网络端口
ONTAP 9

NetApp
February 12, 2026

目录

网络端口

了解ONTAP网络端口配置

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

组合物理端口以创建ONTAP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。

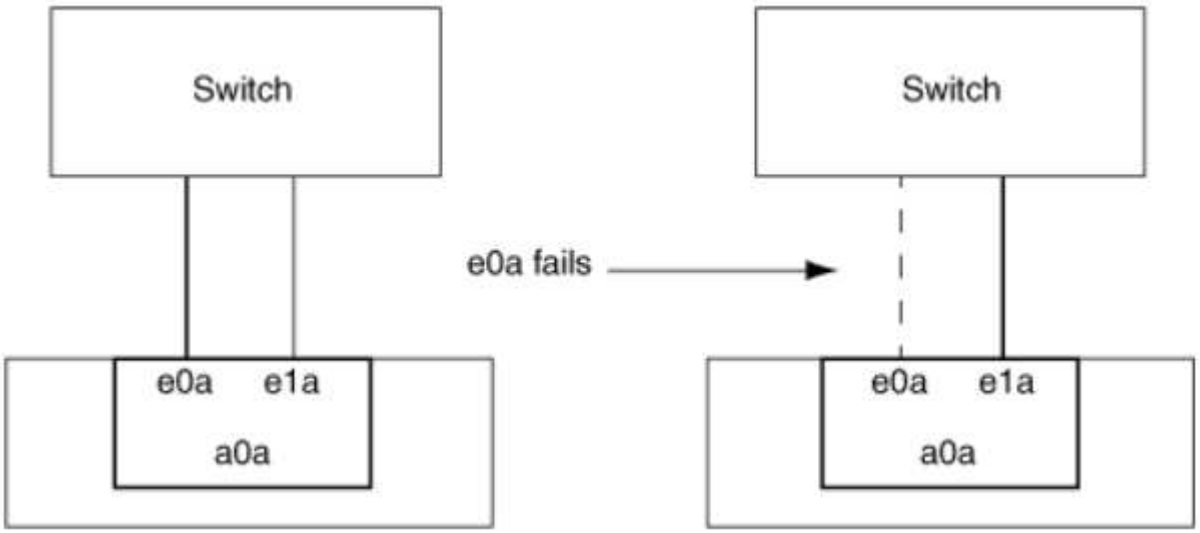
单模式接口组的特征

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

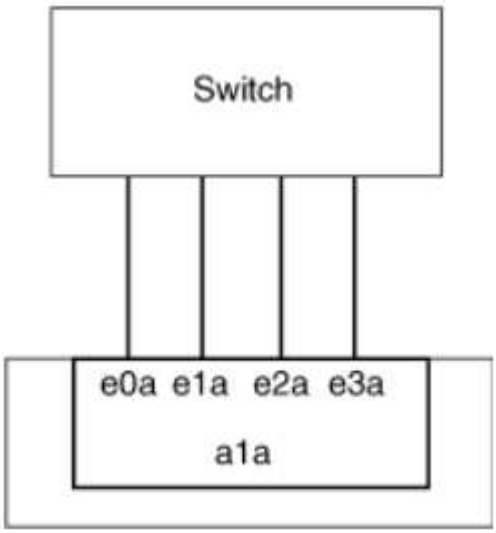
ONTAP 中的静态多模式接口组实施符合 IEEE 802.3ad （静态）标准。任何支持聚合但不具有用于配置聚合的控制数据包交换的交换机都可以与静态多模式接口组结合使用。

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。

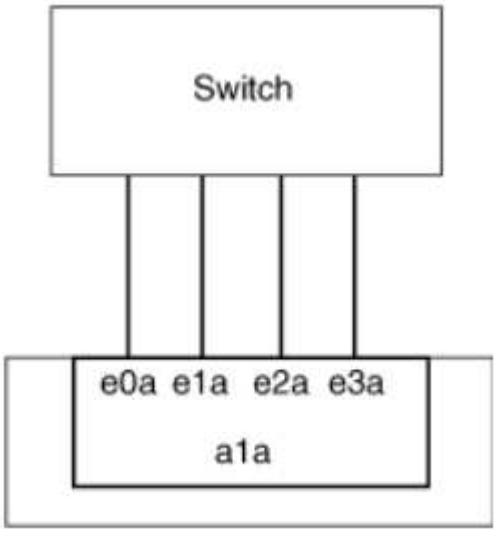
ONTAP 负载平衡算法可确定用于传输出站流量的成员端口，而不控制如何接收入站帧。交换机根据交换机端口通道组中配置的负载平衡算法确定要用于传输的端口通道组的成员（单个物理端口）。因此，交换机配置决定了要接收流量的存储系统的成员端口（单个物理端口）。有关配置交换机的详细信息，请参见交换机供应商提供的文档。

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

您可以通过使用IP地址、MAC地址、顺序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均等分布网络流量、确保多模式接口组的所有接口均可用于传出流量。

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

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。

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

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
```

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：

有关适用于端口接口组"ONTAP 命令参考"的配置限制的详细信息 `network port ifgrp add-port`，请参见。

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
```

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

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。

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

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ONTAP 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 9.14.1 和 9.13.1 中，未被任何逻辑接口 (LIF) 使用且在所连接的交换机上缺少本机 VLAN 连接的未标记端口被标记为已降级。这有助于识别未使用的端口，并不表示中断。本机 VLAN 允许 ifgrp 基本端口上未标记的流量，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`。

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

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：

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

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
```

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

修改**ONTAP**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
```

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

通过转换40GbE NIC端口为ONTAP网络创建10GbE端口

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。

为ONTAP网络配置UTA X1143A-R6端口

默认情况下、X1143A-R6统一目标适配器会在FC目标模式下配置、但您可以将其端口配置为10 Gb以太网和FCoE (CNA)端口或16 Gb FC启动程序或目标端口。这需要不同的 SFP+ 适配器。

如果配置为以太网和 FCoE ，则 X1143A-R6 适配器支持在同一个 10-GbE 端口上同时传输 NIC 和 FCoE 目标流量。如果配置为 FC ，则共享同一 ASIC 的每个双端口对都可以单独配置为 FC 目标模式或 FC 启动程序模式。这意味着，一个 X1143A-R6 适配器可以在一个双端口对上支持 FC 目标模式，而在另一个双端口对上支持 FC 启动程序模式。 连接到同一 ASIC 的端口对必须配置在同一模式下。

在 FC 模式下， X1143A-R6 适配器的行为与任何速度高达 16 Gbps 的现有 FC 设备一样。在 CNA 模式下，您可以使用 X1143A-R6 适配器处理共享同一 10 GbE 端口的并发 NIC 和 FCoE 流量。CNA 模式仅支持 FCoE 功能的 FC 目标模式。

要配置统一目标适配器（ X1143A-R6 ），必须在同一个特性模式下在同一芯片上配置两个相邻端口。

步骤

1. 查看端口配置：

```
system hardware unified-connect show
```

2. 根据需要为光纤通道(FC)或融合网络适配器(CNA)配置端口：

```
system node hardware unified-connect modify -node <node_name> -adapter
<adapter_name> -mode {fcp|cna}
```

3. 为 FC 或 10 Gb 以太网连接适当的缆线。
4. 验证是否已安装正确的 SFP+ ：

```
network fcp adapter show -instance -node -adapter
```

对于 CNA ，您应使用 10 Gb 以太网 SFP 。对于 FC ，您应根据所连接的 FC 网络结构使用 8 Gb SFP 或 16 Gb SFP 。

转换要在ONTAP网络中使用的UTA2端口

您可以将UTA2端口从融合网络适配器(CNA)模式转换为光纤通道(FC)模式、反之亦然。

如果需要更改将端口连接到其网络的物理介质或支持FC启动程序和目标、则应将UTA2特性从CNO模式更改为FC模式。

从**CNNA**模式到**FC**模式

步骤

1. 使适配器脱机：

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. 更改端口模式：

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode fcp
```

3. 重新启动节点，然后使适配器联机：

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin up
```

4. 通知管理员或 VIF 管理器删除或删除此端口（如果适用）：
   - 如果此端口用作 LIF 的主端口，接口组（ ifgrp ）的成员或托管 VLAN ，则管理员应执行以下操作：
     - 分别移动 LIF ，从 ifgrp 中删除端口或删除 VLAN 。
     - 运行命令以手动删除此端口 `network port delete`。如果 `network port delete`命令失败、管理员应解决错误、然后再次运行命令。
   - 如果此端口未用作 LIF 的主端口，不是 ifgrp 的成员且未托管 VLAN ，则 VIF 管理器应在重新启动时从其记录中删除此端口。如果VIF管理器未删除此端口、则管理员必须在重新启动后使用命令手动删除此端口 `network port delete`。

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

5. 验证是否已安装正确的 SFP+ ：

```
network fcp adapter show -instance -node -adapter
```

   对于 CNA ，您应使用 10 Gb 以太网 SFP 。对于 FC ，在更改节点上的配置之前，您应使用 8 Gb SFP 或 16 Gb SFP 。

从**FC**模式到**CNNA**模式

步骤

1. 使适配器脱机：

```
network fcp adapter modify -node <node_name> -adapter <adapter_name>
-status-admin down
```

2. 更改端口模式：

```
ucadmin modify -node <node_name> -adapter <adapter_name> -mode cna
```

3. 重新启动节点。
4. 验证是否已安装正确的SFP+。

   对于 CNA ，您应使用 10 Gb 以太网 SFP 。

转换ONTAP网络的CNA/UTA2光纤模块

您应更改统一目标适配器（ CNA/UTA2 ）上的光纤模块，以支持为适配器选择的个性化模式。

步骤

1. 验证卡中使用的当前 SFP+ 。然后，将当前 SFP+ 替换为适用于首选特性（ FC 或 CNA ）的 SFP+ 。
2. 从 X1143A-R6 适配器中删除当前光纤模块。
3. 为首选个性化模式（ FC 或 CNA ）光纤插入正确的模块。
4. 验证是否已安装正确的 SFP+ ：

```
network fcp adapter show -instance -node -adapter
```

   中列出了支持的 SFP+ 模块和 Cisco 品牌铜缆（双轴） "NetApp Hardware Universe"。

从ONTAP集群节点中删除NIC

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。

ONTAP 9.7及更早版本中删除NIC的过程有所不同。如果需要从运行ONTAP 9.7及更早版本的ONTAP集群节点中删除NIC，请参阅过程"从节点中删除NIC (ONTAP 9.7或更早版本)"。

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

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：

相关信息

- "cluster controller-replacement network placed-interface delete"
- "network interface modify"

监控网络端口

监控**ONTAP**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。

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

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：

有关的详细信息 `network options port-health-monitor modify`，请参见"ONTAP 命令参考"。

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。

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

监控**ONTAP**网络端口的可访问状态

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。

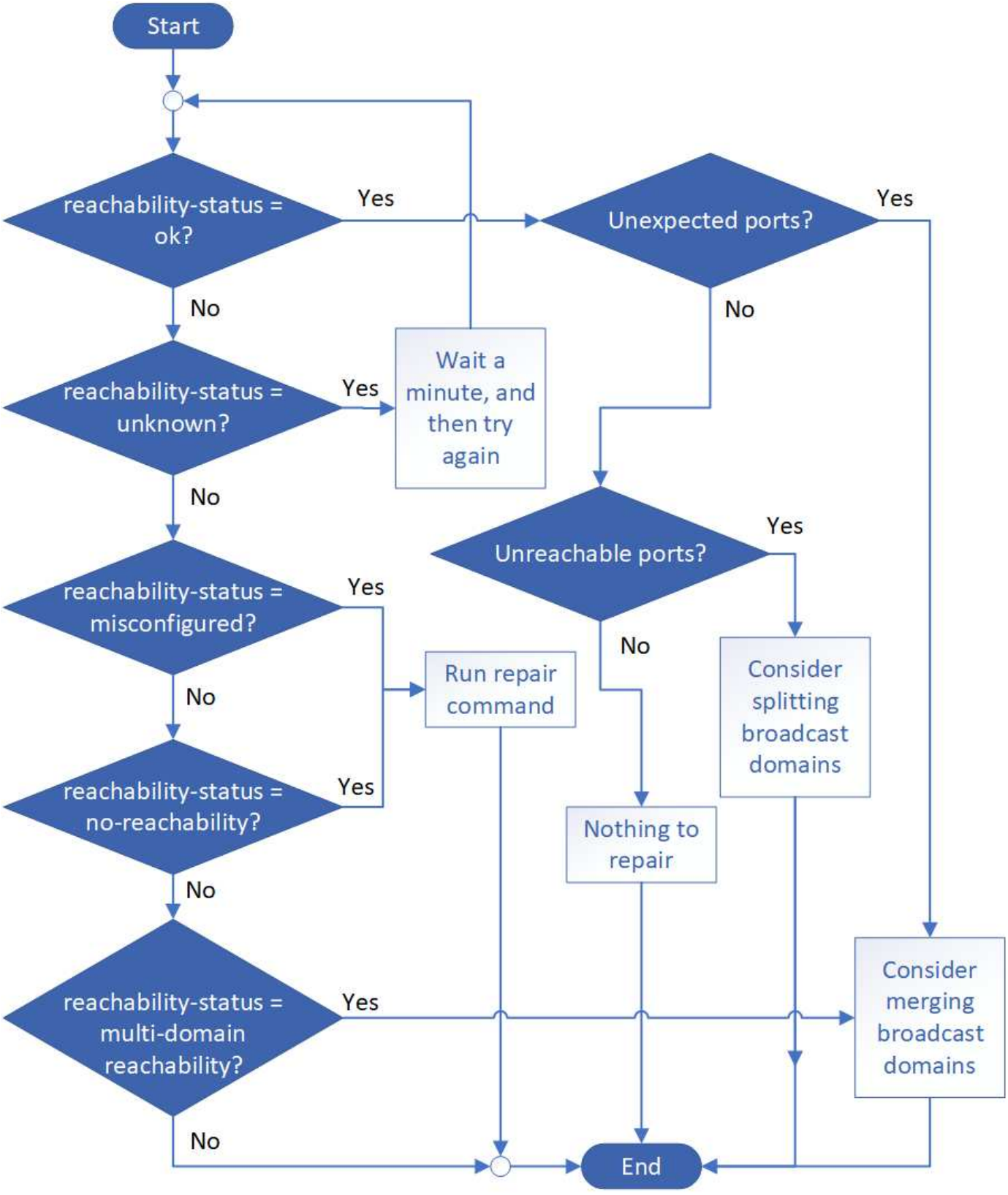
步骤

1. 查看端口可访问性：

```
network port reachability show
```

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

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

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"。

了解**ONTAP**网络上的端口使用情况

为与特定服务进行ONTAP通信、保留了几个众所周知的端口。如果存储网络环境中的端口值与ONTAP端口上的值相同、则会发生端口冲突。

入站流量

ONTAP存储上的入站流量使用以下协议和端口：

协议	Port	目的
所有 ICMP	全部	Ping 实例
TCP	22.	对集群管理LIF或节点管理LIF的IP地址进行安全Shell访问
TCP	80	对集群管理LIF IP地址的网页访问权限
TCP/UDP	111	rpc绑 定、NFS的远程过程调用
UDP	123.	NTP、网络时间协议
TCP	135	MRPC、Microsoft远程过程调用
TCP	139	Netbios-SSN、用于CIFS的NetBIOS服务会话
TCP/UDP	161-162	SNMP、简单网络管理协议
TCP	443	对集群管理LIF的IP地址进行安全网页访问
TCP	445	MS Active Domain Services、基于TCP的Microsoft SMB/CCIFS、带NetBIOS帧
TCP/UDP	635	NFS挂载、可与远程文件系统进行交互、就像该系统位于本地一样
TCP	749	Kerberos
UDP	953	名称守护进程
TCP/UDP	2049	NFS 服务器守护进程
TCP	2050	NRV、NetApp远程卷协议

TCP	3260	通过 iSCSI 数据 LIF 进行 iSCSI 访问
TCP/UDP	4045	NFS 锁定守护进程
TCP/UDP	4046	NFS 的网络状态监视器
UDP	4049-51	NFS RPC报价
UDP	4444	KRB524、Kerberos 524
UDP	5353	多播 DNS
TCP	10000	使用网络数据管理协议(NDMP)备份
TCP	11104	对SnapMirror的集群间通信会话进行集群对等和双向管理
TCP	11105	使用集群间SnapMirror进行集群对等、双向集群间LUN数据传输
SSL/TLS	30000	通过安全套接字 (SSL/TLS) 接受 DMA 和 NDMP 服务器之间的 NDMP 安全控制连接。安全扫描器可以报告端口 30000 上的漏洞。

出站流量

您可以根据业务需求使用基本或高级规则设置ONTAP存储上的出站流量。

基本外向规则

所有端口均可用于通过ICMP、TCP和UDP协议传输的所有出站流量。

协议	Port	目的
所有 ICMP	全部	所有出站流量
所有 TCP	全部	所有出站流量
所有 UDP	全部	所有出站流量

高级出站规则

如果您需要对出站流量设置严格的规则、则可以使用以下信息仅打开ONTAP出站通信所需的端口。

Active Directory

协议	Port	源	目标	目的
TCP	88	节点管理LIF、数据LIF (NFS、CIFS、iSCSI)	Active Directory 目录林	Kerberos V 身份验证
UDP	137	节点管理LIF、数据LIF (NFS、CIFS)	Active Directory 目录林	NetBIOS 名称服务
UDP	138	节点管理LIF、数据LIF (NFS、CIFS)	Active Directory 目录林	NetBIOS 数据报服务
TCP	139	节点管理LIF、数据LIF (NFS、CIFS)	Active Directory 目录林	NetBIOS 服务会话

TCP	389	节点管理LIF、数据LIF (NFS、CIFS)	Active Directory 目录林	LDAP
UDP	389	节点管理LIF、数据LIF (NFS、CIFS)	Active Directory 目录林	LDAP
TCP	445	节点管理LIF、数据LIF (NFS、CIFS)	Active Directory 目录林	Microsoft SMB/CIFS over TCP （通过 TCP ）和 NetBIOS 成帧
TCP	464	节点管理LIF、数据LIF (NFS、CIFS)	Active Directory 目录林	更改并设置Kerberos V密码(set_change)
UDP	464	节点管理LIF、数据LIF (NFS、CIFS)	Active Directory 目录林	Kerberos 密钥管理
TCP	749	节点管理LIF、数据LIF (NFS、CIFS)	Active Directory 目录林	更改并设置Kerberos V密码(RPCSEC_GSS)

AutoSupport

协议	Port	源	目标	目的
TCP	80	节点管理 LIF	support.netapp.com	AutoSupport （仅当传输协议从 HTTPS 更改为 HTTP 时）

SNMP

协议	Port	源	目标	目的
TCP/UDP	162	节点管理 LIF	监控服务器	通过 SNMP 陷阱进行监控

SnapMirror

协议	Port	源	目标	目的
TCP	11104	集群间 LIF	ONTAP 集群间 LIF	管理 SnapMirror 的集群间通信会话

其他服务

协议	Port	源	目标	目的
TCP	25	节点管理 LIF	邮件服务器	SMTP 警报、可用于 AutoSupport
UDP	53	节点管理 LIF 和数据 LIF （NFS 、 CIFS ）	DNS	DNS
UDP	67	节点管理 LIF	DHCP	DHCP服务器
UDP	68	节点管理 LIF	DHCP	首次设置 DHCP 客户端
UDP	514.	节点管理 LIF	系统日志服务器	系统日志转发消息

TCP	5010	集群间 LIF	备份端点或还原端点	备份到 S3 功能的备份和还原操作
TCP	18600 至18699	节点管理 LIF	目标服务器	NDMP 副本

了解**ONTAP**内部端口

下表列出了 ONTAP 内部使用的端口及其功能。ONTAP使用这些端口执行各种功能，例如建立集群内 LIF 通信。

此列表并不详尽，并且可能在不同环境中有所不同。

端口 / 协议	组件/功能
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
930	内核服务和管理功能（KSMF）
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
975	密钥管理互操作性协议（ KMIP ）
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
7700	集群会话管理器 (CSM)
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
7835-7839 和 7845-7849	用于集群内通信的 TCP 端口
8023.	节点范围 Telnet
8443	适用于 Amazon FSx 的 ONTAP S3 NAS 端口
8514.	节点范围 RSH
9877	KMIP 客户端端口（仅限内部本地主机）
10006	用于 HA 互连通信的 TCP 端口