网络管理
ONTAP 9

NetApp
April 24, 2024

目录

网络管理

入门

网络管理概述

您可以使用System Manager或命令行界面使用以下信息执行基本存储网络管理。您可以配置物理和虚拟网络端口（ VLAN 和接口组），使用 IPv4 和 IPv6 创建 LIF ，管理集群中的路由和主机解析服务，使用负载平衡优化网络流量以及使用 SNMP 监控集群。

除非另有说明、否则命令行界面过程适用于所有版本的ONTAP 9。

要了解每个ONTAP 9版本提供的网络功能的影响、请参见 "《 ONTAP 发行说明》"。

从 ONTAP 9.8 开始，您可以使用 System Manager 显示一个图形，其中显示了网络的组件和配置。从ONTAP 9.12开始、您可以在网络接口网格上查看LIF和子网关联。如果您使用的是经典System Manager (仅适用于ONTAP 9.7及更早版本)、请参见 "管理网络"。

通过新的网络可视化功能，用户可以在图形界面中查看主机，端口， SVM ，卷等之间的网络连接路径。

选择 * 网络 > 概述 * 或选择时，将显示此图 → 信息板的 * 网络 * 部分。

图中显示了以下组件类别：

- 主机
- 存储端口
- 网络接口
- Storage VM
- 数据访问组件

每个部分都显示了其他详细信息，您可以将鼠标悬停在这些详细信息上或选择执行网络管理和配置任务。

示例

以下是您可以通过多种方式与图形交互来查看每个组件的详细信息或启动操作来管理网络的一些示例：

- 单击某个主机可查看其配置：端口、网络接口、Storage VM以及与其关联的数据访问组件。
- 将鼠标悬停在 Storage VM 中的卷数上可选择一个卷以查看其详细信息。
- 选择一个 iSCSI 接口以查看其上周的性能。
- 单击 ⋮ 在组件旁边启动操作以修改该组件。
- 快速确定网络中可能出现的问题，这些问题由运行不正常的组件旁边的 "X" 指示。

System Manager 网络可视化视频

从**ONTAP 9.7x**或更早版本升级**ONTAP**后、请验证您的网络配置

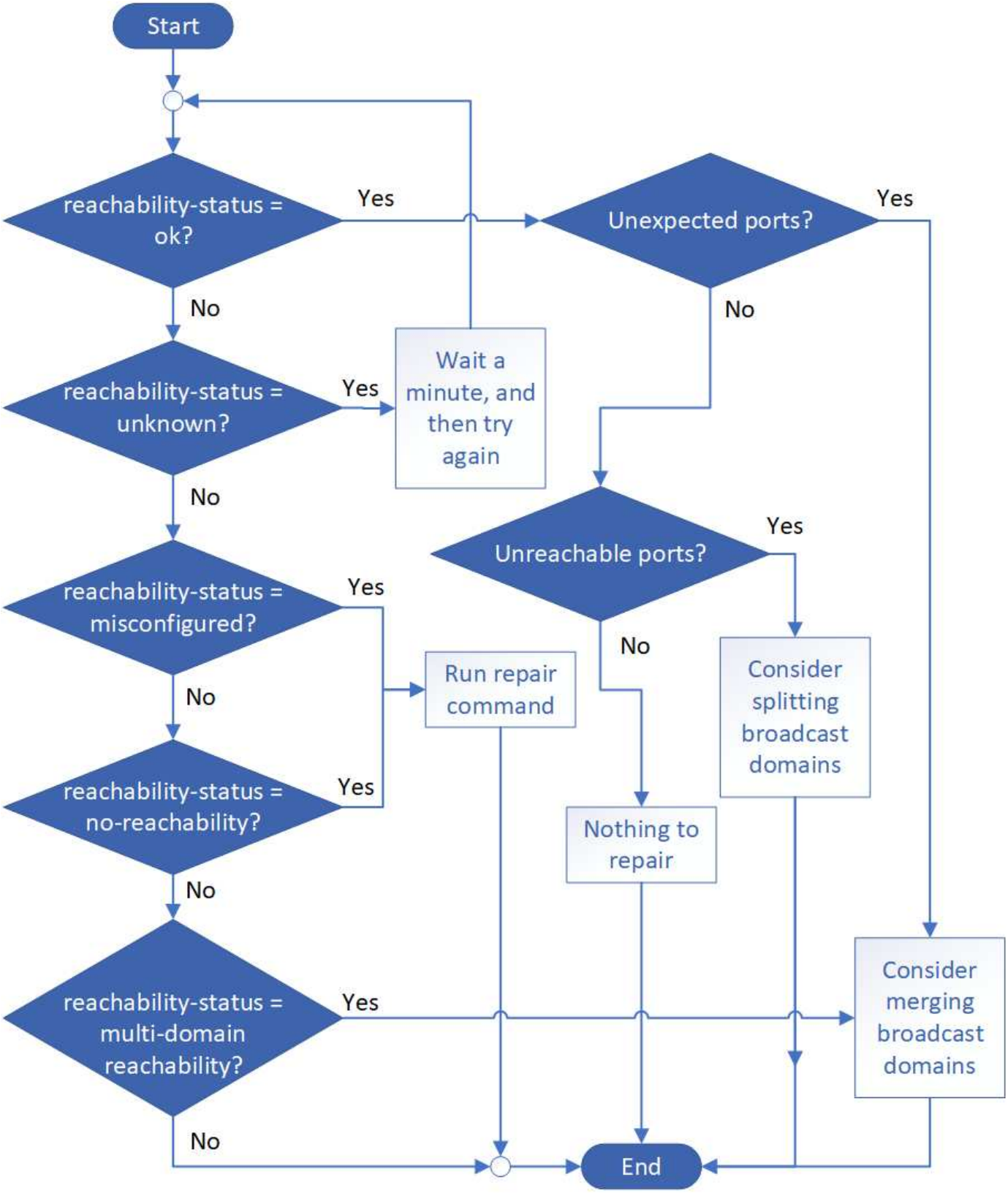
从ONTAP 9.7x或更早版本升级到ONTAP 9.8或更高版本后、您应验证网络配置。升级后，ONTAP 会自动监控第 2 层可访问性。

步骤

1. 验证每个端口是否可访问其预期广播域：

```
network port reachability show -detail
```

命令输出包含可访问性结果。使用以下决策树和表了解可访问性结果（可访问性状态），并确定下一步要执行的操作（如果有）。



可访问性状态	Description

确定	此端口可通过第 2 层访问其分配的广播域。 如果可访问性状态为 " 正常 " ，但存在 " 意外端口 " ，请考虑合并一个或多个广播域。有关详细信息，请参见 "合并广播域"。 如果可访问性状态为 " 正常 " ，但存在 " 无法访问的端口 " ，请考虑拆分一个或多个广播域。有关详细信息，请参见 "拆分广播域"。 如果可访问性状态为 " 正常 " ，并且没有意外或无法访问的端口，则表示您的配置正确。
配置不当的可访问性	此端口无法通过第 2 层访问其分配的广播域；但是，此端口确实可以通过第 2 层访问其他广播域。 您可以修复端口可访问性。运行以下命令时，系统会将此端口分配给其可访问性所在的广播域： `network port reachability repair -node -port` 有关详细信息，请参见 "修复端口可访问性"。
不可访问性	此端口无法通过第 2 层访问任何现有广播域。 您可以修复端口可访问性。运行以下命令时，系统会将此端口分配给默认 IP 空间中自动创建的新广播域： `network port reachability repair -node -port` 有关详细信息，请参见 "修复端口可访问性"。
多域可访问性	此端口可通过第 2 层访问其分配的广播域；但是，它也可通过第 2 层访问至少其他一个广播域。 检查物理连接和交换机配置以确定它是否不正确，或者端口分配的广播域是否需要与一个或多个广播域合并。 有关详细信息，请参见 "合并广播域" 或 "修复端口可访问性"。
未知	如果可访问性状态为 "unknown" ，请等待几分钟，然后重试此命令。

修复端口后，您需要检查并解决已替换的 LIF 和 VLAN 。如果端口属于某个接口组，则还需要了解该接口组发生了什么情况。 有关详细信息，请参见 "修复端口可访问性"。

网络组件

集群的网络组件概述

在设置集群之前，您应熟悉集群的网络组件。将集群的物理网络组件配置为逻辑组件可在

ONTAP 中提供灵活性和多租户功能。

集群中的各种网络组件如下所示：

- 物理端口

  网络接口卡（ NIC ）和主机总线适配器（ HBA ）提供从每个节点到物理网络（管理和数据网络）的物理（以太网和光纤通道）连接。

  有关站点要求，交换机信息，端口布线信息和控制器板载端口布线，请参见上的 Hardware Universe "hwu.netapp.com"。

- 逻辑端口

  虚拟局域网（ VLAN ）和接口组构成逻辑端口。接口组将多个物理端口视为一个端口，而 VLAN 则将一个物理端口细分为多个单独的端口。

- IP 空间

  您可以使用 IP 空间为集群中的每个 SVM 创建不同的 IP 地址空间。这样，在管理上独立的网络域中的客户端就可以访问集群数据，同时使用来自同一 IP 地址子网范围的重叠 IP 地址。

- 广播域

  广播域驻留在 IP 空间中，并包含一组网络端口，这些端口可能来自集群中的多个节点，这些端口属于同一个第 2 层网络。组中的端口用于 SVM 中的数据流量。

- Subnets

  子网是在广播域中创建的，其中包含属于同一第 3 层子网的 IP 地址池。此 IP 地址池可简化创建 LIF 期间的 IP 地址分配。

- 逻辑接口

  逻辑接口（ LIF ）是指与端口关联的 IP 地址或全球通用端口名称（ WWPN ）。它与故障转移组，故障转移规则和防火墙规则等属性相关联。LIF 通过当前绑定到的端口（物理或逻辑）通过网络进行通信。

  集群中不同类型的 LIF 包括数据 LIF ，集群范围的管理 LIF ，节点范围的管理 LIF ，集群间 LIF 和集群 LIF 。LIF 的所有权取决于 LIF 所在的 SVM 。数据 LIF 属于数据 SVM ，节点范围的管理 LIF ，集群范围的管理 LIF 和集群间 LIF 属于管理 SVM ，集群 LIF 属于集群 SVM 。

- DNS 区域

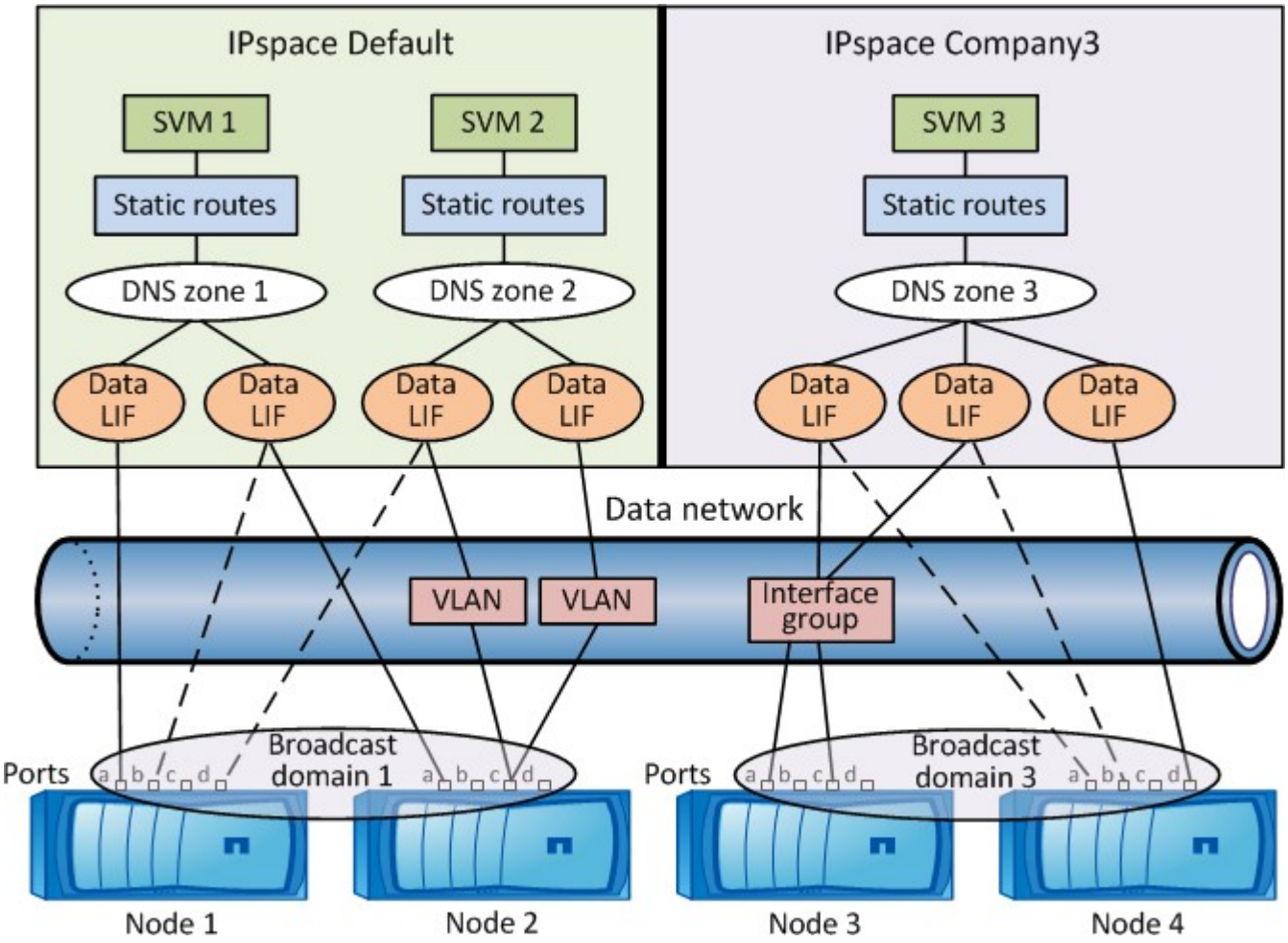
  可以在创建 LIF 期间指定 DNS 区域，从而为要通过集群的 DNS 服务器导出的 LIF 提供一个名称。多个 LIF 可以共享同一个名称，从而使 DNS 负载平衡功能可以根据负载为该名称分配 IP 地址。

  SVM 可以具有多个 DNS 区域。

- 路由

  每个 SVM 在网络连接方面均可自行使用。SVM 拥有可访问每个已配置外部服务器的 LIF 和路由。

  下图说明了不同的网络组件在四节点集群中的关联方式：

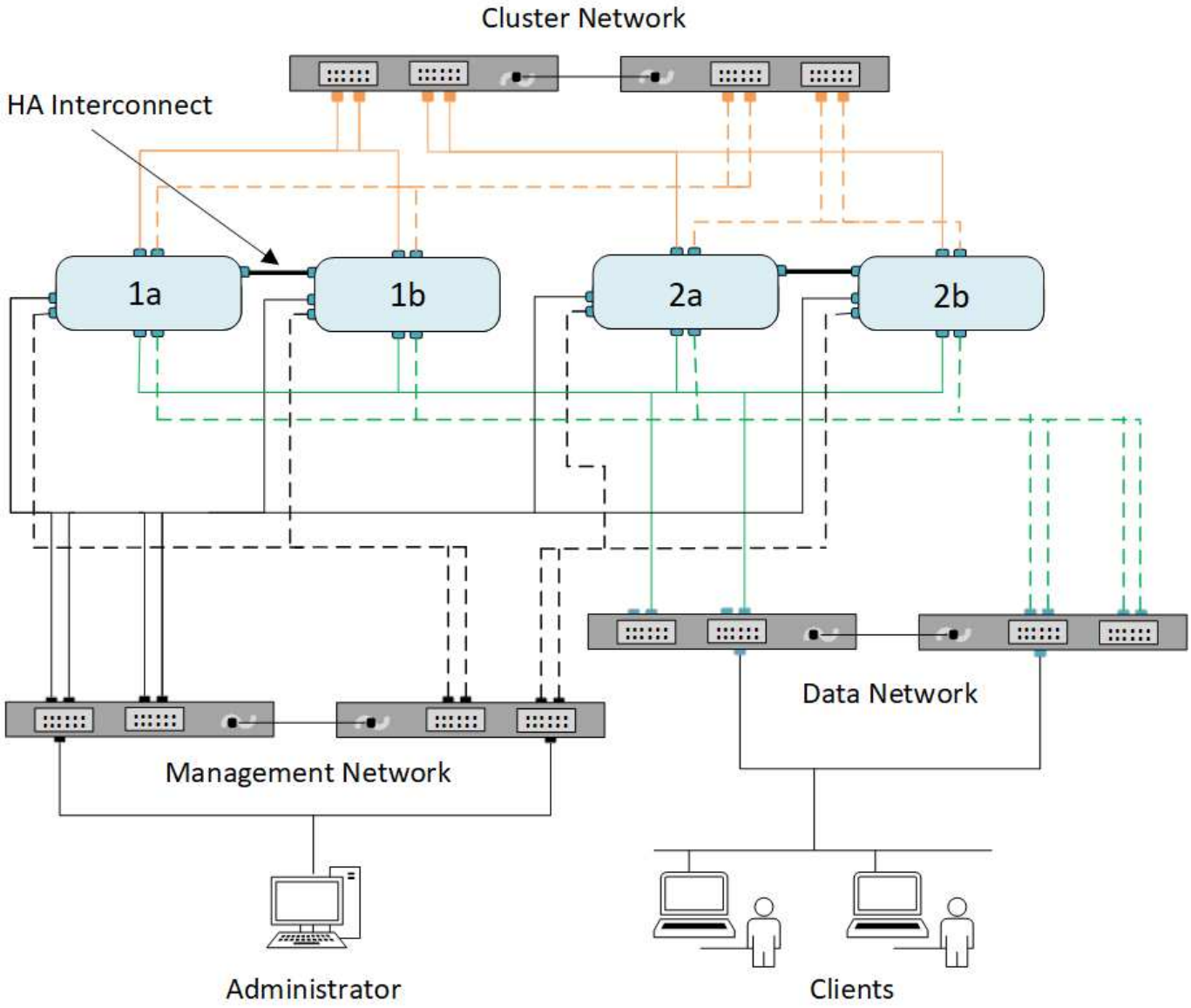


网络布线准则

网络布线最佳实践可将流量分隔到以下网络：集群，管理和数据。

您应该为集群布线，使集群流量与所有其他流量位于一个单独的网络上。将网络管理流量与数据和集群内流量分开是一种可选的做法，但建议这样做。通过维护单独的网络，您可以提高性能，简化管理，并提高对节点的安全性和管理访问。

下图显示了包含三个独立网络的四节点 HA 集群的网络布线：



在为网络连接布线时，应遵循以下特定准则：

- 每个节点应连接到三个不同的网络。

  一个网络用于管理，一个网络用于数据访问，一个网络用于集群内通信。管理网络和数据网络可以在逻辑上分开。

- 您可以为每个节点建立多个数据网络连接，以改善客户端（数据）流量。
- 可以在不连接数据网络的情况下创建集群，但集群必须包括集群互连连接。
- 每个节点应始终有两个或更多集群连接。

有关网络布线的详细信息，请参见 "AFF 和 FAS 系统文档中心" 和 "Hardware Universe"。

广播域，故障转移组和故障转移策略之间的关系

广播域，故障转移组和故障转移策略协同工作，以确定在配置了 LIF 的节点或端口发生故

障时哪个端口将接管。

广播域列出了同一第 2 层以太网网络中可访问的所有端口。广播域中的所有其他端口都会看到从其中一个端口发送的以太网广播数据包。广播域的这种可访问性特征对于 LIF 非常重要，因为如果 LIF 要故障转移到广播域中的任何其他端口，它仍可访问从原始端口访问的每个本地和远程主机。

故障转移组用于定义广播域中彼此提供 LIF 故障转移覆盖的端口。每个广播域都有一个故障转移组，该故障转移组包含其所有端口。包含广播域中所有端口的此故障转移组是 LIF 的默认和建议故障转移组。您可以使用定义的较小子集创建故障转移组，例如，广播域中链路速度相同的故障转移端口组。

故障转移策略用于指示在节点或端口发生故障时 LIF 如何使用故障转移组的端口。将故障转移策略视为一种应用于故障转移组的筛选器。LIF （ LIF 可以故障转移到的一组端口）的故障转移目标是通过将 LIF 的故障转移策略应用于广播域中 LIF 的故障转移组来确定的。

您可以使用以下命令行界面命令查看 LIF 的故障转移目标：

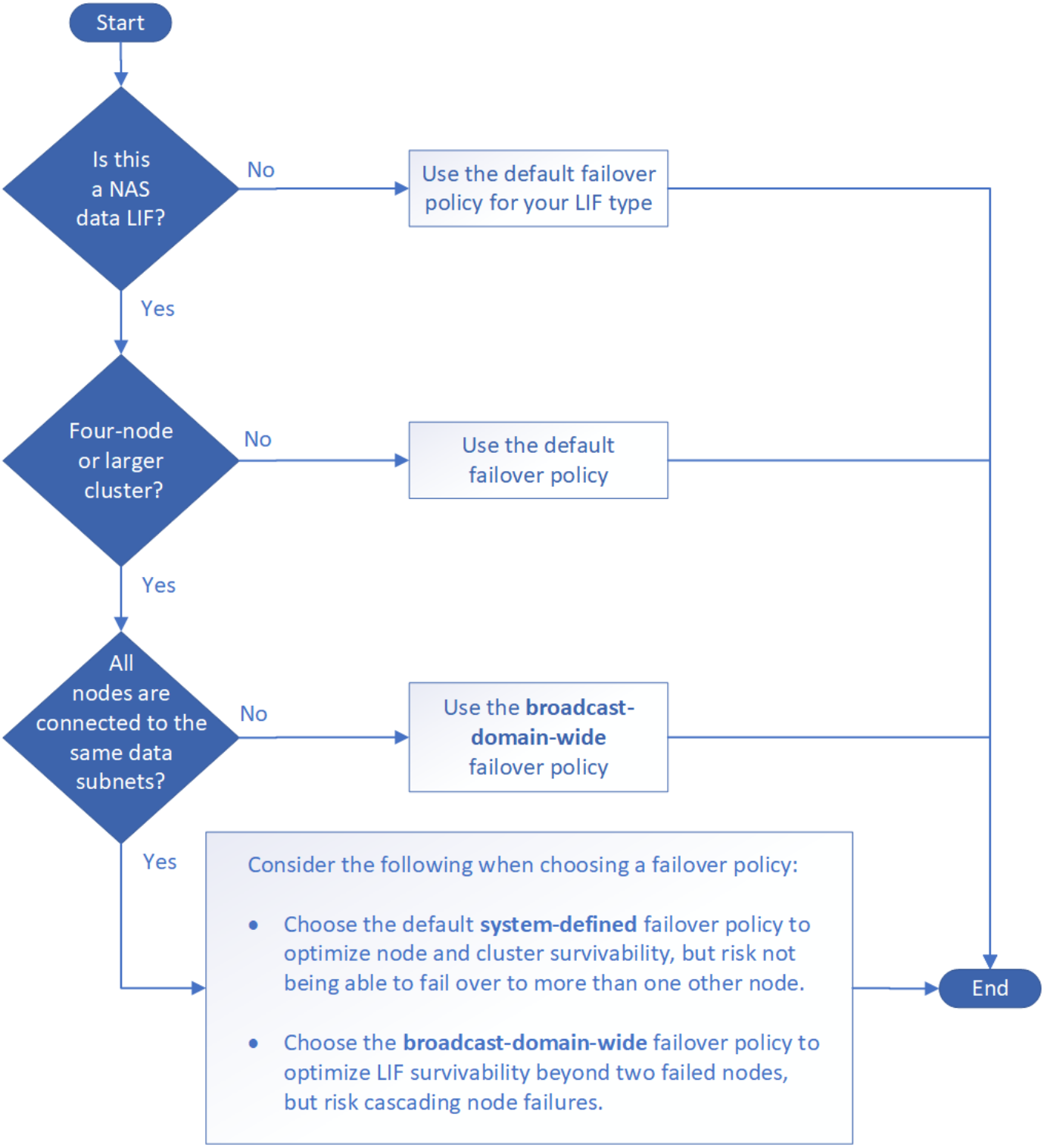
```
network interface show -failover
```

NetApp 强烈建议对您的 LIF 类型使用默认故障转移策略。

确定要使用的 **LIF** 故障转移策略

确定是否使用建议的默认故障转移策略，或者是否根据您的 LIF 类型和环境对其进行更改。

故障转移策略决策树



按 **LIF** 类型显示的默认故障转移策略

LIF类型	默认故障转移策略	Description
BGP LIF	已禁用	LIF 不会故障转移到其他端口。
集群 LIF	仅限本地	LIF 仅故障转移到同一节点上的端口。
集群管理 LIF	广播域范围	LIF 故障转移到集群中任意节点上同一广播域中的端口。

集群间 LIFs	仅限本地	LIF 仅故障转移到同一节点上的端口。
NAS 数据 LIF	系统定义的	LIF 故障转移到不是 HA 配对节点的另一个节点。
节点管理 LIFs	仅限本地	LIF 仅故障转移到同一节点上的端口。
SAN 数据 LIF	已禁用	LIF 不会故障转移到其他端口。

"仅SFO配对节点"故障转移策略不是默认策略、但当您希望LIF故障转移到主节点上的端口或仅SFO配对节点上的端口时、可以使用此策略。

NAS路径故障转移工作流(ONTAP 9.8及更高版本)

关于NAS路径故障转移(ONTAP 9.8及更高版本)

此工作流将指导您完成为 ONTAP 9.8 及更高版本设置 NAS 路径故障转移的网络配置步骤。此工作流假定满足以下条件：

- 您希望在简化网络配置的工作流中使用 NAS 路径故障转移最佳实践。
- 您希望使用命令行界面，而不是 System Manager 。
- 您正在运行 ONTAP 9.8 或更高版本的新系统上配置网络连接。

如果您运行的 ONTAP 版本早于 9.8 ，则应使用以下适用于 ONTAP 9.0 到 9.7 的 NAS 路径故障转移操作步骤：

- "ONTAP 9.1-9.7 NAS 路径故障转移工作流"

如果您需要网络管理详细信息，应使用网络管理参考资料：

- 网络管理概述

工作流(ONTAP 9.8及更高版本)

如果您已经熟悉基本网络概念，则可以通过查看 NAS 路径故障转移配置的 " 实践 " 工作流来节省网络设置时间。

在 NAS LIF 的当前端口出现链路故障后，该 LIF 会自动迁移到正常运行的网络端口。您可以依靠 ONTAP 默认值来管理路径故障转移。

SAN LIF 不会迁移（除非您在链路出现故障后手动移动）。相反，主机上的多路径技术会将流量转移到其他 LIF 。有关详细信息，请参见 "SAN 管理"。

1. "填写工作表"

使用工作表规划NAS路径故障转移。

2 "创建 IP 空间"

为集群中的每个SVM创建一个不同的IP地址空间。

3 "将广播域移动到 IP 空间"

将广播域移动到IP空间。

4 "创建 SVM"

创建SVM以向客户端提供数据。

5 "创建 LIF"

在要用于访问数据的端口上创建SIFs。

6 "为SVM配置DNS服务"

在创建NFS或SMB服务器之前、为SVM配置DNS服务。

NAS路径故障转移配置工作表(ONTAP 9.8及更高版本)

在配置 NAS 路径故障转移之前，您应完成工作表的所有部分。

IPspace 配置

您可以使用 IP 空间为集群中的每个 SVM 创建不同的 IP 地址空间。这样，在管理上独立的网络域中的客户端就可以访问集群数据，同时使用来自同一 IP 地址子网范围的重叠 IP 地址。

信息	是否必需?	您的价值
IPspace 名称 IP空间的唯一标识符。	是的。	

广播域配置

广播域对属于同一第 2 层网络的端口进行分组，并为广播域端口设置 MTU 。

广播域将分配给 IP 空间。一个 IP 空间可以包含一个或多个广播域。

> LIF 故障转移到的端口必须是 LIF 故障转移组的成员。对于 ONTAP 创建的每个广播域，还会创建一个同名的故障转移组，其中包含广播域中的所有端口。

信息	是否必需?	您的价值

IPspace 名称 将广播域分配到的 IP 空间。 此 IP 空间必须存在。	是的。	
广播域名 广播域的名称。 此名称在 IP 空间中必须是唯一的。	是的。	
MTU 广播域的最大传输单元值，通常设置为*1500*或*9000*。 MTU 值将应用于广播域中的所有端口以及稍后添加到广播域的任何端口。 MTU值应与连接到该网络的所有设备匹配。请注意、e0M端口处理管理和服务处理器流量的MTU应设置为不超过1500字节。	是的。	
端口 端口会根据可访问情况分配给广播域。端口分配完成后、运行以检查可访问性 `network port reachability show` 命令： 这些端口可以是物理端口， VLAN 或接口组。	是的。	

子网配置

子网包含 IP 地址池和一个默认网关，可将其分配给 IP 空间中的 SVM 所使用的 LIF 。

- 在 SVM 上创建 LIF 时，您可以指定子网的名称，而不是提供 IP 地址和子网。
- 由于子网可以使用默认网关进行配置，因此在创建 SVM 时，不必单独创建默认网关。
- 广播域可以包含一个或多个子网。
- 您可以通过将多个子网与 IP 空间的广播域关联来配置位于不同子网上的 SVM LIF 。
- 每个子网都必须包含不与分配给同一 IP 空间中其他子网的 IP 地址重叠的 IP 地址。
- 您可以为 SVM 数据 LIF 分配特定的 IP 地址，并为 SVM 创建默认网关，而不是使用子网。

信息	是否必需?	您的价值
IPspace 名称 子网将分配到的 IP 空间。 此 IP 空间必须存在。	是的。	

Subnet name 子网的名称。 此名称在 IP 空间中必须是唯一的。	是的。	
广播域名 子网将分配到的广播域。 此广播域必须驻留在指定的 IP 空间中。	是的。	
子网名称和掩码 IP 地址所在的子网和掩码。	是的。	
网关 您可以为子网指定默认网关。 如果在创建子网时未分配网关，则可以稍后分配一个网关。	否	
IP 地址范围 您可以指定 IP 地址范围或特定 IP 地址。 例如，您可以指定一个范围，例如： `192.168.1.1-192.168.1.100, 192.168.1.112, 192.168.1.145` 如果未指定 IP 地址范围，则指定子网中的整个 IP 地址范围可分配给 LIF 。	否	
强制更新 LIF 关联 指定是否强制更新现有 LIF 关联。 默认情况下，如果任何服务处理器接口或网络接口使用提供范围内的 IP 地址，则子网创建将失败。 使用此参数可将任何手动寻址的接口与子网相关联，并使命令成功执行。	否	

SVM配置

您可以使用 SVM 为客户端和主机提供数据。

您记录的值用于创建默认数据 SVM 。如果要创建 MetroCluster 源 SVM ，请参见 "《光纤连接的 MetroCluster 安装和配置指南》" 或 "《延伸型 MetroCluster 安装和配置指南》"。

信息	是否必需?	您的价值

SVM name SVM的完全限定域名(FQDN)。 此名称在集群联盟中必须是唯一的。	是的。	
根卷名称 SVM 根卷的名称。	是的。	
Aggregate name 保存 SVM 根卷的聚合的名称。 此聚合必须存在。	是的。	
安全风格 SVM 根卷的安全模式。 可能的值包括 * NTFS * ， * UNIX * 和 * 混合 * 。	是的。	
IPspace 名称 SVM 分配到的 IP 空间。 此 IP 空间必须存在。	否	
SVM 语言设置 SVM 及其卷使用的默认语言。 如果未指定默认语言，则默认 SVM 语言将设置为 * 。 C.UTF-8 * 。 SVM 语言设置用于确定用于显示 SVM 中所有 NAS 卷的文件名和数据的字符集。 您可以在创建 SVM 后修改此语言。	否	

LIF配置

SVM 通过一个或多个网络逻辑接口（ LIF ）向客户端和主机提供数据。

信息	是否必需?	您的价值
SVM name LIF 的 SVM 名称。	是的。	

LIF 名称 LIF的名称。 您可以为每个节点分配多个数据 LIF ，并且可以为集群中的任何节点分配 LIF ，前提是该节点具有可用的数据端口。 要提供冗余，应为每个数据子网至少创建两个数据 LIF ，并为分配给特定子网的 LIF 分配不同节点上的主端口。 * 重要说明： * 如果要将 SMB 服务器配置为通过 SMB 托管 Hyper-V 或 SQL Server 以实现无中断运行解决方案，则 SVM 必须在集群中的每个节点上至少具有一个数据 LIF 。	是的。	
服务策略 LIF的服务策略。 服务策略定义了哪些网络服务可以使用 LIF 。内置服务和服务策略可用于管理数据和系统 SVM 上的数据和管理流量。	是的。	
允许的协议 基于IP的生命周期管理不需要支持的协议、请改用服务策略行。 为 FibreChannel 端口上的 SAN LIF 指定允许的协议。这些协议可以使用该 LIF 。创建 LIF 后，无法修改使用 LIF 的协议。配置 LIF 时，应指定所有协议。	否	
Home node 将 LIF 还原到其主端口时 LIF 返回到的节点。 您应为每个数据 LIF 记录一个主节点。	是的。	
主端口或广播域 选择以下选项之一： **Port**：指定将LIF还原到其主端口时逻辑接口返回到的端口。只有 IP 空间子网中的第一个 LIF 才会执行此操作，否则不需要执行此操作。 * 广播域 * ：指定广播域，系统将选择在将 LIF 还原到其主端口时逻辑接口返回到的相应端口。	是的。	
Subnet name 要分配给 SVM 的子网。 用于创建与应用程序服务器的持续可用 SMB 连接的所有数据 LIF 必须位于同一子网中。	是（如果使用子网）	

DNS配置

在创建 NFS 或 SMB 服务器之前，必须在 SVM 上配置 DNS 。

信息	是否必需?	您的价值
SVM name 要在其中创建 NFS 或 SMB 服务器的 SVM 的名称。	是的。	
DNS domain name 执行主机到 IP 名称解析时要附加到主机名的域名列表。 首先列出本地域，然后列出最常进行 DNS 查询的域名。	是的。	
DNS服务器的IP地址 要为NFS或SMB服务器提供名称解析的DNS服务器的IP地址列表。 列出的DNS服务器必须包含为SMB服务器将加入的域查找Active Directory LDAP服务器和域控制器所需的服务位置记录(SRV)。 SRV 记录用于将服务名称映射到提供该服务的服务器的 DNS 计算机名称。如果 ONTAP 无法通过本地 DNS 查询获取服务位置记录，则 SMB 服务器创建将失败。 确保 ONTAP 可以找到 Active Directory SRV 记录的最简单方法是将 Active Directory 集成的 DNS 服务器配置为 SVM DNS 服务器。 您可以使用非 Active Directory 集成的 DNS 服务器，前提是 DNS 管理员已手动将 SRV 记录添加到包含 Active Directory 域控制器信息的 DNS 区域。 有关 Active Directory 集成的 SRV 记录的信息，请参见主题 "Microsoft TechNet 上适用于 Active Directory 的 DNS 支持的工作原理"。	是的。	

动态 **DNS** 配置

在使用动态 DNS 自动向 Active Directory 集成的 DNS 服务器添加 DNS 条目之前，必须在 SVM 上配置动态 DNS （ DDNS ）。

系统会为 SVM 上的每个数据 LIF 创建 DNS 记录。通过在 SVM 上创建多个数据 LIF ，您可以对客户端与分配的数据 IP 地址的连接进行负载平衡。DNS 以轮循方式对使用主机名与分配的 IP 地址建立的连接进行负载平衡。

信息	是否必需?	您的价值
SVM name 要在其中创建 NFS 或 SMB 服务器的 SVM 。	是的。	

是否使用 DDNS 指定是否使用 DDNS 。 SVM 上配置的 DNS 服务器必须支持 DDNS 。默认情况下， DDNS 处于禁用状态。	是的。	
是否使用安全 DDNS 只有 Active Directory 集成的 DNS 才支持安全 DDNS 。 如果 Active Directory 集成的 DNS 仅允许安全 DDNS 更新，则此参数的值必须为 true 。 默认情况下，安全 DDNS 处于禁用状态。 只有在为 SVM 创建 SMB 服务器或 Active Directory 帐户后，才能启用安全 DDNS 。	否	
DNS 域的 FQDN DNS 域的 FQDN 。 您必须使用为 SVM 上的 DNS 名称服务配置的相同域名。	否	

NAS路径故障转移工作流(ONTAP 9.7及更早版本)

设置NAS路径故障转移(ONTAP 9.7及更早版本)

此工作流将指导您完成为 ONTAP 9.0 - 9.7 设置 NAS 路径故障转移的网络配置步骤。此工作流假定满足以下条件：

- 您希望使用 NAS 路径故障转移最佳实践来简化网络配置。
- 您希望使用命令行界面，而不是 System Manager 。
- 您正在运行 ONTAP 9.0 到 9.7 的新系统上配置网络连接。

如果您运行的 ONTAP 版本高于 9.7 ，则应使用适用于 ONTAP 9.8 或更高版本的 NAS 路径故障转移操作步骤：

- ONTAP 9.8 及更高版本的 NAS 路径故障转移工作流

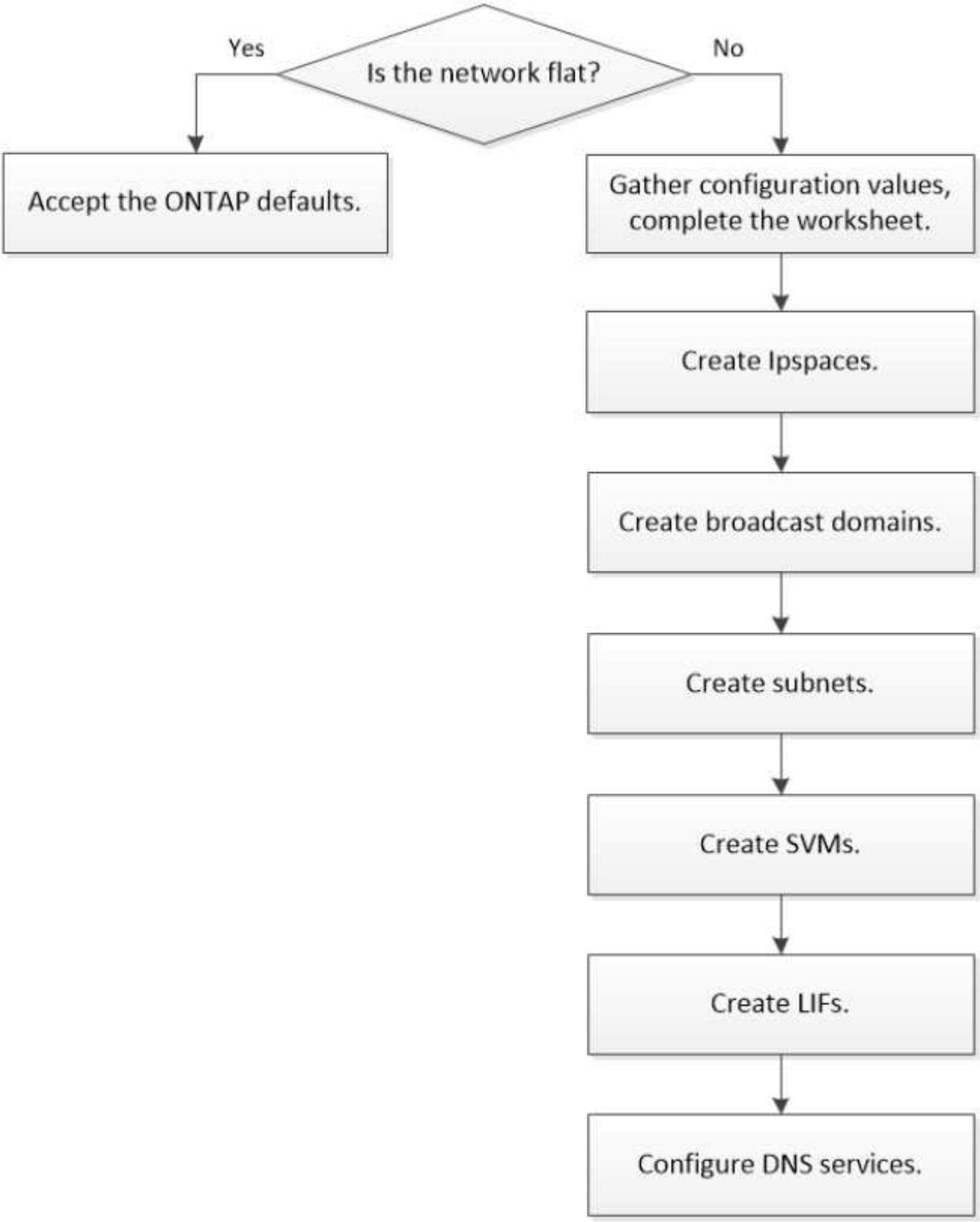
如果您需要有关网络组件和管理的详细信息，应使用网络管理参考资料：

- 网络管理概述

工作流(ONTAP 9.7及更早版本)

如果您已经熟悉基本网络概念，则可以通过查看 NAS 路径故障转移配置的 " 实践 " 工作流来节省网络设置时间。

在 NAS LIF 的当前端口出现链路故障后，该 LIF 会自动迁移到正常运行的网络端口。如果您的网络正常运行，则可以依靠 ONTAP 默认值来管理路径故障转移。否则，您应按照此工作流中的步骤配置路径故障转移。



SAN LIF 不会迁移（除非您在链路出现故障后手动移动）。相反，主机上的多路径技术会将流量转移到其他 LIF 。有关详细信息，请参见 "SAN 管理"。

1. "填写工作表"

使用工作表规划NAS路径故障转移。

2 "创建 IP 空间"

为集群中的每个SVM创建一个不同的IP地址空间。

3 "创建广播域"

创建广播域。

4 "创建子网"

创建子网。

5 "创建 SVM"

创建SVM以向客户端提供数据。

6 "创建 LIF"

在要用于访问数据的端口上创建SIFs。

7 "为SVM配置DNS服务"

在创建NFS或SMB服务器之前、为SVM配置DNS服务。

NAS路径故障转移配置工作表(ONTAP 9.7及更早版本)

在配置 NAS 路径故障转移之前，您应完成工作表的所有部分。

IPspace 配置

您可以使用 IP 空间为集群中的每个 SVM 创建不同的 IP 地址空间。这样，在管理上独立的网络域中的客户端就可以访问集群数据，同时使用来自同一 IP 地址子网范围的重叠 IP 地址。

信息	是否必需?	您的价值
IPspace 名称 • IP 空间的名称。 • 此名称在集群中必须是唯一的。	是的。	

广播域配置

广播域对属于同一第 2 层网络的端口进行分组，并为广播域端口设置 MTU 。

广播域将分配给 IP 空间。一个 IP 空间可以包含一个或多个广播域。

> LIF 故障转移到的端口必须是 LIF 故障转移组的成员。创建广播域时， ONTAP 会自动创建同名的故障转移组。故障转移组包含分配给广播域的所有端口。

信息	是否必需?	您的价值
IPspace 名称 • 将广播域分配到的 IP 空间。 • IP 空间必须存在。	是的。	
广播域名 • 广播域的名称。 • 此名称在 IP 空间中必须是唯一的。	是的。	
MTU • 广播域的 MTU 。 • 通常设置为* 1500 或 9000 *。 • MTU 值将应用于广播域中的所有端口以及稍后添加到广播域的任何端口。 MTU值应与连接到该网络的所有设备匹配。请注意、e0M端口处理管理和服务处理器流量的MTU应设置为不超过1500字节。	是的。	
端口 • 要添加到广播域的网络端口。 • 分配给广播域的端口可以是物理端口， VLAN 或接口组（ ifgroups ）。 • 如果某个端口位于另一个广播域中，则必须先将其删除，然后才能将其添加到广播域。 • 通过指定节点名称和端口来分配端口：例如 node1： e0d 。	是的。	

子网配置

子网包含 IP 地址池和一个默认网关，可将其分配给 IP 空间中的 SVM 所使用的 LIF 。

- 在 SVM 上创建 LIF 时，您可以指定子网的名称，而不是提供 IP 地址和子网。
- 由于子网可以使用默认网关进行配置，因此在创建 SVM 时，不必单独创建默认网关。
- 广播域可以包含一个或多个子网。
  您可以通过将多个子网与 IP 空间的广播域关联来配置位于不同子网上的 SVM LIF 。
- 每个子网都必须包含不与分配给同一 IP 空间中其他子网的 IP 地址重叠的 IP 地址。
- 您可以为 SVM 数据 LIF 分配特定的 IP 地址，并为 SVM 创建默认网关，而不是使用子网。

信息	是否必需?	您的价值
IPspace 名称 • 子网将分配到的 IP 空间。 • IP 空间必须存在。	是的。	
Subnet name • 子网的名称。 • 此名称在 IP 空间中必须是唯一的。	是的。	
广播域名 • 子网将分配到的广播域。 • 广播域必须驻留在指定的 IP 空间中。	是的。	
子网名称和掩码 • IP 地址所在的子网和掩码。	是的。	
网关 • 您可以为子网指定默认网关。 • 如果在创建子网时未分配网关，则可以随时为子网分配一个网关。	否	

IP 地址范围
 	
• 您可以指定 IP 地址范围或特定 IP 地址。
例如，您可以指定一个范围，例如：
`192.168.1.1-192.168.1.100,`
`192.168.1.112,`
`192.168.1.145`
 	
• 如果未指定 IP 地址范围，则指定子网中的整个 IP 地址范围可分配给 LIF 。
	否	

强制更新 LIF 关联 • 指定是否强制更新现有 LIF 关联。 • 默认情况下，如果任何服务处理器接口或网络接口使用提供范围内的 IP 地址，则子网创建将失败。 • 使用此参数可将任何手动寻址的接口与子网相关联，并使命令成功执行。	否	

SVM配置

您可以使用 SVM 为客户端和主机提供数据。

您记录的值用于创建默认数据 SVM 。如果要创建 MetroCluster 源 SVM ，请参见 "安装光纤连接的MetroCluster" 或 "安装延伸型MetroCluster"。

信息	是否必需?	您的价值
SVM name • SVM 的名称。 • 您应使用完全限定域名（FQDN），以确保 SVM 名称在集群联盟中是唯一的。	是的。	
根卷名称 • SVM 根卷的名称。	是的。	

Aggregate name • 保存 SVM 根卷的聚合的名称。 • 此聚合必须存在。	是的。	
安全风格 • SVM 根卷的安全模式。 • 可能的值包括 * NTFS * ， * UNIX * 和 * 混合 * 。	是的。	
IPspace 名称 • SVM 分配到的 IP 空间。 • 此 IP 空间必须存在。	否	
SVM 语言设置 • SVM 及其卷使用的默认语言。 • 如果未指定默认语言，则默认 SVM 语言将设置为 * 。 C.UTF-8 * 。 • SVM 语言设置用于确定用于显示 SVM 中所有 NAS 卷的文件名和数据的字符集。 您可以在创建 SVM 后修改此语言。	否	

LIF配置

SVM 通过一个或多个网络逻辑接口（ LIF ）向客户端和主机提供数据。

信息	是否必需?	您的价值
SVM name • LIF 的 SVM 名称。	是的。	

LIF 名称 • LIF的名称。 • 您可以为每个节点分配多个数据 LIF ，并且可以为集群中的任何节点分配 LIF ，前提是该节点具有可用的数据端口。 • 要提供冗余，应为每个数据子网至少创建两个数据 LIF ，并为分配给特定子网的 LIF 分配不同节点上的主端口。 • 重要说明： * 如果要将 SMB 服务器配置为通过 SMB 托管 Hyper-V 或 SQL Server 以实现无中断运行解决方案，则 SVM 必须在集群中的每个节点上至少具有一个数据 LIF 。	是的。	
LIF 角色 • LIF 的角色。 • 数据 LIF 分配有数据角色。	是的。 从ONTAP 9.6中弃用	数据
服务策略 LIF的服务策略。 服务策略定义了哪些网络服务可以使用 LIF 。内置服务和服务策略可用于管理数据和系统 SVM 上的数据和管理流量。	是的。 从ONTAP 9.6开始	
允许的协议 • 可使用 LIF 的协议。 • 默认情况下，允许 SMB ， NFS 和 FlexCache 。 通过 FlexCache 协议，可以在运行 7- 模式 Data ONTAP 的系统上将卷用作 FlexCache 卷的初始卷。 创建 LIF 后，无法修改使用 LIF 的协议。配置 LIF 时，应指定所有协议。	否	

Home node • 将 LIF 还原到其主端口时 LIF 返回到的节点。 • 您应为每个数据 LIF 记录一个主节点。	是的。	
主端口或广播域 • 将 LIF 还原到其主端口时逻辑接口返回到的端口。 • 您应为每个数据 LIF 记录一个主端口。	是的。	
Subnet name • 要分配给 SVM 的子网。 • 用于创建与应用程序服务器的持续可用 SMB 连接的所有数据 LIF 必须位于同一子网中。	是（如果使用子网）	

DNS配置

在创建 NFS 或 SMB 服务器之前，必须在 SVM 上配置 DNS 。

信息	是否必需?	您的价值
SVM name • 要在其中创建 NFS 或 SMB 服务器的 SVM 的名称。	是的。	
DNS domain name • 执行主机到 IP 名称解析时要附加到主机名的域名列表。 • 首先列出本地域，然后列出最常进行 DNS 查询的域名。	是的。	

DNS服务器的IP地址 • 要为NFS或SMB服务器提供名称解析的DNS服务器的IP地址列表。 • 列出的DNS服务器必须包含为SMB服务器将加入的域查找Active Directory LDAP服务器和域控制器所需的服务位置记录(SRV)。 SRV 记录用于将服务名称映射到提供该服务的服务器的 DNS 计算机名称。如果 ONTAP 无法通过本地 DNS 查询获取服务位置记录，则 SMB 服务器创建将失败。 确保 ONTAP 可以找到 Active Directory SRV 记录的最简单方法是将 Active Directory 集成的 DNS 服务器配置为 SVM DNS 服务器。 您可以使用非 Active Directory 集成的 DNS 服务器，前提是 DNS 管理员已手动将 SRV 记录添加到包含 Active Directory 域控制器信息的 DNS 区域。 • 有关 Active Directory 集成的 SRV 记录的信息，请参见主题 "Microsoft TechNet 上适用于 Active Directory 的 DNS 支持的工作原理"。	是的。	

动态 **DNS** 配置

在使用动态 DNS 自动向 Active Directory 集成的 DNS 服务器添加 DNS 条目之前，必须在 SVM 上配置动态 DNS （ DDNS ）。

系统会为 SVM 上的每个数据 LIF 创建 DNS 记录。通过在 SVM 上创建多个数据 LIF ，您可以对客户端与分配的数据 IP 地址的连接进行负载平衡。DNS 以轮循方式对使用主机名与分配的 IP 地址建立的连接进行负载平衡。

信息	是否必需?	您的价值
SVM name • 要在其中创建 NFS 或 SMB 服务器的 SVM 。	是的。	

是否使用 DDNS • 指定是否使用 DDNS 。 • SVM 上配置的 DNS 服务器必须支持 DDNS 。默认情况下，DDNS 处于禁用状态。	是的。	
是否使用安全 DDNS • 只有 Active Directory 集成的 DNS 才支持安全 DDNS 。 • 如果 Active Directory 集成的 DNS 仅允许安全 DDNS 更新，则此参数的值必须为 true 。 • 默认情况下，安全 DDNS 处于禁用状态。 • 只有在为 SVM 创建 SMB 服务器或 Active Directory 帐户后，才能启用安全 DDNS 。	否	
DNS 域的 FQDN • DNS 域的 FQDN 。 • 您必须使用为 SVM 上的 DNS 名称服务配置的相同域名。	否	

网络端口

配置网络端口概述

端口可以是物理端口（ NIC ），也可以是虚拟化端口，例如接口组或 VLAN 。

虚拟局域网（ VLAN ）和接口组构成虚拟端口。接口组将多个物理端口视为一个端口，而 VLAN 则将一个物理端口细分为多个单独的逻辑端口。

- 物理端口：可以直接在物理端口上配置 LIF 。
- 接口组：一个端口聚合，其中包含两个或更多物理端口，用作单个中继端口。接口组可以是单模式，多模式或动态多模式。
- VLAN ：一种逻辑端口，用于接收和发送带有 VLAN 标记（ IEEE 802.1Q 标准）的流量。VLAN 端口特征包括端口的 VLAN ID 。底层物理端口或接口组端口被视为 VLAN 中继端口，必须将连接的交换机端口配置为对 VLAN ID 进行中继。

  VLAN 端口的底层物理端口或接口组端口可以继续托管 LIF ，从而传输和接收未标记的流量。

- 虚拟 IP （ VIP ）端口：用作 VIP LIF 主端口的逻辑端口。VIP 端口由系统自动创建，仅支持有限数量的操作。从 ONTAP 9.5 开始，支持 VIP 端口。

端口命名约定为 *enumberletter*：

- 第一个字符用于描述端口类型。
  "e" 表示以太网。
- 第二个字符表示端口适配器所在的编号插槽。
- 第三个字符表示端口在多端口适配器上的位置。
  "a" 表示第一个端口， "b" 表示第二个端口，依此类推。

例如： `e0b` 表示以太网端口是节点主板上的第二个端口。

VLAN必须使用语法进行命名 `port_name-vlan-id`。

`port_name` 指定物理端口或接口组。

`vlan-id` 指定网络上的VLAN标识。例如： `e1c-80` 是有效的VLAN名称。

配置网络端口

将物理端口组合在一起以创建接口组

接口组也称为链路聚合组(Link Aggregation Group、LAG)、它是通过将同一节点上的两个或更多物理端口组合为一个逻辑端口来创建的。逻辑端口可提高故障恢复能力，提高可用性并实现负载共享。

接口组类型

存储系统支持三种类型的接口组：单模式，静态多模式和动态多模式。每个接口组提供不同级别的容错。多模式接口组提供了对网络流量进行负载平衡的方法。

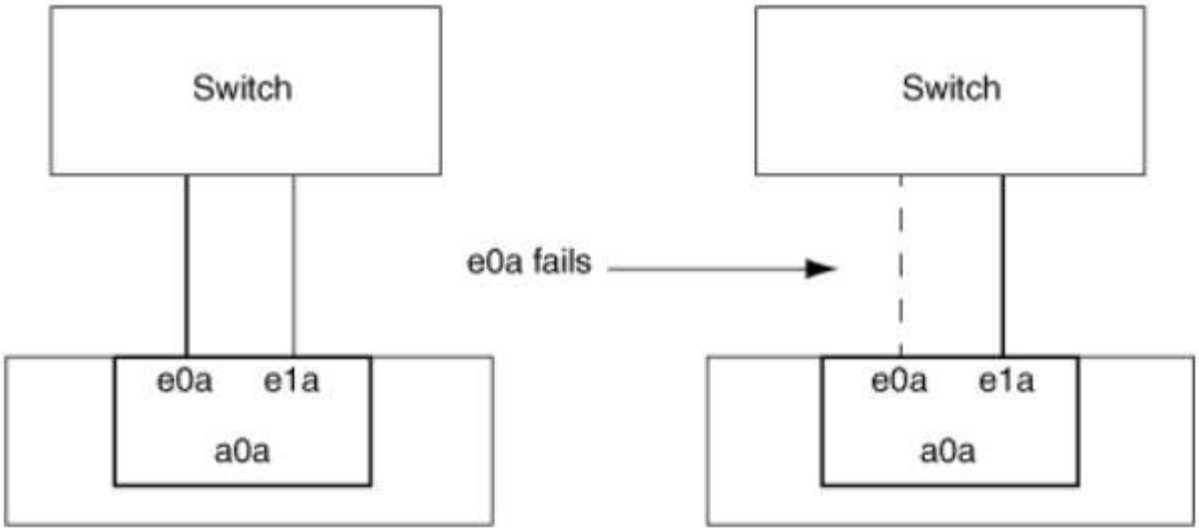
单模式接口组的特征

在单模式接口组中，该接口组中只有一个接口处于活动状态。其他接口处于备用状态，可在活动接口发生故障时接管。

单模式接口组的特征：

- 对于故障转移，集群会监控主动链路并控制故障转移。
  由于集群监控活动链路，因此不需要配置交换机。
- 一个单模式接口组中可以有多个接口处于备用状态。
- 如果单模式接口组跨越多个交换机，则必须使用交换机间链路（ ISL ）连接这些交换机。
- 对于单模式接口组，交换机端口必须位于同一广播域中。
- 源地址为 0.0.0.0 的链路监控 ARP 数据包将通过端口发送，以验证端口是否位于同一广播域中。

下图是单模式接口组的示例。在图中， e0a 和 e1a 属于 a0a 单模式接口组。如果活动接口 e0a 发生故障，备用 e1a 接口将接管并保持与交换机的连接。



> 要实现单模式功能，建议改用故障转移组。通过使用故障转移组，第二个端口仍可用于其他 LIF ，无需保持未使用状态。此外，故障转移组可以跨越两个以上的端口，也可以跨越多个节点上的端口。

静态多模式接口组的特征

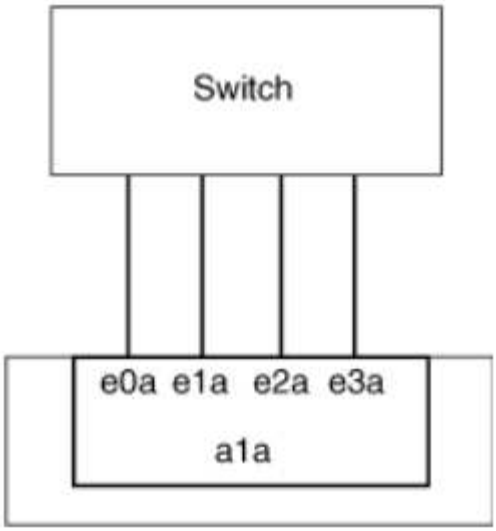
ONTAP 中的静态多模式接口组实施符合 IEEE 802.3ad （静态）标准。任何支持聚合但不具有用于配置聚合的控制数据包交换的交换机都可以与静态多模式接口组结合使用。

静态多模式接口组不符合 IEEE 802.3ad （动态），也称为链路聚合控制协议（ LACP ）。LACP 相当于 Cisco 专有链路聚合协议端口聚合协议（ PAgP ）。

以下是静态多模式接口组的特征：

- 接口组中的所有接口均处于活动状态，并共享一个 MAC 地址。
  - 接口组中的接口之间分布有多个单独的连接。
  - 每个连接或会话都使用接口组中的一个接口。
    使用顺序负载平衡方案时，所有会话都会按数据包分布在可用链路之间，并且不会绑定到接口组中的特定接口。
- 静态多模式接口组可以从多达 "n-1 " 接口故障中恢复，其中 n 是构成该接口组的接口总数。
- 如果端口发生故障或已拔出，则遍历故障链路的流量会自动重新分配到其余接口之一。
- 静态多模式接口组可以检测到链路丢失，但无法检测到与客户端的连接断开或交换机配置不当，从而可能影响连接和性能。
- 静态多模式接口组需要一个支持通过多个交换机端口进行链路聚合的交换机。
  配置交换机后，接口组的链路所连接的所有端口都属于一个逻辑端口。某些交换机可能不支持为巨型帧配置的端口的链路聚合。有关详细信息，请参见交换机供应商的文档。
- 可以使用多种负载平衡选项在静态多模式接口组的接口之间分布流量。

下图是静态多模式接口组的示例。接口 e0a ， e1a ， e2a 和 e3a 属于 A1A 多模式接口组。A1A 多模式接口组中的所有四个接口均处于活动状态。



通过多种技术，可以在一个聚合链路中的流量分布在多个物理交换机上。用于实现此功能的技术因网络产品而异。ONTAP 中的静态多模式接口组符合 IEEE 802.3 标准。如果某种特定的多交换机链路聚合技术可与 IEEE 802.3 标准互操作或符合这些标准，则该技术应与 ONTAP 配合使用。

IEEE 802.3 标准规定，聚合链路中的传输设备决定了传输的物理接口。因此， ONTAP 仅负责分配出站流量，无法控制入站帧的到达方式。如果要管理或控制聚合链路上的入站流量传输，则必须在直连网络设备上修改此传输。

动态多模式接口组

动态多模式接口组可通过链路聚合控制协议（ Link Aggregation Control Protocol ， LACP ）将组成员资格传递给直连交换机。LACP 可用于检测链路丢失状态以及节点无法与直连交换机端口通信。

ONTAP 中的动态多模式接口组实施符合 IEEE 802.3 AD （ 802.1 AX ）的要求。ONTAP 不支持端口聚合协议（ PAgP ），它是 Cisco 提供的一种专有链路聚合协议。

动态多模式接口组需要支持 LACP 的交换机。

ONTAP 在不可配置的主动模式下实施 LACP ，与配置为主动或被动模式的交换机配合使用效果良好。ONTAP 实施长 LACP 计时器和短 LACP 计时器（用于不可配置的值 3 秒和 90 秒），如 IEEE 802.3 AD （ 802.1AX ）中所指定。

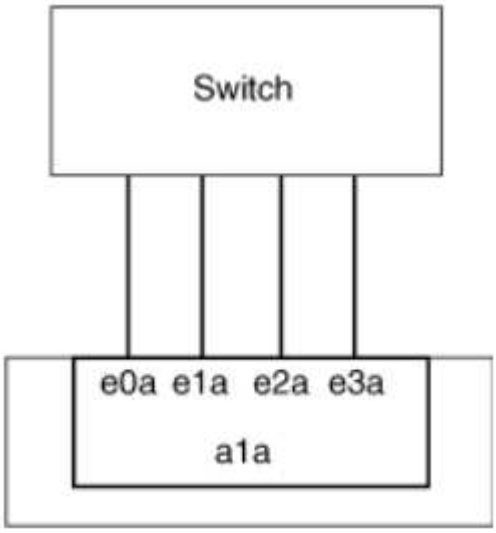
ONTAP 负载平衡算法可确定用于传输出站流量的成员端口，而不控制如何接收入站帧。交换机根据交换机端口通道组中配置的负载平衡算法确定要用于传输的端口通道组的成员（单个物理端口）。因此，交换机配置决定了要接收流量的存储系统的成员端口（单个物理端口）。有关配置交换机的详细信息，请参见交换机供应商提供的文档。

如果单个接口无法接收连续的 LACP 协议数据包，则该接口将在 "ifgrp status" 命令的输出中标记为 "lag_inactive" 。现有流量会自动重新路由到任何剩余的活动接口。

使用动态多模式接口组时，以下规则适用：

- 动态多模式接口组应配置为使用基于端口，基于 IP ，基于 MAC 或轮循负载平衡方法。
- 在动态多模式接口组中，所有接口都必须处于活动状态并共享一个 MAC 地址。

下图是动态多模式接口组的一个示例。接口 e0a ， e1a ， e2a 和 e3a 属于 A1A 多模式接口组。A1A 动态多模式接口组中的所有四个接口都处于活动状态。



多模式接口组中的负载平衡

通过使用 IP 地址， MAC 地址，顺序负载平衡或基于端口的负载平衡方法在多模式接口组的网络端口上平均分布网络流量，您可以确保多模式接口组的所有接口都能均衡地用于传出流量。

只有在创建多模式接口组时，才能为该接口组指定负载平衡方法。

- 最佳实践 *： 建议尽可能实现基于端口的负载平衡。请使用基于端口的负载平衡，除非网络中存在特定的原因或限制，以阻止此负载平衡。

基于端口的负载平衡

建议使用基于端口的负载平衡方法。

您可以使用基于端口的负载平衡方法根据传输层（ TCP/UDP ）端口均衡多模式接口组上的流量。

基于端口的负载平衡方法对源和目标 IP 地址以及传输层端口号使用快速哈希算法。

IP 地址和 **MAC** 地址负载平衡

IP 地址和 MAC 地址负载平衡是用于平衡多模式接口组上的流量的方法。

这些负载平衡方法对源地址和目标地址（ IP 地址和 MAC 地址）使用快速哈希算法。如果哈希算法的结果映射到的接口不处于 up 链路状态，则会使用下一个活动接口。

> 在直接连接到路由器的系统上创建接口组时，请勿选择 MAC 地址负载平衡方法。在这种设置中，对于每个传出 IP 帧，目标 MAC 地址是路由器的 MAC 地址。因此，只会使用接口组的一个接口。

IPv4 和 IPv6 地址的 IP 地址负载平衡工作方式相同。

顺序负载平衡

您可以使用顺序负载平衡，使用轮循算法在多个链路之间平均分布数据包。您可以使用顺序选项在多个链路之间对单个连接的流量进行负载平衡，以提高单个连接的吞吐量。

但是，由于顺序负载平衡可能发生原因会导致数据包交付无序，因此可能会导致性能极差。因此，通常不建议进行顺序负载平衡。

创建接口组或LAG

您可以通过组合聚合网络端口的功能来创建接口组或LAG (单模式、静态多模式或动态多模式(LACP))、以便为客户端提供一个接口。

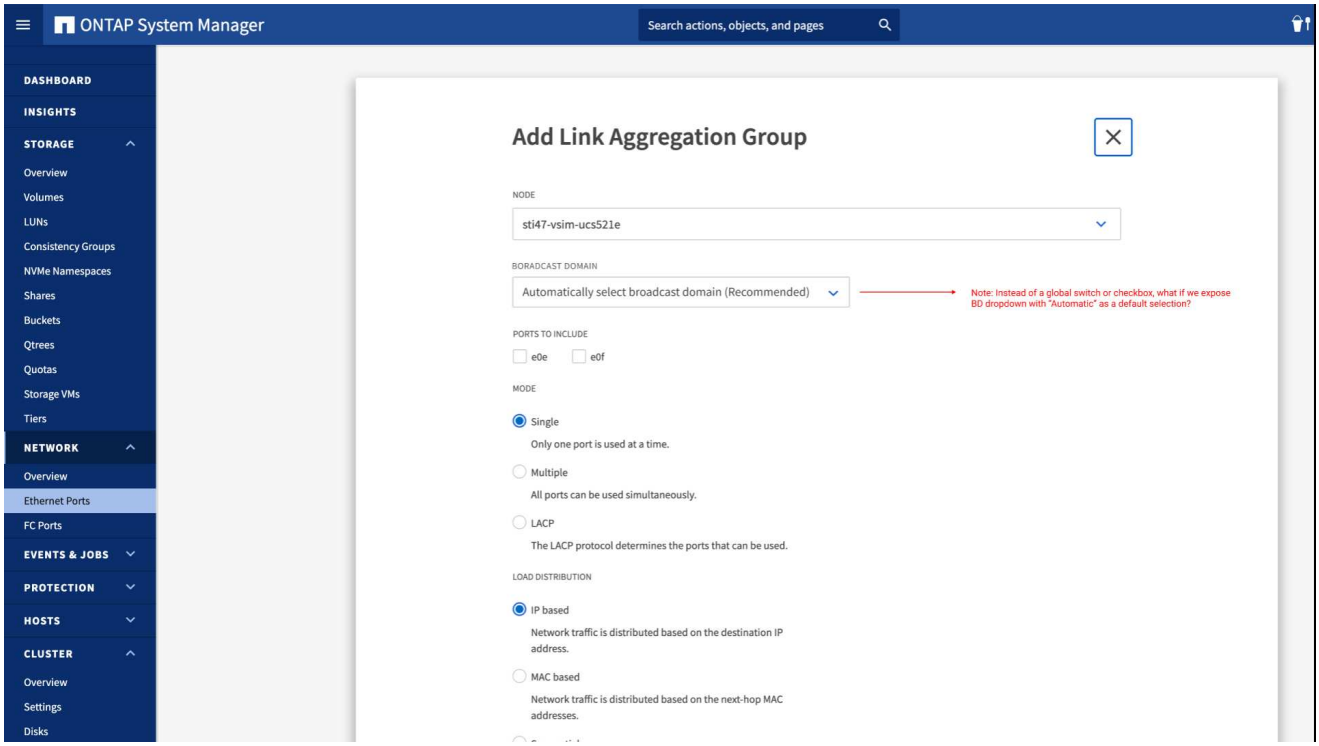
您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

*使用System Manager创建LAG *

步骤

1. 选择*网络>以太网端口>+链路聚合组*以创建LAG。
2. 从下拉列表中选择节点。
3. 从以下选项中进行选择：
   a. ONTAP 自动选择广播域(建议)。
   b. 手动选择广播域。
4. 选择要形成LAG的端口。
5. 选择模式：
   a. Single：一次仅使用一个端口。
   b. Multiple：可以同时使用所有端口。
   c. LACP：LACP协议确定可使用的端口。
6. 选择负载平衡：
   a. 基于IP
   b. 基于Mac
   c. Port
   d. 顺序
7. 保存所做的更改。



命令行界面

使用命令行界面创建接口组

有关适用于端口接口组的配置限制的完整列表、请参见 `network port ifgrp add-port` 手册页。

创建多模式接口组时，您可以指定以下任一负载平衡方法：

- `port`：网络流量基于传输层(TCP/UDP)端口分布。这是建议的负载平衡方法。
- `mac`：网络流量基于MAC地址进行分布。
- `ip`：网络流量按IP地址分布。
- `sequential`：网络流量在收到时即会分布。

> 接口组的 MAC 地址取决于底层端口的顺序以及这些端口在启动期间的初始化方式。因此，您不应假定 ifgrp MAC 地址在重新启动或 ONTAP 升级后持久存在。

步骤

使用 `network port ifgrp create` 用于创建接口组的命令。

接口组必须使用语法进行命名 `a<number><letter>`。例如， a0a ， a0b ， a1c 和 a2a 是有效的接口组名称。

有关此命令的详细信息，请参见 "ONTAP 9 命令"。

以下示例显示了如何创建一个名为 a0a 的接口组，该接口组具有端口的分发功能和多模式：

```
network port ifgrp create -node cluster-1-01 -ifgrp a0a -distr-func port -mode multimode
```

将端口添加到接口组或**LAG**

对于所有端口速度、您最多可以将16个物理端口添加到一个接口组或LAG中。

您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

使用**System Manager**向**LAG**添加端口

步骤

1. 选择*网络>以太网端口> LAG *以编辑LAG。
2. 选择同一节点上的其他端口以添加到LAG。
3. 保存所做的更改。

命令行界面

使用命令行界面向接口组添加端口

步骤

将网络端口添加到接口组：

```
network port ifgrp add-port
```

有关此命令的详细信息，请参见 "ONTAP 9 命令"。

以下示例显示了如何将端口 e0c 添加到名为 a0a 的接口组：

```
network port ifgrp add-port -node cluster-1-01 -ifgrp a0a -port e0c
```

从 ONTAP 9.8 开始，在将第一个物理端口添加到接口组后大约一分钟，接口组会自动放置到相应的广播域中。如果您不希望ONTAP执行此操作、而希望手动将ifgrp置于广播域中、请指定 `-skip-broadcast-domain-placement` 参数作为的一部分 `ifgrp add-port` 命令：

从接口组或**LAG**中删除端口

您可以从托管 LIF 的接口组中删除端口，但前提是它不是接口组中的最后一个端口。考虑到您不会从接口组中删除最后一个端口，因此不要求接口组不能托管 LIF 或接口组不能是 LIF 的主端口。但是，如果要删除最后一个端口，则必须先从接口组迁移或移动 LIF 。

关于此任务

您最多可以从一个接口组或LAG中删除16个端口(物理接口)。

您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

使用**System Manager**从**LAG**中删除端口

步骤

1. 选择*网络>以太网端口> LAG *以编辑LAG。
2. 选择要从LAG中删除的端口。
3. 保存所做的更改。

命令行界面

使用命令行界面从接口组中删除端口

步骤

从接口组中删除网络端口：

```
network port ifgrp remove-port
```

以下示例显示了如何从名为 a0a 的接口组中删除端口 e0c：

```
network port ifgrp remove-port -node cluster-1-01 -ifgrp a0a -port e0c
```

删除接口组或**LAG**

如果要直接在底层物理端口上配置LIF、或者决定更改接口组或LAG模式或分发功能、则可以删除接口组或LAG。

开始之前

- 接口组或LAG不得托管LIF。
- 接口组或LAG既不能是LIF的主端口、也不能是LIF的故障转移目标。

您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

*使用System Manager删除LAG *

步骤

1. 选择*网络>以太网端口> LAG *以删除LAG。
2. 选择要删除的LAG。
3. 删除LAG。

命令行界面

使用命令行界面删除接口组

步骤

使用 `network port ifgrp delete` 用于删除接口组的命令。

有关此命令的详细信息，请参见 "ONTAP 9 命令"。

以下示例显示了如何删除名为 a0b 的接口组：

```
network port ifgrp delete -node cluster-1-01 -ifgrp a0b
```

通过物理端口配置 **VLAN**

您可以在ONTAP中使用VLAN来创建单独的广播域、这些广播域是在交换机端口上定义的、而不是在物理边界上定义的传统广播域、从而实现网络的逻辑分段。

一个 VLAN 可以跨越多个物理网段。属于 VLAN 的终端工作站按功能或应用程序相关联。

例如， VLAN 中的终端工作站可以按部门（如工程和会计）或项目（如 release1 和 release2 ）进行分组。由于终端工作站的物理位置在 VLAN 中并不重要，因此您可以将终端工作站分散在不同的地理位置，并且仍会将广播域包含在交换网络中。

在ONTAP 9.13.1和9.14.1中、任何逻辑接口(Logical Interface、lifs)未使用且所连接交换机上缺少本机VLAN连接的未标记端口将标记为已降级。这有助于确定未使用的端口、并不表示发生中断。本机VLAN允许在ifgrp基本端口上传输未标记的流量、例如ONTAP CFM广播。在交换机上配置本机VLAN、以防止阻止未标记的流量。

您可以通过创建，删除或显示 VLAN 的相关信息来管理 VLAN 。

> 您不应在标识符与交换机的原生 VLAN 相同的网络接口上创建 VLAN 。例如，如果网络接口 e0b 位于原生 VLAN 10 上，则不应在此接口上创建 VLAN e0b-10 。

创建**VLAN**

您可以使用System Manager或创建VLAN、以便在同一网络域中维护单独的广播域 `network port vlan create` 命令：

开始之前

确认已满足以下要求：

- 网络中部署的交换机必须符合 IEEE 802.1Q 标准，或者实施供应商专用的 VLAN 。
- 要支持多个 VLAN ，必须静态配置一个终端工作站，使其属于一个或多个 VLAN 。
- VLAN 未连接到托管集群 LIF 的端口。
- VLAN 未连接到分配给集群 IP 空间的端口。
- 不会在不包含任何成员端口的接口组端口上创建 VLAN 。

关于此任务

创建 VLAN 会将 VLAN 连接到集群中指定节点上的网络端口。

首次通过端口配置 VLAN 时，此端口可能会关闭，从而导致网络暂时断开连接。随后向同一端口添加 VLAN 不会影响端口状态。

> 您不应在标识符与交换机的原生 VLAN 相同的网络接口上创建 VLAN 。例如，如果网络接口 e0b 位于原生 VLAN 10 上，则不应在此接口上创建 VLAN e0b-10 。

您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

使用**System Manager**创建**VLAN**

从ONTAP 9.12.0开始、您可以自动选择广播域或从列表中手动选择On。以前、始终会根据第2层连接自动选择广播域。如果您手动选择广播域、则会显示一条警告、指出手动选择广播域可能会导致连接丢失。

步骤

1. 选择*网络>以太网端口>+ VLAN*。
2. 从下拉列表中选择节点。
3. 从以下选项中进行选择：
   a. ONTAP 自动选择广播域(建议)。
   b. 从列表中手动选择广播域。
4. 选择要构成VLAN的端口。
5. 指定VLAN ID。
6. 保存所做的更改。

命令行界面

使用命令行界面创建**VLAN**

在某些情况下、如果要在已降级的端口上创建VLAN端口、而不更正硬件问题描述或任何软件配置错误、则可以设置 `-ignore-health-status` 的参数 `network port modify` 命令作为 `true`。

步骤

1. 使用 `network port vlan create` 命令以创建VLAN。
2. 您必须指定 `vlan-name` 或 `port` 和 `vlan-id` 选项。
   VLAN 名称是端口（或接口组）名称和网络交换机 VLAN 标识符的组合，两者之间带有连字符。例如：`e0c-24` 和 `e1c-80` 是有效的VLAN名称。

以下示例显示了如何创建VLAN `e1c-80` 已连接到网络端口 `e1c` 在节点上 `cluster-1-01`：

```
network port vlan create -node cluster-1-01 -vlan-name e1c-80
```

从 ONTAP 9.8 开始， VLAN 会在创建后大约一分钟自动放置到相应的广播域中。如果您不希望ONTAP执行此操作、而希望手动将VLAN置于广播域中、请指定 `-skip-broadcast-domain-placement` 参数作为的一部分 `vlan create` 命令：

有关此命令的详细信息，请参见 "ONTAP 9 命令"。

编辑**VLAN**

您可以更改广播域或禁用VLAN。

使用**System Manager**编辑**VLAN**

从ONTAP 9.12.0开始、您可以自动选择广播域或从列表中手动选择On。以前的广播域始终会根据第2层连接自动选择。如果您手动选择广播域、则会显示一条警告、指出手动选择广播域可能会导致连接丢失。

步骤

1. 选择*网络>以太网端口> VLAN*。
2. 选择编辑图标。
3. 执行以下操作之一：
   - 通过从列表中选择其他广播域来更改此广播域。
   - 清除*已启用*复选框。
4. 保存所做的更改。

删除VLAN

在从插槽中删除 NIC 之前，您可能需要删除 VLAN 。删除 VLAN 时，它会自动从使用它的所有故障转移规则和组中删除。

开始之前

确保没有与 VLAN 关联的 LIF 。

关于此任务

从端口删除最后一个 VLAN 可能发生原因会导致网络与端口暂时断开连接。

您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

使用**System Manager**删除**VLAN**

步骤

1. 选择*网络>以太网端口> VLAN*。
2. 选择要删除的VLAN。
3. 单击 * 删除 * 。

命令行界面

使用命令行界面删除**VLAN**

步骤

使用 `network port vlan delete` 命令删除VLAN。

以下示例显示了如何删除VLAN `e1c-80` 从网络端口 `e1c` 在节点上 `cluster-1-01`：

```
network port vlan delete -node cluster-1-01 -vlan-name e1c-80
```

修改网络端口属性

您可以修改物理网络端口的自动协商，双工，流量控制，速度和运行状况设置。

开始之前

要修改的端口不能托管任何 LIF 。

关于此任务

- 建议不要修改100 GbE、40 GbE、10 GbE或1 GbE网络接口的管理设置。

  为双工模式和端口速度设置的值称为管理设置。根据网络限制，管理设置可能与操作设置不同（即端口实际使用的双工模式和速度）。

- 建议不要修改接口组中底层物理端口的管理设置。

  。 `-up-admin` 参数(在高级权限级别可用)用于修改端口的管理设置。

- 建议不要设置 `-up-admin` 对于节点上的所有端口或节点上托管最后一个正常运行的集群LIF的端口、管理设置为false。
- 建议不要修改管理端口的MTU大小、 `e0M`。
- 广播域中端口的 MTU 大小不能与为广播域设置的 MTU 值进行更改。
- VLAN 的 MTU 大小不能超过其基本端口的 MTU 大小值。

步骤

1. 修改网络端口的属性：

   ```
   network port modify
   ```

2. 您可以设置 `-ignore-health-status` 字段设置为true、用于指定系统可以忽略指定端口的网络端口运行状况。

   网络端口运行状况会自动从已降级更改为运行状况良好，此端口现在可用于托管 LIF 。您应将集群端口的流量控制设置为 `none`。默认情况下、流量控制设置为 `full`。

以下命令通过将流量控制设置为 none 来禁用端口 e0b 上的流量控制：

```
network port modify -node cluster-1-01 -port e0b -flowcontrol-admin none
```

将 **40GbE NIC** 端口转换为多个 **10GbE** 端口以实现 **10GbE** 连接

您可以将 X1144A-R6 和 X91440A-R6 40GbE 网络接口卡（ NIC ）转换为支持四个 10GbE 端口。

如果要将支持其中一个 NIC 的硬件平台连接到支持 10GbE 集群互连和客户数据连接的集群，则必须转换此 NIC 以提供必要的 10GbE 连接。

开始之前

您必须使用受支持的分支缆线。

关于此任务

有关支持 NIC 的平台的完整列表，请参见 "Hardware Universe"。

> 在 X1144A-R6 NIC 上，只能转换端口 A 以支持四个 10GbE 连接。转换端口 A 后，端口 e 将不可用。

步骤

1. 进入维护模式。
2. 将 NIC 从 40GbE 支持转换为 10GbE 支持。

```
nicadmin convert -m [40G | 10G] [port-name]
```

3. 使用 convert 命令后，暂停节点。
4. 安装或更换缆线。
5. 根据硬件型号，使用 SP （服务处理器）或 BMC （基板管理控制器）重新启动节点，以使转换生效。

从节点中删除**NIC (ONTAP 9.8**及更高版本**)**

本主题 适用场景 ONTAP 9.8及更高版本。出于维护目的，您可能需要从插槽中删除故障 NIC 或将此 NIC 移至其他插槽。

步骤

1. 关闭节点。
2. 从插槽中物理卸下 NIC 。
3. 打开节点电源。
4. 验证是否已删除此端口：

```
network port show
```

> ONTAP 会自动从任何接口组中删除此端口。如果端口是接口组的唯一成员，则会删除该接口组。

5. 如果端口上配置了任何 VLAN ，则这些 VLAN 将被替换。您可以使用以下命令查看已替换的 VLAN ：

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

> 。 `displaced-interface show`， `displaced-vlans show`，和 `displaced-vlans restore` 命令是唯一的、不需要以开头的完全限定命令名称 `cluster controller-replacement network`。

6. 这些 VLAN 将被删除，但可以使用以下命令进行还原：

```
displaced-vlans restore
```

7. 如果此端口配置了任何 LIF ，则 ONTAP 会自动为同一广播域中另一个端口上的 LIF 选择新的主端口。如果在同一个存储器上找不到合适的主端口，则会将这些 LIF 视为已替换。您可以使用以下命令查看已替换的 LIF ：

   ```
   displaced-interface show
   ```

8. 将新端口添加到同一节点上的广播域后， LIF 的主端口将自动还原。或者、您也可以使用设置主端口 `network interface modify -home-port -home-node or use the displaced- interface restore` 命令：

从节点中删除**NIC (ONTAP 9.7**或更早版本**)**

本主题为适用场景 ONTAP 9.7 或更早版本。出于维护目的，您可能需要从插槽中删除故障 NIC 或将此 NIC 移至其他插槽。

开始之前

- 必须已迁移或删除 NIC 端口上托管的所有 LIF 。
- 任何 NIC 端口都不能是任何 LIF 的主端口。
- 要从 NIC 中删除端口，您必须具有高级权限。

步骤

1. 从 NIC 中删除端口：

   ```
   network port delete
   ```

2. 验证端口是否已删除：

   ```
   network port show
   ```

3. 如果 network port show 命令的输出仍显示已删除的端口，请重复步骤 1 。

监控网络端口

监控网络端口的运行状况

网络端口的 ONTAP 管理包括自动运行状况监控和一组运行状况监控器，可帮助您确定可能不适合托管 LIF 的网络端口。

关于此任务

如果运行状况监控器确定某个网络端口运行状况不正常，则会通过 EMS 消息向管理员发出警告或将此端口标记为已降级。如果该 LIF 有其他正常运行的故障转移目标，则 ONTAP 可避免在降级的网络端口上托管 LIF 。端口可能会因链路摆动（链路在启动和关闭之间快速来回切换）或网络分区等软故障事件而降级：

- 如果集群 IP 空间中的网络端口遇到链路摆动或无法通过第 2 层（ L2 ）访问广播域中的其他网络端口，则这

些端口会标记为已降级。

- 如果非集群 IP 空间中的网络端口遇到链路摆动，则这些端口会标记为已降级。

您必须了解已降级端口的以下行为：

- 已降级的端口不能包含在 VLAN 或接口组中。

  如果接口组的成员端口标记为已降级，但接口组仍标记为运行状况良好，则 LIF 可以托管在该接口组上。

- LIF 会自动从已降级的端口迁移到运行正常的端口。
- 在故障转移事件期间，已降级的端口不会被视为故障转移目标。如果没有运行正常的端口可用，则降级的端口将根据正常故障转移策略托管 LIF 。
- 您不能创建 LIF ，将其迁移或还原到已降级的端口。

  您可以修改 `ignore-health-status` 将网络端口设置为 `true`。然后，您可以在运行正常的端口上托管 LIF 。

步骤

1. 登录到高级权限模式：

   ```
   set -privilege advanced
   ```

2. 检查已启用哪些运行状况监控器以监控网络端口运行状况：

   ```
   network options port-health-monitor show
   ```

   端口的运行状况由运行状况监控器的值决定。

   默认情况下， ONTAP 中提供并启用了以下运行状况监控器：

   - 链路摆动运行状况监控器：监控链路摆动

     如果某个端口在五分钟内发生多次链路摆动，则此端口将标记为已降级。

   - L2 可访问性运行状况监控器：监控在同一广播域中配置的所有端口是否具有 L2 可访问性

     此运行状况监控器会报告所有 IP 空间中的 L2 可访问性问题；但是，它仅会将集群 IP 空间中的端口标记为已降级。

   - CRC monitor ：监控端口上的 CRC 统计信息

     此运行状况监控器不会将端口标记为已降级，但会在观察到极高的 CRC 故障率时生成 EMS 消息。

3. 根据需要使用为IP空间启用或禁用任何运行状况监控器 `network options port-health-monitor modify` 命令：
4. 查看端口的详细运行状况：

```
network port show -health
```

命令输出将显示端口的运行状况、 `ignore health status` 设置、以及端口标记为已降级的原因列表。

端口运行状况可以是 `healthy` 或 `degraded`。

如果 `ignore health status` 设置为 `true`、表示端口运行状况已从修改 `degraded` to `healthy` 由管理员执行。

如果 `ignore health status` 设置为 `false`，端口运行状况由系统自动确定。

监控网络端口的可访问性(ONTAP 9.8及更高版本)

ONTAP 9.8 及更高版本内置了可访问性监控功能。使用此监控功能确定物理网络拓扑何时与 ONTAP 配置不匹配。在某些情况下， ONTAP 可以修复端口可访问性。在其他情况下，需要执行其他步骤。

关于此任务

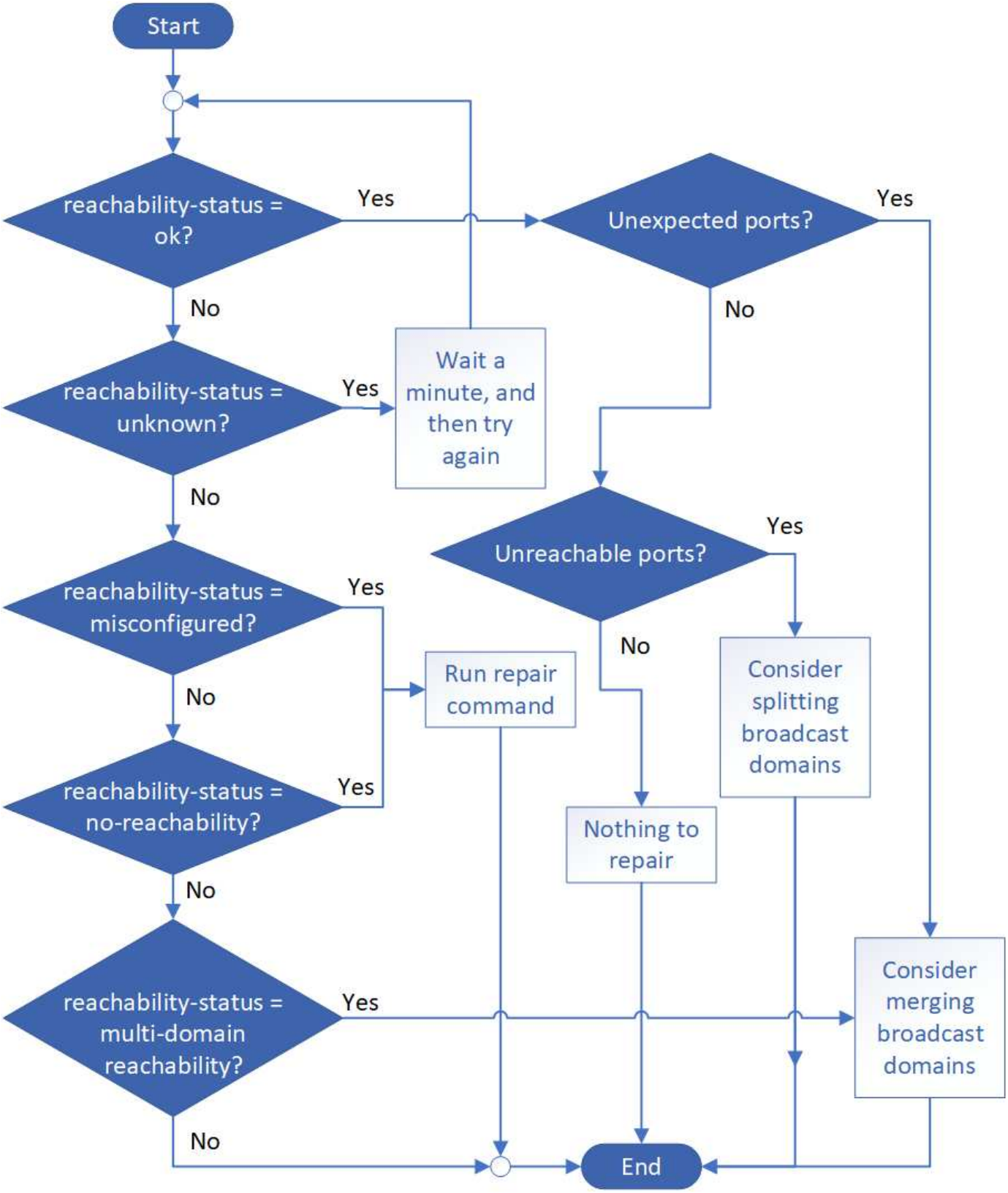
使用以下命令验证，诊断和修复因 ONTAP 配置与物理布线或网络交换机配置不匹配而导致的网络配置错误。

步骤

1. 查看端口可访问性：

```
network port reachability show
```

2. 使用以下决策树和表确定下一步（如果有）。



可访问性状态	Description

确定	此端口可通过第 2 层访问其分配的广播域。 如果可访问性状态为 " 正常 " ，但存在 " 意外端口 " ，请考虑合并一个或多个广播域。有关详细信息，请参见以下 _unexpected ports_行 。 如果可访问性状态为 " 正常 " ，但存在 " 无法访问的端口 " ，请考虑拆分一个或多个广播域。有关详细信息，请参见以下 _Unreachable ports_行 。 如果可访问性状态为 " 正常 " ，并且没有意外或无法访问的端口，则表示您的配置正确。
意外端口	此端口可通过第 2 层访问其分配的广播域；但是，它也可通过第 2 层访问至少其他一个广播域。 检查物理连接和交换机配置以确定它是否不正确，或者端口分配的广播域是否需要与一个或多个广播域合并。 有关详细信息，请参见 "合并广播域"。
无法访问的端口	如果一个广播域已分区为两个不同的可访问性集，则可以拆分一个广播域，以便将 ONTAP 配置与物理网络拓扑同步。 通常，不可访问的端口列表定义了在确认物理和交换机配置准确之后应拆分为另一个广播域的一组端口。 有关详细信息，请参见 "拆分广播域"。
配置不当的可访问性	此端口无法通过第 2 层访问其分配的广播域；但是，此端口确实可以通过第 2 层访问其他广播域。 您可以修复端口可访问性。运行以下命令时，系统会将此端口分配给其可访问性所在的广播域： `network port reachability repair -node -port` 有关详细信息，请参见 "修复端口可访问性"。
不可访问性	此端口无法通过第 2 层访问任何现有广播域。 您可以修复端口可访问性。运行以下命令时，系统会将此端口分配给默认 IP 空间中自动创建的新广播域： `network port reachability repair -node -port` 有关详细信息，请参见 "修复端口可访问性"。
多域可访问性	此端口可通过第 2 层访问其分配的广播域；但是，它也可通过第 2 层访问至少其他一个广播域。 检查物理连接和交换机配置以确定它是否不正确，或者端口分配的广播域是否需要与一个或多个广播域合并。 有关详细信息，请参见 "合并广播域" 或 "修复端口可访问性"。

未知	如果可访问性状态为 "unknown" ，请等待几分钟，然后重试此命令。

修复端口后，您需要检查并解决已替换的 LIF 和 VLAN 。如果端口属于某个接口组，则还需要了解该接口组发生了什么情况。有关详细信息，请参见 "修复端口可访问性"。

ONTAP端口概述

为与特定服务进行 ONTAP 通信预留了许多已知端口。如果存储网络环境中的端口值与 ONTAP 端口上的端口值相同，则会发生端口冲突。

下表列出了 ONTAP 使用的 TCP 端口和 UDP 端口。

服务	端口 / 协议	Description
SSH	22/TCP	安全 Shell 登录
Telnet	23TCP	远程登录
DNS	53/TCP	负载平衡 DNS
HTTP	80/TCP	超文本传输协议
rpcbind	111/TCP	远程操作步骤调用
rpcbind	111/UDP	远程操作步骤调用
NTP	123/UDP	网络时间协议
MSRPC	135/UDP	MSRPC
Netbios-SSN	139/TCP	NetBIOS 服务会话
SNMP	161/UDP	简单网络管理协议
HTTPS	443/TCP	基于 TLS 的 HTTP
Microsoft DS	445/TCP	Microsoft DS
挂载	635/TCP	NFS 挂载
挂载	635/UDP	NFS 挂载
已命名	953/UDP	名称守护进程
NFS	2049 UDP	NFS 服务器守护进程
NFS	2049/TCP	NFS 服务器守护进程
Nrv	20205/TCP	NetApp 远程卷协议
iSCSI	3260/TCP	iSCSI 目标端口
锁定	4045/TCP	NFS 锁定守护进程
锁定	4045/UDP	NFS 锁定守护进程
NSM	4046/ TCP	网络状态监控器
NSM	4046/UDP	网络状态监控器
rquotad	4049/UDP	NFS Rquotad 协议

krb524	444/UDP	Kerberos 524
mDNS	5533/UDP	多播 DNS
HTTPS	5986/UDP	HTTPS 端口—侦听二进制协议
HTTPS	843/TCP	通过 https 使用 7MTT GUI 工具
NDMP	10000/TCP	网络数据管理协议
集群对等	11104/TCP	集群对等、双向
集群对等、双向	11105/TCP	集群对等
NDMP	18600 - 18699/TCP	NDMP
NDMP	30000/TCP	通过安全插槽接受控制连接
CIFS 见证端口	40001/TCP	CIFS 见证端口
TLS	50000/TCP	传输层安全性
iSCSI	65200/TCP	iSCSI 端口

ONTAP 内部端口

下表列出了 ONTAP 内部使用的 TCP 端口和 UDP 端口。这些端口用于建立集群内 LIF 通信：

端口 / 协议	Description
514.	系统日志
900	NetApp 集群 RPC
902.	NetApp 集群 RPC
904	NetApp 集群 RPC
905	NetApp 集群 RPC
910.	NetApp 集群 RPC
911	NetApp 集群 RPC
913	NetApp 集群 RPC
914	NetApp 集群 RPC
91.	NetApp 集群 RPC
918	NetApp 集群 RPC
92.	NetApp 集群 RPC
921.	NetApp 集群 RPC
924	NetApp 集群 RPC
925	NetApp 集群 RPC
927	NetApp 集群 RPC
928	NetApp 集群 RPC

929.	NetApp 集群 RPC
931	NetApp 集群 RPC
932	NetApp 集群 RPC
933	NetApp 集群 RPC
934	NetApp 集群 RPC
935)	NetApp 集群 RPC
936	NetApp 集群 RPC
937	NetApp 集群 RPC
939	NetApp 集群 RPC
940	NetApp 集群 RPC
951	NetApp 集群 RPC
954	NetApp 集群 RPC
955	NetApp 集群 RPC
956	NetApp 集群 RPC
958	NetApp 集群 RPC
961.	NetApp 集群 RPC
963	NetApp 集群 RPC
9664	NetApp 集群 RPC
966	NetApp 集群 RPC
967	NetApp 集群 RPC
982.	NetApp 集群 RPC
983.	NetApp 集群 RPC
5125	磁盘的备用控制端口
5133	磁盘的备用控制端口
5144	磁盘的备用控制端口
65502	节点范围 SSH
65503	LIF 共享
7810.	NetApp 集群 RPC
7811.	NetApp 集群 RPC
7812.	NetApp 集群 RPC
7813.	NetApp 集群 RPC
7814.	NetApp 集群 RPC
7815.	NetApp 集群 RPC
7816.	NetApp 集群 RPC

7817.	NetApp 集群 RPC
7818.	NetApp 集群 RPC
7819.	NetApp 集群 RPC
7820.	NetApp 集群 RPC
7821.	NetApp 集群 RPC
7822.	NetApp 集群 RPC
7823.	NetApp 集群 RPC
7824.	NetApp 集群 RPC
8023.	节点范围 Telnet
8514.	节点范围 RSH
9877	KMIP 客户端端口（仅限内部本地主机）

IP 空间

配置IP空间概述

您可以通过 IP 空间配置一个 ONTAP 集群，以便客户端可以从多个管理上独立的网络域访问该集群，即使这些客户端使用相同的 IP 地址子网范围也是如此。这样可以隔离客户端流量，以确保隐私和安全。

IP 空间定义了 Storage Virtual Machine （ SVM ）所在的不同 IP 地址空间。为 IP 空间定义的端口和 IP 地址仅适用于该 IP 空间。系统会为 IP 空间中的每个 SVM 维护一个不同的路由表；因此，不会发生跨 SVM 或跨 IP 空间的流量路由。

> IP 空间支持其路由域上的 IPv4 和 IPv6 地址。

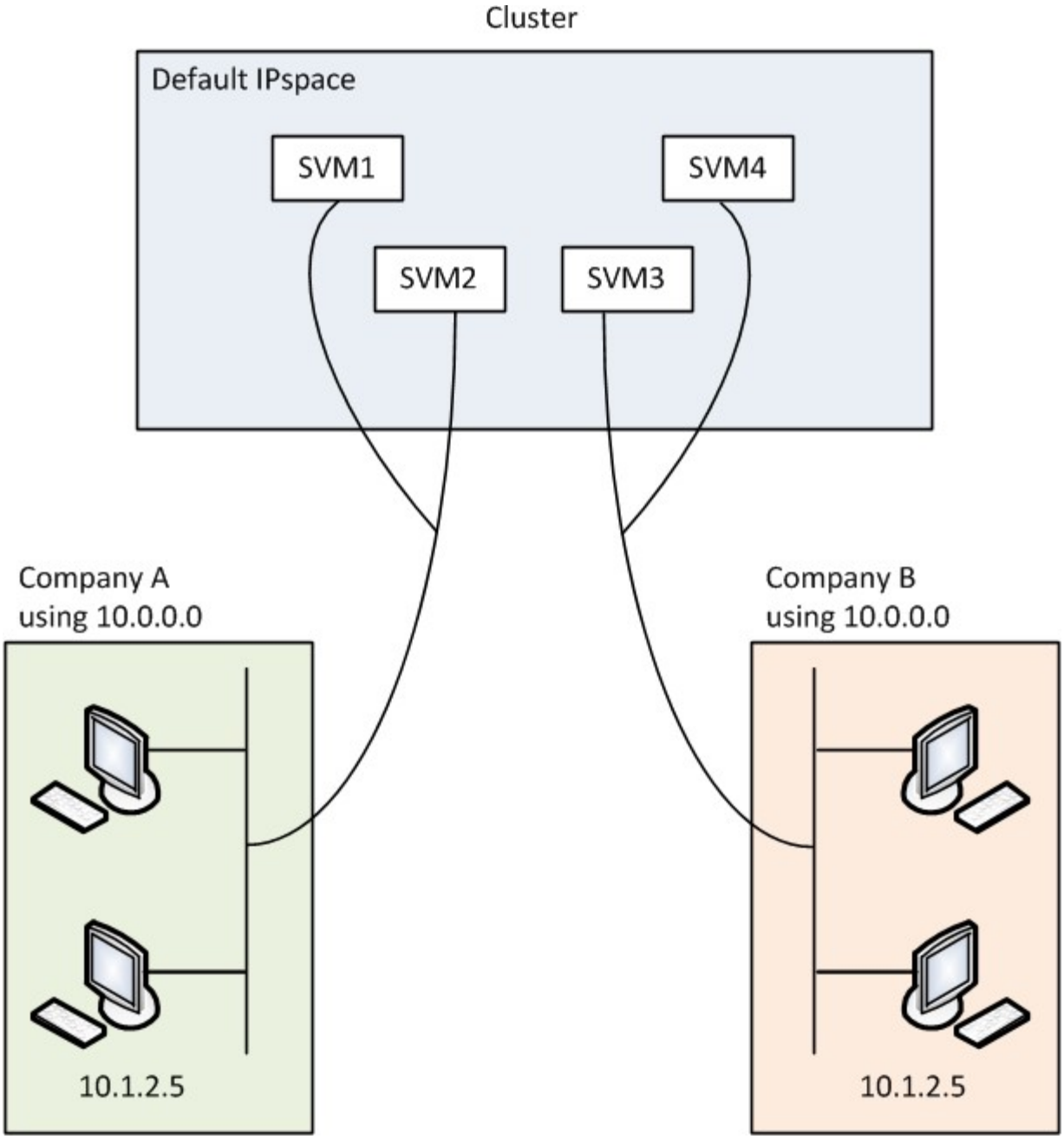
如果您要管理单个组织的存储，则无需配置 IP 空间。如果您要在一个 ONTAP 集群上管理多家公司的存储，并且确定您的客户没有任何网络配置冲突，则也不需要使用 IP 空间。在许多情况下，可以使用 Storage Virtual Machine （ SVM ）及其各自不同的 IP 路由表来隔离唯一的网络配置，而不是使用 IP 空间。

使用 IP 空间的示例

使用 IP 空间的一个常见应用是，当存储服务提供商（ SSP ）需要将公司 A 和 B 的客户连接到 SSP 内部的 ONTAP 集群时，这两家公司都使用相同的专用 IP 地址范围。

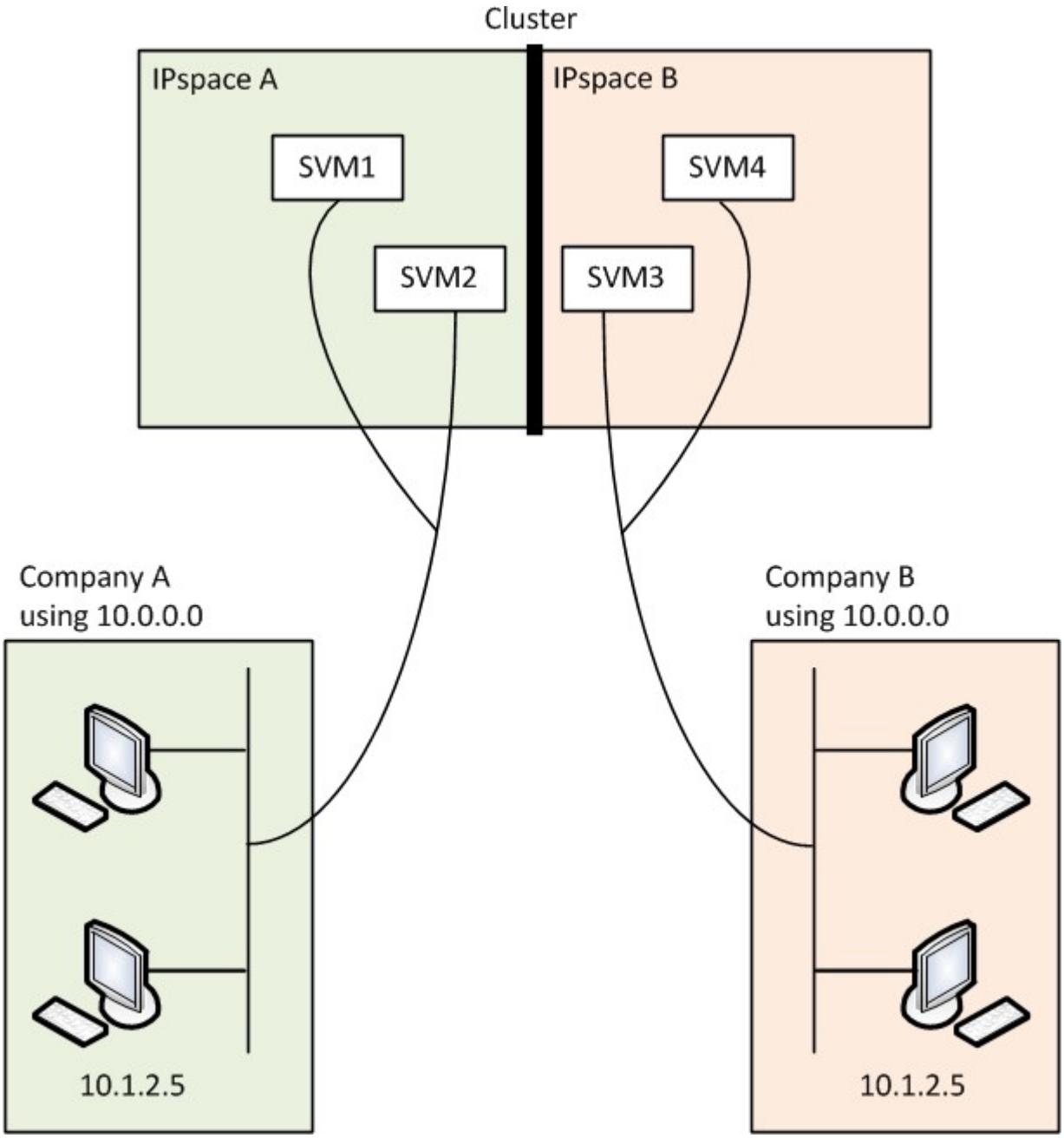
SSP 在集群上为每个客户创建 SVM ，并提供从两个 SVM 到公司 A 网络以及从其他两个 SVM 到公司 B 网络的专用网络路径。

下图显示了这种类型的部署，如果这两家公司都使用非专用 IP 地址范围，则此部署也适用。但是，图中显示了这两家公司使用相同的专用 IP 地址范围，这会导致出现问题。



这两家公司都使用专用 IP 地址子网 10.0.0.0 ，从而导致以下问题：

- 如果这两家公司决定为各自的 SVM 使用相同的 IP 地址，则位于 SSP 位置的集群中的 SVM 具有冲突的 IP 地址。
- 即使两家公司同意为其 SVM 使用不同的 IP 地址，也可能会出现问题。
- 例如，如果 A 网络中的任何客户端与 B 网络中的客户端具有相同的 IP 地址，则发往 A 地址空间中的客户端的数据包可能会路由到 B 地址空间中的客户端，反之亦然。
- 如果这两家公司决定使用互斥的地址空间（例如， A 使用网络掩码为 255.128.0.0 的 10.0.0.0 地址空间， B 使用网络掩码为 255.128.0.0 的 10.128.0.0 地址空间）， SSP 需要在集群上配置静态路由，以便将流量正确路由到 A 和 B 的网络。
- 此解决方案既不可扩展（因为存在静态路由），也不安全（广播流量会发送到集群的所有接口）。为了解决这些问题， SSP 会在集群上定义两个 IP 空间—每个公司一个。由于不路由跨 IP 空间流量，因此，即使所有 SVM 都配置在 10.0.0.0 地址空间中，每个公司的数据也会安全路由到各自的网络，如下图所示：



此外、各种配置文件(例如)引用的IP地址 `/etc/ hosts` 文件、 `/etc/hosts.equiv` 文件、然后 `the /etc/rc` 文件中的IP空间。因此，通过 IP 空间， SSP 可以为多个 SVM 的配置和身份验证数据配置相同的 IP 地址，而不会产生冲突。

IP 空间的标准属性

默认情况下，在首次创建集群时会创建特殊的 IP 空间。此外，还会为每个 IP 空间创建特殊的 Storage Virtual Machine （ SVM ）。

初始化集群时，系统会自动创建两个 IP 空间：

- " 默认 "IP 空间

  此 IP 空间是用于提供数据的端口，子网和 SVM 的容器。如果您的配置不需要为客户端使用单独的 IP 空间，则可以在此 IP 空间中创建所有 SVM 。此 IP 空间还包含集群管理端口和节点管理端口。

- " 集群 "IP 空间

  此 IP 空间包含集群中所有节点的所有集群端口。它会在创建集群时自动创建。它可提供与内部专用集群网络的连接。当其他节点加入集群时，这些节点的集群端口将添加到 " 集群 " IP 空间中。

每个 IP 空间都有一个 " 系统 " SVM 。创建 IP 空间时，系统会创建一个同名的默认系统 SVM ：

- " 集群 " IP 空间的系统 SVM 在内部专用集群网络上的集群节点之间传输集群流量。

  它由集群管理员管理，名称为 "Cluster" 。

- "Default" IP 空间的系统 SVM 传输集群和节点的管理流量，包括集群之间的集群间流量。

  它由集群管理员管理，并使用与集群相同的名称。

- 您创建的自定义 IP 空间的系统 SVM 传输该 SVM 的管理流量。

  它由集群管理员管理，并使用与 IP 空间相同的名称。

客户端的一个或多个 SVM 可以位于一个 IP 空间中。每个客户端 SVM 都有自己的数据卷和配置，并独立于其他 SVM 进行管理。

创建 IP 空间

IP 空间是 Storage Virtual Machine （ SVM ）所在的不同 IP 地址空间。当您需要 SVM 具有自己的安全存储，管理和路由时，您可以创建 IP 空间。您可以使用 IP 空间为集群中的每个 SVM 创建不同的 IP 地址空间。这样，在管理上独立的网络域中的客户端就可以访问集群数据，同时使用来自同一 IP 地址子网范围的重叠 IP 地址。

关于此任务

集群范围内的 IP 空间限制为 512 个。对于包含具有6 GB RAM的节点的集群、集群范围的IP空间限制将减少到256个。请参见 Hardware Universe 以确定您的平台是否具有其他限制。

"NetApp Hardware Universe"

> IP 空间名称不能为 "all" ，因为 "all" 是系统保留名称。

开始之前

您必须是集群管理员才能执行此任务。

步骤

1. 创建 IP 空间：

   ```
   network ipspace create -ipspace ipspace_name
   ```

   `ipspace_name` 是要创建的IP空间的名称。以下命令将在集群上创建 IP 空间 ipspace1 ：

```
network ipspace create -ipspace ipspace1
```

2. 显示IP空间：

   network ipspace show

```
IPspace             Vserver List          Broadcast Domains
------------------- --------------------- ----------------------------
Cluster             Cluster               Cluster
Default             Cluster1              Default
ipspace1            ipspace1              -
```

   此时将创建 IP 空间以及此 IP 空间的系统 SVM 。系统 SVM 传输管理流量。

完成后

如果在采用 MetroCluster 配置的集群中创建 IP 空间，则必须手动将 IP 空间对象复制到配对集群。在复制 IP 空间之前创建并分配给此 IP 空间的任何 SVM 都不会复制到配对集群。

广播域会自动在 " 默认 "IP 空间中创建，并可使用以下命令在 IP 空间之间移动：

```
network port broadcast-domain move
```

例如，如果要将广播域从 "Default" 移动到 "ips1" ，请使用以下命令：

```
network port broadcast-domain move -ipspace Default -broadcast-domain
Default -to-ipspace ips1
```

显示 **IP** 空间

您可以显示集群中的 IP 空间列表，也可以查看分配给每个 IP 空间的 Storage Virtual Machine （ SVM ），广播域和端口。

步骤

显示集群中的 IP 空间和 SVM ：

```
network ipspace show [-ipspace ipspace_name]
```

以下命令显示集群中的所有 IP 空间， SVM 和广播域：

```
network ipspace show
IPspace        Vserver List             Broadcast Domains
-------------  ------------------------  -------------------
Cluster
               Cluster                  Cluster
Default
               vs1, cluster-1            Default
ipspace1
               vs3, vs4, ipspace1       bcast1
```

以下命令显示属于 IP 空间 ipspace1 的节点和端口：

```
network ipspace show -ipspace ipspace1
IPspace name: ipspace1
Ports: cluster-1-01:e0c, cluster-1-01:e0d, cluster-1-01:e0e, cluster-1-
02:e0c, cluster-1-02:e0d, cluster-1-02:e0e
Broadcast Domains: Default-1
Vservers: vs3, vs4, ipspace1
```

删除 IP 空间

如果您不再需要 IP 空间，可以将其删除。

开始之前

不能存在与要删除的 IP 空间关联的广播域，网络接口或 SVM 。

无法删除系统定义的 "Default" 和 "Cluster" IP 空间。

步骤

删除 IP 空间：

```
network ipspace delete -ipspace ipspace_name
```

以下命令将从集群中删除 IP 空间 ipspace1 ：

```
network ipspace delete -ipspace ipspace1
```

广播域

广播域(ONTAP 9.8及更高版本)

广播域概述(ONTAP 9.8及更高版本)

广播域用于对属于同一第 2 层网络的网络端口进行分组。然后， Storage Virtual Machine （ SVM ）可以使用组中的端口来传输数据或管理流量。

广播域驻留在 IP 空间中。在集群初始化期间，系统会创建两个默认广播域：

- "Default" 广播域包含位于 "Default" IP 空间中的端口。

  这些端口主要用于提供数据。集群管理和节点管理端口也位于此广播域中。

- " 集群 " 广播域包含位于 " 集群 " IP 空间中的端口。

  这些端口用于集群通信，并包括集群中所有节点的所有集群端口。

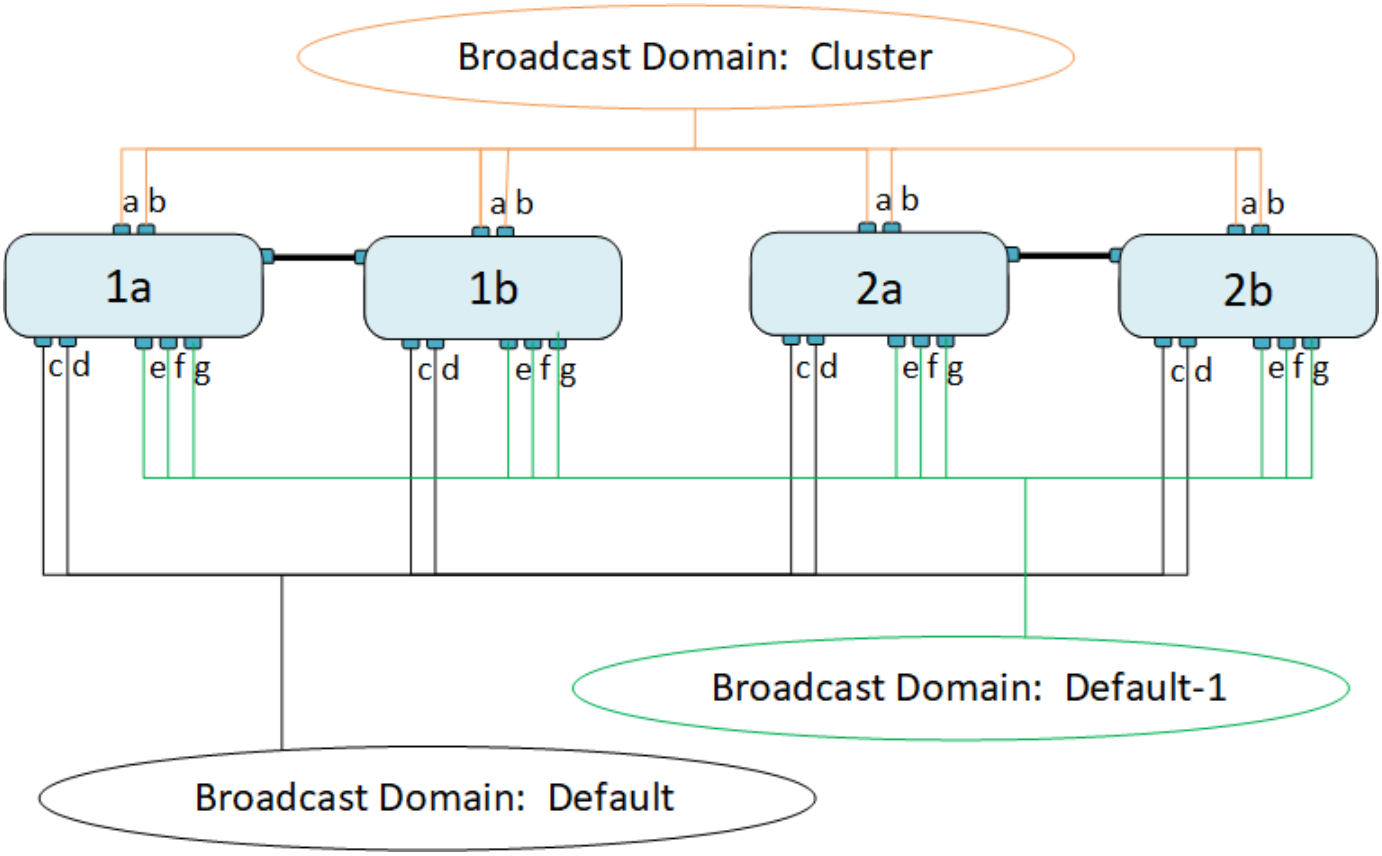
  系统会根据需要在默认 IP 空间中创建其他广播域。" 默认 " 广播域包含管理 LIF 的主端口，以及可通过第 2 层访问该端口的任何其他端口。其他广播域名为 "Default-1" ， "Default-2" 等。

使用广播域的示例

广播域是同一 IP 空间中的一组网络端口，也具有第 2 层可相互访问性，通常包括集群中许多节点的端口。

图中显示了分配给四节点集群中三个广播域的端口：

- " 集群 " 广播域会在集群初始化期间自动创建，其中包含集群中每个节点的端口 a 和 b 。
- " 默认 " 广播域也会在集群初始化期间自动创建，其中包含集群中每个节点的端口 c 和 d 。
- 在集群初始化期间，系统会根据第 2 层网络可访问性自动创建任何其他广播域。这些附加广播域名为 Default-1 ， Default-2 等。



系统会自动创建一个与每个广播域名称相同且网络端口相同的故障转移组。此故障转移组由系统自动管理，这意味着在从广播域添加或删除端口时，这些端口会自动添加或从此故障转移组中删除。

添加广播域

广播域对集群中属于同一第2层网络的网络端口进行分组。然后， SVM 可以使用这些端口。

从 ONTAP 9.8 开始，在集群创建或加入操作期间会自动创建广播域。从ONTAP 9.12.0开始、除了自动创建的广播域之外、您还可以在System Manager中手动添加广播域。

开始之前

计划添加到广播域的端口不能属于另一个广播域。如果要使用的端口属于另一个广播域、但未使用、请从原始广播域中删除这些端口。

关于此任务

- 所有广播域名在 IP 空间中必须是唯一的。
- 添加到广播域的端口可以是物理网络端口、VLAN或链路聚合组/接口组(LAG/ifgrp)。
- 如果要使用的端口属于另一个广播域、但未使用、请先将其从现有广播域中删除、然后再将其添加到新广播域。
- 添加到广播域的端口的最大传输单元(MTU)将更新为在广播域中设置的MTU值。
- MTU 值必须与连接到该第 2 层网络的所有设备匹配，但处理管理流量的 e0M 端口除外。
- 如果未指定 IP 空间名称，则会在 " 默认 "IP 空间中创建广播域。

为了简化系统配置，系统会自动创建一个同名的故障转移组，该故障转移组包含相同的端口。

System Manager

步骤

1. 选择*网络>概述>广播域*。
2. 单击 + Add
3. 命名广播域。
4. 设置MTU。
5. 选择 IP 空间。
6. 保存广播域。

您可以在添加广播域后对其进行编辑或删除。

命令行界面

在ONTAP 9.7或更早版本中、您可以手动创建广播域。

如果使用的是ONTAP 9.8及更高版本、则会根据第2层可访问性自动创建广播域。有关详细信息，请参见 "修复端口可访问性"。

步骤

1. 查看当前未分配给广播域的端口：

   ```
   network port show
   ```

   如果显示屏较大、请使用 `network port show -broadcast-domain` 命令以仅查看未分配的端口。

2. 创建广播域：

   ```
   network port broadcast-domain create -broadcast-domain
   broadcast_domain_name -mtu mtu_value [-ipspace ipspace_name] [-ports
   ports_list]
   ```

   a. `broadcast_domain_name` 是要创建的广播域的名称。

   b. `mtu_value` 是IP数据包的MTU大小；1500和9000是典型值。

      此值将应用于添加到此广播域的所有端口。

   c. `ipspace_name` 是要将此广播域添加到的IP空间的名称。

      除非为此参数指定值，否则将使用 "Default" IP 空间。

   d. `ports_list` 是要添加到广播域的端口的列表。

      此时将以格式添加端口 `node_name:port_number`，例如， `node1:e0c`。

3. 验证是否已根据需要创建广播域：

   ```
   network port show -instance -broadcast-domain new_domain
   ```

示例

以下命令会在默认 IP 空间中创建广播域 bcast1 ，将 MTU 设置为 1500 ，并添加四个端口：

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports
cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

完成后

您可以通过创建子网来定义广播域中可用的 IP 地址池，也可以此时将 SVM 和接口分配给 IP 空间。有关详细信息，请参见 "集群和 SVM 对等"。

如果需要更改现有广播域的名称、请使用 `network port broadcast-domain rename` 命令：

从广播域添加或删除端口**(ONTAP 9.8**及更高版本**)**

在集群创建或加入操作期间，系统会自动创建广播域。您无需手动从广播域中删除端口。

如果通过物理网络连接或交换机配置更改了网络端口可访问性，并且某个网络端口属于其他广播域，请参见以下主题：

"修复端口可访问性"

System Manager

从ONTAP 9.14.1开始、您可以使用System Manager在广播域之间重新分配以太网端口。建议将每个以太网端口分配给广播域。因此、如果从广播域取消分配以太网端口、则必须将其重新分配到其他广播域。

步骤

要重新分配以太网端口、请执行以下步骤：

1. 选择*网络>概述*。
2. 在*广播域*部分中，选择 ⋮ 域名旁边。
3. 在下拉菜单中，选择 * 编辑 * 。
4. 在*编辑广播域*页上，取消选择要重新分配给另一个域的以太网端口。
5. 对于每个取消选择的端口，将显示*ReassignEthernet Port*(重新分配以太网端口)窗口。选择要将端口重新分配到的广播域，然后选择*Reassign*。
6. 选择要分配给当前广播域的所有端口并保存更改。

命令行界面

如果通过物理网络连接或交换机配置更改了网络端口可访问性，并且某个网络端口属于其他广播域，请参见以下主题：

"修复端口可访问性"

或者、您也可以使用手动在广播域中添加或删除端口 `network port broadcast-domain add-ports` 或 `network port broadcast-domain remove-ports` 命令：

开始之前

- 您必须是集群管理员才能执行此任务。
- 计划添加到广播域的端口不能属于另一个广播域。
- 不能将已属于接口组的端口单独添加到广播域中。

关于此任务

添加和删除网络端口时，应遵循以下规则：

添加端口时 …	删除端口时 …
端口可以是网络端口， VLAN 或接口组（ ifgrp ）。	不适用
这些端口将添加到广播域的系统定义的故障转移组中。	端口将从广播域中的所有故障转移组中删除。
端口的 MTU 将更新为广播域中设置的 MTU 值。	端口的 MTU 不变。
端口的 IP 空间将更新为广播域的 IP 空间值。	这些端口将移至 " 默认 "IP 空间，而不具有广播域属性。

> 如果使用删除接口组的最后一个成员端口 `network port ifgrp remove-port` 命令中、则会导致接口组端口从广播域中删除、因为广播域中不允许使用空接口组端口。

步骤

1. 使用显示当前已分配或未分配给广播域的端口 `network port show` 命令：
2. 在广播域中添加或删除网络端口：

如果您要 …	使用 …
向广播域添加端口	`network port broadcast-domain add-ports`
从广播域中删除端口	`network port broadcast-domain remove-ports`

3. 验证是否已在广播域中添加或删除端口：

   ```
   network port show
   ```

有关这些命令的详细信息，请参见 "ONTAP 9 命令"。

添加和删除端口的示例

以下命令会将节点 cluster-1-01 上的端口 e0g 和节点 cluster-1-02 上的端口 e0g 添加到默认 IP 空间中的广播域 bcast1 ：

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1
-ports cluster-1-01:e0g,cluster1-02:e0g
```

以下命令会将两个集群端口添加到集群 IP 空间中的广播域集群：

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

以下命令将从默认 IP 空间的广播域 bcast1 中删除节点 cluster1-01 上的端口 e0e ：

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain
bcast1 -ports cluster-1-01:e0e
```

将广播域移动到**IP**空间**(ONTAP 9.8**及更高版本**)**

将系统根据第 2 层可访问性创建的广播域移动到您创建的 IP 空间中。

在移动广播域之前，您必须验证广播域中端口的可访问性。

端口的自动扫描可以确定哪些端口可以彼此连接并将其放置在同一广播域中，但此扫描无法确定适当的 IP 空间。如果广播域属于非默认 IP 空间，则必须使用本节中的步骤手动移动它。

开始之前

广播域会在集群创建和加入操作中自动配置。ONTAP 将 " 默认 " 广播域定义为一组端口，这些端口通过第 2 层连接到集群中创建的第一个节点上管理接口的主端口。如果需要，还会创建其他广播域，这些域的名称为 * 默认 -1* ， * 默认 -2* 等。

当节点加入现有集群时，其网络端口会根据其第 2 层可访问性自动加入现有广播域。如果它们无法访问现有广播域，则会将这些端口置于一个或多个新广播域中。

关于此任务

- 具有集群 LIF 的端口会自动置于 " 集群 " IP 空间中。
- 可访问节点管理 LIF 主端口的端口将置于 " 默认 " 广播域中。
- 其他广播域由 ONTAP 在集群创建或加入操作期间自动创建。
- 添加 VLAN 和接口组时，它们会在创建后大约一分钟自动放置到相应的广播域中。

步骤

1. 验证广播域中端口的可访问性。ONTAP 会自动监控第 2 层可访问性。使用以下命令验证每个端口是否已添加到广播域并具有 " 正常 " 可访问性。

   ```
   network port reachability show -detail
   ```

2. 如有必要，请将广播域移动到其他 IP 空间：

   ```
   network port broadcast-domain move
   ```

   例如，如果要将广播域从 "Default" 移动到 "ips1"：

   ```
   network port broadcast-domain move -ipspace Default -broadcast-domain Default
   -to-ipspace ips1
   ```

将广播域移动到**IP**空间**(ONTAP 9.8**及更高版本**)**

将系统根据第 2 层可访问性创建的广播域移动到您创建的 IP 空间中。

在移动广播域之前，您必须验证广播域中端口的可访问性。

端口的自动扫描可以确定哪些端口可以彼此连接并将其放置在同一广播域中，但此扫描无法确定适当的 IP 空间。如果广播域属于非默认 IP 空间，则必须使用本节中的步骤手动移动它。

开始之前

广播域会在集群创建和加入操作中自动配置。ONTAP 将 " 默认 " 广播域定义为一组端口，这些端口通过第 2 层连接到集群中创建的第一个节点上管理接口的主端口。如果需要，还会创建其他广播域，这些域的名称为 * 默认 -1* ， * 默认 -2* 等。

当节点加入现有集群时，其网络端口会根据其第 2 层可访问性自动加入现有广播域。如果它们无法访问现有广播域，则会将这些端口置于一个或多个新广播域中。

关于此任务

- 具有集群 LIF 的端口会自动置于 " 集群 " IP 空间中。
- 可访问节点管理 LIF 主端口的端口将置于 " 默认 " 广播域中。
- 其他广播域由 ONTAP 在集群创建或加入操作期间自动创建。
- 添加 VLAN 和接口组时，它们会在创建后大约一分钟自动放置到相应的广播域中。

步骤

1. 验证广播域中端口的可访问性。ONTAP 会自动监控第 2 层可访问性。使用以下命令验证每个端口是否已添加到广播域并具有 " 正常 " 可访问性。

```
network port reachability show -detail
```

2. 如有必要，请将广播域移动到其他 IP 空间：

```
network port broadcast-domain move
```

例如，如果要将广播域从 "Default" 移动到 "ips1"：

```
network port broadcast-domain move -ipspace Default -broadcast-domain Default
-to-ipspace ips1
```

拆分广播域(**ONTAP 9.8**及更高版本)

如果通过物理网络连接或交换机配置更改了网络端口可访问性， 先前在一个广播域中配置的一组网络端口已分区为两个不同的可访问性集，您可以拆分一个广播域，以便将 ONTAP 配置与物理网络拓扑同步。

要确定网络端口广播域是否已分区为多个可访问性集、请使用 `network port reachability show -details` 命令并注意哪些端口之间没有连接("无法访问的端口")。通常、在确认物理和交换机配置准确之后、无法访问的端口列表定义了应拆分为另一个广播域的端口集。

步骤

将广播域拆分为两个广播域：

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` 是广播域所在IP空间的名称。
- `-broadcast-domain` 是要拆分的广播域的名称。
- `-new-broadcast-domain` 是要创建的新广播域的名称。
- `-ports` 是要添加到新广播域的节点名称和端口。

合并广播域(**ONTAP 9.8**及更高版本)

如果通过物理网络连接或交换机配置更改了网络端口可访问性，并且先前在多个广播域中配置的两组网络端口现在都共享可访问性，则可以通过合并两个广播域将 ONTAP 配置与物理网络拓扑同步。

要确定多个广播域是否属于一个可访问性集，请使用 "network port reachability show -details" 命令，并注意在另一个广播域中配置的端口实际彼此连接（ " 意外端口 " ）。通常，意外端口列表会定义在确认物理和交换机配置准确后应合并到广播域中的一组端口。

步骤

将一个广播域中的端口合并到现有广播域中：

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name` 是广播域所在IP空间的名称。
- `-broadcast-domain` 是要合并的广播域的名称。
- `-into-broadcast-domain` 是将接收其他端口的广播域的名称。

更改广播域中端口的MTU值(ONTAP 9.8及更高版本)

您可以修改广播域的 MTU 值，以更改该广播域中所有端口的 MTU 值。这样可以支持在网络中进行的拓扑更改。

开始之前

MTU 值必须与连接到该第 2 层网络的所有设备匹配，但处理管理流量的 e0M 端口除外。

关于此任务

更改 MTU 值会导致受影响端口上的流量短暂中断。系统将显示一条提示，提示您必须使用 y 进行问题解答才能进行 MTU 更改。

步骤

更改广播域中所有端口的 MTU 值：

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

- `broadcast_domain` 是广播域的名称。
- `mtu` 是IP数据包的MTU大小；1500和9000是典型值。
- `ipspace` 是此广播域所在IP空间的名称。除非为此选项指定值，否则将使用 "Default" IP 空间。以下命令会将广播域 bcast1 中所有端口的 MTU 更改为 9000：

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <
9000 >
Warning: Changing broadcast domain settings will cause a momentary data-
serving interruption.
Do you want to continue? {y|n}: <y>
```

显示广播域(ONTAP 9.8及更高版本)

您可以显示集群中每个 IP 空间内的广播域列表。输出还会显示每个广播域的端口列表和 MTU 值。

步骤

显示集群中的广播域和关联端口：

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

以下命令显示集群中的所有广播域和关联端口：

```
network port broadcast-domain show
IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  ---------------------- --------------
Cluster Cluster      9000
                            cluster-1-01:e0a       complete
                            cluster-1-01:e0b       complete
                            cluster-1-02:e0a       complete
                            cluster-1-02:e0b       complete
Default Default      1500
                            cluster-1-01:e0c       complete
                            cluster-1-01:e0d       complete
                            cluster-1-02:e0c       complete
                            cluster-1-02:e0d       complete
        Default-1    1500
                            cluster-1-01:e0e       complete
                            cluster-1-01:e0f       complete
                            cluster-1-01:e0g       complete
                            cluster-1-02:e0e       complete
                            cluster-1-02:e0f       complete
                            cluster-1-02:e0g       complete
```

以下命令显示 Default-1 广播域中更新状态为 error 的端口，这表示此端口无法正确更新：

```
network port broadcast-domain show -broadcast-domain Default-1 -port
-update-status error

IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  ---------------------- --------------
Default Default-1   1500
                            cluster-1-02:e0g       error
```

有关详细信息，请参见 "ONTAP 9 命令"。

删除广播域

如果您不再需要广播域，可以将其删除。此操作会将与此广播域关联的端口移至 " 默认 "IP 空间。

开始之前

不能存在与要删除的广播域关联的子网，网络接口或 SVM 。

关于此任务

- 无法删除系统创建的 " 集群 " 广播域。
- 删除此广播域时，系统会删除与此广播域相关的所有故障转移组。

您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

从**ONTAP 9.12.0**开始、您可以使用**System Manager**删除广播域

如果广播域包含端口或与子网关联、则不会显示删除选项。

步骤

1. 选择*网络>概述>广播域*。
2. 选择 … ⋮ 要删除的广播域旁边的*>删除*。

命令行界面

使用命令行界面删除广播域

步骤

删除广播域：

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

以下命令将删除 IP 空间 ipspace1 中的广播域 Default-1 ：

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

广播域(ONTAP 9.7及更早版本)

广播域概述(ONTAP 9.7及更早版本)

广播域用于对属于同一第 2 层网络的网络端口进行分组。然后， Storage Virtual Machine （ SVM ）可以使用组中的端口来传输数据或管理流量。

广播域驻留在 IP 空间中。在集群初始化期间，系统会创建两个默认广播域：

- 默认广播域包含位于默认 IP 空间中的端口。
  这些端口主要用于提供数据。集群管理和节点管理端口也位于此广播域中。
- 集群广播域包含位于集群 IP 空间中的端口。
  这些端口用于集群通信，并包括集群中所有节点的所有集群端口。

如果您创建了唯一的 IP 空间来分隔客户端流量，则需要在其中每个 IP 空间中创建广播域。

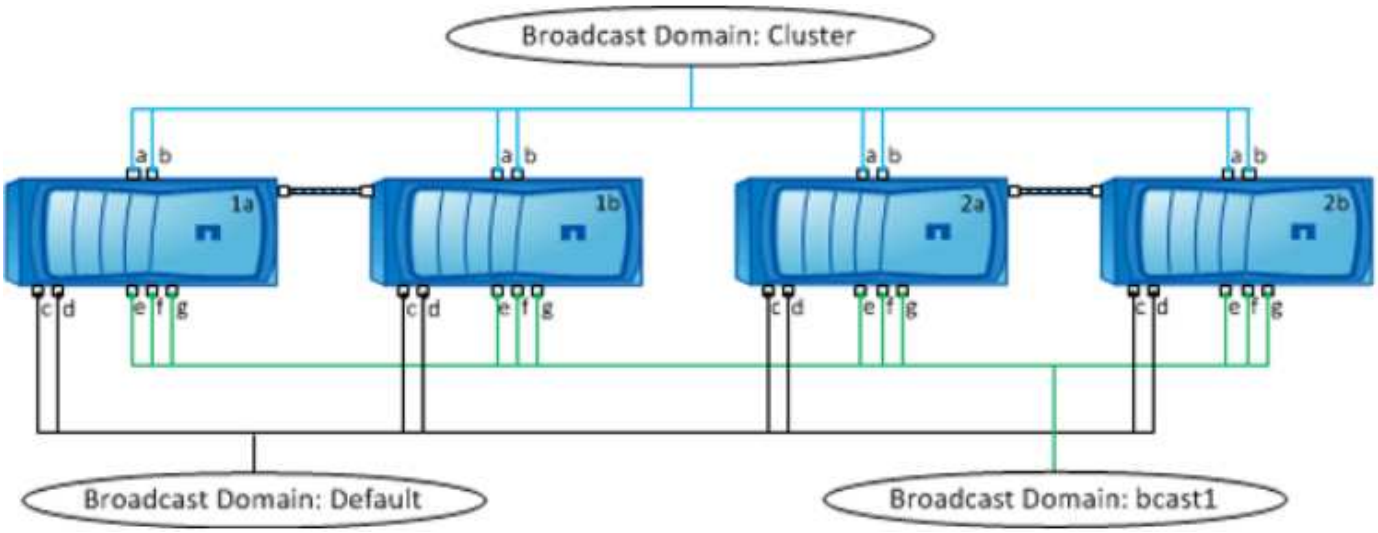
> 创建广播域，以便对集群中属于同一第 2 层网络的网络端口进行分组。然后， SVM 可以使用这些端口。

使用广播域的示例

广播域是同一 IP 空间中的一组网络端口，也具有第 2 层可相互访问性，通常包括集群中许多节点的端口。

图中显示了分配给四节点集群中三个广播域的端口：

- 集群广播域会在集群初始化期间自动创建，其中包含集群中每个节点的端口 a 和 b 。
- 默认广播域也会在集群初始化期间自动创建，其中包含集群中每个节点的端口 c 和 d 。
- bcast1 广播域已手动创建，其中包含集群中每个节点的端口 e ， f 和 g 。
  此广播域由系统管理员专门为新客户端创建，用于通过新 SVM 访问数据。



系统会自动创建一个与每个广播域名称相同且网络端口相同的故障转移组。此故障转移组由系统自动管理，这意味着在从广播域添加或删除端口时，这些端口会自动添加或从此故障转移组中删除。

确定哪些端口可用于广播域**(ONTAP 9.7**及更早版本**)**

在配置要添加到新 IP 空间的广播域之前，您必须先确定哪些端口可用于此广播域。

> 此任务与 ONTAP 9.0 - 9.7 相关，而不是与 ONTAP 9.8 相关。

开始之前

您必须是集群管理员才能执行此任务。

关于此任务

- 端口可以是物理端口， VLAN 或接口组（ ifgroups ）。
- 不能将要添加到新广播域的端口分配给现有广播域。
- 如果要添加到广播域的端口已位于另一个广播域中（例如，默认 IP 空间中的默认广播域），则必须先从该广播域中删除这些端口，然后再将其分配给新的广播域。
- 无法从广播域中删除已分配 LIF 的端口。
- 由于集群管理和节点管理 LIF 已分配给默认 IP 空间中的默认广播域，因此无法从默认广播域中删除分配给这些 LIF 的端口。

步骤

1. 确定当前端口分配。

   ```
   network port show
   ```

   ```
   Node   Port IPspace  Broadcast Domain Link   MTU  Admin/Oper
   ------ ---- -------  ---------------- ----- ----  ------------
   node1
          e0a  Cluster  Cluster          up    9000  auto/1000
          e0b  Cluster  Cluster          up    9000  auto/1000
          e0c  Default  Default          up    1500  auto/1000
          e0d  Default  Default          up    1500  auto/1000
          e0e  Default  Default          up    1500  auto/1000
          e0f  Default  Default          up    1500  auto/1000
          e0g  Default  Default          up    1500  auto/1000
   node2
          e0a  Cluster  Cluster          up    9000  auto/1000
          e0b  Cluster  Cluster          up    9000  auto/1000
          e0c  Default  Default          up    1500  auto/1000
          e0d  Default  Default          up    1500  auto/1000
          e0e  Default  Default          up    1500  auto/1000
          e0f  Default  Default          up    1500  auto/1000
          e0g  Default  Default          up    1500  auto/1000
   ```

   在此示例中，命令的输出提供了以下信息：

   - 端口 `e0c`， `e0d`， `e0e`， `e0f`，和 `e0g` 在每个节点上、系统会将其分配给默认广播域。
   - 这些端口可能可在要创建的 IP 空间的广播域中使用。

2. 确定默认广播域中的哪些端口已分配给 LIF 接口，因此无法移动到新的广播域。

   ```
   network interface show
   ```

```
          Logical      Status     Network          Current   Current Is
Vserver   Interface    Admin/Oper Address/Mask     Node      Port    Home
-------   ----------   ---------- ------------   --------- -------  ----
Cluster
          node1_clus1  up/up       10.0.2.40/24   node1     e0a     true
          node1_clus2  up/up       10.0.2.41/24   node1     e0b     true
          node2_clus1  up/up       10.0.2.42/24   node2     e0a     true
          node2_clus2  up/up       10.0.2.43/24   node2     e0b     true

cluster1
          cluster_mgmt up/up       10.0.1.41/24   node1     e0c     true
          node1_mgmt   up/up       10.0.1.42/24   node1     e0c     true
          node2_mgmt   up/up       10.0.1.43/24   node2     e0c     true
```

在以下示例中，命令的输出提供了以下信息：

- 节点端口将分配给端口 `e0c` 在每个节点上、并且集群管理LIF的主节点处于打开状态 `e0c` 开启 `node1`。
- 端口 `e0d`， `e0e`， `e0f`，和 `e0g` 在每个节点上、均不托管任何生命周期、可以从默认广播域中删除、然后将其添加到新IP空间的新广播域中。

创建广播域**(ONTAP 9.7**及更早版本**)**

在 ONTAP 9.7 及更早版本中，您可以创建一个广播域，以便对集群中属于同一第 2 层网络的网络端口进行分组。然后， SVM 可以使用这些端口。您必须为自定义 IP 空间创建广播域。在 IP 空间中创建的 SVM 使用广播域中的端口。

此任务与 ONTAP 9.0 - 9.7 相关，而不是与 ONTAP 9.8 相关。

开始之前

您必须是集群管理员才能执行此任务。

从 ONTAP 9.8 开始，在集群创建或加入操作期间会自动创建广播域。如果您运行的是 ONTAP 9.8 或更高版本，则不需要执行这些步骤。

在 ONTAP 9.7 及更早版本中，计划添加到广播域的端口不能属于另一个广播域。

关于此任务

LIF 故障转移到的端口必须是 LIF 故障转移组的成员。创建广播域时， ONTAP 会自动创建同名的故障转移组。故障转移组包含分配给广播域的所有端口。

- 所有广播域名在 IP 空间中必须是唯一的。
- 添加到广播域的端口可以是物理网络端口， VLAN 或接口组（ ifgrp ）。
- 如果要使用的端口属于另一个广播域、但未使用、请使用 `network port broadcast-domain remove-ports` 命令以从现有广播域中删除端口。
- 添加到广播域的端口的 MTU 将更新为在广播域中设置的 MTU 值。

- MTU 值必须与连接到该第 2 层网络的所有设备匹配，但处理管理流量的 e0M 端口除外。
- 如果未指定 IP 空间名称，则会在 " 默认 "IP 空间中创建广播域。

为了简化系统配置，系统会自动创建一个同名的故障转移组，该故障转移组包含相同的端口。

步骤

1. 查看当前未分配给广播域的端口：

   ```
   network port show
   ```

   如果显示屏较大、请使用 `network port show -broadcast-domain` 命令以仅查看未分配的端口。

2. 创建广播域：

   ```
   network port broadcast-domain create -broadcast-domain broadcast_domain_name
   -mtu mtu_value [-ipspace ipspace_name] [-ports ports_list]
   ```

   - *`broadcast_domain_name`* 是要创建的广播域的名称。
   - *`mtu_value`* 是IP数据包的MTU大小；1500和9000是典型值。

     此值将应用于添加到此广播域的所有端口。

   - *`ipspace_name`* 是要将此广播域添加到的IP空间的名称。

     除非为此参数指定值，否则将使用 "Default" IP 空间。

   - *`ports_list`* 是要添加到广播域的端口的列表。

     此时将以格式添加端口 *`node_name:port_number`*，例如， `node1:e0c`。

3. 验证是否已根据需要创建广播域：
   `network port show -instance -broadcast-domain` *`new_domain`*

示例

以下命令会在默认 IP 空间中创建广播域 bcast1 ，将 MTU 设置为 1500 ，并添加四个端口：

```
network port broadcast-domain create -broadcast-domain bcast1 -mtu 1500 -ports
cluster1-01:e0e,cluster1-01:e0f,cluster1-02:e0e,cluster1-02:e0f
```

完成后

您可以通过创建子网来定义广播域中可用的 IP 地址池，也可以此时将 SVM 和接口分配给 IP 空间。有关详细信息，请参见 "集群和 SVM 对等"。

如果需要更改现有广播域的名称、请使用 `network port broadcast-domain rename` 命令：

从广播域添加或删除端口(ONTAP 9.7及更早版本)

您可以在最初创建广播域时添加网络端口，也可以在已存在的广播域中添加或删除端口。这样，您就可以高效地使用集群中的所有端口。

如果要添加到新广播域的端口已位于另一个广播域中，则必须先从该广播域中删除这些端口，然后再将其分配给新广播域。

> 此任务与 ONTAP 9.0 - 9.7 相关，而不是与 ONTAP 9.8 相关。

开始之前

- 您必须是集群管理员才能执行此任务。
- 计划添加到广播域的端口不能属于另一个广播域。
- 不能将已属于接口组的端口单独添加到广播域中。

关于此任务

添加和删除网络端口时，应遵循以下规则：

添加端口时 …	删除端口时 …
端口可以是网络端口， VLAN 或接口组（ ifgrp ）。	不适用
这些端口将添加到广播域的系统定义的故障转移组中。	端口将从广播域中的所有故障转移组中删除。
端口的 MTU 将更新为广播域中设置的 MTU 值。	端口的 MTU 不变。
端口的 IP 空间将更新为广播域的 IP 空间值。	这些端口将移至 " 默认 "IP 空间，而不具有广播域属性。

> 如果使用删除接口组的最后一个成员端口 `network port ifgrp remove-port` 命令中、则会导致接口组端口从广播域中删除、因为广播域中不允许使用空接口组端口。

步骤

1. 使用显示当前已分配或未分配给广播域的端口 `network port show` 命令：
2. 在广播域中添加或删除网络端口：

如果您要 …	使用 …
向广播域添加端口	`network port broadcast-domain add-ports`
从广播域中删除端口	`network port broadcast-domain remove-ports`

3. 验证是否已在广播域中添加或删除端口：

```
network port show
```

有关这些命令的详细信息，请参见 "ONTAP 9 命令"。

添加和删除端口的示例

以下命令会将节点 cluster-1-01 上的端口 e0g 和节点 cluster-1-02 上的端口 e0g 添加到默认 IP 空间中的广播域 bcast1 ：

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain bcast1
```

```
-ports cluster-1-01:e0g,cluster1-02:e0g
```

以下命令会将两个集群端口添加到集群 IP 空间中的广播域集群：

```
cluster-1::> network port broadcast-domain add-ports -broadcast-domain Cluster
-ports cluster-2-03:e0f,cluster2-04:e0f -ipspace Cluster
```

以下命令将从默认 IP 空间的广播域 bcast1 中删除节点 cluster1-01 上的端口 e0e：

```
cluster-1::> network port broadcast-domain remove-ports -broadcast-domain bcast1
-ports cluster-1-01:e0e
```

拆分广播域**(ONTPA 9.7**或更早版本**)**

您可以通过将现有广播域拆分为两个不同的广播域来修改该广播域，每个广播域包含分配给原始广播域的一些原始端口。

关于此任务

- 如果端口位于故障转移组中，则必须拆分故障转移组中的所有端口。
- 如果端口具有关联的 LIF ，则 LIF 不能属于子网范围。

步骤

将广播域拆分为两个广播域：

```
network port broadcast-domain split -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -new-broadcast-domain
<broadcast_domain_name> -ports <node:port,node:port>
```

- `ipspace_name` 是广播域所在IP空间的名称。
- `-broadcast-domain` 是要拆分的广播域的名称。
- `-new-broadcast-domain` 是要创建的新广播域的名称。
- `-ports` 是要添加到新广播域的节点名称和端口。

合并广播域**(ONTAP 9.7**及更早版本**)**

您可以使用 merge 命令将所有端口从一个广播域移动到现有广播域。

如果要从广播域中删除所有端口，然后将这些端口添加到现有广播域，则此操作会减少所需的步骤。

步骤

将一个广播域中的端口合并到现有广播域中：

```
network port broadcast-domain merge -ipspace <ipspace_name> -broadcast
-domain <broadcast_domain_name> -into-broadcast-domain
<broadcast_domain_name>
```

- `ipspace_name` 是广播域所在IP空间的名称。
- `-broadcast-domain` 是要合并的广播域的名称。
- `-into-broadcast-domain` 是将接收其他端口的广播域的名称。

示例

以下示例将广播域 bd-data1 合并到广播域 bd-data2 中：

```
network port -ipspace Default broadcast-domain bd-data1 into-broadcast-domain bd-
data2
```

更改广播域中端口的**MTU**值**(ONTAP 9.7**及更早版本**)**

您可以修改广播域的 MTU 值，以更改该广播域中所有端口的 MTU 值。这样可以支持在网络中进行的拓扑更改。

开始之前

MTU 值必须与连接到该第 2 层网络的所有设备匹配，但处理管理流量的 e0M 端口除外。

关于此任务

更改 MTU 值会导致受影响端口上的流量短暂中断。系统将显示一条提示，提示您必须使用 y 进行问题解答才能进行 MTU 更改。

步骤

更改广播域中所有端口的 MTU 值：

```
network port broadcast-domain modify -broadcast-domain
<broadcast_domain_name> -mtu <mtu_value> [-ipspace <ipspace_name>]
```

- `broadcast_domain` 是广播域的名称。
- `mtu` 是IP数据包的MTU大小；1500和9000是典型值。
- `ipspace` 是此广播域所在IP空间的名称。除非为此选项指定值，否则将使用 "Default" IP 空间。以下命令会将广播域 bcast1 中所有端口的 MTU 更改为 9000：

```
network port broadcast-domain modify -broadcast-domain <Default-1> -mtu <
9000 >
Warning: Changing broadcast domain settings will cause a momentary data-
serving interruption.
Do you want to continue? {y|n}: <y>
```

显示广播域(**ONTAP 9.7**及更早版本)

您可以显示集群中每个 IP 空间内的广播域列表。输出还会显示每个广播域的端口列表和 MTU 值。

步骤

显示集群中的广播域和关联端口：

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

以下命令显示集群中的所有广播域和关联端口：

```
network port broadcast-domain show
IPspace Broadcast                                 Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  --------------------- --------------
Cluster Cluster      9000
                           cluster-1-01:e0a       complete
                           cluster-1-01:e0b       complete
                           cluster-1-02:e0a       complete
                           cluster-1-02:e0b       complete
Default Default      1500
                           cluster-1-01:e0c       complete
                           cluster-1-01:e0d       complete
                           cluster-1-02:e0c       complete
                           cluster-1-02:e0d       complete
        bcast1       1500
                           cluster-1-01:e0e       complete
                           cluster-1-01:e0f       complete
                           cluster-1-01:e0g       complete
                           cluster-1-02:e0e       complete
                           cluster-1-02:e0f       complete
                           cluster-1-02:e0g       complete
```

以下命令显示 bcast1 广播域中更新状态为 error 的端口，这表示端口无法正确更新：

```
network port broadcast-domain show -broadcast-domain bcast1 -port-update
-status error

IPspace Broadcast                                  Update
Name    Domain Name  MTU   Port List              Status Details
------- ----------- -----  ---------------------- --------------
Default bcast1       1500
                            cluster-1-02:e0g       error
```

有关详细信息，请参见 "ONTAP 9 命令"。

删除广播域

如果您不再需要广播域，可以将其删除。此操作会将与此广播域关联的端口移至 " 默认 "IP 空间。

开始之前

不能存在与要删除的广播域关联的子网，网络接口或 SVM 。

关于此任务

- 无法删除系统创建的 " 集群 " 广播域。
- 删除此广播域时，系统会删除与此广播域相关的所有故障转移组。

您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

从**ONTAP 9.12.0**开始、您可以使用**System Manager**删除广播域

如果广播域包含端口或与子网关联、则不会显示删除选项。

步骤

1. 选择*网络>概述>广播域*。
2. 选择 … ⋮ 要删除的广播域旁边的*>删除*。

命令行界面

使用命令行界面删除广播域

步骤

删除广播域：

```
network port broadcast-domain delete -broadcast-domain broadcast_domain_name
[-ipspace ipspace_name]
```

以下命令将删除 IP 空间 ipspace1 中的广播域 Default-1：

```
network port broadcast-domain delete -broadcast-domain Default-1 -ipspace
ipspace1
```

故障转移组和策略

LIF故障转移概述

LIF 故障转移是指在 LIF 的当前端口发生链路故障时， LIF 自动迁移到其他网络端口。这是为 SVM 连接提供高可用性的一个关键组件。配置 LIF 故障转移包括创建故障转移组，修改 LIF 以使用故障转移组以及指定故障转移策略。

故障转移组包含一组来自集群中一个或多个节点的网络端口（物理端口， VLAN 和接口组）。故障转移组中的网络端口定义了可用于 LIF 的故障转移目标。可以为故障转移组分配集群管理，节点管理，集群间和 NAS 数据 LIF 。

> 如果在配置 LIF 时没有有效的故障转移目标，则在 LIF 尝试进行故障转移时会发生中断。您可以使用 "network interface show -failover" 命令验证故障转移配置。

创建广播域时，系统会自动创建一个同名的故障转移组，该故障转移组包含相同的网络端口。此故障转移组由系统自动管理，这意味着在从广播域添加或删除端口时，这些端口会自动添加或从此故障转移组中删除。对于不想管理自己的故障转移组的管理员来说，这是一种效率。

创建故障转移组

您可以创建网络端口的故障转移组，以便在 LIF 的当前端口发生链路故障时， LIF 可以自动迁移到其他端口。这样，系统就可以将网络流量重新路由到集群中的其他可用端口。

关于此任务

您可以使用 `network interface failover-groups create` 命令以创建组并向组中添加端口。

- 添加到故障转移组的端口可以是网络端口， VLAN 或接口组（ ifgrp ）。
- 添加到故障转移组的所有端口必须属于同一广播域。
- 一个端口可以驻留在多个故障转移组中。
- 如果 LIF 位于不同的 VLAN 或广播域中，则必须为每个 VLAN 或广播域配置故障转移组。
- 故障转移组不适用于 SAN iSCSI 或 FC 环境。

步骤

创建故障转移组：

```
network interface failover-groups create -vserver vserver_name -failover-group
failover_group_name -targets ports_list
```

- *`vserver_name`* 是可使用故障转移组的SVM的名称。
- *`failover_group_name`* 是要创建的故障转移组的名称。
- *`ports_list`* 是要添加到故障转移组的端口列表。
  添加的端口格式为 *node_name*>： <*port_number*> ，例如 node1： e0c 。

以下命令将为 SVM vs3 创建故障转移组 fg3 并添加两个端口：

```
network interface failover-groups create -vserver vs3 -failover-group fg3
-targets cluster1-01:e0e,cluster1-02:e0e
```

完成后

- 既然已创建故障转移组，您应将此故障转移组应用于 LIF 。
- 如果应用的故障转移组不能为 LIF 提供有效的故障转移目标，则会显示一条警告消息。

  如果没有有效故障转移目标的 LIF 尝试进行故障转移，可能会发生中断。

在 **LIF** 上配置故障转移设置

您可以通过将故障转移策略和故障转移组应用于 LIF 来将 LIF 配置为故障转移到一组特定的网络端口。您还可以禁止 LIF 故障转移到其他端口。

关于此任务

- 创建 LIF 时，默认情况下会启用 LIF 故障转移，可用目标端口的列表由默认故障转移组和故障转移策略根据 LIF 类型和服务策略确定。

  从 9.5 开始，您可以为 LIF 指定一个服务策略，用于定义可以使用 LIF 的网络服务。某些网络服务会对 LIF 实施故障转移限制。

  ⓘ 如果更改 LIF 的服务策略以进一步限制故障转移，则系统会自动更新 LIF 的故障转移策略。

- 您可以通过在 network interface modify 命令中为 -failover-group 和 -failover-policy 参数指定值来修改 LIF 的故障转移行为。
- 修改 LIF 后，如果 LIF 没有有效的故障转移目标，则会显示一条警告消息。

  如果没有有效故障转移目标的 LIF 尝试进行故障转移，可能会发生中断。

- 从ONTAP 9.11.1开始、在纯闪存SAN阵列(ASA)平台上、系统会在新创建的Storage VM上新创建的iSCSI LIF上自动启用iSCSI LIF故障转移。

  此外，您还可以 "在已有iSCSI LIF上手动启用iSCSI LIF故障转移"，表示在升级到ONTAP 9.11.1或更高版本之前创建的LUN。

- 以下列表介绍了 -failover-policy 设置如何影响从故障转移组中选择的目标端口：

> 对于iSCSI LIF故障转移、仅限故障转移策略 `local-only`， `sfo-partner-only` 和 `disabled` 受支持。

- `broadcast-domain-wide` 适用场景故障转移组中所有节点上的所有端口。
- `system-defined` 仅适用场景LIF主节点和集群中另一个节点上的端口、如果存在、通常为非SFR配对节点。
- `local-only` 仅适用场景LIF主节点上的端口。
- `sfo-partner-only` 仅适用场景LIF主节点及其SFo配对节点上的端口。
- `disabled` 表示没有为LIF配置故障转移。

步骤

为现有接口配置故障转移设置：

```
network interface modify -vserver <vserver_name> -lif <lif_name> -failover
-policy <failover_policy> -failover-group <failover_group>
```

配置故障转移设置和禁用故障转移的示例

以下命令会将故障转移策略设置为 broadcast-domain-wide ，并使用故障转移组 fg3 中的端口作为 SVM vs3 上 LIF data1 的故障转移目标：

```
network interface modify -vserver vs3 -lif data1 failover-policy
broadcast-domain-wide - failover-group fg3

network interface show -vserver vs3 -lif * -fields failover-
group,failover-policy

vserver lif              failover-policy       failover-group
------- -------------- ---------------        --------------
vs3     data1           broadcast-domain-wide  fg3
```

以下命令将对 SVM vs3 上的 LIF data1 禁用故障转移：

```
network interface modify -vserver vs3 -lif data1 failover-policy disabled
```

用于管理故障转移组和策略的命令

您可以使用 `network interface failover-groups` 用于管理故障转移组的命令。您可以使用 `network interface modify` 命令以管理应用于LIF的故障转移组和故障转移策略。

如果您要 ...	使用此命令 ...
将网络端口添加到故障转移组	`network interface failover-groups add-targets`
从故障转移组中删除网络端口	`network interface failover-groups remove-targets`
修改故障转移组中的网络端口	`network interface failover-groups modify`
显示当前故障转移组	`network interface failover-groups show`
在 LIF 上配置故障转移	`network interface modify -failover -group -failover-policy`
显示每个 LIF 正在使用的故障转移组和故障转移策略	`network interface show -fields failover-group, failover-policy`
重命名故障转移组	`network interface failover-groups rename`
删除故障转移组	`network interface failover-groups delete`

> 如果修改故障转移组，使其无法为集群中的任何 LIF 提供有效的故障转移目标，则可能会在 LIF 尝试进行故障转移时导致中断。

有关详细信息、请参见的手册页 `network interface failover-groups` 和 `network interface modify` 命令

子网(仅限集群管理员)

子网概述

通过子网，您可以为 ONTAP 网络配置分配特定的 IP 地址块或池。这样、您就可以通过指定子网名称而无需指定IP地址和网络掩码值来更轻松地创建LIF。

子网是在广播域中创建的，它包含属于同一第 3 层子网的 IP 地址池。创建 LIF 时，子网中的 IP 地址会分配给广播域中的端口。删除 LIF 后， IP 地址将返回到子网池，并可用于未来的 LIF 。

建议您使用子网，因为子网可以更轻松地管理 IP 地址，并简化 LIF 的创建过程。此外，如果在定义子网时指定了网关，则在使用该子网创建 LIF 时，指向该网关的默认路由会自动添加到 SVM 中。

创建子网

您可以创建子网来分配特定的IPv4或IPv6地址块、以便稍后在为SVM创建LIF时使用。

这样，您就可以通过指定子网名称，而不必为每个 LIF 指定 IP 地址和网络掩码值来更轻松地创建 LIF 。

开始之前

您必须是集群管理员才能执行此任务。

要添加子网的广播域和 IP 空间必须已存在。

关于此任务

- 所有子网名称在 IP 空间中必须是唯一的。
- 在将 IP 地址范围添加到子网时，您必须确保网络中没有重叠的 IP 地址，以便不同的子网或主机不会尝试使用相同的 IP 地址。
- 如果在定义子网时指定了网关，则在使用该子网创建 LIF 时，指向该网关的默认路由会自动添加到 SVM 中。如果不使用子网、或者在定义子网时未指定网关、则需要使用 `route create` 命令以手动向SVM添加路由。

操作步骤

您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

从ONTAP 9.12.0开始、您可以使用System Manager创建子网。

步骤

1. 选择*网络>概述>子网*。
2. 单击 + Add 以创建子网。
3. 为子网命名。
4. 指定子网IP地址。
5. 设置子网掩码。
6. 定义构成子网的IP地址范围。
7. 如果有用、请指定网关。
8. 选择子网所属的广播域。
9. 保存所做的更改。
   a. 如果输入的IP地址或范围已被某个接口使用、则会显示以下消息：
      `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. 单击*确定*后、现有LIF将与子网关联。

命令行界面

使用命令行界面创建子网。

```
network subnet create -subnet-name subnet_name -broadcast-domain
<broadcast_domain_name> [- ipspace <ipspace_name>] -subnet
<subnet_address> [-gateway <gateway_address>] [-ip-ranges
<ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` 是要创建的第3层子网的名称。

  此名称可以是 "Mgmt " 等文本字符串，也可以是 192.0.2.0/24 等特定子网 IP 值。

- `broadcast_domain_name` 是子网所在广播域的名称。
- `ipspace_name` 是广播域所属IP空间的名称。

  除非为此选项指定值，否则将使用 "Default" IP 空间。

- `subnet_address` 是子网的IP地址和掩码；例如192.0.2.0/24。
- `gateway_address` 是子网默认路由的网关；例如192.0.2.1。
- `ip_address_list` 是要分配给子网的IP地址的列表或范围。

  IP 地址可以是单个地址， IP 地址范围或逗号分隔列表中的组合。

- 值 `true` 可以为设置 `-force-update-lif-associations` 选项

  如果任何服务处理器或网络接口当前正在使用指定范围内的 IP 地址，则此命令将失败。如果将此值设置为 true ，则会将任何手动寻址的接口与当前子网相关联，并允许命令成功执行。

以下命令将在默认 IP 空间的广播域 Default-1 中创建子网 sub1 。它会添加 IPv4 子网 IP 地址和掩码，网关以及一系列 IP 地址：

```
network subnet create -subnet-name sub1 -broadcast-domain Default-1
-subnet 192.0.2.0/24 - gateway 192.0.2.1 -ip-ranges 192.0.2.1-
192.0.2.100, 192.0.2.122
```

以下命令将在 "Default" IP 空间的广播域 Default 中创建子网 sub2 。它会添加一系列 IPv6 地址：

```
network subnet create -subnet-name sub2 -broadcast-domain Default
-subnet 3FFE::/64 - gateway 3FFE::1 -ip-ranges "3FFE::10-3FFE::20"
```

完成后

您可以使用子网中的地址将 SVM 和接口分配给 IP 空间。

如果需要更改现有子网的名称、请使用 `network subnet rename` 命令：

在子网中添加或删除 **IP** 地址

您可以在最初创建子网时添加 IP 地址，也可以将 IP 地址添加到已存在的子网中。您还可以从现有子网中删除 IP 地址。这样，您就可以仅为 SVM 分配所需的 IP 地址。

您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

从**ONTAP 9.12.0**开始、您可以使用**System Manager**在子网中添加或删除**IP**地址

步骤

1. 选择*网络>概述>子网*。
2. 选择 … ⋮ 要更改的子网旁边的*>编辑*。
3. 添加或删除IP地址。
4. 保存所做的更改。
   a. 如果输入的IP地址或范围已被某个接口使用、则会显示以下消息：
      `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. 单击*确定*后、现有LIF将与子网关联。

命令行界面

使用命令行界面在子网中添加或删除**IP**地址

关于此任务

添加 IP 地址时，如果任何服务处理器或网络接口正在使用所添加范围内的 IP 地址，则会收到错误。如果要将任何手动寻址的接口与当前子网关联、可以设置 `-force-update-lif-associations` 选项 `true`。

删除 IP 地址时，如果任何服务处理器或网络接口正在使用要删除的 IP 地址，则会收到错误。如果您希望接口在从子网中删除IP地址后继续使用这些地址、则可以设置 `-force-update-lif-associations` 选项 `true`。

步骤

在子网中添加或删除 IP 地址：

如果您要 …	使用此命令 …
将 IP 地址添加到子网	网络子网添加范围
从子网中删除 IP 地址	网络子网删除范围

有关这些命令的详细信息，请参见手册页。

以下命令会将 IP 地址 192.0.2.82 到 192.0.2.85 添加到子网 sub1：

```
network subnet add-ranges -subnet-name <sub1> -ip-ranges <192.0.2.82-192.0.2.85>
```

以下命令从子网 sub3 中删除 IP 地址 198.51.100.9：

```
network subnet remove-ranges -subnet-name <sub3> -ip-ranges
<198.51.100.9>
```

如果当前范围包括 1 到 10 以及 20 到 40 ，并且您要添加 11 到 19 以及 41 到 50 （基本上允许 1 到 50 ），则可以使用以下命令重叠现有地址范围。此命令仅添加新地址，不会影响现有地址：

```
network subnet add-ranges -subnet-name <sub3> -ip-ranges <198.51.10.1-
198.51.10.50>
```

更改子网属性

您可以更改现有子网中的子网地址和掩码值，网关地址或 IP 地址范围。

关于此任务

- 修改 IP 地址时，必须确保网络中的 IP 地址不重叠，以便不同的子网或主机不会尝试使用相同的 IP 地址。
- 如果添加或更改网关 IP 地址，则在使用子网在新 SVM 中创建 LIF 时，修改后的网关将应用于这些 SVM 。如果 SVM 还不存在网关的默认路由，则会为该路由创建。更改网关 IP 地址时，您可能需要手动向 SVM 添加新路由。

您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

从**ONTAP 9.12.0**开始、您可以使用**System Manager**更改子网属性

步骤

1. 选择*网络>概述>子网*。
2. 选择 … ⋮要更改的子网旁边的*>编辑*。
3. 进行更改。
4. 保存所做的更改。
   a. 如果输入的IP地址或范围已被某个接口使用、则会显示以下消息：
      `An IP address in this range is already in use by a LIF. Associate the LIF with this subnet?`
   b. 单击*确定*后、现有LIF将与子网关联。

命令行界面

使用命令行界面更改子网属性

步骤

修改子网属性：

```
network subnet modify -subnet-name <subnet_name> [-ipspace
<ipspace_name>] [-subnet <subnet_address>] [-gateway <gateway_address>]
[-ip-ranges <ip_address_list>] [-force-update-lif-associations <true>]
```

- `subnet_name` 是要修改的子网的名称。
- `ipspace` 是子网所在IP空间的名称。
- `subnet` 是子网的新地址和掩码(如果适用)；例如192.0.2.0/24。
- `gateway` 是子网的新网关(如果适用)；例如192.0.2.1。输入 * "* 将删除网关条目。
- `ip_ranges` 是要分配给子网的IP地址的新列表或范围(如果适用)。IP 地址可以是单个地址，范围或 IP 地址，也可以是逗号分隔列表中的组合。此处指定的范围将替换现有 IP 地址。
- `force-update-lif-associations` 更改IP地址范围时需要。修改 IP 地址范围时，可以将此选项的值设置为 * true * 。如果任何服务处理器或网络接口使用指定范围内的 IP 地址，则此命令将失败。如果将此值设置为 * true * ，则会将任何手动寻址的接口与当前子网相关联，并允许命令成功执行。

以下命令修改子网 sub3 的网关 IP 地址：

```
network subnet modify -subnet-name <sub3> -gateway <192.0.3.1>
```

显示子网

您可以显示分配给 IP 空间中每个子网的 IP 地址列表。输出还会显示每个子网中可用的 IP

地址总数以及当前正在使用的地址数。

您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

从**ONTAP 9.12.0**开始、您可以使用**System Manager**显示子网

步骤

1. 选择*网络>概述>子网*。
2. 查看子网列表。

命令行界面

使用命令行界面显示子网

步骤

显示子网列表以及这些子网中使用的关联 IP 地址范围：

```
network subnet show
```

以下命令显示子网和子网属性：

```
network subnet show

IPspace: Default
Subnet                  Broadcast                Avail/
Name   Subnet           Domain    Gateway        Total   Ranges
-----  --------------- --------- ------------ --------
-----------------------
sub1   192.0.2.0/24     bcast1   192.0.2.1     5/9     192.0.2.92-
192.0.2.100
sub3   198.51.100.0/24  bcast3   198.51.100.1   3/3
198.51.100.7,198.51.100.9
```

删除子网

如果您不再需要子网，并希望取消分配分配给该子网的 IP 地址，可以将其删除。

您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

从**ONTAP 9.12.0**开始、您可以使用**System Manager**删除子网

步骤

1. 选择*网络>概述>子网*。
2. 选择 … ⋮ 要删除的子网旁边的*> Delete*。
3. 保存所做的更改。

命令行界面

使用命令行界面删除子网

关于此任务

如果任何服务处理器或网络接口当前正在使用指定范围内的 IP 地址，则会收到错误消息。如果您希望接口在删除子网后仍继续使用 IP 地址，则可以将 -force-update-lif-associations 选项设置为 true ，以删除子网与 LIF 的关联。

步骤

删除子网：

```
network subnet delete -subnet-name subnet_name [-ipspace ipspace_name] [-
force-update-lif- associations true]
```

以下命令将删除 IP 空间 ipspace1 中的子网 sub1 ：

```
network subnet delete -subnet-name sub1 -ipspace ipspace1
```

创建 SVM

您必须创建 SVM 以向客户端提供数据。

开始之前

- 您必须是集群管理员才能执行此任务。
- 您必须知道 SVM 根卷将采用哪种安全模式。

  如果您计划在此 SVM 上通过 SMB 解决方案实施 Hyper-V 或 SQL Server ，则应对根卷使用 NTFS 安全模式。包含 Hyper-V 文件或 SQL 数据库文件的卷在创建时必须设置为 NTFS 安全性。通过将根卷安全模式设置为 NTFS ，您可以确保不会无意中创建 UNIX 或混合安全模式数据卷。

- 从ONTAP 9.13.1开始、您可以为Storage VM设置最大容量。您还可以在SVM接近阈值容量级别时配置警报。有关详细信息，请参见 管理SVM容量。

System Manager

您可以使用System Manager创建Storage VM。

步骤

1. 选择*存储VM*。
2. 单击 + Add 创建Storage VM。
3. 为Storage VM命名。
4. 选择访问协议：
    - SMB/CIFS、NFS
    - iSCSI
    - FC
    - NVMe
        i. 如果选择*启用SMB/CIFS*、请完成以下配置：

字段或复选框	Description
管理员名称	指定SMB/CIFS Storage VM的管理员用户名。
Password	指定SMB/CIFS Storage VM的管理员密码。
服务器名称	指定SMB/CIFS Storage VM的服务器名称。
Active Directory域	指定用于为SMB/CIFS Storage VM提供用户身份验证的Active Directory域。
组织单位	指定Active Directory域中与SMB/CIFS服务器关联的组织单位。"cn=compones"是默认值、可以进行修改。
访问Storage VM中的共享时对数据进行加密	选中此复选框可使用SMB 3.0对数据进行加密、以防止未经授权访问SMB/CIFS Storage VM中的共享上的文件。
域	为SMB/CIFS Storage VM添加、删除或重新排列列出的域。
名称服务器	添加、删除SMB/CIFS Storage VM的名称服务器或对其重新排序。
默认语言	指定Storage VM及其卷的默认语言编码设置。使用命令行界面更改Storage VM中各个卷的设置。

网络接口	对于为Storage VM配置的每个网络接口、请选择一个现有子网(如果至少存在一个子网)或指定*不使用子网*并填写* IP地址*和*子网掩码*字段。 如果有用、请选中*对以下所有接口使用相同的子网掩码和网关*复选框。 您可以允许系统自动选择主端口、也可以从列表中手动选择要使用的端口。
管理管理员帐户	如果要管理Storage VM管理员帐户、请选中此复选框。选中后、指定用户名、密码、确认密码并指示是否要添加用于Storage VM管理的网络接口。

1. 如果选择*启用NFS*、请完成以下配置：

字段或复选框	Description
允许NFS客户端访问复选框	如果在NFS Storage VM上创建的所有卷都应使用根卷路径"/"进行挂载和遍历、请选中此复选框。向导出策略"default"添加规则、以允许无中断挂载遍历。
rules	单击 + Add 以创建规则。 • 客户端规范：指定主机名、IP地址、网络组或域。 • 访问协议：选择以下选项的组合： ◦ SMB/CIFS ◦ FlexCache ◦ NFS ▪ NFSv3 ▪ NFSv4 • 访问详细信息：对于每种类型的用户、指定访问级别：只读、读/写或超级用户。用户类型包括： ◦ 全部 ◦ 全部(以匿名用户身份) ◦ "unix" ◦ Kerberos 5. ◦ Kerberos 5i ◦ Kerberos 5p ◦ NTLM 保存规则。

默认语言	指定Storage VM及其卷的默认语言编码设置。使用命令行界面更改Storage VM中各个卷的设置。
网络接口	对于为Storage VM配置的每个网络接口、请选择一个现有子网(如果至少存在一个子网)或指定*不使用子网*并填写* IP地址*和*子网掩码*字段。 如果有用、请选中*对以下所有接口使用相同的子网掩码和网关*复选框。 您可以允许系统自动选择主端口、也可以从列表中手动选择要使用的端口。
管理管理员帐户	如果要管理Storage VM管理员帐户、请选中此复选框。选中后、指定用户名、密码、确认密码并指示是否要添加用于Storage VM管理的网络接口。

1. 如果选择*启用iSCSI*、请完成以下配置：

字段或复选框	Description
网络接口	对于为Storage VM配置的每个网络接口、请选择一个现有子网(如果至少存在一个子网)或指定*不使用子网*并填写* IP地址*和*子网掩码*字段。 如果有用、请选中*对以下所有接口使用相同的子网掩码和网关*复选框。 您可以允许系统自动选择主端口、也可以从列表中手动选择要使用的端口。
管理管理员帐户	如果要管理Storage VM管理员帐户、请选中此复选框。选中后、指定用户名、密码、确认密码并指示是否要添加用于Storage VM管理的网络接口。

1. 如果选择*Enable FC*，请完成以下配置：

字段或复选框	Description
配置FC端口	选择要包含在Storage VM中的节点上的网络接口。建议每个节点使用两个网络接口。
管理管理员帐户	如果要管理Storage VM管理员帐户、请选中此复选框。选中后、指定用户名、密码、确认密码并指示是否要添加用于Storage VM管理的网络接口。

1. 如果选择*启用NVMe/FC*、请完成以下配置：

字段或复选框	Description

配置FC端口	选择要包含在Storage VM中的节点上的网络接口。建议每个节点使用两个网络接口。
管理管理员帐户	如果要管理Storage VM管理员帐户、请选中此复选框。选中后、指定用户名、密码、确认密码并指示是否要添加用于Storage VM管理的网络接口。

1. 如果选择*启用NVMe/tcp*、请完成以下配置：

字段或复选框	Description
网络接口	对于为Storage VM配置的每个网络接口、请选择一个现有子网(如果至少存在一个子网)或指定*不使用子网*并填写* IP地址*和*子网掩码*字段。 如果有用、请选中*对以下所有接口使用相同的子网掩码和网关*复选框。 您可以允许系统自动选择主端口、也可以从列表中手动选择要使用的端口。
管理管理员帐户	如果要管理Storage VM管理员帐户、请选中此复选框。选中后、指定用户名、密码、确认密码并指示是否要添加用于Storage VM管理的网络接口。

1. 保存所做的更改。

命令行界面

使用ONTAP 命令行界面创建子网。

步骤

1. 确定哪些聚合是包含 SVM 根卷的候选聚合。

   ```
   storage aggregate show -has-mroot false
   ```

   您必须选择至少具有 1 GB 可用空间的聚合来容纳根卷。如果要在 SVM 上配置 NAS 审核，则根聚合上必须至少有 3 GB 的额外可用空间，并在启用审核时使用额外空间来创建审核暂存卷。

   > 如果已在现有 SVM 上启用 NAS 审核，则聚合的暂存卷将在成功创建聚合后立即创建。

2. 记录要在其中创建 SVM 根卷的聚合的名称。
3. 如果您计划在创建 SVM 时指定语言，但不知道要使用的值，请确定并记录要指定的语言值：

   ```
   vserver create -language ?
   ```

4. 如果您计划在创建 SVM 时指定 Snapshot 策略，但不知道该策略的名称，请列出可用策略并确定并记录要使用的 Snapshot 策略的名称：

   ```
   volume snapshot policy show -vserver vserver_name
   ```

5. 如果您计划在创建 SVM 时指定配额策略，但不知道该策略的名称，请列出可用策略并确定并记录要使用的配额策略的名称：

   ```
   volume quota policy show -vserver vserver_name
   ```

6. 创建 SVM：

   ```
   vserver create -vserver vserver_name -aggregate aggregate_name -rootvolume
   root_volume_name -rootvolume-security-style {unix|ntfs|mixed} [-ipspace
   IPspace_name] [-language <language>] [-snapshot-policy
   snapshot_policy_name] [-quota-policy quota_policy_name] [-comment comment]
   ```

   ```
   vserver create -vserver vs1 -aggregate aggr3 -rootvolume vs1_root
   -rootvolume-security-style ntfs -ipspace ipspace1 -language
   en_US.UTF-8
   ```

   ```
   [Job 72] Job succeeded: Vserver creation completed
   ```

7. 验证 SVM 配置是否正确。

   ```
   vserver show -vserver vs1
   ```

   ```
   Vserver: vs1
   Vserver Type: data
   Vserver Subtype: default
   Vserver UUID: 11111111-1111-1111-1111-111111111111
   Root Volume: vs1_root
   Aggregate: aggr3
   NIS Domain: -
   Root Volume Security Style: ntfs
   LDAP Client: -
   Default Volume Language Code: en_US.UTF-8
   Snapshot Policy: default
   Comment:
   Quota Policy: default
   List of Aggregates Assigned: -
   Limit on Maximum Number of Volumes allowed: unlimited
   Vserver Admin State: running
   Vserver Operational State: running
   Vserver Operational State Stopped Reason: -
   Allowed Protocols: nfs, cifs, ndmp
   Disallowed Protocols: fcp, iscsi
   QoS Policy Group: -
   Config Lock: false
   IPspace Name: ipspace1
   Is Vserver Protected: false
   ```

在此示例中，命令会在 IP 空间 "ipspace1" 中创建名为 "VS1" 的 SVM 。根卷名为 vs1_root ，并在 aggr3 上使用 NTFS 安全模式创建。

从ONTAP 9.13.1开始、您可以设置自适应QoS策略组模板、以便为SVM中的卷应用吞吐量下限和上限限制。只有在创建SVM之后、才能应用此策略。要了解有关此过程的更多信息、请参见 设置自适应策略组模板。

逻辑接口（LIF）

LIF概述

配置文件配置概览

LIF （逻辑接口）表示集群中某个节点的网络访问点。您可以在集群通过网络发送和接收通信的端口上配置 LIF 。

集群管理员可以创建，查看，修改，迁移，还原， 或删除 LIF 。SVM 管理员只能查看与 SVM 关联的 LIF 。

LIF 是指具有相关特征的 IP 地址或 WWPN ，例如服务策略，主端口，主节点，故障转移到的端口列表以及防火墙策略。您可以在集群通过网络发送和接收通信的端口上配置 LIF 。

从ONTAP 9.10.1开始、防火墙策略已弃用、并完全替换为LIF服务策略。有关详细信息，请参见 "为 LIF 配置防火墙策略"。

LIF 可以托管在以下端口上：

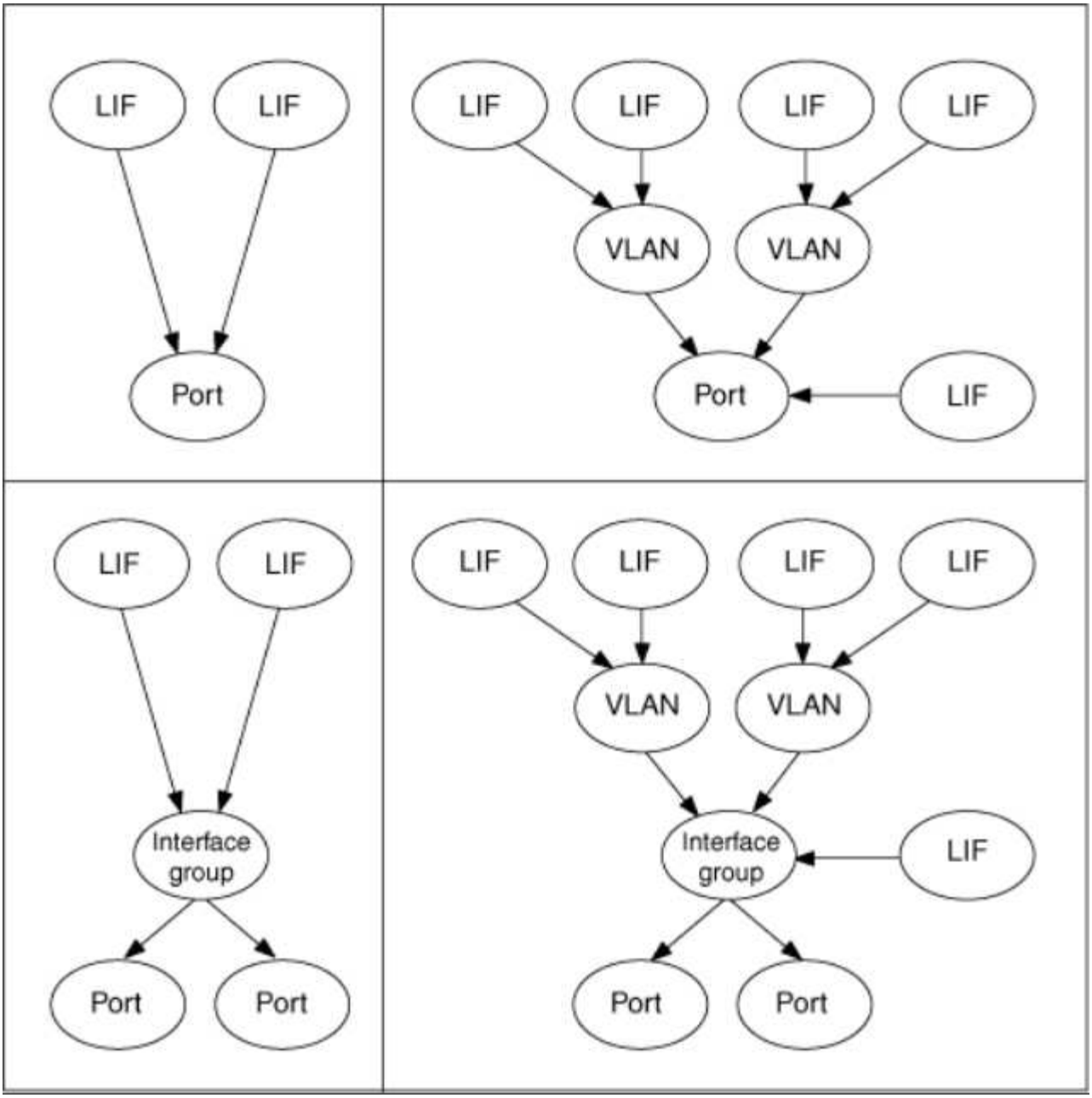
- 不属于接口组的物理端口
- 接口组
- VLAN
- 托管 VLAN 的物理端口或接口组
- 虚拟 IP （ VIP ）端口

  从 ONTAP 9.5 开始，支持 VIP LIF 并托管在 VIP 端口上。

在 LIF 上配置 FC 等 SAN 协议时，它将与 WWPN 关联。

"SAN 管理"

下图显示了 ONTAP 系统中的端口层次结构：



LIF故障转移和恢复

当LIF从其主节点或端口移至其HA配对节点或端口时、会发生LIF故障转移。LIF故障转移可以由ONTAP自动触发、也可以由集群管理员手动触发、以处理某些事件、例如物理以太网链路断开或节点退出复制的数据库(RDB)仲裁。发生LIF故障转移时、ONTAP会继续在配对节点上正常运行、直到故障转移的原因得以解决为止。当主节点或端口恢复运行状况时、LIF将从HA配对节点还原回其主节点或端口。 此恢复称为"恢复"。

对于LIF故障转移和恢复、每个节点的端口都需要属于同一广播域。要检查每个节点上的相关端口是否属于同一广播域、请参见以下内容：

- ONTAP 9.8及更高版本： "修复端口可访问性"
- ONTAP 9.7及更早版本： "在广播域中添加或删除端口"

对于已启用LIF故障转移(自动或手动)的LIF、以下情况适用：

- 对于使用数据服务策略的生命周期、您可以检查故障转移策略限制：
  - ONTAP 9.6及更高版本： "ONTAP 9.6 及更高版本中的 LIF 和服务策略"
  - ONTAP 9.5及更早版本： "ONTAP 9.5 及更早版本中的 LIF 角色"
- 如果将自动还原设置为、则会自动还原此项 `true` 以及LIF的主端口运行状况良好且能够托管LIF的情况。
- 在计划内或计划外节点接管时、被接管节点上的LIF将故障转移到HA配对节点。LIF故障转移所使用的端口由VIF Manager确定。
- 故障转移完成后、LIF将正常运行。
- 启动交还后、如果将自动还原设置为、则LIF将还原回其主节点和端口 `true`。
- 如果托管一个或多个BIF的端口上的以太网链路发生故障、则VIF Manager会将此BIF从已关闭的端口迁移到同一广播域中的其他端口。新端口可以位于同一节点或其HA配对节点中。如果将自动还原设置为、则在还原链路后执行此操作 `true`、则VIF Manager会将这些IF还原回其主节点和主端口。
- 当某个节点退出复制的数据库(RDB)仲裁时、VIF Manager会将此脱离仲裁节点的生命周期迁移到其HA配对节点。在节点恢复仲裁后、如果将自动还原设置为 `true`、则VIF Manager会将这些IF还原回其主节点和主端口。

LIF 与端口类型的兼容性

LIF 可以具有不同的特性来支持不同的端口类型。

> 如果在同一子网中配置了集群间和管理 LIF ，则管理流量可能会被外部防火墙阻止，并且 AutoSupport 和 NTP 连接可能会失败。您可以通过运行来恢复系统 `network interface modify -vserver` *`vserver name`* `-lif` *`intercluster LIF`* `-status-admin up|down` 命令切换集群间LIF。但是，您应在不同子网中设置集群间 LIF 和管理 LIF ，以避免使用此问题描述。

LIF	Description
数据 LIF	与 Storage Virtual Machine （ SVM ）关联并用于与客户端通信的 LIF 。一个端口上可以有多个数据 LIF 。这些接口可以在整个集群中进行迁移或故障转移。您可以通过将数据 LIF 的防火墙策略修改为 mgmt 来将其用作 SVM 管理 LIF 。 与 NIS ， LDAP ， Active Directory ， WINS 和 DNS 服务器建立的会话使用数据 LIF 。
集群 LIF	一种 LIF ，用于在集群中的节点之间传输集群内流量。必须始终在集群端口上创建集群 LIF 。 集群 LIF 可以在同一节点上的集群端口之间进行故障转移，但不能迁移或故障转移到远程节点。当新节点加入集群时，系统会自动生成 IP 地址。但是，如果要手动为集群 LIF 分配 IP 地址，则必须确保新 IP 地址与现有集群 LIF 位于同一子网范围内。
集群管理 LIF	为整个集群提供一个管理接口的 LIF 。 集群管理 LIF 可以故障转移到集群中的任何节点。它无法故障转移到集群或集群间端口

集群间 LIF	一种用于跨集群通信，备份和复制的 LIF 。您必须先在集群中的每个节点上创建一个集群间 LIF ，然后才能建立集群对等关系。 这些 LIF 只能故障转移到同一节点中的端口。它们不能迁移或故障转移到集群中的另一个节点。
节点管理 LIF	一种 LIF ，用于提供用于管理集群中特定节点的专用 IP 地址。节点管理 LIF 是在创建或加入集群时创建的。这些 LIF 用于系统维护，例如，当节点无法从集群访问时。
VIP LIF	VIP LIF 是指在 VIP 端口上创建的任何数据 LIF 。要了解更多信息，请参见 "配置虚拟 IP （ VIP ） LIF"。

ONTAP 9.6及更高版本

您可以将服务策略(而不是LIF角色或防火墙策略)分配给LIF、以确定LIF支持的流量类型。服务策略定义 LIF 支持的一组网络服务。ONTAP 提供了一组可与 LIF 关联的内置服务策略。

您可以使用以下命令显示服务策略及其详细信息：

```
network interface service-policy show
```

未绑定到特定服务的功能将使用系统定义的行为为出站连接选择生命周期。

系统 **SVM** 的服务策略

管理 SVM 和任何系统 SVM 都包含可用于该 SVM 中 LIF 的服务策略，包括管理和集群间 LIF 。创建 IP 空间时，系统会自动创建这些策略。

下表列出了截至ONTAP 9.12.1的系统SVM中的内置的LUN策略。对于其他版本，使用以下命令显示服务策略及其详细信息：

```
network interface service-policy show
```

策略	包括的服务	等效角色	Description
default-intercluster	集群间核心，管理 https	集群间	由传输集群间流量的 LIF 使用。 注意： ONTAP 9.5 提供了名称为 net-intercluster service policy 的服务集群间核心。
default-route-announce	管理 BGP	-	由传输BGP对等连接的生命周期管理器使用 注意：从ONTAP 9.5开始提供、名称为net-route-n탔 늼 服务策略。

default-management	management-core、management-https、management-http、management-ssh、management-autosupport、management-EMS、management-dns-client、management-ad-client、management-ldap-client、management-nis-client、management-ntp-client、management-log-forwarding	node-mgmt 或 cluster-mgmt	使用此系统范围的管理策略创建系统SVM所拥有的节点和集群范围的管理LIF。这些LIF可用于到DNS、AD、LDAP或NIS服务器的出站连接、以及一些附加连接、以支持代表整个系统运行的应用程序。 从ONTAP 9.12.1开始、您可以使用 `management-log-forwarding` 用于控制用于将审核日志转发到远程系统日志服务器的LIF的服务。

下表列出了自ONTAP 9.11.1之日LIF可在系统SVM上使用的服务：

服务	故障转移限制	Description
集群间核心	仅主节点	核心集群间服务
管理核心	-	核心管理服务
management-ssh	-	用于 SSH 管理访问的服务
management-http	-	用于HTTP管理访问的服务
management-https	-	用于HTTPS管理访问的服务
management-autosupport	-	与发布 AutoSupport 有效负载相关的服务
管理 BGP	仅主端口	与 BGP 对等交互相关的服务
backup-ndmp-control	-	NDMP 备份控制服务
管理 EMS	-	用于管理消息访问的服务
management-ntp-client	-	在ONTAP 9.10.1中引入。 用于 NTP 客户端访问的服务。
management-ntp-server	-	在ONTAP 9.11.1中推出。 用于 NTP 服务器管理访问的服务

management-portmap	-	端口映射管理服务
management-rsh-server	-	用于 RSH 服务器管理的服务
management-snmp-server	-	SNMP 服务器管理服务
management-telnet-server	-	用于 telnet 服务器管理的服务
management-log-forwarding	-	在ONTAP 9.12.1中推出。 用于审核日志转发的服务

数据 SVM 的服务策略

所有数据 SVM 都包含可由该 SVM 中的 LIF 使用的服务策略。

下表列出了自ONTAP 9.11.1之日数据SVM中LIF的内置策略。对于其他版本，使用以下命令显示服务策略及其详细信息：

```
network interface service-policy show
```

策略	包括的服务	等效数据协议	Description
default-management	management-https、management-http、management-ssh、management-ds-client、management-ad-client、management-ldap-client、management-nis-client	无	使用此SVM范围的管理策略创建数据SVM所拥有的SVM管理LIF。这些 LIF 可用于为 SVM 管理员提供 SSH 或 HTTPS 访问权限。必要时、可以使用这些LIF与外部DNS、AD、LDAP或NIS服务器进行出站连接。
default-data-blocks	数据核心，数据iSCSI	iSCSI	由传输面向块的SAN数据流量的LIF使用。从ONTAP 9.10.1开始、"default-data-blocs"策略已弃用。请改用"default-data-iscsi"服务策略。

default-data-files	data-fpolicy-client、data-ds-server、data-FlexCache、data-cifs、data-nfs、management-dns-client、management-ad-client、management-ldap-client、management-nis-client	NFS， CIFS，fcache	使用default-data-files策略创建支持基于文件的数据协议的NAS LIF。有时、SVM中只有一个LIF、因此、此策略允许使用此LIF与外部DNS、AD、LDAP或NIS服务器进行出站连接。如果您希望这些连接仅使用管理LIF、则可以从此策略中删除这些服务。
default-data-iscsi	数据核心，数据iSCSI	iSCSI	由传输iSCSI数据流量的LIF使用。
default-data-NVMe-tcp	数据核心、数据NVMe-TCP	NVMe-TCP	由传输NVMe/TCP数据流量的LIF使用。

下表列出了数据SVM上可使用的服务以及每个服务自ONTAP 9.11.1之日对LIF的故障转移策略施加的任何限制：

服务	故障转移限制	Description
management-ssh	-	用于 SSH 管理访问的服务
management-http	-	在ONTAP 9.10.1中推出 用于HTTP管理访问的服务
management-https	-	用于HTTPS管理访问的服务
management-portmap	-	用于 portmap 管理访问的服务
management-snmp-server	-	在ONTAP 9.10.1中推出 用于SNMP服务器管理访问的服务
数据核心	-	核心数据服务
数据 NFS	-	NFS 数据服务
数据 CIFS	-	CIFS数据服务
数据 FlexCache	-	FlexCache 数据服务
数据 iSCSI	仅主端口	iSCSI 数据服务
backup-ndmp-control	-	在ONTAP 9.10.1中推出 备份 NDMP 控制数据服务

data-ds-server	-	在ONTAP 9.10.1中推出 DNS 服务器数据服务
data-fpolicy-client	-	文件筛选策略数据服务
data-NVMe-tcp	仅主端口	在ONTAP 9.10.1中推出 NVMe TCP 数据服务
data-s3-server	-	简单存储服务（ S3 ）服务器数据服务

您应了解如何将服务策略分配给数据 SVM 中的 LIF：

- 如果创建的数据 SVM 包含一系列数据服务，则会使用指定的服务创建该 SVM 中的内置 "default-data-files" 和 "default-data-blocs" 服务策略。
- 如果在创建数据 SVM 时未指定数据服务列表，则会使用默认数据服务列表创建该 SVM 中的内置 "default-data-files" 和 "default-data-blocs" 服务策略。

  默认数据服务列表包括iSCSI、NFS、NVMe、SMB和FlexCache 服务。

- 创建包含数据协议列表的 LIF 时，系统会为 LIF 分配与指定数据协议等效的服务策略。
- 如果不存在等效服务策略，则会创建自定义服务策略。
- 如果创建 LIF 时没有服务策略或数据协议列表，则默认情况下会将 default-data-files 服务策略分配给 LIF 。

数据核心服务

通过数据核心服务，以前使用具有数据角色的 LIF 的组件可以在已升级的集群上按预期工作，以便使用服务策略而不是 LIF 角色（在 ONTAP 9.6 中已弃用）来管理 LIF 。

将数据核心指定为服务不会打开防火墙中的任何端口，但此服务应包含在数据 SVM 的任何服务策略中。例如，default-data-files 服务策略默认包含以下服务：

- 数据核心
- 数据 NFS
- 数据 CIFS
- 数据 FlexCache

策略中应包含数据核心服务，以确保使用 LIF 的所有应用程序均按预期运行，但如果需要，可以删除其他三项服务。

客户端 **LIF** 服务

从 ONTAP 9.10.1 开始， ONTAP 为多个应用程序提供客户端 LIF 服务。这些服务可代表每个应用程序控制用于出站连接的 LIF 。

以下新服务可使管理员控制哪些 LIF 用作某些应用程序的源地址。

服务	SVM 限制	Description

management-ad-client	-	从ONTAP 9.11.1开始、ONTAP 为与外部AD服务器的出站连接提供Active Directory客户端服务。
management-dns-client	-	从ONTAP 9.11.1开始、ONTAP 为与外部DNS服务器的出站连接提供DNS客户端服务。
management-ldap-client	-	从ONTAP 9.11.1开始、ONTAP为与外部LDAP服务器的出站连接提供LDAP客户端服务。
management-nis-client	-	从ONTAP 9.11.1开始、ONTAP为与外部NIS服务器的出站连接提供NIS客户端服务。
management-ntp-client	仅限系统	从 ONTAP 9.10.1 开始， ONTAP 为与外部 NTP 服务器的出站连接提供 NTP 客户端服务。
data-fpolicy-client	纯数据	从 ONTAP 9.8 开始， ONTAP 为出站 FPolicy 连接提供客户端服务。

每个新服务都会自动包含在某些内置服务策略中，但管理员可以从内置策略中删除这些服务，或者将其添加到自定义策略中，以代表每个应用程序控制用于出站连接的 LIF 。

LIF角色(ONTAP 9.5及更早版本)

具有不同角色的 LIF 具有不同的特征。LIF 角色可确定接口支持的流量类型，适用的故障转移规则，已设置的防火墙限制，每个 LIF 的安全性，负载平衡以及路由行为。LIF 可以具有以下任一角色：集群，集群管理，数据，集群间，节点管理， 和 UNDEF （未定义）。BGP LIF 使用 UNDEF 角色。

从 ONTAP 9.6 开始， LIF 角色已弃用。您应为 LIF 指定服务策略，而不是为角色指定服务策略。使用服务策略创建 LIF 时，无需指定 LIF 角色。

LIF 安全性

	数据 LIF	集群 LIF	节点管理 LIF	集群管理 LIF	集群间 LIF
是否需要专用 IP 子网?	否	是的。	否	否	否
是否需要安全网络?	否	是的。	否	否	是的。
默认防火墙策略	限制性很强	完全开放	中等	中等	限制性很强
防火墙是否可自定义?	是的。	否	是的。	是的。	是的。

LIF 故障转移

	数据 LIF	集群 LIF	节点管理 LIF	集群管理 LIF	集群间 LIF

默认行为	仅限同一故障转移组中位于 LIF 主节点和非 SFO 配对节点上的端口	仅限同一故障转移组中位于 LIF 主节点上的端口	仅限同一故障转移组中位于 LIF 主节点上的端口	同一故障转移组中的任何端口	仅限同一故障转移组中位于 LIF 主节点上的端口
是否可自定义?	是的。	否	是的。	是的。	是的。

LIF 路由

	数据 LIF	集群 LIF	节点管理 LIF	集群管理 LIF	集群间 LIF
何时需要默认路由?	客户端或域控制器位于不同的 IP 子网上	从不	当任何主要流量类型需要访问其他 IP 子网时	管理员从另一个 IP 子网进行连接时	其他集群间 LIF 位于不同的 IP 子网上时
何时需要静态路由到特定 IP 子网?	极少	从不	极少	极少	另一个集群的节点的集群间 LIF 位于不同的 IP 子网中
何时需要静态主机路由到特定服务器?	要使其中一种流量类型列在节点管理 LIF 下，请执行数据 LIF ，而不是节点管理 LIF 。这需要相应地更改防火墙。	从不	极少	极少	极少

LIF 重新平衡

	数据 LIF	集群 LIF	节点管理 LIF	集群管理 LIF	集群间 LIF
DNS ： 是否用作 DNS 服务器?	是的。	否	否	否	否
DNS ： 是否导出为区域?	是的。	否	否	否	否

LIF 主要流量类型

	数据 LIF	集群 LIF	节点管理 LIF	集群管理 LIF	集群间 LIF
主要流量类型	NFS 服务器，CIFS 服务器，NIS 客户端，Active Directory ， LDAP ，WINS ， DNS 客户端和服务器，iSCSI 和 FC 服务器	集群内	SSH 服务器，HTTPS 服务器，NTP 客户端，SNMP ，AutoSupport 客户端， DNS 客户端，正在加载软件更新	SSH 服务器，HTTPS 服务器	跨集群复制

管理生命周期

配置 LIF 服务策略

您可以配置 LIF 服务策略以确定要使用 LIF 的单个服务或服务列表。

为 LIF 创建服务策略

您可以为 LIF 创建服务策略。您可以将服务策略分配给一个或多个 LIF ，从而使 LIF 能够传输单个服务或一系列服务的流量。

您需要具有高级权限才能运行 `network interface service-policy create` 命令：

关于此任务

内置服务和服务策略可用于管理数据和系统 SVM 上的数据和管理流量。大多数使用情形均可通过内置服务策略来满足，而不是创建自定义服务策略。

如果需要，您可以修改这些内置服务策略。

步骤

1. 查看集群中可用的服务：

   ```
   network interface service show
   ```

   服务表示 LIF 访问的应用程序以及集群提供服务的应用程序。每个服务包含零个或多个应用程序正在侦听的 TCP 和 UDP 端口。

   此外，还提供了以下附加数据和管理服务：

   ```
   cluster1::> network interface service show

   Service                     Protocol:Ports
   -------                     --------------
   cluster-core                -
   data-cifs                   -
   data-core                   -
   data-flexcache              -
   data-iscsi                  -
   data-nfs                    -
   intercluster-core           tcp:11104-11105
   management-autosupport      -
   management-bgp              tcp:179
   management-core             -
   management-https            tcp:443
   management-ssh              tcp:22
   12 entries were displayed.
   ```

2. 查看集群中存在的服务策略：

```
cluster1::> network interface service-policy show

Vserver   Policy                      Service: Allowed Addresses
--------- --------------------------
----------------------------------------
cluster1
          default-intercluster        intercluster-core: 0.0.0.0/0
                                      management-https: 0.0.0.0/0

          default-management          management-core: 0.0.0.0/0
                                      management-autosupport: 0.0.0.0/0
                                      management-ssh: 0.0.0.0/0
                                      management-https: 0.0.0.0/0

          default-route-announce      management-bgp: 0.0.0.0/0

Cluster
          default-cluster             cluster-core: 0.0.0.0/0

vs0
          default-data-blocks         data-core: 0.0.0.0/0
                                      data-iscsi: 0.0.0.0/0

          default-data-files          data-core: 0.0.0.0/0
                                      data-nfs: 0.0.0.0/0
                                      data-cifs: 0.0.0.0/0
                                      data-flexcache: 0.0.0.0/0

          default-management          data-core: 0.0.0.0/0
                                      management-ssh: 0.0.0.0/0
                                      management-https: 0.0.0.0/0

7 entries were displayed.
```

3. 创建服务策略：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver <svm_name>
-policy <service_policy_name> -services <service_name> -allowed
-addresses <IP_address/mask,...>
```

- "service_name" 指定应包含在策略中的服务列表。
- "ip_address/mask" 指定允许访问服务策略中服务的地址的子网掩码列表。默认情况下，添加所有指定服务时，默认允许的地址列表为 0.0.0.0/0 ，允许来自所有子网的流量。如果提供了非默认允许的地址列表，则会将使用此策略的 LIF 配置为阻止源地址与任何指定掩码不匹配的所有请求。

  以下示例显示了如何为包含_nfs_和_smb_服务的SVM创建数据服务策略_svm1_data_policy_：

  ```
  cluster1::> set -privilege advanced
  Warning: These advanced commands are potentially dangerous; use them
  only when directed to do so by technical support.
  Do you wish to continue? (y or n): y

  cluster1::> network interface service-policy create -vserver svm1
  -policy svm1_data_policy -services data-nfs,data-cifs,data-core
  ```

  以下示例显示了如何创建集群间服务策略：

```
cluster1::> set -privilege advanced
Warning: These advanced commands are potentially dangerous; use them
only when directed to do so by technical support.
Do you wish to continue? (y or n): y

cluster1::> network interface service-policy create -vserver cluster1
-policy intercluster1 -services intercluster-core
```

4. 验证是否已创建服务策略。

```
cluster1::> network interface service-policy show
```

以下输出显示了可用的服务策略：

```
cluster1::> network interface service-policy show

Vserver   Policy                      Service: Allowed Addresses
--------- --------------------------
----------------------------------------
cluster1
          default-intercluster       intercluster-core: 0.0.0.0/0
                                     management-https: 0.0.0.0/0

          intercluster1              intercluster-core: 0.0.0.0/0

          default-management         management-core: 0.0.0.0/0
                                     management-autosupport: 0.0.0.0/0
                                     management-ssh: 0.0.0.0/0
                                     management-https: 0.0.0.0/0

          default-route-announce     management-bgp: 0.0.0.0/0

Cluster
          default-cluster            cluster-core: 0.0.0.0/0

vs0
          default-data-blocks        data-core: 0.0.0.0/0
                                     data-iscsi: 0.0.0.0/0

          default-data-files         data-core: 0.0.0.0/0
                                     data-nfs: 0.0.0.0/0
                                     data-cifs: 0.0.0.0/0
                                     data-flexcache: 0.0.0.0/0

          default-management         data-core: 0.0.0.0/0
                                     management-ssh: 0.0.0.0/0
                                     management-https: 0.0.0.0/0

          svm1_data_policy           data-core: 0.0.0.0/0
                                     data-nfs: 0.0.0.0/0
                                     data-cifs: 0.0.0.0/0

9 entries were displayed.
```

完成后

在创建 LIF 时或通过修改现有 LIF 将服务策略分配给 LIF 。

为 LIF 分配服务策略

您可以在创建 LIF 时为 LIF 分配服务策略，也可以通过修改 LIF 来分配服务策略。服务策略用于定义可与 LIF 一起使用的服务列表。

关于此任务

您可以在管理和数据 SVM 中为 LIF 分配服务策略。

步骤

根据您要将服务策略分配给 LIF 的时间，请执行以下操作之一：

如果您 ...	分配服务策略 ...
创建 LIF	网络接口 create -vserver svm_name -lif <lif_name> -home-node <node_name> -home-port <port_name> ｛ （ -address <IP_address> -netmask <IP_address> ） -subnet-name <subnet_name> ｝ -service-policy <service_policy_name>
修改 LIF	network interface modify -vserver <svm_name> -lif <lif_name> -service-policy <service_policy_name>

为 LIF 指定服务策略时，无需为此 LIF 指定数据协议和角色。此外，还支持通过指定角色和数据协议来创建 LIF 。

> 服务策略只能由创建服务策略时指定的同一 SVM 中的 LIF 使用。

示例

以下示例显示了如何修改 LIF 的服务策略以使用默认管理服务策略：

```
cluster1::> network interface modify -vserver cluster1 -lif lif1 -service
-policy default-management
```

用于管理 LIF 服务策略的命令

使用 `network interface service-policy` 用于管理LIF服务策略的命令。

开始之前

修改活动SnapMirror关系中LIF的服务策略会中断复制计划。如果将LIF从集群间转换为非集群间(或反之)、则这些更改不会复制到对等集群。要在修改LIF服务策略后更新对等集群、请先执行 `snapmirror abort` 操作 重新同步复制关系。

如果您要 ...	使用此命令 ...
创建服务策略(需要高级权限)	`network interface service-policy create`
向现有服务策略添加其他服务条目(需要高级权限)	`network interface service-policy add-service`

如果您要 ...	使用此命令 ...
克隆现有服务策略(需要高级权限)	`network interface service-policy clone`
修改现有服务策略中的服务条目(需要高级权限)	`network interface service-policy modify-service`
从现有服务策略中删除服务条目(需要高级权限)	`network interface service-policy remove-service`
重命名现有服务策略(需要高级权限)	`network interface service-policy rename`
删除现有服务策略(需要高级权限)	`network interface service-policy delete`
将内置服务策略还原到其原始状态(需要高级权限)	`network interface service-policy restore-defaults`
显示现有服务策略	`network interface service-policy show`

创建**LIF** (网络接口)

SVM 通过一个或多个网络逻辑接口（ LIF ）向客户端提供数据。您必须在要用于访问数据的端口上创建 LIF 。LIF (网络接口)是与物理或逻辑端口关联的IP地址。如果组件出现故障，则 LIF 可以故障转移到或迁移到其他物理端口，从而继续与网络通信。

最佳实践

连接到ONTAP的交换机端口应配置为生成树边缘端口、以减少LIF迁移期间的延迟。

开始之前

- 您必须是集群管理员才能执行此任务。
- 底层物理或逻辑网络端口必须已配置为管理启动状态。
- 如果您计划使用子网名称为 LIF 分配 IP 地址和网络掩码值，则此子网必须已存在。

  子网包含属于同一第 3 层子网的 IP 地址池。它们是使用System Manager或创建的 `network subnet create` 命令：

- 用于指定 LIF 处理的流量类型的机制已发生更改。对于 ONTAP 9.5 及更早版本， LIF 使用角色指定要处理的流量类型。从 ONTAP 9.6 开始， LIF 使用服务策略指定要处理的流量类型。

关于此任务

- 您不能将 NAS 和 SAN 协议分配给同一个 LIF 。

  支持的协议包括 SMB ， NFS ， FlexCache ， iSCSI 和 FC ； iSCSI 和 FC 不能与其他协议结合使用。但是， NAS 和基于以太网的 SAN 协议可以位于同一物理端口上。

  - 您不应将传输SMB流量的LUN配置为自动还原到其主节点。如果SMB服务器要托管解决方案、以便通过

基于SMB的Hyper-V或SQL Server实现无中断运行、则必须遵循此建议。

- 您可以在同一网络端口上创建 IPv4 和 IPv6 LIF 。
- SVM 使用的所有名称映射和主机名解析服务，例如 DNS ， NIS ， LDAP 和 Active Directory 。 必须可从至少一个处理 SVM 数据流量的 LIF 进行访问。
- 处理节点之间集群内流量的 LIF 不应与处理管理流量的 LIF 或处理数据流量的 LIF 位于同一子网上。
- 如果创建的 LIF 没有有效的故障转移目标，则会显示一条警告消息。
- 如果集群中存在大量LIF、则可以验证集群上支持的LIF容量：
  - System Manager：从ONTAP 9.12.0开始、查看网络接口网格上的吞吐量。
  - 命令行界面：使用 `network interface capacity show` 命令以及每个节点上支持的LIF容量 `network interface capacity details show` 命令(在高级权限级别)。
- 从 ONTAP 9.7 开始，如果同一子网中已存在 SVM 的其他 LIF ，则无需指定 LIF 的主端口。ONTAP 会自动在与已在同一子网中配置的其他 LIF 位于同一广播域的指定主节点上选择一个随机端口。

  从 ONTAP 9.4 开始，支持 FC-NVMe 。如果要创建 FC-NVMe LIF ，应注意以下事项：

  - 创建 LIF 的 FC 适配器必须支持 NVMe 协议。
  - FC-NVMe 可以是数据 LIF 上的唯一数据协议。
- 必须为支持 SAN 的每个 Storage Virtual Machine （ SVM ）配置一个 LIF 处理管理流量。
- NVMe LIF 和命名空间必须托管在同一节点上。
- 每个 SVM 只能配置一个处理数据流量的 NVMe LIF 。
- 创建具有子网的网络接口时、ONTAP 会自动从选定子网中选择一个可用的IP地址并将其分配给网络接口。如果有多个子网、您可以更改此子网、但不能更改IP地址。
- 在为网络接口创建(添加) SVM时、不能指定现有子网范围内的IP地址。您将收到子网冲突错误。此问题描述会发生在网络接口的其他工作流中、例如在SVM设置或集群设置中创建或修改集群间网络接口。
- 从ONTAP 9.10.1开始、将显示 `network interface` CLI命令包括 `-rdma-protocols` 基于RDMA的NFS配置的参数。从ONTAP 9.12.1开始、System Manager支持为基于RDMA的NFS配置创建网络接口。有关详细信息，请参见 通过RDMA为NFS配置LIF。
- 从ONTAP 9.11.1开始、全闪存SAN阵列(ASA)平台可提供自动iSCSI LIF故障转移功能。

  系统会自动启用iSCSI LIF故障转移(故障转移策略设置为) `sfo-partner-only` 自动还原值设置为 `true`)在新创建的iSCSI LIF上(如果指定SVM中不存在iSCSI LIF、或者指定SVM中的所有现有iSCSI LIF均已启用iSCSI LIF故障转移)。

  如果在升级到ONTAP 9.11.1或更高版本后、某个SVM中存在未启用iSCSI LIF故障转移功能的现有iSCSI LIF、而您又在同一SVM中创建了新的iSCSI LIF、则新的iSCSI LIF将采用相同的故障转移策略 (`disabled`)。

  "适用于ASA 平台的iSCSI LIF故障转移"

从 ONTAP 9.7 开始，只要该 IP 空间的同一子网中至少已存在一个 LIF ， ONTAP 就会自动选择 LIF 的主端口。ONTAP 会选择与该子网中的其他 LIF 位于同一广播域中的主端口。您仍然可以指定主端口，但不再需要此端口（除非指定 IP 空间中的子网中尚不存在 LIF ）。

从ONTAP 9.12.0开始、您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

使用**System Manager**添加网络接口

步骤

1. 选择*网络>概述>网络接口*。
2. 选择 … + Add 。
3. 选择以下接口角色之一：
   a. 数据
   b. 集群间
   c. SVM管理
4. 选择协议：
   a. SMB/CIFS和NFS
   b. iSCSI
   c. FC
   d. NVMe/FC
   e. NVMe/TCP
5. 为LIF命名或接受从先前选择生成的名称。
6. 接受主节点或使用下拉列表选择一个。
7. 如果在选定SVM的IP空间中至少配置了一个子网、则会显示子网下拉列表。
   a. 如果选择子网、请从下拉列表中选择它。
   b. 如果继续操作而不使用子网、则会显示广播域下拉列表：
      i. 指定IP地址。如果此IP地址正在使用中、则会显示一条警告消息。
      ii. 指定子网掩码。
8. 从广播域中选择主端口、可以自动(建议)选择、也可以从下拉菜单中选择一个。主端口控制将根据广播域或子网选择显示。
9. 保存网络接口。

命令行界面

使用命令行界面创建**LIF**

步骤

1. 确定要用于 LIF 的广播域端口。

```
network port broadcast-domain show -ipspace ipspace1
```

```
IPspace     Broadcast                         Update
Name        Domain name   MTU   Port List   Status Details
ipspace1
            default       1500
                                  node1:e0d   complete
                                  node1:e0e   complete
                                  node2:e0d   complete
                                  node2:e0e   complete
```

2. 验证要用于 LIF 的子网是否包含足够的未使用 IP 地址。

   `network subnet show -ipspace` *`ipspace1`*

3. 在要用于访问数据的端口上创建一个或多个 LIF 。

```
network interface create -vserver _SVM_name_ -lif _lif_name_
-service-policy _service_policy_name_ -home-node _node_name_ -home
-port port_name {-address _IP_address_ - netmask _Netmask_value_ |
-subnet-name _subnet_name_} -firewall- policy _policy_ -auto-revert
{true|false}
```

   - `-home-node` 是LIF返回到的节点 `network interface revert` 命令将在LIF上运行。

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

   - `-home-port` 是LIF返回到的物理或逻辑端口 `network interface revert` 命令将在LIF上运行。
   - 您可以使用指定IP地址 `-address` 和 `-netmask` 选项、或者使用启用从子网分配 `-subnet_name` 选项
   - 使用子网提供 IP 地址和网络掩码时，如果使用网关定义了子网，则在使用该子网创建 LIF 时，系统会自动向 SVM 添加指向该网关的默认路由。
   - 如果您手动分配 IP 地址（而不使用子网），则在其他 IP 子网上存在客户端或域控制器时，可能需要配置指向网关的默认路由。。 `network route create` 手册页包含有关在SVM中创建静态路由的信息。
   - `-auto-revert` 用于指定在启动、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`，但您可以将其设置为 `true` 具体取决于您环境中的网络管理策略。
   - `-service-policy` 从ONTAP 9.5开始、您可以使用为LIF分配服务策略 `-service-policy` 选项为 LIF 指定服务策略时，将使用该策略为 LIF 构建默认角色，故障转移策略和数据协议列表。在 ONTAP 9.5 中，只有集群间和 BGP 对等服务才支持服务策略。在 ONTAP 9.6 中，您可以为多个数据和管理服务创建服务策略。
   - `-data-protocol` 用于创建支持FCP或NVMe/FC协议的LIF。创建 IP LIF 时不需要此选项。

4. 可选：在-address选项中分配IPv6地址：

a. 使用 network ndp prefix show 命令查看在各种接口上获取的 RA 前缀列表。

   。 `network ndp prefix show` 命令可在高级权限级别下使用。

b. 使用格式 `prefix::id` 手动构建IPv6地址。

   `prefix` 是在各种接口上获取的前缀。

用于派生 `id`下，选择一个随机的64位十六进制数。

5. 验证 LIF 接口配置是否正确。

   `network interface show -vserver vs1`

```
           Logical    Status     Network          Current   Current Is
Vserver    Interface  Admin/Oper Address/Mask     Node      Port
Home
--------- ---------- ---------- --------------- --------- -------
----
vs1
            lif1       up/up      10.0.0.128/24   node1     e0d
true
```

6. 验证故障转移组配置是否符合要求。

   `network interface show -failover -vserver vs1`

```
          Logical    Home       Failover        Failover
Vserver   interface  Node:Port  Policy          Group
-------- ---------- ---------  ---------       --------
vs1
          lif1       node1:e0d  system-defined  ipspace1
Failover Targets: node1:e0d, node1:e0e, node2:e0d, node2:e0e
```

7. 验证配置的 IP 地址是否可访问：

要验证 …	使用 …
IPv4 地址	网络 ping
IPv6地址	网络 ping6.

示例

以下命令将使用创建LIF并指定IP地址和网络掩码值 `-address` 和 `-netmask` 参数：

```
network interface create -vserver vs1.example.com -lif datalif1
-service-policy default-data-files -home-node node-4 -home-port e1c
-address 192.0.2.145 -netmask 255.255.255.0 -auto-revert true
```

以下命令将创建一个 LIF ，并从指定子网（名为 client1_sub ）分配 IP 地址和网络掩码值：

```
network interface create -vserver vs3.example.com -lif datalif3
-service-policy default-data-files -home-node node-3 -home-port e1c
-subnet-name client1_sub - auto-revert true
```

以下命令将创建NVMe/FC LIF并指定 `nvme-fc` 数据协议：

```
network interface create -vserver vs1.example.com -lif datalif1 -data
-protocol nvme-fc -home-node node-4 -home-port 1c -address 192.0.2.145
-netmask 255.255.255.0 -auto-revert true
```

修改 **LIF**

您可以通过更改主节点或当前节点，管理状态， IP 地址，网络掩码，故障转移策略等属性来修改 LIF 。 防火墙策略和服务策略。您还可以将 LIF 的地址系列从 IPv4 更改为 IPv6 。

关于此任务

- 将 LIF 的管理状态修改为 down 时，任何未完成的 NFSv4 锁定都将保持，直到 LIF 的管理状态恢复为 up 为止。

  为了避免在其他 LIF 尝试访问锁定文件时可能发生锁定冲突，您必须先将 NFSv4 客户端移动到其他 LIF ，然后再将管理状态设置为 down 。

- 您不能修改 FC LIF 使用的数据协议。但是，您可以修改分配给服务策略的服务或更改分配给 IP LIF 的服务策略。

  要修改 FC LIF 使用的数据协议，必须删除并重新创建 LIF 。要更改 IP LIF 的服务策略，更新期间会短暂中断。

- 您不能修改节点范围的管理 LIF 的主节点或当前节点。
- 使用子网更改 LIF 的 IP 地址和网络掩码值时，系统会从指定子网分配 IP 地址；如果 LIF 的上一个 IP 地址来自不同子网，则会将 IP 地址返回到该子网。
- 要将LIF的地址系列从IPv4修改为IPv6、必须对IPv6地址使用冒号表示法、并为添加新值 `-netmask -length` 参数。
- 您不能修改自动配置的链路本地 IPv6 地址。
- 修改 LIF 后，如果 LIF 没有有效的故障转移目标，则会显示一条警告消息。

  如果没有有效故障转移目标的 LIF 尝试进行故障转移，可能会发生中断。

- 从 ONTAP 9.5 开始，您可以修改与 LIF 关联的服务策略。

  在 ONTAP 9.5 中，只有集群间和 BGP 对等服务才支持服务策略。在 ONTAP 9.6 中，您可以为多个数据和管理服务创建服务策略。

- 从ONTAP 9.11.1开始、全闪存SAN阵列(ASA)平台可提供自动iSCSI LIF故障转移功能。

  对于已有的iSCSI LUN (即在升级到9.11.1或更高版本之前创建的LUN)、您可以将故障转移策略修改为 "启用自动iSCSI LIF故障转移"。

您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

从**ONTAP 9.12.0**开始、您可以使用**System Manager**编辑网络接口

步骤

1. 选择*网络>概述>网络接口*。
2. 选择 … ⋮ 要更改的网络接口旁边的*>编辑*。
3. 更改一个或多个网络接口设置。有关详细信息，请参见 "创建 LIF"。
4. 保存所做的更改。

命令行界面

使用命令行界面修改**LIF**

步骤

1. 使用修改LIF的属性 `network interface modify` 命令：

   以下示例显示了如何使用子网 client1_sub 中的 IP 地址和网络掩码值修改 LIF datalif2 的 IP 地址和网络掩码：

   ```
   network interface modify -vserver vs1 -lif datalif2 -subnet-name
   client1_sub
   ```

   以下示例显示了如何修改 LIF 的服务策略。

   ```
   network interface modify -vserver siteA -lif node1_inter1 -service
   -policy example
   ```

2. 验证 IP 地址是否可访问。

如果您使用的是 …	然后使用 …
IPv4 地址	`network ping`
IPv6地址	`network ping6`

迁移 **LIF**

如果 LIF 端口出现故障或需要维护，则可能需要将此端口迁移到集群中同一节点或不同节点上的其他端口。迁移 LIF 与 LIF 故障转移类似，但 LIF 迁移是手动操作，而 LIF 故障转移则是在 LIF 当前网络端口出现链路故障时自动迁移 LIF 。

开始之前

- 必须已为 LIF 配置故障转移组。
- 目标节点和端口必须正常运行，并且必须能够访问与源端口相同的网络。

关于此任务

- BGP LIF 位于主端口上，不能迁移到任何其他节点或端口。
- 在从节点中删除 NIC 之前，必须将属于 NIC 的端口上托管的 LIF 迁移到集群中的其他端口。
- 您必须执行命令，从托管集群 LIF 的节点迁移集群 LIF 。
- 无法将节点范围的 LIF （例如，节点范围的管理 LIF ，集群 LIF ，集群间 LIF ）迁移到远程节点。
- 在节点之间迁移 NFSv4 LIF 时，在新端口上提供 LIF 之前，最多会出现 45 秒的延迟。

  要解决此问题，请在未遇到延迟的情况下使用 NFSv4.1 。

- 您可以在运行ONTAP 9.11.1或更高版本的全闪存SAN阵列(ASA)平台上迁移iSCSI LUN。

  迁移iSCSI LIF仅限于主节点或HA配对节点上的端口。

- 如果您的平台不是运行ONTAP 9.11.1或更高版本的纯闪存SAN阵列(ASA)平台、则无法将iSCSI LUN从一个节点迁移到另一个节点。

  要解决此限制，您必须在目标节点上创建 iSCSI LIF 。了解相关信息 "创建iSCSI LIF"。

- 如果要通过RDMA迁移NFS的LIF (网络接口)、则必须确保目标端口支持RoCE。要使用命令行界面迁移LIF、必须运行ONTAP 9.10.1或更高版本、或者要使用System Manager迁移ONTAP 9.12.1.在System Manager中、选择支持RoCE的目标端口后、必须选中*使用RoCE端口*旁边的框才能成功完成迁移。了解更多信息 "通过RDMA为NFS配置LIF"。
- 迁移源或目标 LIF 时， VMware VAAI 副本卸载操作失败。了解副本卸载：
  - "NFS环境"
  - "SAN 环境"

您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

使用**System Manager**迁移网络接口

步骤

1. 选择*网络>概述>网络接口*。
2. 选择 … ⋮ 要更改的网络接口旁边的*> Migrate *。

   > 对于iSCSI LIF、在*迁移接口*对话框中、选择HA配对节点的目标节点和端口。

   如果要永久迁移iSCSI LIF、请选中此复选框。iSCSI LIF必须处于脱机状态、才能进行永久迁移。此外、永久迁移iSCSI LIF后、它将无法撤消。没有还原选项。

3. 单击 * 迁移 * 。
4. 保存所做的更改。

命令行界面

使用命令行界面迁移**LIF**

步骤

根据您要迁移特定 LIF 还是所有 LIF ，请执行相应的操作：

要迁移的对象	输入以下命令 …
特定 LIF	`network interface migrate`
节点上的所有数据和集群管理 LIF	`network interface migrate-all`
端口的所有 LIF	`network interface migrate-all -node <node> -port <port>`

以下示例显示了如何迁移名为的LIF `datalif1` 在SVM上 `vs0` 连接到端口 `e0d` 开启 `node0b`：

```
network interface migrate -vserver vs0 -lif datalif1 -dest-node node0b
-dest-port e0d
```

以下示例显示了如何从当前（本地）节点迁移所有数据和集群管理 LIF ：

```
network interface migrate-all -node local
```

将 **LIF** 还原到其主端口

您可以在 LIF 发生故障转移或手动或自动迁移到其他端口后将其还原到主端口。如果特定 LIF 的主端口不可用，则 LIF 将保留在其当前端口，不会还原。

关于此任务

- 如果在设置自动还原选项之前以管理方式将 LIF 的主端口置于 up 状态，则 LIF 不会返回到主端口。
- 除非 "auto-revert" 选项的值设置为 true ，否则 LIF 不会自动还原。
- 您必须确保为 LIF 启用了 "auto-revert" 选项以还原到其主端口。

您关注的操作步骤 取决于您使用的界面—System Manager或命令行界面：

System Manager

使用**System Manager**将网络接口还原到其主端口

步骤

1. 选择*网络>概述>网络接口*。
2. 选择 … ⋮ 要更改的网络接口旁边的*> Revere*。
3. 选择*还原*可将网络接口还原到其主端口。

命令行界面

使用命令行界面将**LIF**还原到其主端口

步骤

手动或自动将 LIF 还原到其主端口：

如果要将 LIF 还原到其主端口 …	然后输入以下命令 …
手动	`network interface revert -vserver vserver_name -lif lif_name`
自动	`network interface modify -vserver vserver_name -lif lif_name -auto-revert true`

ONTAP 9.8 及更高版本：从配置不正确的集群 **LIF** 中恢复

如果集群网络已连接到交换机，则无法创建集群，但集群 IP 空间中配置的所有端口并非都能访问集群 IP 空间中配置的其他端口。

关于此任务

在有交换机集群中、如果集群网络接口(LIF)配置在错误的端口上、或者如果集群端口连接到错误的网络、则为 `cluster create` 命令可能会失败并显示以下错误：

```
Not all local cluster ports have reachability to one another.
Use the "network port reachability show -detail" command for more details.
```

的结果 `network port show` 命令可能会显示已向集群IP空间添加多个端口、因为这些端口连接到配置了集群LIF的端口。但是、的结果 `network port reachability show -detail` 命令可显示哪些端口之间没有连接。

要从配置了集群 LIF 的其他端口无法访问的端口上配置的集群 LIF 进行恢复，请执行以下步骤：

步骤

1. 将集群 LIF 的主端口重置为正确的端口：

   ```
   network port modify -home-port
   ```

2. 从集群广播域中删除未配置集群 LIF 的端口：

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

3. 创建集群：

   ```
   cluster create
   ```

结果

创建完集群后，系统将检测到正确的配置并将端口放置到正确的广播域中。

删除 **LIF**

您可以删除不再需要的网络接口（LIF）。

开始之前

要删除的 LIF 不得正在使用中。

步骤

1. 使用以下命令将要删除的 LIF 标记为 administratively down：

   ```
   network interface modify -vserver vserver_name -lif lif_name -status
   -admin down
   ```

2. 使用 `network interface delete` 用于删除一个或所有LUN的命令：

要删除的内容	输入命令 ...

特定 LIF	`network interface delete -vserver vserver_name -lif lif_name`
所有 LIFs	`network interface delete -vserver vserver_name -lif *`

以下命令将删除 LIF mgmtlif2：

```
network interface delete -vserver vs1 -lif mgmtlif2
```

3. 使用 `network interface show` 命令以确认已删除此LIF。

平衡网络负载

平衡网络概述

您可以将集群配置为通过适当加载的 LIF 提供客户端请求。这样可以更均衡地利用 LIF 和端口，进而提高集群的性能。

DNS 负载平衡有助于选择适当加载的数据 LIF ，并在所有可用端口（物理，接口组和 VLAN ）之间平衡用户网络流量。

使用 DNS 负载平衡时， LIF 与 SVM 的负载平衡区域相关联。站点范围的 DNS 服务器配置为转发所有 DNS 请求，并根据网络流量和端口资源的可用性（ CPU 使用量，吞吐量，打开的连接等）返回负载最少的 LIF 。DNS 负载平衡具有以下优势：

- 新的客户端连接在可用资源之间保持平衡。
- 无需手动干预即可确定挂载特定 SVM 时要使用的 LIF 。
- DNS负载平衡支持NFSv3、NFSv4、NFSv4.1、SMB 2.0、SMB 2.1、 SMB 3.0和S3。

DNS 负载平衡的工作原理

客户端通过指定 IP 地址（与 LIF 关联）或主机名（与多个 IP 地址关联）来挂载 SVM 。默认情况下，站点范围的 DNS 服务器会以轮循方式选择 LIF ，从而在所有 LIF 之间平衡工作负载。

循环负载平衡可能会导致某些 LIF 过载，因此您可以选择使用 DNS 负载平衡区域来处理 SVM 中的主机名解析。使用 DNS 负载平衡区域可确保在可用资源之间更好地平衡新客户端连接，从而提高集群性能。

DNS 负载平衡区域是集群中的 DNS 服务器，用于动态评估所有 LIF 上的负载并返回适当加载的 LIF 。在负载平衡区域中， DNS 会根据负载为每个 LIF 分配权重（度量指标）。

系统会根据每个 LIF 的端口负载及其主节点的 CPU 利用率为其分配权重。负载较低的端口上的 LIF 在 DNS 查询中返回的可能性较高。也可以手动分配权重。

创建 DNS 负载平衡区域

您可以创建 DNS 负载平衡区域，以便根据负载动态选择 LIF ，即装载在 LIF 上的客户端数量。您可以在创建数据 LIF 时创建负载平衡区域。

开始之前

必须将站点范围 DNS 服务器上的 DNS 转发器配置为将负载平衡区域的所有请求转发到已配置的 LIF 。

知识库文章 "如何在集群模式下设置 DNS 负载平衡" NetApp 支持站点上提供了有关使用条件转发配置 DNS 负载平衡的详细信息。

关于此任务

- 任何数据 LIF 都可以响应 DNS 查询，以获取 DNS 负载平衡区域名称。
- DNS 负载平衡区域在集群中必须具有唯一名称，并且此区域名称必须满足以下要求：
  - 不应超过 256 个字符。
  - 它应至少包含一个句点。
  - 第一个和最后一个字符不应是句点或任何其他特殊字符。
  - 字符之间不能包含任何空格。
  - DNS 名称中的每个标签不应超过 63 个字符。

    标签是指在句点之前或之后显示的文本。例如，名为 storage.company.com 的 DNS 区域具有三个标签。

步骤

使用 `network interface create` 命令 `dns-zone` 用于创建DNS负载平衡区域的选项。

如果负载平衡区域已存在，则会将 LIF 添加到该区域中。有关命令的详细信息，请参见 "ONTAP 9 命令"。

以下示例演示如何在创建LIF时创建名为storage.company.com的DNS负载平衡区域 `lif1`：

```
network interface create -vserver vs0 -lif lif1 -home-node node1
-home-port e0c -address 192.0.2.129 -netmask 255.255.255.128 -dns-zone
storage.company.com
```

在负载平衡区域中添加或删除 LIF

您可以从虚拟机（ SVM ）的 DNS 负载平衡区域添加或删除 LIF 。您还可以从负载平衡区域同时删除所有 LIF 。

开始之前

- 负载平衡区域中的所有 LIF 都应属于同一个 SVM 。
- 一个 LIF 只能属于一个 DNS 负载平衡区域。
- 如果 LIF 属于不同的子网，则必须已为每个子网设置故障转移组。

关于此任务

处于管理关闭状态的 LIF 将暂时从 DNS 负载平衡区域中删除。当 LIF 返回到管理 up 状态时， LIF 会自动添加到 DNS 负载平衡区域。

步骤

在负载平衡区域中添加 LIF 或删除 LIF：

如果您要 …	输入 …
添加 LIF	`network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-dns-zone` *`zone_name`* 示例 `network interface modify -vserver vs1 -lif data1 -dns -zone cifs.company.com`

删除一个 LIF	`network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-dns-zone none`
	示例
	`network interface modify -vserver vs1 -lif data1 -dns -zone none`

删除所有 LIF	`network interface modify -vserver` *`vserver_name`* `-lif * -dns-zone none`
	示例
	`network interface modify -vserver vs0 -lif * -dns-zone none`
	您可以通过从负载平衡区域中删除SVM中的所有SVM来从该区域中删除此SVM。

配置DNS服务(ONTAP 9.8及更高版本)

在创建 NFS 或 SMB 服务器之前，您必须为 SVM 配置 DNS 服务。通常， DNS 名称服务器是 NFS 或 SMB 服务器要加入的域的 Active Directory 集成 DNS 服务器。

关于此任务

Active Directory 集成的 DNS 服务器包含域 LDAP 和域控制器服务器的服务位置记录（ SRV ）。如果 SVM 找不到 Active Directory LDAP 服务器和域控制器，则 NFS 或 SMB 服务器设置将失败。

SVM 使用 hosts 名称服务 ns-switch 数据库确定要使用的名称服务以及查找有关主机的信息的顺序。hosts 数据库支持的两个名称服务是 files 和 dns 。

在创建 SMB 服务器之前，您必须确保 DNS 是其中一个源。

> 要查看 mgwd 进程和 SecD 进程的 DNS 名称服务统计信息，请使用统计信息 UI 。

步骤

1. 确定主机名服务数据库的当前配置。在此示例中， hosts 名称服务数据库使用默认设置。

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
Vserver: vs1
Name Service Switch Database: hosts
Vserver: vs1 Name Service Switch Database: hosts
Name Service Source Order: files, dns
```

2. 如果需要，请执行以下操作。

   a. 按所需顺序将 DNS 名称服务添加到主机名称服务数据库中，或者重新排列源。

      在此示例中， hosts 数据库配置为按此顺序使用 DNS 和本地文件。

      ```
      vserver services name-service ns-switch modify -vserver vs1 -database hosts
      -sources dns,files
      ```

   b. 验证名称服务配置是否正确。

      ```
      vserver services name-service ns-switch show -vserver vs1 -database hosts
      ```

```
Vserver: vs1
Name Service Switch Database: hosts
Name Service Source Order: dns, files
```

3. 配置 DNS 服务。

   ```
   vserver services name-service dns create -vserver vs1 -domains
   example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
   ```

   > vserver services name-service dns create 命令会执行自动配置验证，如果 ONTAP 无法与名称服务器联系，则会报告错误消息。

4. 验证 DNS 配置是否正确以及服务是否已启用。

```
Vserver: vs1
Domains: example.com, example2.com Name Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
Maximum Attempts: 1
```

5. 验证名称服务器的状态。

   ```
   vserver services name-service dns check -vserver vs1
   ```

```
Vserver  Name Server  Status  Status Details
vs1      10.0.0.50    up      Response time (msec): 2
vs1      10.0.0.51    up      Response time (msec): 2
```

在 SVM 上配置动态 DNS

如果您希望 Active Directory 集成的 DNS 服务器在 DNS 中动态注册 NFS 或 SMB 服务器的 DNS 记录，则必须在 SVM 上配置动态 DNS （ DDNS ）。

开始之前

必须在 SVM 上配置 DNS 名称服务。如果您使用的是安全 DDNS ，则必须使用 Active Directory 集成的 DNS 名称服务器，并且必须已为 SVM 创建 NFS 或 SMB 服务器或 Active Directory 帐户。

关于此任务

指定的完全限定域名（ FQDN ）必须是唯一的：

指定的完全限定域名（ FQDN ）必须是唯一的：

- 对于NFS、是在中指定的值 `-vserver-fqdn` 作为的一部分 `vserver services name-service dns dynamic-update` 命令将成为为这些生命周期管理器注册的FQDN。
- 对于 SMB ，指定为 CIFS 服务器 NetBIOS 名称和 CIFS 服务器完全限定域名的值将成为 LIF 的注册 FQDN 。这在 ONTAP 中是不可配置的。在以下情形中， LIF FQDN 为 CIFS_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1

                                          Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_VS1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                                   Kerberos Realm: -
                              Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

> 要避免不符合 DDNS 更新的 RFC 规则的 SVM FQDN 配置失败，请使用符合 RFC 的 FQDN 名称。有关详细信息，请参见 "RFC 1123"。

步骤

1. 在 SVM 上配置 DDNS ：

```
vserver services name-service dns dynamic-update modify -vserver vserver_name
-is- enabled true [-use-secure {true|false} -vserver-fqdn
FQDN_used_for_DNS_updates

vserver services name-service dns dynamic-update modify -vserver vs1 -is
-enabled true - use-secure true -vserver-fqdn vs1.example.com
```

星号不能用作自定义 FQDN 的一部分。例如： `*.netapp.com` 无效。

2. 验证 DDNS 配置是否正确：

```
vserver services name-service dns dynamic-update show
```

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

配置DNS服务(ONTAP 9.7及更早版本)

在创建 NFS 或 SMB 服务器之前，您必须为 SVM 配置 DNS 服务。通常， DNS 名称服务器是 NFS 或 SMB 服务器要加入的域的 Active Directory 集成 DNS 服务器。

关于此任务

Active Directory 集成的 DNS 服务器包含域 LDAP 和域控制器服务器的服务位置记录（ SRV ）。如果 SVM 找不到 Active Directory LDAP 服务器和域控制器，则 NFS 或 SMB 服务器设置将失败。

SVM 使用 hosts 名称服务 ns-switch 数据库确定要使用的名称服务以及查找有关主机的信息的顺序。主机数据库支持的两种名称服务为 `files` 和 `dns`。

您必须确保这一点 `dns` 是创建SMB服务器之前的源之一。

> 要查看 mgwd 进程和 SecD 进程的 DNS 名称服务统计信息，请使用统计信息 UI 。

步骤

1. 确定的当前配置 `hosts` 名称服务数据库。

   在此示例中， hosts 名称服务数据库使用默认设置。

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

```
                      Vserver: vs1
Name Service Switch Database: hosts
   Name Service Source Order: files, dns
```

2. 如果需要，请执行以下操作。

a. 按所需顺序将 DNS 名称服务添加到主机名称服务数据库中，或者重新排列源。

   在此示例中， hosts 数据库配置为按此顺序使用 DNS 和本地文件。

```
vserver services name-service ns-switch modify -vserver vs1 -database hosts
-sources dns,files
```

a. 验证名称服务配置是否正确。

```
vserver services name-service ns-switch show -vserver vs1 -database hosts
```

3. 配置 DNS 服务。

```
vserver services name-service dns create -vserver vs1 -domains
example.com,example2.com -name-servers 10.0.0.50,10.0.0.51
```

> Vserver服务 `name-service dns create` 命令会执行自动配置验证、并在ONTAP无法联系名称服务器时报告错误消息。

4. 验证 DNS 配置是否正确以及服务是否已启用。

```
            Vserver: vs1
            Domains: example.com, example2.com Name
            Servers: 10.0.0.50, 10.0.0.51
Enable/Disable DNS: enabled Timeout (secs): 2
  Maximum Attempts: 1
```

5. 验证名称服务器的状态。

```
vserver services name-service dns check -vserver vs1
```

```
Vserver  Name Server  Status  Status Details
-------  -----------  ------  -----------------------
vs1      10.0.0.50    up      Response time (msec): 2
vs1      10.0.0.51    up      Response time (msec): 2
```

在 **SVM** 上配置动态 **DNS**

如果您希望 Active Directory 集成的 DNS 服务器在 DNS 中动态注册 NFS 或 SMB 服务器的 DNS 记录，则必须在 SVM 上配置动态 DNS （ DDNS ）。

开始之前

必须在 SVM 上配置 DNS 名称服务。如果您使用的是安全 DDNS ，则必须使用 Active Directory 集成的 DNS 名称服务器，并且必须已为 SVM 创建 NFS 或 SMB 服务器或 Active Directory 帐户。

关于此任务

指定的完全限定域名（FQDN）必须是唯一的：

- 对于NFS、是在中指定的值 `-vserver-fqdn` 作为的一部分 `vserver services name-service dns dynamic-update` 命令将成为为这些生命周期管理器注册的FQDN。
- 对于 SMB ，指定为 CIFS 服务器 NetBIOS 名称和 CIFS 服务器完全限定域名的值将成为 LIF 的注册 FQDN 。这在 ONTAP 中是不可配置的。在以下情形中， LIF FQDN 为 CIFS_VS1.EXAMPLE.COM":

```
cluster1::> cifs server show -vserver vs1

                                            Vserver: vs1
                        CIFS Server NetBIOS Name: CIFS_VS1
                    NetBIOS Domain/Workgroup Name: EXAMPLE
                      Fully Qualified Domain Name: EXAMPLE.COM
                              Organizational Unit: CN=Computers
Default Site Used by LIFs Without Site Membership:
                                   Workgroup Name: -
                                   Kerberos Realm: -
                              Authentication Style: domain
                CIFS Server Administrative Status: up
                          CIFS Server Description:
                          List of NetBIOS Aliases: -
```

> 要避免不符合 DDNS 更新的 RFC 规则的 SVM FQDN 配置失败，请使用符合 RFC 的 FQDN 名称。有关详细信息，请参见 "RFC 1123"。

步骤

1. 在 SVM 上配置 DDNS：

   `vserver services name-service dns dynamic-update modify -vserver` *`vserver_name`* `-is- enabled` *`true`* `[-use-secure {true|false} -vserver-fqdn` *`FQDN_used_for_DNS_updates`*

   `vserver services name-service dns dynamic-update modify -vserver` *`vs1`* `-is -enabled` *`true`* `- use-secure` *`true`* `-vserver-fqdn` *`vs1.example.com`*

   星号不能用作自定义 FQDN 的一部分。例如： `*.netapp.com` 无效。

2. 验证 DDNS 配置是否正确：

   `vserver services name-service dns dynamic-update show`

```
Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
-------- ---------- ---------- ----------------- -------
vs1      true       true       vs1.example.com   24h
```

配置动态 DNS 服务

如果您希望 Active Directory 集成的 DNS 服务器在 DNS 中动态注册 NFS 或 SMB 服务器的 DNS 记录，则必须在 SVM 上配置动态 DNS （ DDNS ）。

开始之前

必须在 SVM 上配置 DNS 名称服务。如果您使用的是安全 DDNS ，则必须使用 Active Directory 集成的 DNS 名称服务器，并且必须已为 SVM 创建 NFS 或 SMB 服务器或 Active Directory 帐户。

关于此任务

指定的 FQDN 必须是唯一的。

> 要避免不符合 DDNS 更新的 RFC 规则的 SVM FQDN 配置失败，请使用符合 RFC 的 FQDN 名称。

步骤

1. 在 SVM 上配置 DDNS：

   ```
   vserver services name-service dns dynamic-update modify -vserver vserver_name
   -is- enabled true [-use-secure {true|false} -vserver-fqdn
   FQDN_used_for_DNS_updates

   vserver services name-service dns dynamic-update modify -vserver vs1 -is
   -enabled true - use-secure true -vserver-fqdn vs1.example.com
   ```

   星号不能用作自定义 FQDN 的一部分。例如： `*.netapp.com` 无效。

2. 验证 DDNS 配置是否正确：

   ```
   vserver services name-service dns dynamic-update show
   ```

   ```
   Vserver  Is-Enabled Use-Secure Vserver FQDN      TTL
   -------- ---------- ---------- ----------------- -------
   vs1      true       true       vs1.example.com   24h
   ```

主机名解析

主机名解析概述

ONTAP 必须能够将主机名转换为数字 IP 地址，才能为客户端提供访问权限并访问服务。您必须将 Storage Virtual Machine （ SVM ）配置为使用本地或外部名称服务来解析主机信息。ONTAP 支持配置外部 DNS 服务器或配置本地主机文件以进行主机名解析。

使用外部 DNS 服务器时，您可以配置动态 DNS （ DDNS ），它会自动将新的或更改的 DNS 信息从存储系统发送到 DNS 服务器。如果没有动态 DNS 更新，则在新系统联机或现有 DNS 信息发生更改时，您必须手动将 DNS 信息（ DNS 名称和 IP 地址）添加到已标识的 DNS 服务器。此过程缓慢且容易出错。在灾难恢复期间，

手动配置可能会导致长时间停机。

配置 DNS 以进行主机名解析

您可以使用 DNS 访问本地或远程源来获取主机信息。您必须配置 DNS 才能访问其中一个或两个源。

ONTAP 必须能够查找主机信息，才能正确访问客户端。您必须配置名称服务，以使 ONTAP 能够访问本地或外部 DNS 服务以获取主机信息。

ONTAP会将名称服务配置信息存储在一个表中、该表相当于 `/etc/nsswitch.conf` 文件。

使用外部 DNS 服务器配置 SVM 和数据 LIF 以进行主机名解析

您可以使用 `vserver services name-service dns` 命令以在SVM上启用DNS、并将其配置为使用DNS进行主机名解析。主机名可使用外部 DNS 服务器进行解析。

开始之前

站点范围的 DNS 服务器必须可用于主机名查找。

您应配置多个 DNS 服务器，以避免单点故障。。 `vserver services name-service dns create` 如果仅输入一个DNS服务器名称、则命令会发出警告。

关于此任务

请参见 配置动态 DNS 服务 有关在SVM上配置动态DNS的详细信息、请参见。

步骤

1. 在 SVM 上启用 DNS：

```
vserver services name-service dns create -vserver <vserver_name>
-domains <domain_name> -name-servers <ip_addresses> -state enabled
```

以下命令将在 SVM vs1 上启用外部 DNS 服务器：

```
vserver services name-service dns create -vserver vs1.example.com
-domains example.com -name-servers 192.0.2.201,192.0.2.202 -state
enabled
```

> 。 `vserver services name-service dns create` 命令会执行自动配置验证、如果ONTAP无法联系到名称服务器、则会报告错误消息。

2. 使用验证名称服务器的状态 `vserver services name-service dns check` 命令：

```
vserver services name-service dns check -vserver vs1.example.com
                                      Name Server
Vserver             Name Server     Status       Status Details
-------------       --------------- ------------
--------------------------
vs1.example.com     10.0.0.50       up           Response time (msec): 2
vs1.example.com     10.0.0.51       up           Response time (msec): 2
```

有关与DNS相关的服务策略的信息、请参见 "ONTAP 9.6 及更高版本中的 LIF 和服务策略"。

配置名称服务切换表以进行主机名解析

您必须正确配置名称服务切换表，以使 ONTAP 能够查询本地或外部名称服务以检索主机信息。

开始之前

您必须已确定要在环境中使用哪个名称服务进行主机映射。

步骤

1. 将必要的条目添加到名称服务切换表：

```
vserver services name-service ns-switch modify -vserver <vserver_name>
-database <database_name> -source <source_names>
```

2. 验证名称服务切换表是否包含所需顺序的预期条目：

```
vserver services name-service ns-switch show -vserver <vserver_name>
```

示例

以下示例将修改SVM VS1的名称服务切换表中的一个条目、使其首先使用本地主机文件、然后使用外部DNS服务器解析主机名：

```
vserver services name-service ns-switch modify -vserver vs1 -database
hosts -sources files,dns
```

管理主机表（仅限集群管理员）

集群管理员可以在管理 Storage Virtual Machine （ SVM ）的主机表中添加，修改，删除和查看主机名条目。SVM 管理员只能为分配的 SVM 配置主机名条目。

用于管理本地主机名条目的命令

您可以使用 `vserver services name-service dns hosts` 用于创建、修改或删除DNS主机表条目的命令。

在创建或修改 DNS 主机名条目时，您可以指定多个别名地址，并用逗号分隔。

如果您要 ...	使用此命令 ...
创建 DNS 主机名条目	`vserver services name-service dns hosts create`
修改 DNS 主机名条目	`vserver services name-service dns hosts modify`
删除 DNS 主机名条目	`vserver services name-service dns hosts delete`

有关详细信息，请参见 "ONTAP 9 命令" 。 `vserver services name-service dns hosts` 命令

保护您的网络安全

使用联邦信息处理标准（ **FIPS** ）配置网络安全性

对于所有 SSL 连接， ONTAP 均符合联邦信息处理标准（ FIPS ） 140-2 的要求。您可以在 ONTAP 中打开和关闭 SSL FIPS 模式，全局设置 SSL 协议以及关闭 RC4 等任何弱密码。

默认情况下， ONTAP 上的 SSL 设置为禁用 FIPS 合规性，并启用 SSL 协议，其中包括以下内容：

- TLSv1.3 (从ONTAP 9.11.1开始)
- TLSv1.2
- TLSv1.1
- TLSv1.

启用 SSL FIPS 模式后，从 ONTAP 到外部客户端或 ONTAP 外部服务器组件的 SSL 通信将使用 FIPS 兼容的 SSL 加密。

如果您希望管理员帐户使用 SSH 公有密钥访问 SVM ，则在启用 SSL FIPS 模式之前，必须确保主机密钥算法受支持。

注： ONTAP 9.11.1及更高版本对主机密钥算法的支持已发生更改。

ONTAP 版本	支持的密钥类型	不支持的密钥类型
9.11.1及更高版本	ECDSA-SHA2-nistp256	RSA-SHA2-512 RSA-SHA2-256 SSS-ed25519及更高 SSS-DSS SSS-RSA

9.10.1及更早版本	ECDSA-SHA2-nistp256 SSS-ed25519	SSS-DSS SSS-RSA

在启用 FIPS 之前，必须使用支持的密钥类型重新配置不具有受支持密钥算法的现有 SSH 公有密钥帐户，否则管理员身份验证将失败。

有关详细信息，请参见 "启用 SSH 公有密钥帐户"。

有关SSL FIPS模式配置的详细信息、请参见 `security config modify` 手册页。

启用 **FIPS**

建议所有安全用户在系统安装或升级后立即调整其安全配置。启用 SSL FIPS 模式后，从 ONTAP 到外部客户端或 ONTAP 外部服务器组件的 SSL 通信将使用 FIPS 兼容的 SSL 加密。

> 启用FIPS后、您不能安装或创建RSA密钥长度为4096的证书。

步骤

1. 更改为高级权限级别：

   ```
   set -privilege advanced
   ```

2. 启用FIPS：

   ```
   security config modify -interface SSL -is-fips-enabled true
   ```

3. 当系统提示您继续时、输入 `y`
4. 如果您运行的是 ONTAP 9.8 或更早版本，请逐个手动重新启动集群中的每个节点。从 ONTAP 9.1.1 开始，不需要重新启动。

示例

如果您运行的是 ONTAP 9.9.1 或更高版本，则不会看到警告消息。

```
security config modify -interface SSL -is-fips-enabled true

Warning: This command will enable FIPS compliance and can potentially
cause some non-compliant components to fail. MetroCluster and Vserver DR
require FIPS to be enabled on both sites in order to be compatible.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

禁用 **FIPS**

如果您仍在运行较旧的系统配置，并且希望为 ONTAP 配置向后兼容性，则只有在禁用 FIPS 时才能打开 SSLv3。

步骤

1. 更改为高级权限级别：

   ```
   set -privilege advanced
   ```

2. 通过键入以下命令禁用 FIPS：

   ```
   security config modify -interface SSL -is-fips-enabled false
   ```

3. 当系统提示您继续时、输入 `y`。
4. 如果您运行的是 ONTAP 9.8 或更早版本，请手动重新启动集群中的每个节点。从 ONTAP 9.1.1 开始，不需要重新启动。

示例

如果您运行的是 ONTAP 9.9.1 或更高版本，则不会看到警告消息。

```
security config modify -interface SSL -supported-protocols SSLv3

Warning: Enabling the SSLv3 protocol may reduce the security of the
interface, and is not recommended.
Do you want to continue? {y|n}: y

Warning: When this command completes, reboot all nodes in the cluster.
This is necessary to prevent components from failing due to an
inconsistent security configuration state in the cluster. To avoid a
service outage, reboot one node at a time and wait for it to completely
initialize before rebooting the next node. Run "security config status
show" command to monitor the reboot status.
Do you want to continue? {y|n}: y
```

查看 **FIPS** 合规状态

您可以查看整个集群是否正在运行当前安全配置设置。

步骤

1. 逐个重新启动集群中的每个节点。

   请勿同时重新启动所有集群节点。要确保集群中的所有应用程序都运行新的安全配置，并对 FIPS 开关模式，协议和密码进行所有更改，需要重新启动。

2. 查看当前合规状态：

   ```
   security config show
   ```

```
security config show

          Cluster                                                 Cluster
Security
Interface FIPS Mode  Supported Protocols     Supported Ciphers Config
Ready
--------- ---------- ----------------------- -----------------
----------------
SSL       false      TLSv1_2, TLSv1_1, TLSv1 ALL:!LOW:!aNULL:  yes
                                             !EXP:!eNULL
```

通过线缆加密配置 IP 安全性（ IP security ， IPsec ）

ONTAP在传输模式下使用互联网协议安全性(Internet Protocol Security、IPsec)来确保数据持续安全和加密、即使在传输过程中也是如此。IPsec 为所有 IP 流量提供数据加密，包括 NFS ， iSCSI 和 SMB 协议。

从ONTAP 9.12.1开始、MetroCluster IP和MetroCluster 光纤连接配置支持前端主机协议IPsec。MetroCluster 集群中的IPsec支持仅限于前端主机流量、MetroCluster 集群间LIF不支持。

从 ONTAP 9.10.1 开始，您可以使用预共享密钥（ PSK ）或证书通过 IPsec 进行身份验证。以前， IPsec 仅支持 PSK 。

从ONTAP 9.1.1开始、IPsec使用的加密算法已通过FIPS 140-2验证。这些算法由ONTAP 中的NetApp加密模块生成、该模块执行FIPS 140-2验证。

从ONTAP 9.8开始、ONTAP支持在传输模式下使用IPsec。

配置 IPsec 后，客户端和 ONTAP 之间的网络流量将通过预防措施得到保护，以防止重放和中间人（ MIM ）攻击。

对于 NetApp SnapMirror 和集群对等流量加密，仍然建议使用集群对等加密（ Cluster peering encryption ， CPE ）和传输层安全（ Transport Layer Security ， TLS ）而不是通过 IPsec 进行，以便通过线缆进行安全传输。这是因为 TLS 的性能优于 IPsec 。

在集群上启用了 IPsec 功能时，网络需要使用安全策略数据库（ SPD ）条目来匹配要保护的流量，并指定保护详细信息（例如密码套件和身份验证方法），然后才能使流量流动。每个客户端上也需要相应的 SPD 条目。

在集群上启用 **IPsec**

您可以在集群上启用 IPsec ，以确保数据持续安全和加密，即使在传输期间也是如此。

步骤

1. 发现是否已启用 IPsec：

   ```
   security ipsec config show
   ```

   如果结果包括 `IPsec Enabled: false`下，继续下一步。

2. 启用 IPsec：

   ```
   security ipsec config modify -is-enabled true
   ```

3. 再次运行 discovery 命令：

   ```
   security ipsec config show
   ```

   结果现在包括 `IPsec Enabled: true`。

准备使用证书身份验证创建**IPsec**策略

如果您仅使用预共享密钥(PSK)进行身份验证、而不使用证书身份验证、则可以跳过此步骤。

在创建使用证书进行身份验证的IPsec策略之前，必须验证是否满足以下前提条件：

- ONTAP和客户端都必须安装另一方的CA证书、以使最终实体(ONTAP或客户端)证书可由双方验证
- 系统会为参与此策略的 ONTAP LIF 安装证书

ONTAP LIF 可以共享证书。不需要在证书和 LIF 之间进行一对一映射。

步骤

1. 将在相互身份验证期间使用的所有CA证书(包括ONTAP端和客户端CA)安装到ONTAP证书管理中、除非已安装(例如ONTAP自签名根CA)。

   命令示例
   ```
   cluster::> security certificate install -vserver svm_name -type server-ca
   -cert-name my_ca_cert
   ```

2. 要确保安装的CA在身份验证期间位于IPsec CA搜索路径内、请使用将ONTAP证书管理CA添加到IPsec模块 `security ipsec ca-certificate add` 命令：

   命令示例
   ```
   cluster::> security ipsec ca-certificate add -vserver svm_name -ca-certs
   my_ca_cert
   ```

3. 创建并安装一个证书以供 ONTAP LIF 使用。此证书的颁发者 CA 必须已安装到 ONTAP 并添加到 IPsec 中。

   命令示例
   ```
   cluster::> security certificate install -vserver svm_name -type server -cert
   -name my_nfs_server_cert
   ```

有关ONTAP中证书的详细信息，请参见ONTAP 9文档中的security certificates命令。

定义安全策略数据库（ **SPD** ）

在允许流量在网络上流动之前， IPsec 需要 SPD 条目。无论您使用的是 PSk 还是证书进行身份验证，都是如此。

步骤

1. 使用 `security ipsec policy create` 命令：
   a. 选择要参与 ONTAP 传输的 IPsec IP 地址或 IP 地址子网。
   b. 选择要连接到 ONTAP IP 地址的客户端 IP 地址。

      客户端必须使用预共享密钥（ psk ）支持 Internet 密钥交换版本 2 （ IKEv2 ）。

   c. 可选。选择细化的流量参数、例如上层协议(UDP、TCP、ICMP等))、本地端口号和用于保护流量的远程端口号。相应的参数为 `protocols`， `local-ports` 和 `remote-ports` 。

      跳过此步骤可保护 ONTAP IP 地址和客户端 IP 地址之间的所有流量。默认情况下，保护所有流量。

   d. 为输入PSK或公共密钥基础架构(PKI) `auth-method` 所需身份验证方法的参数。
      i. 如果输入PSK、请包含参数、然后按<enter>显示提示、以输入并验证预共享密钥。

         `local-identity` 和 `remote-identity` 如果主机和客户端均使用strong、并且未为主机或客户端选择通配符策略、则参数为可选参数。

ii. 如果输入PKI、则还需要输入 `cert-name`， `local-identity`， `remote-identity` parameters 如果远程端证书标识未知、或者如果需要多个客户端标识、请输入特殊标识 `ANYTHING`。

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32
Enter the preshared key for IPsec Policy _test34_ on Vserver _vs1_:
```

```
security ipsec policy create -vserver vs1 -name test34 -local-ip-subnets
192.168.134.34/32 -remote-ip-subnets 192.168.134.44/32 -local-ports 2049
-protocols tcp -auth-method PKI -cert-name my_nfs_server_cert -local
-identity CN=netapp.ipsec.lif1.vs0 -remote-identity ANYTHING
```

只有在ONTAP和客户端都设置了匹配的IPsec策略并且身份验证凭据(PSK或证书)在两端都到位之后、IP流量才能在客户端和服务器之间流动。有关详细信息、请参见客户端IPsec配置。

使用 **IPsec** 身份

对于预共享密钥身份验证方法、如果主机和客户端都使用strong、并且未为主机或客户端选择通配符策略、则本地和远程标识是可选的。

对于 PKI/ 证书身份验证方法，本地和远程身份都是必需的。这些身份用于指定在每一方的证书中进行认证并在验证过程中使用的身份。如果远程身份未知或可能是多个不同的身份、请使用特殊身份 `ANYTHING`。

关于此任务

在 ONTAP 中，标识是通过修改 SPD 条目或在创建 SPD 策略期间指定的。SPD 可以是 IP 地址或字符串格式的标识名称。

步骤

要修改现有SPD标识设置、请使用以下命令：

```
security ipsec policy modify
```

命令示例

security ipsec policy modify -vserver *vs1* -name *test34* -local-identity *192.168.134.34* -remote-identity *client.fooboo.com*

IPsec 多客户端配置

如果少数客户端需要利用 IPsec ，则为每个客户端使用一个 SPD 条目就足以满足要求。但是，当数百甚至数千个客户端需要利用 IPsec 时， NetApp 建议使用 IPsec 多客户端配置。

关于此任务

ONTAP 支持将多个网络中的多个客户端连接到启用了 IPsec 的单个 SVM IP 地址。您可以使用以下方法之一完成此操作：

- * 子网配置 *

要允许特定子网上的所有客户端(例如192.168.134.0/24)使用单个SPD策略条目连接到单个SVM IP地址、必须指定 `remote-ip-subnets` 子网形式。此外、您还必须指定 `remote-identity` 具有正确客户端标识的字段。

> 在子网配置中使用单个策略条目时，该子网中的 IPsec 客户端将共享 IPsec 身份和预共享密钥（ PSk ）。但是，对于证书身份验证，情况并非如此。使用证书时，每个客户端都可以使用自己的唯一证书或共享证书进行身份验证。ONTAP IPsec 会根据安装在其本地信任存储上的 CA 检查证书的有效性。ONTAP 还支持证书撤消列表（ Certificate Revocation List ， CRL ）检查。

- * 允许所有客户端配置 *

  要允许任何客户端(无论其源IP地址如何)连接到已启用SVM IPsec的IP地址、请使用 `0.0.0.0/0` 指定时使用通配符 `remote-ip-subnets` 字段。

  此外、您还必须指定 `remote-identity` 具有正确客户端标识的字段。对于证书身份验证、您可以输入 `ANYTHING`。

  此外、当 `0.0.0.0/0` 如果使用通配符、则必须配置要使用的特定本地或远程端口号。例如： `NFS port 2049`。

  步骤

  a. 使用以下命令之一为多个客户端配置IPsec。

     i. 如果使用*subnetconfiguration (子网配置)*支持多个IPsec客户端：

     ```
     security ipsec policy create -vserver vserver_name -name policy_name
     -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets
     IP_address/subnet -local-identity local_id -remote-identity remote_id
     ```

     命令示例

     ```
     security ipsec policy create -vserver vs1 -name subnet134 -local-ip-subnets
     192.168.134.34/32 -remote-ip-subnets 192.168.134.0/24 -local-identity
     ontap_side_identity -remote-identity client_side_identity
     ```

     i. 如果使用*允许所有客户端配置*支持多个IPsec客户端：

     ```
     security ipsec policy create -vserver vserver_name -name policy_name
     -local-ip-subnets IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local
     -ports port_number -local-identity local_id -remote-identity remote_id
     ```

     命令示例

     ```
     security ipsec policy create -vserver vs1 -name test35 -local-ip-subnets
     IPsec_IP_address/32 -remote-ip-subnets 0.0.0.0/0 -local-ports 2049 -local
     -identity ontap_side_identity -remote-identity client_side_identity
     ```

IPsec 统计信息

通过协商，可以在 ONTAP SVM IP 地址和客户端 IP 地址之间建立一个称为 "ike 安全关联（ SA） " 的安全通道。IPsec SAS 安装在两个端点上，用于执行实际的数据加密和解密工作。

您可以使用 statistics 命令来检查 IPsec SAS 和 ike SAS 的状态。

命令示例

IKESA 命令示例：

```
security ipsec show-ikesa -node hosting_node_name_for_svm_ip
```

IPsec SA 命令和输出示例：

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip
```

```
cluster1::> security ipsec show-ikesa -node cluster1-node1
            Policy Local           Remote
Vserver     Name   Address         Address         Initator-SPI     State
----------- ------ --------------- --------------- ----------------
-----------
vs1         test34
                   192.168.134.34  192.168.134.44  c764f9ee020cec69
ESTABLISHED
```

IPsec SA 命令和输出示例：

```
security ipsec show-ipsecsa -node hosting_node_name_for_svm_ip

cluster1::> security ipsec show-ipsecsa -node cluster1-node1
            Policy  Local           Remote          Inbound  Outbound
Vserver     Name    Address         Address         SPI      SPI
State
----------- ------- --------------- --------------- -------- --------
---------
vs1         test34
                    192.168.134.34  192.168.134.44  c4c5b3d6 c2515559
INSTALLED
```

为 LIF 配置防火墙策略

设置防火墙可增强集群的安全性，并有助于防止未经授权访问存储系统。默认情况下，板载防火墙配置为允许远程访问数据，管理和集群间 LIF 的一组特定 IP 服务。

从 ONTAP 9.10.1 开始：

- 防火墙策略已弃用、并由LIF服务策略取代。以前，板载防火墙是使用防火墙策略进行管理的。现在，可以使用 LIF 服务策略来实现此功能。
- 所有防火墙策略均为空，不会打开底层防火墙中的任何端口。而是必须使用 LIF 服务策略打开所有端口。
- 升级到9.10.1或更高版本后、无需执行任何操作即可从防火墙策略过渡到LIF服务策略。系统会根据上一

个ONTAP 版本中使用的防火墙策略自动构建LIF服务策略。如果您使用脚本或其他工具创建和管理自定义防火墙策略，则可能需要升级这些脚本以创建自定义服务策略。

要了解更多信息，请参见 "ONTAP 9.6 及更高版本中的 LIF 和服务策略"。

防火墙策略可用于控制对 SSH ， HTTP ， HTTPS ， Telnet ， NTP ， NDMP ， NDMPS ， RSH ， DNS 或 SNMP 。无法为 NFS 或 SMB 等数据协议设置防火墙策略。

您可以通过以下方式管理防火墙服务和策略：

- 启用或禁用防火墙服务
- 显示当前防火墙服务配置
- 使用指定的策略名称和网络服务创建新的防火墙策略
- 将防火墙策略应用于逻辑接口
- 创建与现有策略完全相同的新防火墙策略

  您可以使用此选项在同一 SVM 中创建具有类似特征的策略，或者将此策略复制到其他 SVM 。

- 显示有关防火墙策略的信息
- 修改防火墙策略使用的 IP 地址和网络掩码
- 删除 LIF 未使用的防火墙策略

防火墙策略和 **LIF**

LIF 防火墙策略用于限制通过每个 LIF 对集群的访问。您需要了解默认防火墙策略如何影响通过每种类型的 LIF 进行的系统访问，以及如何自定义防火墙策略以通过 LIF 提高或降低安全性。

使用配置LIF时 `network interface create` 或 `network interface modify` 命令、即为指定的值 `-firewall-policy` 参数用于确定允许访问LIF的服务协议和IP地址。

在许多情况下，您可以接受默认防火墙策略值。在其他情况下，您可能需要限制对某些 IP 地址和某些管理服务协议的访问。可用的管理服务协议包括 SSH ， HTTP ， HTTPS ， Telnet ， NTP ， NDMP ， NDMPS ， RSH ， DNS 和 SNMP 。

所有集群SIFs的防火墙策略默认为 `""` 并且无法修改。

下表介绍了在创建 LIF 时分配给每个 LIF 的默认防火墙策略，具体取决于其角色（ ONTAP 9.5 及更早版本）或服务策略（ ONTAP 9.6 及更高版本）：

防火墙策略	默认服务协议	默认访问	应用于的 LIF
管理	DNS ， http ， https ， NDMP ， NDMPS ， NTP ， SNMP ， ssh	任何地址（ 0.0.0.0/0 ）	集群管理， SVM 管理和节点管理 LIF

MGMT-NFS	DNS ， http ， https ， NDMP ， NDMPS ， NTP ，端口映射， SNMP ， ssh	任何地址（ 0.0.0.0/0 ）	也支持 SVM 管理访问的数据 LIF
集群间	HTTPS ， NDMP ， NDMPS	任何地址（ 0.0.0.0/0 ）	所有集群间 LIF
数据	DNS ， NDMP ， NDMPS ， portmap	任何地址（ 0.0.0.0/0 ）	所有数据 LIF

portmap 服务配置

portmap 服务会将 RPC 服务映射到它们侦听的端口。

portmap 服务在 ONTAP 9.3 及更早版本中始终可访问，在 ONTAP 9.4 至 ONTAP 9.6 中可配置，并从 ONTAP 9.7 开始自动进行管理。

- 在 ONTAP 9.3 及更早版本中， portmap 服务（ rpcbind ）始终可通过网络配置中的端口 111 访问，该端口依赖于内置的 ONTAP 防火墙，而不是第三方防火墙。
- 从 ONTAP 9.4 到 ONTAP 9.6 ，您可以修改防火墙策略，以控制是否可通过特定 LIF 访问 portmap 服务。
- 从 ONTAP 9.7 开始，不再使用 portmap 防火墙服务。而是会自动为支持 NFS 服务的所有 LIF 打开 portmap 端口。
- 在 ONTAP 9.4 到 ONTAP 9.6* 中，可以在防火墙中配置端口映射服务

本主题的其余部分将讨论如何为 ONTAP 9.4 到 ONTAP 9.6 版配置 portmap 防火墙服务。

根据您的配置，您可能会禁止对特定类型的 LIF （通常为管理 LIF 和集群间 LIF ）访问服务。在某些情况下，您甚至可以禁止对数据 LIF 进行访问。

您可以预期的行为

ONTAP 9.4 到 ONTAP 9.6 的行为旨在在升级时实现无缝过渡。如果 portmap 服务已通过特定类型的 LIF 进行访问，则它将继续通过这些类型的 LIF 进行访问。与ONTAP 9.3及更早版本一样、您可以在防火墙策略中为LIF类型指定可在防火墙内访问的服务。

要使此行为生效，集群中的所有节点都必须运行 ONTAP 9.4 到 ONTAP 9.6 。仅影响入站流量。

新规则如下：

- 升级到 9.4 到 9.6 版后， ONTAP 会将 portmap 服务添加到所有现有防火墙策略中，默认或自定义。
- 在创建新集群或新 IP 空间时， ONTAP 仅会将 portmap 服务添加到默认数据策略中，而不会添加到默认管理或集群间策略中。
- 您可以根据需要将 portmap 服务添加到默认策略或自定义策略中，并根据需要删除此服务。

如何添加或删除**portmap**服务

要将 portmap 服务添加到 SVM 或集群防火墙策略中（使其可在防火墙内访问），请输入：

```
system services firewall policy create -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

要从 SVM 或集群防火墙策略中删除 portmap 服务（使其无法在防火墙内访问），请输入：

```
system services firewall policy delete -vserver SVM -policy
mgmt|intercluster|data|custom -service portmap
```

您可以使用 network interface modify 命令将防火墙策略应用于现有 LIF 。有关完整的命令语法，请参见 "ONTAP 9 命令"。

创建防火墙策略并将其分配给 **LIF**

创建 LIF 时，系统会为每个 LIF 分配默认防火墙策略。在许多情况下，默认防火墙设置运行良好，您无需更改它们。如果要更改可访问 LIF 的网络服务或 IP 地址，可以创建自定义防火墙策略并将其分配给 LIF 。

关于此任务

- 您不能使用创建防火墙策略 `policy` name `data`， `intercluster`， `cluster`或 `mgmt`。

  这些值是为系统定义的防火墙策略保留的。

- 您不能为集群 LIF 设置或修改防火墙策略。

  对于所有服务类型，集群 LIF 的防火墙策略均设置为 0.0.0.0/0 。

- 如果需要从策略中删除服务，则必须删除现有防火墙策略并创建新策略。
- 如果集群上启用了 IPv6 ，则可以使用 IPv6 地址创建防火墙策略。

  启用IPv6后、 `data`， `intercluster`，和 `mgmt` 防火墙策略的可接受地址列表中包括：：： /0 (IPv6通配符)。

- 在使用 System Manager 跨集群配置数据保护功能时，您必须确保允许列表中包含集群间 LIF IP 地址，并且允许在集群间 LIF 和公司拥有的防火墙上使用 HTTPS 服务。

  默认情况下、 `intercluster` 防火墙策略允许从所有IP地址(0.0.0.0/0或：：： /0表示IPv6)进行访问、并启用HTTPS、NDMP和NDMP服务。如果修改此默认策略，或者为集群间 LIF 创建自己的防火墙策略，则必须将每个集群间 LIF IP 地址添加到允许列表中并启用 HTTPS 服务。

- 从 ONTAP 9.6 开始，不支持 HTTPS 和 SSH 防火墙服务。

  在ONTAP 9.6中、 `management-https` 和 `management-ssh` LIF服务可用于HTTPS和SSH管理访问。

步骤

1. 创建可供特定 SVM 上的 LIF 使用的防火墙策略：

   ```
   system services firewall policy create -vserver vserver_name -policy
   policy_name -service network_service -allow-list ip_address/mask
   ```

   您可以多次使用此命令为防火墙策略中的每个服务添加多个网络服务和允许的 IP 地址列表。

2. 使用验证是否已正确添加此策略 `system services firewall policy show` 命令：

3. 将防火墙策略应用于 LIF：

   `network interface modify -vserver` *`vserver_name`* `-lif` *`lif_name`* `-firewall-policy` *`policy_name`*

4. 使用验证是否已将此策略正确添加到LIF `network interface show -fields firewall-policy` 命令：

创建防火墙策略并将其应用于**LIF**的示例

以下命令将创建一个名为 data_http 的防火墙策略，用于从 10.10 子网上的 IP 地址访问 HTTP 和 HTTPS 协议，并将该策略应用于 SVM vs1 上名为 data1 的 LIF ，然后显示集群上的所有防火墙策略：

```
system services firewall policy create -vserver vs1 -policy data_http
-service http - allow-list 10.10.0.0/16
```

```
system services firewall policy show

Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
vs1
        data_http
                     http       10.10.0.0/16
                     https      10.10.0.0/16

network interface modify -vserver vs1 -lif data1 -firewall-policy
data_http

network interface show -fields firewall-policy

vserver  lif                  firewall-policy
-------  -------------------- ---------------
Cluster  node1_clus_1
Cluster  node1_clus_2
Cluster  node2_clus_1
Cluster  node2_clus_2
cluster-1 cluster_mgmt         mgmt
cluster-1 node1_mgmt1          mgmt
cluster-1 node2_mgmt1          mgmt
vs1      data1                data_http
vs3      data2                data
```

用于管理防火墙服务和策略的命令

您可以使用 `system services firewall` 用于管理防火墙服务的命令 `system services firewall policy` 用于管理防火墙策略的命令、以及 `network interface modify` 用于管理LIFs的防火墙设置的命令。

如果您要 ...	使用此命令 ...
启用或禁用防火墙服务	`system services firewall modify`
显示防火墙服务的当前配置	`system services firewall show`
创建防火墙策略或向现有防火墙策略添加服务	`system services firewall policy create`
将防火墙策略应用于 LIF	`network interface modify -lif lifname -firewall-policy`
修改与防火墙策略关联的 IP 地址和网络掩码	`system services firewall policy modify`
显示有关防火墙策略的信息	`system services firewall policy show`
创建一个与现有策略完全相同的新防火墙策略	`system services firewall policy clone`
删除 LIF 未使用的防火墙策略	`system services firewall policy delete`

有关详细信息、请参见的手册页 `system services firewall`， `system services firewall policy` ，和 `network interface modify` 中的命令 "ONTAP 9 命令"。

QoS标记(仅限集群管理员)

QoS概述

网络服务质量（ QoS ）标记可帮助您根据网络条件确定不同流量类型的优先级，以便有效地利用网络资源。您可以为每个 IP 空间支持的流量类型设置传出 IP 数据包的差分服务代码点（ DSCP ）值。

UC 合规性的 DSCP 标记

您可以使用默认或用户提供的 DSCP 代码为给定协议的传出（传出） IP 数据包流量启用差分服务代码点（ DSCP ）标记。DSCP 标记是一种对网络流量进行分类和管理的机制，是统一功能（ Unified Capability ， UC ）合规性的组成部分。

DSCP 标记（也称为 *qos marks* 或 *quality of service marks* ）可通过提供 IP 空间，协议和 DSCP 值来启用。可以应用DSCP标记的协议包括NFS、SMB、iSCSI、SnapMirror、NDMP、 FTP、HTTP/HTTPS、SSH、Telnet和SNMP。

如果在为给定协议启用 DSCP 标记时未提供 DSCP 值，则会使用默认值：

- 数据协议 / 流量的默认值为 0x0A （ 10 ）。
- 控制协议 / 流量的默认值为 0x30 （ 48 ）。

修改 **QoS** 标记值

您可以为每个 IP 空间修改不同协议的服务质量（ QoS ）标记值。

开始之前

集群中的所有节点都必须运行相同版本的 ONTAP 。

步骤

使用修改QoS标记值 `network qos-marking modify` 命令：

- 。 `-ipspace` 参数用于指定要修改QoS标记条目的IP空间。
- 。 `-protocol` 参数用于指定要修改QoS标记条目的协议。。 `network qos-marking modify` 手册页介绍了此协议的可能值。
- 。 `-dscp` 参数用于指定差分服务代码点(DSCP)值。可能的值介于 0 到 63 之间。
- 。 `-is-enabled` 参数用于在提供的IP空间中为指定协议启用或禁用QoS标记 `-ipspace` 参数。

以下命令将在默认 IP 空间中为 NFS 协议启用 QoS 标记：

```
network qos-marking modify -ipspace Default -protocol NFS -is-enabled true
```

以下命令会将默认 IP 空间中 NFS 协议的 DSCP 值设置为 20 ：

```
network qos-marking modify -ipspace Default -protocol NFS -dscp 20
```

显示 **QoS** 标记值

您可以为每个 IP 空间显示不同协议的 QoS 标记值。

步骤

使用显示QoS标记值 `network qos-marking show` 命令：

以下命令显示默认 IP 空间中所有协议的 QoS 标记：

```
network qos-marking show -ipspace Default
IPspace              Protocol            DSCP  Enabled?
------------------- ----------------- -----  --------
Default
                     CIFS                  10  false
                     FTP                   48  false
                     HTTP-admin            48  false
                     HTTP-filesrv          10  false
                     NDMP                  10  false
                     NFS                   10  true
                     SNMP                  48  false
                     SSH                   48  false
                     SnapMirror            10  false
                     Telnet                48  false
                     iSCSI                 10  false
11 entries were displayed.
```

管理SNMP (仅限集群管理员)

SNMP概述

您可以将 SNMP 配置为监控集群中的 SVM ，以便在出现问题之前避免出现问题，并在出现问题时对问题做出响应。管理 SNMP 涉及配置 SNMP 用户以及为所有 SNMP 事件配置 SNMP 陷阱主机目标（管理工作站）。默认情况下， SNMP 在数据 LIF 上处于禁用状态。

您可以在数据 SVM 中创建和管理只读 SNMP 用户。必须配置数据 LIF 以接收 SVM 上的 SNMP 请求。

SNMP 网络管理工作站或管理器可以向 SVM SNMP 代理查询相关信息。SNMP 代理会收集信息并将其转发给 SNMP 管理器。SNMP 代理还会在发生特定事件时生成陷阱通知。SVM 上的 SNMP 代理具有只读权限；不能用于任何设置的操作或针对陷阱采取更正操作。ONTAP 提供了一个与 SNMP v1 ， v2c 和 v3 版本兼容的 SNMP 代理。SNMPv3 通过使用密码短语和加密提供高级安全性。

有关 ONTAP 系统中 SNMP 支持的详细信息，请参见 "TR-4220： Data ONTAP 中的 SNMP 支持"。

MIB概述

MIB （管理信息库）是一个文本文件，用于描述 SNMP 对象和陷阱。

MIB 用于描述存储系统管理数据的结构，它们使用包含对象标识符（ OID ）的分层命名空间。每个 OID 标识一个可使用 SNMP 读取的变量。

由于 MIB 不是配置文件，并且 ONTAP 不会读取这些文件，因此 SNMP 功能不受 MIB 的影响。ONTAP 提供了以下 MIB 文件：

- NetApp自定义MIB (`netapp.mib`)

ONTAP 支持 IPv6 （ RFC 2465 ）， TCP （ RFC 4022 ）， UDP （ RFC 4113 ）和 ICMP （ RFC 2466 ）

MIB ，这些 MIB 可显示 IPv4 和 IPv6 数据。

ONTAP还在中的对象标识符(OID)和对象短名称之间提供了一个简短的交叉引用 `traps.dat` 文件

> ONTAP MIB 和“traps.dat”文件的最新版本可从 NetApp 支持站点获得。但是，支持站点上这些文件的版本不一定与 ONTAP 版本的 SNMP 功能相对应。提供这些文件是为了帮助您评估最新 ONTAP 版本中的 SNMP 功能。

SNMP 陷阱

SNMP 陷阱用于捕获系统监控信息，此信息将作为异步通知从 SNMP 代理发送到 SNMP 管理器。

SNMP 陷阱有三种类型：标准陷阱，内置陷阱和用户定义的陷阱。ONTAP 不支持用户定义的陷阱。

可以使用陷阱定期检查 MIB 中定义的操作阈值或故障。如果达到阈值或检测到故障， SNMP 代理会向陷阱主机发送一条消息（陷阱），提醒其发生此事件。

> ONTAP 支持 SNMPv1 陷阱，并在 ONTAP 9.1 中启动 SNMPv3 陷阱。ONTAP 不支持 SNMPv2c 陷阱和通知。

标准 **SNMP** 陷阱

这些陷阱在 RFC 1215 中定义。ONTAP 支持五个标准 SNMP 陷阱： coldstart ， warmStart ， linkDown ， linkUp 和 authenticationFailure 。

> 默认情况下， authenticationFailure 陷阱处于禁用状态。您必须使用 `system snmp authtrap` 命令以启用陷阱。有关详细信息，请参见手册页： "ONTAP 9 命令"

内置 **SNMP** 陷阱

内置陷阱在 ONTAP 中预定义，如果发生事件，它们会自动发送到陷阱主机列表上的网络管理工作站。这些陷阱，例如 diskFailedShutdown ， cpuTooBusy 和 volumeNearlyFull ，均在自定义 MIB 中定义。

每个内置陷阱都由一个唯一的陷阱代码标识。

创建 **SNMP** 社区并将其分配给 **LIF**

使用 SNMPv1 和 SNMPv2c 时，您可以创建 SNMP 社区，作为管理工作站和 Storage Virtual Machine （ SVM ）之间的身份验证机制。

通过在数据SVM中创建SNMP社区、您可以执行等命令 `snmpwalk` 和 `snmpget` 在数据生命周期中。

关于此任务

- 在新安装的 ONTAP 中， SNMPv1 和 SNMPv2c 默认处于禁用状态。

  创建 SNMP 社区后， SNMPv1 和 SNMPv2c 将处于启用状态。

- ONTAP 支持只读社区。
- 默认情况下、分配给数据"LIF"的"数据"防火墙策略会将SNMP服务设置为 `deny`。

您必须创建一个新的防火墙策略、并将SNMP服务设置为 `allow` 为数据SVM创建SNMP用户时。

> 从ONTAP 9.10.1开始、防火墙策略已弃用、并完全替换为LIF服务策略。有关详细信息，请参见 "为 LIF 配置防火墙策略"。

- 您可以为管理 SVM 和数据 SVM 的 SNMPv1 和 SNMPv2c 用户创建 SNMP 社区。
- 由于SVM不是SNMP标准的一部分、因此对数据NetApp的查询必须包括SVM根OID (1.3.6.1.4.1.789)、例如 `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`。

步骤

1. 使用创建SNMP社区 `system snmp community add` 命令：以下命令显示如何在管理 SVM cluster-1 中创建 SNMP 社区：

   ```
   system snmp community add -type ro -community-name comty1 -vserver
   cluster-1
   ```

   以下命令显示如何在数据 SVM vs1 中创建 SNMP 社区：

   ```
   system snmp community add -type ro -community-name comty2 -vserver vs1
   ```

2. 使用 system snmp community show 命令验证是否已创建社区。

   以下命令显示了为 SNMPv1 和 SNMPv2c 创建的两个社区：

   ```
   system snmp community show
   cluster-1
   rocomty1
   vs1
   rocomty2
   ```

3. 使用检查"data"防火墙策略中是否允许SNMP作为服务 `system services firewall policy show` 命令：

   以下命令显示默认 "data" 防火墙策略中不允许使用 SNMP 服务（仅 "mgmt" 防火墙策略中允许使用 SNMP 服务）：

```
system services firewall policy show
Vserver Policy       Service    Allowed
------- ------------ ---------- -------------------
cluster-1
        data
                     dns        0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        intercluster
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
cluster-1
        mgmt
                     dns        0.0.0.0/0
                     http       0.0.0.0/0
                     https      0.0.0.0/0
                     ndmp       0.0.0.0/0
                     ndmps      0.0.0.0/0
                     ntp        0.0.0.0/0
                     snmp       0.0.0.0/0
                     ssh        0.0.0.0/0
```

4. 使用创建允许访问的新防火墙策略 `snmp` 服务 `system services firewall policy create` 命令：

   以下命令将创建一个名为data1的新数据防火墙策略、此策略允许使用 `snmp`

```
system services firewall policy create -policy data1 -service snmp
-vserver  vs1 -allow-list 0.0.0.0/0

cluster-1::> system services firewall policy show -service snmp
Vserver  Policy       Service    Allowed
-------  ------------ ---------- -------------------
cluster-1
         mgmt
                       snmp       0.0.0.0/0
vs1
         data1
                       snmp       0.0.0.0/0
```

5. 使用带有 -firewall-policy 参数的 `network interface modify `命令将防火墙策略应用于数据 LIF 。

   以下命令会将新的 "data1" 防火墙策略分配给 LIF "datalif1"：

```
network interface modify -vserver vs1 -lif datalif1 -firewall-policy
data1
```

在集群中配置 **SNMPv3** 用户

与 SNMPv1 和 SNMPv2c 相比， SNMPv3 是一种安全协议。要使用 SNMPv3 ，必须将 SNMPv3 用户配置为从 SNMP 管理器运行 SNMP 实用程序。

步骤

使用 security login create 命令创建 SNMPv3 用户。

系统将提示您提供以下信息：

- 引擎 ID ： 默认值和建议值为本地引擎 ID
- 身份验证协议
- 身份验证密码
- 隐私协议
- 隐私协议密码

结果

SNMPv3 用户可以使用用户名和密码从 SNMP 管理器登录并运行 SNMP 实用程序命令。

SNMPv3 安全参数

SNMPv3 包括一项身份验证功能，如果选择此功能，则要求用户在调用命令时输入其名称，身份验证协议，身份验证密钥以及所需的安全级别。

下表列出了 SNMPv3 安全参数：

参数	命令行选项	Description
引擎 ID	-e 引擎 ID	SNMP 代理的引擎 ID 。默认值为 local EngineID （建议）。
securityName	-u 名称	用户名不得超过 32 个字符。
authProtocol	-a ｛none	md5
SHA	SHA-256 ｝	身份验证类型可以为 none ， MD5 ， SHA 或 SHA-256 。
authkey	-A 密码短语	至少包含八个字符的密码短语。
安全性级别	-l ｛authNoPriv	AuthPriv

noAuthNoPriv }	安全级别可以是 " 身份验证 "， " 无隐私 "， " 身份验证 "， " 隐私 " 或 " 无身份验证 "， 无隐私。	特权协议
-x ｛ none	des	aes128 }
隐私协议可以是 none ，DES 或 aes128	privPassword	-X 密码

不同安全级别的示例

此示例显示了使用不同安全级别创建的SNMPv3用户如何使用SNMP客户端命令、例如 `snmpwalk`，以查询群集对象。

为了提高性能，您应检索表中的所有对象，而不是表中的单个对象或几个对象。

> 您必须使用 `snmpwalk` 5.3.1或更高版本(如果身份验证协议为SHA)。

安全级别： **AuthPriv**

以下输出显示了使用 authPriv 安全级别创建 SNMPv3 用户的过程。

```
security login create -user-or-group-name snmpv3user -application snmp
-authentication-method usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha, sha2-
256) [none]: md5

Enter the authentication protocol password (minimum 8 characters long):
Enter the authentication protocol password again:
Which privacy protocol do you want to choose (none, des, aes128) [none]:
des
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

FIPS 模式

```
security login create -username snmpv3user -application snmp -authmethod
usm
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (sha, sha2-256) [sha]

Enter authentication protocol password (minimum 8 characters long):
Enter authentication protocol password again:
Which privacy protocol do you want to choose (aes128) [aes128]:
Enter privacy protocol password (minimum 8 characters long):
Enter privacy protocol password again:
```

snmpwalk 测试

以下输出显示了运行 snmpwalk 命令的 SNMPv3 用户：

为了提高性能，您应检索表中的所有对象，而不是表中的单个对象或几个对象。

```
$ snmpwalk -v 3 -u snmpv3user -a SHA -A password1! -x DES -X password1! -l
authPriv 192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

安全级别： **AuthNoPriv**

以下输出显示了使用 authNoPriv 安全级别创建 SNMPv3 用户的过程。

```
security login create -username snmpv3user1 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: md5
```

FIPS 模式

FIPS不允许您为隐私协议选择*无*。因此、无法在FIPS模式下配置authNo特权SNMPv3用户。

snmpwalk 测试

以下输出显示了运行 snmpwalk 命令的 SNMPv3 用户：

为了提高性能，您应检索表中的所有对象，而不是表中的单个对象或几个对象。

```
$ snmpwalk -v 3 -u snmpv3user1 -a MD5 -A password1!  -l authNoPriv
192.0.2.62 .1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

安全级别： **noAuthNoPriv**

以下输出显示了创建具有 noAuthNoPriv 安全级别的 SNMPv3 用户的过程。

```
security login create -username snmpv3user2 -application snmp -authmethod
usm -role admin
Enter the authoritative entity's EngineID [local EngineID]:
Which authentication protocol do you want to choose (none, md5, sha)
[none]: none
```

FIPS 模式

FIPS不允许您为隐私协议选择*无*。

snmpwalk 测试

以下输出显示了运行 snmpwalk 命令的 SNMPv3 用户：

为了提高性能，您应检索表中的所有对象，而不是表中的单个对象或几个对象。

```
$ snmpwalk -v 3 -u snmpv3user2 -l noAuthNoPriv 192.0.2.62
.1.3.6.1.4.1.789.1.5.8.1.2
Enterprises.789.1.5.8.1.2.1028 = "vol0"
Enterprises.789.1.5.8.1.2.1032 = "vol0"
Enterprises.789.1.5.8.1.2.1038 = "root_vs0"
Enterprises.789.1.5.8.1.2.1042 = "root_vstrap"
Enterprises.789.1.5.8.1.2.1064 = "vol1"
```

配置陷阱主机以接收 **SNMP** 通知

您可以将陷阱主机（ SNMP 管理器）配置为在集群中生成 SNMP 陷阱时接收通知（ SNMP 陷阱 PDU ）。您可以指定 SNMP 陷阱主机的主机名或 IP 地址（ IPv4 或 IPv6 ）。

开始之前

- 必须在集群上启用 SNMP 和 SNMP 陷阱。

默认情况下， SNMP 和 SNMP 陷阱处于启用状态。

- 必须在集群上配置 DNS 以解析陷阱主机名称。
- 要使用 IPv6 地址配置 SNMP 陷阱主机，必须在集群上启用 IPv6 。
- 对于 ONTAP 9.1 及更高版本，在创建陷阱主机时，您必须已指定预定义的基于用户的安全模型（ USM ）身份验证和隐私凭据。

步骤

添加 SNMP 陷阱主机：

```
system snmp traphost add
```

只有在至少将一个 SNMP 管理工作站指定为陷阱主机时，才能发送陷阱。

以下命令将使用已知的 USM 用户添加一个名为 yyy.example.com 的新 SNMPv3 陷阱主机：

```
system snmp traphost add -peer-address yyy.example.com -usm-username
MyUsmUser
```

以下命令将使用主机的 IPv6 地址添加陷阱主机：

```
system snmp traphost add -peer-address 2001:0db8:1:1:209:6bff:feae:6d67
```

用于管理 **SNMP** 的命令

您可以使用 `system snmp` 用于管理SNMP、陷阱和陷阱主机的命令。您可以使用 `security` 用于管理每个SVM的SNMP用户的命令。您可以使用 `event` 用于管理与SNMP陷阱相关的事件的命令。

用于配置 **SNMP** 的命令

如果您要 …	使用此命令 …
在集群上启用 SNMP	`options -option-name snmp.enable -option-value on` 管理（ mgmt ）防火墙策略下必须允许 SNMP 服务。您可以使用 system services firewall policy show 命令验证是否允许使用 SNMP 。
在集群上禁用 SNMP	`options -option-name snmp.enable -option-value off`

用于管理 **SNMP v1 ， v2c** 和 **v3** 用户的命令

如果您要 …	使用此命令 …
配置 SNMP 用户	`security login create`
显示 SNMP 用户	`security snmpusers and security login show -application snmp`
删除 SNMP 用户	`security login delete`
修改 SNMP 用户登录方法的访问控制角色名称	`security login modify`

用于提供联系人和位置信息的命令

如果您要 …	使用此命令 …
显示或修改集群的联系详细信息	`system snmp contact`
显示或修改集群的位置详细信息	`system snmp location`

用于管理 **SNMP** 社区的命令

如果您要 …	使用此命令 …
为 SVM 或集群中的所有 SVM 添加只读（ ro ）社区	`system snmp community add`
删除一个社区或所有社区	`system snmp community delete`
显示所有社区的列表	`system snmp community show`

由于SVM不是SNMP标准的一部分、因此对数据NetApp的查询必须包括SVM根OID (1.3.6.1.4.1.789)、例如 `snmpwalk -v 2c -c snmpNFS 10.238.19.14 1.3.6.1.4.1.789`。

用于显示 **SNMP** 选项值的命令

如果您要 …	使用此命令 …
显示所有 SNMP 选项的当前值，包括集群联系人，联系人位置，集群是否配置为发送陷阱，陷阱主机列表以及社区列表和访问控制类型	`system snmp show`

用于管理 **SNMP** 陷阱和陷阱主机的命令

如果您要 …	使用此命令 …

启用从集群发送的 SNMP 陷阱	`system snmp init -init 1`
禁用从集群发送的 SNMP 陷阱	`system snmp init -init 0`
添加一个陷阱主机，用于接收集群中特定事件的 SNMP 通知	`system snmp traphost add`
删除陷阱主机	`system snmp traphost delete`
显示陷阱主机的列表	`system snmp traphost show`

用于管理与 **SNMP** 陷阱相关的事件的命令

如果您要 …	使用此命令 …
显示为其生成 SNMP 陷阱（内置）的事件	`event route show` 使用 `-snmp-support true` 参数以仅查看与SNMP相关的事件。 使用 `instance -messagename <message>` 参数、以查看事件可能发生的原因的详细问题描述以及任何更正操作。 不支持将单个 SNMP 陷阱事件路由到特定陷阱主机目标。所有 SNMP 陷阱事件都会发送到所有陷阱主机目标。
显示 SNMP 陷阱历史记录的列表，这些记录是已发送到 SNMP 陷阱的事件通知	`event snmphistory show`
删除 SNMP 陷阱历史记录	`event snmphistory delete`

有关的详细信息、请参见 `system snmp`， `security`，和 `event` 命令、请参见手册页： "ONTAP 9 命令"

管理 SVM 中的路由

SVM路由概述

SVM 的路由表决定了 SVM 与目标进行通信所使用的网络路径。了解路由表的工作原理非常重要，这样您就可以在发生网络问题之前防患于未然。

路由规则如下：

- ONTAP 会通过最特定的可用路由路由流量。

- 当更多特定路由不可用时， ONTAP 会作为最后一种方法通过默认网关路由（具有 0 位网络掩码）路由流量。

如果路由的目标，网络掩码和度量指标相同，则无法保证系统在重新启动后或升级后使用相同的路由。如果您配置了多个默认路由，则此问题描述尤其如此。

最佳做法是，仅为 SVM 配置一个默认路由。为避免中断，您应确保默认路由能够访问更特定的路由无法访问的任何网络地址。有关详细信息，请参见知识库文章 "SU134： 集群模式 ONTAP 中的路由配置不正确，可能会中断网络访问"

创建静态路由。

您可以在 Storage Virtual Machine （ SVM ）中创建静态路由，以控制 LIF 使用网络传输出站流量的方式。

在创建与 SVM 关联的路由条目时，此路由将由指定 SVM 拥有的所有 LIF 使用，这些 LIF 与网关位于同一子网上。

步骤

使用 `network route create` 用于创建路由的命令。

```
network route create -vserver vs0 -destination 0.0.0.0/0 -gateway
10.61.208.1
```

启用多路径路由

如果多个路由对一个目标具有相同的度量指标，则只会为传出流量选择其中一个路由。这会导致其他路由无法用于发送传出流量。您可以启用多路径路由以平衡负载并利用所有可用路由。

步骤

1. 登录到高级权限级别：

   ```
   set -privilege advanced
   ```

2. 启用多路径路由：

   ```
   network options multipath-routing modify -is-enabled true
   ```

   已为集群中的所有节点启用多路径路由。

```
network options multipath-routing modify -is-enabled true
```

删除静态路由

您可以从 Storage Virtual Machine （ SVM ）中删除不需要的静态路由。

步骤

使用 `network route delete` 用于删除静态路由的命令。

有关此命令的详细信息、请参见 `network route` 手册页： "ONTAP 9 命令"。

以下示例将删除与网关为 10.63.0.1 且目标 IP 地址为 0.0.0.0/0 的 SVM vs0 关联的静态路由：

```
network route delete -vserver vs0 -gateway 10.63.0.1 -destination
0.0.0.0/0
```

显示路由信息

您可以显示集群上每个 SVM 的路由配置信息。这有助于您诊断涉及客户端应用程序或服务与集群中节点上的 LIF 之间连接问题的路由问题。

步骤

1. 使用 `network route show` 命令以显示一个或多个SVM中的路由。以下示例显示了 vs0 SVM 中配置的路由：

   ```
   network route show
     (network route show)
   Vserver             Destination     Gateway         Metric
   ------------------- --------------- --------------- ------
   vs0
                       0.0.0.0/0       172.17.178.1    20
   ```

2. 使用 `network route show-lifs` 命令以显示一个或多个SVM中的路由和LUN的关联。

   以下示例显示了由 vs0 SVM 拥有路由的 LIF ：

   ```
   network route show-lifs
     (network route show-lifs)

   Vserver: vs0
   Destination             Gateway                 Logical Interfaces
   ----------------------  --------------          --------------------
   0.0.0.0/0               172.17.178.1            cluster_mgmt,
                                                   LIF-b-01_mgmt1,
                                                   LIF-b-02_mgmt1
   ```

3. 使用 `network route active-entry show` 命令以显示一个或多个节点、SVM、子网或具有指定目标的路由上的已安装路由。

   以下示例显示了特定 SVM 上安装的所有路由：

```
network route active-entry show -vserver Data0

Vserver: Data0
Node: node-1
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-1
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.0.1               127.0.0.1            lo              10  UHS

Vserver: Data0
Node: node-2
Subnet Group: 0.0.0.0/0
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
127.0.10.1              127.0.20.1           losk            10  UHS
127.0.20.1              127.0.20.1           losk            10  UHS

Vserver: Data0
Node: node-2
Subnet Group: fd20:8b1e:b255:814e::/64
Destination             Gateway              Interface   Metric  Flags
----------------------  -------------------  ---------   ------  -----
default                 fd20:8b1e:b255:814e::1
                                             e0d             20  UGS
fd20:8b1e:b255:814e::/64
                        link#4               e0d              0  UC
fd20:8b1e:b255:814e::1  link#4               e0d              0  UHL
```

```
11 entries were displayed.
```

从路由表中删除动态路由

收到 IPv4 和 IPv6 的 ICMP 重定向后，动态路由将添加到路由表中。默认情况下，动态路由会在 300 秒后删除。如果要将动态路由保留不同的时间，可以更改超时值。

关于此任务

您可以将超时值设置为 0 到 65 ， 535 秒。如果将此值设置为 0 ，则路由永不过期。删除动态路由可防止因持续存在无效路由而导致连接断开。

步骤

1. 显示当前超时值。
   - 对于 IPv4：

     ```
     network tuning icmp show
     ```

   - 对于IPv6：

     ```
     network tuning icmp6 show
     ```

2. 修改超时值。
   - 对于 IPv4：

     ```
     network tuning icmp modify -node node_name -redirect-timeout
     timeout_value
     ```

   - 对于IPv6：

     ```
     network tuning icmp6 modify -node node_name -redirect-v6-timeout
     timeout_value
     ```

3. 验证是否已正确修改超时值。
   - 对于 IPv4：

     ```
     network tuning icmp show
     ```

   - 对于IPv6：

```
network tuning icmp6 show
```

查看网络信息

查看网络信息概述

使用命令行界面、您可以查看与端口、生命周期、路由、故障转移规则、故障转移组、 防火墙规则、DNS、NIS和连接。从ONTAP 9.8开始、您还可以下载System Manager中显示的网络数据。

在重新配置网络设置等情况下或对集群进行故障排除时，此信息非常有用。

如果您是集群管理员，则可以查看所有可用的网络信息。如果您是 SVM 管理员，则只能查看与分配的 SVM 相关的信息。

在System Manager中，当您在_List View_中显示信息时，您可以单击*Download*，显示的对象列表将被下载。

- 此列表将以逗号分隔值（ CSV ）格式下载。
- 仅下载可见列中的数据。
- CSV 文件名采用对象名称和时间戳的格式。

显示网络端口信息

您可以显示有关特定端口或集群中所有节点上所有端口的信息。

关于此任务

此时将显示以下信息：

- Node name
- 端口名称
- IPspace 名称
- 广播域名
- 链路状态（已启动或已关闭）
- MTU 设置
- 端口速度设置和运行状态（每秒 1 千兆位或 10 千兆位）
- 自动协商设置（ true 或 false ）
- 双工模式和运行状态（半双工或全满）
- 端口的接口组（如果适用）
- 端口的 VLAN 标记信息（如果适用）
- 端口的运行状况（运行状况或已降级）

- 端口标记为已降级的原因

如果字段的数据不可用(例如、非活动端口的操作双工和速度将不可用)、则字段值将列为 `-`。

步骤

使用显示网络端口信息 `network port show` 命令：

您可以通过指定来显示每个端口的详细信息 `-instance` 参数、或者通过使用指定字段名称来获取特定信息 `-fields` 参数。

```
network port show
Node: node1

Ignore
                                                     Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  degraded
false
e0d       Default      Default          up   1500  auto/1000  degraded
true
Node: node2

Ignore
                                                     Speed(Mbps) Health
Health
Port      IPspace      Broadcast Domain Link MTU  Admin/Oper  Status
Status
--------- ------------ ---------------- ---- ---- ----------- --------
------
e0a       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0b       Cluster      Cluster          up   9000  auto/1000  healthy
false
e0c       Default      Default          up   1500  auto/1000  healthy
false
e0d       Default      Default          up   1500  auto/1000  healthy
false
8 entries were displayed.
```

显示有关 **VLAN** 的信息（仅限集群管理员）

您可以显示有关特定 VLAN 或集群中所有 VLAN 的信息。

关于此任务

您可以通过指定来显示每个VLAN的详细信息 `-instance` 参数。您可以通过使用指定字段名称来显示特定信息 `-fields` 参数。

步骤

使用显示有关VLAN的信息 `network port vlan show` 命令：以下命令显示有关集群中所有 VLAN 的信息：

```
network port vlan show
                  Network Network
Node   VLAN Name Port    VLAN ID  MAC Address
------ --------- ------- -------- -----------------
cluster-1-01
       a0a-10    a0a     10       02:a0:98:06:10:b2
       a0a-20    a0a     20       02:a0:98:06:10:b2
       a0a-30    a0a     30       02:a0:98:06:10:b2
       a0a-40    a0a     40       02:a0:98:06:10:b2
       a0a-50    a0a     50       02:a0:98:06:10:b2
cluster-1-02
       a0a-10    a0a     10       02:a0:98:06:10:ca
       a0a-20    a0a     20       02:a0:98:06:10:ca
       a0a-30    a0a     30       02:a0:98:06:10:ca
       a0a-40    a0a     40       02:a0:98:06:10:ca
       a0a-50    a0a     50       02:a0:98:06:10:ca
```

显示接口组信息（仅限集群管理员）

您可以显示有关接口组的信息以确定其配置。

关于此任务

此时将显示以下信息：

- 接口组所在的节点
- 接口组中包含的网络端口列表
- 接口组的名称
- 分发功能（ MAC ， IP ，端口或顺序）
- 接口组的介质访问控制（ MAC ）地址
- 端口活动状态；即所有聚合端口是否均处于活动状态（完全参与），某些端口是否处于活动状态（部分参与）或是否无处于活动状态

步骤

使用显示有关接口组的信息 `network port ifgrp show` 命令：

您可以通过指定来显示每个节点的详细信息 `-instance` 参数。您可以通过使用指定字段名称来显示特定信息 `-fields` 参数。

以下命令显示集群中所有接口组的相关信息：

```
network port ifgrp show
         Port     Distribution                    Active
Node     IfGrp    Function     MAC Address        Ports   Ports
-------- -------- ------------ -----------------  ------- --------
cluster-1-01
         a0a      ip           02:a0:98:06:10:b2  full    e7a, e7b
cluster-1-02
         a0a      sequential   02:a0:98:06:10:ca  full    e7a, e7b
cluster-1-03
         a0a      port         02:a0:98:08:5b:66  full    e7a, e7b
cluster-1-04
         a0a      mac          02:a0:98:08:61:4e  full    e7a, e7b
```

以下命令显示单个节点的详细接口组信息：

```
network port ifgrp show -instance -node cluster-1-01

                  Node: cluster-1-01
 Interface Group Name: a0a
Distribution Function: ip
        Create Policy: multimode
          MAC Address: 02:a0:98:06:10:b2
   Port Participation: full
        Network Ports: e7a, e7b
             Up Ports: e7a, e7b
           Down Ports: -
```

显示 **LIF** 信息

您可以查看有关 LIF 的详细信息以确定其配置。

您可能还需要查看此信息以诊断基本的 LIF 问题，例如检查重复的 IP 地址或验证网络端口是否属于正确的子网。Storage Virtual Machine （ SVM ）管理员只能查看与 SVM 关联的 LIF 的信息。

关于此任务

此时将显示以下信息：

- 与 LIF 关联的 IP 地址
- LIF 的管理状态
- LIF 的运行状态

  数据 LIF 的运行状态取决于与数据 LIF 关联的 SVM 的状态。停止 SVM 后， LIF 的运行状态将更改为 down 。当 SVM 重新启动时，运行状态将更改为 up

- 节点以及 LIF 所在的端口

如果字段的数据不可用(例如、如果没有扩展状态信息)、则字段值将列为 –。

步骤

使用 network interface show 命令显示 LIF 信息。

您可以通过指定 -instance 参数来查看每个 LIF 的详细信息，也可以通过使用 -fields 参数指定字段名称来获取特定信息。

以下命令显示有关集群中所有 LIF 的常规信息：

```
network interface show
           Logical    Status     Network          Current      Current Is
Vserver    Interface  Admin/Oper Address/Mask     Node         Port
Home
---------- ---------- ---------- ---------------- ------------ -------
----
example
           lif1         up/up    192.0.2.129/22   node-01
                                                               e0d
false
node
           cluster_mgmt up/up    192.0.2.3/20     node-02
                                                               e0c
false
node-01
           clus1        up/up    192.0.2.65/18    node-01
                                                               e0a
true
           clus2        up/up    192.0.2.66/18    node-01
                                                               e0b
true
           mgmt1        up/up    192.0.2.1/20     node-01
                                                               e0c
true
node-02
           clus1        up/up    192.0.2.67/18    node-02
                                                               e0a
true
           clus2        up/up    192.0.2.68/18    node-02
                                                               e0b
true
           mgmt2        up/up    192.0.2.2/20     node-02
                                                               e0d
true
vs1
           d1           up/up    192.0.2.130/21   node-01
                                                               e0d
false
           d2           up/up    192.0.2.131/21   node-01
                                                               e0d
true
           data3        up/up    192.0.2.132/20   node-02
                                                               e0c
true
```

以下命令显示有关单个 LIF 的详细信息：

```
network interface show -lif data1 -instance

                    Vserver Name: vs1
          Logical Interface Name: data1
                            Role: data
                   Data Protocol: nfs,cifs
                       Home Node: node-01
                       Home Port: e0c
                    Current Node: node-03
                    Current Port: e0c
              Operational Status: up
                 Extended Status: -
                         Is Home: false
                 Network Address: 192.0.2.128
                         Netmask: 255.255.192.0
             Bits in the Netmask: 18
                 IPv4 Link Local: -
                     Subnet Name: -
           Administrative Status: up
                 Failover Policy: local-only
                 Firewall Policy: data
                     Auto Revert: false
   Fully Qualified DNS Zone Name: xxx.example.com
         DNS Query Listen Enable: false
             Failover Group Name: Default
                         FCP WWPN: -
                  Address family: ipv4
                         Comment: -
                  IPspace of LIF: Default
```

显示路由信息

您可以显示有关 SVM 中路由的信息。

步骤

根据要查看的路由信息类型，输入相应的命令：

要查看有关以下内容的信息 ...	输入 ...
静态路由，每个 SVM	`network route show`
每个 SVM 的每个路由上的 LIF	`network route show-lifs`

您可以通过指定来显示每个路由的详细信息 `-instance` 参数。以下命令显示集群 1 中 SVM 内的静态路由：

```
network route show
Vserver             Destination     Gateway         Metric
------------------- --------------- --------------- ------
Cluster
                    0.0.0.0/0       10.63.0.1       10
cluster-1
                    0.0.0.0/0       198.51.9.1      10
vs1
                    0.0.0.0/0       192.0.2.1       20
vs3
                    0.0.0.0/0       192.0.2.1       20
```

以下命令显示 cluster-1 中所有 SVM 中静态路由和逻辑接口（ LIF ）的关联：

```
network route show-lifs
Vserver: Cluster
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               10.63.0.1               -

Vserver: cluster-1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               198.51.9.1              cluster_mgmt,
                                                cluster-1_mgmt1,

Vserver: vs1
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data1_1, data1_2

Vserver: vs3
Destination             Gateway                 Logical Interfaces
----------------------  ----------------------  -------------------
0.0.0.0/0               192.0.2.1               data2_1, data2_2
```

显示 **DNS** 主机表条目（仅限集群管理员）

DNS 主机表条目会将主机名映射到 IP 地址。您可以显示集群中所有 SVM 的主机名和别名及其映射到的 IP 地址。

步骤

使用 vserver services name-service dns hosts show 命令显示所有 SVM 的主机名条目。

以下示例显示了主机表条目：

```
vserver services name-service dns hosts show
Vserver    Address        Hostname        Aliases
---------- -------------- --------------- ---------------------
cluster-1
           10.72.219.36   lnx219-36       -
vs1
           10.72.219.37   lnx219-37       lnx219-37.example.com
```

您可以使用 `vserver services name-service dns` 命令以在SVM上启用DNS、并将其配置为使用DNS进行主机名解析。主机名可使用外部 DNS 服务器进行解析。

显示 DNS 域配置

您可以显示集群中一个或多个 Storage Virtual Machine （ SVM ）的 DNS 域配置，以验证其配置是否正确。

步骤

使用查看DNS域配置 `vserver services name-service dns show` 命令：

以下命令显示集群中所有 SVM 的 DNS 配置：

```
vserver services name-service dns show
                                                  Name
Vserver        State     Domains                  Servers
-------------- --------- ------------------------ -------------
cluster-1       enabled   xyz.company.com          192.56.0.129,
                                                  192.56.0.130
vs1            enabled   xyz.company.com          192.56.0.129,
                                                  192.56.0.130
vs2            enabled   xyz.company.com          192.56.0.129,
                                                  192.56.0.130
vs3            enabled   xyz.company.com          192.56.0.129,
                                                  192.56.0.130
```

以下命令显示 SVM vs1 的详细 DNS 配置信息：

```
vserver services name-service dns show -vserver vs1
               Vserver: vs1
               Domains: xyz.company.com
          Name Servers: 192.56.0.129, 192.56.0.130
    Enable/Disable DNS: enabled
        Timeout (secs): 2
      Maximum Attempts: 1
```

显示有关故障转移组的信息

您可以查看有关故障转移组的信息，包括每个故障转移组中的节点和端口列表，是否已启用或禁用故障转移以及应用于每个 LIF 的故障转移策略类型。

步骤

1. 使用显示每个故障转移组的目标端口 `network interface failover-groups show` 命令：

   以下命令显示有关双节点集群上所有故障转移组的信息：

   ```
   network interface failover-groups show
                                 Failover
   Vserver        Group          Targets
   -------------- -------------- ---------------------------------
   Cluster
                  Cluster
                                 cluster1-01:e0a, cluster1-01:e0b,
                                 cluster1-02:e0a, cluster1-02:e0b
   vs1
                  Default
                                 cluster1-01:e0c, cluster1-01:e0d,
                                 cluster1-01:e0e, cluster1-02:e0c,
                                 cluster1-02:e0d, cluster1-02:e0e
   ```

2. 使用显示特定故障转移组的目标端口和广播域 `network interface failover-groups show` 命令：

   以下命令显示 SVM vs4 的故障转移组 data12 的详细信息：

```
network interface failover-groups show -vserver vs4 -failover-group
data12

       Vserver Name: vs4
Failover Group Name: data12
   Failover Targets: cluster1-01:e0f, cluster1-01:e0g, cluster1-02:e0f,
                     cluster1-02:e0g
   Broadcast Domain: Default
```

3. 使用显示所有LI使用的故障转移设置 `network interface show` 命令：

   以下命令显示每个 LIF 正在使用的故障转移策略和故障转移组：

```
network interface show -vserver * -lif * -fields failover-
group,failover-policy
vserver   lif                  failover-policy        failover-group
--------  ------------------   ---------------------  --------------
Cluster   cluster1-01_clus_1   local-only             Cluster
Cluster   cluster1-01_clus_2   local-only             Cluster
Cluster   cluster1-02_clus_1   local-only             Cluster
Cluster   cluster1-02_clus_2   local-only             Cluster
cluster1  cluster_mgmt         broadcast-domain-wide  Default
cluster1  cluster1-01_mgmt1    local-only             Default
cluster1  cluster1-02_mgmt1    local-only             Default
vs1       data1                disabled               Default
vs3       data2                system-defined         group2
```

显示 LIF 故障转移目标

您可能需要检查 LIF 的故障转移策略和故障转移组是否配置正确。为了防止故障转移规则配置不当，您可以显示一个 LIF 或所有 LIF 的故障转移目标。

关于此任务

通过显示 LIF 故障转移目标，您可以检查以下内容：

- LIF 是否配置了正确的故障转移组和故障转移策略
- 生成的故障转移目标端口列表是否适用于每个 LIF
- 数据 LIF 的故障转移目标是否不是管理端口（ e0M ）

步骤

使用显示LIF的故障转移目标 `failover` 的选项 `network interface show` 命令：

以下命令显示有关双节点集群中所有 LIF 的故障转移目标的信息。。 `Failover Targets` 行显示给定LIF的节

点-端口组合(按优先级排序)列表。

```
network interface show -failover
         Logical       Home                  Failover        Failover
Vserver  Interface     Node:Port             Policy          Group
-------- ------------- --------------------- --------------- ---------
Cluster
         node1_clus1   node1:e0a             local-only      Cluster
                       Failover Targets: node1:e0a,
                                         node1:e0b
         node1_clus2   node1:e0b             local-only      Cluster
                       Failover Targets: node1:e0b,
                                         node1:e0a
         node2_clus1   node2:e0a             local-only      Cluster
                       Failover Targets: node2:e0a,
                                         node2:e0b
         node2_clus2   node2:e0b             local-only      Cluster
                       Failover Targets: node2:e0b,
                                         node2:e0a
cluster1
         cluster_mgmt  node1:e0c             broadcast-domain-wide
                                                             Default
                       Failover Targets: node1:e0c,
                                         node1:e0d,
                                         node2:e0c,
                                         node2:e0d
         node1_mgmt1   node1:e0c             local-only      Default
                       Failover Targets: node1:e0c,
                                         node1:e0d
         node2_mgmt1   node2:e0c             local-only      Default
                       Failover Targets: node2:e0c,
                                         node2:e0d
vs1
         data1         node1:e0e             system-defined  bcast1
                       Failover Targets: node1:e0e,
                                         node1:e0f,
                                         node2:e0e,
                                         node2:e0f
```

显示负载平衡区域中的 LIF

您可以通过显示属于负载平衡区域的所有 LIF 来验证是否已正确配置该区域。您还可以查看特定 LIF 的负载平衡区域或所有 LIF 的负载平衡区域。

步骤

使用以下命令之一显示所需的 LIF 和负载平衡详细信息

要显示 ...	输入 ...
特定负载平衡区域中的 LIF	`network interface show -dns-zone zone_name` `zone_name` 指定负载平衡区域的名称。
特定 LIF 的负载平衡区域	`network interface show -lif lif_name -fields dns-zone`
所有 LIF 的负载平衡区域	`network interface show -fields dns-zone`

显示 **LIF** 的负载平衡区域的示例

以下命令显示 SVM vs0 的负载平衡区域 storage.company.com 中所有 LIF 的详细信息：

```
net int show -vserver vs0 -dns-zone storage.company.com

         Logical    Status     Network            Current   Current Is
Vserver  Interface  Admin/Oper Address/Mask       Node      Port    Home
-------- ---------- ---------- ------------------ --------- ------- ----
vs0
         lif3         up/up    10.98.226.225/20  ndeux-11  e0c     true
         lif4         up/up    10.98.224.23/20   ndeux-21  e0c     true
         lif5         up/up    10.98.239.65/20   ndeux-11  e0c     true
         lif6         up/up    10.98.239.66/20   ndeux-11  e0c     true
         lif7         up/up    10.98.239.63/20   ndeux-21  e0c     true
         lif8         up/up    10.98.239.64/20   ndeux-21  e0c     true
```

以下命令显示 LIF data3 的 DNS 区域详细信息：

```
network interface show -lif data3 -fields dns-zone
Vserver  lif    dns-zone
-------  -----  --------
vs0      data3  storage.company.com
```

以下命令显示集群中所有 LIF 的列表及其对应的 DNS 区域：

```
network interface show -fields dns-zone
Vserver   lif          dns-zone
-------   ------------ --------
cluster   cluster_mgmt none
ndeux-21  clus1        none
ndeux-21  clus2        none
ndeux-21  mgmt1        none
vs0       data1        storage.company.com
vs0       data2        storage.company.com
```

显示集群连接

您可以按客户端，逻辑接口，协议或服务显示集群中的所有活动连接或节点上的活动连接计数。您还可以显示集群中的所有侦听连接。

按客户端显示活动连接（仅限集群管理员）

您可以按客户端查看活动连接，以验证特定客户端正在使用的节点，并查看每个节点的客户端数量之间可能存在的不平衡。

关于此任务

在以下情况下，按客户端显示的活动连接数非常有用：

- 查找繁忙或过载的节点。
- 确定特定客户端对卷的访问速度较慢的原因。

  您可以查看有关客户端正在访问的节点的详细信息，然后将其与卷所在的节点进行比较。如果访问卷需要遍历集群网络，则客户端可能会因远程访问超额预订的远程节点上的卷而导致性能下降。

- 验证所有节点是否均用于数据访问。
- 查找连接数意外高的客户端。
- 验证某些客户端是否已连接到节点。

步骤

使用按客户端显示节点上的活动连接计数 `network connections active show-clients` 命令：

有关此命令的详细信息，请参见手册页： "ONTAP 9 命令"

```
network connections active show-clients
Node    Vserver Name    Client IP Address     Count
------  --------------  -----------------     ------
node0   vs0             192.0.2.253                1
        vs0             192.0.2.252                2
        Cluster         192.10.2.124               5
node1   vs0             192.0.2.250                1
        vs0             192.0.2.252                3
        Cluster         192.10.2.123               4
node2   vs1             customer.example.com       1
        vs1             192.0.2.245                3
        Cluster         192.10.2.122               4
node3   vs1             customer.example.org       1
        vs1             customer.example.net       3
        Cluster         192.10.2.121               4
```

按协议显示活动连接（仅限集群管理员）

您可以按协议（ TCP 或 UDP ）显示节点上的活动连接计数，以比较集群中协议的使用情况。

关于此任务

在以下情况下，按协议显示的活动连接数非常有用：

- 查找断开连接的 UDP 客户端。

  如果某个节点接近其连接限制，则 UDP 客户端将最先被丢弃。

- 验证是否未使用任何其他协议。

步骤

使用按协议显示节点上的活动连接计数 `network connections active show-protocols` 命令：

有关此命令的详细信息，请参见手册页。

```
network connections active show-protocols
Node      Vserver Name  Protocol   Count
-------   ------------  ---------  ------
node0
          vs0           UDP            19
          Cluster       TCP            11
node1
          vs0           UDP            17
          Cluster       TCP             8
node2
          vs1           UDP            14
          Cluster       TCP            10
node3
          vs1           UDP            18
          Cluster       TCP             4
```

按服务显示活动连接（仅限集群管理员）

您可以按服务类型（例如 NFS ， SMB ，挂载等）显示集群中每个节点的活动连接计数。这对于比较集群中的服务使用情况非常有用，有助于确定节点的主工作负载。

关于此任务

在以下情况下，按服务显示的活动连接数非常有用：

- 验证所有节点是否都用于相应的服务，以及该服务的负载平衡是否正常工作。
- 验证是否未使用任何其他服务。使用按服务显示节点上的活动连接计数 `network connections active show-services` 命令：

有关此命令的详细信息，请参见手册页： "ONTAP 9 命令"

```
network connections active show-services
Node        Vserver Name    Service    Count
---------  --------------  ---------  ------
node0
           vs0             mount           3
           vs0             nfs            14
           vs0             nlm_v4          4
           vs0             cifs_srv        3
           vs0             port_map       18
           vs0             rclopcp        27
           Cluster         ctlopcp        60
node1
           vs0             cifs_srv        3
           vs0             rclopcp        16
           Cluster         ctlopcp        60
node2
           vs1             rclopcp        13
           Cluster         ctlopcp        60
node3
           vs1             cifs_srv        1
           vs1             rclopcp        17
           Cluster         ctlopcp        60
```

按 **LIF** 显示节点和 **SVM** 上的活动连接

您可以按节点和 Storage Virtual Machine （ SVM ）显示每个 LIF 的活动连接计数，以查看集群中 LIF 之间的连接不平衡。

关于此任务

在以下情况下，按 LIF 显示的活动连接数非常有用：

- 通过比较每个 LIF 上的连接数来查找过载的 LIF 。
- 验证 DNS 负载平衡是否适用于所有数据 LIF 。
- 比较与各种 SVM 的连接数以查找使用量最多的 SVM 。

步骤

使用按SVM和节点显示每个LIF的活动连接数 `network connections active show-lifs` 命令：

有关此命令的详细信息，请参见手册页： "ONTAP 9 命令"

```
network connections active show-lifs
Node       Vserver Name  Interface Name  Count
--------   ------------  --------------- ------
node0
           vs0           datalif1             3
           Cluster       node0_clus_1         6
           Cluster       node0_clus_2         5
node1
           vs0           datalif2             3
           Cluster       node1_clus_1         3
           Cluster       node1_clus_2         5
node2
           vs1           datalif2             1
           Cluster       node2_clus_1         5
           Cluster       node2_clus_2         3
node3
           vs1           datalif1             1
           Cluster       node3_clus_1         2
           Cluster       node3_clus_2         2
```

显示集群中的活动连接

您可以显示有关集群中活动连接的信息，以查看各个连接使用的 LIF ，端口，远程主机，服务， Storage Virtual Machine （ SVM ）和协议。

关于此任务

在以下情况下，查看集群中的活动连接非常有用：

- 验证各个客户端是否在正确的节点上使用了正确的协议和服务。
- 如果客户端在使用节点，协议和服务的特定组合访问数据时遇到问题，您可以使用此命令查找类似的客户端以进行配置或数据包跟踪比较。

步骤

使用显示集群中的活动连接 `network connections active show` 命令：

有关此命令的详细信息，请参见手册页： "ONTAP 9 命令"

以下命令显示节点 node1 上的活动连接：

```
network connections active show -node node1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ----------------
Node: node1
Cluster  node1_clus_1:50297  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:13387  192.0.2.253:7700    TCP/ctlopcp
Cluster  node1_clus_1:8340   192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:42766  192.0.2.252:7700    TCP/ctlopcp
Cluster  node1_clus_1:36119  192.0.2.250:7700    TCP/ctlopcp
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs3      data2:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
vs3      data2:111           host1.aa.com:12017  UDP/port-map
```

以下命令显示 SVM vs1 上的活动连接：

```
network connections active show -vserver vs1
Vserver  Interface           Remote
Name     Name:Local Port     Host:Port           Protocol/Service
-------  ------------------  ------------------  ----------------
Node: node1
vs1      data1:111           host1.aa.com:10741  UDP/port-map
vs1      data1:111           host1.aa.com:12017  UDP/port-map
```

显示集群中的侦听连接

您可以显示集群中侦听连接的信息，以查看接受给定协议和服务连接的 LIF 和端口。

关于此任务

在以下情况下，查看集群中的侦听连接非常有用：

- 如果客户端与 LIF 的连接始终失败，请验证所需的协议或服务是否正在侦听 LIF 。
- 如果通过另一节点上的 LIF 对某个节点上的卷进行远程数据访问失败，请验证是否在每个集群 LIF 上打开了 UDP/rclopcp 侦听器。
- 如果同一集群中的两个节点之间的 SnapMirror 传输失败，验证是否在每个集群 LIF 上打开了 UDP/rclopcp 侦听器。
- 如果不同集群中两个节点之间的 SnapMirror 传输失败，请验证是否在每个集群间 LIF 上打开了 tcp/ctlopcp 侦听器。

步骤

使用显示每个节点的侦听连接 `network connections listening show` 命令：

```
network connections listening show
Vserver Name     Interface Name:Local Port        Protocol/Service
---------------- -------------------------------  ----------------
Node: node0
Cluster          node0_clus_1:7700                TCP/ctlopcp
vs1              data1:4049                       UDP/unknown
vs1              data1:111                        TCP/port-map
vs1              data1:111                        UDP/port-map
vs1              data1:4046                       TCP/sm
vs1              data1:4046                       UDP/sm
vs1              data1:4045                       TCP/nlm-v4
vs1              data1:4045                       UDP/nlm-v4
vs1              data1:2049                       TCP/nfs
vs1              data1:2049                       UDP/nfs
vs1              data1:635                        TCP/mount
vs1              data1:635                        UDP/mount
Cluster          node0_clus_2:7700                TCP/ctlopcp
```

用于诊断网络问题的命令

您可以使用等命令诊断网络上的问题 `ping`, `traceroute`, `ndp`, 和 `tcpdump`。您也可以使用等命令 `ping6` 和 `traceroute6` 诊断IPv6问题。

如果您要 ...	输入此命令 ...
测试节点是否可以访问网络上的其他主机	`network ping`
测试节点是否可以访问 IPv6 网络上的其他主机	`network ping6`
跟踪 IPv4 数据包到达网络节点的路由	`network traceroute`
跟踪IPv6数据包到达网络节点的路由	`network traceroute6`
管理邻居发现协议（ NDP ）	`network ndp`
显示有关在指定网络接口或所有网络接口上接收和发送的数据包的统计信息	`run -node node_name ifstat` **Note**:此命令可从noberhell中使用。
显示有关从集群中的每个节点和端口发现的相邻设备的信息，包括远程设备类型和设备平台	`network device-discovery show`
查看节点的 CDP 邻居（ ONTAP 仅支持 CDPv1 公告）	`run -node node_name cdpd show-neighbors` **Note**:此命令可从noberhell中使用。
跟踪网络中发送和接收的数据包	`network tcpdump start -node node-name -port port_name` **Note**:此命令可从noberhell中使用。

测量集群间或集群内节点之间的延迟和吞吐量	`network test -path -source-node` *`source_nodename`* *`local`* `-destination -cluster` *`destination_clustername`* `-destination-node` *`destination_nodename`* `-session-type` *`Default`*, *`AsyncMirrorLocal`*, *`AsyncMirrorRemote`*, *`SyncMirrorRemote`*, or *`RemoteDataTransfer`* 有关详细信息，请参见 "性能管理"。

有关这些命令的详细信息，请参见相应的手册页： "ONTAP 9 命令"

显示使用邻居发现协议的网络连接

显示使用邻居发现协议的网络连接

在数据中心中，您可以使用邻居发现协议查看一对物理或虚拟系统及其网络接口之间的网络连接。ONTAP 支持两种邻居发现协议： Cisco 发现协议（ CDP ）和链路层发现协议（ LLDP ）。

通过邻居发现协议，您可以自动发现和查看有关网络中已启用协议的直连设备的信息。每个设备都会公布标识，功能和连接信息。此信息以以以太网帧的形式传输到多播 MAC 地址，并由所有已启用协议的相邻设备接收。

要使两个设备成为邻居，每个设备都必须启用并正确配置一个协议。发现协议功能仅限于直连网络。邻居可以包括启用了协议的设备，例如交换机，路由器，网桥等。ONTAP 支持两种邻居发现协议，可以单独使用，也可以同时使用。

- Cisco 发现协议（ CDP ） *

CDP 是 Cisco Systems 开发的一种专有链路层协议。默认情况下，它在 ONTAP 中对集群端口启用，但必须对数据端口明确启用。

- 链路层发现协议（ LLDP ） *

LLDP 是标准文档 IEEE 802.1AB 中指定的与供应商无关的协议。必须为所有端口显式启用此功能。

使用 **CDP** 检测网络连接

使用 CDP 检测网络连接包括查看部署注意事项，在数据端口上启用它，查看相邻设备以及根据需要调整 CDP 配置值。默认情况下， CDP 在集群端口上处于启用状态。

还必须在任何交换机和路由器上启用 CDP ，才能显示有关相邻设备的信息。

ONTAP 版本	Description
9.10.1及更早版本	集群交换机运行状况监控器还使用 CDP 自动发现集群和管理网络交换机。
9.11.1及更高版本	集群交换机运行状况监控器还使用CDP自动发现集群、存储和管理网络交换机。

相关信息

"系统管理"

使用 CDP 的注意事项

默认情况下， CDP 兼容设备会发送 CDPv2 公告。CDP 兼容设备仅在收到 CDPv1 公告时才会发送 CDPv1 公告。ONTAP 仅支持 CDPv1 。因此，当 ONTAP 节点发送 CDPv1 公告时， CDP 兼容的相邻设备会发回 CDPv1 公告。

在节点上启用 CDP 之前，应考虑以下信息：

- 所有端口均支持 CDP 。
- CDP 公告由处于 up 状态的端口发送和接收。
- 必须在传输和接收设备上启用 CDP ，才能发送和接收 CDP 公告。
- CDP 公告会定期发送，您可以配置时间间隔。
- 更改 LIF 的 IP 地址后，节点会在下一个 CDP 公告中发送更新后的信息。
- ONTAP 9.10.1及更早版本：
  - CDP 始终在集群端口上启用。
  - 默认情况下，所有非集群端口上都会禁用 CDP 。
- ONTAP 9.11.1及更高版本：
  - CDP始终在集群和存储端口上启用。
  - 默认情况下、所有非集群和非存储端口上都会禁用CDP。

> 有时，当节点上的 LIF 发生更改时， CDP 信息不会在接收设备端（例如交换机）进行更新。如果遇到此类问题，应将节点的网络接口配置为 down 状态，然后再配置为 up 状态。

- 只有 IPv4 地址才会在 CDP 公告中公布。
- 对于带有 VLAN 的物理网络端口，该端口上 VLAN 上配置的所有 LIF 都会公布。
- 对于属于接口组的物理端口，该接口组上配置的所有 IP 地址都会在每个物理端口上公布。
- 对于托管 VLAN 的接口组，接口组上配置的所有 LIF 和 VLAN 都会在每个网络端口上公布。
- 由于CDP数据包在端口上限制为不超过1500字节
  配置了大量LIP地址、只能在相邻交换机上报告其中一部分IP地址。

启用或禁用 CDP

要发现并向 CDP 兼容的相邻设备发送公告，必须在集群的每个节点上启用 CDP 。

默认情况下、在ONTAP 9.10.1及更早版本中、CDP会在节点的所有集群端口上启用、并在节点的所有非集群端口上禁用。

默认情况下、在ONTAP 9.11.1及更高版本中、CDP会在节点的所有集群和存储端口上启用、并在节点的所有非集群和非存储端口上禁用。

关于此任务

。 `cdpd.enable` 选项用于控制在节点的端口上启用还是禁用CDP：

- 对于ONTAP 9.10.1及更早版本、on会在非集群端口上启用CDP。
- 对于ONTAP 9.11.1及更高版本、on会在非集群和非存储端口上启用CDP。
- 对于ONTAP 9.10.1及更早版本、off会在非集群端口上禁用CDP；您不能在集群端口上禁用CDP。
- 对于ONTAP 9.11.1及更高版本、off会在非集群和非存储端口上禁用CDP；您不能在集群端口上禁用CDP。

如果在连接到 CDP 兼容设备的端口上禁用 CDP ，则网络流量可能无法优化。

步骤

1. 显示节点或集群中所有节点的当前 CDP 设置：

要查看 CDP 设置 …	输入 …
节点	`run - node <node_name> options cdpd.enable`
集群中的所有节点	`options cdpd.enable`

2. 在节点的所有端口或集群中所有节点的所有端口上启用或禁用 CDP ：

要启用或禁用 CDP ，请执行以下操作 …	输入 …
节点	`run -node node_name options cdpd.enable {on or off}`
集群中的所有节点	`options cdpd.enable {on or off}`

查看 **CDP** 邻居信息

您可以查看有关连接到集群节点的每个端口的相邻设备的信息，前提是该端口连接到 CDP 兼容设备。您可以使用 `network device-discovery show -protocol cdp` 命令以查看邻居信息。

关于此任务

在ONTAP 9.10.1及更早版本中、由于CDP始终为集群端口启用、因此始终会显示这些端口的CDP邻居信息。必须在非集群端口上启用 CDP ，才能显示这些端口的邻居信息。

在ONTAP 9.11.1及更高版本中、由于CDP始终为集群和存储端口启用、因此始终会显示这些端口的CDP邻居信息。必须在非集群和非存储端口上启用CDP、才能显示这些端口的邻居信息。

步骤

显示有关连接到集群中节点上端口的所有 CDP 兼容设备的信息：

```
network device-discovery show -node node -protocol cdp
```

以下命令显示了连接到节点sti2650/212上端口的邻居：

```
network device-discovery show -node sti2650-212 -protocol cdp
Node/       Local  Discovered
Protocol    Port   Device (LLDP: ChassisID)  Interface         Platform
----------- ------ ------------------------- ----------------
----------------
sti2650-212/cdp
            e0M    RTP-LF810-510K37.gdl.eng.netapp.com(SAL1942R8JS)
                                             Ethernet1/14      N9K-
C93120TX
            e0a    CS:RTP-CS01-510K35        0/8               CN1610
            e0b    CS:RTP-CS01-510K36        0/8               CN1610
            e0c    RTP-LF350-510K34.gdl.eng.netapp.com(FDO21521S76)
                                             Ethernet1/21      N9K-
C93180YC-FX
            e0d    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/22      N9K-
C93180YC-FX
            e0e    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/23      N9K-
C93180YC-FX
            e0f    RTP-LF349-510K33.gdl.eng.netapp.com(FDO21521S4T)
                                             Ethernet1/24      N9K-
C93180YC-FX
```

输出列出了连接到指定节点的每个端口的 Cisco 设备。

配置 CDP 消息的保持时间

保持时间是 CDP 公告存储在相邻 CDP 兼容设备的缓存中的时间段。保持时间在每个 CDPv1 数据包中公布，并且每当节点收到 CDPv1 数据包时都会更新。

- 的值 `cdpd.holdtime` 选项应在HA对的两个节点上设置为相同的值。
- 默认保持时间值为 180 秒，但您可以输入 10 秒到 255 秒之间的值。
- 如果在保持时间到期之前删除 IP 地址，则会缓存 CDP 信息，直到保持时间到期为止。

步骤

1. 显示节点或集群中所有节点的当前 CDP 保持时间：

要查看保持时间 …	输入 …
节点	`run -node node_name options cdpd.holdtime`
集群中的所有节点	`options cdpd.holdtime`

2. 在节点的所有端口或集群中所有节点的所有端口上配置 CDP 保持时间：

要设置保持时间 …	输入 …
节点	`run -node node_name options cdpd.holdtime holdtime`
集群中的所有节点	`options cdpd.holdtime holdtime`

设置发送 CDP 公告的间隔

CDP 公告会定期发送到 CDP 邻居。您可以根据网络流量和网络拓扑变化增加或减少发送 CDP 公告的间隔。

- 的值 `cdpd.interval` 选项应在HA对的两个节点上设置为相同的值。
- 默认间隔为 60 秒，但您可以输入一个介于 5 秒到 900 秒之间的值。

步骤

1. 显示节点或集群中所有节点的当前 CDP 公告时间间隔：

要查看间隔 …	输入 …
节点	`run -node node_name options cdpd.interval`
集群中的所有节点	`options cdpd.interval`

2. 配置为节点的所有端口或集群中所有节点的所有端口发送 CDP 公告的间隔：

要设置间隔 …	输入 …
节点	`run -node node_name options cdpd.interval interval`
集群中的所有节点	`options cdpd.interval interval`

查看或清除 CDP 统计信息

您可以查看每个节点上的集群和非集群端口的 CDP 统计信息，以检测潜在的网络连接问题。CDP 统计信息是自上次清除以来累积的。

关于此任务

在ONTAP 9.10.1及更早版本中、由于CDP始终为端口启用、因此始终会显示这些端口上的流量的CDP统计信息。必须在端口上启用CDP、才能显示这些端口的统计信息。

在ONTAP 9.11.1及更高版本中、由于CDP始终为集群和存储端口启用、因此始终为这些端口上的流量显示CDP统计信息。必须在非集群或非存储端口上启用CDP、才能显示这些端口的统计信息。

步骤

显示或清除节点上所有端口的当前 CDP 统计信息：

如果您要 …	输入 …

查看 CDP 统计信息	`run -node node_name cdpd show-stats`
清除 CDP 统计信息	`run -node node_name cdpd zero-stats`

显示和清除统计信息的示例

以下命令显示清除之前的 CDP 统计信息。输出将显示自上次清除统计信息以来已发送和接收的数据包总数。

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:          9116  | Csum Errors:       0  | Unsupported Vers:  4561
 Invalid length:      0  | Malformed:         0  | Mem alloc fails:      0
 Missing TLVs:        0  | Cache overflow:    0  | Other errors:         0

TRANSMIT
 Packets:          4557  | Xmit fails:        0  | No hostname:          0
 Packet truncated:    0  | Mem alloc fails:   0  | Other errors:         0

OTHER
 Init failures:       0
```

以下命令将清除 CDP 统计信息：

```
run -node node1 cdpd zero-stats
```

```
run -node node1 cdpd show-stats

RECEIVE
 Packets:             0  | Csum Errors:       0  | Unsupported Vers:     0
 Invalid length:      0  | Malformed:         0  | Mem alloc fails:      0
 Missing TLVs:        0  | Cache overflow:    0  | Other errors:         0

TRANSMIT
 Packets:             0  | Xmit fails:        0  | No hostname:          0
 Packet truncated:    0  | Mem alloc fails:   0  | Other errors:         0

OTHER
 Init failures:       0
```

清除统计信息后，在发送或接收下一个 CDP 公告后，这些统计信息将开始累积。

使用**LDP**检测网络连接

使用 LLDP 检测网络连接包括查看部署注意事项，在所有端口上启用 LLDP ，查看相邻设备以及根据需要调整 LLDP 配置值。

此外、还必须在任何交换机和路由器上启用CDP、才能显示有关相邻设备的信息。

ONTAP 当前报告以下类型 - 长度 - 值结构（ TLV ）：

- 机箱 ID
- 端口 ID
- 生存时间（ TTL ）
- 系统名称

  系统名称 TLV 不会在 CNA 设备上发送。

某些融合网络适配器（ CNA ）（例如 X1143 适配器和 UTA2 板载端口）包含 LLDP 卸载支持：

- LLDP 卸载用于数据中心桥接（ DCB ）。
- 显示的信息可能因集群和交换机而异。

  对于CNA端口和非CNA端口、交换机显示的机箱ID和端口ID数据可能有所不同。

例如：

- 对于非CNA端口：
  - 机箱ID是节点上某个端口的固定MAC地址
  - port ID是节点上相应端口的端口名称
- 对于CNA端口：
  - 机箱ID和端口ID是节点上相应端口的MAC地址。

但是、对于这些端口类型、集群显示的数据是一致的。

> LLDP 规范定义了通过 SNMP MIB 访问收集的信息。但是， ONTAP 当前不支持 LLDP MIB 。

启用或禁用**LDP**

要发现公告并将其发送到符合LDP的相邻设备、必须在集群的每个节点上启用LDP。从 ONTAP 9.7 开始，默认情况下会在节点的所有端口上启用 LLDP 。

关于此任务

对于ONTAP 9.10.1及更早版本、 `lldp.enable` 选项用于控制节点的端口上是启用还是禁用了LDP：

- `on` 在所有端口上启用LDP。
- `off` 在所有端口上禁用LDP。

对于ONTAP 9.11.1及更高版本、 `lldp.enable` 选项用于控制是否在节点的非集群和非存储端口上启用了LDP：

- `on` 在所有非集群和非存储端口上启用LDP。
- `off` 在所有非集群和非存储端口上禁用LDP。

步骤

1. 显示某个节点或集群中所有节点的当前LDP设置：
   - 单个节点 `run -node node_name options lldp.enable`
   - 所有节点：选项 `lldp.enable`
2. 在一个节点的所有端口或集群中所有节点的所有端口上启用或禁用LDP：

要启用或禁用的LDP…	输入 …
节点	`run -node node_name options lldp.enable {on
off}`	集群中的所有节点
`options lldp.enable {on	off}`

   - 单个节点

```
run -node node_name options lldp.enable {on|off}
```

   - 所有节点：

```
options lldp.enable {on|off}
```

查看LDP邻居信息

您可以查看有关连接到集群节点的每个端口的相邻设备的信息，前提是该端口连接到 LLDP 兼容的设备。您可以使用 network device-discovery show 命令查看邻居信息。

步骤

1. 显示有关连接到集群中某个节点上的端口的所有符合LDP的设备的信息：

```
network device-discovery show -node node -protocol lldp
```

以下命令显示了连接到节点 cluster-1_01 上端口的邻居。输出列出了连接到指定节点的每个端口且已启用 LLDP 的设备。如果 `-protocol` 如果省略选项、则输出还会列出已启用CDP的设备。

```
network device-discovery show -node cluster-1_01 -protocol lldp
Node/       Local  Discovered
Protocol    Port   Device                    Interface         Platform
----------- ------ ------------------------- ----------------
----------------
cluster-1_01/lldp
            e2a    0013.c31e.5c60            GigabitEthernet1/36
            e2b    0013.c31e.5c60            GigabitEthernet1/35
            e2c    0013.c31e.5c60            GigabitEthernet1/34
            e2d    0013.c31e.5c60            GigabitEthernet1/33
```

调整传输 **LLDP** 公告的间隔

将定期向lld邻居发送lld公告。您可以根据网络流量和网络拓扑的变化增加或减少发送LLDP公告的间隔。

关于此任务

IEEE 建议的默认间隔为 30 秒，但您可以输入一个介于 5 秒到 300 秒之间的值。

步骤

1. 显示某个节点或集群中所有节点的当前LDP公告时间间隔：
   - 单个节点

     ```
     run -node <node_name> options lldp.xmit.interval
     ```

   - 所有节点：

     ```
     options lldp.xmit.interval
     ```

2. 调整节点的所有端口或集群中所有节点的所有端口发送 LLDP 公告的间隔：
   - 单个节点

     ```
     run -node <node_name> options lldp.xmit.interval <interval>
     ```

   - 所有节点：

     ```
     options lldp.xmit.interval <interval>
     ```

调整 **LLDP** 公告的生存时间值

生存时间（ TTL ）是 LLDP 公告存储在相邻 LLDP 兼容设备的缓存中的时间段。TTL 会在每个 LLDP 数据包中

公布，并在节点收到 LLDP 数据包时进行更新。可以在传出 LLDP 帧中修改 TTL 。

关于此任务

- TTL是计算得出的值、即传输间隔的乘积 (`lldp.xmit.interval`)和保持乘数 (`lldp.xmit.hold`)加上一个。
- 默认保持倍数值为 4 ，但您可以输入 1 到 100 之间的值。
- 因此，根据 IEEE 的建议，默认 TTL 为 121 秒，但通过调整传输间隔和保持乘数值，您可以为传出帧指定一个介于 6 秒到 30001 秒之间的值。
- 如果在 TTL 过期之前删除 IP 地址，则 LLDP 信息将缓存，直到 TTL 过期为止。

步骤

1. 显示节点或集群中所有节点的当前保持乘数值：
   - 单个节点

     ```
     run -node <node_name> options lldp.xmit.hold
     ```

   - 所有节点：

     ```
     options lldp.xmit.hold
     ```

2. 调整节点的所有端口或集群中所有节点的所有端口上的保持倍数值：
   - 单个节点

     ```
     run -node <node_name> options lldp.xmit.hold <hold_value>
     ```

   - 所有节点：

     ```
     options lldp.xmit.hold <hold_value>
     ```

查看或清除LLDP统计信息

您可以查看每个节点上集群和非集群端口的LLDP统计信息、以检测潜在的网络连接问题。LLDP统计信息是自上次清除以来累积的。

关于此任务

对于ONTAP 9.10.1及更早版本、由于LLDP始终为集群端口启用、因此始终会显示这些端口上的流量的LLDP统计信息。必须在非集群端口上启用LLDP、才能显示这些端口的统计信息。

对于ONTAP 9.11.1及更高版本、由于LLDP始终为集群和存储端口启用、因此始终会显示这些端口上的流量的LLDP统计信息。必须在非集群和非存储端口上启用LLDP、才能显示这些端口的统计信息。

步骤

显示或清除节点上所有端口的当前LLDP统计信息：

如果您要 ...	输入 ...
查看LLDP统计信息	`run -node node_name lldp stats`
清除LLDP统计信息	`run -node node_name lldp stats -z`

显示并清除统计信息示例

以下命令显示清除前的LLDP统计信息。输出将显示自上次清除统计信息以来已发送和接收的数据包总数。

```
cluster-1::> run -node vsim1 lldp stats

RECEIVE
 Total frames:     190k  | Accepted frames:   190k | Total drops:
0
TRANSMIT
 Total frames:     5195  | Total failures:      0
OTHER
 Stored entries:      64
```

以下命令将清除LLDP统计信息。

```
cluster-1::> The following command clears the LLDP statistics:
run -node vsim1 lldp stats -z
run -node node1 lldp stats

RECEIVE
 Total frames:        0  | Accepted frames:     0  | Total drops:
0
TRANSMIT
 Total frames:        0  | Total failures:      0
OTHER
 Stored entries:      64
```

清除统计信息后、在发送或接收下一个LLDP公告后、这些统计信息将开始累积。