 。

步骤

1. 启动 node2 。
2. 继续执行节点对升级操作步骤。

在聚合重新定位期间，节点 3 在第一个资源重新获取阶段崩溃

如果在 node2 将聚合重新定位到 node3 时 node3 崩溃，则在 node3 启动后，此任务将继续执行。

关于此任务

Node2 将继续为其余聚合提供服务，但已重新定位到 Node3 的聚合会在 Node3 启动期间发生客户端中断。

步骤

1. 启动 node3 。
2. 继续升级控制器。

在检查后阶段重新启动，崩溃或重新启动

在后检查阶段，节点 2 或节点 3 崩溃

HA 对已禁用，因此不是接管。重新启动的节点中的聚合发生客户端中断。

步骤

1. 启动节点。
2. 继续执行节点对升级操作步骤。

在第二个资源释放阶段重新启动，崩溃或重新启动

Node3 在第二个资源释放阶段崩溃

如果 node2 重新定位聚合时 node3 崩溃，则在 node3 启动后，此任务将继续执行。

关于此任务

Node2 继续为其余聚合提供服务，但已重新定位到 Node3 和 Node3 自己的聚合的聚合在 Node3 启动期间会发生客户端中断。

步骤

1. 启动 node3 。
2. 继续执行控制器升级操作步骤。

Node2 在第二个资源释放阶段崩溃

如果节点 2 在聚合重新定位期间崩溃，则不会接管节点 2 。

关于此任务

node3 将继续为已重新定位的聚合提供服务，但 node2 拥有的聚合会发生客户端中断。

步骤

1. 启动 node2 。
2. 继续执行控制器升级操作步骤。

在第二个验证阶段重新启动，崩溃或重新启动

Node3 在第二个验证阶段崩溃

如果节点 3 在此阶段崩溃，则不会发生接管，因为 HA 对已禁用。

关于此任务

在 node3 重新启动之前，所有聚合都会发生客户端中断。

步骤

1. 启动 node3 。
2. 继续执行节点对升级操作步骤。

Node4 在第二个验证阶段崩溃

如果节点 4 在此阶段崩溃，则不会发生接管。node3 从聚合提供数据。

关于此任务

非根聚合发生中断，这些聚合已重新定位，直到 node4 重新启动。

步骤

1. 启动 node4 。
2. 继续执行节点对升级操作步骤。

操作步骤的多个阶段可能会出现的问题

某些问题可能会在操作步骤的不同阶段发生。

意外的 "storage failover show" 命令输出

在操作步骤期间，如果托管所有数据聚合的节点发生崩溃或意外重新启动，您可能会在重新启动，崩溃或重新启动前后看到 `storage failover show` 命令的意外输出。

关于此任务

您可能会在阶段 2，阶段 3，阶段 4 或阶段 5 中看到 `storage failover show` 命令的意外输出。

以下示例显示了托管所有数据聚合的节点上没有重新启动或崩溃时 `storage failover show` 命令的预期输出：

```
cluster::> storage failover show

Node      Partner      Takeover
-----  -
node1     node2        Possible  State Description
-----  -
node1     node2        false     Unknown
node2     node1        false     Node owns partner aggregates as part of the
non-disruptive head upgrade procedure. Takeover is not possible: Storage
failover is disabled.
```

以下示例显示了重新启动或崩溃后 `storage failover show` 命令的输出：

```
cluster::> storage failover show

Node      Partner      Takeover
-----  -
node1     node2        Possible  State Description
-----  -
node1     node2        -         Unknown
node2     node1        false     Waiting for node1, Partial giveback, Takeover
is not possible: Storage failover is disabled
```

尽管输出显示某个节点正在进行部分交还，并且已禁用存储故障转移，但您可以忽略此消息。

步骤

无需执行任何操作；请继续执行节点对升级操作步骤。

LIF 迁移失败

迁移 LIF 后，它们可能无法在迁移到阶段 2，阶段 3 或阶段 5 后联机。

步骤

1. 验证端口 MTU 大小是否与源节点的端口 MTU 大小相同。

例如，如果源节点上的集群端口 MTU 大小为 9000，则目标节点上的 MTU 大小应为 9000。

2. 如果端口的物理状态为 down，请检查网络缆线的物理连接。

参考资料

在执行此内容中的过程时，您可能需要查看参考内容或访问参考网站。

- [\[参考内容\]](#)
- [\[参考站点\]](#)

参考内容

下表列出了此升级的特定内容。

内容	Description
"CLI 管理概述"	介绍如何管理 ONTAP 系统，向您展示如何使用命令行界面，如何访问集群，如何管理节点等。
"确定是使用 System Manager 还是使用 ONTAP 命令行界面进行集群设置"	介绍如何设置和配置 ONTAP。
"使用 CLI 管理磁盘和聚合"	介绍如何使用命令行界面管理 ONTAP 物理存储。其中介绍了如何创建，扩展和管理聚合，如何使用 Flash Pool 聚合，如何管理磁盘以及如何管理 RAID 策略。
"《 FlexArray 虚拟化安装要求和参考》"	包含 FlexArray 虚拟化系统的布线说明和其他信息。
"HA对管理"	介绍如何安装和管理高可用性集群配置，包括存储故障转移和接管 / 交还。
"使用 CLI 进行逻辑存储管理"	介绍如何使用卷，FlexClone 卷，文件和 LUN 高效管理逻辑存储资源，FlexCache 卷，重复数据删除，数据压缩，qtree 和配额。
"MetroCluster 升级和扩展"	介绍升级 MetroCluster 配置中的控制器和存储型号，从 MetroCluster FC 过渡到 MetroCluster IP 配置以及通过添加更多节点扩展 MetroCluster 配置的过程。
"网络管理"	介绍如何在集群中配置和管理物理和虚拟网络端口（VLAN 和接口组），LIF，路由和主机解析服务；如何通过负载均衡优化网络流量；以及如何使用 SNMP 监控集群。
"《 ONTAP 9.13.1 命令：手册页参考》"	介绍支持的 ONTAP 9.13.1 命令的语法和用法。
"《 ONTAP 9.14.1 命令：手册页参考》"	介绍支持的 ONTAP 9.14.1 命令的语法和用法。
"《 ONTAP 9.15.1 命令：手册页参考》"	介绍支持的 ONTAP 9.15.1 命令的语法和用法。
"使用 CLI 进行 SAN 管理"	介绍如何使用 iSCSI 和 FC 协议配置和管理 LUN，igroup 和目标，以及使用 NVMe/FC 协议的命名空间和子系统。

内容	Description
"SAN 配置参考"	包含有关 FC 和 iSCSI 拓扑和布线方案的信息。
"通过移动卷或存储进行升级"	介绍如何通过移动存储或卷快速升级集群中的控制器硬件。还介绍如何将受支持的型号转换为磁盘架。
"升级 ONTAP"	包含有关下载和升级 ONTAP 的说明。
"使用 system controller Replace 命令升级同一机箱中的控制器型号"	介绍无中断升级系统(保留旧系统机箱和磁盘)所需的聚合重新定位过程。
"使用 system controller replace 命令升级运行 ONTAP 9.8 或更高版本的控制器硬件"	介绍使用 system controller replace 命令无中断升级运行 ONTAP 9.8 的控制器所需的聚合重新定位过程。
"使用聚合重新定位手动升级运行 ONTAP 9.8 或更高版本的控制器硬件"	介绍运行 ONTAP 9.8 或更高版本时执行手动无中断控制器升级所需的聚合重新定位过程。

参考站点

。"NetApp 支持站点" 此外，还包含有关网络接口卡（NIC）以及可能与系统结合使用的其他硬件的文档。它还包含 "Hardware Universe"，提供有关新系统支持的硬件的信息。

访问 "ONTAP 9 文档"。

访问 "Active IQ Config Advisor" 工具。

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。