



准备无副本过渡

ONTAP 7-Mode Transition

NetApp
December 19, 2023

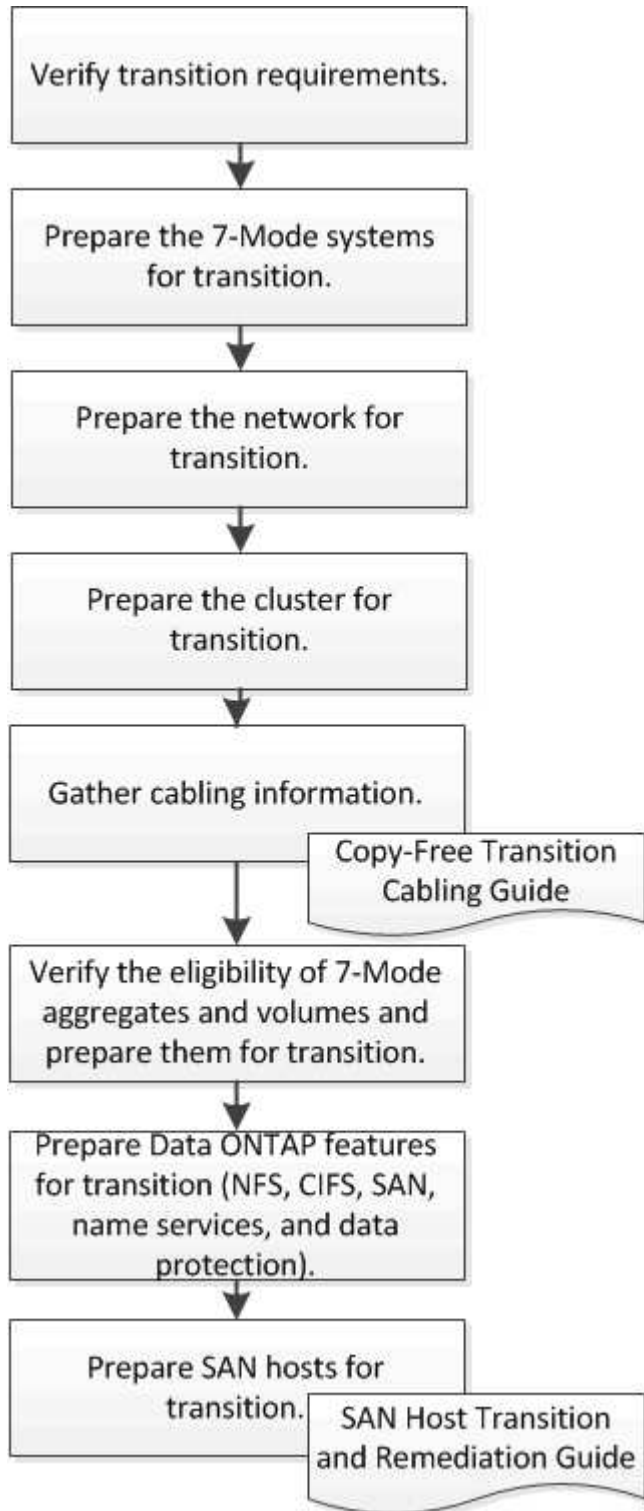
This PDF was generated from https://docs.netapp.com/zh-cn/ontap-7mode-transition/copy-free/concept_requirements_for_copy_free_transition.html on December 19, 2023. Always check docs.netapp.com for the latest.

目录

- 准备无副本过渡 1
 - 无副本过渡的要求 2
 - 无副本过渡所需的工具和文档 3
 - 与 7- 模式过渡工具通信的端口要求 3
 - 准备 7- 模式 HA 对以进行过渡 4
 - 在 7- 模式系统上设置 SP 或 RLM 用于无副本过渡 5
 - 准备网络以进行过渡 8
 - 准备集群以进行过渡 9
 - 收集用于过渡的布线信息 10
 - 准备 7- 模式聚合和卷以进行过渡 13
 - 正在准备过渡名称服务 19
 - 为 NFS 过渡做准备 21
 - 为 SMB/CIFS 过渡做准备 28
 - 为 SAN 过渡做准备 34
 - 准备数据保护功能以进行过渡 37

准备无副本过渡

在开始无副本过渡之前，您必须确定要过渡的 7- 模式 HA 对，了解迁移的要求和限制，并为过渡准备 7- 模式系统和集群。此外，您还必须了解过渡支持和不支持的 Data ONTAP 功能。



• 相关信息 *

无副本过渡的要求

您应了解无副本过渡对 7- 模式系统，集群，ONTAP 版本和磁盘架的要求。

请务必查阅当前的 7- 模式过渡工具 *Release Notes*，了解有关受支持的目标版本和已知问题的最新信息。

"《7- 模式过渡工具发行说明》"

- * 平台型号 *

只有中端和高端 FAS 系统以及 IBM N 系列系统才支持无副本过渡。。"[NetApp 互操作性表工具](#)" 提供了有关 7- 模式系统和目标集群节点支持的平台的最新信息。

- * 7- 模式源系统中的 Data ONTAP *

有关 7- 模式过渡工具支持迁移的 7- 模式版本列表，请参见 "[NetApp 互操作性表工具](#)"

- * ONTAP 目标系统 *

7- 模式过渡工具 3.3.1 版支持使用无副本方法过渡到以下 ONTAP 版本：

- ONTAP 9.4 及更早版本的 ONTAP 9
- 集群模式 Data ONTAP 8.3.2 及更高版本 8.x * 注意： * 不能使用 7- 模式过渡工具使用无副本方法过渡到 ONTAP 9.5 或更高版本。为此，您必须先使用 7- 模式过渡工具 3.3.1 过渡到 ONTAP 9.4，然后再将集群升级到 ONTAP 9.5 或更高版本。7- 模式过渡工具 3.3.2 不支持无副本过渡。

- * 高可用性配置 *

7- 模式控制器和目标集群节点必须采用 HA 配置。HA 对必须运行状况良好，并且任何节点都不能处于接管模式。无副本过渡不支持独立控制器。

- * 磁盘架型号 *

支持以下磁盘架型号：

- DS4486
- DS4246
- DS4243



ONTAP 9.2 和 ONTAP 9.4 不支持磁盘架型号 DS4243。从 ONTAP 9.2P1 和 ONTAP 9.3 开始的所有 ONTAP 9.2 修补程序版本均支持此模式。7- 模式过渡工具 3.3.1 支持使用磁盘架型号 DS4243 进行过渡，以便通过 ONTAP 9.3 无副本过渡到 ONTAP 9.2P1。

- DS2246
- DS14mk4 FC （ONTAP 9.0 及更高版本不支持）
- DS14mk2 AT （在 ONTAP 9.0 及更高版本中不受支持）



不支持磁盘架型号 DS14mk2 FC。

- * 磁盘固件 *

您必须在 7- 模式系统和目标集群节点上下载并安装最新的磁盘认证包，磁盘固件以及磁盘架和 ACP 固件。

["NetApp 下载：磁盘认证包"](#)

["NetApp 下载：磁盘驱动器固件"](#)

["NetApp 下载：磁盘架固件"](#)

- * 用于验证布线的工具 *

在过渡期间将 7- 模式磁盘架连接到目标集群节点后，必须使用 Config Advisor 验证布线。

["NetApp 下载： Config Advisor"](#)

无副本过渡所需的工具和文档

Config Advisor 是无副本过渡所需的工具。您应使用 Config Advisor 验证磁盘架的布线。此外，还提供了有关 SAN 主机修复的其他文档。

Config Advisor

在将 7- 模式磁盘架连接到目标集群节点后，您应使用 Config Advisor 中的 "`transition` " 执行配置文件来验证布线情况。

["NetApp 下载： Config Advisor"](#)

文档。

介绍使用无副本过渡进行过渡时必须在 SAN 主机上执行的过渡前和过渡后步骤。

["SAN 主机过渡和修复"](#)

与 7- 模式过渡工具通信的端口要求

7- 模式过渡工具通过特定端口与 7- 模式系统和集群进行通信。您必须确保 7- 模式系统和集群上的这些端口处于打开状态，以允许与 7- 模式过渡工具进行通信。

必须在 7- 模式系统上打开的端口

7- 模式过渡工具使用 HTTPS 在端口 443 上与 7- 模式系统进行通信。

必须在集群上打开的端口

7- 模式过渡工具使用 HTTPS 在端口 443 上与集群进行通信。

必须在 7- 模式过渡工具上打开的端口

必须为 Web 界面打开 7- 模式过渡工具的端口 8444 。

要过渡网络组和 CIFS 本地用户和组，必须满足以下要求：

- 7- 模式过渡工具的端口 8088 必须可用。

要替代端口 8088，您必须更改 7- 模式过渡工具安装目录的 `transition-tool.conf` 文件中的 `tool.http.port` 参数指定的端口。



更改配置文件中的端口后，必须重新启动 7- 模式过渡工具服务。

- 集群中的每个节点必须至少为目标 SVM 配置一个数据 LIF。
- 所有 SVM 数据 LIF 都必须能够与 7- 模式过渡工具端口 8088 或 `transition-tool.conf` 文件中的 `tool.http.port` 参数指定的端口进行通信。



您必须确认防火墙不会阻止此流量。

- 相关信息 *

["7- 模式过渡工具安装和管理"](#)

准备 7- 模式 HA 对以进行过渡

开始过渡之前，您必须在 7- 模式系统上完成某些任务，例如，启用 7- 模式系统与目标集群通信以及启用 HTTPS 和 TLS。

HA 对必须运行状况良好，并且任何节点都不能处于接管模式，可以使用 `cf status` 命令进行验证。您还可以使用 NetApp AutoSupport 工具检测任何错误或存在风险的情况。

1. 如果存储系统上未启用 HTTPS，请启用 HTTPS：

```
` * options httpd.admin.ssl.enable on`
```

默认情况下，HTTPS 处于启用状态。

2. 在 7- 模式存储系统上启用 TLS，以使 7- 模式过渡工具能够与 7- 模式系统通信：

- a. 如果存储系统上尚未启用 SSL，请设置并启动 SSL：+` * SecureAdmin setup ssl`

默认情况下，为存储系统设置 SSL。如果先前已为存储系统设置 SSL，系统会询问您是否要继续。如果您不想进行任何更改，可以退出 SSL 设置。

- b. 启用 SSL：+` * options ssl.enable on`

要允许通过 TLS 进行通信，必须启用此选项。

- c. 启用 TLS：+` * options tls.enable on`

d. 在 7- 模式系统上禁用 SSLv2 和 SSLv3 : + `` * options ssl.v2.enable off``

`` * 选项 ssl.v3.enable off``

7- 模式过渡工具使用 TLS 或 SSL 协议与 7- 模式存储系统进行通信。如果在存储系统上启用了 TLS , 则该工具将使用 TLS 协议与存储系统进行通信。如果在存储系统上禁用了 TLS 且启用了 SSLv3 , 则该工具将使用 SSLv3 与存储系统进行通信。

+ 重要信息: 最佳实践是启用 TLS 并禁用 SSLv2 和 SSLv3 , 以避免出现安全漏洞。

在 7- 模式系统上设置 SP 或 RLM 用于无副本过渡

如果尚未在 7- 模式存储系统上配置服务处理器 (SP) 或远程 LAN 模块 (RLM) , 或者您已为 SP 或 RLM 配置了 IPv6 地址, 则必须为 SP 或 RLM 配置 IPv4 地址。

- 安装了 7- 模式过渡工具的主机必须支持 SSHv2 。
- 您必须能够使用 "admin" 角色或具有 "login-sp" 功能的角色的凭据访问 SP 或 RLM "naroot" 帐户或 Data ONTAP 用户帐户。

在过渡期间系统暂停时, 7- 模式过渡工具会使用远程管理设备访问 7- 模式系统, 该设备可以是 SP 或 RLM , 具体取决于您的系统上根据平台型号提供的任何设备。您必须使用 IPv4 地址配置 SP 或 RLM 。过渡不支持 IPv6 配置。

步骤

- 配置 SP 并为安装了 7- 模式过渡工具的主机提供 SP 访问权限。

a. 使用 IPv4 地址 + `` * sp setup`` 配置并启用 SP 网络

```
system1> sp setup
The Service Processor (SP) provides remote management capabilities
including console redirection, logging and power control.
It also extends autosupport by sending
additional system event alerts. Your autosupport settings are use
for sending these alerts via email over the SP LAN interface.
Would you like to configure the SP? y
Would you like to enable DHCP on the SP LAN interface? n
Please enter the IP address of the SP []: 192.168.123.98
Please enter the netmask of the SP []: 255.255.255.0
Please enter the IP address for the SP gateway []: 192.168.123.1
Do you want to enable IPv6 on the SP ? n
Verifying mailhost settings for SP use...
```

b. 验证 SP 网络配置设置:

`` * sp status``

```

system1> sp status
      Service Processor      Status: Online
      Firmware Version:      1.2
      Mgmt MAC Address:      00:A0:98:01:7D:5B
      Ethernet Link:         up
      Using DHCP:            no
IPv4 configuration:
      IP Address:            192.168.123.98
      Netmask:               255.255.255.0
      Gateway:               192.168.123.1

```

c. 提供对安装了 7- 模式过渡工具的主机的 SP 访问权限：

```
` * options sp.ssh.access host=7mtt_host_*
```

`7mtt_host` 是安装了 7- 模式过渡工具的主机的主机名或 IP 地址。



配置 SP 时，默认情况下会为所有主机授予访问权限。如果要限制对特定主机的访问，则必须执行此步骤。

d. 从安装了 7- 模式过渡工具的主机登录到 SP： + ` * ssh username@SP_IP_address*`

出现提示时，输入用户名的密码。

此时将显示 SP 提示符，指示您有权访问 SP 命令行界面。

- 配置 RLM 并为安装了 7- 模式过渡工具的主机提供 RLM 访问权限。

a. 使用 IPv4 地址配置 RLM 网络： + ` * RLM setup*`

在 RLM 命令行界面向导中，必须输入 RLM 的 IP 地址，网络掩码和网关。


```

system> rlm setup
    The Remote LAN Module (RLM) provides remote management
capabilities
    including console redirection, logging and power control.
    It also extends autosupport by sending
    additional system event alerts. Your autosupport settings are
used
    for sending these alerts via email over the RLM LAN interface.
Would you like to configure the RLM? y
Would you like to enable DHCP on the RLM LAN interface? n
Please enter the IP address for the RLM []:192.168.123.98
Please enter the netmask for the RLM []:255.255.255.0
Please enter the IP address for the RLM gateway []:192.168.123.1
Do you want to enable IPv6 on the RLM ? n
Verifying mailhost settings for RLM use...

```

b. 验证 RLM 网络配置是否正确：

` * RLM status`

```

system> rlm status
Remote LAN Module      Status: Online
  Part Number:         110-00030
  Revision:            A0
  Serial Number:       123456
  Firmware Version:    4.0
  Mgmt MAC Address:    00:A0:98:01:7D:5B
  Ethernet Link:       up, 100Mb, full duplex, auto-neg complete
  Using DHCP:          no
IPv4 configuration:
  IP Address:          192.168.123.98
  Netmask:             255.255.255.0
  Gateway:             192.168.123.1

```

c. 为安装了 7- 模式过渡工具的主机提供 RLM 访问权限：

` + 选项 rlm.ssh.access host=7mtt_host `

7mtt_host 是安装了 7- 模式过渡工具的主机的主机名或 IP 地址。



配置 RLM 时，默认情况下会为所有主机授予访问权限。如果要限制对特定主机的访问，则必须执行此步骤。

d. 从安装了 7- 模式过渡工具的主机登录到 RLM：

```
` * ssh username@RLM_IP_address`
```

出现提示时，您必须输入用户名的密码。

此时将显示 RLM 提示符，指示您有权访问 RLM 命令行界面。

准备网络以进行过渡

您必须通过创建逻辑端口（VLAN 和接口组）来准备要过渡的集群数据网络。

必须配置 NTP 服务器，并且必须在 7- 模式系统和集群之间同步时间。

步骤

1. 根据需要在目标集群节点上创建 VLAN 或接口组：

```
` * 网络端口 vlan cre`
```

或

```
` * 网络端口 ifgrp cre`
```

要在过渡后提供网络连接，您应将 7- 模式 IP 地址过渡到 ONTAP 中类似的网络拓扑。例如，如果在物理端口上配置了 7- 模式 IP 地址，则应将 IP 地址过渡到 ONTAP 中的相应物理端口。同样，在 VLAN 端口或接口组上配置的 IP 地址应过渡到 ONTAP 中的相应 VLAN 端口或接口组。

2. 如果希望 SVM 位于非默认 IP 空间中，请创建所需的 IP 空间：

```
` * 网络 IP 空间 cre`
```

选择进行过渡的 7- 模式 IP 地址或新 LIF 将在映射的 SVM 的 IP 空间中创建。



IPv6 地址无法过渡，必须在过渡后手动配置。

◦ 相关信息 *

"网络和 LIF 管理"

过渡 7- 模式 IP 地址的注意事项

在 ONTAP 中将 7- 模式 IP 地址过渡到 Storage Virtual Machine（SVM）时，您必须了解某些注意事项。

- 您可以使用 7- 模式过渡工具过渡现有的 7- 模式 IP 地址或指定要在 SVM 上配置的新 IP 地址。
 - 在应用配置（预转换）阶段的管理 `down` 状态下，在 SVM 上创建现有的 7- 模式 IP 地址。
 - 在应用配置（预转换）阶段的管理 `up` 状态下，在 SVM 上创建新的 IP 地址。
- IPv6 地址无法过渡，必须在过渡后手动配置。
- iSCSI 和 FC LIF 不会过渡，必须在过渡后手动配置。

准备集群以进行过渡

过渡之前，您必须准备好集群以与 7- 模式过渡工具通信，并准备要过渡的 SVM 。您可以过渡到具有数据聚合的目标 HA 对。


- 必须已设置集群，并且目标集群节点必须加入集群。

"软件设置"

- 必须创建 SVM 并将其分配给 IP 空间。
- 您可以将 7- 模式磁盘架过渡到具有已有数据聚合和卷的目标 HA 对。

对于双节点集群，您必须拥有一个数据聚合来托管目标 SVM 的根卷。对于具有四个或更多节点的集群，SVM 的根卷可以托管在过渡的目标节点上，也可以托管在集群中的其他节点上。

过渡期间，不应将集群升级到其他 ONTAP 版本。

 如果需要，您可以将集群升级到相同 ONTAP 版本的修补程序版本。

1. 从管理主机中，使用集群管理 LIF 验证集群是否可访问：

```
` * ssh username@cluster_mgmt_IP`
```

2. 在集群上启用 SSLv3 或 FIPS :

如果要启用 ...	输入 ...
SSLv3	` * 系统服务 Web 修改 -ssl3-enabled true`
FIPS 140-2 合规性	` * 系统服务 Web 修改 -ssl-fips-enabled true`

启用 FIPS 140-2 合规性后，SSLv3 将被禁用。启用 FIPS 140-2 合规性后，ONTAP 会阻止您启用 SSLv3 。如果启用 FIPS 140-2 后又将其禁用，SSLv3 将保持禁用状态。

 最佳做法是，由于 SSLv3 中存在安全漏洞，启用 FIPS 。

3. 验证集群管理 LIF 是否允许使用 HTTPS :

- a. 查看集群管理 LIF 的防火墙策略： + ` * network interface show -vserver svm_name -lif cluster_mgmt_lif -fields firewall-policy`

```
cluster1::> network interface show -vserver cluster1 -lif
cluster_mgmt -fields firewall-policy
vserver lif      firewall-policy
-----
cluster1  cluster_mgmt mgmt
```

- b. 验证与集群管理 LIF 关联的防火墙策略是否允许 HTTPS 访问：+`* 系统服务防火墙策略 show -policy mgmt`

```
cluster1::> system services firewall policy show -policy mgmt
Policy           Service      Action IP-List
-----
mgmt
                dns         allow  0.0.0.0/0, ::/0
                http        allow  0.0.0.0/0, ::/0
                https       allow  0.0.0.0/0, ::/0
                ndmp        allow  0.0.0.0/0, ::/0
                ntp         allow  0.0.0.0/0, ::/0
                rsh         deny   0.0.0.0/0, ::/0
                snmp        allow  0.0.0.0/0, ::/0
                ssh         allow  0.0.0.0/0, ::/0
                telnet      deny   0.0.0.0/0, ::/0
9 entries were displayed.
```

"系统管理"

收集用于过渡的布线信息

在开始无副本过渡之前，您必须收集有关 7- 模式控制器的适配器，端口，磁盘架和存储连接的信息，然后规划如何将 7- 模式磁盘架连接到目标集群节点。

您必须已打印无副本过渡布线工作表。

无副本过渡布线工作表

1. 使用 Config Advisor 对 7- 模式存储和布线执行运行状况检查并收集布线数据。

您应使用 Data ONTAP 7 和 8 （7- 模式）` 执行配置文件中的 7- 模式安装检查 选项。

2. 使用以下命令收集有关每个 7- 模式控制器的所需信息：

```
`* sysconfig slot_number`
```

您可以使用此命令的输出来确定用于磁盘架连接的端口。

```

host1> sysconfig 3
    slot 3: SAS Host Adapter 3a
        24 Disks:                13440.0GB
        1 shelf with IOM3
    slot 3: SAS Host Adapter 3b
        24 Disks:                13440.0GB
        1 shelf with IOM3
    slot 3: SAS Host Adapter 3c
        24 Disks:                13440.0GB
        1 shelf with IOM3
    slot 3: SAS Host Adapter 3d
        24 Disks:                13440.0GB
        1 shelf with IOM3

```

3. 在集群中，对每个节点运行以下 `nodeshell` 命令：

```
` * 系统节点 run -node node_name -command sysconfig -A`
```

您可以使用此命令的输出来获取有关可用端口和扩展卡插槽的信息。

4. 在目标集群节点上，规划用于连接 7- 模式磁盘架的端口：

- a. 查看可用（开放）端口。
- b. 查看扩展卡插槽。
- c. 规划扩展卡配置。

如果目标平台和 ONTAP 版本也支持扩展卡，您可以计划将其从 7- 模式系统中移动。如果需要，您还可以规划 PAM 卡。

["NetApp Hardware Universe"](#)

- d. 规划用于磁盘架布线的目标端口。

选择目标端口取决于以下某些因素：

- 单独或现有磁盘架堆栈
- 端口可用性
- SAS 或 FC 连接
- 板载端口或扩展卡的可用性

5. 转至数据中心，在布线工作表中以物理方式记录 7- 模式控制器和目标集群节点上的端口连接：

- a. 在布线工作表中记录 7- 模式控制器上使用的端口。
- b. 在布线工作表中记录目标集群节点上的已用端口。
- c. 按照步骤中的计划，记录用于连接 7- 模式磁盘架的目标端口
[#sted_D0CFE719A0384F7FA5D9E73C8EA6C2E7](#)。

布线工作表示例

7- 模式布线				集群模式 Data ONTAP 布线			
控制器 A（主机名）： 7hostA				节点 A（主机名）： cluster1-01			
地点：科罗拉多楼层：第三机架： 8				地点：科罗拉多楼层：五楼机架： 3			
模块 A 端口	模块 B 端口	磁盘架类型 / 资产标签	磁盘架 ID	模块 A 端口	模块 B 端口	磁盘架类型 / 资产标签	磁盘架 ID
1a.	0a	DS4243/150 254-7	10-13	1a.	0a	DS4243/174 243-2	10-11
1b.	0b	DS4243/151 205-2	30-37	1b.	0b	DS4243/150 254-7	20-23
1c（脱机）	0c（脱机）	不适用	不适用	1c	0c	DS4243/151 205-2	30-37
一维	0D	DS4243/143 921-4	14-15	一维	0D	DS4243/143 921-4	14-15
• 控制器 B（主机名）： 7hostB*	• 节点 B（主机名）： cluster1-02*	• 位置： 科罗拉多楼层： 第三机架： 8*	• 位置： 科罗拉多楼层： 五楼机架： 3*	• 模块 A 端口 *	• 模块 B 端口 *	• 磁盘架类型 / 资产标记 *	• 磁盘架 ID*
• 模块 A 端口 *	• 模块 B 端口 *	• 磁盘架类型 / 资产标记 *	• 磁盘架 ID*	1a.	0a	DS4243/174 263-6	10-13
1a.	0a	DS4243/174 23-2	10-11	1b（脱机）	0b（脱机）	不适用	不适用
1b.	0b	DS4243/174 263-6	20-23	1c	0c	DS4243/174 274-9	30-37
1c	0c	DS4243/174 274-9	30-37	一维	0D	DS4243/174 285-6	14-15

准备 7- 模式聚合和卷以进行过渡

过渡之前，您必须确保 7- 模式聚合和卷符合过渡条件，并在过渡之前执行一些手动步骤。例如，某些卷类型无法过渡，过渡前必须从 7- 模式系统中删除任何 32 位数据。

过渡 7- 模式聚合和卷的限制

您必须了解过渡 7- 模式聚合和卷的某些限制。某些限制是由于 ONTAP 不支持的功能造成的。对于某些限制，您可以执行更正操作以继续过渡。

卷类型

不支持过渡以下类型的卷：

- 传统卷

您可以使用基于主机的过渡方法过渡传统卷。

["NetApp 技术报告 4052：《成功过渡到集群模式 Data ONTAP》（Data ONTAP 8.2.x 和 8.3）"](#)

- SnapLock 卷

所有最新的 ONTAP 版本均支持过渡 SnapLock 卷。

- FlexCache 卷

聚合和卷状态

如果为过渡选择的任何 7- 模式聚合和卷处于以下状态之一，则过渡将被阻止：

- 脱机
- 受限
- 不一致 (WAFL inconsistent)

FlexClone 卷

在无副本过渡期间，克隆层次结构和存储效率会保留下来。但是，您必须确保父 FlexVol 卷及其所有 FlexClone 卷属于同一个 vFiler 单元。如果 FlexClone 卷与父卷位于不同的 vFiler 单元中，则必须选择以下操作之一：

- 将 FlexClone 卷移动到拥有父 FlexVol 卷的 vFiler 单元。
- 从父 FlexClone 卷拆分克隆，然后将这些卷作为 FlexVol 卷进行过渡。

包含属于其他 vFiler 单元的 qtree 的卷

您不能过渡具有 qtree 的卷，其中 qtree 的所有权与卷的 vFiler 单元不同。过渡之前，必须执行以下操作之一，确保每个卷及其所有 qtree 都属于同一个 vFiler 单元：

- 将 qtree 移动到拥有卷的 vFiler 单元。
- 删除 qtree。

索引节点到父路径名的转换设置

必须在每个卷上启用索引节点到父路径名的转换。您可以通过关闭 no_i2p 选项来启用父级到路径名的转换：


```
` * vol options vol_name no_i2p off`
```

您无需等待 I2P 扫描完成，即可继续过渡准备工作。

准备过渡具有 32 位聚合的 7- 模式系统

ONTAP 8.3 及更高版本不支持 32 位聚合，卷和 Snapshot 副本。因此，必须将 32 位聚合扩展到 64 位，然后在过渡之前查找并删除 7- 模式系统中的任何 32 位卷和 Snapshot 副本。

- * 32 位聚合 *
- a. [将聚合扩展为 64 位格式](#)
- b. [查找和删除 32 位卷和 Snapshot 副本](#)
- * 32 位卷或 Snapshot 副本 *

即使只有 64 位聚合和卷，也可能会保留某些 32 位或混合格式的 FlexVol 卷或 Snapshot 副本。过渡前，必须删除这些卷和 Snapshot 副本。

[查找和删除 32 位卷和 Snapshot 副本](#)

- 相关信息 *

"[NetApp 技术报告 3978](#) : 《32 位聚合原位扩展到 64 位概述和最佳实践》"

将聚合扩展为 64 位格式

如果您的系统包含 32 位聚合，则必须在过渡到 Data ONTAP 8.3 或更高版本之前的 7- 模式系统上将其扩展到 64 位格式，因为这些版本的 Data ONTAP 不支持 32 位格式。

- 如果聚合包含与 32 位源卷建立的 SnapMirror 关系的目标卷，则必须先扩展包含源卷的聚合，然后再扩展包含目标卷的聚合。

对于 SnapMirror 关系中的卷，目标卷会在镜像完好无损的情况下继承源卷的格式。如果要扩展的聚合包含源卷为 32 位卷的目标卷，并且在扩展聚合之前中断了镜像，则目标卷将扩展为 64 位格式。但是，如果重新建立镜像，并且源卷仍为 32 位，则目标卷将恢复为 32 位格式。因此，如果要将聚合中的所有 32 位卷扩展为 64 位格式，则必须先扩展包含源卷的聚合，然后再重新建立 SnapMirror 关系。

步骤

1. 进入高级权限模式：

```
` * priv set advanced`
```

2. 启动扩展：

```
` * aggr 64bit-upgrade start aggr_name`
```

3. 执行相应的操作：

如果命令 ...	那么 ...
已成功启动	继续执行下一步。
表示一个或多个卷无法扩展 因为他们没有足够的空间	添加 <code>grow-all</code> 选项后重试此命令。
表示部分扩展无法完成 其他原因	根据错误消息中所述的问题描述执行相应的操作。

4. 显示扩展的状态：

```
` * aggr 64bit-upgrade status aggr_name *`
```

此时将显示扩展的当前状态。如果此消息指示没有正在进行的升级，则表示扩展已完成。

5. 确认聚合中的所有卷均为 64 位格式：

```
` * aggr 64bit-upgrade status aggr_name -all *`
```

6. 返回到管理权限模式：`priv set admin`

聚合扩展为 64 位格式。但是，即使所有卷均已扩展，也可能会保留一些 32 位 Snapshot 副本。如果源卷中存在 32 位 Snapshot 副本，则无法升级或过渡到 Data ONTAP 8.3 或更高版本。

查找和删除 32 位卷和 Snapshot 副本

即使您已将所有聚合扩展为 64 位格式，也可以保留某些 32 位或混合格式的 FlexVol 卷或 Snapshot 副本。必须先删除这些卷和 Snapshot 副本，然后运行 Data ONTAP 8.3 或更高版本的集群才能访问您的数据。

- 您必须已将系统上的所有 32 位聚合扩展到 64 位格式。

您必须对包含 32 位卷和 Snapshot 副本的每个聚合重复此任务中的步骤。

步骤

1. 进入高级模式：

```
` * priv set advanced *`
```

2. 显示聚合中所有卷的格式：

```
` * aggr 64bit-upgrade status aggr_name -all *`
```

聚合中的每个卷都会按其格式显示。

3. 对于每个 32 位或混合格式的卷，确定卷未扩展到 64 位格式的原因，然后采取相应的措施。

如果无法确定卷未扩展的原因，请重试聚合扩展。

如果卷 ...	那么 ...
是 SnapMirror 关系的目標	将包含源卷的聚合扩展为 64 位格式。
是只读卷（但不是 SnapMirror 目标）	使卷可写并重试扩展，或者销毁此卷。
未扩展，因为中的可用空间不足 卷或聚合	增加卷或聚合中的可用空间，然后重试扩展。

聚合中的所有 32 位和混合格式卷现在都是 64 位卷。您可以通过重复上一步来确认此操作。

4. 显示系统上所有 Snapshot 副本的格式：

```
` * snap list -fs-block-format`
```

5. 使用 snap delete 命令删除 32 位 Snapshot 副本。



此操作将删除 Snapshot 副本中的数据。在删除 Snapshot 副本之前，必须确保不需要保留这些副本。或者，您也可以等待 32 位 Snapshot 副本过期。所需时间取决于 Snapshot 副本计划。

如果 Snapshot 副本是 FlexClone 卷的基本 Snapshot 副本，则必须先将 FlexClone 卷从其父卷拆分，然后才能删除 Snapshot 副本。

删除所有 32 位 Snapshot 副本。您可以通过重复上一步来确认此操作。

6. 返回到管理权限级别：

```
` * priv set admin`
```

过渡时的聚合空间要求

过渡之前，必须确保 7- 模式聚合具有足够的可用空间。7- 模式过渡工具会根据物理空间，逻辑空间， Snapshot 副本占用的空间以及空间保证设置对聚合执行各种空间检查。此外，您还必须了解 Flash Pool 聚合的空间注意事项。

聚合中的物理空间

如果 7- 模式聚合中的可用空间小于物理空间的 5%，则过渡将被阻止。最佳实践是，过渡前，在 7- 模式聚合中至少有 20% 的可用空间。

由于以下原因，聚合中需要额外空间：

- 在期间为每个 7- 模式聚合创建聚合级别 Snapshot 副本 导出阶段
- 使用新数据在过渡后的聚合上测试工作负载 在预生产测试阶段

如果没有额外空间，则可以在过渡前向 7- 模式系统添加磁盘。如果添加磁盘不可行，或者您可以确保在预生产阶段仅在过渡后的卷上写入有限数量的数据，则可以使用 7- 模式过渡工具确认此错误并继续过渡。但是，您必须在过渡期间继续监控聚合空间，并确保聚合在预生产测试阶段不会增长。

聚合中的逻辑空间

如果 7- 模式聚合中的逻辑空间已满 97% 以上，则 7- 模式过渡工具会在预检期间引发阻塞错误。您可以在规划阶段忽略此错误并继续过渡；但是，您必须通过减小此类聚合中的卷大小或向聚合添加更多磁盘来确保在执行导出并暂停操作之前已用逻辑空间小于 97%。您不能在导出和暂停阶段忽略此错误。

Snapshot 溢出

如果 7- 模式聚合中的 Snapshot 副本占用的空间超过为 Snapshot 副本预留分配的空间，则在导出并暂停操作中创建聚合级 Snapshot 副本可能会失败。7- 模式过渡工具在对此情况进行预检期间引发阻塞错误。在这种情况下，您必须在规划阶段删除所有现有的聚合级别 Snapshot 副本。

如果您不想删除现有 Snapshot 副本，则可以在规划阶段忽略此错误并继续过渡；但是，在执行导出并暂停操作之前，必须确保 Snapshot 副本的已用容量百分比小于 100%。

空间保证设置

如果 7- 模式控制器中的卷具有以下空间保证设置，则 7- 模式过渡工具会在预检期间引发阻止错误：

- 禁用了保证的卷保证卷
- 文件保证卷
- * 禁用保证的卷保证卷 *

在某些情况下，由于聚合中缺少空间，卷保证卷的空间保证将被禁用。

您必须在 7- 模式聚合上创建足够的可用空间，然后使用以下 7- 模式命令为此类 7- 模式卷启用空间保证：

```
` * vol options volume_name guarantee volume*`
```

如果您不想对 7- 模式执行任何更正操作，可以忽略此错误。过渡后，请检查已禁用保证的卷，并使用以下命令手动启用保证：

```
` * volume modify -vserver -volume -space-guarantee volume*`
```

- * 文件保证卷 *

ONTAP 不支持文件保证。

如果您有文件保证卷，则必须执行以下操作之一：

- 如果 7- 模式卷包含空间预留的 LUN 或文件，请使用 7- 模式命令将卷的空间保证类型更改为 volume：
+ ` * vol options *volume_name* guarantee volume*`

在运行此命令之前，必须确保 7- 模式聚合上有足够的可用空间。

- 如果 7- 模式卷不包含任何预留空间的 LUN 或文件，请使用以下 7- 模式命令将卷的空间保证更改为 none：
+ ` * vol options *volume_name* guarantee none*` 如果您不想对 7- 模式执行任何更正操作，则可以忽略此错误并继续过渡。

过渡期间，如果这些卷包含预留了空间的 LUN 或文件，则其空间保证将自动转换为 volume，但空间保证最初将被禁用。您必须在聚合上创建足够的可用空间，然后使用以下命令手动启用保证：

+ ` * volume modify -vserver -volume -space-guarantee volume*`

+ 如果卷不包含任何空间预留的 LUN 或文件，则在过渡期间，其空间保证将自动转换为 none。

有关 Flash Pool 聚合的其他注意事项

如果 Flash Pool 聚合的 SSD 中的可用空间小于 SSD 总磁盘空间的 5%，则不支持过渡。要继续过渡，您必须禁用 SSD 缓存或添加更多 SSD。

- 相关信息 *

过渡期间发生可忽略的错误

"磁盘和聚合管理"

正在准备过渡名称服务

名称服务配置，包括 DNS，LDAP，NIS，主机，名称服务开关，7- 模式过渡工具可过渡 UNIX 用户和组以及网络组配置。过渡名称服务配置之前，您必须了解一些注意事项。

名称服务过渡：支持和不支持的配置以及所需的手动步骤

您必须了解 7- 模式过渡工具过渡的名称服务配置。某些名称服务配置不会过渡到 ONTAP，因为这些配置在 ONTAP 中不受支持，或者必须手动过渡。

您应验证所有预检错误和警告消息，以评估此类配置对过渡的影响。

已过渡的配置

概括地说，以下名称服务配置由 7- 模式过渡工具过渡：

- DNS 配置（` /etc/resolv.conf`）
- LDAP 配置
- NIS 配置
- 名称服务交换机配置（` /etc/nsswitch.conf` 和 ` /etc/resolv.conf`）
- 主机配置（` /etc/hosts`）
- UNIX 用户和组（` /etc/passwd` 和 ` /etc/group`）
- 网络组配置（` /etc/netgroup`）

有关这些名称服务配置的详细信息，请参见预检结果。

ONTAP 中不支持的配置

- NIS 从属服务器
- NIS 广播
- NIS 组缓存

- 动态 DNS
- DNS 缓存
- 影子数据库
- 文件或 DNS 以外的主机数据库源

ONTAP 仅支持使用文件和 DNS 进行主机查找；不支持其他数据库源。过渡期间会忽略 `/etc/nsswitch.conf` 中的主机查找顺序。

必须手动配置的配置

您必须在 SVM 上手动配置以下 LDAP 选项：

- `ldap.usermap.attribute.unixaccount`
- `ldap.password`
- `ldap.usermap.base`
- `ldap.ssl.enable`
- 相关信息 *

自定义 7- 模式配置的过渡

"NFS 管理"

"网络和 LIF 管理"

过渡 DNS ， NIS 和 LDAP 配置的注意事项

您应了解如何过渡在 7- 模式下运行的 Data ONTAP 中的 DNS ， NIS 和 LDAP 配置并将其应用到 ONTAP 中。

DNS 过渡注意事项

对于 DNS 配置，ONTAP 最多支持每个 SVM 使用 6 个域名和 3 个名称服务器。如果 7- 模式系统和目标 SVM 之间的唯一域名或名称服务器数量超过支持的限制，则 7- 模式过渡工具会报告阻止错误。要继续过渡，您应忽略该工具中的 DNS 配置过渡。



如果忽略了 DNS 配置的过渡，则必须在目标 SVM 上手动配置 DNS 。

NIS 过渡注意事项

- 7- 模式系统上的 NIS 域名长度不得超过 64 个字符。
- 要过渡到运行 ONTAP 9.1 或更早版本的目标集群版本，7- 模式系统上的 `nis.servers` 选项必须仅配置 IP 地址，而不是完全限定域名（FQDN）。

如果要过渡到运行 ONTAP 9.1 或更早版本的集群，则过渡前必须使用 IP 地址在 7- 模式系统上配置 `nis.servers` 选项。如果在配置了 FQDN 的 7- 模式系统上使用 `nis.servers` 选项，并且要过渡到运行 9.2 到 9.5 之间的任何 ONTAP 版本的集群，则支持过渡。

LDAP 过渡注意事项

- 如果为 7- 模式系统中的用户映射（`ldap.usermap.base`）和用户密码（`ldap.base.passwd`）查找指定了单独的基本值和范围值，则仅过渡用户密码的基本值和范围值。

基本值和范围值用于 ONTAP 中的用户映射和用户密码查找，这可能会导致发生原因安全问题。过渡后，如果需要，必须手动将用于用户映射的基本值和范围值添加到 ONTAP 中的用户可分辨名称（User Distinguished Name，DN）选项中。

过渡网络组以及 UNIX 用户和组的注意事项

只有当 7- 模式 `/etc/netgroup` 文件小于 5 MB 时，才会过渡网络组配置。只有当 SVM 上的 UNIX 用户和组总数不超过 ONTAP 中用户和组的限制时，才会过渡 UNIX 用户和组。

网络组注意事项

如果 7- 模式上的 `/etc/netgroup` 文件大于 5 MB，则不会过渡网络组配置。要继续过渡，必须执行以下操作之一：

- 排除网络组的过渡。

[自定义 7- 模式配置的过渡](#)

- 过渡前，将网络组配置移动到 NIS 或 LDAP 服务器。

UNIX 用户和组的注意事项

如果过渡的 UNIX 用户和组总数超过 ONTAP 中 UNIX 用户和组的限制，7- 模式过渡工具将阻止过渡。要继续过渡，必须执行以下操作之一：

- 排除 UNIX 用户和组的过渡。

[自定义 7- 模式配置的过渡](#)

- 过渡前，将 UNIX 用户和组移动到 NIS 或 LDAP 服务器。
- 相关信息 *

["NFS 管理"](#)

为 NFS 过渡做准备

如果 NFS 已获得许可，并且 NFS 服务正在 7- 模式系统上运行，则必须手动准备集群和目标 SVM 以过渡 NFS 配置。此外，您还必须了解要过渡的配置。

ONTAP 不支持某些在 7- 模式下运行的 NFS 配置。某些配置不会通过 7- 模式过渡工具进行过渡，必须手动应用于 SVM。

过渡 NFS 配置的前提条件

只有在 7- 模式系统和集群满足特定前提条件时，7- 模式过渡工具才会过渡 NFS 配置。如果不满足任何条件，该工具将不会过渡配置。

7- 模式前提条件

- NFS 必须获得许可。
- 如果 MultiStore 已获得许可，则必须在所有 vFiler 单元上启用 NFS 。
- 过渡期间，7- 模式系统上必须运行 NFS 服务。

即使在断开客户端访问并准备开始导出阶段后，该服务也必须在 7- 模式系统上运行。

- 如果要过渡内存导出规则，必须在过渡前将其添加到 `/etc/exports` 文件中。

7- 模式过渡工具仅过渡在 `/etc/exports` 文件中定义的持久导出规则。

集群前提条件

- NFS 必须获得许可。
- 相关信息 *

["NetApp 文档：ONTAP 9"](#)

NFS 过渡：支持和不支持的配置以及所需的手动步骤

某些 NFS 配置不会过渡到 ONTAP，因为它们在 ONTAP 中不受支持，与 7- 模式存在功能差异，或者必须手动过渡。您应验证所有预检错误和警告消息，以评估此类配置对过渡的影响。

支持过渡的配置

从较高层面来看，7- 模式过渡工具会过渡以下 NFS 配置：

- NFS 选项：
 - `nfs.udp.xfersize`
 - `nfs.v4.id.domain`
 - `nfs.v4.acl.max.aces`
 - `nfs.tcp.xfersize`
 - `nfs.rpcsec.ctx.high`
 - `nfs.rpcsec.ctx.idle`
 - `nfs.response.trigger`
 - `wapl.default_nt_user`

- `nfs.mount_rootonly`
- `nfs.tcp.enable`
- `nfs.udp.enable`
- `nfs.response.trace`
- `nfs.v4.read_delegation`
- `nfs.v4.write_delegation`
- `nfs.v4.acl.enable`
- `nfs.vStorage.enable`
- `nfs.v3.enable`
- `nfs.v4.enable`

- NFS 导出规则：

如果导出规则配置了 `-actual` 选项，则会忽略导出的路径（别名路径），并使用实际路径配置导出规则。

- 具有 Kerberos 安全 `krb5p` 的导出规则

有关这些 NFS 配置的详细信息，请参见预检结果。

ONTAP 中不支持的配置

ONTAP 不支持以下 NFS 配置：

- 除 `qtree` 级 NFS 导出以外的子卷 NFS 导出
- WebNFS
- PC-NFS
- NFSv2
- 从一个或多个文件系统隔离 NFS 客户端 路径
- 一些 NFS 选项

有关不支持的选项的完整列表，请参见预检警告消息。

必须手动过渡的配置

ONTAP 中支持某些 NFS 配置，但 7- 模式过渡工具不会过渡这些配置。

以下 NFS 配置会在预检操作中生成警告消息，您必须在 SVM 上手动应用这些配置：

- NFS 审核配置
- NFS 选项：
 - `rpc.Nsm.tcp.port`
 - `rpc.Nsm.udp.port`

- `rpc.mount.tcp.port`
- `rpc.mount.udp.port`
- `nfs.export.neg.timeout`
- `nfs.export.pos.timeout`
- `nfs.export.harvest.timeout` 使用 `vserver nfs modify` 命令修改启用了 NFS 的 Storage Virtual Machine (SVM) 的配置。

- Kerberos 配置

在 ONTAP 中功能不同的配置

以下 NFS 配置在 ONTAP 中的功能有所不同：

- NFS 导出规则
- NFS 导出访问缓存
- NFS 诊断命令
- 支持 `showmount` 命令
- NFS Kerberos 加密
- NLM 版本支持
- 相关信息 *

自定义 7- 模式配置的过渡

"NFS 管理"

NFS 导出的过渡方式

您必须了解过渡后如何在 SVM 上配置 NFS 导出。如果 ONTAP 不支持 7- 模式导出配置，则可能需要执行一些手动步骤。

您必须了解有关 NFS 导出过渡的以下注意事项：

- 如果未导出 SVM 根卷以允许对所有 NFS 客户端进行只读访问，则 7- 模式过渡工具会创建一个新的导出策略，允许所有 NFS 客户端进行只读访问，并使用新的导出策略导出 SVM 的根卷。

要确保所有过渡后的卷或 qtree 均可挂载，必须允许所有 NFS 客户端对 SVM 的根卷进行只读访问。

- 过渡具有 ONTAP 不支持的导出配置的 7- 模式卷时，这些卷将被导出，以禁止访问所有 NFS 客户端。

过渡后，必须手动配置这些卷的导出策略，以提供所需的访问权限。

- 过渡具有 ONTAP 不支持的导出配置的 7- 模式 qtree 时，它们将继承父卷的导出策略。

过渡后，必须手动配置这些 qtree 的导出策略，以提供所需的访问权限。

- 在 ONTAP 中，要使 NFS 客户端能够挂载 qtree，NFS 客户端必须在所有父接合路径上具有只读权限，直到 SVM 的根卷接合路径（即 /）为止。

要使 NFS 客户端能够挂载 qtree，qtree 必须属于具有只读权限的卷。如果在卷级别没有只读权限，NFS 客户端将无法挂载 qtree。

- 如果在只读，读写和 root 访问权限列表的组合中指定了同一主机，则必须在过渡后评估过渡后的导出规则，以确定这些主机的适当访问权限。

"NetApp 技术报告 4067：《NFS 最佳实践和实施指南》"

示例：修改卷的导出策略以允许访问 **qtree**

请考虑在 7- 模式存储系统（192.168.26.18）中配置的以下导出规则，该规则允许 NFS 客户端 192.168.10.10 对卷 volstd10 和 qtree qtree1 进行读 / 写访问：

```
/vol/volstd10/qtree1 -sec=sys,rw=192.168.10.10,nosuid  
/vol/volstd10 -sec=sys,rw=192.168.11.11,nosuid
```

过渡后，ONTAP 中卷 volsdt10 的导出策略如下所示：

```
cluster-01::> export-policy rule show -vserver std_22 -policyname std_2226  
-instance  
(vserver export-policy rule show)  
  
Vserver: std_22  
Policy Name: std_2226  
Rule Index: 1  
Access Protocol: any  
Client Match Hostname, IP Address, Netgroup, or Domain: 192.168.11.11  
RO Access Rule: sys  
RW Access Rule: sys  
User ID To Which Anonymous Users Are Mapped:65534  
Superuser Security Types: none  
Honor SetUID Bits in SETATTR: false  
Allow Creation of Devices: true  
  
cluster-01::>
```

过渡后，ONTAP 中 qtree qtree1 的导出策略如下所示：

```

cluster-01::> export-policy rule show -vserver std_22 -policyname
std_2225 -instance
(vserver export-policy rule show)

Vserver: std_22
Policy Name: std_2225
Rule Index: 1
Access Protocol: any
Client Match Hostname, IP Address, Netgroup, or Domain: 192.168.10.10
RO Access Rule: sys
RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: none
Honor SetUID Bits in SETATTR: false
Allow Creation of Devices: true
cluster-01::>

```

要使 NFS 客户端 192.168.10.10 能够访问 qtree ， NFS 客户端 192.168.10.10 必须对 qtree 的父卷具有只读访问权限。

以下输出显示 NFS 客户端在挂载 qtree 时被拒绝访问：

```

[root@192.168.10.10 ]# mount 192.168.35.223:/vol/volstd10/mtree1
transition_volume_mtreemount:192.168.35.223:/vol/volstd10/mtree1 failed,
reason
given by server: Permission denied [root@192.168.10.10 ]#

```

您必须手动修改卷的导出策略，以便为 NFS 客户端 192.168.10.10 提供只读访问权限。

```

cluster-01::> export-policy rule create -vserver std_22 -policyname
std_2226 -clientmatch
192.168.10.10 -rorule sys -rwrule never -allow-suid false -allow-dev true
-superuser none -protocol nfs
(vserver export-policy rule create)

cluster-01::> export-policy rule show -vserver std_22 -policyname std_2226
-instance
(vserver export-policy rule show)

Vserver: std_22
Policy Name: std_2226
Rule Index: 1
Access Protocol: any
Client Match Hostname, IP Address, Netgroup, or Domain: 192.168.11.11
RO Access Rule: sys
RW Access Rule: sys
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: none
Honor SetUID Bits in SETATTR: false
Allow Creation of Devices: true

**
Vserver: std_22
Policy Name: std_2226
Rule Index: 2
Access Protocol: nfs
Client Match Hostname, IP Address, Netgroup, or Domain: 192.168.10.10
RO Access Rule: sys
RW Access Rule: never
User ID To Which Anonymous Users Are Mapped: 65534
Superuser Security Types: none
Honor SetUID Bits in SETATTR: false
Allow Creation of Devices: true**

cluster-01::>

```

示例：**qtree** 导出规则在 **7-** 模式和 **ONTAP** 中有何不同

在 7- 模式存储系统中，当 NFS 客户端通过 **qtree** 的父卷的挂载点访问 **qtree** 时，**qtree** 导出规则将被忽略，其父卷的导出规则将生效。但是，在 **ONTAP** 中，无论 NFS 客户端是直接挂载到 **qtree**，还是通过 **qtree** 的父卷的挂载点访问 **qtree**，**qtree** 导出规则始终会强制执行。此示例专门适用于 NFSv4。

以下是 7- 模式存储系统（192.168.26.18）上的导出规则示例：

```
/vol/volstd10/qtrees1 -sec=sys,ro=192.168.10.10,nosuid
/vol/volstd10 -sec=sys,rw=192.168.10.10,nosuid
```

在 7- 模式存储系统上，NFS 客户端 192.168.10.10 仅对 qtrees 具有只读访问权限。但是，当客户端通过其父卷的挂载点访问 qtrees 时，客户端可以向 qtrees 写入数据，因为客户端对卷具有读 / 写访问权限。

```
[root@192.168.10.10]# mount 192.168.26.18:/vol/volstd10 transition_volume
[root@192.168.10.10]# cd transition_volume/qtrees1
[root@192.168.10.10]# ls transition_volume/qtrees1
[root@192.168.10.10]# mkdir new_folder
[root@192.168.10.10]# ls
new_folder
[root@192.168.10.10]#
```

在 ONTAP 中，当 NFS 客户端 192.168.10.10 直接访问 qtrees qtrees1 或通过 qtrees 父卷的挂载点访问 qtrees 时，该客户端仅对该 qtrees 具有只读访问权限。

过渡后，您必须评估强制实施 NFS 导出策略的影响，如果需要，请将这些过程修改为在 ONTAP 中强制实施 NFS 导出策略的新方式。

- 相关信息 *

["NFS 管理"](#)

为 SMB/CIFS 过渡做准备

如果 SMB/CIFS 已获得许可，而 SMB/CIFS 服务正在 7- 模式系统上运行，则必须在目标集群和 SVM 上手动执行一些任务，例如添加 SMB/CIFS 许可证和创建 SMB/CIFS 服务器，以便过渡 SMB/CIFS 配置。

此外，您还必须了解要过渡的配置。ONTAP 不支持某些在 7- 模式下运行的 SMB/CIFS 配置。某些配置不会通过 7- 模式过渡工具进行过渡，必须手动应用于 SVM。

过渡 CIFS 配置的前提条件

只有在 7- 模式系统和集群满足特定前提条件时，7- 模式过渡工具才会过渡 CIFS 配置。如果不满足任何条件，该工具将不会过渡配置。

7- 模式前提条件

- 必须添加 CIFS 许可证。
- 如果启用了 MultiStore 许可证，则必须将 CIFS 添加到拥有过渡卷的 vFiler 单元的允许协议列表中。
- 过渡期间必须设置并运行 CIFS。

即使在断开客户端访问并准备开始导出阶段后，CIFS 服务也必须在 7- 模式系统上运行。

- CIFS 的身份验证类型必须为 Active Directory （AD ）或工作组。

集群前提条件

- 必须添加 CIFS 许可证。
- 不同的 ONTAP 版本支持以下 CIFS 身份验证方法：
 - 集群模式 Data ONTAP 8.2.x 和 8.3.x 支持 AD 身份验证。
 - ONTAP 9.0 或更高版本支持 AD 身份验证和工作组身份验证。
- 下表列出了必须在目标 SVM 上使用的身份验证方法：

7- 模式身份验证方法	集群模式 Data ONTAP 8.2.x 和 8.3.x 身份验证方法	ONTAP 9.5 或更早版本的身份验证方法
AD	AD	AD
工作组	AD	工作组或 AD

- 如果 7- 模式 CIFS 服务器和目标 SVM CIFS 服务器之间的 AD 域不匹配，则可以将 CIFS 配置从 7- 模式过渡到 ONTAP 。

检测到 AD 域名不匹配时，该工具会触发可忽略的阻止错误。要继续过渡，您可以确认阻止错误。

- 必须在应用配置（预转换）阶段之前手动配置 CIFS 服务器。

您可以通过以下两种方式在 SVM 上创建 CIFS 服务器：

如果您要 ...	执行以下操作 ...
<p>将 CIFS 服务器标识传输或保留到目标 SVM</p>	<div data-bbox="844 159 1484 373" style="border: 1px solid #ccc; padding: 10px; margin-bottom: 10px;"> <p>You have the following two options to create the CIFS server: .. 适用于所有版本的 ONTAP :</p> </div> <p>+ * 在 SVM 配置阶段之前，您必须使用临时 CIFS 标识在 7- 模式系统上重新配置 CIFS 服务器。</p> <p>+ 通过这种重新配置，可以在 SVM 上配置原始 CIFS 服务器标识。您必须使用新的临时标识在 " SVM 配置 " 和 "导出并暂停` " 阶段验证 CIFS 服务器是否正在 7- 模式系统上运行。要在 SVM 配置和 "导出并暂停` " 阶段从 7- 模式读取 CIFS 配置，需要执行此操作。</p> <ul style="list-style-type: none"> • 您必须使用原始 7- 模式 CIFS 标识在目标 SVM 上配置 CIFS 服务器。 • 满足这些条件后，您可以执行 " SVM 配置 " 操作，然后执行 "导出并暂停` " 操作，以使客户端能够访问 ONTAP 卷。 <ul style="list-style-type: none"> a. 适用于 ONTAP 9.0 至 9.5 版： • 使用 <code>vserver cifs modify</code> 命令更改 CIFS 服务器名称（CIFS 服务器 NetBIOS 名称）。 使用此功能，您应使用临时标识在目标 SVM 上创建 CIFS 服务器，然后执行 " SVM 配置 " 操作。 • 在 "import` " 阶段之后，您可以在目标集群上运行 <code>vserver cifs modify</code> 命令，将目标 SVM CIFS 标识替换为 7- 模式 CIFS 标识。

如果您要 ...	执行以下操作 ...
使用新标识	<ul style="list-style-type: none"> 在 " SVM 配置 " 阶段之前，您必须使用新的 CIFS 标识在目标 SVM 上配置 CIFS 服务器。 在 " SVM 配置 " 和 " 导出并暂停 " 阶段，您必须验证 CIFS 服务器是否已在 7- 模式系统上启动并运行。 <p>要在 " SVM 配置 和 " 导出并暂停 " 期间从 7- 模式读取 CIFS 配置，需要执行此操作。</p> <ul style="list-style-type: none"> 验证这些条件后，您可以执行 " SVM 配置 " 操作。 <p>然后，您可以测试 SVM 配置，然后计划执行存储转换。</p>

过渡到 **ONTAP** 时支持和不支持的 **CIFS** 配置

某些 CIFS 配置不会过渡到 ONTAP ，因为它们在 ONTAP 中不受支持或必须手动过渡。您应验证所有预检错误和警告消息，以评估此类配置对过渡的影响。

支持过渡的配置

从较高层面来看， 7- 模式过渡工具会过渡以下 CIFS 配置：

- CIFS 首选 DC 配置
- 用户映射配置：
 - `/etc/usermap.cfg`
 - `WAFL.NT_admin_priv_map_to_root_`
- CIFS 本地用户和组
- 符号链接和 Widelink 配置 (`/etc/symlink.translations`)
- CIFS 审核配置
- CIFS 共享
- CIFS 共享 ACL
- CIFS 主目录配置
- CIFS 选项：
 - `cifs.GPO.enable`
 - `cifs.smb2.enable`
 - `cifs.smb2.signation.required`
 - `cifs.Wins_servers`
 - `cifs.grant_implicit_exe_perms`

- `cifs.restrict_anonymous`

- SMB2 连接到外部服务器，例如域控制器。以下命令可实现此支持：
 - ``* cifs security modify -vserver SVM1 -smb2-enabled-for-dc-connections*``
- FPolicy 原生文件阻止配置

有关这些 CIFS 配置的详细信息，请参见预检结果。

ONTAP 不支持的配置

ONTAP 不支持以下 7- 模式配置。因此，无法过渡这些配置。

- NT4 和密码身份验证类型
- SMB1 和 SMB2 签名的不同选项
- 每个客户端的 CIFS 统计信息 *
 - 对 Windows NT 之前的客户端进行身份验证
- 审核本地用户和组的帐户管理事件
- 包含 IP 地址，主机名，网络名称或以点分表示法指定子网的网络名称的用户映射条目
- 对计算机帐户具有访问限制的 CIFS 共享

过渡后，计算机帐户可以访问所有共享。

必须手动过渡的配置

ONTAP 支持某些 CIFS 配置，但 7- 模式过渡工具不会过渡这些配置。

以下 CIFS 配置会在预检中生成警告消息。您必须在 SVM 上手动应用以下配置：

- 防病毒设置
- FPolicy 配置

7- 模式 FPolicy 和防病毒服务器不支持 ONTAP。要升级这些服务器，您必须联系服务器供应商。但是，在提交过渡之前，不得停用 7- 模式 FPolicy 和防病毒服务器。如果您决定回滚过渡，则必须执行这些操作。

- BranchCache 配置
- 字符映射配置（`charmap`）
- 用于使用创建文件的 CIFS 共享的 `Forcegroup` 属性 已将 UNIX 组指定为所属组
- 指定最大数量的 CIFS 共享的 `Maxusers` 属性 允许同时连接到 7- 模式 CIFS 共享的数量
- 存储级别访问防护（`SLAG`）配置
- 具有 UNIX 模式权限的共享级 ACL
- 为 UNIX 用户和组共享 ACL
- LAN Manager 身份验证级别
- NetBIOS 别名

- CIFS 搜索域
- 某些 CIFS 选项

有关这些选项的详细信息，请参见预检结果。

- 相关信息 *

自定义 7- 模式配置的过渡

过渡 CIFS 本地用户和组的注意事项

迁移 CIFS 本地用户和组时，您必须了解运行过渡操作的注意事项。

- 不支持将 CIFS 数据提供卷从具有本地用户和组的 7- 模式控制器或 vFiler 单元过渡到具有非 BUILTIN CIFS 本地用户和组的 SVM。

要进行过渡，SVM 只能具有 BUILTIN CIFS 本地用户和组。

- 您必须确保 7- 模式中的本地用户和组数量不超过 ONTAP 的本地用户和组限制。

如果 7- 模式中的本地用户和组数量超过 ONTAP 中定义的限制，您必须联系技术支持。

- 在 7- 模式系统中，密码为空的本地用户帐户或密码超过 14 个字符的本地用户帐户将过渡到密码为 ` * cifsUser@1*` 的 ONTAP 软件。

过渡完成后，您可以使用密码 ` * cifsUser@1*` 从 Windows 系统访问这些用户。然后，您必须使用以下命令手动更改 SVM 上此类 CIFS 本地用户的密码：

```
` * cifs users-and-groups local-user set-password -vserver svm_name -user-name user_name*`
```

- 如果无法从目标 ONTAP 软件访问 7- 模式过渡工具 IP 地址，则 7- 模式过渡工具会阻止在预检阶段将 CIFS 本地用户和组过渡到 ONTAP 软件。如果您在预检阶段发现此错误，请使用

```
` * 网络 ping -node local -destination ip_address*`
```

命令以确保可从目标 ONTAP 软件访问 7- 模式过渡工具 IP 地址。您可以编辑随 7- 模式过渡工具安装的 ` \etc\conf\transition-tool.conf` 文件，以修改该工具使用的任何配置选项，例如 7- 模式过渡工具 IP 地址。

- 要将本地用户和组过渡到的 SVM 必须具有数据 LIF。
- 如果本地组将多个成员系统标识符（SID）映射到 7- 模式系统上的单个域用户或组，则 7- 模式过渡工具会阻止在预检阶段将本地用户和组过渡到 ONTAP。

如果您在预检阶段看到此错误，则必须手动删除映射到 7- 模式系统上的单个域用户或组的其他 SID。然后，您必须重新运行预检操作，并且仅将一个 SID 映射到域用户或组。

["故障排除工作流：CIFS：连接到系统的设备无法正常运行"](#)

- 相关信息 *

"SMB/CIFS 管理"

为 SAN 过渡做准备

过渡 SAN 环境之前，您必须了解 SAN 过渡支持哪些配置，在 SVM 上创建 SAN LIF 并为 SAN 主机做好过渡准备。

过渡前创建 SAN LIF

由于 7- 模式过渡工具不会过渡 FC 和 iSCSI LIF，因此过渡前必须在 SVM 上创建这些 LIF。您必须在拥有 LUN 的节点和节点的 HA 配对节点上配置 SAN LIF。

必须将所需的 SAN（FC 或 iSCSI）许可证添加到集群中。

为了实现冗余，您必须在托管 LUN 的节点及其 HA 配对节点上创建 SAN LIF。

步骤

1. 根据所使用的协议，在 LUN 过渡到的目标节点上创建 FC 或 iSCSI LIF：

` * 网络接口 cre*`

如果要重复使用 iSCSI LIF 的 7- 模式 IP 地址，则必须在管理关闭状态下创建 LIF。您可以在转换操作后将这些 LIF 置于管理启动状态。

2. 在节点的 HA 配对节点上创建 LIF。
3. 验证是否已正确设置 LIF：

` * 网络接口显示 *`

◦ 相关信息 *

"SAN 管理"

使用 FC 分区计划配置分区

过渡 SAN FC 环境之前，您必须使用 FC 分区规划器对启动程序主机和目标进行分组来配置分区。

- 必须使用生成 FC 分区规划器 7- 模式过渡工具的收集和访问功能
- FC 分区脚本文件必须可访问。
 - a. 如果 7- 模式系统上的 igroup 配置发生任何更改，请修改并重新生成 FC 分区计划。

[通过向 7- 模式添加系统来生成评估报告 过渡工具](#)

- b. 登录到交换机的命令行界面。
- c. 一次复制并执行一个所需的分区命令。

以下示例将在交换机上运行 zone 命令：

```
switch1:admin>config terminal
# Enable NPIV feature
feature npiv
zone name auto_transition_igroup_d3l_194bf3 vsan 10
member pwnn 21:00:00:c0:dd:19:4b:f3
member pwnn 20:07:00:a0:98:32:99:07
member pwnn 20:09:00:a0:98:32:99:07
.....
.....
.....
copy running-config startup-config
```

- a. 使用测试启动程序主机验证从集群进行的数据访问。
- b. 验证完成后，请执行以下步骤：
 - i. 断开测试启动程序主机的连接。
 - ii. 删除分区配置。

准备 SAN 主机以进行过渡

过渡 SAN 环境之前，您必须执行一些手动步骤来准备要过渡的 SAN 主机。

您必须已使用清单收集工具为 SAN 主机生成清单工作簿。

"主机和存储过渡信息收集"

步骤

1. 验证主机是否支持过渡。

"NetApp 互操作性表工具"

2. 在主机上执行过渡前步骤。

"SAN 主机过渡和修复"

SAN 过渡：支持和不支持的配置以及所需的手动步骤

您必须了解 7- 模式过渡工具过渡的 SAN 配置。此外，您还应了解 ONTAP 不支持的 7- 模式 SAN 功能，以便在过渡之前采取任何必要的措施。

您应验证所有预检错误和警告消息，以评估此类配置对过渡的影响。

已过渡的配置

7- 模式过渡工具会过渡以下 SAN 配置：

- FC 和 iSCSI 服务
- igroup 和 LUN 映射



- 未映射到任何 LUN 的 7- 模式 igroup 不会过渡到目标 SVM。
- 对于集群模式 Data ONTAP 8.3.0 和 8.3.1，在预转换操作期间不支持过渡 igroup 和 LUN 映射配置。

而是在转换操作期间创建所需的 igroup。对于主卷和独立卷，LUN 会在转换操作期间映射到 igroup。但是，对于二级卷，在转换操作期间不支持将 LUN 映射到 igroup。完成主卷的过渡后，必须手动映射二级 LUN。

- 对于 ONTAP 8.3.2 及更高版本支持的版本，将在预转换操作期间应用 igroup 和 LUN 映射配置。

ONTAP 中不支持的配置

ONTAP 中不支持的配置如下：

- 7- 模式 Snapshot 副本支持的 LUN 克隆

任何还原操作都不支持 Snapshot 副本中存在的 Snapshot 副本支持的 LUN 克隆。在 ONTAP 中无法访问这些 LUN。过渡前，必须拆分或删除 7- 模式 Snapshot 副本支持的 LUN 克隆。

- ostype 参数值为 vld，image 或任何用户定义的字符串的 LUN

过渡前，您必须更改此类 LUN 的 ostype 参数值或删除这些 LUN。

- LUN 克隆拆分

过渡前，您必须等待活动的 LUN 克隆拆分操作完成，或者中止 LUN 克隆拆分并删除 LUN。

以下 7- 模式功能可用于继续过渡过程，但在 ONTAP 中不受支持：

- 命令 `lun share`

通过 NAS 协议共享 LUN

- SnapValidator

必须手动过渡的配置

必须手动过渡以下配置：

- SAN LIF

过渡前，必须手动创建 LIF。

- 端口集

过渡后，必须手动配置绑定到端口集的 igroup。

- iSCSI 访问列表信息
- iSNS 配置
- iSCSI CHAP 和 RADIUS 配置
- 相关信息 *

["NFS 管理"](#)

["网络和 LIF 管理"](#)

过渡 **SAN** 卷时的空间注意事项

过渡期间，您必须确保卷中有足够的可用空间。除了存储数据和 Snapshot 副本所需的空
间之外，过渡过程还需要每个 LUN 1 MB 的空间来更新某些文件系统元数据。

您可以在 7- 模式卷上使用 `df -h` 命令来验证卷中的每个 LUN 是否有 1 MB 的可用空间。卷还应具有与主机暂
停前预期写入卷的数据量等效的可用空间。如果卷没有足够的可用空间，则必须向 7- 模式卷添加所需的空
间量。

如果在导入阶段由于卷上缺少空间而导致过渡失败，则会生成以下 EMS 消息：

`LUN.vol.proc.fail.no.space`：由于空间不足，无法处理卷 `vol_name` 中的 LUN。

如果卷包含预留了空间的 LUN，则将每个 LUN 的卷增加 1 MB 可能无法提供足够的空间。在这种情况下，需要
添加的空间量是卷的 Snapshot 预留大小。向卷添加空间后，您可以使用 `lun transition start` 命令过渡
LUN。

- 相关信息 *

[从失败的 LUN 过渡中恢复](#)

["NetApp 文档：ONTAP 9"](#)

准备数据保护功能以进行过渡

过渡 7- 模式 SnapMirror 关系时，必须执行一些手动步骤。此外，您还必须了解支持和
不支持过渡的数据保护关系。

准备集群以过渡卷 **SnapMirror** 关系

要过渡 7- 模式卷 SnapMirror 关系，必须将 SnapMirror 许可证添加到源集群和目标集群。
您还必须在 SnapMirror 关系中的主卷和二级卷要过渡到的集群之间创建集群对等关系，并
创建 SnapMirror 计划。

您必须已记录 7- 模式二级系统的 `/etc/snapmirror.conf` 文件中定义的 SnapMirror 计划。

步骤

1. 在源集群和目标集群上添加 SnapMirror 许可证：

```
` * 系统许可证 add license_code`
```

2. 在每个集群中，创建集群对等关系。

"集群和 SVM 对等快速配置"

3. 在与 7- 模式二级系统中的计划匹配的二级 SVM 上创建计划：

` * 作业计划 cron cre*`

◦ 相关信息 *

"ONTAP 9 命令"

数据保护过渡：支持和不支持的配置

您可以过渡属于 SnapMirror 关系的卷。但是，某些数据保护和灾难恢复配置不支持过渡，因此您必须执行一些手动步骤来过渡这些配置。

支持的配置

您可以使用 7- 模式过渡工具过渡卷 SnapMirror 关系。您可以对主 HA 对和二级 HA 对执行无副本过渡。然后，您必须在过渡后手动设置卷 SnapMirror 关系。

过渡 SnapMirror 关系

不支持的配置

- SnapVault 关系

可以迁移作为 SnapVault 关系源的卷，但不会过渡 SnapVault 关系。作为 SnapVault 关系目标的卷只能在 SnapVault 备份停止后迁移。

"NetApp 技术报告 4052：《成功过渡到集群模式 Data ONTAP》（Data ONTAP 8.2.x 和 8.3）"

- qtree SnapMirror 关系

可以过渡 qtree 作为 qtree SnapMirror 关系源的卷，但不会过渡 qtree SnapMirror 关系。只有在 qtree SnapMirror 关系中断后，才能迁移 qtree 作为 qtree SnapMirror 关系目标的卷。

- 灾难恢复 vFiler 单元

可以迁移作为灾难恢复 vFiler 单元源的卷；但是，灾难恢复 vFiler 单元不会过渡。只有在删除灾难恢复关系后，才能迁移作为灾难恢复 vFiler 单元目标的卷。

- NDMP 配置

过渡完成后，您必须在 ONTAP 中手动为过渡后的卷设置备份策略。

"使用磁带备份保护数据"

- 同步 SnapMirror 关系

ONTAP 不支持此功能；但是，属于此关系一部分的卷可以过渡。

- 相关信息 *

自定义 7- 模式配置的过渡

版权信息

版权所有 © 2023 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。