管理NFS中继

ONTAP 9

NetApp
January 09, 2026

This PDF was generated from https://docs.netapp.com/zh-cn/ontap/nfs-trunking/index.html on January 09, 2026. Always check docs.netapp.com for the latest.

目录

管理NFS中继 1
了解ONTAP NFS中继 1
如何使用中继 1
支持的客户端 1
NFS中继与nconnect之间的区别 2
为中继配置新的NFS服务器和导出 2
在ONTAP SVM上创建启用了中继的NFS服务器 2
为ONTAP NFS中继准备网络 3
创建ONTAP卷导出策略 5
挂载ONTAP卷或数据共享以进行NFS中继 6
调整现有NFS导出以用于中继 7
为ONTAP NFS中继调整单路径导出 7
在ONTAP NFS服务器上启用中继 7
更新ONTAP NFS中继网络 7
修改ONTAP卷导出策略 9
重新挂载ONTAP卷或数据共享以进行NFS中继 10

管理NFS中继

了解ONTAP NFS中继

从ONTAP 9.14.1开始、NFSv4.1客户端可以利用会话中继打开与NFS服务器上不同的LUN的多个连接、从而提高数据传输速度并通过多路径提供故障恢复能力。

对于将FlexVol卷导出到具有中继功能的客户端(尤其是VMware和Linux客户端)、或者对于基于RDMA、TCP或pNFS的NFS、中继非常有用。

在ONTAP 9.14.1中、中继仅限于单个节点上的LUN；中继不能跨多个节点的LUN。

中继支持FlexGroup卷。虽然这样可以提高性能、但只能在单个节点上配置对FlexGroup卷的多路径访问。

此版本中的多路径仅支持会话中继。

如何使用中继

要利用中继提供的多路径优势、您需要一组与包含已启用中继的NFS服务器的SVM关联的LF (称为_TRUNKING group_)。中继组中的LUN必须在集群的同一节点上具有主端口、并且它们必须驻留在这些主端口上。最佳实践是、一个中继组中的所有LUN都属于同一个故障转移组。

ONTAP支持从给定客户端为每个节点建立多达16个中继连接。

当客户端挂载启用了中继的服务器中的导出时、它们会为中继组中的LID指定多个IP地址。客户端连接到第一个LIF后、只有在符合中继组要求的情况下、才会向NFSv4.1会话添加其他LIF并将其用于中继。然后、客户端会根据自己的算法(例如轮循)在多个连接上分布NFS操作。

为了获得最佳性能、您应在专用于提供多路径导出的SVM中配置中继、而不是单路径导出。也就是说、您只能在SVM中的NFS服务器上启用中继、而此SVM的导出仅提供给已启用中继的客户端。

支持的客户端

ONTAP NFSv4.1服务器支持与任何支持NFSv4.1会话中继的客户端进行中继。

以下客户端已通过ONTAP 9.14.1的测试：

- VMware—ESXi 7.0U3及更高版本
- Linux—Red Hat Enterprise Linux (RHEL) 8.8和9.3

> 如果在故障转移事件(例如控制器故障转移)中将中继的RIF迁移到另一个节点、RHEL NFS客户端将不会重新建立中继。将LUN迁移到另一节点后、它们将从中继组中删除。如果中继组中的所有LIF均已迁移、则NFS客户端将仅使用第一个LIF继续I/O

> 在NFS服务器上启用中继后、在不支持中继的NFS客户端上访问导出共享的用户可能会看到性能下降。这是因为多个SVM数据SVM挂载只使用一个TCP连接。

NFS中继与nconnect之间的区别

从 ONTAP 9.8 开始，如果启用了 NFSv4.1 ，则默认情况下可以使用 nconnect 功能。在支持nconnect的客户端上、一个NFS挂载可以通过一个LIF建立多个TCP连接(最多16个)。

相比之下、中继是_multiPathing_功能、可通过多个LIFs提供多个TCP连接。如果您能够在环境中使用其他NIC、则中继可以提供比nconnect更出色的并行处理能力和性能。

详细了解 "n连接"。

为中继配置新的NFS服务器和导出

在ONTAP SVM上创建启用了中继的NFS服务器

从ONTAP 9.14.1开始、可以在NFS服务器上启用中继。创建NFS服务器时、默认情况下会启用NFSv4.1。

开始之前

创建启用了中继的NFS服务器需要SVM。SVM必须：

- 有足够的存储作为后盾、可满足客户端数据要求。
- 已为NFS启用。

您可以使用现有SVM；但是、启用中继需要重新挂载所有NFSv4.x客户端、这可能会造成系统中断。如果无法重新挂载、请为NFS服务器创建一个新的SVM。

步骤

1. 如果不存在合适的SVM、请创建一个：

   ```
   vserver create -vserver svm_name -rootvolume root_volume_name -aggregate
   aggregate_name -rootvolume-security-style unix -language C.UTF-8
   ```

2. 验证新创建的 SVM 的配置和状态：

   ```
   vserver show -vserver svm_name
   ```

   了解更多信息 "创建SVM"。

3. 创建NFS服务器：

   ```
   vserver nfs create -vserver svm_name -v3 disabled -v4.0 disabled -v4.1 enabled
   -v4.1-trunking enabled -v4-id-domain my_domain.com
   ```

4. 验证 NFS 是否正在运行：

   ```
   vserver nfs status -vserver svm_name
   ```

5. 验证是否已根据需要配置 NFS ：

   ```
   vserver nfs show -vserver svm_name
   ```

了解更多信息 "NFS服务器配置。"

完成后

根据需要配置以下服务：

- "DNS"
- "LDAP"
- "Kerberos"

为ONTAP NFS中继准备网络

要利用NFSv4.1中继、中继组中的LUN必须位于同一节点上、并且主端口位于同一节点上。应在同一节点上的故障转移组中配置这些LUN。

关于此任务

LIS和NIC的一对一映射可获得最大的性能提升、但不需要启用中继。至少安装两个NIC可以提高性能、但这并不是必需的。

中继组中的所有LUN都应属于同一个故障转移组。请注意、如果在同一节点上的故障转移组中配置了这些LUN、则该节点上的控制器故障转移可能会导致这些LUN脱机。如果未在同一节点上的故障转移组中配置这些LUN并故障转移到另一节点、则中继将不再起作用。

在故障转移组中添加或删除连接(和底层NIC)时、您应随时调整中继故障转移组。

开始之前

- 要创建故障转移组、您必须知道与NIC关联的端口名称。
- 这些端口必须都位于同一节点上。

步骤

1. 验证您计划使用的网络端口的名称和状态：

```
network port show
```

2. 创建故障转移组：

```
network interface failover-groups create -vserver <svm_name> -failover-group
<failover_group_name> -targets <ports_list>
```

> 虽然不要求具有故障转移组、但强烈建议这样做。

   - `<svm_name>`是包含NFS服务器的SVM的名称。
   - `<ports_list>`是要添加到故障转移组的端口列表。

     以格式添加端口 `<node_name>:<port_number>`，例如： `node1:e0c`。

     以下命令将为SVM VS1创建故障转移组fg3并添加三个端口：

```
network interface failover-groups create -vserver vs1 -failover-group fg3
-targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
```

了解更多信息 "故障转移组。"

有关的详细信息 `network interface failover-groups create`，请参见"ONTAP 命令参考"。

3. 如果需要、为中继组的成员创建LUN：

```
network interface create -vserver <svm_name> -lif <lif_name> -home-node
<node_name> -home-port <port_name> -address <IP_address> -netmask <IP_address>
[-service-policy <policy>] [-auto-revert <true|false>]
```

- `-home-node` -在对LIF运行network interface还原命令时、LIF返回到的节点。

  您还可以使用指定LIF是否应自动还原到主节点和主端口 `-auto-revert` 选项

- `-home-port` 是对LIF运行network interface还原命令时LIF返回到的物理或逻辑端口。
- 您可以使用指定IP地址 `-address` 和 `-netmask` 选项、而不是使用 `-subnet` 选项
- 分配IP地址时、如果不同IP子网上有客户端或域控制器、则可能需要配置网关的默认路由。有关在SVM中创建静态路由的详细信息 `network route create`，请参见"ONTAP 命令参考"。
- `-service-policy` - LIF的服务策略。如果未指定策略、则会自动分配默认策略。使用 `network interface service-policy show` 命令以查看可用的服务策略。
- `-auto-revert` 指定在启动、更改管理数据库状态或建立网络连接等情况下、数据LIF是否自动还原到其主节点。默认设置为false、但您可以根据环境中的网络管理策略将其设置为true。

  对中继组中的每个LIF重复此步骤。

  以下命令将创建 `lif-A` 对于SVM `vs1`，在端口上 `e0c` 节点的 `cluster1_01`：

```
network interface create -vserver vs1 -lif lif-A -service-policy default-
intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
```

了解更多信息 "创建LIF。"

4. 验证是否已创建这些生命周期：

```
network interface show
```

5. 验证配置的IP地址是否可访问：

要验证 ...	使用 ...
IPv4 地址	`network ping`
IPv6地址	`network ping6`

相关信息

- "网络 ping"
- "网络接口"
- "network port show"

创建ONTAP卷导出策略

要为客户端提供对数据共享的访问权限、您必须创建一个或多个卷、并且此卷的导出策略必须至少具有一个规则。

客户端导出要求：

- Linux客户端必须为每个中继连接(即每个LIF)具有单独的挂载和单独的挂载点。
- VMware客户端只需要为一个已导出的卷创建一个挂载点、并指定多个生命周期。

  VMware客户端需要在导出策略中具有root访问权限。

步骤

1. 创建导出策略

   ```
   vserver export-policy create -vserver svm_name -policyname policy_name
   ```

   策略名称最长可为 256 个字符。

2. 验证是否已创建导出策略：

   ```
   vserver export-policy show -policyname policy_name
   ```

   示例
   以下命令将在名为 vs1 的 SVM 上创建并验证是否已创建名为 exp1 的导出策略：

   ```
   vs1::> vserver export-policy create -vserver vs1 -policyname exp1
   ```

3. 创建导出规则并将其添加到现有导出策略：

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   。 `-clientmatch` 参数应标识要挂载导出的具有中继功能的Linux或VMware客户端。

   了解更多信息 "正在创建导出规则。"

4. 创建具有接合点的卷：

   ```
   volume create -vserver svm_name -volume volume_name -aggregate aggregate_name
   -size {integer[KB|MB|GB|TB|PB]} -security-style unix -user user_name_or_number
   -group group_name_or_number -junction-path junction_path -policy
   export_policy_name
   ```

了解相关信息 "正在创建卷。"

5. 验证是否已使用所需的接合点创建卷：

```
volume show -vserver svm_name -volume volume_name -junction-path
```

挂载ONTAP卷或数据共享以进行NFS中继

支持中继的Linux和VMware客户端可以从启用了中继的ONTAP NFSv4.1服务器挂载卷或数据共享。

了解相关信息 "支持的客户端"。

Linux客户端要求

如果使用9.16.1 9.161或更高版本以及Red Hat Enterprise Linux 8.7或更高版本(适用于RHEL 8)或9.2或更高版本(适用于RHEL 9)作为Linux客户端、则中继组只需要一个挂载点。使用以下选项、使用此命令挂载导出的卷 `trunkdiscovery`：

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

否则、中继组中的每个连接都需要一个单独的挂载点。使用选项、使用类似于以下内容的命令挂载导出的卷 `max_connect`：

```
mount <lif1_ip>:<volume_name> </mount_path1> -o vers=4.1,max_connect=16
```

```
mount <lif2_ip>:<volume_name> </mount_path2> -o vers=4.1,max_connect=16
```

版本 (`vers`)值应为 `4.1` 或更高版本。

。 `max_connect` 值对应于中继组中的连接数。

VMware客户端要求

需要使用mount语句、其中包含中继组中每个连接的IP地址。

使用类似以下内容的命令挂载导出的数据存储库：

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

。 `-H` 值对应于中继组中的连接。

调整现有NFS导出以用于中继

为ONTAP NFS中继调整单路径导出

您可以调整现有单路径(非中继) NFSv4.1导出以使用中继。只要满足服务器和客户端的前提条件、支持中继的客户端就可以在服务器上启用中继后立即利用性能的提高。

通过调整单路径导出以用于中继、您可以在其现有卷和SVM中维护导出的数据集。为此、您必须在NFS服务器上启用中继、更新网络和导出配置、并在客户端上重新挂载导出的共享。

启用中继会重新启动服务器。然后、VMware客户端必须重新挂载导出的数据存储库；Linux客户端必须使用重新挂载导出的卷 `max_connect` 选项

在ONTAP NFS服务器上启用中继

必须在NFS服务器上显式启用中继。创建NFS服务器时、默认情况下会启用NFSv4.1。

启用中继后、验证是否已根据需要配置以下服务。

- "DNS"
- "LDAP"
- "Kerberos"

步骤

1. 启用中继并确保已启用NFSv4.1：

   ```
   vserver nfs create -vserver svm_name -v4.1 enabled -v4.1-trunking enabled
   ```

2. 验证 NFS 是否正在运行： `vserver nfs status -vserver svm_name`
3. 验证是否已根据需要配置 NFS ：

   ```
   vserver nfs show -vserver svm_name
   ```

   了解更多信息 "NFS服务器配置。" ...如果要从此SVM为Windows客户端提供服务、请先移动共享、然后再删除服务器。 `vserver cifs show -vserver svm_name`

   + `vserver cifs delete -vserver svm_name`

更新ONTAP NFS中继网络

要利用NFSv4.1中继、中继组中的LUN必须位于同一节点上、并且主端口位于同一节点上。应在同一节点上的故障转移组中配置这些LUN。

关于此任务

LIS和NIC的一对一映射可获得最大的性能提升、但不需要启用中继。至少安装两个NIC可以提高性能、但这并不是必需的。

中继组中的所有LUN都应属于同一个故障转移组。请注意、如果在同一节点上的故障转移组中配置了这些LUN、则该节点上的控制器故障转移可能会导致这些LUN脱机。如果未在同一节点上的故障转移组中配置这些LUN并故障转移到另一节点、则中继将不再起作用。

在故障转移组中添加或删除连接(和底层NIC)时、您应随时调整中继故障转移组。

开始之前

- 要创建故障转移组、您必须知道与NIC关联的端口名称。
- 这些端口必须都位于同一节点上。

步骤

1. 验证您计划使用的网络端口的名称和状态：

   ```
   network port show
   ```

   有关的详细信息 `network port show`，请参见"ONTAP 命令参考"。

2. 创建中继故障转移组或修改现有中继故障转移组：

   ```
   network interface failover-groups create -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>

   network interface failover-groups modify -vserver <svm_name> -failover-group
   <failover_group_name> -targets <ports_list>
   ```

   > 虽然不要求具有故障转移组、但强烈建议这样做。

   - `<svm_name>`是包含NFS服务器的SVM的名称。
   - `<ports_list>`是要添加到故障转移组的端口列表。

     以格式添加端口 `<node_name>:<port_number>`，例如 `node1:e0c`。

     以下命令将创建故障转移组 `fg3` 对于SVM VS1、添加了三个端口：

     ```
     network interface failover-groups create -vserver vs1 -failover-group fg3
     -targets cluster1-01:e0c,cluster1-01:e0d,cluster1-01:e0e
     ```

   了解更多信息 "故障转移组。"

3. 根据需要为中继组成员创建其他的LUN：

   ```
   network interface create -vserver <svm_name> -lif <lif_name> -home-node
   <node_name> -home-port <port_name> -address <IP_address> -netmask <IP_address>
   [-service-policy <policy>] [-auto-revert <true|false>]
   ```

   - `-home-node` -在对LIF运行network interface还原命令时、LIF返回到的节点。

     您可以使用指定LIF是否应自动还原到主节点和主端口 `-auto-revert` 选项

   - `-home-port` 是对LIF运行network interface还原命令时LIF返回到的物理或逻辑端口。

- 您可以使用指定IP地址 `-address` 和 `-netmask` 选项
- 手动分配IP地址(不使用子网)时、如果其他IP子网上有客户端或域控制器、则可能需要配置网关的默认路由。 `network route create`命令页面包含有关在SVM中创建静态路由的信息。有关的详细信息 `network route create`，请参见"ONTAP 命令参考"。
- `-service-policy` - LIF的服务策略。如果未指定策略、则会自动分配默认策略。使用 `network interface service-policy show` 命令以查看可用的服务策略。

  有关的详细信息 `network interface service-policy show`，请参见"ONTAP 命令参考"。

- `-auto-revert` 指定在启动、更改管理数据库状态或建立网络连接等情况下、数据LIF是否自动还原到其主节点。默认设置为**false**，但您可以根据环境中的网络管理策略将其设置为true。

  对中继组中所需的每个附加LIF重复此步骤。

  以下命令将创建 `lif-A` 对于SVM `vs1`，在端口上 `e0c` 节点的 `cluster1_01`：

  ```
  network interface create -vserver vs1 -lif lif-A -service-policy default-
  intercluster -home-node cluster1_01 -home-port e0c -address 192.0.2.0
  ```

了解更多信息 "创建LIF。"

4. 验证是否已创建这些生命周期：

   ```
   network interface show
   ```

5. 验证配置的 IP 地址是否可访问：

要验证 ...	使用 ...
IPv4 地址	`network ping`
IPv6地址	`network ping6`

相关信息

- "网络 ping"
- "网络接口"

修改ONTAP卷导出策略

要使客户端能够利用现有数据共享的中继、您可能需要修改导出策略和规则及其所连接的卷。Linux客户端和VMware数据存储库具有不同的导出要求。

客户端导出要求：

- Linux客户端必须为每个中继连接(即每个LIF)具有单独的挂载和单独的挂载点。

  如果要升级到ONTAP 9.14.1、并且已导出卷、则可以继续在中继组中使用该卷。

- VMware客户端只需要为一个已导出的卷创建一个挂载点、并指定多个生命周期。

  VMware客户端需要在导出策略中具有root访问权限。

步骤

1. 验证现有导出策略是否已到位：

   ```
   vserver export-policy show
   ```

2. 验证现有导出策略规则是否适用于中继配置：

   ```
   vserver export-policy rule show -policyname policy_name
   ```

   特别是、请验证 `-clientmatch` 参数可正确标识要挂载导出的具有中继功能的Linux或VMware客户端。

   如果需要进行调整、请使用修改规则 `vserver export-policy rule modify` 命令或创建新规则：

   ```
   vserver export-policy rule create -vserver svm_name -policyname policy_name
   -ruleindex integer -protocol nfs4 -clientmatch { text | "text,text,…" }
   -rorule security_type -rwrule security_type -superuser security_type -anon
   user_ID
   ```

   了解更多信息 "正在创建导出规则。"

3. 验证现有导出的卷是否联机：

   ```
   volume show -vserver svm_name
   ```

重新挂载ONTAP卷或数据共享以进行NFS中继

要将非中继客户端连接转换为中继连接、必须卸载Linux和VMware客户端上的现有挂载、然后使用LIFs相关信息重新挂载。

了解相关信息 "支持的客户端"。

> 卸载VMware客户端会对数据存储库上的任何VM造成中断。另一种方法是、创建一个启用了中继的新数据存储库、然后使用*存储VMVMotion将VM从旧数据存储库移动到新数据存储库。有关详细信息、请参见VMware文档。

Linux客户端要求

如果使用9.16.1 9.161或更高版本以及Red Hat Enterprise Linux 8.7或更高版本(适用于RHEL 8)或9.2或更高版本(适用于RHEL 9)作为Linux客户端、则中继组只需要一个挂载点。使用以下选项、使用此命令挂载导出的卷 `trunkdiscovery`：

```
mount <lif_ip>:<volume_name> </mount_path> -o trunkdiscovery,vers=4.1
```

否则、中继组中的每个连接都需要一个单独的挂载点。使用选项、使用类似于以下内容的命令挂载导出的卷 `max_connect`：

```
mount <lif1_ip>:<volume_name> </mount_path1> -o vers=4.1,max_connect=16
```

```
mount <lif2_ip>:<volume_name> </mount_path2> -o vers=4.1,max_connect=16
```

版本 (`vers`)值应为 `4.1` 或更高版本。

。 `max_connect` 值对应于中继组中的连接数。

VMware客户端要求

需要使用mount语句、其中包含中继组中每个连接的IP地址。

使用类似以下内容的命令挂载导出的数据存储库：

```
#esxcli storage nfs41 -H lif1_ip, lif2_ip -s /mnt/sh are1 -v nfs41share
```

。 `-H` 值应与中继组中的连接相对应。

版权信息

版权所有 © 2026 NetApp, Inc.。保留所有权利。中国印刷。未经版权所有者事先书面许可，本文档中受版权保护的任何部分不得以任何形式或通过任何手段（图片、电子或机械方式，包括影印、录音、录像或存储在电子检索系统中）进行复制。

从受版权保护的 NetApp 资料派生的软件受以下许可和免责声明的约束：

本软件由 NetApp 按“原样”提供，不含任何明示或暗示担保，包括但不限于适销性以及针对特定用途的适用性的隐含担保，特此声明不承担任何责任。在任何情况下，对于因使用本软件而以任何方式造成的任何直接性、间接性、偶然性、特殊性、惩罚性或后果性损失（包括但不限于购买替代商品或服务；使用、数据或利润方面的损失；或者业务中断），无论原因如何以及基于何种责任理论，无论出于合同、严格责任或侵权行为（包括疏忽或其他行为），NetApp 均不承担责任，即使已被告知存在上述损失的可能性。

NetApp 保留在不另行通知的情况下随时对本文档所述的任何产品进行更改的权利。除非 NetApp 以书面形式明确同意，否则 NetApp 不承担因使用本文档所述产品而产生的任何责任或义务。使用或购买本产品不表示获得 NetApp 的任何专利权、商标权或任何其他知识产权许可。

本手册中描述的产品可能受一项或多项美国专利、外国专利或正在申请的专利的保护。

有限权利说明：政府使用、复制或公开本文档受 DFARS 252.227-7013（2014 年 2 月）和 FAR 52.227-19（2007 年 12 月）中“技术数据权利 — 非商用”条款第 (b)(3) 条规定的限制条件的约束。

本文档中所含数据与商业产品和/或商业服务（定义见 FAR 2.101）相关，属于 NetApp, Inc. 的专有信息。根据本协议提供的所有 NetApp 技术数据和计算机软件具有商业性质，并完全由私人出资开发。 美国政府对这些数据的使用权具有非排他性、全球性、受限且不可撤销的许可，该许可既不可转让，也不可再许可，但仅限在与交付数据所依据的美国政府合同有关且受合同支持的情况下使用。除本文档规定的情形外，未经 NetApp, Inc. 事先书面批准，不得使用、披露、复制、修改、操作或显示这些数据。美国政府对国防部的授权仅限于 DFARS 的第 252.227-7015(b)（2014 年 2 月）条款中明确的权利。

商标信息

NetApp、NetApp 标识和 http://www.netapp.com/TM 上所列的商标是 NetApp, Inc. 的商标。其他公司和产品名称可能是其各自所有者的商标。