

# vSphere 网络连接

ESXi 6.5

vCenter Server 6.5

在本文档被更新的版本替代之前，本文档支持列出的每个产品的版本和所有后续版本。要查看本文档的更新版本，请访问 <http://www.vmware.com/cn/support/pubs>。

ZH\_CN-002315-00

**vmware**<sup>®</sup>

最新的技术文档可以从 VMware 网站下载：

<http://www.vmware.com/cn/support/>

VMware 网站还提供最近的产品更新信息。

您如果对本文档有任何意见或建议，请把反馈信息提交至：

[docfeedback@vmware.com](mailto:docfeedback@vmware.com)

版权所有 © 2009 – 2016 VMware, Inc. 保留所有权利。 [版权和商标信息](#)。

**VMware, Inc.**  
3401 Hillview Ave.  
Palo Alto, CA 94304  
[www.vmware.com](http://www.vmware.com)

北京办公室  
北京市海淀区科学院南路 2 号  
融科资讯中心 C 座南 8 层  
[www.vmware.com/cn](http://www.vmware.com/cn)

上海办公室  
上海市浦东新区浦东南路 999 号  
新梅联合广场 23 楼  
[www.vmware.com/cn](http://www.vmware.com/cn)

广州办公室  
广州市天河北路 233 号  
中信广场 7401 室  
[www.vmware.com/cn](http://www.vmware.com/cn)

# 目录

关于 vSphere 网络连接	11
<b>1 网络简介</b>	<b>13</b>
网络概念概述	13
ESXi 中的网络服务	14
VMware ESXi Dump Collector 支持	14
<b>2 使用 vSphere 标准交换机设置网络连接</b>	<b>15</b>
vSphere 标准交换机	15
创建 vSphere 标准交换机	17
虚拟机的端口组配置	18
添加虚拟机端口组	18
编辑标准交换机端口组	19
从 vSphere 标准交换机移除端口组	20
vSphere 标准交换机属性	20
更改 vSphere 标准交换机上 MTU 的大小	20
更改物理适配器的速度	20
在 vSphere 标准交换机中添加物理适配器并使这些适配器成组	21
查看 vSphere 标准交换机的拓扑图	21
<b>3 使用 vSphere Distributed Switch 设置网络连接</b>	<b>23</b>
vSphere Distributed Switch 架构	24
创建 vSphere Distributed Switch	27
将 vSphere Distributed Switch 升级到更高版本	28
编辑 vSphere Distributed Switch 常规和高级设置	29
在 vSphere Distributed Switch 上管理多个主机上的网络连接	30
在 vSphere Distributed Switch 上管理主机网络的任务	31
将主机添加到 vSphere Distributed Switch	31
在 vSphere Distributed Switch 上配置物理网络适配器	33
将 VMkernel 适配器迁移到 vSphere Distributed Switch	33
在 vSphere Distributed Switch 上创建 VMkernel 适配器	34
将虚拟机网络迁移到 vSphere Distributed Switch	36
使用主机作为模板为 vSphere Distributed Switch 创建统一的网络配置	36
从 vSphere Distributed Switch 中移除主机	37
在主机代理交换机上管理网络连接	37
将主机上的网络适配器迁移到 vSphere Distributed Switch	38
将主机上的 VMkernel 适配器迁移到 vSphere 标准交换机	39
将主机的物理网卡分配给 vSphere Distributed Switch	39
从 vSphere Distributed Switch 移除物理网卡	39

- 从活动虚拟机中移除网卡 40
  - 分布式端口组 40
    - 添加分布式端口组 40
    - 编辑常规分布式端口组设置 43
    - 在端口级别配置替代网络策略 43
    - 移除分布式端口组 44
  - 使用分布式端口 44
    - 监控分布式端口的状况 44
    - 配置分布式端口设置 45
  - 在 vSphere Distributed Switch 上配置虚拟机网络连接 45
    - 将虚拟机迁入或迁出 vSphere Distributed Switch 45
    - 将单个虚拟机连接到分布式端口组 46
  - vSphere Web Client 中的 vSphere Distributed Switch 拓扑图 46
    - 查看 vSphere Distributed Switch 的拓扑 47
    - 查看主机代理交换机的拓扑 48
- 4 设置 VMkernel 网络 49
  - VMkernel 网络层 50
  - 查看有关主机上的 VMkernel 适配器的信息 51
  - 在 vSphere 标准交换机上创建 VMkernel 适配器 52
  - 在与 vSphere Distributed Switch 关联的主机上创建 VMkernel 适配器 54
  - 编辑 VMkernel 适配器配置 55
  - 替代 VMkernel 适配器的默认网关 56
  - 使用 ESXCLI 配置 VMkernel 适配器网关 57
  - 查看主机上的 TCP/IP 堆栈配置 57
  - 更改主机上的 TCP/IP 堆栈配置 57
  - 创建自定义 TCP/IP 堆栈 58
  - 移除 VMkernel 适配器 58
- 5 vSphere Distributed Switch 上的 LACP 支持 61
  - 转换为 vSphere Distributed Switch 上的增强型 LACP 支持 63
  - 分布式端口组的 LACP 成组和故障切换配置 64
  - 配置链路聚合组处理分布式端口组的流量 64
    - 创建链路聚合组 65
      - 在分布式端口组的绑定和故障切换顺序中将链路聚合组设置为备用状态 66
      - 将物理网卡分配给链路聚合组的端口 66
      - 在分布式端口组的绑定和故障切换顺序中将链路聚合组设置为活动状态 67
  - 编辑链路聚合组 68
  - 在上行链路端口组上启用 LACP 5.1 支持 69
  - vSphere Distributed Switch 的 LACP 支持限制 69
- 6 备份和还原网络配置 71
  - 备份和还原 vSphere Distributed Switch 配置 71
    - 导出 vSphere Distributed Switch 配置 71
    - 导入 vSphere Distributed Switch 配置 72
    - 还原 vSphere Distributed Switch 配置 72

导出、导入和还原 vSphere 分布式端口组配置	73
导出 vSphere 分布式端口组配置	73
导入 vSphere 分布式端口组配置	73
还原 vSphere 分布式端口组配置	74
<b>7 管理网络的回滚和恢复</b>	<b>75</b>
vSphere 网络连接回滚	75
禁用网络回滚	76
使用 vCenter Server 配置文件禁用网络回滚	76
解决 vSphere Distributed Switch 上的管理网络配置中的错误	77
<b>8 网络策略</b>	<b>79</b>
在 vSphere 标准交换机或 Distributed Switch 上应用网络策略	80
在端口级别配置替代网络策略	81
成组和故障切换策略	81
可用于虚拟交换机的负载均衡算法	82
在 vSphere 标准交换机或标准端口组上配置网卡绑定、故障切换和负载均衡	85
在分布式端口组或分布式端口上配置网卡绑定、故障切换和负载均衡	86
VLAN 策略	88
在分布式端口组或分布式端口上配置 VLAN 标记	88
配置上行链路端口组或上行链路端口上的 VLAN 标记	89
安全策略	90
配置 vSphere Standard Switch 或标准端口组的安全策略	90
配置分布式端口组或分布式端口的安全策略	91
流量调整策略	92
配置 vSphere Standard Switch 或标准端口组的流量调整	92
编辑分布式端口组或分布式端口的流量调整策略	93
资源分配策略	94
编辑分布式端口组的资源分配策略	94
编辑分布式端口的资源分配策略	94
监控策略	95
在分布式端口组或分布式端口上启用或禁用 NetFlow 监控	95
流量筛选和标记策略	95
分布式端口组或上行链路端口组的流量筛选和标记	96
分布式端口或上行链路端口的流量筛选和标记	101
限定要筛选和标记的流量	107
管理 vSphere Distributed Switch 上的多个端口组的策略	109
端口阻止策略	113
编辑分布式端口组的端口阻止策略	113
编辑分布式端口或上行链路端口的阻止策略	113
<b>9 使用 VLAN 隔离网络流量</b>	<b>115</b>
VLAN 配置	115
专用 VLAN	116
创建专用 VLAN	116
移除主专用 VLAN	117

移除次专用 VLAN 117

## 10 管理网络资源 119

### DirectPath I/O 119

为主机上的网络设备启用直通功能 120

在虚拟机上配置 PCI 设备 120

在虚拟机上通过 vMotion 启用 DirectPath I/O 121

### 单根 I/O 虚拟化 (SR-IOV) 122

SR-IOV 支持 122

SR-IOV 组件架构和交互 124

vSphere 和虚拟功能交互 126

DirectPath I/O 和 SR-IOV 126

配置虚拟机以使用 SR-IOV 127

与已启用 SR-IOV 的虚拟机关联的流量网络选项 129

使用 SR-IOV 物理适配器处理虚拟机流量 129

使用主机配置文件或 ESXCLI 命令启用 SR-IOV 130

由于主机的中断向量已耗尽，因此使用 SR-IOV 虚拟功能的虚拟机打开电源失败 131

### 虚拟机的远程直接内存访问 132

PVRDMA 支持 132

为 ESXi 主机配置 PVRDMA 133

向虚拟机分配 PVRDMA 适配器 134

聚合以太网 RDMA 的网络要求 134

### 巨帧 135

在 vSphere Distributed Switch 上启用巨帧 135

在 vSphere 标准交换机上启用巨帧 135

为 VMkernel 适配器启用巨帧 136

在虚拟机上启用巨帧支持 136

### TCP 分段清除 137

在 VMkernel 中启用或禁用软件 TSO 137

确定在 ESXi 主机的物理网络适配器上是否支持 TSO 137

在 ESXi 主机上启用或禁用 TSO 137

确定 TSO 在 ESXi 主机上是否处于启用状态 138

在 Linux 虚拟机上启用或禁用 TSO 138

在 Windows 虚拟机上启用或禁用 TSO 139

### 大型接收卸载 139

为 ESXi 主机上的所有 VMXNET3 适配器启用硬件 LRO 140

为 ESXi 主机上的所有 VMXNET3 适配器启用或禁用软件 LRO 140

确保是否为 ESXi 主机上的 VMXNET3 适配器启用了 LRO 140

更改 VMXNET 3 适配器的 LRO 缓冲区大小 141

为 ESXi 主机上的所有 VMkernel 适配器启用或禁用 LRO 141

更改 VMkernel 适配器的 LRO 缓冲区大小 141

在 Linux 虚拟机的 VMXNET3 适配器上启用或禁用 LRO 141

在 Windows 虚拟机的 VMXNET3 适配器上启用或禁用 LRO 142

在 Windows 虚拟机上全局启用 LRO 143

### NetQueue 和网络性能 143

在主机上启用 NetQueue 143

在主机上禁用 NetQueue	144
<b>11 vSphere Network I/O Control</b>	<b>145</b>
关于 vSphere Network I/O Control 版本 3	145
将 vSphere Distributed Switch 上的 Network I/O Control 升级到版本 3	146
在 vSphere Distributed Switch 上启用 Network I/O Control	148
系统流量的带宽分配	148
系统流量的带宽分配参数	149
系统流量的带宽预留示例	149
配置系统流量的带宽分配	150
虚拟机流量的带宽分配	151
关于为虚拟机分配带宽	151
虚拟机流量的带宽分配参数	153
虚拟机带宽的接入控制	153
创建网络资源池	154
向网络资源池中添加分布式端口组	154
为虚拟机配置带宽分配	155
在多个虚拟机上配置带宽分配	156
更改网络资源池的配额	157
从网络资源池中移除分布式端口组	157
删除网络资源池	157
将物理适配器移到 Network I/O Control 的范围之外	158
使用 Network I/O Control 版本 2	158
在 Network I/O Control 版本 2 中创建网络资源池	159
在 Network I/O Control 版本 2 中编辑网络资源池的设置	160
<b>12 MAC 地址管理</b>	<b>161</b>
从 vCenter Server 的 MAC 地址分配	161
VMware OUI 分配	162
基于前缀的 MAC 地址分配	162
基于范围的 MAC 地址分配	162
分配 MAC 地址	162
在 ESXi 主机上生成 MAC 地址	164
为虚拟机设置静态 MAC 地址	165
静态 MAC 地址的 VMware OUI	165
通过使用 vSphere Web Client 分配静态 MAC 地址	166
在虚拟机配置文件中分配静态 MAC 地址	166
<b>13 针对 IPv6 配置 vSphere</b>	<b>167</b>
vSphere IPv6 连接	167
在 IPv6 中部署 vSphere	168
在 vSphere 安装中启用 IPv6	169
在升级的 vSphere 环境中启用 IPv6	169
在主机上启用或禁用 IPv6 支持	170
在 ESXi 主机上设置 IPv6	171

- 在 vCenter Server 上设置 IPv6 171
  - 在 vCenter Server Appliance 上设置 IPv6 171
  - 使用 IPv6 在 Windows 中设置 vCenter Server 172
- 14 监控网络连接和流量 173**
  - 使用 `pktcap-uw` 实用程序捕获和跟踪网络数据包 173
    - 用于捕获数据包的 `pktcap-uw` 命令语法 173
    - 用于跟踪数据包的 `pktcap-uw` 命令语法 175
    - 用于输出控制的 `pktcap-uw` 选项 175
    - 用于筛选数据包的 `pktcap-uw` 选项 176
    - 使用 `pktcap-uw` 实用程序捕获数据包 177
    - 使用 `pktcap-uw` 实用程序跟踪数据包 184
  - 配置 vSphere Distributed Switch 的 NetFlow 设置 185
  - 使用端口镜像 186
    - 端口镜像版本兼容性 186
    - 端口镜像互操作性 187
    - 创建端口镜像会话 188
    - 查看端口镜像会话详细信息 190
    - 编辑端口镜像会话详细信息、源和目标 190
  - vSphere Distributed Switch 运行状况检查 192
    - 启用或禁用 vSphere Distributed Switch 健康状况检查 192
    - 查看 vSphere Distributed Switch 健康状况 193
  - 交换机发现协议 193
    - 在 vSphere Distributed Switch 上启用 Cisco 发现协议 193
    - 在 vSphere Distributed Switch 上启用链路层发现协议 194
    - 查看交换机信息 194
- 15 配置用于虚拟机网络连接的协议配置文件 195**
  - 添加网络协议配置文件 195
    - 选择网络协议配置文件的名称和网络 196
    - 指定网络协议配置文件中的 IPv4 配置 196
    - 指定网络协议配置文件的 IPv6 配置 196
    - 指定网络协议配置文件的 DNS 和其他配置 197
    - 完成网络协议配置文件的创建 197
  - 将端口组与网络协议配置文件关联 197
  - 配置虚拟机或 vApp 以使用网络协议配置文件 198
- 16 多播筛选 199**
  - 多播筛选模式 199
  - 在 vSphere Distributed Switch 上启用多播侦听 200
  - 编辑多播侦听的查询时间间隔 200
  - 编辑 IGMP 和 MLD 的源 IP 地址数量 200
- 17 无状态网络部署 203**



18	网络最佳做法	205
----	--------	-----

	索引	207
--	----	-----



# 关于 vSphere 网络连接

---

《vSphere 网络连接》提供有关配置 VMware vSphere® 网络连接的信息，包括如何创建 vSphere Distributed Switch 和 vSphere 标准交换机。

《vSphere 网络连接》还提供有关监控网络、管理网络资源和网络连接最佳做法的信息。

## 目标读者

提供的信息面向熟悉网络配置和虚拟机技术的有经验的 Windows 或 Linux 系统管理员。

## vSphere Web Client 和 vSphere Client

本指南中的任务说明基于 vSphere Web Client。您也可以使用新的 vSphere Client 执行本指南中的大部分任务。新的 vSphere Client 用户界面术语、拓扑及工作流与 vSphere Web Client 用户界面的相同方面和元素保持高度一致。可以将 vSphere Web Client 说明应用到新的 vSphere Client，除非另有指示。

---

**注意** 在 vSphere 6.5 版本中，并未针对 vSphere Client 实现 vSphere Web Client 中的所有功能。有关不受支持的功能的最新列表，请参见《vSphere Client 功能更新指南》，网址为 <http://www.vmware.com/info?id=1413>。

---



# 网络简介

将讨论 ESXi 网络的基本概念以及如何在 vSphere 环境中设置和配置网络。

本章讨论了以下主题：

- [第 13 页](#)，“网络概念概述”
- [第 14 页](#)，“ESXi 中的网络服务”
- [第 14 页](#)，“VMware ESXi Dump Collector 支持”

## 网络概念概述

一些概念对透彻了解虚拟网络至关重要。如果您是 ESXi 的新用户，则了解这些概念将对您很有帮助。

<b>物理网络</b>	为了使物理机之间能够收发数据，在物理机间建立的网络。VMware ESXi 运行于物理机之上。
<b>虚拟网络</b>	在单台物理机上运行的虚拟机之间为了互相发送和接收数据而相互逻辑连接所形成的网络。虚拟机可连接到在添加网络时创建的虚拟网络。
<b>物理以太网交换机</b>	管理物理网络上计算机之间的网络流量。一台交换机可具有多个端口，每个端口都可与网络上的一台计算机或其他交换机连接。可按某种方式对每个端口的行为进行配置，具体取决于其所连接的计算机的需求。交换机将会了解到连接其端口的主机，并使用该信息向正确的物理机转发流量。交换机是物理网络的核心。可将多个交换机连接在一起，以形成较大的网络。
<b>vSphere 标准交换机</b>	其运行方式与物理以太网交换机十分相似。它检测与其虚拟端口进行逻辑连接的虚拟机，并使用该信息向正确的虚拟机转发流量。可使用物理以太网适配器（也称为上行链路适配器）将虚拟网络连接至物理网络，以将 vSphere 标准交换机连接到物理交换机。此类型的连接类似于将物理交换机连接在一起以创建较大的网络。即使 vSphere 标准交换机的运行方式与物理交换机十分相似，但它不具备物理交换机所拥有的一些高级功能。
<b>标准端口组</b>	标准端口组为每个成员端口指定了诸如带宽限制和 VLAN 标记策略之类的端口配置选项。网络服务通过端口组连接到标准交换机。端口组定义通过交换机连接网络的方式。通常，单个标准交换机与一个或多个端口组关联。
<b>vSphere Distributed Switch</b>	它可充当数据中心中所有关联主机的单一交换机，以提供虚拟网络的集中式置备、管理以及监控。您可以在 vCenter Server 系统上配置 vSphere Distributed Switch，该配置将传播至与该交换机关联的所有主机。这使得虚拟机可在跨多个主机进行迁移时确保其网络配置保持一致。

<b>主机代理交换机</b>	驻留在与 vSphere Distributed Switch 关联的每个主机上的隐藏标准交换机。主机代理交换机会将 vSphere Distributed Switch 上设置的网络配置复制到特定主机。
<b>分布式端口</b>	连接到主机的 VMkernel 或虚拟机的网络适配器的 vSphere Distributed Switch 上的一个端口。
<b>分布式端口组</b>	与 vSphere Distributed Switch 关联的一个端口组，并为每个成员端口指定端口配置选项。分布式端口组可定义通过 vSphere Distributed Switch 连接到网络的方式。
<b>网卡绑定</b>	当多个上行链路适配器与单个交换机相关联以形成小组时，就会发生网卡绑定。小组将物理网络和虚拟网络之间的流量负载分摊给其所有或部分成员，或在出现硬件故障或网络中断时提供被动故障切换。
<b>VLAN</b>	VLAN 可用于将单个物理 LAN 分段进一步分段，以便使端口组中的端口互相隔离，如同位于不同物理分段上一样。标准是 802.1Q。
<b>VMkernel TCP/IP 网络层</b>	VMkernel 网络层提供与主机的连接，并处理 vSphere vMotion、IP 存储、Fault Tolerance 和 Virtual SAN 的标准基础架构流量。
<b>IP 存储</b>	将 TCP/IP 网络通信用作其基础的任何形式的存储。iSCSI 可用作虚拟机数据存储，NFS 可用作虚拟机数据存储并用于直接挂载 .iso 文件，这些文件对于虚拟机显示为 CD-ROM。
<b>TCP 分段卸载</b>	TCP 分段卸载 (TSO) 可使 TCP/IP 堆栈发出非常大的帧（达到 64 KB），即使接口的最大传输单元 (MTU) 较小也是如此。然后网络适配器将较大的帧分成 MTU 大小的帧，并预置一份初始 TCP/IP 标头的调整后副本。

## ESXi 中的网络服务

虚拟网络向主机和虚拟机提供了多种服务。

可以在 ESXi 中启用两种类型的网络服务：

- 将虚拟机连接到物理网络以及相互连接虚拟机。
- 将 VMkernel 服务（如 NFS、iSCSI 或 vMotion）连接至物理网络。

## VMware ESXi Dump Collector 支持

当系统遇到重大故障时，ESXi Dump Collector 会将 VMkernel 内存（即核心转储）的状态发送到网络服务器。

ESXi 5.1 及更高版本中的 ESXi Dump Collector 支持 vSphere 标准交换机和 vSphere Distributed Switch。ESXi Dump Collector 还可将任意活动上行链路适配器运用于收集器，此活动上行链路适配器来自处理 VMkernel 适配器的端口组组合。

如果已配置的 VMkernel 适配器的 IP 地址发生更改，则对 ESXi Dump Collector 接口 IP 地址的更改也将自动更新。如果 VMkernel 适配器的网关配置发生更改，ESXi Dump Collector 也将调整其默认网关。

如果您尝试删除 ESXi Dump Collector 使用的 VMkernel 网络适配器，操作会失败并显示警告消息。要删除 VMkernel 网络适配器，请禁用转储收集，然后再删除适配器。

从已崩溃的主机到 ESXi Dump Collector 的文件传输会话中不存在身份验证或加密。您应尽可能在单独的 VLAN 上配置 ESXi Dump Collector，以便将 ESXi 核心转储与常规网络流量隔离。

有关安装和配置 ESXi Dump Collector 的信息，请参见 *vSphere 安装和设置* 文档。

## 使用 vSphere 标准交换机设置网络连接

---

在 vSphere 部署中，vSphere 标准交换机在主机级别处理网络流量。

本章讨论了以下主题：

- 第 15 页，[“vSphere 标准交换机”](#)
- 第 17 页，[“创建 vSphere 标准交换机”](#)
- 第 18 页，[“虚拟机的端口组配置”](#)
- 第 20 页，[“vSphere 标准交换机属性”](#)

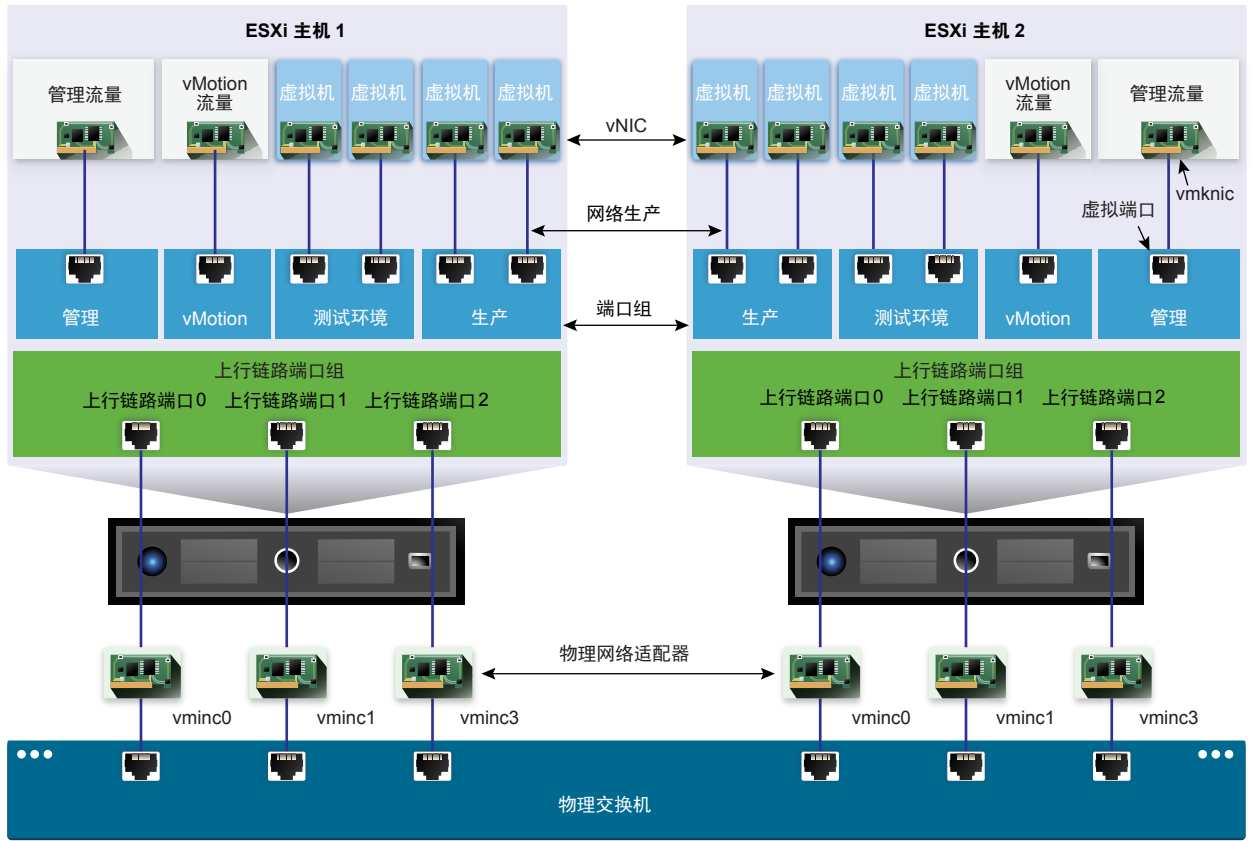
### vSphere 标准交换机

可以创建名为 vSphere 标准交换机的抽象网络设备。使用标准交换机来提供主机和虚拟机的网络连接。标准交换机可在同一 VLAN 中的虚拟机之间进行内部流量桥接，并链接至外部网络。

#### 标准交换机概览

要提供主机和虚拟机的网络连接，请在标准交换机上将主机的物理网卡连接到上行链路端口。虚拟机具有在标准交换机上连接到端口组的网络适配器 (vNIC)。每个端口组可使用一个或多个物理网卡来处理其网络流量。如果某个端口组没有与其连接的物理网卡，则相同端口组上的虚拟机只能彼此进行通信，而无法与外部网络进行通信。

图 2-1 vSphere 标准交换机架构



vSphere 标准交换机与物理以太网交换机非常相似。主机上的虚拟机网络适配器和物理网卡使用交换机上的逻辑端口，每个适配器使用一个端口。标准交换机上的每个逻辑端口都是单一端口组的成员。有关允许的最大端口和端口组数的信息，请参见《最高配置》文档。

## 标准端口组

标准交换机上的每个标准端口组都由一个对于当前主机必须保持唯一的网络标签来标识。可以使用网络标签来使虚拟机的网络配置可在主机间移植。应为数据中心的端口组提供相同标签，这些端口组使用在物理网络中连接到一个广播域的物理网卡。反过来，如果两个端口组连接不同广播域中的物理网卡，则这两个端口组应具有不同的标签。

例如，可以创建**生产**和**测试环境**端口组来作为在物理网络中共享同一广播域的主机上的虚拟机网络。

**VLAN ID** 是可选的，它用于将端口组流量限制在物理网络内的一个逻辑以太网网段中。要使端口组接收同一个主机可见、但来自多个 **VLAN** 的流量，必须将 **VLAN ID** 设置为 **VGT (VLAN 4095)**。

## 标准端口数

为了确保高效使用主机资源，在运行 **ESXi 5.5** 及更高版本的主机上，标准交换机的端口数将按比例自动增加和减少。此主机上的标准交换机可扩展至主机上支持的最大端口数。



## 创建 vSphere 标准交换机

创建 vSphere 标准交换机，以便为主机和虚拟机提供网络连接并处理 VMkernel 流量。根据要创建的连接类型，可以使用 VMkernel 适配器创建新的 vSphere 标准交换机，仅将物理网络适配器连接到新交换机，或使用虚拟机端口组创建交换机。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开网络，然后选择虚拟交换机。
- 3 单击添加主机网络。
- 4 选择要使用新标准交换机的连接类型，然后单击下一步。

选项	描述
<b>VMkernel 网络适配器</b>	创建新的 VMkernel 适配器，以便处理主机管理流量、vMotion、网络存储、容错或 Virtual SAN 流量。
<b>物理网络适配器</b>	将物理网络适配器添加到现有或新的标准交换机。
<b>标准交换机的虚拟机端口组</b>	为虚拟机网络创建新的端口组。

- 5 选择新建标准交换机，然后单击下一步。
- 6 将物理网络适配器添加到新的标准交换机。
  - a 在“分配的适配器”下，单击添加适配器。
  - b 从列表中选择一个或多个物理网络适配器。
  - c 在故障切换顺序组下拉菜单中，从“活动”或“备用”故障切换列表中进行选择。  
若要实现更高的吞吐量并提供冗余，请在“活动”列表中至少配置两个物理网络适配器。
  - d 单击确定。
- 7 如果使用 VMkernel 适配器或虚拟机端口组创建新的标准交换机，请输入适配器或端口组的连接设置。

选项	描述
<b>VMkernel 适配器</b>	<ol style="list-style-type: none"> <li>a 输入表示 VMkernel 适配器的流量类型的标签，例如 vMotion。</li> <li>b 设置 VLAN ID 以标识 VMkernel 适配器的网络流量将使用的 VLAN。</li> <li>c 选择 IPv4、IPv6 或同时选择两者。</li> <li>d 选择一个 TCP/IP 堆栈。为 VMkernel 适配器设置 TCP/IP 堆栈后，以后便无法再更改该堆栈。如果选择 vMotion 或置备 TCP/IP 堆栈，您将只能使用此堆栈来处理主机上的 vMotion 或置备流量。</li> <li>e 如果使用默认 TCP/IP 堆栈，请从可用服务中进行选择。</li> <li>f 配置 IPv4 和 IPv6 设置。</li> </ol>
<b>虚拟机端口组</b>	<ol style="list-style-type: none"> <li>a 输入网络标签或端口组，或接受生成的标签。</li> <li>b 设置 VLAN ID，以便在端口组中配置 VLAN 处理。</li> </ol>

- 8 在“即将完成”页面上，单击确定。

### 下一步

- 可能需要更改新标准交换机的绑定和故障切换策略。例如，如果主机连接到物理交换机上的以太网通道，则必须将 vSphere 标准交换机配置为使用基于 IP 哈希的路由作为负载平衡算法。有关详细信息，请参见第 81 页，“成组和故障切换策略”。
- 如果使用端口组为虚拟机网络创建新的标准交换机，请将虚拟机连接到端口组。

## 虚拟机的端口组配置

您可以添加或修改虚拟机端口组，以便对一组虚拟机设置流量管理。

vSphere Web Client 中的添加网络向导将引导您完成与虚拟机相连接的虚拟网络的创建过程，包括创建 vSphere 标准交换机和配置网络标签设置。

设置虚拟机网络时，需要考虑是否在主机之间的网络中迁移虚拟机。如果需要，请确保两台主机均位于同一广播域（即同一第 2 层子网）内。

ESXi 不支持在不同广播域中的主机之间进行虚拟机迁移，因为迁移后的虚拟机可能需要新网络中不再可访问的系统和资源。即使网络配置设置为高可用性环境或包括可解决不同网络中虚拟机需求的智能交换机，当 ARP 表格为虚拟机进行更新并恢复网络流量时，仍会遇到网络延迟。

虚拟机通过上行链路适配器接入物理网络。只有当一个或多个网络适配器附加到 vSphere 标准交换机时，vSphere 标准交换机才能将数据传输到外部网络。当两个或多个适配器连接到单个标准交换机时，它们便以透明方式进行组合。

## 添加虚拟机端口组

在 vSphere 标准交换机中创建端口组，以便为虚拟机提供连接和常用网络配置。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 右键单击主机，然后选择**添加网络**。
- 3 在**选择连接类型**中，选择**标准交换机的虚拟机端口组**，然后单击**下一步**。
- 4 在**选择目标设备**中，选择现有标准交换机或创建新的标准交换机。
- 5 如果新端口组用于现有标准交换机，请导航至该交换机。
  - a 单击**浏览**。
  - b 从列表中选择标准交换机，然后单击**确定**。
  - c 单击**下一步**，然后转至**步骤 7**。
- 6 （可选）在“创建标准交换机”页面上，将物理网络适配器分配给该标准交换机。

创建标准交换机不一定需要适配器。

如果创建的标准交换机不带物理网络适配器，则该交换机上的所有流量仅限于其内部。物理网络上的其他主机或其他标准交换机上的虚拟机均无法通过此标准交换机发送或接收流量。如果想要一组虚拟机互相进行通信但不与其他主机或虚拟机组之外的虚拟机进行通信，则可创建一个不带物理网络适配器的标准交换机。

- a 单击**添加适配器**。
- b 从**网络适配器**列表选择一个适配器。
- c 使用**故障切换顺序组**下拉菜单将该适配器分配到“活动适配器”、“备用适配器”或“未用的适配器”，然后单击**确定**。
- d （可选）根据需要在**分配的适配器**列表中使用向上和向下箭头更改适配器的位置。
- e 单击**下一步**。

- 7 在“连接设置”页面上，标识通过该组的各个端口的流量。
  - a 为端口组键入**网络标签**，或接受生成的标签。
  - b 设置 **VLAN ID**，以便在端口组中配置 VLAN 处理。

VLAN ID 也会在端口组中反映 VLAN 标记模式。

VLAN 标记模式	VLAN ID	描述
外部交换机标记 (EST)	0	虚拟交换机不会传递与 VLAN 关联的流量。
虚拟交换机标记 (VST)	从 1 到 4094	虚拟交换机将使用输入的标记来标记流量。
虚拟客户机标记 (VGT)	4095	虚拟机会处理 VLAN。虚拟交换机会传递来自任意 VLAN 的流量。

- c 单击**下一步**。
  - 8 在“即将完成”页面中查看端口组设置，然后单击**完成**。
- 如果要更改任何设置，请单击**上一步**。

## 编辑标准交换机端口组

可以使用 vSphere Web Client 编辑标准交换机端口组的名称和 VLAN ID，并在端口组级别替代网络策略。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
  - 2 在**配置**选项卡上，展开**网络**，然后选择**虚拟交换机**。
  - 3 在列表中选择一個标准交换机。
- 此时将显示交换机的拓扑图。
- 4 在交换机的拓扑图中，单击端口组的名称。
  - 5 在拓扑图标题下，单击**编辑设置**图标。
  - 6 在“属性”页面的**网络标签**文本字段中，重命名端口组。
  - 7 在 **VLAN ID** 下拉菜单中配置 VLAN 标记。

VLAN 标记模式	VLAN ID	描述
外部交换机标记 (EST)	0	虚拟交换机不会传递与 VLAN 关联的流量。
虚拟交换机标记 (VST)	从 1 到 4094	虚拟交换机将使用输入的标记来标记流量。
虚拟客户机标记 (VGT)	4095	虚拟机会处理 VLAN。虚拟交换机会传递来自任意 VLAN 的流量。

- 8 在“安全”页面上，替代交换机设置，以防止 MAC 地址模拟，并在混杂模式下运行虚拟机。
- 9 在“流量调整”页面上，在端口组级别替代平均带宽、峰值带宽和突发的大小。
- 10 在“绑定和故障切换”页面上，替代从标准交换机继承的绑定和故障切换设置。

您可以在与端口组关联的物理适配器之间配置流量分布和重新路由。也可以更改发生故障时使用主机物理适配器的顺序。

- 11 单击**确定**。

## 从 vSphere 标准交换机移除端口组

如果不再需要关联的带标记网络，则可从 vSphere 标准交换机移除端口组。

### 前提条件

确认要移除的端口组未连接任何已打开电源的虚拟机。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开网络，然后选择虚拟交换机。
- 3 选择标准交换机。
- 4 从交换机的拓扑图中，单击端口组的标签以选择要移除的端口组。
- 5 在交换机拓扑的工具栏中，单击移除选定的端口组操作图标。

## vSphere 标准交换机属性

vSphere 标准交换机设置可控制端口的交换机层面默认值，而每个标准交换机的端口组设置均可覆盖这些值。您可以编辑标准交换机属性，如上行链路配置和可用端口数。

## ESXi 主机上的端口数量

为了确保高效使用主机资源，在运行 ESXi 5.5 及更高版本的主机上，虚拟交换机的端口数将按比例动态增加和减少。此主机上的交换机可扩展至主机上支持的最大端口数。端口限制基于主机可处理的最大虚拟机数来确定。

运行 ESXi 5.1 及更低版本的主机上的每个虚拟交换机均提供有限数量的端口，虚拟机和网络服务可以通过这些端口访问一个或多个网络。您必须根据您的部署要求手动增加或减少端口数。

---

**注意** 增加交换机的端口数将导致预留和消耗主机上更多的资源。如果某些端口未被占用，则某些可能需要用于其他操作的主机资源将保持锁定和未使用状态。

---

## 更改 vSphere 标准交换机上 MTU 的大小

更改 vSphere 标准交换机上最大传输单元 (MTU) 的大小，即增加使用单个数据包传输的负载数据量（也就是启用巨帧）来提高网络效率。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开网络，然后选择虚拟交换机。
- 3 从表中选择一台标准交换机，然后单击编辑设置。
- 4 更改标准交换机的 MTU (字节) 值。  
您可以通过设置大于 1500 的 MTU 值启用巨帧。设置的 MTU 大小不能超过 9000 字节。
- 5 单击确定。

## 更改物理适配器的速度

如果物理适配器速度与应用程序要求不匹配，则该适配器可能会成为网络流量的瓶颈。您可以更改物理适配器的连接速度和双工模式，以便按照流量速率来传输数据。

如果该物理适配器支持 SR-IOV，可以启用它，并配置虚拟机网络连接要使用的虚拟功能数。

**步骤**

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开**网络**，然后选择**物理适配器**。  
主机的物理网络适配器会显示在一个表中，该表包含每个物理网络适配器的详细信息。
- 3 从列表中选择物理网络适配器，然后单击**编辑适配器设置**图标。
- 4 从下拉菜单中选择该物理网络适配器的速度和双工模式。
- 5 单击**确定**。

**在 vSphere 标准交换机中添加物理适配器并使这些适配器成组**

向标准交换机分配物理适配器可提供与主机上的虚拟机和 VMkernel 适配器的连接。可以组建一个网卡组，以分布流量负载并配置故障切换。

网卡绑定可将多个网络连接组合在一起以增加吞吐量，并在链路出现故障时提供冗余。要创建组，请将多个物理适配器与一个 vSphere 标准交换机关联起来。

**步骤**

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开**网络**，然后选择**虚拟交换机**。
- 3 选择要添加物理适配器的标准交换机。
- 4 单击**管理已连接到选定交换机的物理网络适配器**图标。
- 5 向交换机添加一个或多个可用的物理网络适配器。
  - a 单击**添加适配器**。
  - b 选择要向其分配适配器的故障切换顺序组。  
该故障切换组将决定适配器与外部网络交换数据的角色，即活动、备用或未使用。默认情况下，适配器会作为活动角色添加到标准交换机。
  - c 单击**确定**  
选定适配器会显示在“分配的适配器”列表下的选定故障切换组列表中。
- 6 （可选）使用向上和向下箭头可更改适配器在故障切换组中的位置。
- 7 单击**确定**应用物理适配器配置。

**查看 vSphere 标准交换机的拓扑图**

可以使用 vSphere 标准交换机的拓扑图检查该交换机的结构和组件。

标准交换机的拓扑图提供连接到该交换机的适配器和端口组的直观表示。

在该拓扑图中，您可以编辑所选端口组和所选适配器的设置。

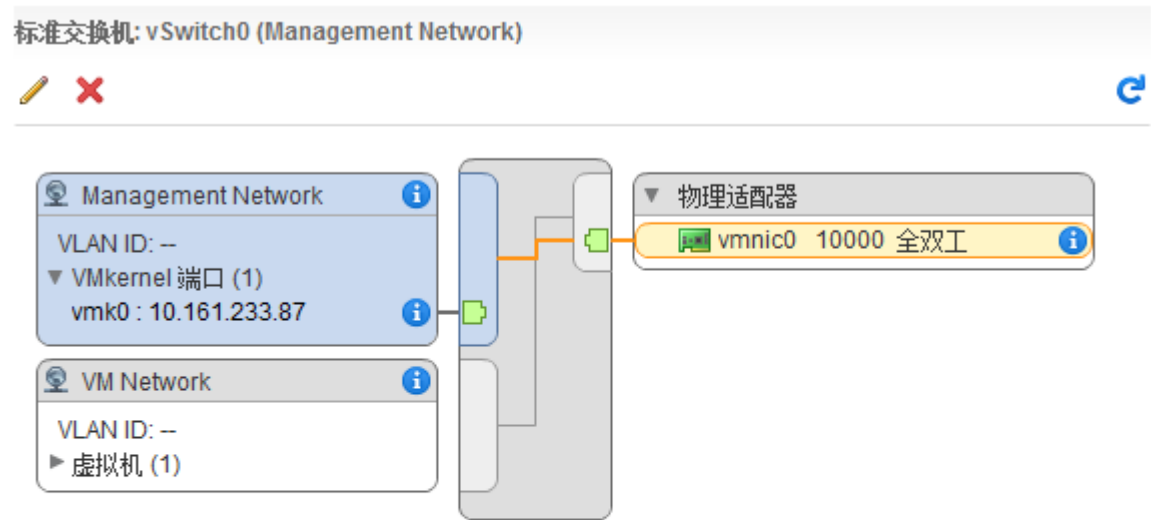
**步骤**

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开**网络**，然后选择**虚拟交换机**。
- 3 在列表中选择标准交换机。  
拓扑图将显示在主机上虚拟交换机的列表下。

## 示例：将 VMkernel 和虚拟机连接到网络的标准交换机图

在您的虚拟环境中，vSphere 标准交换机为 vSphere vMotion 和管理网络处理 VMkernel 适配器以及分组的虚拟机。可以使用中心拓扑图来检查虚拟机或 VMkernel 适配器是否连接到外部网络，并确定承载数据的物理适配器。

图 2-2 将 VMkernel 和虚拟机连接到网络的标准交换机拓扑图



# 使用 vSphere Distributed Switch 设置 网络连接

---

# 3

通过 vSphere Distributed Switch，可以在 vSphere 环境中设置和配置网络连接。

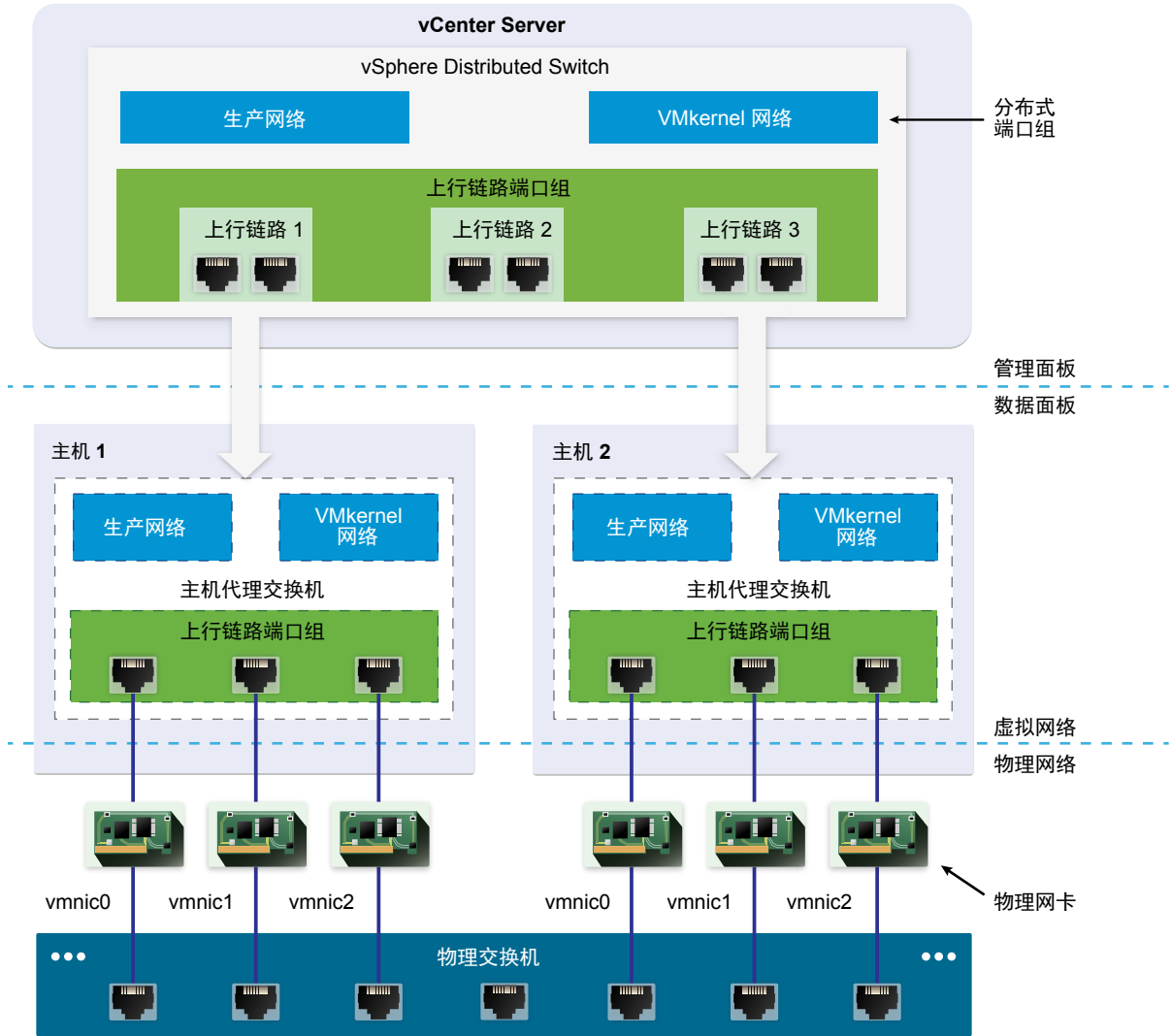
本章讨论了以下主题：

- 第 24 页，[“vSphere Distributed Switch 架构”](#)
- 第 27 页，[“创建 vSphere Distributed Switch”](#)
- 第 28 页，[“将 vSphere Distributed Switch 升级到更高版本”](#)
- 第 29 页，[“编辑 vSphere Distributed Switch 常规和高级设置”](#)
- 第 30 页，[“在 vSphere Distributed Switch 上管理多个主机上的网络连接”](#)
- 第 37 页，[“在主机代理交换机上管理网络连接”](#)
- 第 40 页，[“分布式端口组”](#)
- 第 44 页，[“使用分布式端口”](#)
- 第 45 页，[“在 vSphere Distributed Switch 上配置虚拟机网络连接”](#)
- 第 46 页，[“vSphere Web Client 中的 vSphere Distributed Switch 拓扑图”](#)

## vSphere Distributed Switch 架构

vSphere Distributed Switch 为与交换机关联的所有主机的网络连接配置提供集中化管理和监控。您可以在 vCenter Server 系统上设置 Distributed Switch，其设置将传播至与该交换机关联的所有主机。

图 3-1 vSphere Distributed Switch 架构



vSphere 中的网络交换机由两个逻辑部分组成：数据面板和管理面板。数据面板可实现软件包交换、筛选和标记等。管理面板是用于配置数据面板功能的控制结构。vSphere 标准交换机同时包含数据面板和管理面板，您可以单独配置和维护每个标准交换机。

vSphere Distributed Switch 的数据面板和管理面板相互分离。Distributed Switch 的管理功能驻留在 vCenter Server 系统上，您可以在数据中心级别管理环境的网络配置。数据面板则保留在与 Distributed Switch 关联的每台主机本地。Distributed Switch 的数据面板部分称为主机代理交换机。在 vCenter Server（管理面板）上创建的网络配置将被自动向下推送至所有主机代理交换机（数据面板）。



vSphere Distributed Switch 引入的两个抽象概念可用于为物理网卡、虚拟机和 VMkernel 服务创建一致的网络配置。

### 上行链路端口组

上行链路端口组或 dvuplink 端口组在创建 Distributed Switch 期间进行定义，可以具有一个或多个上行链路。上行链路是可用于配置主机物理连接以及故障切换和负载均衡策略的模板。您可以将主机的物理网卡映射到 Distributed Switch 上的上行链路。在主机级别，每个物理网卡将连接到特定 ID 的上行链路端口。您可以对上行链路设置故障切换和负载均衡策略，这些策略将自动传播到主机代理交换机或数据面板。因此，您可以为与 Distributed Switch 关联的所有主机的物理网卡应用一致的故障切换和负载均衡配置。

### 分布式端口组

分布式端口组可向虚拟机提供网络连接并供 VMkernel 流量使用。您使用对于当前数据中心唯一的网络标签来标识每个分布式端口组。您可以在分布式端口组上配置网卡成组、故障切换、负载均衡、VLAN、安全、流量调整和其他策略。连接到分布式端口组的虚拟端口具有为该分布式端口组配置的相同属性。与上行链路端口组一样，在 vCenter Server（管理面板）上为分布式端口组设置的配置将通过其主机代理交换机（数据面板）自动传播到 Distributed Switch 上的所有主机。因此，您可以配置一组虚拟机以共享相同的网络配置，方法是将虚拟机与同一分布式端口组关联。

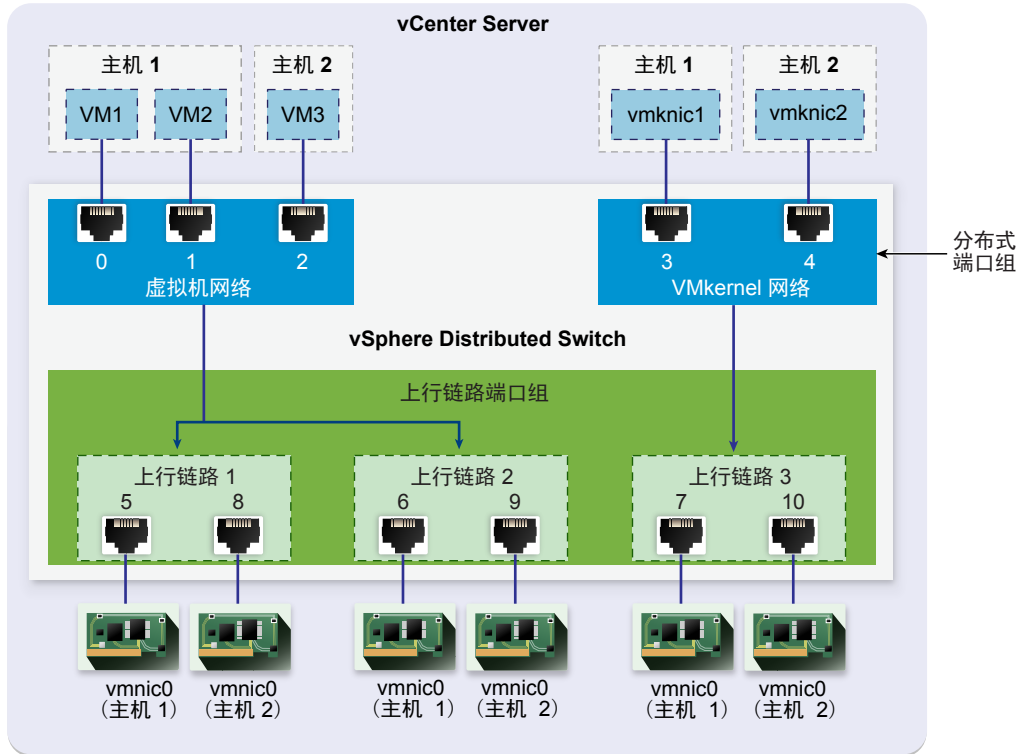
例如，假设在数据中心创建一个 vSphere Distributed Switch，然后将两个主机与其关联。您为上行链路端口组配置了三个上行链路，然后将每个主机的一个物理网卡连接到一个上行链路。通过此方法，每个上行链路可将每个主机的两个物理网卡映射到其中，例如上行链路 1 使用主机 1 和主机 2 的 vmnic0 进行配置。接下来，您可以为虚拟机网络和 VMkernel 服务创建生产和 VMkernel 网络分布式端口组。此外，还会分别在主机 1 和主机 2 上创建生产和 VMkernel 网络端口组的表示。您为生产和 VMkernel 网络端口组设置的所有策略都将传播到其在主机 1 和主机 2 上的表示。

为了确保有效地利用主机资源，将在运行 ESXi 5.5 及更高版本的主机上动态地按比例增加和减少代理交换机的分布式端口数。此主机上的代理交换机可扩展至主机上支持的最大端口数。端口限制基于主机可处理的最大虚拟机数来确定。

## vSphere Distributed Switch 数据流

从虚拟机和 VMkernel 适配器向下传递到物理网络的数据流取决于为分布式端口组设置的网卡成组和负载均衡策略。数据流还取决于 Distributed Switch 上的端口分配。

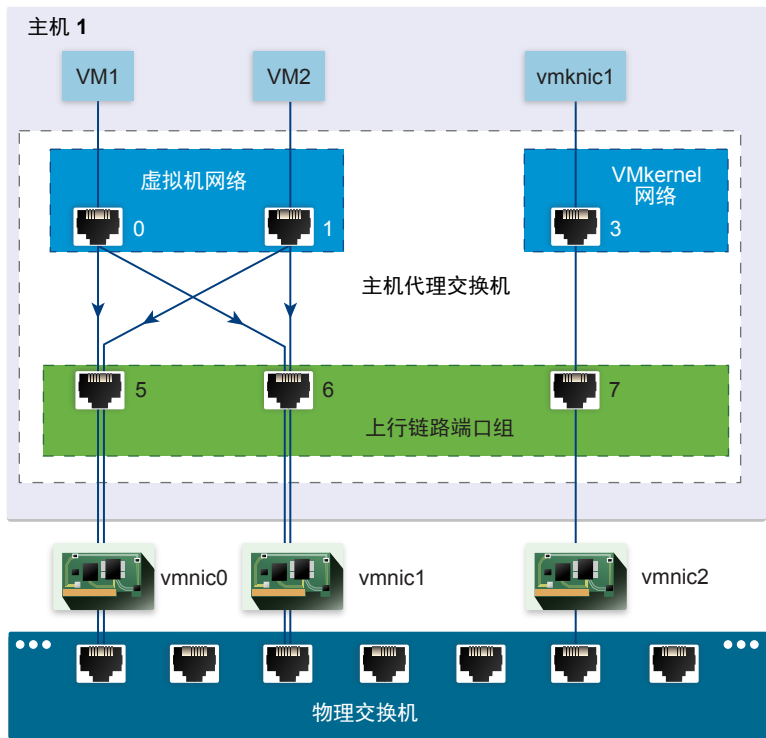
图 3-2 vSphere Distributed Switch 上的网卡成组和端口分配



例如，假设创建分别包含 3 个和 2 个分布式端口的虚拟机网络和 VMkernel 网络分布式端口组。Distributed Switch 会按 ID 从 0 到 4 的顺序分配端口，该顺序与创建分布式端口组的顺序相同。然后，将主机 1 和主机 2 与 Distributed Switch 关联。Distributed Switch 会为主机上的每个物理网卡分配端口，端口将按添加主机的顺序从 5 继续编号。要在每个主机上提供网络连接，请将 vmnic0 映射到上行链路 1、将 vmnic1 映射到上行链路 2、将 vmnic2 映射到上行链路 3。

要向虚拟机提供连接并供 VMkernel 流量使用，可以为虚拟机网络端口组和 VMkernel 网络端口组配置成组和故障切换。上行链路 1 和上行链路 2 处理虚拟机网络端口组的流量，而上行链路 3 处理 VMkernel 网络端口组的流量。

图 3-3 主机代理交换机上的数据包流量



在主机端，虚拟机和 VMkernel 服务的数据包流量将通过特定端口传递到物理网络。例如，从主机 1 上的 VM1 发送的数据包将先到达虚拟机网络分布式端口组上的端口 0。由于上行链路 1 和上行链路 2 处理虚拟机网络端口组的流量，数据包可以通过上行链路端口 5 或上行链路端口 6 继续传递。如果数据包通过上行链路端口 5，则将继续传递到 vmnic0；如果数据包通过上行链路端口 6，则将继续传递到 vmnic1。

## 创建 vSphere Distributed Switch

在数据中心创建 vSphere Distributed Switch，以便在一个中央位置同时处理多个主机的网络配置。

### 步骤

- 1 在 vSphere Web Client 中，导航到数据中心。
- 2 在导航器中，右键单击数据中心，并选择 **Distributed Switch > 新建 Distributed Switch**。
- 3 在“名称和位置”页面上，键入新的 Distributed Switch 的名称，或接受生成的名称，然后单击**下一步**。
- 4 在“选择版本”页面上，选择 Distributed Switch 版本，然后单击**下一步**。

选项	描述
Distributed Switch: 6.5.0	与 ESXi 6.5 及更高版本兼容。
Distributed Switch: 6.0.0	与 ESXi 6.0 及更高版本兼容。不支持与更高版本的 vSphere Distributed Switch 一起发布的功能。
Distributed Switch: 5.5.0	与 ESXi 5.5 及更高版本兼容。不支持与更高版本的 vSphere Distributed Switch 一起发布的功能。
Distributed Switch: 5.1.0	与 VMware ESXi 5.1 及更高版本兼容。不支持与更高版本的 vSphere Distributed Switch 一起发布的功能。
Distributed Switch: 5.0.0	与 VMware ESXi 5.0 及更高版本兼容。 不支持与更高版本的 vSphere Distributed Switch 一起发布的功能。

- 5 在“编辑设置”页面上，配置 Distributed Switch 设置。
  - a 使用箭头按钮选择**上行链路数**。  
上行链路端口将 Distributed Switch 连接到关联主机上的物理网卡。上行链路端口数是允许每台主机与 Distributed Switch 建立的最大物理连接数。
  - b 使用此下拉菜单启用或禁用 **Network I/O Control**。  
利用 Network I/O Control 可以根据部署要求设定特定类型基础架构的网络资源以及工作负载流量的访问优先级。Network I/O Control 会持续监控整个网络的 I/O 负载，并动态地分配可用资源。
  - c 选中**创建默认端口组**复选框使用默认设置为该交换机创建新的分布式端口组。
  - d （可选）要创建默认的分布式端口组，可以在**端口组名称**中键入端口组的名称，或者接受生成的名称。  
如果系统具有自定义端口组要求，则在添加 Distributed Switch 后，创建满足这些要求的分布式端口组。
  - e 单击**下一步**。
- 6 在“即将完成”页面上，查看您选择的设置，然后单击**完成**。  
使用**上一步**按钮可编辑任何设置。

Distributed Switch 即在数据中心创建完毕。您可以通过导航到该新的 Distributed Switch 并单击**摘要**选项卡，查看该 Distributed Switch 支持的功能及其他详细信息。

#### 下一步

为 Distributed Switch 添加主机，并配置这些主机在交换机上的网络适配器。

## 将 vSphere Distributed Switch 升级到更高版本

您可以将 vSphere Distributed Switch 5.x 版升级到更高版本。升级可以使 Distributed Switch 利用仅在更高版本中提供的功能。

升级 Distributed Switch 的过程是一个非破坏性操作，也就是说，连接到交换机的主机和虚拟机根本不会发生停机。

---

**注意** 要能够在升级失败时还原虚拟机和 VMkernel 适配器的连接，请备份 Distributed Switch 的配置。

如果升级不成功，要使用其端口组和连接的主机重新创建交换机，可以导入交换机配置文件。请参见第 71 页，“导出 vSphere Distributed Switch 配置”和第 72 页，“导入 vSphere Distributed Switch 配置”。

---

#### 前提条件

- 将 vCenter Server 升级到版本 6.5。
- 将连接到 Distributed Switch 的所有主机升级到 ESXi 6.5。

#### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 右键单击 Distributed Switch，然后选择**升级 > 升级 Distributed Switch**。
- 3 选择要将交换机升级到的 vSphere Distributed Switch 版本，然后单击**下一步**。

选项	描述
<b>版本 6.5.0</b>	与 ESXi 6.5 及更高版本兼容。
<b>版本 6.0.0</b>	与 ESXi 6.0 版及更高版本兼容。不支持与更高版本的 vSphere Distributed Switch 一起发布的功能。

选项	描述
<b>5.5.0 版</b>	与 ESXi 5.5 及更高版本兼容。不支持与更高版本的 vSphere Distributed Switch 一起发布的功能。
<b>版本 5.1.0</b>	与 ESXi 5.1 及更高版本兼容。不支持与更高版本的 vSphere Distributed Switch 一起发布的功能。

- 4 检查主机兼容性，然后单击**下一步**。

连接到该 Distributed Switch 的一些 ESXi 实例可能与选定的目标版本不兼容。进行升级或移除不兼容的主机，或者选择 Distributed Switch 的其他升级版本。

- 5 完成升级配置，然后单击**完成**。



**小心** 升级 vSphere Distributed Switch 后，无法将其恢复到早期版本。也无法添加正在运行的版本低于该交换机新版本的 ESXi 主机。

- a 查看升级设置。
- b 如果从 vSphere Distributed Switch 5.1 进行升级，请计划转换为增强型 LACP 支持。
- c 如果从 vSphere Distributed Switch 5.1 及更高版本进行升级，请计划转换为 Network I/O Control 版本 3。

有关转换为增强型 LACP 支持的信息，请参见第 63 页，“[转换为 vSphere Distributed Switch 上的增强型 LACP 支持](#)”。

有关转换为 Network I/O Control 版本 3 的信息，请参见第 146 页，“[将 vSphere Distributed Switch 上的 Network I/O Control 升级到版本 3](#)”。

## 编辑 vSphere Distributed Switch 常规和高级设置

vSphere Distributed Switch 的常规设置包括交换机名称和上行链路数量。Distributed Switch 的高级设置包括 Cisco 发现协议和交换机的最大 MTU。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在**配置**选项卡上，展开**设置**并选择**属性**。
- 3 单击**编辑**。
- 4 单击**常规**以编辑 vSphere Distributed Switch 设置。

选项	描述
<b>名称</b>	键入 Distributed Switch 的名称。
<b>上行链路数</b>	选择 Distributed Switch 的上行链路端口数。 单击 <b>编辑上行链路名称</b> 更改上行链路的名称。
<b>端口数</b>	该 Distributed Switch 的端口数。该信息不能编辑。
<b>Network I/O Control</b>	使用此下拉菜单启用或禁用 Network I/O Control。
<b>描述</b>	添加或修改 Distributed Switch 设置的描述。

- 5 单击 **高级编辑** vSphere Distributed Switch 设置。

选项	描述
<b>MTU (字节)</b>	vSphere Distributed Switch 的最大 MTU 大小。要启用巨帧，请设置一个大于 1500 字节的值。
<b>多播筛选模式</b>	<ul style="list-style-type: none"> <li>■ <b>基本</b>。Distributed Switch 根据从组 IPv4 地址的最后 23 位生成的 MAC 地址转发与多播组相关的流量。</li> <li>■ <b>IGMP/MLD 侦听</b>。Distributed Switch 使用由 Internet 组管理协议 (IGMP) 和多播侦听器发现协议定义的成员身份消息，根据已订阅多播组的 IPv4 和 IPv6 地址将多播流量转发到虚拟机。</li> </ul>
<b>发现协议</b>	<p>a 从<b>类型</b>下拉菜单中选择“Cisco 发现协议”、“链路层发现协议”或“(已禁用)”。</p> <p>b 将“操作”设置为“侦听”、“通告”或“二者”。</p> <p>有关发现协议的信息，请参见第 193 页，“交换机发现协议”。</p>
<b>管理员联系方式</b>	键入 Distributed Switch 管理员的姓名和其他详细信息。

- 6 单击**确定**。

## 在 vSphere Distributed Switch 上管理多个主机上的网络连接

可以通过将主机添加到交换机并将其网络适配器连接到交换机，在 vSphere Distributed Switch 上创建和管理虚拟网络。要在 Distributed Switch 的多个主机上创建统一的网络连接配置，可以选择一个主机作为模板，并将其配置应用到其他主机。

- 在 [vSphere Distributed Switch 上管理主机网络的任务](#) 第 31 页，  
您可以为 vSphere Distributed Switch 添加新主机、将网络适配器连接到交换机以及从交换机移除主机。在生产环境中，当您管理 Distributed Switch 上的主机时，可能需要保持虚拟机和 VMkernel 服务的网络连接有效。
- 将主机添加到 [vSphere Distributed Switch](#) 第 31 页，  
要使用 vSphere Distributed Switch 管理 vSphere 环境的网络，必须将主机与交换机关联。可以将主机的物理网卡、VMkernel 适配器和虚拟机网络适配器连接到 Distributed Switch。
- 在 [vSphere Distributed Switch 上配置物理网络适配器](#) 第 33 页，  
对于与 Distributed Switch 关联的主机，可以将物理网卡分配给交换机上的上行链路。可以在 Distributed Switch 上一次为多个主机配置物理网卡。
- 将 VMkernel 适配器迁移到 [vSphere Distributed Switch](#) 第 33 页，  
如果想要仅使用 vSphere Distributed Switch 来处理 VMkernel 服务的流量，并且不再需要其他标准交换机或 Distributed Switch 上的适配器，请将 VMkernel 适配器迁移到 vSphere Distributed Switch。
- 在 [vSphere Distributed Switch 上创建 VMkernel 适配器](#) 第 34 页，  
在与 Distributed Switch 关联的主机上创建 VMkernel 适配器，以便向主机提供网络连接并处理 vSphere vMotion、IP 存储、Fault Tolerance 日志记录和 Virtual SAN 的流量。可以通过使用添加和管理主机向导同时在多个主机上创建 VMkernel 适配器。
- 将虚拟机网络迁移到 [vSphere Distributed Switch](#) 第 36 页，  
要使用 Distributed Switch 管理虚拟机网络连接，请将虚拟机网络适配器迁移到交换机上有标记的网络。
- 使用主机作为模板为 [vSphere Distributed Switch](#) 创建统一的网络配置 第 36 页，  
如果您计划使多台主机拥有统一的网络配置，则可选择其中一台主机作为模板，并将其物理网卡和 VMkernel 适配器的配置应用到 Distributed Switch 上的其他主机。
- 从 [vSphere Distributed Switch](#) 中移除主机 第 37 页，  
如果为主机配置了其他交换机，则可以从 vSphere Distributed Switch 中移除主机。

## 在 vSphere Distributed Switch 上管理主机网络的任务

您可以为 vSphere Distributed Switch 添加新主机、将网络适配器连接到交换机以及从交换机移除主机。在生产环境中，当您管理 Distributed Switch 上的主机时，可能要保持虚拟机和 VMkernel 服务的网络连接有效。

### 为 vSphere Distributed Switch 添加主机

在为 Distributed Switch 添加主机之前，应考虑做好环境准备。

- 为虚拟机网络创建分布式端口组。
- 为 VMkernel 服务创建分布式端口组。例如，为管理网络、vMotion 和 Fault Tolerance 创建分布式端口组。
- 在 Distributed Switch 上为要连接交换机的所有物理网卡配置足够的上行链路。例如，如果要连接 Distributed Switch 的每个主机都有八个物理网卡，则在 Distributed Switch 上配置八个上行链路。
- 确保为具有特殊网络要求的服务准备了 Distributed Switch 的配置。例如，iSCSI 对用来连接 iSCSI VMkernel 适配器的分布式端口组的绑定和故障切换配置具有特殊要求。

可以在 vSphere Web Client 中使用 添加和管理主机向导一次添加多个主机。

### 在 vSphere Distributed Switch 上管理网络适配器

为 Distributed Switch 添加主机后，可以将物理网卡连接到交换机上的上行链路、配置虚拟机网络适配器以及管理 VMkernel 网络。

如果 Distributed Switch 上的部分主机与数据中心内的其他主机关联，可以将网络适配器迁移到 Distributed Switch，或者从 Distributed Switch 中迁移出网络适配器。

如果迁移虚拟机网络适配器或 VMkernel 适配器，应确保目标分布式端口组至少有一个活动的上行链路，并且该链路与主机上的物理网卡连接。另一个方法是同时迁移物理网卡、虚拟网络适配器和 VMkernel 适配器。

如果迁移物理网卡，至少应使一个网卡处于活动状态，以处理端口组的流量。例如，如果 *vmnic0* 和 *vmnic1* 处理 VM Network 端口组的流量，则迁移 *vmnic0*，并使 *vmnic1* 与该组保持连接。

### 从 vSphere Distributed Switch 移除主机

从 Distributed Switch 移除主机之前，必须将使用中的网络适配器迁移到不同的交换机。

- 要在不同的 Distributed Switch 中添加主机，可以使用添加和管理主机向导将主机上的所有网络适配器一起迁移到新的交换机。然后便可以从当前的 Distributed Switch 中安全地移除主机。
- 要将主机网络迁移到标准交换机，必须分阶段迁移网络适配器。例如，使每个主机上的一个物理网卡与交换机保持连接以保证网络连接有效，即可从 Distributed Switch 移除主机上的物理网卡。接着，将物理网卡连接到标准交换机，并将 VMkernel 适配器和虚拟机网络适配器迁移到交换机。最后，将与 Distributed Switch 保持连接的物理网卡迁移到标准交换机。

## 将主机添加到 vSphere Distributed Switch

要使用 vSphere Distributed Switch 管理 vSphere 环境的网络，必须将主机与交换机关联。可以将主机的物理网卡、VMkernel 适配器和虚拟机网络适配器连接到 Distributed Switch。

### 前提条件

- 验证 Distributed Switch 上有足够的可用上行链路，可以分配给要连接交换机的物理网卡。
- 确认在 Distributed Switch 上至少有一个分布式端口组。
- 确认分布式端口组的绑定和故障切换策略中已配置了活动上行链路。

如果为 iSCSI 迁移或创建 VMkernel 适配器，请确认目标分布式端口组的绑定和故障切换策略满足 iSCSI 的要求：

- 确认只有一个上行链路处于活动状态，待机列表为空，其余上行链路未被使用。
- 确认每个主机只有一个物理网卡分配给活动上行链路。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 从操作菜单中，选择**添加和管理主机**。
- 3 在“选择任务”页面上，选择**添加主机**，然后单击**下一步**。
- 4 在“选择主机”页面上，单击**新主机**，选择数据中心内的主机，单击**确定**，然后单击**下一步**。
- 5 在“选择网络适配器任务”页面上，选择配置 Distributed Switch 的网络适配器的任务，然后单击**下一步**。
- 6 在“管理物理网络适配器”页面上，配置 Distributed Switch 上的物理网卡。
  - a 从“其他交换机上/空闲”列表中选择物理网卡。  
如果选择已经连接其他交换机的物理网卡，这些物理网卡即迁移到当前的 Distributed Switch 上。
  - b 单击**分配上行链路**。
  - c 选择一个上行链路，然后单击**确定**。  
为实现网络配置的一致性，可以将每个主机上的一个相同的物理网卡与 Distributed Switch 上的相同的上行链路连接。  
例如，如果要添加两个主机，则将每个主机上的 *vmnic1* 与 Distributed Switch 上的 *Uplink1* 连接。
- 7 单击**下一步**。
- 8 在“管理 VMkernel 网络适配器”页面上，配置 VMkernel 适配器。
  - a 选择 VMkernel 适配器并单击**分配端口组**。
  - b 选择分布式端口组，然后单击**确定**。
- 9 查看受影响的服务以及影响的程度。
 

选项	描述
<b>无影响</b>	应用新的网络连接配置之后，iSCSI 将继续执行其常规功能。
<b>重要影响</b>	如果应用了新的网络连接配置，则可能会中断 iSCSI 的常规功能。
<b>严重影响</b>	如果应用了新的网络连接配置，则将中断 iSCSI 的常规功能。

  - a 如果 iSCSI 受到的影响非常重要或严重，请单击 **iSCSI** 条目，然后查看“分析详细信息”窗格中所显示的原因。
  - b 排除对 iSCSI 造成的影响之后，请继续进行网络连接配置。
- 10 单击**下一步**。
- 11 在“迁移虚拟机网络”页面上，配置虚拟机网络连接。
  - a 要将某个虚拟机的所有网络适配器连接到分布式端口组，请选择该虚拟机，或者选择单个网络适配器以仅连接该适配器。
  - b 单击**分配端口组**。
  - c 从列表中选择一个分布式端口组，然后单击**确定**。
- 12 单击**下一步**，然后单击**完成**。



下一步

将主机与 Distributed Switch 关联后，可以管理物理网卡、VMkernel 适配器和虚拟机网络适配器。

在 vSphere Distributed Switch 上配置物理网络适配器

对于与 Distributed Switch 关联的主机，可以将物理网卡分配给交换机上的上行链路。可以在 Distributed Switch 上一次为多个主机配置物理网卡。

要确保所有主机的网络连接配置保持一致，可以将每个主机上的相同物理网卡分配到 Distributed Switch 上的相同上行链路。例如，可以将主机 *ESXi A* 和 *ESXi B* 中的 *vmnic1* 分配到 *Uplink 1*。

步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 从操作菜单中，选择添加和管理主机。
- 3 在选择任务中，选择管理主机网络，然后单击下一步。
- 4 在选择主机中，单击连接的主机，然后从与 Distributed Switch 关联的主机中进行选择。
- 5 单击下一步。
- 6 在选择网络适配器任务中，选择管理物理适配器，然后单击下一步。
- 7 在管理物理网络适配器中，从“其他交换机上/空闲”列表选择一个物理网卡。  
如果选择已分配到其他交换机的物理网卡，请将其迁移至当前的 Distributed Switch。
- 8 单击分配上行链路。
- 9 选择一个上行链路或选择自动分配。
- 10 单击下一步。
- 11 查看受影响的服务以及影响的程度。

选项	描述
无影响	应用新的网络连接配置之后，iSCSI 将继续执行其常规功能。
重要影响	如果应用了新的网络连接配置，则可能会中断 iSCSI 的常规功能。
严重影响	如果应用了新的网络连接配置，则将中断 iSCSI 的常规功能。

- a 如果 iSCSI 受到的影响非常重要或严重，请单击 iSCSI 条目，然后查看“分析详细信息”窗格中所显示的原因。
  - b 排除对 iSCSI 造成的影响之后，请继续进行网络连接配置。
- 12 单击下一步，然后单击完成。

将 VMkernel 适配器迁移到 vSphere Distributed Switch

如果想要仅使用 vSphere Distributed Switch 来处理 VMkernel 服务的流量，并且不再需要其他标准交换机或 Distributed Switch 上的适配器，请将 VMkernel 适配器迁移到 vSphere Distributed Switch。

步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 从操作菜单中，选择添加和管理主机。
- 3 在选择任务中，选择管理主机网络，然后单击下一步。
- 4 在选择主机中，单击连接的主机，然后从与 Distributed Switch 关联的主机中进行选择。

- 5 单击下一步。
- 6 在**选择网络适配器任务**中，选择**管理 VMkernel 适配器**，然后单击下一步。
- 7 在**管理 VMkernel 网络适配器**中，选择适配器并单击**分配端口组**。
- 8 选择分布式端口组，然后单击**确定**。
- 9 单击下一步。
- 10 查看受影响的服务以及影响的程度。

选项	描述
<b>无影响</b>	应用新的网络连接配置之后，iSCSI 将继续执行其常规功能。
<b>重要影响</b>	如果应用了新的网络连接配置，则可能会中断 iSCSI 的常规功能。
<b>严重影响</b>	如果应用了新的网络连接配置，则将中断 iSCSI 的常规功能。

- a 如果 iSCSI 受到的影响非常重要或严重，请单击 **iSCSI** 条目，然后查看“分析详细信息”窗格中所显示的原因。
  - b 排除对 iSCSI 造成的影响之后，请继续进行网络连接配置。
- 11 单击下一步，然后单击**完成**。

## 在 vSphere Distributed Switch 上创建 VMkernel 适配器

在与 Distributed Switch 关联的主机上创建 VMkernel 适配器，以便向主机提供网络连接并处理 vSphere vMotion、IP 存储、Fault Tolerance 日志记录和 Virtual SAN 的流量。可以通过使用添加和管理主机向导同时在多个主机上创建 VMkernel 适配器。

应专门针对每个 VMkernel 适配器使用一个分布式端口组。一个 VMkernel 适配器应仅处理一种流量类型。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 从**操作菜单**中，选择**添加和管理主机**。
- 3 在**选择任务**中，选择**管理主机网络**，然后单击下一步。
- 4 在**选择主机**中，单击**连接的主机**，然后从与 Distributed Switch 关联的主机中进行选择。
- 5 单击下一步。
- 6 在**选择网络适配器任务**中，选择**管理 VMkernel 适配器**，然后单击下一步。
- 7 单击**新建适配器**。  
此时会打开添加网络向导。
- 8 在**选择目标设备**中，选择一个分布式端口组，然后单击下一步。
- 9 在“端口属性”页面上，配置 VMkernel 适配器的设置。

选项	描述
<b>网络标签</b>	网络标签从分布式端口组的标签继承。
<b>IP 设置</b>	选择 IPv4、IPv6 或同时选择两者。 <b>注意</b> 在未启用 IPv6 的主机上，IPv6 选项不会显示。

选项	描述
<b>TCP/IP 堆栈</b>	在列表中选择一个 TCP/IP 堆栈。为 VMkernel 适配器设置了 TCP/IP 堆栈后，日后将不能再进行更改。如果选择 vMotion 或置备 TCP/IP 堆栈，您将只能使用这些堆栈处理主机上的 vMotion 或置备流量。默认 TCP/IP 堆栈上所有适用于 vMotion 的 VMkernel 适配器将被禁止用于未来的 vMotion 会话。如果设置了置备 TCP/IP 堆栈，默认 TCP/IP 堆栈上的 VMkernel 适配器将被禁止用于包括置备流量的操作，例如虚拟机冷迁移、克隆和快照创建。
<b>启用服务</b>	<p>可以为主机上的默认 TCP/IP 堆栈启用服务。请从以下可用服务中选择：</p> <ul style="list-style-type: none"> <li>■ <b>vMotion 流量</b>。允许 VMkernel 适配器向另一台主机播发声明，自己就是发送 vMotion 流量所应使用的网络连接。如果未对默认 TCP/IP 堆栈上的任何 VMkernel 适配器启用 vMotion 服务，或者根本不存在使用 vMotion TCP/IP 堆栈的适配器，将不能使用 vMotion 迁移到选定的主机。</li> <li>■ <b>置备流量</b>。处理为用于虚拟机冷迁移、克隆和快照创建而传输的数据。</li> <li>■ <b>Fault Tolerance 流量</b>。在主机上启用 Fault Tolerance 日志记录。对每台主机的 FT 流量只能使用一个 VMkernel 适配器。</li> <li>■ <b>管理流量</b>。为主机和 vCenter Server 启用管理流量。通常，安装 ESXi 软件后，主机将创建这样的 VMkernel 适配器。可以为主机上的管理流量创建其他 VMkernel 适配器以提供冗余。</li> <li>■ <b>vSphere Replication 流量</b>。处理从源 ESXi 主机发送到 vSphere Replication 服务器的出站复制数据。</li> <li>■ <b>vSphere Replication NFC 流量</b>。处理目标复制站点上的入站复制数据。</li> <li>■ <b>Virtual SAN</b>。在主机上启用 Virtual SAN 流量。属于 Virtual SAN 群集的每台主机都必须具有这样的 VMkernel 适配器。</li> </ul>

- 10 如果选择了 vMotion TCP/IP 或置备堆栈，在显示的警告对话框中单击**确定**。
- 如果实时迁移已启动，即使已在默认 TCP/IP 堆栈上禁止将涉及的 VMkernel 适配器用于 vMotion，该迁移也会成功完成。同样，在默认 TCP/IP 堆栈上包括为置备流量设置的 VMkernel 适配器也是一样。
- 11 （可选）在“IPv4 设置”页面上，选择用于获取 IP 地址的选项。

选项	描述
<b>自动获取 IPv4 设置</b>	使用 DHCP 获取 IP 设置。网络上必须存在 DHCP 服务器。
<b>使用静态 IPv4 设置</b>	<p>输入 VMkernel 适配器的 IPv4 IP 地址和子网掩码。</p> <p>IPv4 的 VMkernel 默认网关和 DNS 服务器地址将从选定的 TCP/IP 堆栈中获取。</p> <p>如果要为 VMkernel 适配器指定其他网关，请选中<b>替代此适配器的默认网关</b>复选框并输入网关地址。</p>

- 12 （可选）在“IPv6 设置”页面上，选择用于获取 IPv6 地址的选项。

选项	描述
<b>通过 DHCP 自动获取 IPv6 地址</b>	使用 DHCP 获取 IPv6 地址。网络上必须存在 DHCPv6 服务器。
<b>通过路由器播发自动获取 IPv6 地址</b>	<p>使用路由器播发获取 IPv6 地址。</p> <p>在 ESXi 6.5 和更高版本中，路由器播发在默认情况下处于启用状态，并且支持符合 RFC 4861 的 M 和 O 标记。</p>
<b>静态 IPv6 地址</b>	<p>a 单击<b>添加 IPv6 地址</b>以添加新的 IPv6 地址。</p> <p>b 输入 IPv6 地址和子网前缀长度，然后单击<b>确定</b>。</p> <p>c 要更改 VMkernel 默认网关，请单击<b>替代此适配器的默认网关</b>。</p> <p>IPv6 的 VMkernel 默认网关地址将从选定的 TCP/IP 堆栈中获取。</p>

- 13 检查“即将完成”页面上的设置选项，然后单击**完成**。
- 14 按照提示完成向导。

## 将虚拟机网络迁移到 vSphere Distributed Switch

要使用 Distributed Switch 管理虚拟机网络连接，请将虚拟机网络适配器迁移到交换机上有标记的网络。

### 前提条件

验证 Distributed Switch 上是否至少有一个适用于虚拟机网络连接的分布式端口组。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 从**操作**菜单中，选择**添加和管理主机**。
- 3 在**选择任务**中，选择**管理主机网络**，然后单击**下一步**。
- 4 在**选择主机**中，单击**连接的主机**，然后从与 Distributed Switch 关联的主机中进行选择。
- 5 单击**下一步**。
- 6 在**选择网络适配器任务**中，选择**迁移虚拟机网络**，然后单击**下一步**。
- 7 为 Distributed Switch 配置虚拟机网络适配器。
  - a 要将某个虚拟机的所有网络适配器连接到分布式端口组，请选择该虚拟机，或者选择单个网络适配器以仅连接该适配器。
  - b 单击**分配端口组**。
  - c 从列表中选择一個分布式端口组，然后单击**确定**。
- 8 单击**下一步**，然后单击**完成**。

## 使用主机作为模板为 vSphere Distributed Switch 创建统一的网络配置

如果您计划使多台主机拥有统一的网络配置，则可选择其中一台主机作为模板，并将其物理网卡和 VMkernel 适配器的配置应用到 Distributed Switch 上的其他主机。

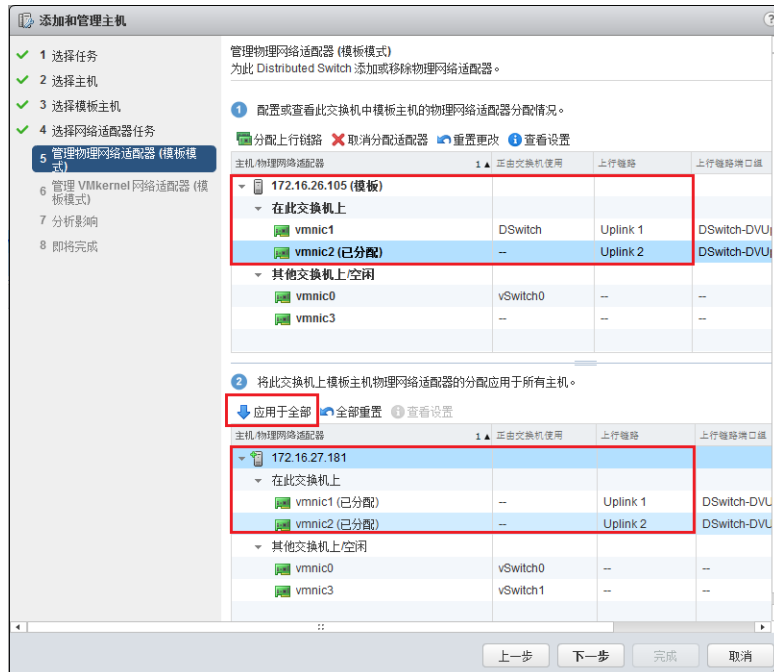
### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 从**操作**菜单中，选择**添加和管理主机**。
- 3 选择**管理主机网络**的任务，然后单击**下一步**。
- 4 选择要在 Distributed Switch 上添加或进行管理的主机。
- 5 在对话框的底部，选择**在多个主机上配置相同的网络设置**，然后单击**下一步**。
- 6 选择要用作模板的主机，然后单击**下一步**。
- 7 选择**网络适配器任务**，然后单击**下一步**。
- 8 在“管理物理网络适配器”和“管理 VMkernel 网络适配器”页面上，对模板主机进行所需的配置更改，然后针对所有其他主机单击**应用于全部**。
- 9 在“即将完成”页面上，单击**完成**。

### 示例：使用模板主机配置物理网卡

在添加和管理主机向导中使用模板主机模式将两台主机上的物理网卡同时连接到 vSphere Distributed Switch。在此向导的“管理物理网络适配器”页面上，将两个物理网卡分配给模板主机上的上行链路，然后单击**应用于全部**以便在其他主机上创建相同的配置。

图 3-4 使用模板主机在 vSphere Distributed Switch 上应用物理网卡配置



## 从 vSphere Distributed Switch 中移除主机

如果为主机配置了其他交换机，则可以从 vSphere Distributed Switch 中移除主机。

### 前提条件

- 确认将目标主机上的物理网卡迁移到其他交换机。
- 确认将主机上的 VMkernel 适配器迁移到其他交换机。
- 确认将虚拟机网络适配器迁移到其他交换机。

有关将网络适配器迁移到其他交换机的详细信息，请参见第 31 页，“在 vSphere Distributed Switch 上管理主机网络的任务”

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 从操作菜单中，选择添加和管理主机。
- 3 选择移除主机，然后单击下一步。
- 4 选择要移除的主机，然后单击下一步。
- 5 单击完成。

## 在主机代理交换机上管理网络连接

您可以更改与 vSphere Distributed Switch 关联的各个主机上的代理交换机的配置。您可以管理物理网卡、VMkernel 适配器和虚拟机网络适配器。

有关在主机代理交换机上设置 VMkernel 网络的详细信息，请参见第 34 页，“在 vSphere Distributed Switch 上创建 VMkernel 适配器”。

## 将主机上的网络适配器迁移到 vSphere Distributed Switch

对于与 Distributed Switch 关联的主机，可以将网络适配器从标准交换机迁移至 Distributed Switch。可以同时迁移物理网卡、VMkernel 适配器和虚拟机网络适配器。

如果迁移虚拟机网络适配器或 VMkernel 适配器，应确保目标分布式端口组至少有一个活动的上行链路，并且该链路与此主机上的物理网卡连接。或者，也可以同时迁移物理网卡、虚拟网络适配器和 VMkernel 适配器。

要迁移物理网卡，请确保标准交换机上的源端口组至少具有一个物理网卡以处理其流量。例如，如果要迁移分配给虚拟机网络的端口组的物理网卡，请确保该端口组至少连接到一个物理网卡。否则，标准交换机上同一 VLAN 中的虚拟机将相互连接，但与外部网络之间无连接。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开**网络**，然后选择**虚拟交换机**。
- 3 选择目标 Distributed Switch，然后单击**将物理网络适配器或虚拟网络适配器迁移到此 Distributed Switch**。
- 4 选择迁移网络适配器的任务，然后单击**下一步**。
- 5 配置物理网卡。
  - a 从**其他交换机上/空闲**列表中，选择一个物理网卡，然后单击**分配上行链路**。
  - b 选择一个上行链路，然后单击**确定**。
  - c 单击**下一步**。
- 6 配置 VMkernel 适配器。
  - a 选择一个适配器，然后单击**分配端口组**。
  - b 选择分布式端口组，然后单击**确定**。  
一次应将一个 VMkernel 适配器连接到一个分布式端口组。
  - c 单击**下一步**。
- 7 检查受新网络配置影响的服务。
  - a 如果某个服务中报告了重要的或严重的影响，请单击该服务并检查分析详细信息。  
例如，可能会报告 iSCSI 上由迁移 iSCSI VMkernel 适配器的分布式端口组上不正确的绑定和故障切换配置导致的重要影响。必须在分布式端口组的绑定和故障切换顺序中保留一个活动的上行链路，将备用列表保留为空，并将其余的上行链路移至未使用。
  - b 对受影响的服务造成的任何影响进行故障排除后，单击**下一步**。
- 8 配置虚拟机网络适配器。
  - a 选择一个虚拟机或虚拟机网络适配器，然后单击**分配端口组**。  
如果选择虚拟机，则应迁移虚拟机上的所有网络适配器。如果选择网络适配器，则只需迁移此网络适配器。
  - b 从列表中选择一個分布式端口组，然后单击**确定**。
  - c 单击**下一步**。
- 9 在“即将完成”页上，检查新网络配置并单击**完成**。

## 将主机上的 VMkernel 适配器迁移到 vSphere 标准交换机

如果主机与 Distributed Switch 关联，则可以将 VMkernel 适配器从 Distributed Switch 迁移到标准交换机。

有关在 vSphere Distributed Switch 上创建 VMkernel 适配器的详细信息，请参见第 34 页，“在 vSphere Distributed Switch 上创建 VMkernel 适配器”。

### 前提条件

确认目标标准交换机至少有一个物理网卡。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
  - 2 在配置选项卡上，展开网络，然后选择虚拟交换机。
  - 3 在列表中选择目标标准交换机。
  - 4 单击将 VMkernel 网络适配器迁移到选定交换机。
  - 5 在“选择 VMkernel 网络适配器”页面上，在列表中选择要迁移到标准交换机的虚拟网络适配器。
  - 6 在“配置设置”页面上，编辑网络适配器的网络标签和 VLAN ID。
  - 7 在“即将完成”页面上，检查迁移详细信息，然后单击完成。
- 单击上一步以编辑设置。

## 将主机的物理网卡分配给 vSphere Distributed Switch

您可以将与 Distributed Switch 关联的主机的物理网卡分配给主机代理交换机上的上行链路端口。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开网络，然后选择虚拟交换机。
- 3 从列表中选择 Distributed Switch。
- 4 单击管理已连接到选定交换机的物理网络适配器图标。
- 5 从列表选择一个空闲的上行链路，然后单击添加适配器。
- 6 选择物理网卡，然后单击确定。

## 从 vSphere Distributed Switch 移除物理网卡

您可以从 vSphere Distributed Switch 的上行链路中移除主机的物理网卡。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开网络，然后选择虚拟交换机。
- 3 选择 Distributed Switch。
- 4 单击管理已连接到选定交换机的物理网络适配器图标。
- 5 选择上行链路，然后单击移除选定适配器。
- 6 单击确定。

## 下一步

从活动虚拟机中移除物理网卡时，可能会看到 vSphere Web Client 中报告已移除的网卡。请参见第 40 页，[“从活动虚拟机中移除网卡”](#)。

## 从活动虚拟机中移除网卡

从活动虚拟机中移除网卡时，可能仍会看到 vSphere Web Client 中已移除的网卡。

### 从未安装客户机操作系统的活动虚拟机中移除网卡

不能从未安装任何操作系统的活动虚拟机中移除网卡。

vSphere Web Client 可能会报告网卡已被移除，但是您看到它仍然附加在虚拟机上。

### 从已安装客户机操作系统的活动虚拟机中移除网卡

可以从活动虚拟机中移除网卡，但有时这可能不会报告给 vSphere Web Client。如果您单击虚拟机的**编辑设置**，可能会看到被移除的网卡仍被列出，即便移除任务已完成。虚拟机的“编辑设置”对话框不会立即显示移除的网卡。

如果虚拟机的客户机操作系统不支持热移除网卡，则您可能仍会看到网卡附加在虚拟机上。

## 分布式端口组

分布式端口组为 vSphere Distributed Switch 上的每个成员端口指定端口配置选项。分布式端口组可定义连接到网络的方式。

## 添加分布式端口组

将分布式端口组添加到 vSphere Distributed Switch 以为虚拟机创建 Distributed Switch 网络并关联 VMkernel 适配器。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 右键单击 Distributed Switch，然后选择**分布式端口组 > 新建分布式端口组**。
- 3 在“选择名称和位置”页面上，键入新分布式端口组的名称，或接受生成的名称，然后单击**下一步**。
- 4 在“配置设置”页面上，设置新分布式端口组的常规属性，然后单击**下一步**。

设置	描述
<b>端口绑定</b>	选择将端口分配到与该分布式端口组相连的虚拟机的时间。 <ul style="list-style-type: none"> <li>■ <b>静态绑定</b>：虚拟机连接到分布式端口组后，为该虚拟机分配一个端口。</li> <li>■ <b>动态绑定</b>：虚拟机连接到分布式端口组后首次打开该虚拟机的电源时，为该虚拟机分配一个端口。自 ESXi 5.0 开始，已弃用动态绑定。</li> <li>■ <b>极短 - 无绑定</b>：无端口绑定。此外，连接到主机时，还可以将虚拟机分配给带有极短端口绑定的分布式端口组。</li> </ul>
<b>端口分配</b>	<ul style="list-style-type: none"> <li>■ <b>弹性</b>：默认端口数为 8 个。分配了所有端口后，将创建一组新的 8 个端口。这是默认行为。</li> <li>■ <b>固定</b>：默认端口数设置为 8 个。分配了所有端口后，不会创建额外端口。</li> </ul>
<b>端口数</b>	输入分布式端口组上的端口数。
<b>网络资源池</b>	使用下拉菜单将新的分布式端口组分配给用户定义的网络资源池。如果尚未创建网络资源池，则此菜单为空。



设置	描述
<b>VLAN</b>	<p>使用 <b>VLAN 类型</b> 下拉菜单选择 VLAN 选项：</p> <ul style="list-style-type: none"> <li>■ <b>无</b>：不使用 VLAN。</li> <li>■ <b>VLAN</b>：在 <b>VLAN ID</b> 字段中，输入一个介于 1 和 4094 之间的数字。</li> <li>■ <b>VLAN 中继</b>：输入 VLAN 中继范围。</li> <li>■ <b>专用 VLAN</b>：选择专用 VLAN 条目。如果未创建任何专用 VLAN，则此菜单为空。</li> </ul>
<b>高级</b>	选中该复选框可为新的分布式端口组自定义策略配置。

- 5 （可选）在“安全”页面上，编辑安全异常，然后单击**下一步**。

设置	描述
<b>混杂模式</b>	<ul style="list-style-type: none"> <li>■ <b>拒绝</b>。在客户机操作系统中将适配器置于混杂模式不会导致接收其他虚拟机的帧。</li> <li>■ <b>接受</b>。如果在客户机操作系统中将适配器置于混杂模式，则交换机将允许客户机适配器按照该适配器所连接到的端口上的活动 VLAN 策略接收在交换机上传递的所有帧。</li> </ul> <p>防火墙、端口扫描程序、入侵检测系统等需要在混杂模式下运行。</p>
<b>MAC 地址更改</b>	<ul style="list-style-type: none"> <li>■ <b>拒绝</b>。如果将此选项设置为<b>拒绝</b>，并且客户机操作系统将适配器的 MAC 地址更改为不同于 .vmx 配置文件中的地址，则交换机会丢弃所有到虚拟机适配器的入站帧。</li> <li>■ <b>接受</b>。如果客户机操作系统更改了网络适配器的 MAC 地址，则适配器会将帧接收到其新地址。</li> </ul> <p>如果客户机操作系统恢复 MAC 地址，则虚拟机将再次收到帧。</p>
<b>伪信号</b>	<ul style="list-style-type: none"> <li>■ <b>拒绝</b>。如果任何出站帧的源 MAC 地址不同于 .vmx 配置文件中的源 MAC 地址，则交换机会丢弃该出站帧。</li> <li>■ <b>接受</b>。交换机不执行筛选，允许所有出站帧通过。</li> </ul>

- 6 （可选）在“流量调整”页面上，启用或禁用“输入流量调整”或“输出流量调整”，然后单击**下一步**。

设置	描述
<b>状态</b>	如果启用 <b>输入流量调整</b> 或 <b>输出流量调整</b> ，将为与该特定端口组关联的每个虚拟适配器设置网络连接带宽分配量的限制。如果禁用策略，则在默认情况下，服务将能够自由、顺畅地连接物理网络。
<b>平均带宽</b>	规定某段时间内允许通过端口的平均每秒位数。这是允许的平均负载。
<b>峰值带宽</b>	当端口发送和接收流量突发时，每秒钟允许通过该端口的最大位数。此数值是端口使用额外突发时所能使用的最大带宽。
<b>突发大小</b>	突发中所允许的最大字节数。如果设置了此参数，则在端口没有使用为其分配的所有带宽时可能会获取额外的突发。当端口所需带宽大于 <b>平均带宽</b> 所指定的值时，如果有额外突发可用，则可能会临时以更高的速度传输数据。此参数为额外突发中可累积的最大字节数，使数据能以更高速度传输。

- 7 （可选）在“绑定和故障切换”页面上，编辑设置，然后单击**下一步**。

设置	描述
<b>负载平衡</b>	<p>指定如何选择上行链路。</p> <ul style="list-style-type: none"> <li>■ <b>基于源虚拟端口的路由。</b>根据流量进入 Distributed Switch 所经过的虚拟端口选择上行链路。</li> <li>■ <b>基于 IP 哈希的路由。</b>根据每个数据包的源和目标 IP 地址哈希值选择上行链路。对于非 IP 数据包，偏移量中的任何值都将用于计算哈希值。</li> <li>■ <b>基于源 MAC 哈希的路由。</b>根据源以太网哈希值选择上行链路。</li> <li>■ <b>基于物理网卡负载的路由。</b>根据物理网卡的当前负载选择上行链路。</li> <li>■ <b>使用明确故障切换顺序。</b>始终使用“活动适配器”列表中位于最前列的符合故障切换检测标准的上行链路。</li> </ul> <p><b>注意</b> 基于 IP 的绑定要求为物理交换机配置以太网通道。对于所有其他选项，禁用以太网通道。</p>
<b>网络故障检测</b>	<p>指定用于故障切换检测的方法。</p> <ul style="list-style-type: none"> <li>■ <b>仅链路状态。</b>仅依靠网络适配器提供的链路状态。该选项可检测故障（如拔掉线缆和物理交换机电源故障），但无法检测配置错误（如物理交换机端口受跨树阻止、配置到了错误的 VLAN 中或者拔掉了物理交换机另一端的线缆）。</li> <li>■ <b>信标探测。</b>发出并侦听组中所有网卡上的信标探测，使用此信息并结合链路状态来确定链接故障。该选项可检测上述许多仅通过链路状态无法检测到的故障。</li> </ul> <p><b>注意</b> 不要使用包含 IP 哈希负载平衡的信标探测。</p>
<b>通知交换机</b>	<p>选择<b>是</b>或<b>否</b>指定发生故障切换时是否通知交换机。如果选择<b>是</b>，则每当虚拟网卡连接到 Distributed Switch 或虚拟网卡的流量因故障切换事件而由网卡组中的其他物理网卡路由时，都将通过网络发送通知以更新物理交换机的查看表。几乎在所有情况下，为了使出现故障切换以及通过 vMotion 迁移时的延迟最短，最好使用此过程。</p> <p><b>注意</b> 当使用端口组的虚拟机正在以单播模式使用 Microsoft 网络负载平衡时，请勿使用此选项。以多播模式运行网络负载平衡时不存在此问题。</p>
<b>故障恢复</b>	<p>选择<b>是</b>或<b>否</b>以禁用或启用故障恢复。</p> <p>此选项确定物理适配器从故障恢复后如何返回到活动的任务。如果故障恢复设置为<b>是</b>（默认值），则适配器将在恢复后立即返回到活动任务，并取代接替其位置的备用适配器（如果有）。如果故障恢复设置为<b>否</b>，那么，即使发生故障的适配器已经恢复，它仍将保持非活动状态，直到当前处于活动状态的另一个适配器发生故障并要求替换为止。</p>
<b>故障切换顺序</b>	<p>指定如何分布上行链路的工作负载。要使用一部分上行链路，保留另一部分来应对使用的上行链路发生故障时的紧急情况，请通过将它们移到不同的组来设置此条件：</p> <ul style="list-style-type: none"> <li>■ <b>活动上行链路。</b>当网络适配器连接正常且处于活动状态时，继续使用此上行链路。</li> <li>■ <b>备用上行链路。</b>如果其中一个活动适配器的连接中断，则使用此上行链路。</li> <li>■ <b>未使用的上行链路。</b>不使用此上行链路。</li> </ul> <p><b>注意</b> 当使用 IP 哈希负载平衡时，不要配置待机上行链路。</p>

- 8 （可选）在“监控”页面上，启用或禁用 NetFlow，然后单击**下一步**。

设置	描述
<b>已禁用</b>	在分布式端口组上禁用了 NetFlow。
<b>已启用</b>	在分布式端口组上启用了 NetFlow。可以在 vSphere Distributed Switch 级别配置 NetFlow 设置。

- 9 （可选）在“其他”页面上，选择**是**或**否**，然后单击**下一步**。

选择**是**可关闭端口组中的所有端口。该操作可能中断正在使用这些端口的主机或虚拟机的正常网络操作。

- 10 （可选）在“编辑其他设置”页面上，添加对端口组的描述并设置每个端口的任何策略替代项，然后单击下一步。
- 11 在“即将完成”页面上，检查设置，然后单击**完成**。  
单击**上一步**按钮可更改任何设置。

## 编辑常规分布式端口组设置

可以编辑常规分布式端口组设置，例如分布式端口组名称、端口设置和网络资源池。

### 步骤

- 1 在 vSphere Web Client 中找到分布式端口组。
  - a 选择 Distributed Switch，然后单击**网络**选项卡。
  - b 单击**分布式端口组**。
- 2 右键单击分布式端口组，然后选择**编辑设置**。
- 3 选择**常规**以编辑下面的分布式端口组设置。

选项	描述
<b>名称</b>	分布式端口组的名称。您可在文本字段中编辑名称。
<b>端口绑定</b>	选择将端口分配到与该分布式端口组相连的虚拟机的时间。 <ul style="list-style-type: none"> <li>■ <b>静态绑定</b>：虚拟机连接到分布式端口组后，为该虚拟机分配一个端口。</li> <li>■ <b>动态绑定</b>：在虚拟机连接到分布式端口组后首次打开该虚拟机的电源时，为该虚拟机分配一个端口。自 ESXi 5.0 开始，已弃用动态绑定。</li> <li>■ <b>极短</b>：无端口绑定。此外，连接到主机时，还可以将虚拟机分配给带有极短端口绑定的分布式端口组。</li> </ul>
<b>端口分配</b>	<ul style="list-style-type: none"> <li>■ <b>弹性</b>：默认端口数设置为八个。分配了所有端口后，将创建一组新的 8 个端口。这是默认行为。</li> <li>■ <b>固定</b>：默认端口数设置为 8 个。分配了所有端口后，不会创建额外端口。</li> </ul>
<b>端口数</b>	输入分布式端口组上的端口数。
<b>网络资源池</b>	使用下拉菜单将新的分布式端口组分配给用户定义的网络资源池。如果尚未创建网络资源池，则此菜单为空。
<b>描述</b>	请在描述字段中输入有关分布式端口组的信息。

- 4 单击**确定**。

## 在端口级别配置替代网络策略

要对分布式端口应用不同的策略，您可以配置在端口组级别设置的每个端口替代策略。当分布式端口与虚拟机断开连接时，您也可以启用重置在每个端口级别设置的任何配置。

### 步骤

- 1 在 vSphere Web Client 中找到分布式端口组。
  - a 选择 Distributed Switch，然后单击**网络**选项卡。
  - b 单击**分布式端口组**。
- 2 右键单击分布式端口组，然后选择**编辑设置**。

- 3 选择**高级**页面。

选项	描述
<b>断开连接时配置重置</b>	从下拉菜单中启用或禁用断开连接时重置。 当分布式端口与虚拟机断开连接时，分布式端口的配置重置为分布式端口组设置。每个端口的替代都会被丢弃。
<b>替代端口策略</b>	选择要在每个端口级别替代的分布式端口组策略。

- 4 （可选）使用策略页面设置每个端口策略的替代。
- 5 单击**确定**。

## 移除分布式端口组

当您不再需要相应的有标记网络时，请移除分布式端口组，以便为虚拟机或 VMkernel 网络提供连接及配置连接设置。

### 前提条件

- 验证已将连接到相应有标记网络的所有虚拟机迁移到其他有标记网络。
- 验证已将连接到分布式端口组的所有 VMkernel 适配器迁移到其他端口组，或已将其删除。

### 步骤

- 1 在 vSphere Web Client 中找到分布式端口组。
  - a 选择 Distributed Switch，然后单击**网络**选项卡。
  - b 单击**分布式端口组**。
- 2 选择分布式端口组。
- 3 在**操作**菜单中，选择**删除**。

## 使用分布式端口

分布式端口是连接到 VMkernel 或虚拟机的网络适配器的 vSphere Distributed Switch 上的一个端口。

默认分布式端口配置是由分布式端口组设置确定的，但可以替代各个分布式端口的某些设置。

## 监控分布式端口的状况

vSphere 可以监控分布式端口并提供关于每个端口的当前状况和运行时统计信息。

### 步骤

- 1 在 vSphere Web Client 中找到分布式端口组。
  - a 选择 Distributed Switch，然后单击**网络**选项卡。
  - b 单击**分布式端口组**。
- 2 双击分布式端口组。
- 3 单击**端口**选项卡，然后从列表中选择端口。

- 4 单击**开始监控端口状况**图标。
- 分布式端口组的端口表将显示每个分布式端口的运行时统计信息。
- 状况**列会显示每个分布式端口的当前状况。

选项	描述
已连接	此分布式端口的链接已打开。
已断开	此分布式端口的链接已关闭。
已阻止	此分布式端口已阻止。
--	当前此分布式端口的状况不可用。

配置分布式端口设置

可以更改分布式端口的常规设置，如端口名称和描述。

步骤

- 在 vSphere Web Client 中找到分布式端口组。
  - 选择 Distributed Switch，然后单击**网络**选项卡。
  - 单击**分布式端口组**。
- 在列表中双击一个分布式端口组。
- 单击**端口**选项卡，然后从表中选择分布式端口。

有关分布式端口的信息会显示在屏幕底部。
- 单击**编辑分布式端口设置**图标。
- 在“属性”页面和策略页面上，编辑有关分布式端口的信息，然后单击**确定**。

如果不允许替代项，则策略选项将处于禁用状态。

您可以通过更改分布式端口组的**高级**设置允许端口级别的替代项。请参见第 43 页，“在端口级别配置替代网络策略”。

在 vSphere Distributed Switch 上配置虚拟机网络连接

可以通过配置单个虚拟机网卡，或通过从 vSphere Distributed Switch 自身迁移多组虚拟机，将虚拟机连接到 vSphere Distributed Switch。

通过将虚拟机关联的虚拟网络适配器连接到分布式端口组，可以将虚拟机连接到 vSphere Distributed Switch。对于单个虚拟机，可以通过修改虚拟机的网络适配器配置来完成；对于虚拟机组，可以通过将虚拟机从现有虚拟网络迁移到 vSphere Distributed Switch 来完成。

将虚拟机迁入或迁出 vSphere Distributed Switch

除了在单个虚拟机级别将虚拟机连接到 Distributed Switch 以外，还可以在 vSphere Distributed Switch 网络和 vSphere 标准交换机网络之间迁移一组虚拟机。

步骤

- 在 vSphere Web Client 中，导航到数据中心。
- 在导航器中右键单击数据中心，然后选择**将虚拟机迁移到其他网络**。

- 3 选择源网络。
  - 选择**特定网络**并使用**浏览**按钮选择一个特定源网络。
  - 选择**无网络**可迁移未连接到任何其他网络的所有虚拟机网络适配器。
- 4 使用**浏览**选择一个目标网络，然后单击**下一步**。
- 5 从列表中选择要从源网络迁移到目标网络的虚拟机，然后单击**下一步**。
- 6 检查选择内容，然后单击**完成**。  
单击**上一步**以编辑任何选择。

## 将单个虚拟机连接到分布式端口组

通过修改虚拟机的网卡配置，可将单个虚拟机连接到 vSphere Distributed Switch。

### 步骤

- 1 在 vSphere Web Client 中找到虚拟机。
  - a 选择数据中心、文件夹、群集、资源池或主机，然后单击**虚拟机**选项卡。
  - b 单击**虚拟机**，然后从列表中双击虚拟机。
- 2 在虚拟机的**配置**选项卡上，展开**设置**，然后选择**虚拟机硬件**。
- 3 单击**编辑**。
- 4 展开**网络适配器**部分，并从**网络适配器**下拉菜单选择**显示更多网络**。
- 5 在“选择网络”对话框中，选择一个分布式端口组，然后单击**确定**。
- 6 单击**确定**。

## vSphere Web Client 中的 vSphere Distributed Switch 拓扑图

vSphere Web Client 中的 vSphere Distributed Switch 拓扑图显示了交换机中虚拟机适配器、VMkernel 适配器和物理适配器的结构。

您可以检查端口组中排列的组件（其流量由交换机进行处理）以及这些组件之间的连接。此拓扑图显示了有关将虚拟适配器连接到外部网络的物理适配器的信息。

您可以查看在整个 Distributed Switch 上以及在加入此 Distributed Switch 的每台主机上运行的组件。

有关可从 vSphere Distributed Switch 拓扑图执行的操作，请观看视频。



使用 VDS 拓扑图处理虚拟网络连接

([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_using\\_vds\\_topology\\_diagram](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_using_vds_topology_diagram))

### 中心拓扑图

您可使用交换机的中心拓扑图找到并编辑与多个主机关联的分布式端口组和上行链路组的设置。可以启动将虚拟机适配器从端口组迁移到相同或其他交换机上的目标位置的操作。此外，还可以使用添加和管理主机向导重新组织交换机上的主机及其网络。

### 主机代理交换机的拓扑图

主机代理交换机的拓扑图显示了连接到主机上的交换机端口的适配器。您可以编辑 VMkernel 适配器和物理适配器的设置。

## 图表筛选器

您可使用图表筛选器来限制拓扑图中显示的信息。默认筛选器将限制拓扑图只显示 32 个端口组、32 台主机和 1024 台虚拟机。

不使用任何筛选器或应用自定义筛选器可更改图表的范围。通过使用自定义筛选器，您可以查看仅与某一组虚拟机、特定主机上的某一组端口组或某一端口组相关的信息。您可以通过 Distributed Switch 的中心拓扑图创建筛选器。

## 查看 vSphere Distributed Switch 的拓扑

在 vCenter Server 中检查跨主机连接 Distributed Switch 的组件的组织。

### 步骤

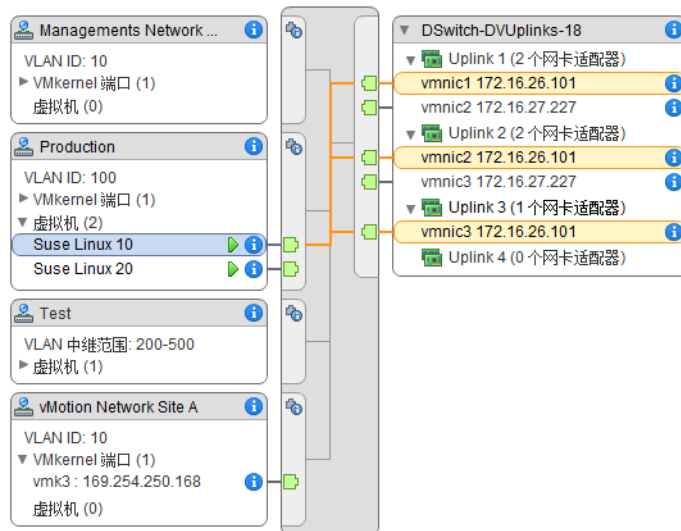
- 1 导航至 vSphere Web Client 中的 vSphere Distributed Switch。
- 2 在配置选项卡上，展开设置，然后选择拓扑。

默认情况下，此图最多显示 32 个分布式端口组、32 个主机和 1024 个虚拟机。

### 示例：将 VMkernel 和虚拟机连接网络的 Distributed Switch 图

在您的虚拟环境中，vSphere Distributed Switch 为 vSphere vMotion 和管理网络处理 VMkernel 适配器以及分组的虚拟机。可以使用中心拓扑图来检查虚拟机或 VMkernel 适配器是否连接到外部网络，并确定承载数据的物理适配器。

图 3-5 处理 VMkernel 和虚拟机网络连接的 Distributed Switch 的拓扑图



### 下一步

可以执行 Distributed Switch 的拓扑中的下列常见任务：

- 使用筛选器仅查看特定主机上选定的端口组、选择的虚拟机或端口的网络连接组件。
- 使用迁移虚拟机网络向导在主机和端口组之间查找、配置和迁移虚拟机网络连接组件。
- 使用迁移虚拟机网络向导检测未向其分配网络的虚拟机适配器，并将这些虚拟机适配器移至选定的端口组。
- 使用添加和管理主机向导处理多个主机上的网络连接组件。

- 查看承载与选定的虚拟机适配器或 VMkernel 适配器关联的流量的物理网卡或网卡组。  
通过此方法，还可以查看驻留选定 VMkernel 适配器的主机。选择适配器，跟踪到关联的物理网卡的路由，并查看位于网卡旁边的 IP 地址或域名称。
- 确定端口组的 VLAN 模式和 ID。有关 VLAN 模式的信息，请参见第 115 页，“VLAN 配置”。

## 查看主机代理交换机的拓扑

检查并重新组织 vSphere Distributed Switch 在主机上处理的 VMkernel 和虚拟机的网络连接。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开网络，然后选择虚拟交换机。
- 3 从列表中选择 Distributed Switch。

主机代理交换机的拓扑会显示在列表下方。



## 设置 VMkernel 网络

---

可设置 VMkernel 适配器向主机提供网络连接并接受 vMotion、IP 存储器、Fault Tolerance 日志记录、Virtual SAN 等服务的系统流量。

- [VMkernel 网络层](#)第 50 页，  
VMkernel 网络层提供与主机的连接，并处理 vSphere vMotion、IP 存储、Fault Tolerance、Virtual SAN 等其他服务的标准系统流量。您还可以在源和目标 vSphere Replication 主机上创建 VMkernel 适配器，以隔离复制数据流量。
- [查看有关主机上的 VMkernel 适配器的信息](#)第 51 页，  
您可以查看每个 VMkernel 适配器的已分配的服务、关联的交换机、端口设置、IP 设置、TCP/IP 堆栈、VLAN ID 和策略。
- [在 vSphere 标准交换机上创建 VMkernel 适配器](#)第 52 页，  
在 vSphere 标准交换机上创建 VMkernel 网络适配器，可为主机提供网络连接并处理 vSphere vMotion、IP 存储、Fault Tolerance 日志记录、Virtual SAN 等服务的系统流量。您还可以在源和目标 vSphere Replication 主机上创建 VMkernel 适配器，以隔离复制数据流量。将 VMkernel 适配器专用于一种流量类型。
- [在与 vSphere Distributed Switch 关联的主机上创建 VMkernel 适配器](#)第 54 页，  
在与 Distributed Switch 关联的主机上创建 VMkernel 适配器，可向主机提供网络连接并处理 vSphere vMotion、IP 存储器、Fault Tolerance 日志记录、Virtual SAN 等服务的流量。您可为 vSphere 标准交换机和 vSphere Distributed Switch 上的标准系统流量设置 VMkernel 适配器。
- [编辑 VMkernel 适配器配置](#)第 55 页，  
您可能需要更改 VMkernel 适配器所支持的流量类型或者 IPv4 或 IPv6 地址的获取方式。
- [替代 VMkernel 适配器的默认网关](#)第 56 页，  
可能需要替代 VMkernel 适配器的默认网关，以便为 vMotion、Fault Tolerance 日志记录和 Virtual SAN 等服务提供不同的网关。
- [使用 ESXCLI 配置 VMkernel 适配器网关](#)第 57 页，  
可替代 VMkernel 适配器的默认网络，以便为 vMotion、Fault Tolerance 日志记录和 Virtual SAN 之类的服务提供不同的网关。
- [查看主机上的 TCP/IP 堆栈配置](#)第 57 页，  
您可查看主机上 TCP/IP 堆栈的 DNS 和路由配置。还可查看 IPv4 和 IPv6 路由表、拥堵控制算法和允许的最大连接数。
- [更改主机上的 TCP/IP 堆栈配置](#)第 57 页，  
您可更改主机上 TCP/IP 堆栈的 DNS 和默认路由配置。还可更改自定义 TCP/IP 堆栈的拥堵控制算法、最大连接数和名称。

- [创建自定义 TCP/IP 堆栈](#)第 58 页，  
可以在主机上创建一个自定义 TCP/IP 堆栈通过自定义应用程序转发网络流量。
- [移除 VMkernel 适配器](#)第 58 页，  
不再需要 VMkernel 适配器时，请从 vSphere Distributed Switch 或标准交换机中移除该适配器。确保在主机上至少保留一个用于管理流量的 VMkernel 适配器，以保持网络连接不中断。

## VMkernel 网络层

VMkernel 网络层提供与主机的连接，并处理 vSphere vMotion、IP 存储、Fault Tolerance、Virtual SAN 等其他服务的标准系统流量。您还可以在源和目标 vSphere Replication 主机上创建 VMkernel 适配器，以隔离复制数据流量。

### VMkernel 级别的 TCP/IP 堆栈

<b>默认 TCP/IP 堆栈</b>	为 vCenter Server 与 ESXi 主机之间的管理流量和 vMotion、IP 存储、Fault Tolerance 等服务的系统流量提供网络支持。
<b>vMotion TCP/IP 堆栈</b>	为虚拟机实时迁移的流量提供支持。使用 vMotion TCP/IP 可以为 vMotion 流量提供更好的隔离。在 vMotion TCP/IP 堆栈上创建 VMkernel 适配器后，只能将此堆栈用于此主机上的 vMotion。默认 TCP/IP 堆栈上的 VMkernel 适配器对于 vMotion 服务均处于禁用状态。如果某个实时迁移使用默认 TCP/IP 堆栈，而您却使用 vMotion TCP/IP 堆栈配置了 VMkernel 适配器时，迁移会成功完成。但是，默认 TCP/IP 堆栈上的 VMkernel 适配器对于未来 vMotion 会话将处于禁用状态。
<b>置备 TCP/IP 堆栈</b>	为虚拟机冷迁移、克隆和快照生成的流量提供支持。在远距离 vMotion 期间，可以使用置备 TCP/IP 处理网络文件复制 (Network File Copy, NFC) 流量。NFC 为 vSphere 提供文件特定的 FTP 服务。ESXi 使用 NFC 在数据存储之间复制和移动数据。使用置备 TCP/IP 堆栈配置的 VMkernel 适配器会处理在长途 vMotion 中克隆已迁移虚拟机的虚拟磁盘的流量。置备 TCP/IP 堆栈可用于隔离单独网关上克隆操作的流量。使用置备 TCP/IP 堆栈配置 VMkernel 适配器后，默认 TCP/IP 堆栈上的所有适配器对于置备流量均处于禁用状态。
<b>自定义 TCP/IP 堆栈</b>	您可以添加 VMkernel 级别的自定义 TCP/IP 堆栈，并通过自定义应用程序处理网络流量。

### 确保系统流量安全

采取适当的安全措施来防止对 vSphere 环境中的管理和系统的未授权访问。例如，在仅包括参与迁移的 ESXi 主机的单独网络中隔离 vMotion 流量。在只有网络和安全管理员能够访问的网络中隔离管理流量。有关详细信息，请参见《vSphere 安全性》和《vSphere 安装和设置》。

## 系统流量类型

专门针对每种流量类型使用单独的 VMkernel 适配器。对于 Distributed Switch，专门针对每个 VMkernel 适配器使用单独的分布式端口组。

### 管理流量

承载着 ESXi 主机和 vCenter Server 以及主机对主机 High Availability 流量的配置和管理通信。默认情况下，在安装 ESXi 软件时，会在主机上为管理流量创建 vSphere 标准交换机以及 VMkernel 适配器。为提供冗余，可以将两个或更多个物理网卡连接到 VMkernel 适配器以进行流量管理。

### vMotion 流量

容纳 vMotion。源主机和目标主机上都需要一个用于 vMotion 的 VMkernel 适配器。将用于 vMotion 的 VMkernel 适配器配置为仅处理 vMotion 流量。为了实现更好的性能，可以配置多网卡 vMotion。要拥有多网卡 vMotion，可以将两个或更多端口组专门用于 vMotion 流量，每个端口组必须分别有一个与其关联的 vMotion VMkernel 适配器。然后将一个或多个物理网卡连接到每个端口组。这样，有多个物理网卡用于 vMotion，从而可以增加带宽。

---

**注意** vMotion 网络流量未加密。应置备安全专用网络，仅供 vMotion 使用。

---

### 置备流量

处理虚拟机冷迁移、克隆和快照生成传输的数据。

### IP 存储流量和发现

处理使用标准 TCP/IP 网络和取决于 VMkernel 网络的存储类型的连接。此类存储类型包括软件 iSCSI、从属硬件 iSCSI 以及 NFS。如果 iSCSI 具有两个或多个物理网卡，则可以配置 iSCSI 多路径。ESXi 主机支持 NFS 3 和 4.1。要配置软件以太网光纤通道 (FCoE) 适配器，必须使用专用的 VMkernel 适配器。软件 FCoE 使用 Cisco 发现协议 (CDP) VMkernel 模块通过数据中心桥接交换 (DCBX) 协议传递配置信息。

### Fault Tolerance 流量

处理主容错虚拟机通过 VMkernel 网络层向辅助容错虚拟机发送的数据。vSphere HA 群集中的每台主机上都需要用于 Fault Tolerance 日志记录的单独 VMkernel 适配器。

### vSphere Replication 流量

处理源 ESXi 主机传输至 vSphere Replication 服务器的出站复制数据。在源站点上使用一个专用的 VMkernel 适配器，以隔离出站复制流量。

### vSphere Replication NFC 流量

处理目标复制站点上的进站复制数据。

### Virtual SAN 流量

加入 Virtual SAN 群集的每台主机都必须有用于处理 Virtual SAN 流量的 VMkernel 适配器。

## 查看有关主机上的 VMkernel 适配器的信息

您可以查看每个 VMkernel 适配器的已分配的服务、关联的交换机、端口设置、IP 设置、TCP/IP 堆栈、VLAN ID 和策略。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 单击**配置**选项卡，然后展开**网络**菜单。
- 3 要查看有关主机上所有 VMkernel 适配器的信息，请选择 **VMkernel 适配器**。

- 从 VMkernel 适配器列表选择一个适配器以查看其设置。

选项卡	描述
全部	显示有关 VMkernel 适配器的所有配置信息。此信息包括端口和网卡设置、IPv4 和 IPv6 设置、流量调整、绑定和故障切换以及安全策略。
属性	显示 VMkernel 适配器的端口属性和网卡设置。端口属性包括与该适配器关联的端口组（网络标签）、VLAN ID 和已启用的服务。网卡设置包括 MAC 地址和已配置的 MTU 大小。
IP 设置	显示 VMkernel 适配器的所有 IPv4 和 IPv6 设置。如果未在主机上启用 IPv6，则不会显示 IPv6 信息。
策略	显示已配置的流量调整、绑定和故障切换以及安全策略，这些策略将应用于 VMkernel 适配器所连接到的端口组。

## 在 vSphere 标准交换机上创建 VMkernel 适配器

在 vSphere 标准交换机上创建 VMkernel 网络适配器，可为主机提供网络连接并处理 vSphere vMotion、IP 存储、Fault Tolerance 日志记录、Virtual SAN 等服务的系统流量。您还可以在源和目标 vSphere Replication 主机上创建 VMkernel 适配器，以隔离复制数据流量。将 VMkernel 适配器专用于一种流量类型。

### 步骤

- 在 vSphere Web Client 中，导航到主机。
- 在配置选项卡上，展开网络，然后选择 VMkernel 适配器。
- 单击添加主机网络。
- 在“选择连接类型”页面上，选择 VMkernel 网络适配器，然后单击下一步。
- 在“选择目标设备”页面上，选择现有标准交换机或选择新建标准交换机。
- （可选）在“创建标准交换机”页面上，为交换机分配物理网卡。

可以创建不带物理网卡的标准交换机，稍后再配置网卡。在此期间没有物理网卡连接到主机，从而主机无法通过网络连接到物理网络上的其他主机。主机上的各个虚拟机能够互相通信。

- 单击添加适配器，然后根据需要选择物理网卡数。
  - 使用上下箭头配置活动网卡和备用网卡。
- 在“端口属性”页面上，配置 VMkernel 适配器的设置。

选项	描述
网络标签	请为该标签键入一个值以表示 VMkernel 适配器的流量类型，例如 <b>Management traffic</b> 或 <b>vMotion</b> 。
VLAN ID	设置 VLAN ID 以标识 VMkernel 适配器的网络流量将使用的 VLAN。
IP 设置	选择 IPv4、IPv6 或同时选择两者。 <b>注意</b> 在未启用 IPv6 的主机上，IPv6 选项不会显示。

选项	描述
<b>TCP/IP 堆栈</b>	在列表选择一个 TCP/IP 堆栈。为 VMkernel 适配器设置 TCP/IP 堆栈后，以后便无法再更改该堆栈。如果选择 vMotion 或置备 TCP/IP 堆栈，您将只能使用此堆栈来处理主机上的 vMotion 或置备流量。默认 TCP/IP 堆栈上所有适用于 vMotion 的 VMkernel 适配器将被禁止用于未来的 vMotion 会话。如果使用置备 TCP/IP 堆栈，将对包括置备流量的操作（如虚拟机冷迁移、克隆和快照生成）禁用默认 TCP/IP 堆栈上的 VMkernel 适配器。
<b>启用服务</b>	<p>可以为主机上的默认 TCP/IP 堆栈启用服务。请从以下可用服务中选择：</p> <ul style="list-style-type: none"> <li>■ <b>vMotion 流量</b>。允许 VMkernel 适配器向另一台主机播发声明，自己就是发送 vMotion 流量所应使用的网络连接。如果默认 TCP/IP 堆栈上的任何 VMkernel 适配器均未启用 vMotion 服务，或任何适配器均未使用 vMotion TCP/IP 堆栈，则无法使用 vMotion 迁移到所选主机。</li> <li>■ <b>置备流量</b>。处理为用于虚拟机冷迁移、克隆和快照创建而传输的数据。</li> <li>■ <b>Fault Tolerance 流量</b>。在主机上启用 Fault Tolerance 日志记录。对每台主机的 FT 流量只能使用一个 VMkernel 适配器。</li> <li>■ <b>管理流量</b>。为主机和 vCenter Server 启用管理流量。通常，安装 ESXi 软件后，主机将创建这样的 VMkernel 适配器。可以为主机上的管理流量创建其他 VMkernel 适配器以提供冗余。</li> <li>■ <b>vSphere Replication 流量</b>。处理源 ESXi 主机发送至 vSphere Replication 服务器的出站复制数据。</li> <li>■ <b>vSphere Replication NFC 流量</b>。处理目标复制站点上的入站复制数据。</li> <li>■ <b>Virtual SAN</b>。在主机上启用 Virtual SAN 流量。属于 Virtual SAN 群集的每台主机都必须具有这样的 VMkernel 适配器。</li> </ul>

- 8 如果选择了 vMotion TCP/IP 或置备堆栈，在显示的警告对话框中单击**确定**。
- 如果实时迁移已启动，即使已在默认 TCP/IP 堆栈上禁止将涉及的 VMkernel 适配器用于 vMotion，该迁移也会成功完成。同样，在默认 TCP/IP 堆栈上包括为置备流量设置的 VMkernel 适配器也是一样。
- 9 （可选）在“IPv4 设置”页面上，选择用于获取 IP 地址的选项。

选项	描述
<b>自动获取 IPv4 设置</b>	使用 DHCP 获取 IP 设置。网络上必须存在 DHCP 服务器。
<b>使用静态 IPv4 设置</b>	<p>输入 VMkernel 适配器的 IPv4 IP 地址和子网掩码。</p> <p>IPv4 的 VMkernel 默认网关和 DNS 服务器地址将从选定的 TCP/IP 堆栈中获取。</p> <p>如果要为 VMkernel 适配器指定其他网关，请选中<b>替代此适配器的默认网关</b>复选框并输入网关地址。</p>

- 10 （可选）在“IPv6 设置”页面上，选择用于获取 IPv6 地址的选项。

选项	描述
<b>通过 DHCP 自动获取 IPv6 地址</b>	使用 DHCP 获取 IPv6 地址。网络上必须存在 DHCPv6 服务器。
<b>通过路由器播发自动获取 IPv6 地址</b>	<p>使用路由器播发获取 IPv6 地址。</p> <p>在 ESXi 6.5 和更高版本中，路由器播发在默认情况下处于启用状态，并且支持符合 RFC 4861 的 M 和 O 标记。</p>
<b>静态 IPv6 地址</b>	<p>a 单击<b>添加 IPv6 地址</b>以添加新的 IPv6 地址。</p> <p>b 输入 IPv6 地址和子网前缀长度，然后单击<b>确定</b>。</p> <p>c 要更改 VMkernel 默认网关，请单击<b>替代此适配器的默认网关</b>。</p> <p>IPv6 的 VMkernel 默认网关地址将从选定的 TCP/IP 堆栈中获取。</p>

- 11 检查“即将完成”页面上的设置选项，然后单击**完成**。

## 在与 vSphere Distributed Switch 关联的主机上创建 VMkernel 适配器

在与 Distributed Switch 关联的主机上创建 VMkernel 适配器，可向主机提供网络连接并处理 vSphere vMotion、IP 存储器、Fault Tolerance 日志记录、Virtual SAN 等服务的流量。您可为 vSphere 标准交换机和 vSphere Distributed Switch 上的标准系统流量设置 VMkernel 适配器。

应为每个 VMkernel 适配器指定一个专用的分布式端口组。为了进行更好的隔离，您应使用一种流量类型配置一个 VMkernel 适配器。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开网络，然后选择 VMkernel 适配器。
- 3 单击添加主机网络。
- 4 在“选择连接类型”页面上，选择 VMkernel 网络适配器，然后单击下一步。
- 5 从选择现有网络选项中，选择一个分布式端口组，然后单击下一步。
- 6 在“端口属性”页面上，配置 VMkernel 适配器的设置。

选项	描述
网络标签	网络标签从分布式端口组的标签继承。
IP 设置	选择 IPv4、IPv6 或同时选择两者。 <b>注意</b> 在未启用 IPv6 的主机上，IPv6 选项不会显示。
TCP/IP 堆栈	在列表选择一个 TCP/IP 堆栈。为 VMkernel 适配器设置了 TCP/IP 堆栈后，日后将不能再进行更改。如果选择 vMotion 或置备 TCP/IP 堆栈，您将只能使用这些堆栈处理主机上的 vMotion 或置备流量。默认 TCP/IP 堆栈上所有适用于 vMotion 的 VMkernel 适配器将被禁止用于未来的 vMotion 会话。如果设置了置备 TCP/IP 堆栈，默认 TCP/IP 堆栈上的 VMkernel 适配器将被禁止用于包括置备流量的操作，例如虚拟机冷迁移、克隆和快照创建。
启用服务	<p>可以为主机上的默认 TCP/IP 堆栈启用服务。请从以下可用服务中选择：</p> <ul style="list-style-type: none"> <li>■ <b>vMotion 流量。</b>允许 VMkernel 适配器向另一台主机播发声明，自己就是发送 vMotion 流量所应使用的网络连接。如果未对默认 TCP/IP 堆栈上的任何 VMkernel 适配器启用 vMotion 服务，或者根本不存在使用 vMotion TCP/IP 堆栈的适配器，将不能使用 vMotion 迁移到选定的主机。</li> <li>■ <b>置备流量。</b>处理为用于虚拟机冷迁移、克隆和快照创建而传输的数据。</li> <li>■ <b>Fault Tolerance 流量。</b>在主机上启用 Fault Tolerance 日志记录。对每台主机的 FT 流量只能使用一个 VMkernel 适配器。</li> <li>■ <b>管理流量。</b>为主机和 vCenter Server 启用管理流量。通常，安装 ESXi 软件后，主机将创建这样的 VMkernel 适配器。可以为主机上的管理流量创建其他 VMkernel 适配器以提供冗余。</li> <li>■ <b>vSphere Replication 流量。</b>处理从源 ESXi 主机发送到 vSphere Replication 服务器的出站复制数据。</li> <li>■ <b>vSphere Replication NFC 流量。</b>处理目标复制站点上的进站复制数据。</li> <li>■ <b>Virtual SAN。</b>在主机上启用 Virtual SAN 流量。属于 Virtual SAN 群集的每台主机都必须具有这样的 VMkernel 适配器。</li> </ul>

- 7 如果选择了 vMotion TCP/IP 或置备堆栈，在显示的警告对话框中单击确定。

如果实时迁移已启动，即使已在默认 TCP/IP 堆栈上禁止将涉及的 VMkernel 适配器用于 vMotion，该迁移也会成功完成。同样，在默认 TCP/IP 堆栈上包括为置备流量设置的 VMkernel 适配器也是一样。

- 8 （可选）在“IPv4 设置”页面上，选择用于获取 IP 地址的选项。

选项	描述
<b>自动获取 IPv4 设置</b>	使用 DHCP 获取 IP 设置。网络上必须存在 DHCP 服务器。
<b>使用静态 IPv4 设置</b>	输入 VMkernel 适配器的 IPv4 IP 地址和子网掩码。 IPv4 的 VMkernel 默认网关和 DNS 服务器地址将从选定的 TCP/IP 堆栈中获取。 如果要为 VMkernel 适配器指定其他网关，请选中 <b>替代此适配器的默认网关</b> 复选框并输入网关地址。

- 9 （可选）在“IPv6 设置”页面上，选择用于获取 IPv6 地址的选项。

选项	描述
<b>通过 DHCP 自动获取 IPv6 地址</b>	使用 DHCP 获取 IPv6 地址。网络上必须存在 DHCPv6 服务器。
<b>通过路由器播发自动获取 IPv6 地址</b>	使用路由器播发获取 IPv6 地址。 在 ESXi 6.5 和更高版本中，路由器播发在默认情况下处于启用状态，并且支持符合 RFC 4861 的 M 和 O 标记。
<b>静态 IPv6 地址</b>	a 单击 <b>添加 IPv6 地址</b> 以添加新的 IPv6 地址。 b 输入 IPv6 地址和子网前缀长度，然后单击 <b>确定</b> 。 c 要更改 VMkernel 默认网关，请单击 <b>替代此适配器的默认网关</b> 。 IPv6 的 VMkernel 默认网关地址将从选定的 TCP/IP 堆栈中获取。

- 10 检查“即将完成”页面上的设置选项，然后单击**完成**。

## 编辑 VMkernel 适配器配置

您可能需要更改 VMkernel 适配器所支持的流量类型或者 IPv4 或 IPv6 地址的获取方式。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在**配置**选项卡上，展开**网络**，然后选择 **VMkernel 适配器**。
- 3 选择驻留在目标 Distributed Switch 或标准交换机上的 VMkernel 适配器，然后单击**编辑**。
- 4 在“端口属性”页面上，选择要启用的服务。

复选框	描述
<b>vMotion 流量</b>	允许 VMkernel 适配器向另一台主机播发声明，自己就是发送 vMotion 流量所应使用的网络连接。如果没有为任何 VMkernel 适配器启用此属性，则无法通过 vMotion 向所选主机进行迁移。
<b>置备流量</b>	处理为用于虚拟机冷迁移、克隆和快照创建而传输的数据。
<b>Fault Tolerance 流量</b>	在主机上启用 Fault Tolerance 日志记录。对每台主机的 FT 流量只能使用一个 VMkernel 适配器。
<b>管理流量</b>	为主机和 vCenter Server 启用管理流量。通常，安装 ESXi 软件后，主机将创建这样的 VMkernel 适配器。您可以为主机上的管理流量添加额外的 VMkernel 适配器以提供冗余。
<b>vSphere Replication 流量</b>	处理从源 ESXi 主机发送到 vSphere Replication 服务器的出站复制数据。
<b>vSphere Replication NFC 流量</b>	处理目标复制站点上的入站复制数据。
<b>Virtual SAN</b>	启用主机上的 Virtual SAN 流量。属于 Virtual SAN 群集的每台主机都必须具有这样的 VMkernel 适配器。

- 5 在“网卡设置”页面上，为网络适配器设置 MTU。

- 6 在启用 IPv4 的情况下，在“IPv4 设置”部分中选择 IP 地址的获取方法。

选项	描述
<b>自动获取 IPv4 设置</b>	使用 DHCP 获取 IP 设置。网络上必须存在 DHCP 服务器。
<b>使用静态 IPv4 设置</b>	输入 VMkernel 适配器的 IPv4 IP 地址和子网掩码。 IPv4 的 VMkernel 默认网关和 DNS 服务器地址将从选定的 TCP/IP 堆栈中获取。 如果要为 VMkernel 适配器指定其他网关，请选中 <b>替代此适配器的默认网关</b> 复选框并输入网关地址。

- 7 在启用 IPv6 的情况下，在“IPv6 设置”中选择用于获取 IPv6 地址的选项。

**注意** 在未启用 IPv6 的主机上，IPv6 选项不会显示。

选项	描述
<b>通过 DHCP 自动获取 IPv6 地址</b>	使用 DHCP 获取 IPv6 地址。网络上必须存在 DHCPv6 服务器。
<b>通过路由器播发自动获取 IPv6 地址</b>	使用路由器播发获取 IPv6 地址。 在 ESXi 6.5 和更高版本中，路由器播发在默认情况下处于启用状态，并且支持符合 RFC 4861 的 M 和 O 标记。
<b>静态 IPv6 地址</b>	<ul style="list-style-type: none"> <li>a 单击<b>添加 IPv6 地址</b>以添加新的 IPv6 地址。</li> <li>b 输入 IPv6 地址和子网前缀长度，然后单击<b>确定</b>。</li> <li>c 要更改 VMkernel 默认网关，请单击<b>替代此适配器的默认网关</b>。</li> </ul> IPv6 的 VMkernel 默认网关地址将从选定的 TCP/IP 堆栈中获取。

在“IPv6 设置”页面上，单击“高级设置”以移除 IPv6 地址。如果启用了路由器通告，则在此处移除的地址可能会再次出现。不支持移除 VMkernel 适配器上的 DHCP 地址。这些地址只能在 DHCP 选项处于关闭状态时移除。

- 8 在“分析影响”页面上，验证对 VMkernel 适配器所做的更改是否会中断其他操作。
- 9 单击**确定**。

## 替代 VMkernel 适配器的默认网关

可能需要替代 VMkernel 适配器的默认网关，以便为 vMotion、Fault Tolerance 日志记录和 Virtual SAN 等服务提供不同的网关。

主机上的每个 TCP/IP 堆栈只能有一个默认网关。此默认网关是路由表的一部分，在 TCP/IP 堆栈上运行的所有服务都会使用该网关。

例如，可以在主机上配置 VMkernel 适配器 vmk0 和 vmk1。

- vmk0 用于 10.162.10.0/24 子网上的管理流量，默认网关为 10.162.10.1
- vmk1 用于 172.16.1.0/24 子网上 vMotion 流量

如果将 172.16.1.1 设置为 vmk1 的默认网关，vMotion 将 vmk1 与网关 172.16.1.1 一起用作其输出接口。172.16.1.1 网关是 vmk1 配置的一部分，不在路由表中。只有将 vmk1 指定为输出接口的服务使用此网关。这为需要多个网关的服务提供了额外的第 3 层连接选项。

可以使用 vSphere Web Client 或 ESXCLI 命令配置 VMkernel 适配器的默认网关。

请参见第 52 页，“在 vSphere 标准交换机上创建 VMkernel 适配器”、第 54 页，“在与 vSphere Distributed Switch 关联的主机上创建 VMkernel 适配器”和第 57 页，“使用 ESXCLI 配置 VMkernel 适配器网关”。



## 使用 ESXCLI 配置 VMkernel 适配器网关

可替代 VMkernel 适配器的默认网络，以便为 vMotion、Fault Tolerance 日志记录和 Virtual SAN 之类的服务提供不同的网关。

### 步骤

- 1 打开与主机的 SSH 连接。
- 2 以 root 用户身份登录。
- 3 运行 ESXCLI 命令。

```
esxcli network ip interface ipv4 set -i vmknics -t static -g gateway -I IP address -N mask
```

其中 *vmknics* 是 VMkernel 适配器的名称，*gateway* 是网关的 IP 地址，*IP address* 是 VMkernel 适配器的地址，*mask* 是网络掩码。

## 查看主机上的 TCP/IP 堆栈配置

您可查看主机上 TCP/IP 堆栈的 DNS 和路由配置。还可查看 IPv4 和 IPv6 路由表、拥堵控制算法和允许的最大连接数。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开网络，然后选择 TCP/IP 配置。
- 3 从“TCP/IP 堆栈”表中选择堆栈。

如果主机上未配置自定义 TCP/IP 堆栈，则查看主机上的默认堆栈、vMotion 堆栈和置备 TCP/IP 堆栈。

选定 TCP/IP 堆栈的相关 DNS 和路由详细信息显示在“TCP/IP 堆栈”表下方。您可以查看 IPv4 和 IPv6 路由表以及堆栈的 DNS 和路由配置。

---

**注意** 仅在主机上启用了 IPv6 时才能看到 IPv6 路由表。

---

高级选项卡包含有关配置的拥堵控制算法和堆栈允许的最大连接数的信息。

## 更改主机上的 TCP/IP 堆栈配置

您可更改主机上 TCP/IP 堆栈的 DNS 和默认路由配置。还可更改自定义 TCP/IP 堆栈的拥堵控制算法、最大连接数和名称。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开网络，然后选择 TCP/IP 配置。

- 从表中选择一个堆栈，单击**编辑**并进行适当更改。

页面	选项
名称	更改自定义 TCP/IP 堆栈的名称
DNS 配置	<p>选择 DNS 服务器的获取方法。</p> <ul style="list-style-type: none"> <li>■ 选择<b>自动从 VMkernel 网络适配器获取设置</b>，然后从 <b>VMKernel 网络适配器</b> 下拉菜单中选择一个网络适配器</li> <li>■ 选择<b>手动输入设置</b>，然后编辑 DNS 配置设置。 <ul style="list-style-type: none"> <li>a 编辑主机名。</li> <li>b 编辑域名。</li> <li>c 键入首选 DNS 服务器 IP 地址。</li> <li>d 键入备用 DNS 服务器 IP 地址。</li> <li>e （可选）使用<b>搜索域</b>文本框指定解析非限定域名时要在 DNS 搜索中使用的 DNS 后缀。</li> </ul> </li> </ul>
路由	<p>编辑 VMkernel 网关信息。</p> <p><b>注意</b> 移除默认网关可能会导致客户端与主机断开连接。</p>
高级	编辑堆栈的最大连接数和拥堵控制算法

- 单击**确定**应用更改。

#### 下一步

您可以使用 CLI 命令将静态路由添加到其他网关。有关详细信息，请参见 <http://kb.vmware.com/kb/2001426>。

## 创建自定义 TCP/IP 堆栈

可以在主机上创建一个自定义 TCP/IP 堆栈通过自定义应用程序转发网络流量。

#### 步骤

- 打开与主机的 SSH 连接。
- 以 root 用户身份登录。
- 运行以下 vSphere CLI 命令。

```
esxcli network ip netstack add -N="stack_name"
```

在主机上创建自定义 TCP/IP 堆栈。可以将 VMkernel 适配器分配给该堆栈。

## 移除 VMkernel 适配器

不再需要 VMkernel 适配器时，请从 vSphere Distributed Switch 或标准交换机中移除该适配器。确保在主机上至少保留一个用于管理流量的 VMkernel 适配器，以保持网络连接不中断。

#### 步骤

- 在 vSphere Web Client 中，导航到主机。
- 在**配置**选项卡上，展开**网络**，然后选择 **VMkernel 适配器**。
- 从列表中选择 VMkernel 适配器，然后单击**移除选定的网络适配器**图标。
- 在确认对话框中，单击**分析影响**。

- 5 如果使用具有端口绑定的软件 iSCSI 适配器，请查看对其网络配置的影响。

选项	描述
<b>无影响</b>	应用新的网络连接配置之后，iSCSI 将继续执行其常规功能。
<b>重要影响</b>	如果应用了新的网络连接配置，则可能会中断 iSCSI 的常规功能。
<b>严重影响</b>	如果应用了新的网络连接配置，则将中断 iSCSI 的常规功能。

- a 如果 iSCSI 受到的影响非常重要或严重，请单击 **iSCSI** 条目，然后查看“分析详细信息”窗格中所显示的原因。
  - b 请取消移除 VMkernel 适配器，直到解决对服务产生的任何严重或重要影响的原因，或者，如果不存在受影响的服务，请关闭“分析影响”对话框。
- 6 单击**确定**。



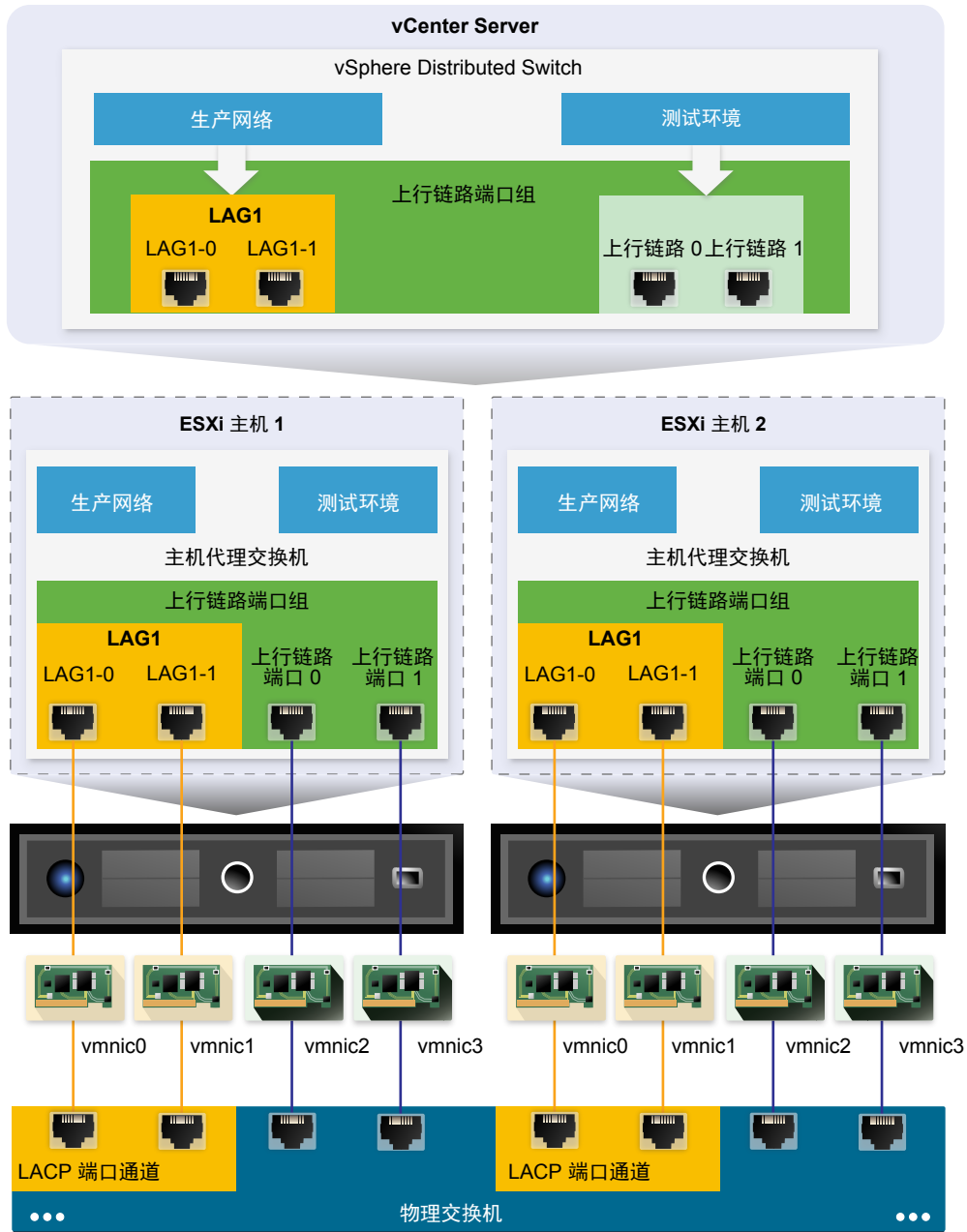
# vSphere Distributed Switch 上的 LACP 支持

---

# 5

通过 vSphere Distributed Switch 上的 LACP 支持，您可以使用动态链路聚合将 ESXi 主机连接到物理交换机。您可以在 Distributed Switch 上创建多个链路聚合组 (LAG)，以汇总连接到 LACP 端口通道的 ESXi 主机上的物理网卡带宽。

图 5-1 vSphere Distributed Switch 上的增强型 LACP 支持



## Distributed Switch 上的 LACP 配置

您可以配置一个具有两个或多个端口的 LAG，然后将物理网卡连接到这些端口。LAG 的端口在 LAG 中以成组形式存在，网络流量通过 LACP 哈希算法在这些端口之间实现负载均衡。您可以使用 LAG 处理分布式端口组的流量，以便为端口组提供增强型网络带宽、冗余和负载均衡。

在 Distributed Switch 上创建 LAG 时，同时会在与 Distributed Switch 相连的每个主机的代理交换机上创建 LAG 对象。例如，如果创建包含两个端口的 LAG1，则将在连接到 Distributed Switch 的每台主机上创建具有相同端口数的 LAG1。

在主机代理交换机上，一个物理网卡只能连接到一个 LAG 端口。在 Distributed Switch 上，一个 LAG 端口可能具有来自所连接的不同主机的多个物理网卡。必须将连接到 LAG 端口的主机上的物理网卡连接到加入物理交换机上的 LACP 端口通道的链路。

最多可以在一个 Distributed Switch 上创建 64 个 LAG。一个主机最多可支持 32 个 LAG。但是，您实际可以使用的 LAG 数量取决于基础物理环境的功能和虚拟网络的拓扑。例如，如果物理交换机在 LACP 端口通道中最多支持四个端口，则最多可将每台主机的四个物理网卡连接到 LAG。

## 物理交换机上的端口通道配置

对于每个要使用 LACP 的主机，必须在物理交换机上为其创建一个单独的 LACP 端口通道。在物理交换机上配置 LACP 时，必须考虑以下要求：

- LACP 端口通道中的端口数量必须等于要在主机上建组的物理网卡数量。例如，如果要在主机上聚合两个物理网卡的带宽，必须在物理交换机上创建一个具有两个端口的 LACP 端口通道。Distributed Switch 上的 LAG 必须至少配置两个端口。
- 物理交换机上的 LACP 端口通道的哈希算法必须与 Distributed Switch 上为 LAG 配置的哈希算法相同。
- 所有要连接到 LACP 端口通道的物理网卡必须采用相同的速度和双工配置。

本章讨论了以下主题：

- [第 63 页，“转换为 vSphere Distributed Switch 上的增强型 LACP 支持”](#)
- [第 64 页，“分布式端口组的 LACP 成组和故障切换配置”](#)
- [第 64 页，“配置链路聚合组处理分布式端口组的流量”](#)
- [第 68 页，“编辑链路聚合组”](#)
- [第 69 页，“在上行链路端口组上启用 LACP 5.1 支持”](#)
- [第 69 页，“vSphere Distributed Switch 的 LACP 支持限制”](#)

## 转换为 vSphere Distributed Switch 上的增强型 LACP 支持

在将 vSphere Distributed Switch 从版本 5.1 升级到版本 5.5、6.0 或 6.5 之后，可以转换为增强型 LACP 支持，以便在 Distributed Switch 上创建多个 LAG。

如果 Distributed Switch 上已存在 LACP 配置，增强 LACP 支持将创建一个新的 LAG，并将所有物理网卡从独立上行链路迁移到 LAG 端口。要创建不同的 LACP 配置，应禁用上行链路端口组上的 LACP 支持，然后再启动转换。

如果转换为增强型 LACP 支持失败，请参见《*vSphere 故障排除*》了解有关手动完成该过程的详细信息。

### 前提条件

- 确认 vSphere Distributed Switch 的版本是 5.5、6.0 或 6.5。
- 确认所有分布式端口组都不允许替代单个端口上的上行链路绑定策略。
- 如果从现有 LACP 配置进行转换，请确认 Distributed Switch 上只有一个上行链路端口组。
- 确认加入 Distributed Switch 的主机已连接并有响应。
- 确认对交换机上的分布式端口组具有 **dvPort 组.修改** 特权。
- 确认对 Distributed Switch 上的主机具有 **主机.配置.修改** 特权。

---

**注意** 将 vSphere Distributed Switch 从版本 5.1 升级到版本 6.5 时，将自动增强 LACP 支持。如果升级前已在 Distributed Switch 上启用基本 LACP 支持，则应手动增强 LACP 支持。

---

**步骤**

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 选择**摘要**。
- 3 在“功能”部分中，单击链路聚合控制协议旁的**增强**。
- 4 （可选）选择**导出配置**以备份 Distributed Switch 的配置，然后单击**下一步**。

该备份过程仅存储 vCenter Server 端的 Distributed Switch 配置。如果转换为增强型 LACP 支持失败，您可以使用备份创建一个具有相同配置的新 Distributed Switch，或手动完成转换。

- 5 查看验证必备条件。

必备条件	描述
<b>端口组的可访问性</b>	您有访问和修改交换机上的上行链路和分布式端口组所需的足够特权。
<b>LACP 配置</b>	Distributed Switch 上仅有一个上行链路端口组。
<b>上行链路绑定策略替代</b>	分布式端口组不允许替代单个端口上的上行链路绑定策略。
<b>主机的可访问性</b>	您有修改连接到 Distributed Switch 的主机的网络连接配置所需的足够特权。
<b>主机的连接</b>	加入 Distributed Switch 的主机已连接并有响应。

- 6 单击**下一步**。
- 7 如果从现有 LACP 配置进行转换，请在“名称”文本字段中键入新 LAG 的名称。
- 8 单击**下一步**查看有关转换的详细信息，然后单击**完成**。

已在 vSphere Distributed Switch 上转换为增强型 LACP 支持。

**下一步**

在 Distributed Switch 上创建 LAG 以汇总所关联的主机上多个物理网卡的带宽。

**分布式端口组的 LACP 成组和故障切换配置**

要使用 LAG 处理分布式端口组的网络流量，您可以为 LAG 端口分配物理网卡，并将分布式端口组的成组和故障切换顺序中的 LAG 设置为活动。

**表 5-1 分布式端口组的 LACP 成组和故障切换配置**

故障切换顺序	上行链路	描述
活动	单个 LAG	只能使用一个活动 LAG 或多个独立上行链路来处理分布式端口组的流量。无法配置多个活动 LAG，也无法配置活动 LAG 和独立上行链路的混合设置。
备用	空	支持一个活动 LAG 和备用上行链路组合，但不支持备用 LAG 和活动上行链路组合。不支持一个活动 LAG 和另一个备用 LAG 的组合。
未使用	所有独立上行链路和其他 LAG（如果有）	由于只能有一个 LAG 处于活动状态，且“备用”列表必须为空，因此必须将所有独立上行链路和其他 LAG 设置为“未使用”。

**配置链路聚合组处理分布式端口组的流量**

要聚合主机上多个物理网卡的带宽，您可以在 Distributed Switch 上创建一个链路聚合组 (LAG)，并将其用于处理分布式端口组的流量。

新建的 LAG 未用于分布式端口组的成组和故障切换顺序中，其端口也未分配物理网卡。要使用 LAG 处理分布式端口组的网络流量，必须将流量从独立上行链路迁移到 LAG。



前提条件

- 验证对于每个要使用 LACP 的主机，物理交换机上是否都有一个单独的 LACP 端口通道。请参见第 61 页，第 5 章 “vSphere Distributed Switch 上的 LACP 支持”。
- 验证配置 LAG 所在的 vSphere Distributed Switch 的版本是 5.5 还是 6.0。
- 验证 Distributed Switch 上是否支持增强型 LACP。

步骤

- 1 创建链路聚合组第 65 页，  
要将分布式端口组的网络流量迁移到链路聚合组 (LAG)，请在 Distributed Switch 上创建新的 LAG。
- 2 在分布式端口组的绑定和故障切换顺序中将链路聚合组设置为备用状态第 66 页，  
默认情况下，新的链路聚合组 (LAG) 未包含在分布式端口组的绑定和故障切换顺序中。对于分布式端口组而言，由于只有一个 LAG 或独立上行链路可以处于活动状态，因此必须创建一个中间绑定和故障切换配置，其中 LAG 为备用状态。在保持网络连接正常的情况下，可以通过此配置将物理网卡迁移到 LAG 端口。
- 3 将物理网卡分配给链路聚合组的端口第 66 页，  
您已在分布式端口组的绑定和故障切换顺序中将新的链路聚合组 (LAG) 设置为备用状态。通过将 LAG 设置为备用状态，可在不丢失网络连接的情况下，将物理网卡安全地从独立上行链路迁移到 LAG 端口。
- 4 在分布式端口组的绑定和故障切换顺序中将链路聚合组设置为活动状态第 67 页，  
您已将物理网卡迁移到链路聚合组 (LAG) 的端口。请在分布式端口组的绑定和故障切换顺序中将 LAG 设置为活动状态，并将所有独立的上行链路移至未使用状态。

创建链路聚合组

要将分布式端口组的网络流量迁移到链路聚合组 (LAG)，请在 Distributed Switch 上创建新的 LAG。

步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在配置选项卡上，展开设置并选择 LACP。
- 3 单击新建链路聚合组图标。
- 4 命名新的 LAG。
- 5 设置 LAG 的端口数。  
请将为 LAG 设置与物理交换机上的 LACP 端口通道中相同的端口数。LAG 端口具有与 Distributed Switch 上的上行链路相同的功能。所有 LAG 端口将构成 LAG 上下文中的网卡组。
- 6 选择 LAG 的 LACP 协商模式。

选项	描述
主动节点	所有 LAG 端口都处于主动协商模式。LAG 端口通过发送 LACP 数据包启动与物理交换机上的 LACP 端口通道的协商。
被动节点	LAG 端口处于被动协商模式。端口对接收的 LACP 数据包做出响应，但是不会启动 LACP 协商。

如果物理交换机上启用 LACP 的端口处于主动协商模式，则可以将 LAG 端口置于被动模式，反之亦然。

- 7 从 LACP 定义的哈希算法中选择一个负载均衡模式。

**注意** 该哈希算法必须与为物理交换机上的 LACP 端口通道设置的哈希算法相同。

## 8 为 LAG 设置 VLAN 和 NetFlow 策略。

当在上行链路端口组中启用了按单个上行链路端口替代 VLAN 和 NetFlow 策略时，此选项将处于活动状态。如果为 LAG 设置了 VLAN 和 NetFlow 策略，则这些策略将替代上行链路端口组级别上设置的策略。

## 9 单击**确定**。

新的 LAG 未包含在分布式端口组的绑定和故障切换顺序中。未向 LAG 端口分配任何物理网卡。

和独立上行链路一样，LAG 在每个与 Distributed Switch 关联的主机上都有表示形式。例如，如果您在 Distributed Switch 上创建包含两个端口的 LAG1，将在每个与该 Distributed Switch 关联的主机上创建一个具有两个端口的 LAG1。

## 下一步

在分布式端口组的绑定和故障切换配置中将 LAG 设置为备用状态。通过这一方式可以创建中间配置，从而将网络流量迁移到 LAG 而不会断开网络连接。

## 在分布式端口组的绑定和故障切换顺序中将链路聚合组设置为备用状态

默认情况下，新的链路聚合组 (LAG) 未包含在分布式端口组的绑定和故障切换顺序中。对于分布式端口组而言，由于只有一个 LAG 或独立上行链路可以处于活动状态，因此必须创建一个中间绑定和故障切换配置，其中 LAG 为备用状态。在保持网络连接正常的情况下，可以通过此配置将物理网卡迁移到 LAG 端口。

## 步骤

- 1 导航至 Distributed Switch。
- 2 在**操作**菜单中，选择**分布式端口组 > 管理分布式端口组**。
- 3 选择**绑定和故障切换**，然后单击**下一步**。
- 4 选择要在其中使用 LAG 的端口组。
- 5 在“故障切换顺序”中，选择 LAG 并使用向上箭头将其移至备用上行链路列表中。
- 6 单击**下一步**，查看通知您有关中间绑定和故障切换配置的使用情况的消息，然后单击**确定**。
- 7 在“即将完成”页面上，单击**完成**。

## 下一步

将物理网卡从独立上行链路迁移到 LAG 端口。

## 将物理网卡分配给链路聚合组的端口

您已在分布式端口组的绑定和故障切换顺序中将新的链路聚合组 (LAG) 设置为备用状态。通过将 LAG 设置为备用状态，可在不丢失网络连接的情况下，将物理网卡安全地从独立上行链路迁移到 LAG 端口。

## 前提条件

- 确认所有 LAG 端口以及物理交换机上对应的已启用 LACP 的端口均处于主动 LACP 协商模式。
- 确认要为 LAG 端口分配的物理网卡具有相同的速度，并配置为全双工。

## 步骤

- 1 在 vSphere Web Client 中，导航到 LAG 所在的 Distributed Switch。
- 2 从**操作**菜单中，选择**添加和管理主机**。
- 3 选择**管理主机网络**。
- 4 选择要为 LAG 端口分配其物理网卡的主机，然后单击**下一步**。

- 5 在“选择网络适配器任务”页面上，选择**管理物理适配器**，然后单击**下一步**。
- 6 在“管理物理网络适配器”页面上，选择某个网卡，然后单击**分配上行链路**。
- 7 选择 LAG 端口，然后单击**确定**。
- 8 对要分配给 LAG 端口的所有物理网卡重复**步骤 6**和**步骤 7**。
- 9 完成向导中的操作。

### 示例：在“添加和管理主机”向导中为 LAG 分配两个物理网卡

例如，如果一个 LAG 中包含两个端口，则可以在添加和管理主机向导中为每个 LAG 端口配置一个物理网卡。

#### 下一步

在分布式端口组的绑定和故障切换顺序中将 LAG 设置为活动状态，并将所有独立上行链路设置为未使用状态。

## 在分布式端口组的绑定和故障切换顺序中将链路聚合组设置为活动状态

您已将物理网卡迁移到链路聚合组 (LAG) 的端口。请在分布式端口组的绑定和故障切换顺序中将 LAG 设置为活动状态，并将所有独立的上行链路移至未使用状态。

#### 步骤

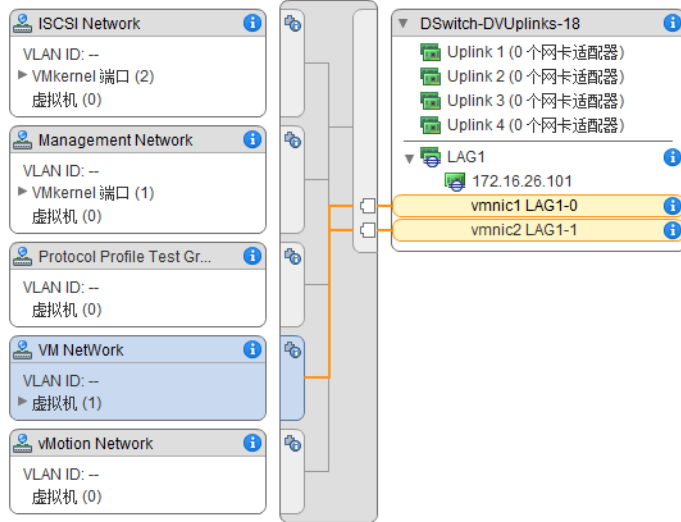
- 1 导航至 Distributed Switch。
- 2 在**操作菜单**中，选择**分布式端口组 > 管理分布式端口组**。
- 3 选择**绑定和故障切换**，然后单击**下一步**。
- 4 选择将 LAG 设置为备用状态的端口组，然后单击**下一步**。
- 5 在故障切换顺序中，使用向上和向下箭头移动“活动”列表中的 LAG、“未使用”列表中的所有独立上行链路，并将“备用”列表留空。
- 6 单击**下一步**，然后单击**完成**。

您已安全地将网络流量从独立上行链路迁移至分布式端口组的 LAG，并且为组创建了有效的 LACP 绑定和故障切换配置。

### 示例：使用 LAG 的 Distributed Switch 的拓扑

如果您配置了一个具有两个端口的 LAG 以处理分布式端口组流量，则可以检查 Distributed Switch 的拓扑以查看新配置所导致的拓扑更改。

图 5-2 具有一个 LAG 的 Distributed Switch 拓扑



## 编辑链路聚合组

如果需要向链路聚合组 (LAG) 添加多个端口或者更改 LACP 协商模式、负载平衡算法或 VLAN 和 NetFlow 策略，请编辑该 LAG 的设置。

### 步骤

- 1 在 vSphere Web Client 中，导航到 vSphere Distributed Switch。
- 2 在配置选项卡上，展开设置并选择 LACP。
- 3 单击新建链路聚合组图标。
- 4 在名称文本框中，键入 LAG 的新名称。
- 5 如果要向 LAG 添加更多物理网卡，请更改 LAG 的端口数。

必须将新网卡连接到属于物理交换机上某个 LACP 端口通道的端口。

- 6 更改 LAG 的 LACP 协商模式。

如果物理 LACP 端口通道上的所有端口均处于“主动”LACP 模式，则可以将 LAG 的 LACP 模式更改为“被动”，反之亦然。

- 7 更改 LAG 的负载平衡模式。

可从 LACP 定义的负载平衡算法中进行选择。

- 8 更改 VLAN 和 NetFlow 策略。

如果上行链路端口组支持替代各个端口的 VLAN 和 NetFlow 策略，此选项将处于活动状态。如果更改了 LAG 的 VLAN 和 NetFlow 策略，则这些策略将替代上行链路端口组级别上设置的策略。

- 9 单击确定。

## 在上行链路端口组上启用 LACP 5.1 支持

您可以为 vSphere Distributed Switch 5.1 和已升级到 5.5 或 6.0 但无增强型 LACP 支持的交换机的上行链路端口组启用 LACP 支持。

### 前提条件

- 验证对于每个要使用 LACP 的主机，物理交换机上是否都有一个单独的 LACP 端口通道。
- 验证分布式端口组是否已将其负载平衡策略设置为 IP 哈希。
- 验证物理交换机上的 LACP 端口通道是否配置了 IP 哈希负载平衡。
- 验证分布式端口组是否已将网络故障检测策略设置仅为链路状态。
- 验证分布式端口组是否已将所有上行链路在其绑定和故障切换顺序中设置为活动。
- 验证连接到上行链路的所有物理网卡是否速度相同并配置为采用全双工模式。

### 步骤

- 1 在 vSphere Web Client 中，导航到上行链路端口组。
  - a 选择 Distributed Switch，然后单击**网络**选项卡。
  - b 单击**上行链路端口组**，然后选择上行链路端口组。
- 2 单击**配置**选项卡，然后选择**属性**。
- 3 单击**编辑**。
- 4 在“LACP”部分中，使用下拉列表启用 LACP。
- 5 为上行链路端口组设置 LACP 协商模式。

选项	描述
<b>主动节点</b>	该组中的所有上行链路端口都处于主动协商模式。上行链路端口通过发送 LACP 数据包对物理交换机上启用了 LACP 的端口启动协商。
<b>被动节点</b>	所有上行链路端口处于被动协商模式。端口对接收的 LACP 数据包做出响应，但是不会启动 LACP 协商。

如果物理交换机上启用了 LACP 的端口处于主动协商模式，则可以将上行链路端口置于被动模式，反之亦然。

- 6 单击**确定**。

## vSphere Distributed Switch 的 LACP 支持限制

vSphere Distributed Switch 上的 LACP 支持允许网络设备通过向对等设备发送 LACP 数据包来协商链路的自动绑定。但是，vSphere Distributed Switch 上的 LACP 支持具有限制。

- LACP 支持与软件 iSCSI 多路径不兼容。
- LACP 支持设置在主机配置文件中不可用。
- 无法在两个嵌套的 ESXi 主机之间使用 LACP 支持。
- LACP 支持无法与 ESXi Dump Collector 一起使用。
- LACP 支持无法与端口镜像一起使用。
- 成组和故障切换健康状况检查不适用于 LAG 端口。LACP 检查 LAG 端口的连接性。
- 当只有一个 LAG 处理每个分布式端口或端口组的流量时，增强型 LACP 支持可以正常运行。

- LACP 5.1 支持只能与 IP 哈希负载平衡和链路状态网络故障切换检测一起使用。
- LACP 5.1 支持只为每个 Distributed Switch 和每台主机提供一个 LAG。

## 备份和还原网络配置

---

如果发生无效更改或转移到其他部署，vSphere 5.1 及更高版本可使您能够备份和还原 vSphere Distributed Switch、分布式端口组和上行链路端口组的配置。

本章讨论了以下主题：

- 第 71 页，“备份和还原 vSphere Distributed Switch 配置”
- 第 73 页，“导出、导入和还原 vSphere 分布式端口组配置”

### 备份和还原 vSphere Distributed Switch 配置

vCenter Server 提供 vSphere Distributed Switch 配置的备份和还原功能。如数据库故障或升级失败，可以还原虚拟网络配置。还可以将已保存的交换机配置用作模板，以在相同或新的 vSphere 环境中创建交换机的副本。

可以导入或导出分布式交换机（包括其端口组）的配置。有关导出、导入和还原端口组配置的信息，请参见第 73 页，“导出、导入和还原 vSphere 分布式端口组配置”。

---

**注意** 您可以使用已保存的配置文件来还原 Distributed Switch 上的策略和主机关联。无法还原物理网卡与上行链路端口或链路聚合组端口的连接。

---

### 导出 vSphere Distributed Switch 配置

可以将 vSphere Distributed Switch 和分布式端口组配置导出到某一文件。该文件保留有效的网络配置，使这些配置能够传输至其他环境。

此功能仅适用于 vCenter Server 5.1 及更高版本。

如果从 vCenter Server 5.1 进行升级，则可以先导出交换机的配置，然后再升级 vCenter Server。如果从 5.1 之前的版本升级 vCenter Server，请先将 vCenter Server 升级到 6.0 版，然后再备份交换机的配置。

#### 前提条件

验证 vCenter Server 是否为 5.1 版或更高版本。

#### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 右键单击 Distributed Switch，然后选择**设置 > 导出配置**。
- 3 选择导出分布式交换机配置，或者导出分布式交换机配置和所有端口组。
- 4 （可选）在**描述**字段中输入有关此配置的说明。
- 5 单击**确定**。

- 6 单击 **是** 可将配置文件保存到您的本地系统。

### 下一步

通过使用已导出配置文件，可执行以下任务：

- 在 vSphere 环境中，为导出的 Distributed Switch 创建一份副本。请参见第 72 页，“[导入 vSphere Distributed Switch 配置](#)”。
  - 覆盖现有 Distributed Switch 中的设置。请参见第 72 页，“[还原 vSphere Distributed Switch 配置](#)”。
- 也可以仅导出、导入和还原端口组配置。请参见第 73 页，“[导出、导入和还原 vSphere 分布式端口组配置](#)”。

## 导入 vSphere Distributed Switch 配置

导入存储的配置文件可创建一个新 vSphere Distributed Switch 或还原之前已删除的交换机。

在 vSphere 5.1 及更高版本中，可以使用 vSphere Web Client 导入 Distributed Switch。

配置文件中包含交换机的网络连接设置。使用 vSphere Web Client，还可以复制其他虚拟环境中的虚拟机。

---

**注意** 可以使用已保存的配置文件复制交换机实例、其主机关联以及策略。无法复制物理网卡到上行链路端口或链路聚合组上的端口的连接。

---

### 前提条件

验证 vCenter Server 是否为 5.1.0 版或更高版本。

### 步骤

- 1 在 vSphere Web Client 中，导航到数据中心。
- 2 右键单击该数据中心，然后选择 **Distributed Switch > 导入 Distributed Switch**。
- 3 浏览到配置文件的位置。
- 4 要将配置文件中的密钥分配给交换机及其端口组，请选中 **保留原始 Distributed Switch 标识符和端口组标识符** 复选框，然后单击 **下一步**。

在以下情况中，可以使用 **保留原始 Distributed Switch 标识符和端口组标识符** 选项：

- 重新创建已删除的交换机。
- 还原升级失败的交换机。

所有端口组均重新创建，已连接到交换机的主机重新添加。

- 5 检查交换机的设置，然后单击 **完成**。

系统将使用配置文件中的设置创建一个新 Distributed Switch。如果在配置文件中包含了分布式端口组信息，则也会创建端口组。

## 还原 vSphere Distributed Switch 配置

使用还原选项将现有分布式交换机的配置重置为配置文件中的设置。还原分布式交换机会将所选交换机的设置改回配置文件中保存的设置。

---

**注意** 您可以使用已保存的配置文件来还原 Distributed Switch 上的策略和主机关联。无法还原物理网卡与上行链路端口或链路聚合组端口的连接。

---

### 前提条件

验证 vCenter Server 是否为 5.1 版或更高版本。



**步骤**

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在导航器中右键单击 Distributed Switch，然后选择**设置 > 还原配置**。
- 3 浏览到要使用的配置备份文件。
- 4 选择**还原 Distributed Switch 和所有端口组**或**仅还原 Distributed Switch**，然后单击**下一步**。
- 5 查看还原的摘要信息。  
还原分布式交换机将覆盖分布式交换机及其端口组的当前设置。不会删除不属于配置文件的现有端口组。
- 6 单击**完成**。  
分布式交换机配置即已还原到配置文件中的设置。

## 导出、导入和还原 vSphere 分布式端口组配置

可以将 vSphere 分布式端口组配置导出到某一文件。通过该配置文件，可以保留有效的端口组配置，从而将这些配置分发到其他部署。

在导出 Distributed Switch 配置时，可以同时导出端口组信息。请参见第 71 页，“[备份和还原 vSphere Distributed Switch 配置](#)”。

### 导出 vSphere 分布式端口组配置

可以将分布式端口组配置导出到某一文件。该配置保留有效的网络配置，使这些配置能够分发到其他部署。

该功能仅在 vSphere Web Client 5.1 或更高版本中可用。但是，如果您使用 vSphere Web Client 5.1 或更高版本，则可以从任何版本的分布式端口导出设置。

**步骤**

- 1 在 vSphere Web Client 中找到分布式端口组。
  - a 选择 Distributed Switch，然后单击**网络**选项卡。
  - b 单击**分布式端口组**。
- 2 右键单击分布式端口组，然后选择**导出配置**。
- 3 （可选）在**描述**字段中，键入有关此配置的备注。
- 4 单击**确定**。  
单击**是**可将配置文件保存到您的本地系统。

现在即拥有一个包含选定分布式端口组的所有设置的配置文件。您可以使用这一文件在现有部署中创建该配置的多个副本，或者覆盖现有分布式端口组的设置以符合选定设置。

**下一步**

通过使用已导出配置文件，可执行以下任务：

- 若要创建已导出分布式端口组的副本，请参见第 73 页，“[导入 vSphere 分布式端口组配置](#)”。
- 若要覆盖现有分布式端口组中的设置，请参见第 74 页，“[还原 vSphere 分布式端口组配置](#)”。

### 导入 vSphere 分布式端口组配置

使用导入可从配置文件创建分布式端口组。

如果现有端口组与已导入的端口组同名，则新端口组名称末尾将包含一个放在括号内的数字。已导入配置的设置将应用到新端口组，而原始端口组的设置保持不变。

该功能仅在 vSphere Web Client 5.1 或更高版本中可用。但是，如果您使用 vSphere Web Client 5.1 及更高版本，则可以从任何版本的分布式端口导出设置。

#### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 右键单击 Distributed Switch，然后选择**分布式端口组 > 导入分布式端口组**。
- 3 浏览到已保存的配置文件的位置，然后单击**下一步**。
- 4 请在完成导入之前检查导入设置。
- 5 单击**完成**。

## 还原 vSphere 分布式端口组配置

使用还原选项将现有分布式端口组的配置重置为配置文件中的设置。

该功能仅在 vSphere Web Client 5.1 或更高版本中可用。但是，如果使用 vSphere Web Client 5.1 或更高版本，则可从任何版本的 Distributed Switch 还原设置。

#### 步骤

- 1 在 vSphere Web Client 中找到分布式端口组。
  - a 选择 Distributed Switch，然后单击**网络**选项卡。
  - b 单击**分布式端口组**。
- 2 右键单击分布式端口组，然后选择**还原配置**。
- 3 选择以下选项之一，然后单击**下一步**：
  - ◆ **还原为之前的配置**可将您的端口组配置回滚一个步骤。如果您已执行多个步骤，则无法完全还原端口组配置。
  - ◆ **从文件还原配置**使您从一个导出的备份文件还原端口组配置。您还可以使用 Distributed Switch 备份文件，只要其包含端口组的配置信息即可。
- 4 查看还原的摘要信息。
 

还原操作将使用备份中的设置覆盖分布式端口组的当前设置。如果从交换机备份文件还原端口组配置，则还原操作不会删除不属于该文件的当前端口组。
- 5 单击**完成**。

## 管理网络的回滚和恢复

在 vSphere 5.1 及更高版本中，可以使用 vSphere Distributed Switch 和 vSphere 标准交换机的回滚和恢复支持防止管理网络配置错误并从配置错误中恢复。

回滚可用于标准交换机和 Distributed Switch。要修复管理网络的无效配置，可以直接连接到主机，通过 DCUI 修复该问题。

本章讨论了以下主题：

- [第 75 页，“vSphere 网络连接回滚”](#)
- [第 77 页，“解决 vSphere Distributed Switch 上的管理网络配置中的错误”](#)

### vSphere 网络连接回滚

通过回滚配置更改，vSphere 可防止错误配置管理网络导致主机丢失与 vCenter Server 的连接。

在 vSphere 5.1 及更高版本中，默认启用网络连接回滚。但是，您可以在 vCenter Server 级别启用或禁用回滚。

#### 主机网络连接回滚

如果对与 vCenter Server 的连接的网络连接配置所做的更改无效，则将发生主机网络连接回滚。每个可断开主机连接的网络更改也将触发回滚。以下是可能触发回滚的对主机网络配置的更改示例：

- 更新物理网卡的速度或双工。
- 更新 DNS 和路由设置。
- 更新包含管理 VMkernel 网络适配器的标准端口组的成组和故障切换策略或流量调整策略。
- 更新包含管理 VMkernel 网络适配器的标准端口组的 VLAN。
- 将管理 VMkernel 网络适配器及其交换机的 MTU 增加至物理基础架构不支持的值。
- 更改管理 VMkernel 网络适配器的 IP 设置。
- 从标准交换机或 Distributed Switch 中移除管理 VMkernel 网络适配器。
- 移除包含管理 VMkernel 网络适配器的标准交换机或 Distributed Switch 的物理网卡。
- 将管理 VMkernel 适配器从 vSphere Standard Switch 迁移到 Distributed Switch。

如果出于其中任一原因而断开网络连接，任务将失败并且主机将恢复为上次有效配置。

## vSphere Distributed Switch 回滚

当对 Distributed Switch、分布式端口组或分布式端口进行无效更新时，将发生 Distributed Switch 回滚。对 Distributed Switch 配置进行以下更改将触发回滚：

- 更改 Distributed Switch 的 MTU。
- 更改管理 VMkernel 网络适配器的分布式端口组中的以下设置：
  - 成组和故障切换
  - VLAN
  - 流量调整
- 阻止包含管理 VMkernel 网络适配器的分布式端口组中的所有端口。
- 在管理 VMkernel 网络适配器的分布式端口级别替代策略。

如果由于任意更改导致配置无效，则一台或多台主机可能无法与 Distributed Switch 保持同步。

如果您知道有冲突的配置设置的所在位置，可以手动更正设置。例如，如果将管理 VMkernel 网络适配器迁移到了一个新的 VLAN，则该 VLAN 实际可能无法在物理交换机上进行中继。更正物理交换机配置后，下一次 Distributed Switch-主机同步将解决配置问题。

如果您不知道问题出自哪里，可以将 Distributed Switch 或分布式端口组的状态还原到以前的配置。请参见 [第 74 页](#)，“还原 vSphere 分布式端口组配置”。

## 禁用网络回滚

默认情况下，回滚在 vSphere 5.1 及更高版本中处于启用状态。您可以使用 vSphere Web Client 在 vCenter Server 中禁用回滚。

### 步骤

- 1 在 vSphere Web Client 中，导航到 vCenter Server 实例。
- 2 在配置选项卡上，展开设置，然后选择高级设置。
- 3 单击编辑。
- 4 选择 config.vpxd.network.rollback 项，然后将值更改为 false。

如果未提供该密钥，您可添加并将值设置为 false。

- 5 单击确定。
- 6 重新启动 vCenter Server 应用更改。

## 使用 vCenter Server 配置文件禁用网络回滚

默认情况下，回滚在 vSphere 5.1 及更高版本中处于启用状态。可以通过直接编辑 vCenter Server 的 vpxd.cfg 配置文件禁用回滚。

### 步骤

- 1 在 vCenter Server 的主机上，导航到包含配置文件的目录：
  - 在 Windows Server 操作系统上，目录的位置为 C:\ProgramData\VMware\CIS\cfg\vmware-vpx。
  - 在 vCenter Server Appliance 上，目录的位置为 /etc/vmware-vpx。
- 2 打开 vpxd.cfg 文件进行编辑。

- 3 在 <network> 元素中，将 <rollback> 元素设置为 **false**：

```
<config>
<vpzd>
<network>
<rollback>false</rollback>
</network>
</vpzd>
</config>
```

- 4 保存并关闭文件。
- 5 重新启动 vCenter Server 系统。

## 解决 vSphere Distributed Switch 上的管理网络配置中的错误

在 vSphere 5.1 及更高版本中，可以使用直接控制台用户界面 (DCUI) 还原 vCenter Server 与主机（通过 Distributed Switch 访问管理网络）之间的连接。

如果禁用了网络连接回滚，则在 Distributed Switch 上错误配置管理网络的端口组将会导致 vCenter Server 与添加到交换机的主机之间的连接丢失。必须使用 DCUI 分别连接每个主机。

如果用来还原管理网络的上行链路也由处理其他类型流量（vMotion、Fault Tolerance 等）的 VMkernel 适配器使用，则适配器会在还原后丢失网络连接。

有关访问和使用 DCUI 的详细信息，请参见 *vSphere 安全性* 文档。

---

**注意** 无状态的 ESXi 实例不支持在 Distributed Switch 上恢复管理连接。

---

### 前提条件

验证 Distributed Switch 的端口组上是否已配置管理网络。

### 步骤

- 1 连接到主机的 DCUI。
- 2 从**网络还原选项**菜单中，选择**还原 vDS**。
- 3 配置上行链路并可选择为管理网络配置 VLAN。
- 4 应用配置。

DCUI 将创建本地极短端口并应用为 VLAN 和上行链路所提供的值。DCUI 将管理网络的 VMkernel 适配器移至新的本地端口，以便还原到 vCenter Server 的连接。

### 下一步

还原主机到 vCenter Server 的连接之后，请更正分布式端口组的配置并将 VMkernel 适配器重新添加到组中。



## 网络策略

在标准交换机或分布式端口组级别设置的策略将应用于该标准交换机上的所有端口组，或者应用于该分布式端口组中的端口。可在标准端口组或分布式端口组级别替代的配置选项是例外。

有关 vSphere Standard Switch 和 Distributed Switch 上的应用网络连接策略，请观看视频。



使用网络连接策略 ([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_working\\_with\\_network\\_policies](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_working_with_network_policies))

- [在 vSphere 标准交换机或 Distributed Switch 上应用网络策略](#) 第 80 页，  
对 vSphere 标准交换机和 vSphere Distributed Switch 应用不同的网络策略。并非所有适用于 vSphere Distributed Switch 的策略也适用于 vSphere 标准交换机。
- [在端口级别配置替代网络策略](#) 第 81 页，  
要对分布式端口应用不同的策略，您可以配置在端口组级别设置的每个端口替代策略。当分布式端口与虚拟机断开连接时，您也可以启用重置在每个端口级别设置的任何配置。
- [成组和故障切换策略](#) 第 81 页，  
通过网卡成组，您可以在组中加入两个或多个物理网卡来增加虚拟交换机的网络容量。要确定如何在适配器发生故障时重新路由流量，您可以在故障切换顺序中加入物理网卡。要确定虚拟交换机在组内的物理网卡之间如何分布网络流量，您可以根据您的环境需要和功能选择负载均衡算法。
- [VLAN 策略](#) 第 88 页，  
VLAN 策略决定了 VLAN 在网络环境中的运行方式。
- [安全策略](#) 第 90 页，  
网络安全策略可保护流量免受 MAC 地址模拟和有害端口扫描的威胁。
- [流量调整策略](#) 第 92 页，  
流量调整策略是由平均带宽、峰值带宽和突发大小所定义的。可以为每个端口组和每个分布式端口或分布式端口组建立流量调整策略。
- [资源分配策略](#) 第 94 页，  
可以使用资源分配策略将分布式端口或端口组与用户创建的网络资源池关联。通过此策略可以更有效地控制为端口或端口组指定的带宽。
- [监控策略](#) 第 95 页，  
监控策略在分布式端口或端口组上启用或禁用 NetFlow 监控。
- [流量筛选和标记策略](#) 第 95 页，  
在 vSphere Distributed Switch 5.5 及更高版本中，通过使用流量筛选和标记策略，您可以避免虚拟网络进入有害的流量和遭受安全攻击，或将 QoS 标记应用于某种类型的流量。

- [管理 vSphere Distributed Switch 上的多个端口组的策略](#)第 109 页，  
可以修改 vSphere Distributed Switch 上多个端口组的网络连接策略。
- [端口阻止策略](#)第 113 页，  
端口阻止策略允许有选择地阻止端口发送或接收数据。

## 在 vSphere 标准交换机或 Distributed Switch 上应用网络策略

对 vSphere 标准交换机和 vSphere Distributed Switch 应用不同的网络策略。并非所有适用于 vSphere Distributed Switch 的策略也适用于 vSphere 标准交换机。

**表 8-1 应用策略的虚拟交换机对象**

虚拟交换机	虚拟交换机对象	描述
vSphere 标准交换机	整个交换机	对整个标准交换机应用策略时，策略将传播到交换机上的所有标准端口组。
	标准端口组	通过替代从交换机继承的策略，您可以对单个端口组应用不同的策略。
vSphere Distributed Switch	分布式端口组	对分布式端口组应用策略时，策略将传播到组中的所有端口。
	分布式端口	通过替代从分布式端口组继承的策略，您可以对单个分布式端口应用不同的策略。
	上行链路端口组	您可以在上行链路端口组级别应用策略，策略将传播到组中的所有端口。
	上行链路端口	通过替代从上行链路端口组继承的策略，您可以对单个上行链路端口应用不同的策略。

**表 8-2 适用于 vSphere 标准交换机和 vSphere Distributed Switch 的策略**

策略	标准交换机	Distributed Switch	描述
成组和故障切换	是	是	可用于配置物理网卡以处理标准交换机、标准端口组、分布式端口组或分布式端口的网络流量。您可以在故障切换顺序中排列物理网卡，并对其应用不同的负载均衡策略。
安全	是	是	可保护流量免受 MAC 地址模拟和有害端口扫描的威胁。在网络协议堆栈的第 2 层执行网络安全策略。
流量调整	是	是	可限制端口的可用网络带宽，但也可以允许流量突发，使流量以更高的速度通过端口。ESXi 调整标准交换机上的出站网络流量以及分布式交换机上的入站和出站流量。
VLAN	是	是	可用于配置标准交换机或 Distributed Switch 的 VLAN 标记。您可以配置外部交换机标记 (EST)、虚拟交换机标记 (VST) 和虚拟客户机标记 (VGT)。
正在监控	否	是	在分布式端口或端口组上启用和禁用 NetFlow 监控。
流量筛选和标记	否	是	可以避免虚拟网络进入有害的流量和遭受安全攻击，或将 QoS 标记应用于某种类型的流量。
资源分配	否	是	可以将分布式端口或端口组与用户定义的网络资源池关联。通过此方式，您可以更有效地控制端口或端口组可用的带宽。您可以在 vSphere Network I/O Control 版本 2 和 3 中使用资源分配策略。
端口阻止	否	是	可以有选择地阻止端口发送和接收数据。



## 在端口级别配置替代网络策略

要对分布式端口应用不同的策略，您可以配置在端口组级别设置的每个端口替代策略。当分布式端口与虚拟机断开连接时，您也可以启用重置在每个端口级别设置的任何配置。

### 步骤

- 1 在 vSphere Web Client 中找到分布式端口组。
  - a 选择 Distributed Switch，然后单击**网络**选项卡。
  - b 单击**分布式端口组**。
- 2 右键单击分布式端口组，然后选择**编辑设置**。
- 3 选择**高级**页面。

选项	描述
<b>断开连接时配置重置</b>	从下拉菜单中启用或禁用断开连接时重置。 当分布式端口与虚拟机断开连接时，分布式端口的配置重置为分布式端口组设置。每个端口的替代都会被丢弃。
<b>替代端口策略</b>	选择要在每个端口级别替代的分布式端口组策略。

- 4 （可选）使用策略页面设置每个端口策略的替代。
- 5 单击**确定**。

## 成组和故障切换策略

通过网卡成组，您可以在组中加入两个或多个物理网卡来增加虚拟交换机的网络容量。要确定如何在适配器发生故障时重新路由流量，您可以在故障切换顺序中加入物理网卡。要确定虚拟交换机在组内的物理网卡之间如何分布网络流量，您可以根据您的环境需要和功能选择负载均衡算法。

### 网卡成组策略

可以使用网卡成组将虚拟交换机连接至主机上的多个物理网卡，以增加交换机的网络带宽以及提供冗余。网卡组可在其成员之间分布流量，并在出现适配器故障或网络中断时提供被动故障切换。您可以在虚拟交换机或端口组级别设置 vSphere 标准交换机的网卡成组策略，以及在端口组或端口级别设置 vSphere Distributed Switch 的网卡成组策略。

**注意** 同一组内物理交换机上的所有端口必须位于第 2 层的同一广播域内。

### 负载均衡策略

负载均衡策略确定网络流量如何在网卡组中的网络适配器之间分布。vSphere 虚拟交换机仅对出站流量进行负载均衡。输入流量由物理交换机上的负载均衡策略控制。

有关每个负载均衡算法的详细信息，请参见第 82 页，“可用于虚拟交换机的负载均衡算法”。

### 网络故障检测策略

您可以指定下列方法之一以供虚拟交换机用于故障切换检测。

#### 仅链路状态

仅取决于网络适配器提供的链接状态。用于检测故障，如电缆移除和物理交换机电源故障。但是，链路状态不会检测以下配置错误：

- 物理交换机端口被跨接树阻止，或者错误地配置为不正确的 VLAN。

- 拔下了用于将物理交换机与其他网络设备（如上游交换机）相连接的电缆。

### 信标探测

发出并侦听物理网卡发送的以太网广播帧或信标探测，以检测组中所有物理网卡中存在的链路故障。ESXi 主机每秒发送一次信标数据包。信标探测对于检测距离 ESXi 主机最近的物理交换机的故障十分有用，此类故障不会导致主机发生链路关闭事件。

请将信标探测与组中的三个或更多网卡配合使用，因为 ESXi 可以检测单个适配器的故障。如果只分配两个网卡，而其中的一个网卡失去连接，则由于二者均不接收信标，因此所有数据包都发送到这两个上行链路，从而使交换机无法检测需要停用哪个网卡。在此类组中使用至少三个网卡，则允许出现  $n-2$  个故障，其中  $n$  是指该组出现不明确的状态时组中的网卡数量。

## 故障恢复策略

默认情况下，将对网卡组启用故障恢复策略。如果出现故障的物理网卡恢复联机状态，则虚拟交换机会将该网卡重新设置为活动状态，替换接替其位置的备用网卡。

如果在故障切换顺序中位居首位的物理网卡遇到间歇性故障，则故障恢复策略可能导致频繁更改使用的网卡。物理交换机可看到 MAC 地址频繁更改，在适配器联机时，物理交换机端口可能无法立即接受流量。要最大限度地减少此类延迟，可考虑在物理交换机上更改以下设置：

- 对已连接到 ESXi 主机的物理网卡禁用跨树协议 (STP)。
- 对于基于 Cisco 的网络，为访问接口启用 PortFast 模式或为中继接口启用 PortFast 中继模式。在初始化物理交换机端口期间，此操作可节省约 30 秒。
- 禁用中继协商。

## 通知交换机策略

使用通知交换机策略，您可以确定 ESXi 主机如何传达故障切换事件。当物理网卡连接到虚拟交换机或流量重新路由到网卡组中的其他物理网卡时，虚拟交换机将通过网络发送通知，以更新物理交换机上的查找表。为物理交换机发送通知可以在出现故障切换或使用 vSphere vMotion 进行迁移时获得最低延迟。

## 可用于虚拟交换机的负载平衡算法

可以在虚拟交换机上配置各种负载平衡算法，以确定网络流量在网卡组中的物理网卡之间如何分布。

- [基于源虚拟端口的路由](#) 第 83 页，  
虚拟交换机可根据 vSphere 标准交换机或 vSphere Distributed Switch 上的虚拟机端口 ID 选择上行链路。
- [基于源 MAC 哈希的路由](#) 第 83 页，  
虚拟交换机可基于虚拟机 MAC 地址选择虚拟机的上行链路。要计算虚拟机的上行链路，虚拟交换机将使用虚拟机 MAC 地址和网卡组中的上行链路数目。
- [基于 IP 哈希的路由](#) 第 83 页，  
虚拟交换机可根据每个数据包的源和目标 IP 地址选择虚拟机的上行链路。
- [基于物理网卡负载的路由](#) 第 84 页，  
基于物理网卡负载的路由以基于源虚拟端口的路由为基础，其中虚拟交换机将检查上行链路的实际负载，并采取措施以减少过载上行链路上的负载。仅适用于 vSphere Distributed Switch。
- [使用明确故障切换顺序](#) 第 85 页，  
没有可用于此策略的实际负载平衡。虚拟交换机始终使用“活动适配器”列表中按故障切换顺序位于最前列且符合故障切换检测标准的上行链路。如果活动列表中没有可用的上行链路，则虚拟交换机将使用备用列表中的上行链路。

基于源虚拟端口的路由

虚拟交换机可根据 vSphere 标准交换机或 vSphere Distributed Switch 上的虚拟机端口 ID 选择上行链路。

基于源虚拟端口的路由是 vSphere 标准交换机和 vSphere Distributed Switch 上的默认负载平衡方法。

ESXi 主机上运行的每个虚拟机在虚拟交换机上都有一个关联的虚拟端口 ID。要计算虚拟机的上行链路，虚拟交换机将使用虚拟机端口 ID 和网卡组中的上行链路数目。虚拟交换机为虚拟机选择上行链路后，只要该虚拟机在相同的端口上运行，就会始终通过此虚拟机的同一上行链路转发流量。除非在网卡组中添加或移除上行链路，否则虚拟交换机仅计算虚拟机上行链路一次。

当虚拟机在同一主机上运行时，虚拟机的端口 ID 固定不变。如果迁移或删除虚拟机，或者关闭虚拟机电源，则此虚拟机在虚拟交换机上的端口 ID 将变为空闲状态。虚拟交换机将停止向此端口发送流量，这会减少其关联的上行链路的总流量。如果打开虚拟机电源或迁移虚拟机，则虚拟机可能会出现在不同的端口上并使用与新端口关联的上行链路。

表 8-3 使用基于源虚拟端口的路由的注意事项

注意事项	描述
优势	<ul style="list-style-type: none"><li>■ 当组中虚拟网卡数大于物理网卡数时，流量分布均匀。</li><li>■ 资源消耗低，因为在大多数情况下，虚拟交换机仅计算虚拟机上行链路一次。</li><li>■ 无需在物理交换机上进行更改。</li></ul>
劣势	<ul style="list-style-type: none"><li>■ 虚拟交换机无法识别上行链路的流量负载，且不会对很少使用的上行链路的流量进行负载平衡。</li><li>■ 虚拟机可用的带宽受限于与相关端口 ID 关联的上行链路速度，除非该虚拟机具有多个虚拟网卡。</li></ul>

基于源 MAC 哈希的路由

虚拟交换机可基于虚拟机 MAC 地址选择虚拟机的上行链路。要计算虚拟机的上行链路，虚拟交换机将使用虚拟机 MAC 地址和网卡组中的上行链路数目。

表 8-4 使用基于源 MAC 哈希的路由的注意事项

注意事项	描述
优势	<ul style="list-style-type: none"><li>■ 与基于源虚拟端口的路由相比，可更均匀地分布流量，因为虚拟交换机会计算每个数据包的上行链路。</li><li>■ 虚拟机会使用相同的上行链路，因为 MAC 地址是静态地址。启动或关闭虚拟机不会更改虚拟机使用的上行链路。</li><li>■ 无需在物理交换机上进行更改。</li></ul>
劣势	<ul style="list-style-type: none"><li>■ 可用于虚拟机的带宽受限于与相关端口 ID 关联的上行链路速度，除非该虚拟机使用多个源 MAC 地址。</li><li>■ 资源消耗比基于源虚拟端口的路由更高，因为虚拟交换机会计算每个数据包的上行链路。</li><li>■ 虚拟交换机无法识别上行链路的负载，因此上行链路可能会过载。</li></ul>

基于 IP 哈希的路由

虚拟交换机可根据每个数据包的源和目标 IP 地址选择虚拟机的上行链路。

要计算虚拟机的上行链路，虚拟交换机会获取数据包中源和目标 IP 地址的最后一个八位字节并对其执行 XOR 运算，然后根据网卡组中的上行链路数将所得的结果用于另一个计算。结果是一个介于 0 和组中上行链路数减一之间的数字。例如，如果网卡组有四个上行链路，则结果是一个介于 0 和 3 之间的数字，因为每个数字与组中的一个网卡相关联。对于非 IP 数据包，虚拟交换机会从 IP 地址所在的帧或数据包中提取两个 32 位二进制值。

任何虚拟机都可根据源和目标 IP 地址使用网卡组中的任何上行链路。因此，每台虚拟机都可以使用网卡组中任何上行链路的带宽。如果虚拟机在包含大量独立虚拟机的环境中运行，则 IP 哈希算法可在组中的网卡之间均匀地分布流量。当虚拟机与多个目标 IP 地址通信时，虚拟交换机可为每个目标 IP 生成不同的哈希。因此，数据包可以使用虚拟交换机上的不同上行链路，从而可能实现更高的吞吐量。

但是，如果环境中包含的 IP 地址较少，则虚拟交换机可能会始终通过组中的一个上行链路传递流量。例如，如果一个应用程序服务器访问一个数据库服务器，则虚拟交换机会始终计算同一个上行链路，因为只存在一个源-目标对。

### 物理交换机配置

要确保 IP 哈希负载均衡运行正常，必须在物理交换机上配置以太通道。以太通道可以将多个网络适配器合并到单条逻辑链路中。如果将多个端口绑定到一个以太通道，则每次物理交换机接收不同端口上同一虚拟机 MAC 地址发出的数据包时，该交换机会正确更新其内容可寻址内存 (CAM) 表。

例如，如果物理交换机在端口 01 和 02 上收到 MAC 地址 A 发出的数据包，则该交换机会在其 CAM 表中创建 01-A 和 02-A 条目。因此，物理交换机会将入站流量分布到正确的端口。如果没有以太通道，则物理交换机会首先记录下在端口 01 上收到 MAC 地址 A 发出的数据包，然后将同一记录更新为在端口 02 上收到 MAC 地址 A 发出的数据包。因此，物理交换机只会转发端口 02 上的入站流量，并可能导致数据包无法到达其目标以及相应的上行链路过载。

### 限制和配置要求

- ESXi 主机支持单个物理交换机或堆栈交换机上的 IP 哈希成组。
- ESXi 主机仅支持静态模式下的 802.3ad 链路聚合。只能将静态以太通道与 vSphere 标准交换机配合使用。不支持 LACP。要使用 LACP，必须具有 vSphere Distributed Switch 5.1 及更高版本或 Cisco Nexus 1000V。如果启用 IP 哈希负载均衡但无 802.3ad 链路聚合（或者相反），则可能会遇到网络中断。
- 必须使用“仅链路状态”作为网络故障检测方法，并使用 IP 哈希负载均衡。
- 必须在“活动故障切换”列表中设置组的所有上行链路。“备用”和“未使用”列表必须为空。
- 以太通道中的端口数必须与组中的上行链路数相同。

### 使用基于 IP 哈希的路由的注意事项

注意事项	描述
优势	<ul style="list-style-type: none"> <li>■ 与基于源虚拟端口的路由和基于源 MAC 哈希的路由相比，可更均匀地分布负载，因为虚拟交换机会计算每个数据包的上行链路。</li> <li>■ 与多个 IP 地址通信的虚拟机可能实现更高的吞吐量。</li> </ul>
劣势	<ul style="list-style-type: none"> <li>■ 与其他负载均衡算法相比，资源消耗最高。</li> <li>■ 虚拟交换机无法识别上行链路的实际负载。</li> <li>■ 需要在物理网络上进行更改。</li> <li>■ 故障排除较为复杂。</li> </ul>

### 基于物理网卡负载的路由

基于物理网卡负载的路由以基于源虚拟端口的路由为基础，其中虚拟交换机将检查上行链路的实际负载，并采取以减少过载上行链路上的负载。仅适用于 vSphere Distributed Switch。

Distributed Switch 将使用虚拟机端口 ID 和网卡组中的上行链路数目来计算虚拟机的上行链路。Distributed Switch 将每 30 秒测试一次上行链路，如果上行链路的负载超过 75% 的使用率，则拥有最高 I/O 的虚拟机的端口 ID 将移到其他上行链路。

表 8-5 使用基于物理网卡负载的路由的注意事项

注意事项	描述
优势	<ul style="list-style-type: none"><li>■ 资源消耗较低，因为 Distributed Switch 仅计算一次虚拟机的上行链路并检查影响最小的上行链路。</li><li>■ Distributed Switch 可识别上行链路的负载，并在需要时负责减少其负载。</li><li>■ 无需在物理交换机上进行更改。</li></ul>
劣势	<ul style="list-style-type: none"><li>■ 可用于虚拟机的带宽受限于与 Distributed Switch 连接的上行链路。</li></ul>

使用明确故障切换顺序

没有可用于此策略的实际负载平衡。虚拟交换机始终使用“活动适配器”列表中按故障切换顺序位于最前列且符合故障切换检测标准的上行链路。如果活动列表中没有可用的上行链路，则虚拟交换机将使用备用列表中的上行链路。

在 vSphere 标准交换机或标准端口组上配置网卡绑定、故障切换和负载平衡

在组中包括两个或多个物理网卡可增加 vSphere 标准交换机或标准端口组的网络容量。配置故障切换顺序以确定如何在适配器发生故障时重新路由网络流量。选择负载平衡算法以确定标准交换机如何在组内物理网卡之间分布流量。

根据物理交换机的网络配置和标准交换机的拓扑配置网卡绑定、故障切换和负载平衡。有关详细信息，请参见第 81 页，“成组和故障切换策略”和第 82 页，“可用于虚拟交换机的负载平衡算法”。

如果在标准交换机上配置绑定和故障切换策略，该策略将传播到交换机中的所有端口组。如果在标准端口组上配置策略，该策略将替代从交换机继承的策略。

步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开网络，然后选择虚拟交换机。
- 3 导航到标准交换机或标准端口组的绑定和故障切换策略。

选项	操作
标准交换机	<ul style="list-style-type: none"><li>a 从列表中选择交换机。</li><li>b 单击编辑设置，然后选择绑定和故障切换。</li></ul>
标准端口组	<ul style="list-style-type: none"><li>a 选择端口组所在的交换机。</li><li>b 从交换机拓扑图中，选择标准端口组并单击编辑设置。</li><li>c 选择绑定和故障切换。</li><li>d 选择要替代的策略旁边的替代。</li></ul>

- 4 从负载平衡下拉菜单中，指定虚拟交换机如何对组内物理网卡之间的出站流量进行负载平衡。

选项	描述
基于源虚拟端口的路由	根据交换机上的虚拟端口 ID 选择上行链路。虚拟交换机为虚拟机或 VMkernel 适配器选择上行链路后，便始终会通过此虚拟机或 VMkernel 适配器的同一上行链路转发流量。
基于 IP 哈希的路由	根据每个数据包的源和目标 IP 地址哈希选择上行链路。对于非 IP 数据包，交换机在相应字段中使用这些数据来计算哈希值。 基于 IP 的绑定要求为物理交换机配置以太网通道。

选项	描述
<b>基于源 MAC 哈希的路由</b>	根据源以太网的哈希选择上行链路。
<b>使用明确故障切换顺序</b>	在活动适配器列表中，始终使用最前面的上行链路传递故障切换检测条件。此选项不会执行任何实际负载平衡。

- 5 从**网络故障检测**下拉菜单中，选择虚拟交换机用于故障切换检测的方法。

选项	描述
<b>仅链路状态</b>	仅取决于网络适配器提供的链路状态。该选项可用于检测故障，如电缆移除和物理交换机电源故障。
<b>信标探测</b>	发出并侦听组中所有网卡上的信标探测，并使用此信息结合链路状态来确定链接故障。ESXi 每秒发送一次信标数据包。 网卡必须处于活动/活动或活动/备用配置中，因为“未使用”状态中的网卡不会加入信标探测。

- 6 从**通知交换机**下拉菜单中，选择在出现故障切换时，标准交换机或 **Distributed Switch** 是否通知物理交换机。

**注意** 如果连接的虚拟机以单播模式使用 **Microsoft** 网络负载平衡，则将该选项设置为**否**。网络负载平衡在多播模式下运行时不存在任何问题。

- 7 从**故障恢复**下拉菜单中，选择物理适配器从故障恢复后是否返回到活动状态。

如果故障恢复设置为**是**（默认选择），则适配器将在恢复后立即返回到活动任务，并取代接替其位置的备用适配器（如果有）。

如果标准端口的故障恢复设置为**否**，则出现故障的适配器在恢复后仍为非活动状态，直至另有一个当前处于活动状态的适配器出现故障，必须进行更换。

- 8 通过配置“故障切换顺序”列表指定在出现故障切换时如何使用网卡组中的上行链路。

如果要使用部分上行链路而要保留另外一些上行链路，以备使用中的上行链路出现故障时的紧急情况，请使用向上箭头或向下箭头键将这些上行链路移至其他组中。

选项	描述
<b>活动适配器</b>	如果网络适配器连接运行正常并处于活动状态，则继续使用上行链路。
<b>备用适配器</b>	如果其中一个活动物理适配器停机，则使用此上行链路。
<b>未用的适配器</b>	不使用此上行链路。

- 9 单击**确定**。

## 在分布式端口组或分布式端口上配置网卡绑定、故障切换和负载平衡

在组中包括两个或多个物理网卡可增加分布式端口组或端口的网络容量。配置故障切换顺序以确定如何在适配器发生故障时重新路由网络流量。选择负载平衡算法以确定 **Distributed Switch** 如何在组内物理网卡之间进行流量负载平衡。

根据物理交换机的网络配置和 **Distributed Switch** 的拓扑配置网卡绑定、故障切换和负载平衡。有关详细信息，请参见第 81 页，“[成组和故障切换策略](#)”和第 82 页，“[可用于虚拟交换机的负载平衡算法](#)”。

如果为分布式端口组配置绑定和故障切换策略，策略将传播到组中的所有端口。如果为分布式端口配置策略，该策略将替代从组继承的策略。

### 前提条件

要替代分布式端口级别的策略，请为此策略启用端口级别替代选项。请参见第 43 页，“[在端口级别配置替代网络策略](#)”。

**步骤**

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 浏览分布式端口组或端口的绑定和故障切换策略。

选项	操作
分布式端口组	<ol style="list-style-type: none"> <li>a 在<b>操作</b>菜单中，选择<b>分布式端口组 &gt; 管理分布式端口组</b>。</li> <li>b 选择<b>绑定和故障切换</b>。</li> <li>c 选择端口组，然后单击<b>下一步</b>。</li> </ol>
分布式端口	<ol style="list-style-type: none"> <li>a 在<b>网络</b>选项卡上，单击<b>分布式端口组</b>，然后双击分布式端口组。</li> <li>b 在<b>端口</b>选项卡上，选择端口，然后单击<b>编辑分布式端口设置</b>。</li> <li>c 选择<b>绑定和故障切换</b>。</li> <li>d 选择要替代的属性旁边的<b>替代</b>。</li> </ol>

- 3 从**负载平衡**下拉菜单中，指定虚拟交换机如何对组内物理网卡之间的出站流量进行负载平衡。

选项	描述
基于源虚拟端口的路由	根据交换机上的虚拟端口 ID 选择上行链路。虚拟交换机为虚拟机或 VMkernel 适配器选择上行链路后，便始终会通过此虚拟机或 VMkernel 适配器的同一上行链路转发流量。
基于 IP 哈希的路由	根据每个数据包的源和目标 IP 地址哈希选择上行链路。对于非 IP 数据包，交换机在相应字段中使用这些数据来计算哈希值。 基于 IP 的绑定要求为物理交换机配置以太网通道。
基于源 MAC 哈希的路由	根据源以太网的哈希选择上行链路。
基于物理网卡负载的路由	可用于分布式端口组或分布式端口。根据连接到端口组或端口的物理网络适配器的当前负载选择上行链路。如果上行链路 75% 或更高持续 30 秒保持忙碌状态，主机代理交换机会将一部分虚拟机流量移至具有可用容量的物理适配器。
使用明确故障切换顺序	在活动适配器列表中，始终使用最前面的上行链路传递故障切换检测条件。此选项不会执行任何实际负载平衡。

- 4 从**网络故障检测**下拉菜单中，选择虚拟交换机用于故障切换检测的方法。

选项	描述
仅链路状态	仅取决于网络适配器提供的链路状态。该选项可用于检测故障，如电缆移除和物理交换机电源故障。
信标探测	发出并侦听组中所有网卡上的信标探测，并使用此信息结合链路状态来确定链接故障。ESXi 每秒发送一次信标数据包。 网卡必须处于活动/活动或活动/备用配置中，因为“未使用”状态中的网卡不会加入信标探测。

- 5 从**通知交换机**下拉菜单中，选择在出现故障切换时，标准交换机或 Distributed Switch 是否通知物理交换机。

**注意** 如果连接的虚拟机以单播模式使用 Microsoft 网络负载平衡，则将该选项设置为**否**。网络负载平衡在多播模式下运行时不存在任何问题。

- 6 从**故障恢复**下拉菜单中，选择物理适配器从故障恢复后是否返回到活动状态。

如果故障恢复设置为**是**（默认选择），则适配器将在恢复后立即返回到活动任务，并取代接替其位置的备用适配器（如果有）。

如果分布式端口的故障恢复设置为**否**，则仅当关联的虚拟机在运行时，出现故障的适配器才会在恢复后保持非活动状态。当**故障恢复**选项为**否**并且虚拟机已关闭电源时，如果所有活动的物理适配器发生故障，然后其中一个物理适配器恢复，则打开虚拟机电源后，虚拟网卡将连接到恢复的适配器而非待机适配器。关闭虚拟机电源然后再打开电源会将虚拟网卡重新连接到分布式端口。**Distributed Switch** 将该端口视为新添加的端口，并将其作为默认上行链路端口（即活动的上行链路适配器）。

- 7 通过配置“故障切换顺序”列表指定在出现故障切换时如何使用网卡组中的上行链路。

如果要使用部分上行链路而要保留另外一些上行链路，以备使用中的上行链路出现故障时的紧急情况，请使用向上箭头或向下箭头键将这些上行链路移至其他组中。

选项	描述
<b>活动适配器</b>	如果网络适配器连接运行正常并处于活动状态，则继续使用上行链路。
<b>备用适配器</b>	如果其中一个活动物理适配器停机，则使用此上行链路。
<b>未用的适配器</b>	不使用此上行链路。

- 8 查看设置并应用配置。

## VLAN 策略

VLAN 策略决定了 VLAN 在网络环境中的运行方式。

虚拟局域网 (VLAN) 是一组有着共同要求的主机，无论其物理位置如何，都像连接到同一广播域一样进行通信。VLAN 与物理局域网 (LAN) 的属性相同，但是 VLAN 允许终端站组合在一起，即使它们不在同一网络交换机上也是如此。

VLAN 策略的适用范围可以是分布式端口组和端口以及上行链路端口组和端口。

### 在分布式端口组或分布式端口上配置 VLAN 标记

要在所有分布式端口上全局应用 VLAN 标记，必须设置分布式端口组的 VLAN 策略。要以不同于父级分布式端口组的方式将通过该端口的虚拟流量与物理 VLAN 相整合，必须使用分布式端口的 VLAN 策略。

#### 前提条件

要替代分布式端口级别的策略，请为此策略启用端口级别替代选项。请参见第 43 页，“在端口级别配置替代网络策略”。

#### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 导航到分布式端口组或分布式端口的 VLAN 策略。

选项	操作
<b>分布式端口组</b>	<ol style="list-style-type: none"> <li>a 在<b>操作</b>菜单中，选择<b>分布式端口组 &gt; 管理分布式端口组</b>。</li> <li>b 选择 <b>VLAN</b>，然后单击<b>下一步</b>。</li> <li>c 选择端口组，然后单击<b>下一步</b>。</li> </ol>
<b>分布式端口</b>	<ol style="list-style-type: none"> <li>a 在<b>网络</b>选项卡上，单击<b>分布式端口组</b>，然后双击分布式端口组。</li> <li>b 在<b>端口</b>选项卡上，选择端口，然后单击<b>编辑分布式端口设置</b>图标。</li> <li>c 选择 <b>VLAN</b>。</li> <li>d 选择要替代的属性旁边的<b>替代</b>。</li> </ol>



- 3 从 **VLAN 类型** 下拉菜单中选择 **VLAN** 流量筛选和标记的类型，然后单击 **下一步**。

选项	描述
无	不使用 VLAN。 如果是外部交换机标记，则使用此选项。
VLAN	使用 <b>VLAN ID</b> 字段中的 ID 来标记流量。 为虚拟交换机标记键入介于 1 和 4094 之间的数字。
VLAN 中继	将 ID 在 <b>VLAN 中继范围</b> 内的 VLAN 流量传递到客户机操作系统。可以使用逗号分隔的列表来设置多个范围和各个 VLAN。 为虚拟客户机标记使用此选项。
专用 VLAN	将流量与在 Distributed Switch 上创建的专用 VLAN 相关联。

- 4 查看设置并应用配置。

### 配置上行链路端口组或上行链路端口上的 VLAN 标记

通常，要为所有成员上行链路配置 VLAN 流量处理，必须设置上行链路端口的 VLAN 策略。要以不同于父级上行链路端口组的方式处理通过该端口的 VLAN 流量，必须设置上行链路的 VLAN 策略。

在上行链路端口级别使用 VLAN 策略可将 VLAN ID 的中继范围传播至物理网络适配器以执行流量筛选。如果物理网络适配器支持按 VLAN 筛选，这些网络适配器将丢弃来自其他 VLAN 的数据包。设置一个中继范围可改进网络连接性能，因为物理网络适配器负责筛选流量（而非组中的上行链路端口）。

如果您的物理网络适配器不支持 VLAN 筛选，这些 VLAN 仍不会受到阻止。此时，可在分布式端口组或分布式端口上配置 VLAN 筛选。

有关 VLAN 筛选支持的信息，请参见适配器供应商提供的技术文档。

#### 前提条件

要替代端口级别的 VLAN 策略，请启用端口级别替代。请参见第 43 页，“在端口级别配置替代网络策略”。

#### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在 **网络** 选项卡上，单击 **上行链路端口组**。
- 3 导航到上行链路端口组或端口的 VLAN 策略。

选项	操作
上行链路端口组	a 右键单击列表中的上行链路端口组，然后选择 <b>编辑设置</b> 。 b 单击 <b>VLAN</b> 。
上行链路端口	a 双击上行链路端口组。 b 在 <b>端口</b> 选项卡上，选择端口，然后单击 <b>编辑分布式端口设置</b> 选项卡。 c 单击 <b>VLAN</b> 并选中 <b>替代</b> 。

- 4 键入要传播到物理网络适配器的 **VLAN 中继范围** 值。  
要中继多个范围和各个 VLAN，可用逗号分隔各个条目。
- 5 单击 **确定**。

## 安全策略

网络安全策略可保护流量免受 MAC 地址模拟和有害端口扫描的威胁

在网络协议堆栈的第 2 层（数据链路层）执行标准交换机或 Distributed Switch 的安全策略。安全策略的三大要素是杂乱模式、MAC 地址更改和伪信号。有关潜在网络威胁的信息，请参见 *vSphere 安全性* 文档。

### 配置 vSphere Standard Switch 或标准端口组的安全策略

对于 vSphere Standard Switch，您可以在虚拟机的客户机操作系统中配置安全策略以拒绝 MAC 地址和混杂模式更改。可以替代从单个端口组上的标准交换机继承的安全策略。

#### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开网络，然后选择虚拟交换机。
- 3 导航到标准交换机或端口组的安全策略。

选项	操作
<b>vSphere 标准交换机</b>	<ol style="list-style-type: none"> <li>a 在列表选择一个标准交换机。</li> <li>b 单击 <b>编辑设置</b>。</li> <li>c 选择 <b>安全</b>。</li> </ol>
<b>标准端口组</b>	<ol style="list-style-type: none"> <li>a 选择端口组所在的标准交换机。</li> <li>b 在拓扑图中，选择一个标准端口组。</li> <li>c 单击 <b>编辑设置</b>。</li> <li>d 选择 <b>安全</b>，然后选择选项旁边的 <b>替代</b> 以替代。</li> </ol>

- 4 拒绝或接受与标准交换机或端口组相连的虚拟机的客户机操作系统中混杂模式激活或 MAC 地址更改。

选项	描述
<b>混杂模式</b>	<ul style="list-style-type: none"> <li>■ <b>拒绝</b>。虚拟机网络适配器仅接收发送到虚拟机的帧。</li> <li>■ <b>接受</b>。虚拟交换机会将所有帧转发到符合虚拟机网络适配器所连接端口的活动 VLAN 策略的虚拟机。</li> </ul> <p><b>注意</b> 混杂模式是一种不安全的运行模式。防火墙、端口扫描程序、入侵检测系统必须在混杂模式下运行。</p>
<b>MAC 地址更改</b>	<ul style="list-style-type: none"> <li>■ <b>拒绝</b>。如果客户机操作系统将虚拟机的有效 MAC 地址更改为与虚拟机网络适配器的 MAC 地址（在 <code>.vmx</code> 配置文件中设置）不同的值，则交换机会丢弃所有到适配器的入站帧。</li> </ul> <p>如果客户机操作系统将虚拟机的有效 MAC 地址更改回虚拟机网络适配器的 MAC 地址，则虚拟机将重新接收帧。</p> <ul style="list-style-type: none"> <li>■ <b>接受</b>。如果客户机操作系统将虚拟机的有效 MAC 地址更改为与虚拟机网络适配器的 MAC 地址不同的值，则交换机会允许传递到新地址的帧。</li> </ul>
<b>伪信号</b>	<ul style="list-style-type: none"> <li>■ <b>拒绝</b>。如果从虚拟机适配器发出的出站帧的源 MAC 地址不同于 <code>.vmx</code> 配置文件中的源 MAC 地址，则交换机会丢弃该出站帧。</li> <li>■ <b>接受</b>。交换机不执行筛选，并允许所有出站帧通过。</li> </ul>

- 5 单击 **确定**。

## 配置分布式端口组或分布式端口的安全策略

可以对分布式端口组设置安全策略，以允许或拒绝在与端口组关联的虚拟机的客户机操作系统中启用混杂模式和 MAC 地址更改。可以替代从单个端口上的分布式端口组继承的安全策略。

### 前提条件

要替代分布式端口级别的策略，请为此策略启用端口级别替代选项。请参见第 43 页，“在端口级别配置替代网络策略”。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 导航到分布式端口组或端口的安全策略。

选项	操作
分布式端口组	<ol style="list-style-type: none"> <li>a 在<b>操作</b>菜单中，选择<b>分布式端口组 &gt; 管理分布式端口组</b>。</li> <li>b 选择<b>安全</b>。</li> <li>c 选择端口组，然后单击<b>下一步</b>。</li> </ol>
分布式端口	<ol style="list-style-type: none"> <li>a 在<b>网络</b>选项卡上，单击<b>分布式端口组</b>，然后双击分布式端口组。</li> <li>b 在<b>端口</b>选项卡上，选择端口，然后单击<b>编辑分布式端口设置</b>图标。</li> <li>c 选择<b>安全</b>。</li> <li>d 选择要替代的属性旁边的<b>替代</b>。</li> </ol>

- 3 拒绝或接受与分布式端口组或端口相连的虚拟机的客户机操作系统中混杂模式激活或 MAC 地址更改。

选项	描述
混杂模式	<ul style="list-style-type: none"> <li>■ <b>拒绝</b>。虚拟机网络适配器仅接收发送到虚拟机的帧。</li> <li>■ <b>接受</b>。虚拟交换机会将所有帧转发到符合虚拟机网络适配器所连接端口的活动 VLAN 策略的虚拟机。</li> </ul> <p><b>注意</b> 混杂模式是一种不安全的运行模式。防火墙、端口扫描程序、入侵检测系统必须在混杂模式下运行。</p>
MAC 地址更改	<ul style="list-style-type: none"> <li>■ <b>拒绝</b>。如果客户机操作系统将虚拟机的有效 MAC 地址更改为与虚拟机网络适配器的 MAC 地址（在 <code>.vmx</code> 配置文件中设置）不同的值，则交换机会丢弃所有到适配器的入站帧。</li> </ul> <p>如果客户机操作系统将虚拟机的有效 MAC 地址更改回虚拟机网络适配器的 MAC 地址，则虚拟机将重新接收帧。</p> <ul style="list-style-type: none"> <li>■ <b>接受</b>。如果客户机操作系统将虚拟机的有效 MAC 地址更改为与虚拟机网络适配器的 MAC 地址不同的值，则交换机会允许传递到新地址的帧。</li> </ul>
伪信号	<ul style="list-style-type: none"> <li>■ <b>拒绝</b>。如果从虚拟机适配器发出的出站帧的源 MAC 地址不同于 <code>.vmx</code> 配置文件中的源 MAC 地址，则交换机会丢弃该出站帧。</li> <li>■ <b>接受</b>。交换机不执行筛选，并允许所有出站帧通过。</li> </ul>

- 4 查看设置并应用配置。

## 流量调整策略

流量调整策略是由平均带宽、峰值带宽和突发大小所定义的。可以为每个端口组和每个分布式端口或分布式端口组建立流量调整策略。

ESXi 调整标准交换机上的出站网络流量以及分布式交换机上的入站和出站流量。流量调整功能会限制可用于端口的网络带宽，但也可以将其配置为允许流量突发，使流量以更高的速度通过端口。

<b>平均带宽</b>	规定某段时间内允许通过端口的平均每秒位数。此数值是允许的平均负载。
<b>带宽峰值</b>	端口发送或接收突发流量时，每秒允许通过端口的最大位数。此数值会限制端口经历额外突发时所用的带宽。
<b>突发大小</b>	突发中所允许的最大字节数。如果设置了此参数，则在端口没有使用为其分配的所有带宽时可能会获取额外的突发。当端口所需带宽大于平均带宽所指定的值时，如果有额外突发可用，则可能会临时允许以更高的速度传输数据。此参数限制在额外突发中累积的字节数，使流量以更高的速度传输。

## 配置 vSphere Standard Switch 或标准端口组的流量调整

ESXi 允许您调整标准交换机或端口组的出站流量。流量调整程序可限制任意端口的可用网络带宽，但也可将其配置为临时允许流量突发，使流量以更高的速度通过端口。

在交换机或端口组级别设置的流量调整策略适用于加入了该交换机或端口组的每个单独的端口。例如，如果在标准端口组上设置 100000 Kbps 的平均带宽，则一段时间内平均 100000 Kbps 可通过与标准端口组关联的每个端口。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开网络，然后选择虚拟交换机。
- 3 导航到标准交换机或端口组的流量调整策略。

选项	操作
<b>vSphere 标准交换机</b>	<ol style="list-style-type: none"> <li>a 在列表中选择标准交换机。</li> <li>b 单击 <b>编辑设置</b>。</li> <li>c 选择 <b>流量调整</b>。</li> </ol>
<b>标准端口组</b>	<ol style="list-style-type: none"> <li>a 选择端口组所在的标准交换机。</li> <li>b 在拓扑图中，选择一个标准端口组。</li> <li>c 单击 <b>编辑设置</b>。</li> <li>d 选择 <b>流量调整</b>，然后选择选项旁边的 <b>替代</b> 以替代。</li> </ol>

- 4 配置流量调整策略。

选项	描述
<b>状态</b>	针对与标准交换机或端口组关联的每个端口启用了网络带宽分配量的设置限制。
<b>平均带宽</b>	设定每秒允许通过端口的位数，这是一段时间内的平均值（允许的平均负载）。

选项	描述
<b>带宽峰值</b>	发送流量突发时，每秒钟允许通过端口的最大传输位数。该设置是指流量突发时端口使用的最大带宽。此参数永远不能小于平均带宽。
<b>突发大小</b>	突发中所允许的最大字节数。如果设置了此参数，则在端口没有使用为其分配的所有带宽时可能会获取额外的突发。当端口所需带宽大于平均带宽所指定的值时，如果有额外突发可用，则端口可能会临时以更高的速度传输数据。该参数是指流量突发时可累积且以更高速度传输的最大字节数。

- 5 针对每个流量调整策略（**平均带宽**、**峰值带宽**和**突发大小**），输入带宽值。
- 6 单击**确定**。

## 编辑分布式端口组或分布式端口的流量调整策略

可以调整 vSphere 分布式端口组或分布式端口上的入站和出站流量。流量调整程序可限制组中任意端口的网络带宽，但也可将其配置为临时允许流量“突发”，使流量以更高的速度通过端口。

在分布式端口组级别设置的流量调整策略适用于加入该端口组的每一个单独端口。例如，如果在分布式端口组上设置 100000 Kbps 的平均带宽，则与分布式端口组相关联的每个端口在一段时间内平均可通过 100000 Kbps。

### 前提条件

要替代分布式端口级别的策略，请为此策略启用端口级别替代选项。请参见第 43 页，“在端口级别配置替代网络策略”。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 导航到分布式端口组或端口的流量调整策略。

选项	操作
<b>分布式端口组</b>	<ol style="list-style-type: none"> <li>a 在<b>操作</b>菜单中，选择<b>分布式端口组 &gt; 管理分布式端口组</b>。</li> <li>b 选择<b>流量调整</b>。</li> <li>c 选择端口组，然后单击<b>下一步</b>。</li> </ol>
<b>分布式端口</b>	<ol style="list-style-type: none"> <li>a 在<b>网络</b>选项卡上，单击<b>分布式端口组</b>，然后双击分布式端口组。</li> <li>b 在<b>端口</b>选项卡上，选择端口，然后单击<b>编辑分布式端口设置</b>图标。</li> <li>c 选择<b>流量调整</b>。</li> <li>d 选择要替代的属性旁边的<b>替代</b>。</li> </ol>

- 3 配置流量调整策略。

**注意** 流量根据交换机而非主机中的通信方向分为输入流量和输出流量两类。

选项	描述
<b>状态</b>	通过使用 <b>状态</b> 下拉菜单启用 <b>输入流量调整</b> 或 <b>输出流量调整</b> 。
<b>平均带宽</b>	设定每秒允许通过端口的位数，这是一段时间内的平均值，即允许的平均负载。
<b>峰值带宽</b>	端口在发送或接收流量突发时，每秒钟允许通过端口的最大传输位数。该参数是指流量突发时端口使用的最大带宽。
<b>突发大小</b>	突发中所允许的最大字节数。如果设置了此参数，则在端口没有使用为其分配的所有带宽时可能会获取额外的突发。当端口所需带宽大于平均带宽所指定的值时，如果有额外突发可用，则端口可能会临时以更高的速度传输数据。该参数是指流量突发时可累积且以更高速度传输的最大字节数。

- 4 查看设置并应用配置。

## 资源分配策略

可以使用资源分配策略将分布式端口或端口组与用户创建的网络资源池关联。通过此策略可以更有效地控制为端口或端口组指定的带宽。

有关创建和配置网络资源池的信息，请参见第 145 页，第 11 章“vSphere Network I/O Control”。

### 编辑分布式端口组的资源分配策略

通过将分布式端口组与网络资源池关联，您可更有效地控制为分布式端口组分配的带宽。

#### 前提条件

- 在 Distributed Switch 上启用 Network I/O Control。请参见第 148 页，“在 vSphere Distributed Switch 上启用 Network I/O Control”。
- 创建并配置网络资源池。请参见第 154 页，“创建网络资源池”。

#### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
  - 2 在导航器中右键单击 Distributed Switch，然后选择**分布式端口组 > 管理分布式端口组**。
  - 3 选中**资源分配**复选框，然后单击**下一步**。
  - 4 选择要配置的分布式端口组，然后单击**下一步**。
  - 5 在网络资源池中添加或移除分布式端口组，然后单击**下一步**。
    - 要添加分布式端口组，请从**网络资源池**下拉菜单中选择用户定义的资源池。
    - 要移除分布式端口组，请从**网络资源池**下拉菜单中选择**默认**。
  - 6 在**即将完成**部分中查看您的设置，然后单击**完成**。
- 使用上一步按钮更改任意设置。

### 编辑分布式端口的资源分配策略

如果在 vSphere Distributed Switch 中使用 Network I/O Control 版本 2，则可以明确地将分布式端口与用户定义的资源池关联，以使用 Network I/O Control 控制提供给连接到端口的虚拟机的带宽。

#### 前提条件

- 确认 Network I/O Control 为版本 2。
- 在 Distributed Switch 上启用 Network I/O Control。请参见第 148 页，“在 vSphere Distributed Switch 上启用 Network I/O Control”。
- 在 Network I/O Control 版本 2 中创建并配置网络资源池。请参见第 159 页，“在 Network I/O Control 版本 2 中创建网络资源池”。
- 为资源分配策略启用端口级别替代。请参见第 43 页，“在端口级别配置替代网络策略”。

#### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在**配置**选项卡上，展开**更多**，并单击**端口**。
- 3 从列表中选择端口，然后单击**编辑分布式端口设置**图标。
- 4 选择**属性**。

- 5 在“网络资源池”下单击**替代**复选框，并从下拉菜单中向该端口分配网络资源池。
- 如果未为资源分配策略启用端口级别替代，则该选项将处于禁用状态。
- 要将分布式端口与资源池关联，请选择用户定义的资源池。
  - 要移除分布式端口与资源池之间的关联，请选择**默认**。
- 6 单击**确定**。

## 监控策略

监控策略在分布式端口或端口组上启用或禁用 NetFlow 监控。

在 vSphere Distributed Switch 级别配置 NetFlow 设置。请参见第 185 页，“配置 vSphere Distributed Switch 的 NetFlow 设置”。

### 在分布式端口组或分布式端口上启用或禁用 NetFlow 监控

启用 NetFlow 以监控通过分布式端口组的端口或通过单个分布式端口的 IP 数据包。

在 vSphere Distributed Switch 上配置 NetFlow 设置。请参见第 185 页，“配置 vSphere Distributed Switch 的 NetFlow 设置”

#### 前提条件

要替代分布式端口级别的策略，请为此策略启用端口级别替代选项。请参见第 43 页，“在端口级别配置替代网络策略”。

#### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 导航到分布式端口组或分布式端口的监控策略。

选项	操作
分布式端口组	a 在 <b>操作</b> 菜单中，选择 <b>分布式端口组 &gt; 管理分布式端口组</b> 。
	b 选择 <b>监控</b> 。
	c 选择端口组，然后单击 <b>下一步</b> 。
分布式端口	a 在 <b>网络</b> 选项卡上，单击 <b>分布式端口组</b> ，然后双击分布式端口组。
	b 在 <b>端口</b> 选项卡上，选择端口，然后单击 <b>编辑分布式端口设置</b> 图标。
	c 选择 <b>监控</b> 。
	d 选择要替代的属性旁边的 <b>替代</b> 。

- 3 从 **NetFlow** 下拉菜单中启用或禁用 NetFlow，然后单击**下一步**。
- 4 验证设置并应用配置。

## 流量筛选和标记策略

在 vSphere Distributed Switch 5.5 及更高版本中，通过使用流量筛选和标记策略，您可以避免虚拟网络进入有害的流量和遭受安全攻击，或将 QoS 标记应用于某种类型的流量。

流量筛选和标记策略表示一组有序的网络流量规则，用于对通过 Distributed Switch 端口的数据流实施安全保护和应用 QoS 标记。一般而言，规则包括流量限定符以及限制或设置匹配流量优先级的操作。

vSphere Distributed Switch 将规则应用于数据流中不同位置的流量。Distributed Switch 将流量筛选规则应用于虚拟网络适配器与分布式端口之间的数据路径，或将上行链路规则应用于上行链路端口与物理网络适配器之间的数据路径。

## 分布式端口组或上行链路端口组的流量筛选和标记

在分布式端口组级别或上行链路端口组级别设置流量规则，从而引入对通过虚拟机、VMkernel 适配器或物理适配器的流量访问的筛选和优先级标记功能。

- [启用分布式端口组或上行链路端口组的流量筛选和标记](#) 第 96 页，  
如果要在加入端口组的所有虚拟机网络适配器或上行链路适配器上配置流量安全和标记，请为该组启用流量筛选和标记策略。
- [标记分布式端口组或上行链路端口组的流量](#) 第 96 页，  
可向在带宽、低延迟等方面具有较高网络要求的流量（如 VoIP 和流视频）分配优先级标记。您可以在网络协议堆栈的第 2 层使用 CoS 标记或在第 3 层使用 DSCP 标记来标记流量。
- [筛选分布式端口组或上行链路端口组的流量](#) 第 98 页，  
允许或停止流量，以确保流经分布式端口组或上行链路端口组的端口的数据的安全。
- [使用分布式端口组或上行链路端口组上的网络流量规则](#) 第 99 页，  
定义在分布式端口组或上行链路端口组中的流量规则，以引入处理与虚拟机或物理适配器相关的流量的策略。可以筛选特定流量或描述其 QoS 需求。
- [禁用分布式端口组或上行链路端口组的流量筛选和标记](#) 第 100 页，  
通过禁用流量筛选和标记策略来允许流量流向虚拟机或物理适配器，而无需进行与安全或 QoS 相关的其他控制。

### 启用分布式端口组或上行链路端口组的流量筛选和标记

如果要在加入端口组的所有虚拟机网络适配器或上行链路适配器上配置流量安全和标记，请为该组启用流量筛选和标记策略。

---

**注意** 您可以对特定端口禁用流量筛选和标记策略，以避免处理流经该端口的流量。请参见第 106 页，“[禁用分布式端口或上行链路端口的流量筛选和标记](#)”。

---

#### 步骤

- 1 在 vSphere Web Client 中查找分布式端口组或上行链路端口组。
  - a 选择 Distributed Switch，然后单击**网络**选项卡。
  - b 单击**分布式端口组**以查看分布式端口组列表，或单击**上行链路端口组**以查看上行链路端口组列表。
- 2 右键单击端口组，然后选择**编辑设置**。
- 3 选择**流量筛选和标记**。
- 4 从**状态**下拉菜单中选择**已启用**。
- 5 单击**确定**。

#### 下一步

对流经分布式端口组的端口或流经上行链路端口组的数据设置流量标记或筛选。请参见第 96 页，“[标记分布式端口组或上行链路端口组的流量](#)”和第 98 页，“[筛选分布式端口组或上行链路端口组的流量](#)”。

### 标记分布式端口组或上行链路端口组的流量

可向在带宽、低延迟等方面具有较高网络要求的流量（如 VoIP 和流视频）分配优先级标记。您可以在网络协议堆栈的第 2 层使用 CoS 标记或在第 3 层使用 DSCP 标记来标记流量。

优先级标记是一种流量标记机制，用于标记 QoS 需求较高的流量。网络可以利用这一机制识别不同类的流量。网络设备可以根据每个类的优先级和要求来处理其中的流量。



您也可以重新标记流量，以便提高或降低流量的重要性。通过使用较低的 QoS 标记，可以限制客户机操作系统中标记的数据。

### 步骤

- 1 在 vSphere Web Client 中查找分布式端口组或上行链路端口组。
  - a 选择 Distributed Switch，然后单击**网络**选项卡。
  - b 单击**分布式端口组**以查看分布式端口组列表，或单击**上行链路端口组**以查看上行链路端口组列表。
- 2 右键单击端口组，然后选择**编辑设置**。
- 3 选择**流量筛选和标记**。
- 4 如果已禁用“流量筛选和标记”，可从**状态**下拉菜单中将其启用。
- 5 单击**新建**以创建新规则，或者选择一个规则并单击**编辑**以编辑该规则。
- 6 在网络流量规则对话框中，从**操作**下拉菜单中选择**标记**选项。
- 7 为规则范围内的流量设置优先级标记。

选项	描述
<b>CoS 值</b>	在第 2 层网络中使用 CoS 优先级标记来标记与规则匹配的流量。请选择 <b>更新 CoS 标记</b> ，并键入一个介于 0 到 7 之间的值。
<b>DSCP 值</b>	在第 3 层网络中使用 DSCP 标记来标记与规则关联的流量。请选择 <b>更新 DSCP 值</b> ，并键入一个介于 0 到 63 之间的值。

- 8 指定此规则所适用的流量种类。

要确定某一数据流是否位于要标记或筛选的规则范围内，vSphere Distributed Switch 将检查流量的方向、源和目标等属性、VLAN、下一级别协议、基础架构流量类型等。

- a 从**流量方向**下拉菜单中，选择流量必须为输入、输出还是同时为这两者，才能使规则将其视为匹配。此方向还会影响您识别流量源和目标的方式。

- b 通过使用系统数据类型限定符、第 2 层数据包属性和第 3 层数据包属性，可以设置数据包要与规则匹配而需要具备的属性。

一个限定符表示一组与某个网络连接层相关的匹配条件。可以将流量与系统数据类型、第 2 层流量属性和第 3 层流量属性进行匹配。可以使用特定网络连接层的限定符，也可以结合使用多个限定符，以便更精确地匹配数据包。

- 使用系统流量限定符将数据包与流经组端口的虚拟基础架构数据的类型进行匹配。例如，您可以对传输到网络存储的数据选择 NFS。
- 使用 MAC 流量限定符可根据 MAC 地址、VLAN ID 和下一级别协议匹配数据包。  
可以使用虚拟客户机标记 (VGT) 在分布式端口组上查找具有某个 VLAN ID 的流量。如果要在虚拟交换机标记 (VST) 处于活动状态时将流量与 VLAN ID 进行匹配，请对上行链路端口组或上行链路端口使用一个规则。
- 使用 IP 流量限定符可根据 IP 版本、IP 地址以及下一级别协议和端口匹配数据包。

- 9 在规则对话框中，单击**确定**以保存该规则。

### 示例：IP 语音流量标记

IP 语音 (VoIP) 流在低丢弃和低延迟方面具有特殊的 QoS 要求。与 VoIP 的会话发起协议 (SIP) 相关的流量通常有一个等于 26 的 DSCP 标记，该标记值表示保证转发等级为 3 且丢弃概率为低 (AF31)。

例如，要标记到子网 192.168.2.0/24 的出站 SIP UDP 数据包，可以使用以下规则：

规则参数	参数值
操作	标记
DSCP 值	26
流量方向	输出
流量限定符	IP 限定符
协议	UDP
目标端口	5060
源地址	与 192.168.2.0 匹配的前缀长度为 24 的 IP 地址

## 筛选分布式端口组或上行链路端口组的流量

允许或停止流量，以确保流经分布式端口组或上行链路端口组的端口的数据的安全。

### 步骤

- 1 在 vSphere Web Client 中查找分布式端口组或上行链路端口组。
  - a 选择 Distributed Switch，然后单击**网络**选项卡。
  - b 单击**分布式端口组**以查看分布式端口组列表，或单击**上行链路端口组**以查看上行链路端口组列表。
- 2 右键单击端口组，然后选择**编辑设置**。
- 3 选择**流量筛选和标记**。
- 4 如果已禁用“流量筛选和标记”，可从**状态**下拉菜单中将其启用。
- 5 单击**新建**以创建新规则，或者选择一个规则并单击**编辑**以编辑该规则。
- 6 在“网络流量规则”对话框中，使用“操作”选项以允许流量通过分布式端口组或上行链路端口组的端口，或对其进行限制。
- 7 指定此规则所适用的流量种类。
 

要确定某一数据流是否位于要标记或筛选的规则范围内，vSphere Distributed Switch 将检查流量的方向、源和目标等属性、VLAN、下一级别协议、基础架构流量类型等。

  - a 从**流量方向**下拉菜单中，选择流量必须为输入、输出还是同时为这两者，才能使规则将其视为匹配。此方向还会影响您识别流量源和目标的方式。
  - b 通过使用系统数据类型限定符、第 2 层数据包属性和第 3 层数据包属性，可以设置数据包要与规则匹配而需要具备的属性。
 

一个限定符表示一组与某个网络连接层相关的匹配条件。可以将流量与系统数据类型、第 2 层流量属性和第 3 层流量属性进行匹配。可以使用特定网络连接层的限定符，也可以结合使用多个限定符，以便更精确地匹配数据包。

    - 使用系统流量限定符将数据包与流经组端口的虚拟基础架构数据的类型进行匹配。例如，您可以对传输到网络存储的数据选择 NFS。
    - 使用 MAC 流量限定符可根据 MAC 地址、VLAN ID 和下一级别协议匹配数据包。
 

可以使用虚拟客户机标记 (VGT) 在分布式端口组上查找具有某个 VLAN ID 的流量。如果要在虚拟交换机标记 (VST) 处于活动状态时将流量与 VLAN ID 进行匹配，请对上行链路端口组或上行链路端口使用一个规则。
    - 使用 IP 流量限定符可根据 IP 版本、IP 地址以及下一级别协议和端口匹配数据包。
- 8 在规则对话框中，单击**确定**以保存该规则。

## 使用分布式端口组或上行链路端口组上的网络流量规则

定义在分布式端口组或上行链路端口组中的流量规则，以引入处理与虚拟机或物理适配器相关的流量的策略。可以筛选特定流量或描述其 QoS 需求。

**注意** 可以在端口级别替代流量筛选和标记的策略规则。请参见第 104 页，“使用分布式端口或上行链路端口上的网络流量规则”。

- [查看分布式端口组或上行链路组的流量规则](#) 第 99 页，  
查看形成分布式端口组或上行链路端口组的流量筛选和屏蔽策略的流量规则。
- [编辑分布式端口组或上行链路端口组的流量规则](#) 第 99 页，  
可以创建或编辑流量规则，然后使用其参数在分布式端口组或上行链路端口组上配置用于筛选或标记流量的策略。
- [更改分布式端口组或上行链路端口组的规则优先级](#) 第 100 页，  
对组成分布式端口组或上行链路端口组的流量筛选和标记策略的规则进行重新排序可改变处理流量的操作顺序。
- [删除分布式端口组或上行链路端口组的流量规则](#) 第 100 页，  
删除分布式端口组或上行链路端口组上的流量规则，以便以特定方式停止处理数据包流向虚拟机或物理适配器。

### 查看分布式端口组或上行链路组的流量规则

查看形成分布式端口组或上行链路端口组的流量筛选和屏蔽策略的流量规则。

#### 步骤

- 1 在 vSphere Web Client 中查找分布式端口组或上行链路端口组。
  - a 选择 Distributed Switch，然后单击**网络**选项卡。
  - b 单击**分布式端口组**以查看分布式端口组列表，或单击**上行链路端口组**以查看上行链路端口组列表。
- 2 右键单击端口组，然后选择**编辑设置**。
- 3 选择**流量筛选和标记**。
- 4 如果已禁用“流量筛选和标记”，可从**状态**下拉菜单中将其启用。
- 5 检查**操作**以查看此规则是否对流量进行了筛选（允许或拒绝），或者是否对具有特殊 QoS 需求的流量进行了标记（标记）。
- 6 从上方的列表中，选择您要查看流量查找条件的规则。  
此规则的流量限定参数将显示在流量限定符列表中。

### 编辑分布式端口组或上行链路端口组的流量规则

可以创建或编辑流量规则，然后使用其参数在分布式端口组或上行链路端口组上配置用于筛选或标记流量的策略。

#### 步骤

- 1 在 vSphere Web Client 中查找分布式端口组或上行链路端口组。
  - a 选择 Distributed Switch，然后单击**网络**选项卡。
  - b 单击**分布式端口组**以查看分布式端口组列表，或单击**上行链路端口组**以查看上行链路端口组列表。
- 2 右键单击端口组，然后选择**编辑设置**。
- 3 选择**流量筛选和标记**。

- 4 如果已禁用“流量筛选和标记”，可从**状态**下拉菜单中将其启用。
- 5 单击**新建**以创建新规则，或者选择一个规则并单击**编辑**以编辑该规则。

### 下一步

为网络流量规则命名，并拒绝、允许或标记目标流量。

### 更改分布式端口组或上行链路端口组的规则优先级

对组成分布式端口组或上行链路端口组的流量筛选和标记策略的规则进行重新排序可改变处理流量的操作顺序。

vSphere Distributed Switch 将按严格的顺序应用网络流量规则。如果某个数据包已符合某个规则，则该数据包可能不会传递到策略中的下一个规则。

### 步骤

- 1 在 vSphere Web Client 中查找分布式端口组或上行链路端口组。
  - a 选择 Distributed Switch，然后单击**网络**选项卡。
  - b 单击**分布式端口组**以查看分布式端口组列表，或单击**上行链路端口组**以查看上行链路端口组列表。
- 2 右键单击端口组，然后选择**编辑设置**。
- 3 选择**流量筛选和标记**。
- 4 如果已禁用“流量筛选和标记”，可从**状态**下拉菜单中将其启用。
- 5 选择一个规则，并使用箭头按钮来更改其优先级。
- 6 单击**确定**应用更改。

### 删除分布式端口组或上行链路端口组的流量规则

删除分布式端口组或上行链路端口组上的流量规则，以便以特定方式停止处理数据包流向虚拟机或物理适配器。

### 步骤

- 1 在 vSphere Web Client 中查找分布式端口组或上行链路端口组。
  - a 选择 Distributed Switch，然后单击**网络**选项卡。
  - b 单击**分布式端口组**以查看分布式端口组列表，或单击**上行链路端口组**以查看上行链路端口组列表。
- 2 右键单击端口组，然后选择**编辑设置**。
- 3 选择**流量筛选和标记**。
- 4 如果已禁用“流量筛选和标记”，可从**状态**下拉菜单中将其启用。
- 5 选择规则，然后单击**删除**。
- 6 单击**确定**。

### 禁用分布式端口组或上行链路端口组的流量筛选和标记

通过禁用流量筛选和标记策略来允许流量流向虚拟机或物理适配器，而无需进行与安全或 QoS 相关的其他控制。

---

**注意** 您可以对特定端口启用或设置流量筛选和标记策略。请参见第 101 页，“在分布式端口或上行链路端口上启用流量筛选和标记”。

---

**步骤**

- 1 在 vSphere Web Client 中查找分布式端口组或上行链路端口组。
  - a 选择 Distributed Switch，然后单击**网络**选项卡。
  - b 单击**分布式端口组**以查看分布式端口组列表，或单击**上行链路端口组**以查看上行链路端口组列表。
- 2 右键单击端口组，然后选择**编辑设置**。
- 3 选择**流量筛选和标记**。
- 4 从**状态**下拉菜单中选择**已禁用**。
- 5 单击**确定**。

**分布式端口或上行链路端口的流量筛选和标记**

可以通过对分布式端口或上行链路端口配置流量筛选和标记策略，为单个虚拟机、VMkernel 适配器或物理适配器筛选流量或描述其 QoS 需求。

- [在分布式端口或上行链路端口上启用流量筛选和标记](#)第 101 页，  
在端口上启用流量筛选和标记策略，以便在虚拟机网络适配器、VMkernel 适配器或上行链路适配器上配置流量安全和标记。
- [标记分布式端口或上行链路端口的流量](#)第 102 页，  
在规则中为需要特殊处理的流量（如 VoIP 和流视频）分配优先级标记。您可以在网络协议堆栈的第 2 层使用 CoS 标记或在第 3 层使用 DSCP 标记来标记虚拟机、VMkernel 适配器或物理适配器的流量。
- [筛选分布式端口或上行链路端口上的流量](#)第 103 页，  
通过使用规则，可允许或禁止流量，从而确保通过虚拟机、VMkernel 适配器或物理适配器的数据流的安全。
- [使用分布式端口或上行链路端口上的网络流量规则](#)第 104 页，  
定义分布式端口或上行链路端口组中的流量规则，以引入处理与虚拟机或物理适配器相关的流量的策略。可以筛选特定流量或描述其 QoS 需求。
- [禁用分布式端口或上行链路端口的流量筛选和标记](#)第 106 页，  
对端口禁用流量筛选和标记策略，以使流至虚拟机或物理适配器的流量不按照安全性进行筛选或按 QoS 进行标记。

**在分布式端口或上行链路端口上启用流量筛选和标记**

在端口上启用流量筛选和标记策略，以便在虚拟机网络适配器、VMkernel 适配器或上行链路适配器上配置流量安全和标记。

**前提条件**

要替代分布式端口级别的策略，请为此策略启用端口级别替代选项。请参见[第 43 页](#)，“[在端口级别配置替代网络策略](#)”。

**步骤**

- 1 导航到 Distributed Switch，然后导航到分布式端口或上行链路端口。
  - 要导航到交换机的分布式端口，请单击**网络 > 分布式端口组**，双击列表中的分布式端口组，然后单击**端口**选项卡。
  - 要导航到上行链路端口组的上行链路端口，请单击**网络 > 上行链路端口组**，双击列表中的上行链路端口组，然后单击**端口**选项卡。
- 2 从列表中选择端口。

- 3 单击**编辑分布式端口设置**。
- 4 选择**流量筛选和标记**。
- 5 选择**替代**复选框，然后在**状态**下拉菜单中选择**已启用**。
- 6 单击**确定**。

#### 下一步

为流经分布式端口或上行链路端口的数据设置流量筛选或标记。请参见第 102 页，“[标记分布式端口或上行链路端口的流量](#)”和第 103 页，“[筛选分布式端口或上行链路端口上的流量](#)”。

## 标记分布式端口或上行链路端口的流量

在规则中为需要特殊处理的流量（如 VoIP 和流视频）分配优先级标记。您可以在网络协议堆栈的第 2 层使用 CoS 标记或在第 3 层使用 DSCP 标记来标记虚拟机、VMkernel 适配器或物理适配器的流量。

优先级标记是一种流量标记机制，用于标记 QoS 需求较高的流量。网络可以利用这一机制识别不同类的流量。网络设备可以根据每个类的优先级和要求来处理其中的流量。

您也可以重新标记流量，以便提高或降低流量的重要性。通过使用较低的 QoS 标记，可以限制客户机操作系统中标记的数据。

#### 前提条件

要替代分布式端口级别的策略，请为此策略启用端口级别替代选项。请参见第 43 页，“[在端口级别配置替代网络策略](#)”。

#### 步骤

- 1 导航到 **Distributed Switch**，然后导航到分布式端口或上行链路端口。
  - 要导航到交换机的分布式端口，请单击**网络 > 分布式端口组**，双击列表中的分布式端口组，然后单击**端口**选项卡。
  - 要导航到上行链路端口组的上行链路端口，请单击**网络 > 上行链路端口组**，双击列表中的上行链路端口组，然后单击**端口**选项卡。
- 2 从列表中选择端口。
- 3 单击**编辑分布式端口设置**。
- 4 如果没有在端口级别启用流量筛选和标记，请单击**替代**，然后从**状态**下拉菜单中选择**已启用**。
- 5 单击**新建**以创建新规则，或者选择一个规则并单击**编辑**以编辑该规则。
 

您可以更改从分布式端口组或上行链路端口组继承的规则。可以通过这一方式使规则在端口范围内具有唯一性。
- 6 在网络流量规则对话框中，从**操作**下拉菜单中选择**标记**选项。
- 7 为规则范围内的流量设置优先级标记。

选项	描述
<b>CoS 值</b>	在第 2 层网络中使用 CoS 优先级标记来标记与规则匹配的流量。请选择 <b>更新 CoS 标记</b> ，并键入一个介于 0 到 7 之间的值。
<b>DSCP 值</b>	在第 3 层网络中使用 DSCP 标记来标记与规则关联的流量。请选择 <b>更新 DSCP 值</b> ，并键入一个介于 0 到 63 之间的值。

## 8 指定此规则所适用的流量种类。

要确定某一数据流是否位于要标记或筛选的规则范围内，vSphere Distributed Switch 将检查流量的方向、源和目标等属性、VLAN、下一级别协议、基础架构流量类型等。

- a 从**流量方向**下拉菜单中，选择流量必须为输入、输出还是同时为这两者，才能使规则将其视为匹配。  
此方向还会影响您识别流量源和目标的方式。
- b 通过使用系统数据类型限定符、第 2 层数据包属性和第 3 层数据包属性，可以设置数据包要与规则匹配而需要具备的属性。  
  
一个限定符表示一组与某个网络连接层相关的匹配条件。可以将流量与系统数据类型、第 2 层流量属性和第 3 层流量属性进行匹配。可以使用特定网络连接层的限定符，也可以结合使用多个限定符，以便更精确地匹配数据包。
  - 使用系统流量限定符将数据包与流经组端口的虚拟基础架构数据的类型进行匹配。例如，您可以对传输到网络存储的数据选择 NFS。
  - 使用 MAC 流量限定符可根据 MAC 地址、VLAN ID 和下一级别协议匹配数据包。  
  
可以使用虚拟客户机标记 (VGT) 在分布式端口组上查找具有某个 VLAN ID 的流量。如果要在虚拟交换机标记 (VST) 处于活动状态时将流量与 VLAN ID 进行匹配，请对上行链路端口组或上行链路端口使用一个规则。
  - 使用 IP 流量限定符可根据 IP 版本、IP 地址以及下一级别协议和端口匹配数据包。

## 9 在规则对话框中，单击**确定**以保存该规则。

### 筛选分布式端口或上行链路端口上的流量

通过使用规则，可允许或禁止流量，从而确保通过虚拟机、VMkernel 适配器或物理适配器的数据流的安全。

#### 前提条件

要替代分布式端口级别的策略，请为此策略启用端口级别替代选项。请参见第 43 页，“[在端口级别配置替代网络策略](#)”。

#### 步骤

- 1 导航到 **Distributed Switch**，然后导航到分布式端口或上行链路端口。
  - 要导航到交换机的分布式端口，请单击**网络 > 分布式端口组**，双击列表中的分布式端口组，然后单击**端口**选项卡。
  - 要导航到上行链路端口组的上行链路端口，请单击**网络 > 上行链路端口组**，双击列表中的上行链路端口组，然后单击**端口**选项卡。
- 2 从列表中选择端口。
- 3 单击**编辑分布式端口设置**。
- 4 如果没有在端口级别启用流量筛选和标记，请单击**替代**，然后从**状态**下拉菜单中选择**已启用**。
- 5 单击**新建**以创建新规则，或者选择一个规则并单击**编辑**以编辑该规则。  
  
您可以更改从分布式端口组或上行链路端口组继承的规则。可以通过这一方式使规则在端口范围内具有唯一性。
- 6 在网络流量规则对话框中，选择**允许**操作以允许流量通过分布式端口或上行链路端口，或选择**丢弃**操作以对其进行限制。

## 7 指定此规则所适用的流量种类。

要确定某一数据流是否位于要标记或筛选的规则范围内，vSphere Distributed Switch 将检查流量的方向、源和目标等属性、VLAN、下一级别协议、基础架构流量类型等。

- a 从**流量方向**下拉菜单中，选择流量必须为输入、输出还是同时为这两者，才能使规则将其视为匹配。此方向还会影响您识别流量源和目标的方式。

- b 通过使用系统数据类型限定符、第 2 层数据包属性和第 3 层数据包属性，可以设置数据包要与规则匹配而需要具备的属性。

一个限定符表示一组与某个网络连接层相关的匹配条件。可以将流量与系统数据类型、第 2 层流量属性和第 3 层流量属性进行匹配。可以使用特定网络连接层的限定符，也可以结合使用多个限定符，以便更精确地匹配数据包。

- 使用系统流量限定符将数据包与流经组端口的虚拟基础架构数据的类型进行匹配。例如，您可以对传输到网络存储的数据选择 NFS。

- 使用 MAC 流量限定符可根据 MAC 地址、VLAN ID 和下一级别协议匹配数据包。

可以使用虚拟客户机标记 (VGT) 在分布式端口组上查找具有某个 VLAN ID 的流量。如果要在虚拟交换机标记 (VST) 处于活动状态时将流量与 VLAN ID 进行匹配，请对上行链路端口组或上行链路端口使用一个规则。

- 使用 IP 流量限定符可根据 IP 版本、IP 地址以及下一级别协议和端口匹配数据包。

## 8 在规则对话框中，单击**确定**以保存该规则。

### 使用分布式端口或上行链路端口上的网络流量规则

定义分布式端口或上行链路端口组中的流量规则，以引入处理与虚拟机或物理适配器相关的流量的策略。可以筛选特定流量或描述其 QoS 需求。

- [查看分布式端口或上行链路端口上的流量规则](#) 第 104 页，  
查看构成分布式端口或上行链路端口的流量筛选和标记策略的流量规则。
- [编辑分布式端口或上行链路端口上的流量规则](#) 第 105 页，  
创建或编辑流量规则，并使用其参数为分布式端口或上行链路端口配置流量筛选或者标记策略。
- [更改分布式端口或上行链路端口的规则优先级](#) 第 105 页，  
将构成分布式端口或上行链路端口的流量筛选和屏蔽策略的规则重新排序，以更改流量分析的操作顺序，确保安全性和服务质量。
- [删除分布式端口或上行链路端口上的流量规则](#) 第 106 页，  
删除分布式端口或上行链路端口上的流量规则可停止筛选或标记流向虚拟机或物理适配器的特定数据包类型。

### 查看分布式端口或上行链路端口上的流量规则

查看构成分布式端口或上行链路端口的流量筛选和标记策略的流量规则。

#### 前提条件

要替代分布式端口级别的策略，请为此策略启用端口级别替代选项。请参见[第 43 页](#)，“在端口级别配置替代网络策略”。



## 步骤

- 1 导航到 **Distributed Switch**，然后导航到分布式端口或上行链路端口。
  - 要导航到交换机的分布式端口，请单击**网络 > 分布式端口组**，双击列表中的分布式端口组，然后单击**端口**选项卡。
  - 要导航到上行链路端口组的上行链路端口，请单击**网络 > 上行链路端口组**，双击列表中的上行链路端口组，然后单击**端口**选项卡。
- 2 从列表中选择端口。
- 3 单击**编辑分布式端口设置**。
- 4 选择**流量筛选和标记**。
- 5 如果没有在端口级别启用流量筛选和标记，请单击**替代**，然后从**状态**下拉菜单中选择**已启用**。
- 6 检查**操作**以查看此规则是否对流量进行了筛选（允许或拒绝），或者是否对具有特殊 QoS 需求的流量进行了标记（标记）。
- 7 从上方的列表中，选择您要查看流量查找条件的规则。  
此规则的流量限定参数将显示在流量限定符列表中。

## 编辑分布式端口或上行链路端口上的流量规则

创建或编辑流量规则，并使用其参数为分布式端口或上行链路端口配置流量筛选或者标记策略。

## 前提条件

要替代分布式端口级别的策略，请为此策略启用端口级别替代选项。请参见第 43 页，“在端口级别配置替代网络策略”。

## 步骤

- 1 导航到 **Distributed Switch**，然后导航到分布式端口或上行链路端口。
  - 要导航到交换机的分布式端口，请单击**网络 > 分布式端口组**，双击列表中的分布式端口组，然后单击**端口**选项卡。
  - 要导航到上行链路端口组的上行链路端口，请单击**网络 > 上行链路端口组**，双击列表中的上行链路端口组，然后单击**端口**选项卡。
- 2 从列表中选择端口。
- 3 单击**编辑分布式端口设置**。
- 4 选择**流量筛选和标记**。
- 5 如果没有在端口级别启用流量筛选和标记，请单击**替代**，然后从**状态**下拉菜单中选择**已启用**。
- 6 单击**新建**以创建新规则，或者选择一个规则并单击**编辑**以编辑该规则。  
您可以更改从分布式端口组或上行链路端口组继承的规则。可以通过这一方式使规则在端口范围内具有唯一性。

## 下一步

为网络流量规则命名，并拒绝、允许或标记目标流量。

## 更改分布式端口或上行链路端口的规则优先级

将构成分布式端口或上行链路端口的流量筛选和屏蔽策略的规则重新排序，以更改流量分析的操作顺序，确保安全性和服务质量。

vSphere Distributed Switch 将按严格的顺序应用网络流量规则。如果某个数据包已符合某个规则，则该数据包可能不会传递到策略中的下一个规则。

### 前提条件

要替代分布式端口级别的策略，请为此策略启用端口级别替代选项。请参见第 43 页，“在端口级别配置替代网络策略”。

### 步骤

- 1 导航到 Distributed Switch，然后导航到分布式端口或上行链路端口。
  - 要导航到交换机的分布式端口，请单击**网络 > 分布式端口组**，双击列表中的分布式端口组，然后单击**端口**选项卡。
  - 要导航到上行链路端口组的上行链路端口，请单击**网络 > 上行链路端口组**，双击列表中的上行链路端口组，然后单击**端口**选项卡。
- 2 从列表中选择端口。
- 3 单击**编辑分布式端口设置**。
- 4 选择**流量筛选和标记**。
- 5 如果没有在端口级别启用流量筛选和标记，请单击**替代**，然后从**状态**下拉菜单中选择**已启用**。
- 6 选择一个规则，并使用箭头按钮来更改其优先级。
- 7 单击**确定**应用更改。

### 删除分布式端口或上行链路端口上的流量规则

删除分布式端口或上行链路端口上的流量规则可停止筛选或标记流向虚拟机或物理适配器的特定数据包类型。

### 前提条件

要替代分布式端口级别的策略，请为此策略启用端口级别替代选项。请参见第 43 页，“在端口级别配置替代网络策略”。

### 步骤

- 1 导航到 Distributed Switch，然后导航到分布式端口或上行链路端口。
  - 要导航到交换机的分布式端口，请单击**网络 > 分布式端口组**，双击列表中的分布式端口组，然后单击**端口**选项卡。
  - 要导航到上行链路端口组的上行链路端口，请单击**网络 > 上行链路端口组**，双击列表中的上行链路端口组，然后单击**端口**选项卡。
- 2 从列表中选择端口。
- 3 单击**编辑分布式端口设置**。
- 4 选择**流量筛选和标记**。
- 5 如果没有在端口级别启用流量筛选和标记，请单击**替代**，然后从**状态**下拉菜单中选择**已启用**。
- 6 选择规则，然后单击**删除**。
- 7 单击**确定**。

### 禁用分布式端口或上行链路端口的流量筛选和标记

对端口禁用流量筛选和标记策略，以使流至虚拟机或物理适配器的流量不按照安全性进行筛选或按 QoS 进行标记。

### 前提条件

要替代分布式端口级别的策略，请为此策略启用端口级别替代选项。请参见第 43 页，“在端口级别配置替代网络策略”。

## 步骤

- 1 导航到 **Distributed Switch**，然后导航到分布式端口或上行链路端口。
  - 要导航到交换机的分布式端口，请单击**网络 > 分布式端口组**，双击列表中的分布式端口组，然后单击**端口**选项卡。
  - 要导航到上行链路端口组的上行链路端口，请单击**网络 > 上行链路端口组**，双击列表中的上行链路端口组，然后单击**端口**选项卡。
- 2 从列表中选择端口。
- 3 单击**编辑分布式端口设置**。
- 4 选择**流量筛选和标记**。
- 5 单击**替代**，然后从**状态**下拉菜单中，选择**已禁用**。
- 6 单击**确定**。

## 限定要筛选和标记的流量

可以将要筛选或使用 QoS 标记进行标记的流量与承载的基础架构数据（如用于存储、vCenter Server 管理等的数据）的类型以及第 2 层和第 3 层的属性相匹配。

要更精确地匹配规则范围内的流量，可以将系统数据类型、第 2 层标题和第 3 层标题的条件结合使用。

### 系统流量限定符

通过在端口组或端口的规则中使用系统流量限定符，您可以确定是否必须使用 QoS 标记来标记某些系统数据流量，是否允许或丢弃某些系统数据流量。

#### 系统流量类型

可以选择通过组的各个端口的承载系统数据的流量类型，即 vCenter Server、存储、VMware vSphere® vMotion® 和 vSphere Fault Tolerance 中用于管理的流量。您只能标记或筛选特定的流量类型，或者某个基础架构功能以外的所有系统数据流量。例如，您可以用 QoS 值进行标记，或者筛选 vCenter Server、存储和 vMotion 中用于管理的流量，但无法标记或筛选承载 Fault Tolerance 数据的流量。

### MAC 流量限定符

通过在规则中使用 MAC 流量限定符，您可以为数据包的第 2 层（数据链路层）属性（如 MAC 地址、VLAN ID 和占用帧负载的下一级别协议）定义匹配条件。

#### 协议类型

MAC 流量限定符的**协议类型**属性与以太网帧的 EtherType 字段相对应。EtherType 表示将占用帧负载的下一级别协议的类型。

您可以从下拉菜单中选择某个协议或键入其十六进制数字。例如，要捕获链路层发现协议 (LLDP) 的流量，请键入 **88CC**。

#### VLAN ID

您可以使用 MAC 流量限定符的 VLAN ID 属性来标记或筛选特定 VLAN 中的流量。

---

**注意** 在分布式端口组中 VLAN ID 限定符可以与虚拟客户机标记 (VGT) 配合使用。

如果使用 VLAN ID 通过虚拟交换机标记 (VST) 来标记流，则无法使用此 ID 在分布式端口组或分布式端口的规则中找到流。其原因是，交换机取消对流量的标记后，Distributed Switch 会检查规则条件（其中包括 VLAN ID）。在这种情况下，要通过 VLAN ID 成功匹配流量，必须对上行链路端口组或上行链路端口使用一个规则。

---

## 源地址

通过使用“源地址”属性组，可以根据源 MAC 地址或源 MAC 网络匹配数据包。

可以使用比较运算符来标记或筛选具有或没有特定源地址或源 MAC 网络的数据包。

您可以通过多种方法匹配流量源。

**表 8-6 按 MAC 源地址筛选或标记流量的模式**

用于匹配流量源地址的参数	比较运算符	网络连接参数格式
MAC 地址	是或不是	键入用于匹配的 MAC 地址。使用冒号分隔其中的八位字节。
MAC 网络	匹配或不匹配	键入网络的低位地址和通配符掩码。在网络位的位置设置 0，在主机部分设置 1。

例如，对于带有前缀为 05:50:56 且长度为 23 位的 MAC 网络，地址将设置为 **00:50:56:00:00:00**，而掩码为 **00:00:01:ff:ff:ff**。

## 目标地址

通过使用“目标地址”属性组，可以将数据包与其目标地址相匹配。MAC 目标地址选项的格式与源地址的格式相同。

## 比较运算符

要使匹配 MAC 限定符的流量更加符合您的需求，您可以使用肯定比较或否定比较。通过使用这些运算符，可以将具有某些特定属性的数据包之外的所有数据包均包含在规则的范围之内。

## IP 流量限定符

通过在规则中使用 IP 流量限定符，可以针对 IP 版本、IP 地址、下一级别协议和端口等第 3 层（网络层）属性定义匹配的流量标准。

## 协议

IP 流量限定符的协议属性表示占用数据包负载的下一级别协议。您可以从下拉菜单中选择某个协议或按照 RFC 1700 键入其十进制编号。

对于 TCP 和 UDP 协议，还可以按源端口和目标端口匹配流量。

## 源端口

通过使用“源端口”属性，可以按源端口匹配 TCP 或 UDP 数据包。将流量与源端口匹配时，请考虑流量方向。

## 目标端口

通过使用“目标端口”属性，可以按目标端口匹配 TCP 或 UDP 数据包。将流量与目标端口匹配时，请考虑流量方向。

## 源地址

通过使用“源地址”属性，可以按源地址或子网匹配数据包。将流量与源地址或网络匹配时，请考虑流量方向。

可以通过多种方法匹配流量源。

表 8-7 按 IP 源地址筛选或标记流量的模式

用于匹配流量源地址的参数	比较运算符	网络连接参数格式
IP 版本	任意	在下拉菜单中选择 IP 版本。
IP 地址	是或不是	键入要匹配的 IP 地址。
IP 子网	匹配或不匹配	键入子网中的低位地址和子网前缀的位长。

目标地址

使用“目标地址”可根据 IP 地址、子网或 IP 版本匹配数据包。目标地址的格式与源地址的格式相同。

比较运算符

要使匹配 IP 限定符的流量更加符合您的需求，您可以使用肯定比较或否定比较。您可以定义除具有特定属性的数据包外的所有数据包都包含在规则范围内。

管理 vSphere Distributed Switch 上的多个端口组的策略

可以修改 vSphere Distributed Switch 上多个端口组的网络连接策略。

前提条件

创建具有一个或多个端口组的 vSphere Distributed Switch。

步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在对象导航器中右键单击 Distributed Switch，然后选择分布式端口组 > 管理分布式端口组。
- 3 在“选择端口组策略”页面上，选中要修改的策略类别旁边的复选框，然后单击下一步。

选项	描述
安全	为所选端口组设置 MAC 地址更改、伪信号和混杂模式。
流量调整	为所选端口组上的入站和出站流量设置平均带宽、峰值带宽和突发大小。
VLAN	配置所选端口组与物理 VLAN 的连接方式。
成组和故障切换	为所选端口组设置负载均衡、故障切换检测、交换机通知和故障切换顺序。
资源分配	为所选端口组设置网络资源池关联。此选项适用于 vSphere Distributed Switch 版本 5.0 及更高版本。
监控	在所选端口组上启用或禁用 NetFlow。此选项适用于 vSphere Distributed Switch 版本 5.0.0 及更高版本。
流量筛选和标记	配置筛选（允许或丢弃）策略和通过选定端口组中端口的特定类型流量标记策略。此选项适用于 vSphere Distributed Switch 版本 5.5 及更高版本。
其他	在所选端口组上启用或禁用端口阻止。

- 4 在“选择端口组”页面上，选择要编辑的分布式端口组，然后单击下一步。

- 5 （可选）在“安全”页面上，使用下拉菜单以编辑安全例外，然后单击**下一步**。

选项	描述
<b>混杂模式</b>	<ul style="list-style-type: none"> <li>■ <b>拒绝</b>。将客户机适配器置于混杂模式不会对适配器接收哪些帧产生任何影响。</li> <li>■ <b>接受</b>。将客户机适配器置于混杂模式会使其检测经过 vSphere Distributed Switch 且由适配器所连接到的端口组的 VLAN 策略允许的所有帧。</li> </ul>
<b>MAC 地址更改</b>	<ul style="list-style-type: none"> <li>■ <b>拒绝</b>。如果设置为<b>拒绝</b>并且客户机操作系统将适配器的 MAC 地址更改为不同于 .vmx 配置文件的其他任何内容，则会丢失所有入站帧。 如果客户机操作系统将 MAC 地址重新更改为与 .vmx 配置文件中的 MAC 地址匹配的地址，入站帧可以再次通过。</li> <li>■ <b>接受</b>。从客户机操作系统更改 MAC 地址会达到预期效果。会接收传输到新 MAC 地址的帧。</li> </ul>
<b>伪信号</b>	<ul style="list-style-type: none"> <li>■ <b>拒绝</b>。对于任何出站帧，如果源 MAC 地址与当前在适配器上设置的地址不同，则将丢失这些帧。</li> <li>■ <b>接受</b>。不执行筛选，所有出站帧均可通过。</li> </ul>

- 6 （可选）在“流量调整”页面上，使用下拉菜单以启用或禁用输入或输出流量调整，然后单击**下一步**。

选项	描述
<b>状态</b>	如果启用 <b>输入流量调整</b> 或 <b>输出流量调整</b> ，将为与该端口组关联的每个 VMkernel 适配器或虚拟网络适配器设置网络连接带宽分配量的限制。如果禁用策略，则在默认情况下，服务将能够自由、顺畅地连接物理网络。
<b>平均带宽</b>	设定每秒允许通过端口的位数，这是一段时间内的平均值，即允许的平均负载。
<b>峰值带宽</b>	当端口正在发送或接收流量突发时为了通过端口而允许采用的平均每秒最大传输位数。此数值是端口使用额外突发时所能使用的最大带宽。
<b>突发大小</b>	突发中所允许的最大字节数。如果设置了此参数，则在端口没有使用为其分配的所有带宽时可能会获取额外的突发。当端口所需带宽大于 <b>平均带宽</b> 所指定的值时，如果有额外突发可用，则可能会允许以更高的速度传输数据。该参数是指流量突发时可累积且以更高速度传输的最大字节数。

- 7 （可选）在“VLAN”页面上，使用下拉菜单以编辑 VLAN 策略，然后单击**下一步**。

选项	描述
<b>无</b>	不使用 VLAN。
<b>VLAN</b>	在 <b>VLAN ID</b> 字段中，输入一个介于 1 和 4094 之间的数字。
<b>VLAN 中继</b>	输入 <b>VLAN 中继范围</b> 。
<b>专用 VLAN</b>	选择可供使用的专用 VLAN。

- 8 （可选）在“绑定和故障切换”页面上，使用下拉菜单以编辑设置，然后单击**下一步**。

选项	描述
<b>负载平衡</b>	<p>基于 IP 的绑定要求为物理交换机配置以太通道。对于所有其他选项，应禁用以太通道。选择如何选择上行链路。</p> <ul style="list-style-type: none"> <li>■ <b>基于源虚拟端口的路由</b>。根据流量进入 Distributed Switch 所经过的虚拟端口选择上行链路。</li> <li>■ <b>基于 IP 哈希的路由</b>。根据每个数据包的源和目标 IP 地址哈希值选择上行链路。对于非 IP 数据包，偏移量中的任何值都将用于计算哈希值。</li> <li>■ <b>基于源 MAC 哈希的路由</b>。根据源以太网哈希值选择上行链路。</li> <li>■ <b>基于物理网卡负载的路由</b>。根据物理网卡的当前负载选择上行链路。</li> <li>■ <b>使用明确故障切换顺序</b>。始终使用“活动适配器”列表中位于最前列的符合故障切换检测标准的上行链路。</li> </ul>
<b>网络故障检测</b>	<p>选择用于故障切换检测的方法。</p> <ul style="list-style-type: none"> <li>■ <b>仅链路状态</b>。仅依靠网络适配器提供的链路状态。该选项可检测故障（如拔掉线缆和物理交换机电源故障），但无法检测配置错误（如物理交换机端口受跨树阻止、配置到了错误的 VLAN 中或者拔掉了物理交换机另一端的线缆）。</li> <li>■ <b>信标探测</b>。发出并侦听组中所有网卡上的信标探测，使用此信息并结合链路状态来确定链接故障。不要使用包含 IP 哈希负载平衡的信标探测。</li> </ul>
<b>通知交换机</b>	<p>选择<b>是</b>或<b>否</b>指定发生故障切换时是否通知交换机。当使用端口组的虚拟机正在以单播模式使用 Microsoft 网络负载平衡时，请勿使用此选项。</p> <p>如果选择<b>是</b>，则每当虚拟网卡连接到 Distributed Switch 或虚拟网卡的流量因故障切换事件而由网卡组中的其他物理网卡路由时，都将通过网络发送通知以更新物理交换机的查看表。使用此流程，使故障切换和 vMotion 迁移的延迟时间降至最少。</p>
<b>故障恢复</b>	<p>选择<b>是</b>或<b>否</b>以禁用或启用故障恢复。</p> <p>此选项确定物理适配器从故障恢复后如何返回到活动的任务。</p> <ul style="list-style-type: none"> <li>■ <b>是</b>（默认）。适配器将在恢复后立即返回到活动任务，替换接替其位置的备用适配器（如果有）。</li> <li>■ <b>否</b>。即使发生故障的适配器已经恢复，它仍将保持非活动状态，直到当前处于活动状态的另一个适配器发生故障并要求替换为止。</li> </ul>
<b>故障切换顺序</b>	<p>选择如何分布上行链路的工作负载。要使用一部分上行链路，保留另一部分来应对使用的上行链路发生故障时的情况，则可以通过将它们移到不同的组来设置此条件。</p> <ul style="list-style-type: none"> <li>■ <b>活动上行链路</b>。当网络适配器连接正常且处于活动状态时，继续使用此上行链路。</li> <li>■ <b>备用上行链路</b>。如果其中一个活动适配器的连接中断，则使用此上行链路。当使用 IP 哈希负载平衡时，不要配置待机上行链路。</li> <li>■ <b>未使用的上行链路</b>。不使用此上行链路。</li> </ul>

- 9 （可选）在“资源分配”页面上，使用**网络资源池**下拉菜单以添加或移除资源分配，然后单击**下一步**。
- 10 （可选）在“监控”页面上，使用下拉菜单以启用或禁用 NetFlow，然后单击**下一步**。

选项	描述
<b>已禁用</b>	在分布式端口组上禁用了 NetFlow。
<b>已启用</b>	在分布式端口组上启用了 NetFlow。可以在 vSphere Distributed Switch 级别配置 NetFlow 设置。

- 11 （可选）在流量筛选和标记页面，从**状态**下拉菜单中启用或禁用流量筛选和标记，为筛选或标记特定数据流配置流量规则，然后单击**下一步**。

可以设置规则的以下属性，以确定目标流量和其上的操作：

选项	描述
<b>名称</b>	规则的名称
<b>操作</b>	<ul style="list-style-type: none"> <li>■ <b>允许</b>。授予特定类型流量的访问权限。</li> <li>■ <b>丢弃</b>。拒绝特定类型流量的访问权限。</li> <li>■ <b>标记</b>。通过插入 CoS 和 DSCP 标记或使用 CoS 和 DSCP 标记重新标记流量，从而按 QoS 分类流量。</li> </ul>
<b>流量方向</b>	设置规则是否适用于入站流量、出站流量或者入站和出站流量。 此方向还会影响您识别流量源和目标的方式。
<b>系统流量限定符</b>	指示规则适用于系统流量，并设置要应用规则的基础架构协议类型。例如，使用优先级标记标识通过 vCenter Server 管理的流量。
<b>MAC 限定符</b>	<p>根据第 2 层标题限定规则的流量。</p> <ul style="list-style-type: none"> <li>■ <b>协议类型</b>。设置占用负载的下一级别协议（IPv4、IPv6 等）。 此属性与以太网帧中的 <b>EtherType</b> 字段相对应。 可以从下拉菜单中选择某个协议或键入其十六进制数字 例如，要捕获链路层发现协议 (LLDP) 的流量，请键入 <b>88CC</b>。</li> <li>■ <b>VLAN ID</b>。按 VLAN 捕获流量。 在分布式端口组中 VLAN ID 限定符可以与虚拟客户机标记 (VGT) 配合使用。 如果使用 VLAN ID 通过虚拟交换机标记 (VST) 来标记流，则无法使用此 ID 在分布式端口组规则中找到流。其原因是，交换机取消对流量的标记后，Distributed Switch 会检查规则条件（其中包括 VLAN ID）。要成功将流量与 VLAN ID 进行匹配，请为上行链路端口组或上行链路端口使用一个规则。</li> <li>■ <b>源地址</b>。设置单个 MAC 地址或 MAC 网络，以便根据源地址匹配数据包。 为 MAC 网络输入网络中的低位地址和通配符掩码。掩码的网络位位置包含 0，主机部分包含 1。 例如，对于前缀为 05:50:56 且长度为 23 位的 MAC 网络，地址将设置为 <b>00:50:56:00:00:00</b>，而掩码为 <b>00:00:01:ff:ff:ff</b>。</li> <li>■ <b>目标地址</b>。设置单个 MAC 地址或 MAC 网络，以便根据目标地址匹配数据包。MAC 目标地址支持的格式与源地址支持的格式相同。</li> </ul>
<b>IP 限定符</b>	<p>根据第 3 层标题限定规则的流量。</p> <ul style="list-style-type: none"> <li>■ <b>协议</b>。设置占用负载的下一级别协议（TCP、UDP 等）。 可以从下拉菜单中选择某个协议或按照 <i>RFC 1700（指定的编号）</i> 键入其十进制数字。 对于 TCP 和 UDP 协议，还可以设置源端口和目标端口。</li> <li>■ <b>源端口</b>。将 TCP 或 UDP 数据包与源端口相匹配。确定要与数据包相匹配的源端口时，考虑规则范围内流量的方向。</li> <li>■ <b>目标端口</b>。按源端口匹配 TCP 或 UDP 数据包。确定要与数据包相匹配的目标端口时，考虑规则范围内流量的方向。</li> <li>■ <b>源地址</b>。设置 IP 版本、单个 IP 地址或子网，以便按源地址匹配数据包。 为子网输入低位地址和前缀的位长。</li> <li>■ <b>目标地址</b>。设置 IP 版本、单个 IP 地址或子网，以便按源地址匹配数据包。IP 目标地址支持的格式与源地址支持的格式相同。</li> </ul>

- 12 （可选）在“其他”页面上，从下拉菜单中选择**是或否**，然后单击**下一步**。

选择**是**可关闭端口组中的所有端口。此关闭可能会中断正在使用端口的宿主或虚拟机的正常网络操作。



- 13 查看“即将完成”页面上的设置，然后单击**完成**。
- 使用**上一步**按钮更改任意设置。

## 端口阻止策略

端口阻止策略允许有选择地阻止端口发送或接收数据。

### 编辑分布式端口组的端口阻止策略

您可以阻止分布式端口组中的所有端口。

如果阻止分布式端口组的端口，可能会中断正在使用这些端口的主机或虚拟机的正常网络操作。

#### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在对象导航器中右键单击 Distributed Switch，然后选择**分布式端口组 > 管理分布式端口组**。
- 3 选中**其他**复选框，然后单击**下一步**。
- 4 选择要配置的一个或多个分布式端口组，然后单击**下一步**。
- 5 从**阻止所有端口**下拉菜单中启用或禁用端口阻止，然后单击**下一步**。
- 6 查看设置，然后单击**完成**。

### 编辑分布式端口或上行链路端口的阻止策略

您可以阻止单个分布式端口或上行链路端口。

如果阻止通过端口的流量，可能会中断正在使用该端口的主机或虚拟机的正常网络操作。

#### 前提条件

启用端口级别替代。请参见第 43 页，“在端口级别配置替代网络策略”

#### 步骤

- 1 导航到 Distributed Switch，然后导航到分布式端口或上行链路端口。
  - 要导航到交换机的分布式端口，请单击**网络 > 分布式端口组**，双击列表中的分布式端口组，然后单击**端口**选项卡。
  - 要导航到上行链路端口组的上行链路端口，请单击**网络 > 上行链路端口组**，双击列表中的上行链路端口组，然后单击**端口**选项卡。
- 2 从列表中选择端口。
- 3 单击**编辑分布式端口设置**。
- 4 在**其他**部分中，选中**替代**复选框，然后从下拉菜单中启用或禁用端口阻止。
- 5 单击**确定**。



## 使用 VLAN 隔离网络流量

---

VLAN 可让您在网络协议堆栈的第 2 层将网络分段为多个逻辑广播域。

本章讨论了以下主题：

- 第 115 页，“VLAN 配置”
- 第 116 页，“专用 VLAN”

### VLAN 配置

通过虚拟 LAN (VLAN)，单个物理 LAN 分段可进一步隔离，以使端口组互相隔离，就好像它们位于不同物理分段上一样。

#### 在 vSphere 中使用 VLAN 的优点

vSphere 环境中的 VLAN 配置提供了一定的优势。

- 可将 ESXi 主机集成到预先存在的 VLAN 拓扑中。
- 可隔离并确保网络流量的安全。
- 可减少网络流量拥堵情况。

有关在 vSphere 环境中引入 VLAN 的优点和主要原则，请观看视频。



在 vSphere 环境中使用 VLAN ([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_using\\_vlans\\_in\\_vsphere](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_using_vlans_in_vsphere))

#### VLAN 标记模式

在 ESXi 中 vSphere 支持三种 VLAN 标记模式：外部交换机标记 (EST)、虚拟交换机标记 (VST) 和虚拟客户机标记 (VGT)。

标记模式	交换机端口组上的 VLAN ID	描述
EST	0	物理交换机可执行 VLAN 标记。为了访问物理交换机上的端口，会连接主机网络适配器。
VST	介于 1 和 4094 之间。	虚拟交换机可在数据包离开主机前执行 VLAN 标记。主机网络适配器必须连接到物理交换机上的中继端口。
VGT	<ul style="list-style-type: none"> <li>4095（适用于标准交换机）</li> <li>Distributed Switch 的范围和各个 VLAN</li> </ul>	<p>虚拟机可执行 VLAN 标记。虚拟交换机在虚拟机网络堆栈和外部交换机之间转发数据包时，会保留 VLAN 标记。主机网络适配器必须连接到物理交换机上的中继端口。</p> <p>vSphere Distributed Switch 支持修改 VGT。为安全起见，可以将 Distributed Switch 配置为仅传递属于特定 VLAN 的数据包。</p> <p><b>注意</b> 对于 VGT，必须在虚拟机的客户机操作系统上安装 802.1Q VLAN 中继驱动程序。</p>

有关虚拟交换机中 VLAN 标记模式的介绍，请观看视频。



vSphere 中的 VLAN 标记模式 ([http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video\\_vlan\\_tagging\\_modes](http://link.brightcove.com/services/player/bcpid2296383276001?bctid=ref:video_vlan_tagging_modes))

## 专用 VLAN

专用 VLAN 用于解决 VLAN ID 限制，方法是将逻辑广播域的进一步分段添加到多个较小的广播子域中。

专用 VLAN 由其主专用 VLAN ID 标识。主专用 VLAN ID 可以拥有多个与其关联的次专用 VLAN ID。主专用 VLAN 为**杂乱模式**，以便专用 VLAN 上的端口可以与配置为主专用 VLAN 的端口通信。次专用 VLAN 上的端口可以是**已隔离**（仅与杂乱模式端口通信），也可以是**团体**（与同一次专用 VLAN 上的杂乱模式端口和其他端口通信）。

如果要在主机和其余物理网络之间使用专用 VLAN，则与主机相连的物理交换机必须支持专用 VLAN，而且需要用 ESXi 所用的 VLAN ID 进行配置以获取专用 VLAN 功能。对于使用基于动态 MAC+VLAN ID 进行学习的物理交换机，必须首先将所有相应的专用 VLAN ID 输入到交换机的 VLAN 数据库中。

## 创建专用 VLAN

在 vSphere Distributed Switch 上创建必要的专用 VLAN，以便能够分配用于参与专用 VLAN 的分布式端口。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在**配置**选项卡上，展开**设置**并选择**专用 VLAN**。
- 3 单击**编辑**。
- 4 要添加主 VLAN，在“主 VLAN ID”下方单击**添加**，然后输入主 VLAN 的 ID。
- 5 单击“主 VLAN ID”前面的**加号 (+)** 将其添加到列表中。  
主专用 VLAN 也会显示在“辅助专用 VLAN ID”下。
- 6 要添加辅助 VLAN，在右侧面板中单击**添加**，然后输入 VLAN 的 ID。
- 7 单击“辅助 VLAN ID”前面的**加号 (+)** 将其添加到列表中。
- 8 从**辅助 VLAN 类型**列的下拉菜单中，选择**已隔离**或**社区**。
- 9 单击**确定**。

## 下一步

对分布式端口组或端口进行配置，使其将流量与专用 VLAN 关联在一起。请参见第 88 页，“[在分布式端口组或分布式端口上配置 VLAN 标记](#)”。

## 移除主专用 VLAN

从 vSphere Distributed Switch 的配置中移除未使用的主 VLAN。

移除主专用 VLAN 时，也会移除关联的辅助专用 VLAN。

### 前提条件

确认没有端口组配置为使用主 VLAN 及其关联的辅助 VLAN。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在配置选项卡上，展开设置并选择专用 VLAN。
- 3 单击编辑。
- 4 选择要移除的主专用 VLAN。
- 5 在“主 VLAN ID”列表下，单击移除。
- 6 单击确定确认要移除主 VLAN。
- 7 单击确定。

## 移除次专用 VLAN

从 vSphere Distributed Switch 的配置中移除未使用的辅助专用 VLAN。

### 前提条件

确认没有端口组配置为使用辅助 VLAN。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在配置选项卡上，展开设置并选择专用 VLAN。
- 3 单击编辑。
- 4 选择主专用 VLAN。  
与其关联的辅助专用 VLAN 将在右侧显示。
- 5 选择要移除的次专用 VLAN。
- 6 在辅助 VLAN ID 列表下方，单击移除，然后单击确定。



## 管理网络资源

---

vSphere 提供了多种帮助您管理网络资源的不同方法。

本章讨论了以下主题：

- [第 119 页](#)，“DirectPath I/O”
- [第 122 页](#)，“单根 I/O 虚拟化 (SR-IOV)”
- [第 132 页](#)，“虚拟机的远程直接内存访问”
- [第 135 页](#)，“巨帧”
- [第 137 页](#)，“TCP 分段清除”
- [第 139 页](#)，“大型接收卸载”
- [第 143 页](#)，“NetQueue 和网络性能”

### DirectPath I/O

通过 DirectPath I/O，虚拟机可以使用 I/O 内存管理单元访问平台上的物理 PCI 功能。

配置了 DirectPath 的虚拟机不具有以下功能：

- 虚拟设备的热添加和热移除
- 挂起和恢复
- 记录和重放
- Fault Tolerance
- High Availability
- DRS（受限的可用性。虚拟机可以属于某个群集，但不能在主机之间迁移）
- 快照

Cisco 统一计算系统 (UCS) 通过 Cisco Virtual Machine Fabric Extender (VM-FEX) 分布式交换机可支持使用 DirectPath I/O 的虚拟机的迁移和资源管理功能：

- vMotion
- 虚拟设备的热添加和热移除
- 挂起和恢复
- High Availability
- DRS

- 快照

有关支持的交换机以及交换机配置信息的详细情况，请参见 [Cisco VM-FEX 文档](#)。

- [为主机上的网络设备启用直通功能](#) 第 120 页，

直通设备可提供有效的方式来使用资源并提高环境性能。您可以为主机上的网络设备启用 DirectPath I/O 直通功能。

- [在虚拟机上配置 PCI 设备](#) 第 120 页，

直通设备可在您的环境中提供更有效的方式来使用资源并提高性能。可以在 vSphere Web Client 中的虚拟机上配置直通 PCI 设备。

- [在虚拟机上通过 vMotion 启用 DirectPath I/O](#) 第 121 页，

您可以在至少具有一个受支持的 Cisco UCS Virtual Machine Fabric Extender (VM-FEX) 分布式交换机的 Cisco UCS 系统上的数据中心中，通过 vMotion 为虚拟机启用 DirectPath I/O。

## 为主机上的网络设备启用直通功能

直通设备可提供有效的方式来使用资源并提高环境性能。您可以为主机上的网络设备启用 DirectPath I/O 直通功能。



**小心** 如果 ESXi 主机被配置为从连接到 USB 通道的 USB 设备或 SD 卡进行引导，请确保不要为 USB 控制器启用 DirectPath I/O 直通。对通过 USB 设备或 SD 卡进行引导的 ESXi 主机上的 USB 控制器使用直通，可能会使主机进入无法持久保持配置的状态。

### 步骤

- 1 在 vSphere Web Client 导航器中浏览到主机。
- 2 在 **配置** 选项卡上，展开 **硬件** 并单击 **PCI 设备**。
- 3 要为主机上的 PCI 网络设备启用 DirectPath I/O 直通功能，请单击 **编辑**。  
此时将显示可用直通设备的列表。

图标	描述
绿色图标	设备处于活动状态且可启用。
橙色图标	设备的状态已更改，并且您必须先重新引导主机，然后才能使用设备。

- 4 选择要用于直通的网络设备，然后单击 **确定**。  
选定的 PCI 设备会显示在表中。设备信息会显示在屏幕底部。
- 5 重新引导主机，使 PCI 网络设备可供使用。

## 在虚拟机上配置 PCI 设备

直通设备可在您的环境中提供更有效的方式来使用资源并提高性能。可以在 vSphere Web Client 中的虚拟机上配置直通 PCI 设备。

将直通设备与 Linux 内核 2.6.20 或更低版本配合使用时，请避免使用 MSI 和 MSI-X 模式，因为这会明显影响性能。

### 前提条件

验证是否已在虚拟机的主机上配置直通网络连接设备。请参见 [第 120 页](#)，“为主机上的网络设备启用直通功能”。



**步骤**

- 1 在 vSphere Web Client 中找到虚拟机。
  - a 选择数据中心、文件夹、群集、资源池或主机，然后单击**虚拟机**选项卡。
  - b 单击**虚拟机**，然后从列表中双击虚拟机。
- 2 关闭虚拟机电源。
- 3 在虚拟机的**配置**选项卡上，展开**设置**，然后选择**虚拟机硬件**。
- 4 单击**编辑**，然后在显示设置的对话框中选择**虚拟硬件**选项卡。
- 5 展开**内存**部分，然后将**限制**设置为**不受限制**。
- 6 从**新设备**下拉菜单中，选择**PCI 设备**，然后单击**添加**。
- 7 从**新 PCI 设备**下拉菜单中，选择要使用的直通设备，然后单击**确定**。
- 8 打开虚拟机电源。

将 DirectPath I/O 设备添加到虚拟机可将内存预留设置为虚拟机的内存大小。

**在虚拟机上通过 vMotion 启用 DirectPath I/O**

您可以在至少具有一个受支持的 Cisco UCS Virtual Machine Fabric Extender (VM-FEX) 分布式交换机的 Cisco UCS 系统上的数据中心中，通过 vMotion 为虚拟机启用 DirectPath I/O。

**前提条件**

在受支持的 Cisco VM-FEX 分布式交换机上的至少一个 Cisco UCS 端口配置文件上启用高性能网络 I/O。有关支持的交换机和交换机配置，请参见 Cisco 网站 <http://www.cisco.com/go/unifiedcomputing/b-series-doc> 中的文档。

**步骤**

- 1 在 vSphere Web Client 中找到虚拟机。
  - a 选择数据中心、文件夹、群集、资源池或主机，然后单击**虚拟机**选项卡。
  - b 单击**虚拟机**，然后从列表中双击虚拟机。
- 2 关闭虚拟机电源。
- 3 在虚拟机的**配置**选项卡上，展开**设置**，然后选择**虚拟机硬件**。
- 4 单击**编辑**，然后在显示设置的对话框中选择**虚拟硬件**选项卡。
- 5 展开**内存**部分，然后将**限制**设置为**不受限制**。
- 6 展开**网络适配器**部分配置直通设备。
- 7 在 DirectPath I/O 旁边，单击**启用**。
- 8 从“网络”下拉菜单中，选择已启用高性能的端口配置文件，然后单击**确定**。
- 9 打开虚拟机电源。

## 单根 I/O 虚拟化 (SR-IOV)

vSphere 5.1 及更高版本支持单根 I/O 虚拟化 (SR-IOV)。您可将 SR-IOV 用于滞后敏感或需要更多 CPU 资源的虚拟机的网络连接。

### SR-IOV 概览

SR-IOV 是一种规范，使得单根端口下的单个快速外围组件互连 (PCIe) 物理设备可针对管理程序或客户机操作系统显示为多个单独的物理设备。

SR-IOV 使用物理功能 (PF) 和虚拟功能 (VF) 为 SR-IOV 设备管理全局功能。PF 是完整的 PCIe 功能，其能够配置和管理 SR-IOV 功能。可以使用 PF 来配置和控制 PCIe 设备，且 PF 具有将数据移入和移出设备的完整功能。VF 是轻量级的 PCIe 功能，其支持数据流动但具有一套受限的配置资源集。

向管理程序或客户机操作系统提供的虚拟功能数量取决于设备。已启用 SR-IOV 的 PCIe 设备在客户机操作系统驱动程序或管理程序实例中需要适当的 BIOS 和硬件支持以及 SR-IOV 支持。请参见第 122 页，“SR-IOV 支持”。

### 在 vSphere 中使用 SR-IOV

在 vSphere 中，虚拟机可将 SR-IOV 虚拟功能用于网络连接。虚拟机和物理适配器直接交换数据，而不使用 VMkernel 作为中介。绕过 VMkernel 进行网络连接可减少滞后时间并提高 CPU 效率。

在 vSphere 5.5 及更高版本中，虽然虚拟交换机（标准交换机或 Distributed Switch）不会处理连接到交换机的已启用 SR-IOV 的虚拟机的网络流量，但您可使用端口组或端口级别的交换机配置策略来控制已分配的虚拟功能。

### SR-IOV 支持

vSphere 5.1 及更高版本仅在具有特定配置的环境中支持 SR-IOV。某些 vSphere 功能在启用 SR-IOV 后会失效。

#### 支持的配置

要在 vSphere 6.0 中使用 SR-IOV，您的环境必须满足若干配置要求。

**表 10-1 要使用 SR-IOV 所需支持的配置**

组件	要求
vSphere	<ul style="list-style-type: none"> <li>■ 配备 Intel 处理器的主机需要使用 ESXi 5.1 或更高版本。</li> <li>■ 在 ESXi 5.5 或更高版本中，配备 AMD 处理器的主机受 SR-IOV 支持。</li> </ul>
物理主机	<ul style="list-style-type: none"> <li>■ 必须与 ESXi 版本兼容。</li> <li>■ 如果运行 ESXi 5.1，则必须配备 Intel 处理器，如果运行 ESXi 5.5 及更高版本，则必须配备 Intel 或 AMD 处理器。</li> <li>■ 必须支持 I/O 内存管理单元 (IOMMU)，并且必须在 BIOS 中启用 IOMMU。</li> <li>■ 必须支持 SR-IOV，并且必须在 BIOS 中启用 SR-IOV。请联系服务器供应商以确定主机是否支持 SR-IOV。</li> </ul>
物理网卡	<ul style="list-style-type: none"> <li>■ 必须与 ESXi 版本兼容。</li> <li>■ 根据服务器供应商提供的技术文档，必须支持用于主机和 SR-IOV。</li> <li>■ 必须在固件中启用 SR-IOV。</li> <li>■ 必须使用 MSI-X 中断。</li> </ul>
对于物理网卡，在 ESXi 中使用 PF 驱动程序	<ul style="list-style-type: none"> <li>■ 必须经过 VMware 的认证。</li> <li>■ 必须安装在 ESXi 主机上。对于某些网卡，ESXi 版本提供默认驱动程序，而对于其他版本，必须下载并手动安装驱动程序。</li> </ul>

表 10-1 要使用 SR-IOV 所需支持的配置（续）

组件	要求
客户机操作系统	根据网卡供应商提供的技术文档，必须受已安装的 ESXi 版本上的网卡支持。
客户机操作系统中使用 VF 驱动程序	<ul style="list-style-type: none"> <li>■ 必须与网卡兼容。</li> <li>■ 根据网卡供应商提供的技术文档，必须受客户机操作系统版本的支持。</li> <li>■ 必须由 Microsoft WLK 或 WHCK 针对 Windows 虚拟机进行认证。</li> <li>■ 必须安装在操作系统中。对于某些网卡，操作系统版本中包含默认驱动程序，而对于其他网卡，则必须从网卡供应商或主机供应商所提供的位置下载并安装驱动程序。</li> </ul>

要确认物理主机和网卡是否与 ESXi 版本兼容，请参见《VMware 兼容性指南》。

## 功能可用性

以下功能对配置了 SR-IOV 的虚拟机不可用：

- vSphere vMotion
- Storage vMotion
- vShield
- NetFlow
- VXLAN 虚拟线路
- vSphere High Availability
- vSphere Fault Tolerance
- vSphere DRS
- vSphere DPM
- 虚拟机挂起和恢复
- 虚拟机快照
- 用于直通虚拟功能的基于 MAC 的 VLAN
- 热添加和删除虚拟设备、内存和 vCPU
- 加入到群集环境
- 使用 SR-IOV 直通的虚拟机网卡的网络统计信息

**注意** 如果在 vSphere Web Client 中尝试启用或配置使用 SR-IOV 的不受支持的功能，会导致环境中出现意外行为。

## 受支持的网卡

所有网卡必须具有支持 SR-IOV 的驱动程序和固件。某些网卡可能需要在固件上启用 SR-IOV。配置了 SR-IOV 的虚拟机支持以下网卡：

- 基于 Intel 82599ES 10 GB 以太网控制器系列的产品 (Niantic)
- 基于 Intel 以太网控制器 X540 系列的产品 (Twinville)
- 基于 Intel 以太网控制器 X710 系列的产品 (Fortville)
- 基于 Intel 以太网控制器 XL170 系列的产品 (Fortville)

## ■ Emulex OneConnect (BE3)

### 从 vSphere 5.0 及之前的版本升级

如果从 vSphere 5.0 或更早的版本升级到 vSphere 5.5 或更高的版本，则在为 vSphere 版本更新网卡驱动程序之前，无法取得 SR-IOV 支持。必须为网卡启用支持 SR-IOV 的固件和驱动程序，以使 SR-IOV 功能正常运行。

### 从 vSphere 5.1 升级

尽管在满足要求的 ESXi 5.1 主机上支持 SR-IOV，但您无法使用 vSphere Web Client 在这些主机上配置 SR-IOV。使用网卡驱动程序模块的 `max_vfs` 参数在这些主机上启用 SR-IOV。请参见第 130 页，“使用主机配置文件或 ESXCLI 命令启用 SR-IOV”。

您也无法将 SR-IOV 直通适配器分配给此类主机上的虚拟机。该适配器可供与 ESXi 5.5 及更高版本兼容的虚拟机使用。虽然 vCenter Server 5.5 版本可能正在管理 ESXi 5.1 主机，但配置将与版本 5.1 中相同。必须将 PCI 设备添加到虚拟机硬件，并手动为该设备选择 VF。

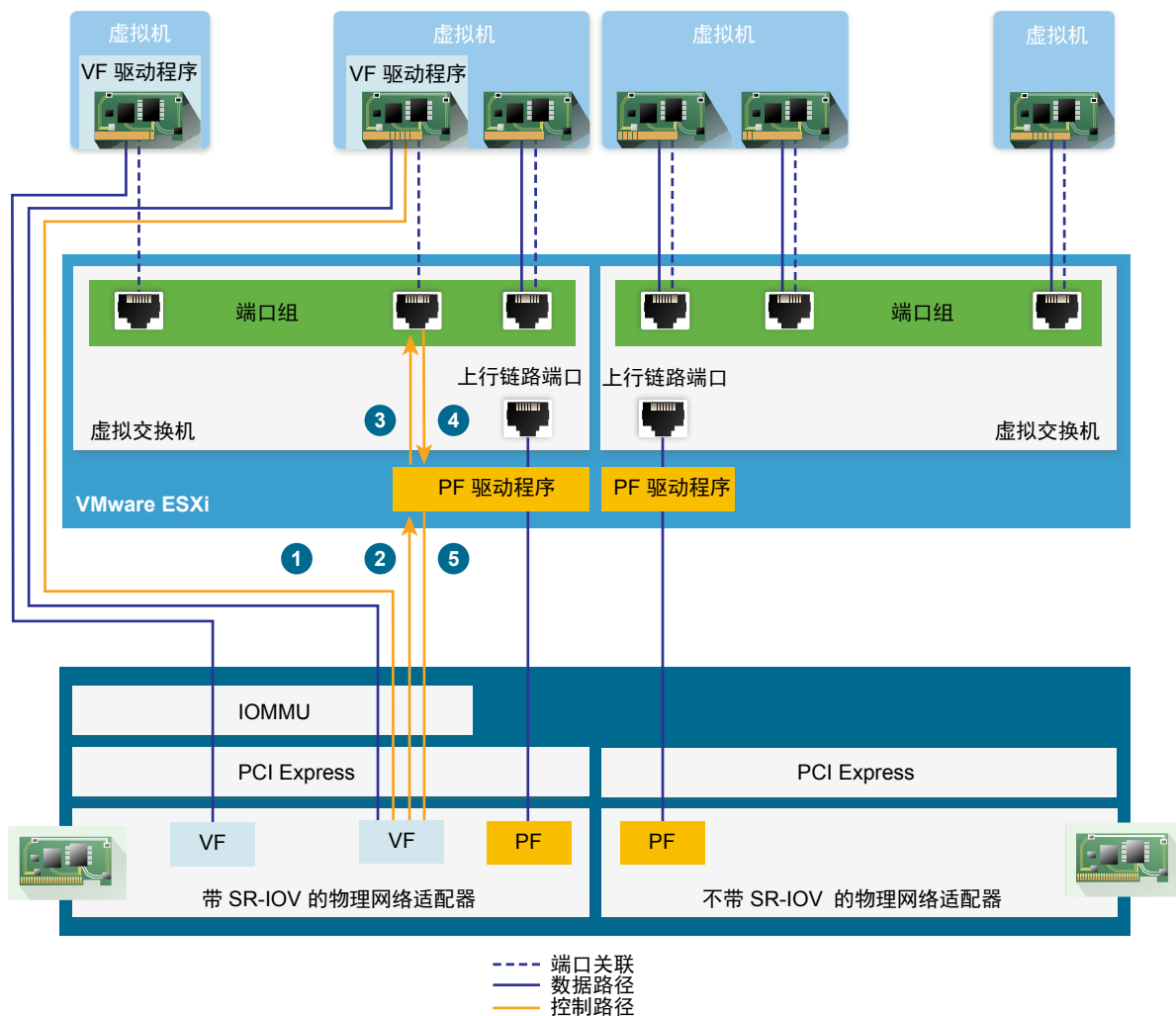
## SR-IOV 组件架构和交互

vSphere SR-IOV 支持依赖于网卡端口虚拟功能 (VF) 和物理功能 (PF) 之间的交互以提高性能，依赖于 PF 驱动程序和主机交换机之间的交互以实现流量控制。

在主机中，如果在 SR-IOV 物理适配器上运行虚拟机流量，则虚拟机适配器将直接联系虚拟功能以传递数据。但是，能否配置网络基于虚拟机所在端口的活动策略。

在没有 SR-IOV 的 ESXi 主机上，虚拟交换机通过主机上的相应端口发送流出或流入相关端口组的物理适配器的外部网络流量。此外，虚拟交换机也会将网络策略应用于受管数据包。

图 10-1 vSphere SR-IOV 支持中的数据路径和配置路径



## SR-IOV 中的数据路径

将虚拟网络适配器分配给某一虚拟功能后，客户机操作系统中的 VF 驱动程序会使用 I/O 内存管理单元 (IOMMU) 技术访问必须通过网络才能接收和发送数据的虚拟功能。VMkernel（尤其是虚拟交换机）不会处理数据流，这缩短了已启用 SR-IOV 的工作负载的整体滞后时间。

## SR-IOV 中的配置路径

当客户机操作系统尝试更改映射到 VF 的虚拟机适配器的配置时，如果与此虚拟机适配器关联的端口上的策略允许此更改，则将执行更改。

配置工作流程包括以下操作：

- 1 客户机操作系统请求更改 VF 的配置。
- 2 VF 通过邮箱机制将该请求转发至 PF。
- 3 PF 驱动程序向虚拟交换机（标准交换机或 Distributed Switch 的主机代理交换机）确认配置请求。
- 4 虚拟交换机根据与已启用 VF 的虚拟机适配器关联的端口上的策略验证配置请求。
- 5 如果新的设置符合虚拟机适配器的端口策略，则 PF 驱动程序将配置 VF。

例如，当 VF 驱动程序尝试修改 MAC 地址时，如果端口组或端口的安全策略不允许更改 MAC 地址，则该地址将保持不变。客户机操作系统可能会显示更改已成功完成，但日志消息将表明此操作失败。因此，客户机操作系统和虚拟设备保存的 MAC 地址不同。客户机操作系统中的网络接口可能无法获取 IP 地址并进行通信。在这种情况下，必须重置客户机操作系统中的接口，以从虚拟设备获得最新的 MAC 地址并获取 IP 地址。

## vSphere 和虚拟功能交互

虚拟功能 (VF) 是轻量级的 PCIe 功能，其包含数据交换所需的所有资源，但仅有一套最精简的配置资源集。vSphere 与 VF 之间的交互是有限的。

- 物理网卡必须使用 MSI-X 中断。
- VF 不在 vSphere 中实现速率控制。每个 VF 都可能使用一个物理链路的整个带宽。
- 将 VF 设备配置为虚拟机上的直通设备时，不支持虚拟机待机和休眠功能。
- 可以创建的最大 VF 数以及可用于直通的最大 VF 数不同。可以实例化的最多 VF 数量取决于网卡功能以及主机的硬件配置。但是，由于可供直通设备使用的中断向量的数量有限，在 ESXi 主机上只能使用数量有限（而非全部）的实例化 VF。

如果使用 32 个 CPU，每个 ESXi 主机上的中断向量总数可以扩展到 4096 个。主机引导时，该主机上的设备（如存储控制器、物理网络适配器和 USB 控制器）将占用这 4096 个向量中的部分向量。如果这些设备需要的向量数超过 1024 个，则可能支持的最多 VF 数量会减少。

- Intel 网卡上支持的 VF 数可能与 Emulex 网卡上支持的数目不同。请参见网卡供应商提供的技术文档。
- 如果具有 Intel 和 Emulex 网卡，并启用了 SR-IOV，则可供 Intel 网卡使用的 VF 数量取决于为 Emulex 网卡配置的 VF 数量，反之亦然。可以使用以下公式估算在所有 3072 个中断向量均可用的情况下可用于直通设备的 VF 的最大数量：

$$3X + 2Y < 3072$$

其中 X 是 Intel VF 的数量，Y 是 Emulex VF 的数量。

如果在主机上的所有 4096 个向量中，由主机上其他类型的设备使用的中断向量数超过 1024 个，则此数值可能会更小。

- vSphere SR-IOV 在支持的 Intel 和 Emulex 网卡上最多支持 1024 个 VF。
- vSphere SR-IOV 在支持的 Intel 或 Emulex 网卡上最多支持 64 个 VF。
- 如果所用的 Intel 网卡连接丢失，则来自物理网卡的所有 VF 将完全停止通信（包括 VF 之间的通信）。
- 如果所用的 Emulex 网卡连接丢失，则所有 VF 都将停止与外部环境通信，但 VF 之间的通信仍可进行。
- VF 驱动程序提供大量不同的功能，如 IPv6 支持、TSO 和 LRO 校验和。有关更多详细信息，请参见网卡供应商的技术文档。

## DirectPath I/O 和 SR-IOV

SR-IOV 对性能的影响利弊与 DirectPath I/O 相似。DirectPath I/O 与 SR-IOV 功能相似，但用于完成不同的任务。

SR-IOV 对于要求数据包传输速率非常高或延迟非常低的工作负载非常有利。与 DirectPath I/O 一样，SR-IOV 与 vMotion 等某些核心虚拟化功能也不兼容。但是，SR-IOV 允许在多个客户机之间共享一个物理设备。

使用 DirectPath I/O，只能将一项物理功能映射到一个虚拟机。使用 SR-IOV，您可共享单个物理设备，使多个虚拟机直接连接到物理功能。

## 配置虚拟机以使用 SR-IOV

要使用 SR-IOV 的功能，必须在主机上启用 SR-IOV 虚拟功能，然后将虚拟机连接到这些功能。

### 前提条件

验证您的环境配置是否支持 SR-IOV。请参见 [第 122 页](#)，“SR-IOV 支持”。

### 步骤

- 1 在[主机物理适配器上启用 SR-IOV](#) [第 127 页](#)，  
请先使用 vSphere Web Client 为主机启用 SR-IOV 并设置虚拟功能的数量，然后才能将虚拟机连接到虚拟功能。
- 2 将虚拟功能作为 [SR-IOV 直通适配器](#) 分配给虚拟机 [第 128 页](#)，  
要确保虚拟机和物理网卡能够交换数据，必须将虚拟机与一个或多个虚拟功能关联作为 SR-IOV 直通网络适配器。

根据标准交换机或 Distributed Switch 的关联端口上的活动策略，流量将从 SR-IOV 直通适配器传递到物理适配器。

要检查为 SR-IOV 直通网络适配器所分配的虚拟功能，请在虚拟机的[摘要](#)选项卡中，展开[虚拟机硬件](#)面板，并检查适配器的属性。

交换机的拓扑图使用图标标记使用虚拟功能的虚拟机适配器。

### 下一步

使用交换机、端口组和端口上的网络连接策略设置通过连接到虚拟机的虚拟功能的流量。请参见 [第 129 页](#)，“与已启用 SR-IOV 的虚拟机关联的流量网络选项”。

## 在主机物理适配器上启用 SR-IOV

请先使用 vSphere Web Client 为主机启用 SR-IOV 并设置虚拟功能的数量，然后才能将虚拟机连接到虚拟功能。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在[配置](#)选项卡上，展开[网络](#)，然后选择[物理适配器](#)。  
您可以查看 SR-IOV 属性，以确定物理适配器是否支持 SR-IOV。
- 3 选择物理适配器，然后单击[编辑适配器设置](#)。
- 4 在 SR-IOV 下，从[状态](#)下拉菜单中选择[已启用](#)。
- 5 在[虚拟功能数](#)文本框中，键入要为此适配器配置的虚拟功能的数量。
- 6 单击[确定](#)。
- 7 重新启动主机。

虚拟功能将在由物理适配器条目表示的网卡端口上变为活动状态。它们将显示在主机的[设置](#)选项卡的 PCI 设备列表中。

可以使用 `esxcli network sriovnic vCLI` 命令来检查主机上的虚拟功能配置。

### 下一步

通过 SR-IOV 直通网络适配器，将虚拟机与虚拟功能相关联。

## 将虚拟功能作为 SR-IOV 直通适配器分配给虚拟机

要确保虚拟机和物理网卡能够交换数据，必须将虚拟机与一个或多个虚拟功能关联作为 SR-IOV 直通网络适配器。

### 前提条件

- 验证主机上是否存在虚拟功能。
- 在主机的**设置**选项卡上的“PCI 设备”列表中确认虚拟功能的直通网络设备处于活动状态。
- 确认虚拟机兼容性为 ESXi 5.5 和更高版本。
- 创建虚拟机时，确认已选择 Red Hat Enterprise Linux 6 和更高版本或 Windows 作为客户机操作系统。

### 步骤

- 1 在 vSphere Web Client 中找到虚拟机。
  - a 选择数据中心、文件夹、群集、资源池或主机，然后单击**虚拟机**选项卡。
  - b 单击**虚拟机**，然后从列表中双击虚拟机。
- 2 关闭虚拟机电源。
- 3 在虚拟机的**配置**选项卡上，展开**设置**，然后选择**虚拟机硬件**。
- 4 单击**编辑**，然后在显示设置的对话框中选择**虚拟硬件**选项卡。
- 5 从**新设备**下拉菜单中，选择**网络**，然后单击**添加**。
- 6 展开“新建网络”部分并将虚拟机连接到端口组。
 

虚拟网卡不会为数据流量使用此端口组。此端口组用于提取要应用于数据流量的网络属性（例如 VLAN 标记）。
- 7 在**适配器类型**下拉菜单中，选择 **SR-IOV 直通**。
- 8 在**物理功能**下拉菜单中，选择要备份直通虚拟机适配器的物理适配器。
- 9 要允许从客户机操作系统更改数据包的 MTU，请使用**客户机操作系统 MTU 更改**下拉菜单。
- 10 展开“内存”部分，选择**预留所有客户机内存 (全部锁定)**，然后单击**确定**。
 

I/O 内存管理单元 (IOMMU) 必须访问所有虚拟机内存，从而使直通设备可以使用直接内存访问 (DMA) 来访问内存。
- 11 打开虚拟机电源。

打开虚拟机电源时，ESXi 主机将从物理适配器中选择可用的虚拟功能，并将其映射到 SR-IOV 直通适配器。主机将根据虚拟机所属的端口组设置来验证虚拟机适配器的所有属性和底层虚拟功能。



## 与已启用 SR-IOV 的虚拟机关联的流量网络选项

在 vSphere 5.5 及更高版本中，可以在与虚拟功能 (VF) 关联的虚拟机适配器上配置特定的网络功能。根据处理流量的虚拟交换机的类型（标准或分布式）来使用交换机、端口组或端口的设置。

**表 10-2 使用 VF 的虚拟机适配器的网络选项**

网络选项	描述
MTU 大小	例如，更改 MTU 的大小以启用巨帧。
VF 流量的安全策略	<ul style="list-style-type: none"><li>■ 如果客户机操作系统更改使用 VF 的虚拟机网络适配器最初设置的 MAC 地址，则通过设置 <b>MAC 地址更改</b> 选项来接受或丢弃新地址的入站帧。</li><li>■ 为虚拟机网络适配器（包括使用 VF 的适配器）启用全局混杂模式。</li></ul>
VLAN 标记模式	在标准交换机或 Distributed Switch 中配置 VLAN 标记，即，启用 VLAN 交换机标记 (VST) 模式；或者使标记的流量访问与 VF 关联的虚拟机，即，启用虚拟客户机标记 (VGT)。

## 使用 SR-IOV 物理适配器处理虚拟机流量


在 vSphere 5.5 及更高版本中，可以将同时支持 SR-IOV 物理适配器的物理功能 (PF) 和虚拟功能 (VF) 配置为处理虚拟机流量。

SR-IOV 物理适配器的 PF 控制虚拟机使用的 VF，并且可以承载流经负责处理启用了 SR-IOV 的虚拟机的网络连接的标准交换机或 Distributed Switch 的流量。

SR-IOV 物理适配器在不同的模式下运行，具体取决于该适配器是否备份交换机的流量。


### 混合模式

物理适配器向连接到交换机的虚拟机提供虚拟功能，并直接处理交换机上来自非 SR-IOV 虚拟机的流量。

可以在交换机的拓扑图中检查 SR-IOV 物理适配器是否处于混合模式。处于混合模式的 SR-IOV 物理适配器在标准交换机的物理适配器列表中或 Distributed Switch 的上行链路组适配器列表中显示时带有  图标。

### 仅 SR-IOV 模式

物理适配器向连接到虚拟交换机的虚拟机提供虚拟功能，但不备份交换机上来自非 SR-IOV 虚拟机的流量。

要验证物理适配器是否处于仅 SR-IOV 模式，请检查交换机的拓扑图。在此模式下，物理适配器位于称为“外部 SR-IOV 适配器”的独立列表中，显示时带有  图标。

### 非 SR-IOV 模式

物理适配器不用于与 VF 感知虚拟机有关的流量。仅负责处理来自非 SR-IOV 虚拟机的流量。

## 使用主机配置文件或 ESXCLI 命令启用 SR-IOV

可以使用 ESXCLI 命令在 ESXi 主机上配置虚拟功能，或者使用主机配置文件同时设置多个主机或设置无状态的主机。

### 在主机配置文件中启用 SR-IOV

对于多台主机或无状态主机，可使用主机配置文件来配置物理网卡的虚拟功能，并使用 Auto Deploy 在主机上应用配置文件。

有关将 Auto Deploy 与主机配置文件结合使用来运行 ESXi 的信息，请参见 *vSphere 安装和设置* 文档。

根据驱动程序文档，还可以通过使用虚拟功能的网卡驱动程序参数中的 `esxcli system module parameters set vCLI` 命令来启用主机上的 SR-IOV 虚拟功能。有关使用 vCLI 命令的详细信息，请参见《vSphere 命令行界面文档》。

#### 前提条件

- 验证您的环境配置是否支持 SR-IOV。请参见 [第 122 页](#)，“SR-IOV 支持”。
- 基于支持 SR-IOV 的主机，创建主机配置文件。请参见《vSphere 主机配置文件》文档。

#### 步骤

- 1 在 vSphere Web Client 主页中，单击**主机配置文件**。
- 2 从列表中选择主机配置文件，然后单击**配置**选项卡。
- 3 单击**编辑主机配置文件**，然后展开**常规系统设置**节点。
- 4 展开**内核模块参数**，然后选择用于创建虚拟功能的物理功能驱动程序的参数。

例如，Intel 物理网卡的物理功能驱动程序的参数为 `max_vfs`。

- 5 在**值**文本框中，键入以逗号分隔的有效虚拟功能的数量列表。

每个列表条目表示要为每项物理功能配置的虚拟功能的数量。值 0 将确保不为该物理功能启用 SR-IOV。

例如，如果配置了双端口，请将该值设置为 `x,y`，其中 `x` 或 `y` 表示要为单个端口启用的虚拟功能的数量。

如果一个主机上的虚拟功能的目标数为 30 个，则可将两个双端口卡设置为 `0,10,10,10`。

---

**注意** 受支持和可配置的虚拟功能数量取决于系统配置。

---

- 6 单击**完成**。
- 7 根据需要，修复主机的主机配置文件。

虚拟功能将显示在主机的主机配置文件的**设置**选项卡的 PCI 设备列表中。

#### 下一步

使用 SR-IOV 直通网络适配器类型将虚拟功能与虚拟机适配器相关联。请参见 [第 128 页](#)，“将虚拟功能作为 SR-IOV 直通适配器分配给虚拟机”。

### 通过使用 ESXCLI 命令为主机物理适配器启用 SR-IOV

在进行某些故障排除或直接配置主机时，可在 ESXi 上运行控制台命令，以便在物理适配器上创建 SR-IOV 虚拟功能。

根据驱动程序文档，可以通过操作虚拟功能的网卡驱动程序参数，从而在主机上创建 SR-IOV 虚拟功能。

## 前提条件

安装 vCLI 软件包、部署 vSphere Management Assistant (vMA) 虚拟机，或者使用 ESXi Shell。请参见 *vSphere Command-Line Interface 入门*。

## 步骤

- 1 要通过设置网卡驱动程序的虚拟功能参数来创建虚拟功能，请在命令提示符下运行 `esxcli system module parameters set` 命令。

```
esxcli system module parameters set -m driver -p vf_param=w,x,y,z
```

其中，*driver* 指网卡驱动程序的名称，*vf\_param* 指创建虚拟功能所需的驱动程序特定的参数。

您可以使用逗号分隔列表设置 *vf\_param* 参数的值，其中每个条目表示端口的虚拟功能数量。值 0 将确保不为该物理功能启用 SR-IOV。

如果配置了两个双端口网卡，则可将值设置为 *w,x,y,z*，其中 *w*、*x*、*y* 和 *z* 指要为单个端口启用的虚拟功能的数量。例如，要使用 `ixgbe` 驱动程序创建分布在两个双端口 Intel 卡上的 30 个虚拟功能，请对 `ixgbe` 驱动程序和 `max_vfs` 参数运行以下命令：

```
esxcli system module parameters set -m ixgbe -p max_vfs=0,10,10,10
```

- 2 重新启动主机以创建虚拟功能。

## 下一步

使用 SR-IOV 直通网络适配器类型将虚拟功能与虚拟机适配器相关联。请参见第 128 页，“[将虚拟功能作为 SR-IOV 直通适配器分配给虚拟机](#)”。

## 由于主机的中断向量已耗尽，因此使用 SR-IOV 虚拟功能的虚拟机打开电源失败

在 ESXi 主机上，使用 SR-IOV 虚拟功能 (VF) 进行网络连接的一个或多个虚拟机电源关闭。

### 问题

在 ESXi 主机中，如果已分配的虚拟功能 (VF) 总数已接近在《vSphere 的最高配置》指南中指定的最多 VF 数量，则使用 SR-IOV 虚拟功能进行网络连接的一个或多个虚拟机打开电源将失败。

虚拟机日志文件 `vmware.log` 包含以下有关 VF 的消息：

```
PCIPassthruChangeIntrSettings:vf_name failed to register interrupt (error code 195887110)
```

VMkernel 日志文件 `vmkernel.log` 包含以下有关分配给虚拟机的 VF 的消息：

```
VMKPCIPassthru:2565: BDF = vf_name intrType = 4 numVectors: 3
WARNING:IntrVector:233: Out of interrupt vectors
```

### 原因

可分配的中断向量数量随着 ESXi 主机上的物理 CPU 数量增加。一个具有 32 个 CPU 的 ESXi 主机共计可提供 4096 个中断向量。主机引导时，该主机上的设备（如存储控制器、物理网络适配器和 USB 控制器）将占用这 4096 个向量中的部分向量。如果这些设备需要的向量数超过 1024 个，则可能支持的最多 VF 数量会减少。

打开虚拟机电源并启动客户机操作系统 VF 驱动程序时，系统将占用中断向量。如果没有所需数量的中断向量，则客户机操作系统将意外关闭，而不会出现任何错误消息。

目前，尚没有规则可以确定主机上已占用的或可用的中断向量数量。该数量取决于主机的硬件配置。

### 解决方案

- ◆ 要打开虚拟机电源，请减少分配给主机上的虚拟机的总 VF 数量。

例如，将虚拟机的 SR-IOV 网络适配器更改为连接到 vSphere 标准交换机或 vSphere Distributed Switch 的适配器。

## 虚拟机的远程直接内存访问

vSphere 6.5 及更高版本支持在具有准虚拟化 RDMA (PVRDMA) 网络适配器的虚拟机之间进行远程直接内存访问 (RDMA) 通信。

### RDMA 概览

RDMA 允许从一台计算机内存到另一台计算机内存的直接内存访问，不会涉及操作系统或 CPU。内存的传输卸载至支持 RDMA 的主机通道适配器 (Host Channel Adapter, HCA)。PVRDMA 网络适配器在虚拟环境中提供远程直接内存访问。

### 在 vSphere 中使用 RDMA

在 vSphere 中，虚拟机可以使用 PVRDMA 网络适配器与其他拥有 PVRDMA 设备的虚拟机进行通信。虚拟机必须连接到同一 vSphere Distributed Switch。

PVRDMA 设备自动选择两个虚拟机之间的通信方法。对于相同 ESXi 主机上运行的虚拟机（无论是否具有物理 RDMA 设备），两个虚拟机之间的数据传输是一种内存复制。这种情况下不使用物理 RDMA 硬件。

对于不同 ESXi 主机上运行的虚拟机（具有物理 RDMA 连接），物理 RDMA 设备必须是 Distributed Switch 上的上行链路。在这种情况下，两个虚拟机之间的 PVRDMA 通信使用底层物理 RDMA 设备。

对于不同 ESXi 主机上运行的两个虚拟机（至少一个虚拟机没有物理 RDMA 设备），通信回退到基于 TCP 的通道，且性能减弱。

### PVRDMA 支持

vSphere 6.5 和更高版本仅在具有特定配置的环境中支持 PVRDMA。

#### 支持的配置

要在 vSphere 6.5 中使用 PVRDMA，您的环境必须满足若干配置要求。

**表 10-3 使用 PVRDMA 所需的支持配置**

组件	要求
vSphere	<ul style="list-style-type: none"> <li>■ ESXi 主机 6.5 或更高版本。</li> <li>■ vCenter Server 或 vCenter Server Appliance 6.5 或更高版本。</li> <li>■ vSphere Distributed Switch。</li> </ul>
物理主机	<ul style="list-style-type: none"> <li>■ 必须与 ESXi 版本兼容。</li> </ul>
主机通道适配器 (HCA)	<ul style="list-style-type: none"> <li>■ 必须与 ESXi 版本兼容。</li> </ul> <p><b>注意</b> 不同 ESXi 主机上的虚拟机需要 HCA 才能使用 RDMA。您必须将 HCA 分配为 vSphere Distributed Switch 的上行链路。PVRDMA 不支持网卡绑定。HCA 必须是 vSphere Distributed Switch 上唯一的上行链路。</p> <p>对于同一 ESXi 主机上的虚拟机或使用基于 TCP 的回退的虚拟机，HCA 不是必需的。</p>

表 10-3 使用 PVRDMA 所需的支持配置（续）

组件	要求
虚拟机	■ 虚拟硬件版本 13 或更高版本。
客户机操作系统	■ Linux (64 位)

要验证物理主机和 HCA 是否与 ESXi 版本兼容，请参见《VMware 兼容性指南》。

**注意** 如果在 vSphere Web Client 中尝试使用 PVRDMA 启用或配置不受支持的功能，则会在该环境中出现意外行为。

## 为 ESXi 主机配置 PVRDMA

配置 ESXi 主机的 VMkernel 适配器和防火墙规则以便实现 PVRDMA 通信。

### 前提条件

确认 ESXi 主机满足 PVRDMA 的要求。请参见第 132 页，“PVRDMA 支持”。

- 为 PVRDMA 标记 VMkernel 适配器第 133 页，  
选择 VMkernel 适配器并启用，以进行 PVRDMA 通信。
- 为 PVRDMA 启用防火墙规则第 133 页，  
在 ESXi 主机的安全配置文件中为 PVRDMA 启用防火墙规则。

### 为 PVRDMA 标记 VMkernel 适配器

选择 VMkernel 适配器并启用，以进行 PVRDMA 通信。

#### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开系统。
- 3 单击高级系统设置。
- 4 找到 Net.PVRDMAvmknic 并单击编辑。
- 5 输入要使用的 VMkernel 适配器的值（例如 vmk0），然后单击确定。

### 为 PVRDMA 启用防火墙规则

在 ESXi 主机的安全配置文件中为 PVRDMA 启用防火墙规则。

#### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开系统。
- 3 单击安全配置文件。
- 4 在“防火墙”部分中，单击编辑。
- 5 滚动到 pvrDMA 规则，然后选中该规则旁边的复选框。
- 6 单击确定。

## 向虚拟机分配 PVRDMA 适配器

要使虚拟机使用 RDMA 交换数据，您必须将该虚拟机与 PVRDMA 网络适配器关联。

### 前提条件

- 确认运行该虚拟机的主机配置了 RDMA。请参见第 133 页，“为 ESXi 主机配置 PVRDMA”。
- 确认主机已连接到 vSphere Distributed Switch。
- 确认虚拟机使用虚拟硬件版本 13。
- 确认客户机操作系统为 Linux 64 位发行版。

### 步骤

- 1 在 vSphere Web Client 中找到虚拟机。
  - a 选择数据中心、文件夹、群集、资源池或主机，然后单击**虚拟机**选项卡。
  - b 单击**虚拟机**，然后从列表中双击虚拟机。
- 2 关闭虚拟机电源。
- 3 在虚拟机的**配置**选项卡上，展开**设置**，然后选择**虚拟机硬件**。
- 4 单击**编辑**，然后在显示设置的对话框中选择**虚拟硬件**选项卡。
- 5 从**新设备**下拉菜单中，选择**网络**，然后单击**添加**。
- 6 展开“新建网络”部分并将虚拟机连接到分布式端口组。
- 7 在**适配器类型**下拉菜单中，选择 PVRDMA。
- 8 展开**内存**部分，选择**预留所有客户机内存 (全部锁定)**，然后单击**确定**。
- 9 打开虚拟机电源。

## 聚合以太网 RDMA 的网络要求

聚合以太网 RDMA 可确保在以太网网络上实现低延迟、高吞吐量的轻量 RDMA 通信。RoCE 需要配置为单独在第 2 层或同时在第 2 层和第 3 层上无损传输信息流量的网络。

聚合以太网 RDMA (RDMA over Converged Ethernet, RoCE) 是一种网络协议，使用 RDMA 为网络密集型应用程序提供更快的数据传输。RoCE 可以在主机之间实现直接的内存传输，而无需使用主机的 CPU。

RoCE 协议有两个版本。RoCE v1 在链接网络层（第 2 层）上运行。RoCE v2 在 Internet 网络层（第 3 层）上运行。RoCE v1 和 RoCE v2 都需要无损网络配置。RoCE v1 需要第 2 层无损网络，而 RoCE v2 则要求为第 2 层和第 3 层均配置无损操作。

### 第 2 层无损网络

要确保第 2 层无损环境，您必须能够控制流量。可以通过在整个网络上启用全局暂停或使用数据中心桥接组 (Data Center Bridging, DCB) 定义的优先级流量控制 (Priority Flow Control, PFC) 协议来实现流量控制。PFC 是第 2 层协议，使用 802.1Q VLAN 标记的服务类字段设置各个流量的优先级。它会根据各个服务类优先级暂停到某个接收方的数据包传输。这样，将由一个链接同时承载无损 RoCE 流量和其他有损但尽力保留的流量。如果发生流量拥堵，可能会影响到重要的有损流量。要隔离不同的流量，可以在启用了 PFC 优先级的 VLAN 中使用 RoCE。

## 第 3 层无损网络

RoCE v2 要求在第 3 层路由设备中保留无损数据传输。要跨第 3 层路由器实现第 2 层 PFC 无损优先级传输，可以对路由器进行相应配置，把数据包的接收优先级设置映射到第 3 层的相应差异化服务代码点 (Differentiated Serviced Code Point, DSCP) QoS 设置。传输的 RDMA 数据包标记了第 3 层 DSCP、第 2 层优先级代码点 (Priority Code Point, PCP) 或同时标记了这两者。路由器使用 DSCP 或 PCP 从数据包中提取优先级。如果使用 PCP，数据包必须带有 VLAN 标记，且路由器必须复制标记的 PCP 位并将其转发到下一个网络。如果数据包标记了 DSCP，则路由器必须保持 DSCP 位不变。

与 RoCE v1 一样，RoCE v2 必须在启用了 PFC 优先级的 VLAN 上运行。

---

**注意** 如果要在 RoCE 网卡上使用 RDMA，切勿绑定这些网卡。

---

有关供应商特定的配置信息，请参考相应设备或交换机供应商的官方文档。

## 巨帧

巨帧允许 ESXi 主机将较大的帧发送到物理网络上。网络必须端到端支持巨帧（包括物理网络适配器、物理交换机和存储设备）。

在启用巨帧之前，请与硬件供应商核对，确保您的物理网络适配器支持巨帧。

通过将最大传输单元 (MTU) 更改为大于 1500 字节的值，可以在 vSphere Distributed Switch 或 vSphere 标准交换机上启用巨帧。您可配置的最大帧大小为 9000 字节。

### 在 vSphere Distributed Switch 上启用巨帧

为流经 vSphere Distributed Switch 的整个流量启用巨帧。

#### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在配置选项卡上，展开设置并选择属性。
- 3 单击编辑。
- 4 单击高级，然后将 MTU 属性设置为一个大于 1500 字节的值。  
不能将 MTU 大小设置为一个大于 9000 字节的值。
- 5 单击确定。

### 在 vSphere 标准交换机上启用巨帧

为主机上流经 vSphere 标准交换机的所有流量启用巨帧。

#### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开网络，然后选择虚拟交换机。
- 3 从虚拟交换机表中选择一台标准交换机，然后单击编辑设置。
- 4 在属性部分，将 MTU 属性设置为大于 1500 字节的值。  
可以将 MTU 的大小最大增大到 9000 个字节。
- 5 单击确定。

## 为 VMkernel 适配器启用巨帧

巨帧减少了由传输数据引起的 CPU 负载。在 VMkernel 适配器上通过更改适配器的最大传输单元 (MTU) 来启用巨帧。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在**配置**选项卡上，展开**网络**，然后选择 **VMkernel 适配器**。
- 3 从适配器表中选择 VMkernel 适配器。  
此时将显示适配器属性。
- 4 单击 VMkernel 适配器的名称。
- 5 单击**编辑**。
- 6 选择**网卡设置**，然后将 **MTU** 属性的值设置为大于 1500。  
可以将 MTU 的大小最大增大到 9000 个字节。
- 7 单击**确定**。

## 在虚拟机上启用巨帧支持

要在虚拟机上启用巨帧支持，该虚拟机需要增强型 VMXNET 适配器。

### 步骤

- 1 在 vSphere Web Client 中找到虚拟机。
  - a 选择数据中心、文件夹、群集、资源池或主机，然后单击**虚拟机**选项卡。
  - b 单击**虚拟机**，然后从列表中双击虚拟机。
- 2 在虚拟机的**配置**选项卡上，展开**设置**，然后选择**虚拟机硬件**。
- 3 单击**编辑**，然后在显示设置的对话框中选择**虚拟硬件**选项卡。
- 4 展开 **网络适配器**部分。记录网络适配器所使用的网络设置和 MAC 地址。
- 5 单击**移除**将该网络适配器从虚拟机中移除。
- 6 从**新设备**下拉菜单中，选择**网络**，然后单击**添加**。
- 7 从**适配器类型**下拉菜单中，选择 **VMXNET 2（增强型）**或 **VMXNET 3**。
- 8 将网络设置设置为记录的旧网络适配器设置。
- 9 将 **MAC 地址**设置为**手动**，然后键入旧网络适配器使用的 MAC 地址。
- 10 单击**确定**。

### 下一步

- 检查增强型 VMXNET 适配器是否连接到已启用巨帧的标准交换机或 Distributed Switch。
- 在客户机操作系统中，配置网络适配器以允许巨帧。请参见您的客户机操作系统文档。
- 将所有的物理交换机以及与该虚拟机相连的任何物理机或虚拟机配置为支持巨帧。



## TCP 分段清除

在 VMkernel 网络适配器和虚拟机中使用 TCP 分段清除 (TSO)，可提高具有严格延迟要求的工作负载中的网络性能。

物理网络适配器和 VMkernel 及虚拟机网络适配器传输路径的 TSO 可降低 TCP/IP 网络操作的 CPU 开销，从而提高 ESXi 主机的性能。如果启用 TSO，网络适配器会将较大的数据块（而非 CPU）分为多个 TCP 分段。VMkernel 和客户机操作系统可以使用更多的 CPU 周期运行应用程序。

要从 TSO 提供的性能改进中受益，请在 ESXi 主机上通过数据路径启用 TSO，包括物理网络适配器、VMkernel 和客户机操作系统。默认情况下，ESXi 主机的 VMkernel 及 VMXNET 2 和 VMXNET 3 虚拟机适配器中会启用 LRO。

有关数据路径中 TCP 数据包分段的位置的信息，请参见 VMware 知识库文章 [《了解 VMware 环境中的 TCP 分段清除 \(TSO\) 和大型接收卸载 \(LRO\)》](#)。

### 在 VMkernel 中启用或禁用软件 TSO

如果物理网络适配器运行 TSO 时遇到问题，则可以在 VMkernel 中临时启用 TSO 软件模拟，直到问题解决。

#### 步骤

- ◆ 运行这些 `esxcli network nic software set` 控制台命令以在 VMkernel 中启用或禁用 TSO 软件模拟。

- 在 VMkernel 中启用 TSO 软件模拟。

```
esxcli network nic software set --ipv4tso=0 -n vmnicX
esxcli network nic software set --ipv6tso=0 -n vmnicX
```

- 在 VMkernel 中禁用 TSO 软件模拟。

```
esxcli network nic software set --ipv4tso=1 -n vmnicX
esxcli network nic software set --ipv6tso=1 -n vmnicX
```

其中，vmnicX 中的 X 表示主机上的网卡端口号。

此配置更改在主机重新引导后仍然保留。

### 确定在 ESXi 主机的物理网络适配器上是否支持 TSO

在估算运行延迟敏感型工作负载的主机上的网络性能时，检查物理网络适配器是否卸载 TCP/IP 数据包分段。如果物理网络适配器支持 TSO，则 TSO 在默认情况下处于启用状态。

#### 步骤

- ◆ 运行此 `esxcli network nic software get` 控制台命令可确定 TSO 在主机的物理网络适配器上是否处于启用状态。

```
esxcli network nic tso get
```

### 在 ESXi 主机上启用或禁用 TSO

在传输路径上启用 TCP 分段清除 (TSO) 可让网卡将较大的数据块分为多个 TCP 分段。禁用 TSO 可让 CPU 执行 TCP 分段。

默认情况下，如果主机的物理适配器支持硬件 TSO，则主机可使用硬件 TSO。

#### 步骤

- 1 在 vSphere Web Client 中，导航到主机。

- 2 在**配置**选项卡上，展开**系统**。
- 3 单击**高级系统设置**。
- 4 编辑 **Net.UseHwTSO**（适用于 IPv4）和 **Net.UseHwTS06**（适用于 IPv6）参数的值。
  - 要启用 TSO，请将 **Net.UseHwTSO** 和 **Net.UseHwTS06** 设置为 **1**。
  - 要禁用 TSO，请将 **Net.UseHwTSO** 和 **Net.UseHwTS06** 设置为 **0**。
- 5 单击**确定**应用更改。
- 6 要重新加载物理适配器的驱动程序模块，请在主机的 ESXi Shell 中运行 `esxcli system module set` 控制台命令。
  - a 要禁用驱动程序，请将 `esxcli system module set` 命令与 `--enabled false` 选项一起运行。

```
esxcli system module set
                        --enabled false
                        --module
                        nic_driver_module
```

- b 要启用驱动程序，请将 `esxcli system module set` 命令与 `--enabled true` 选项一起运行。

```
esxcli system module set
                        --enabled true
                        --module
                        nic_driver_module
```

如果物理适配器不支持硬件 TSO，则 VMkernel 会将来自客户机操作系统的大型 TCP 数据包分段并其发送至适配器。

## 确定 TSO 在 ESXi 主机上是否处于启用状态

在估算运行延迟敏感型工作负载的主机上的网络性能时，检查硬件 TSO 在 VMkernel 中是否处于启用状态。默认情况下，硬件 TSO 在 ESXi 主机上处于启用状态。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在**配置**选项卡上，展开**系统**。
- 3 单击**高级系统设置**。
- 4 检查 **Net.UseHwTSO** 和 **Net.UseHwTS06** 参数的值。

**Net.UseHwTSO** 显示 IPv4 的 TSO 状态，而 **Net.UseHwTS06** 显示 IPv6 的 TSO 状态。如果属性设置为 1，则 TSO 处于启用状态。

## 在 Linux 虚拟机上启用或禁用 TSO

在 Linux 虚拟机的网络适配器上启用 TSO 支持，以便客户机操作系统将需要分段的 TCP 数据包重定向到 VMkernel。

### 前提条件

- 确保 ESXi 6.0 支持 Linux 客户机操作系统。  
请参见 *VMware 兼容性指南* 文档。
- 验证 Linux 虚拟机网络适配器是否为 VMXNET2 或 VMXNET3。

**步骤**

- ◆ 在 Linux 客户机操作系统的终端窗口中，要启用或禁用 TSO，将 `ethtool` 命令与 `-K` 和 `tso` 选项一起运行。

- 要启用 TSO，请运行以下命令：

```
ethtool ethY
        -K ethY
        tso
        on
```

- 要禁用 TSO，请运行以下命令：

```
ethtool ethY
        -K ethY
        tso
        off
```

其中，`ethY` 中的 `Y` 是虚拟机中网卡的序列号。

**在 Windows 虚拟机上启用或禁用 TSO**

默认情况下，TSO 在 Windows 虚拟机的 VMXNET2 和 VMXNET3 网络适配器上处于启用状态。出于性能考虑，您可能希望禁用 TSO。

**前提条件**

- 验证 ESXi 6.0 是否支持 Windows 客户机操作系统。请参见 *VMware 兼容性指南* 文档。
- 验证 Windows 虚拟机网络适配器是否为 VMXNET2 或 VMXNET3。

**步骤**

- 1 在 Windows 控制面板的“网络和共享中心”文件夹中，单击网络适配器的名称。
- 2 单击其名称。  
此时对话框将显示适配器的状态。
- 3 单击**属性**，然后在网络适配器类型下单击**配置**。
- 4 在**高级选项卡**上，将**大量发送卸载 V2 (IPv4)** 和**大量发送卸载 V2 (IPv6)** 属性设置为已启用或已禁用。
- 5 单击**确定**。
- 6 重新启动虚拟机。

**大型接收卸载**

使用大型接收卸载 (LRO) 可降低因高速处理从网络传入的数据包而产生的 CPU 开销。

LRO 将入站网络数据包重新集合到较大的缓冲区，然后将产生的较大但数量较少的数据包传输到主机或虚拟机的网络堆栈中。与禁用 LRO 时相比，CPU 需要处理的数据包减少，从而降低了网络利用率，对于具有高带宽的连接尤为如此。

要从 LRO 性能改进中受益，请在 ESXi 主机的数据路径所涉及的组件上启用 LRO，这些组件包括 VMkernel 和客户机操作系统。默认情况下，VMkernel 和 VMXNET3 虚拟机适配器中会启用 LRO。

有关数据路径中 TCP 数据包聚合的位置的信息，请参见 VMware 知识库文章 [《了解 VMware 环境中的 TCP 分段清除 \(TSO\) 和大型接收卸载 \(LRO\)》](#)。

## 为 ESXi 主机上的所有 VMXNET3 适配器启用硬件 LRO

启用主机物理适配器的硬件功能来为 VMXNET3 虚拟机适配器汇总入站 TCP 数据包，方法是在客户机操作系统中进行组合时使用 LRO 技术而不是消耗资源。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开系统。
- 3 单击高级系统设置。
- 4 编辑 Net.Vmxnet3HwLRO 参数的值。
  - 要启用硬件 LRO，请将 Net.Vmxnet3HwLRO 设置为 1。
  - 要禁用硬件 LRO，请将 Net.Vmxnet3HwLRO 设置为 0。
- 5 单击确定应用更改。

## 为 ESXi 主机上的所有 VMXNET3 适配器启用或禁用软件 LRO

如果主机物理适配器不支持硬件 TSO，则在 VMXNET3 适配器的 VMkernel 后端中可使用软件 LRO 来提高虚拟机的网络性能。

vSphere 5.5 及更高版本可为 IPv4 和 IPv6 数据包提供软件 LRO 支持。

### 前提条件

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开系统。
- 3 单击高级系统设置。
- 4 编辑 VMXNET3 适配器的 Net.Vmxnet3SwLRO 参数的值。
  - 要启用软件 LRO，请将 Net.Vmxnet3SwLRO 设置为 1。
  - 要禁用软件 LRO，请将 Net.Vmxnet3SwLRO 设置为 0。
- 5 单击确定应用更改。

## 确保是否为 ESXi 主机上的 VMXNET3 适配器启用了 LRO

在估算运行了延迟敏感型工作负载的主机上的网络性能时，请检查 ESXi 上的 LRO 状态。

### 前提条件

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开系统。
- 3 单击高级系统设置。
- 4 检查 VMXNET2 和 VMXNET3 的 LRO 参数的值。
  - 对于硬件 LRO，请检查 Net.Vmxnet3HwLRO 参数。如果该参数等于 1，则硬件 LRO 已启用。
  - 对于软件 LRO，请检查 Net.Vmxnet3SwLRO 参数。如果该参数等于 1，则软件 LRO 已启用。

## 更改 VMXNET 3 适配器的 LRO 缓冲区大小

您可以更改用于通过 VMXNET 3 网络适配器的虚拟机连接的数据包汇总的缓冲区大小。增加缓冲区大小可减少 TCP 确认的数量并提高工作负载的效率。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开系统。
- 3 单击高级系统设置。
- 4 为 Net.VmxnetLROMaxLength 参数输入介于 1 和 65535 之间的值以设置 LRO 缓冲区大小（字节）。  
默认情况下，LRO 缓冲区大小等于 32000 字节。

## 为 ESXi 主机上的所有 VMkernel 适配器启用或禁用 LRO

在 ESXi 主机的 VMkernel 网络适配器中使用 LRO 以提高入站基础架构流量的网络性能。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开系统。
- 3 单击高级系统设置。
- 4 编辑 Net.TcpipDefLROEnabled 参数的值。
  - 要为主机上的 VMkernel 网络适配器启用 LRO，请将 Net.TcpipDefLROEnabled 设置为 1。
  - 要为主机上的 VMkernel 网络适配器禁用软件 LRO，请将 Net.TcpipDefLROEnabled 设置为 0。
- 5 单击确定应用更改。

## 更改 VMkernel 适配器的 LRO 缓冲区大小

您可以更改用于 VMkernel 连接的数据包汇总的缓冲区大小。增加缓冲区大小可减少 TCP 确认的数量并提高 VMkernel 中的效率。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开系统。
- 3 单击高级系统设置。
- 4 为 Net.TcpipDefLROMaxLength 参数输入介于 1 和 65535 之间的值以设置 LRO 缓冲区大小（字节）。  
默认情况下，LRO 缓冲区大小等于 32768 字节。

## 在 Linux 虚拟机的 VMXNET3 适配器上启用或禁用 LRO

如果在主机上为 VMXNET3 适配器启用了 LRO，则可在 Linux 虚拟机上激活对网络适配器的 LRO 支持，以确保客户机操作系统不会使用资源将入站数据包汇总成较大的缓存。

### 前提条件

验证 Linux 内核版本是否为 2.6.24 和更高版本。

**步骤**

- ◆ 在 Linux 客户机操作系统的终端窗口中，将 `ethtool` 命令与 `-K` 和 `lro` 选项一起运行。

- 要启用 LRO，请运行以下命令：

```
ethtool
    -K ethY
    lro
    on
```

其中，`ethY` 中的 `Y` 是虚拟机中网卡的序列号。

- 要禁用 LRO，请运行以下命令：

```
ethtool
    -K ethY
    lro
    off
```

其中，`ethY` 中的 `Y` 是虚拟机中网卡的序列号。

**在 Windows 虚拟机的 VMXNET3 适配器上启用或禁用 LRO**

如果在主机上为 VMXNET3 适配器启用了 LRO，则可在 Windows 虚拟机上激活对网络适配器的 LRO 支持，以确保客户机操作系统不会使用资源将入站数据包汇总成较大的缓存。

在 Windows 上，LRO 技术也称为接收方合并 (RSC)。

**前提条件**

- 验证虚拟机是否在 Windows Server 2012 及更高版本或 Windows 8 及更高版本上运行。
- 确认虚拟机兼容性为 ESXi 6.0 和更高版本。
- 验证客户机操作系统上安装的 VMXNET3 驱动程序版本是否为 1.6.6.0 及更高版本。
- 验证在 Windows Server 2012 及更高版本或 Windows 8 及更高版本上运行的虚拟机上是否已全局启用 LRO。请参见第 143 页，“在 Windows 虚拟机上全局启用 LRO”。

**步骤**

- 1 在客户机操作系统控制面板的**网络和共享中心**中，单击网络适配器的名称。  
此时对话框将显示适配器的状态。
- 2 单击**属性**，然后在 VMXNET3 网络适配器类型下单击**配置**。
- 3 在**高级选项卡**上，将**接收段合并 (IPv4)** 和**接收段合并 (IPv6)** 设置为已启用或已禁用。
- 4 单击**确定**。

## 在 Windows 虚拟机上全局启用 LRO

要在运行 Windows 8 及更高版本或 Windows Server 2012 及更高版本的 VMXNET3 适配器上使用 LRO，必须在客户机操作系统上全局启用 LRO。在 Windows 上，LRO 技术也称为接收方合并 (RSC)。

### 步骤

- 1 要验证在 Windows 8 及更高版本或 Windows Server 2012 客户机操作系统上是否已全局禁用 LRO，请在命令提示符下运行 `netsh int tcp show global` 命令。

```
netsh int tcp show global
```

该命令将显示在 Windows 8.x 操作系统上设置的 TCP 全局参数的状态。

TCP 全局参数

```
-----
接收方缩放状态: 已启用
烟囱卸载状态: 已禁用
NetDMA 状况: 已禁用
直接缓存访问 (DCA): 已禁用
接收窗口自动调谐级别: 正常
附加拥塞控制提供程序: 无
ECN 能力: 已禁用
RFC 1323 时间戳: 已禁用
初始 RTO: 3000
接收段合并状态: 已禁用
```

如果在 Windows 8 及更高版本或 Windows Server 2012 计算机上全局禁用 LRO，则“接收段合并状态”属性将显示为“已禁用”。

- 2 要在 Windows 操作系统上全局启用 LRO，请在命令提示符下运行 `netsh int tcp set global` 命令：

```
netsh int tcp set global rsc=enabled
```

### 下一步

为 Windows 8 及更高版本或 Windows Server 2012 虚拟机上的 VMXNET3 适配器启用 LRO。请参见[第 142 页](#)，“在 Windows 虚拟机的 VMXNET3 适配器上启用或禁用 LRO”。

## NetQueue 和网络性能

NetQueue 会利用一些网络适配器的功能，以多个可分别处理的接收队列的形式将网络流量传输到系统，这样可以使处理扩展到多个 CPU，从而提高接收端的网络性能。

### 在主机上启用 NetQueue

NetQueue 在默认情况下处于启用状态。要在禁用 NetQueue 之后使用 NetQueue，必须重新启用它。

#### 前提条件

#### 步骤

- 1 在主机 ESXi Shell 中，键入以下命令：

```
esxcli system settings kernel set --setting="netNetqueueEnabled" --value="TRUE"
```

- 2 使用 `esxcli module parameters set` 命令将网卡驱动程序配置为使用 NetQueue。  
例如，在双端口 Emulex 网卡上，运行此 ESXCLI 命令可用 8 个接收队列配置驱动程序。  

```
esxcli system module parameters set -m tg3 -p force_netq=8,8
```
- 3 重新引导主机。

## 在主机上禁用 NetQueue

NetQueue 在默认情况下处于启用状态。

### 前提条件

熟悉《vSphere 命令行界面入门》中有关配置网卡驱动程序的信息。

### 步骤

- 1 在 VMware vSphere CLI 中，请根据主机版本使用以下命令：  

```
esxcli system settings kernel set --setting="netNetqueueEnabled" --value="FALSE"
```
- 2 要在网卡驱动程序上禁用 NetQueue，请使用 `esxcli module parameters set` 命令。  
例如，在双端口 Emulex 网卡上，运行此 ESXCLI 命令可用 1 个接收队列配置驱动程序。  

```
esxcli system module parameters set -m tg3 -p force_netq=1,1
```
- 3 重新引导主机。



## vSphere Network I/O Control

---

使用 vSphere Network I/O Control 可向关键业务应用程序分配网络带宽以及解决多种流量争用通用资源的情况。

- [关于 vSphere Network I/O Control 版本 3](#) 第 145 页，  
vSphere Network I/O Control 版本 3 引入了一种基于主机上物理适配器的容量为系统流量预留带宽的机制。这种机制可以在虚拟机网络适配器级别实现精细的资源控制，类似于分配 CPU 和内存资源使用的模型。
- [将 vSphere Distributed Switch 上的 Network I/O Control 升级到版本 3](#) 第 146 页，  
如果已将 vSphere Distributed Switch 升级到版本 6.0.0，而未将 Network I/O Control 转换为版本 3，您可以升级 Network I/O Control，以使用系统流量和单个虚拟机的带宽分配的增强模型。
- [在 vSphere Distributed Switch 上启用 Network I/O Control](#) 第 148 页，  
在 vSphere Distributed Switch 上启用网络资源管理以保证用于系统流量针对 vSphere 功能和用于虚拟机流量的带宽最小值。
- [系统流量的带宽分配](#) 第 148 页，  
您可以基于份额、预留和限制配置 Network I/O Control，以便为 vSphere Fault Tolerance、iSCSI 存储器、vSphere vMotion 等服务生成的流量分配一定量的带宽。
- [虚拟机流量的带宽分配](#) 第 151 页，  
Network I/O Control 版本 3 允许为单个虚拟机配置带宽要求。还可以使用可在其中为虚拟机流量分配聚合预留的带宽配额的网络资源池，然后将池的带宽分配给单个虚拟机。
- [将物理适配器移到 Network I/O Control 的范围之外](#) 第 158 页，  
在某些情况下，您可能需要从 Network I/O Control 版本 3 的带宽分配模型中排除容量小的物理适配器。
- [使用 Network I/O Control 版本 2](#) 第 158 页，  
在 vSphere Distributed Switch 5.x 上，以及在已升级到 6.0、但未将 Network I/O Control 增强到版本 3 的 vSphere Distributed Switch 上，您可确保系统流量和虚拟机可以使用 Network I/O Control 版本 2 的资源池模型收到所需的操作带宽。

### 关于 vSphere Network I/O Control 版本 3

vSphere Network I/O Control 版本 3 引入了一种基于主机上物理适配器的容量为系统流量预留带宽的机制。这种机制可以在虚拟机网络适配器级别实现精细的资源控制，类似于分配 CPU 和内存资源使用的模型。

Network I/O Control 版本 3 的功能改进了整个交换机上的网络资源预留和分配。

## 带宽资源预留的模型

Network I/O Control 版本 3 支持与基础架构服务（如 vSphere Fault Tolerance）相关的系统流量的资源管理和虚拟机的资源管理的单独模型。

这两种流量类别性质不同。系统流量与 ESXi 主机紧密相关。当在环境中迁移虚拟机时，网络流量路由会更改。要在忽略主机的情况下为虚拟机提供网络资源，您可在 Network I/O Control 中为在整个 Distributed Switch 的范围内有效的虚拟机配置资源分配。

## 为虚拟机保证带宽

Network I/O Control 版本 3 使用份额构成、预留和限制为虚拟机的网络适配器置备带宽。若要基于这些构成收到充足的带宽，虚拟化的工作负载可依赖 vSphere Distributed Switch、vSphere DRS 和 vSphere HA 中的接入控制。请参见第 153 页，“虚拟机带宽的接入控制”。

## vSphere 6.0 中的 Network I/O Control 版本 2 和版本 3

在 vSphere 6.0 中，Network I/O Control 版本 2 和版本 3 是同时存在的。这两个版本为虚拟机和系统流量分配带宽所实施的模型不同。在 Network I/O Control 版本 2 中，可以在物理适配器级别配置虚拟机的带宽分配。而在版本 3 中，则是在整个 Distributed Switch 级别设置虚拟机的带宽分配。

升级 Distributed Switch 时，Network I/O Control 也会升级到版本 3，除非您正在使用的某些功能在 Network I/O Control 版本 3 中不可用，如 CoS 标记和用户定义的网络资源池。在这种情况下，版本 2 和版本 3 资源分配模型的差别不允许进行非破坏性升级。您可以继续使用版本 2 保留虚拟机的带宽分配设置，也可以切换到版本 3 并在所有交换机主机间量身定制带宽策略。

**表 11-1** 根据 vSphere Distributed Switch 和 ESXi 的版本确定的 Network I/O Control 版本

vSphere Network I/O Control	vSphere Distributed Switch 版本	ESXi 版本
2.0	5.1.0	■ 5.1
		■ 5.5
		■ 6.0
	5.5.0	■ 5.5 ■ 6.0
3.0	6.0.0	6.0

## 功能可用性

SR-IOV 不适用于配置为使用 Network I/O Control 版本 3 的虚拟机。

## 将 vSphere Distributed Switch 上的 Network I/O Control 升级到版本 3

如果已将 vSphere Distributed Switch 升级到版本 6.0.0，而未将 Network I/O Control 转换为版本 3，您可以升级 Network I/O Control，以使用系统流量和单个虚拟机的带宽分配的增强模型。

将 Network I/O Control 版本 2 升级到版本 3 时，在版本 2 中定义的所有现有系统网络资源池的设置均转换为系统流量的份额构成、预留和限制。默认情况下，不为所有已转换的系统流量类型设置预留。

将 Distributed Switch 升级到版本 3 是一个破坏性事件。某些功能仅可在 Network I/O Control 版本 2 中使用，并在升级到版本 3 的过程中被删除。

表 11-2 升级到 Network I/O Control 版本 3 的过程中被删除的功能

升级过程中被删除的功能	描述
用户定义的资源池，其中包括这些池与现有分布式端口组之间的所有关联	通过将用户定义的网络资源池的份额传输至单个网络适配器份额，您可以保留部分资源分配设置。因此，在升级到 Network I/O Control 版本 3 之前，请确保升级未显著影响在 Network I/O Control 版本 2 中为虚拟机配置的带宽分配。
端口与用户定义的网络资源池之间的现有关联	在 Network I/O Control 版本 3 中，无法将单个分布式端口与分配给父级端口组的池之外的网络资源池相关联。相较于版本 2，Network I/O Control 版本 3 不支持替代端口级别的资源分配策略。
与网络资源池关联的流量的 CoS 标记功能	Network I/O Control 版本 3 不支持用 CoS 标记标记 QoS 需求更高的流量。升级后，若要还原与用户定义的网络资源池关联的流量的 CoS 标记功能，请使用流量筛选和标记网络策略。请参见第 96 页，“标记分布式端口组或上行链路端口组的流量”和第 102 页，“标记分布式端口或上行链路端口的流量”。

### 前提条件

- 验证 vSphere Distributed Switch 的版本是否为 6.0.0。
- 验证 Distributed Switch 的 Network I/O Control 功能是否为版本 2。
- 验证对交换机上的分布式端口组是否具有 **dvPort 组修改** 特权。
- 验证交换机上的所有主机是否都连接到 vCenter Server。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 从**操作**菜单中，选择**升级 > 升级 Network I/O Control**。  
此时将显示升级 Network I/O Control 向导。
- 3 （可选）在“概览”页面上，创建一份交换机配置的备份。  
如果升级失败，可以使用该备份来还原交换机配置。
- 4 查看升级引起的更改，然后单击**下一步**。
- 5 验证 Distributed Switch 满足升级的验证必备条件，然后单击**下一步**。

必备条件	描述
端口组的可访问性	您有访问和修改交换机上的上行链路和分布式端口组所需的特权。
主机状态	交换机上的所有主机是否都连接到 vCenter Server。
系统流量的 CoS 优先级标记	Distributed Switch 没有已分配 CoS 标记的网络资源池。
用户定义的网络资源池	Distributed Switch 不包含用于虚拟机带宽控制的用户定义的资源池。
资源分配策略替代	交换机上的分布式端口组不允许在单个端口上替代 Network I/O Control 策略。

- 6 如果 Distributed Switch 包含用户定义的资源池，请将版本 2 中用户定义的资源池的份额传输至版本 3 中单个虚拟机网络适配器的份额，然后单击**下一步**。  
传输份额使您能够保留虚拟机的部分带宽分配设置。

**注意** 在转换期间，用户定义的资源池的限制不会保留。

- 7 查看升级设置，然后单击**完成**。

**下一步**

- 创建网络资源池并将它们与虚拟机连接到的分布式端口组相关联，以向连接到交换机的一组虚拟机分配预留带宽配额。请参见第 154 页，“创建网络资源池”和第 154 页，“向网络资源池中添加分布式端口组”。

如果已传输版本 2 的原始份额，则在关联网络资源池与虚拟机的端口组时强制执行。

- 使用份额、预留和限制向单个虚拟机分配带宽配额。请参见第 155 页，“为虚拟机配置带宽分配”。

**在 vSphere Distributed Switch 上启用 Network I/O Control**

在 vSphere Distributed Switch 上启用网络资源管理以保证用于系统流量针对 vSphere 功能和用于虚拟机流量的带宽最小值。

**前提条件**

验证 vSphere Distributed Switch 的版本是否为 5.1.0 或更高版本。

**步骤**

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 从操作菜单中，选择编辑设置。
- 3 从 Network I/O Control 下拉菜单中，选择启用。
- 4 单击确定。

启用后，Network I/O Control 用来处理系统流量和虚拟机流量带宽分配的模型基于 Distributed Switch 上活动的 Network I/O Control 版本。请参见第 145 页，“关于 vSphere Network I/O Control 版本 3”。

**系统流量的带宽分配**

您可以基于份额、预留和限制配置 Network I/O Control，以便为 vSphere Fault Tolerance、iSCSI 存储器、vSphere vMotion 等服务生成的流量分配一定量的带宽。

可以使用 Distributed Switch 上的 Network I/O Control 为与 vSphere 中主要系统功能相关的流量配置带宽分配：

- 管理
- Fault Tolerance
- iSCSI
- NFS
- Virtual SAN
- vMotion
- vSphere Replication
- vSphere Data Protection 备份
- 虚拟机

vCenter Server 将 Distributed Switch 的分配传播到连接到该交换机的主机上的每个物理适配器。

- [系统流量的带宽分配参数](#)第 149 页，  
通过使用多个配置参数，Network I/O Control 可以将带宽分配给基本 vSphere 系统功能的流量。
- [系统流量的带宽预留示例](#)第 149 页，  
物理适配器的容量决定要保证的带宽。根据此容量，可保证用于某个系统功能进行其最佳操作的带宽最小值。

- [配置系统流量的带宽分配](#)第 150 页，  
为连接到 vSphere Distributed Switch 的物理适配器上的主机管理、iSCSI 存储器、NFS 存储器、vSphere vMotion、vSphere Fault Tolerance、Virtual SAN 和 vSphere Replication 分配带宽。

系统流量的带宽分配参数

通过使用多个配置参数，Network I/O Control 可以将带宽分配给基本 vSphere 系统功能的流量。

表 11-3 系统流量的分配参数

带宽分配参数	描述
份额	份额从 1 到 100，反映某个系统流量类型对于同一物理适配器上活动的其他系统流量类型的相对优先级。 某个系统流量类型可用的带宽量由其相对份额和其他系统功能正在传输的数据量决定。 例如，您向 vSphere FT 流量和 iSCSI 流量分配 100 个份额，而每个其他网络资源池有 50 个份额。配置了一个物理适配器用于发送 vSphere Fault Tolerance、iSCSI 和管理流量。在某一时刻，vSphere Fault Tolerance 和 iSCSI 是该物理适配器上的活动流量类型，并且用光了其容量。每个流量会收到 50% 的可用带宽。在另一时刻，所有三个流量类型使该适配器呈饱和状态。在这种情况下，vSphere FT 流量和 iSCSI 流量可分别获得 40% 的适配器容量，vMotion 则可获得 20%。
预留	单个物理适配器上必须保证的带宽最小值 (Mbps)。为所有系统流量类型预留的总带宽不得超过容量最低的物理网络适配器所能提供的带宽的 75%。 未使用的预留带宽可用于其他类型的系统流量。但是，Network I/O Control 不会重新分配系统流量未用于虚拟机放置的容量。例如，您为 iSCSI 配置了 2 Gbps 的预留。 Distributed Switch 可能从不在物理适配器上强制实施此预留，因为 iSCSI 使用单一路径。未使用的带宽不会分配给虚拟机系统流量，从而使 Network I/O Control 能够安全地满足系统流量对带宽的潜在需求，例如，如果使用新的 iSCSI 路径，您必须为新的 VMkernel 适配器提供带宽。
限制	系统流量类型在单个物理适配器上可消耗的带宽最大值 (Mbps 或 Gbps)。

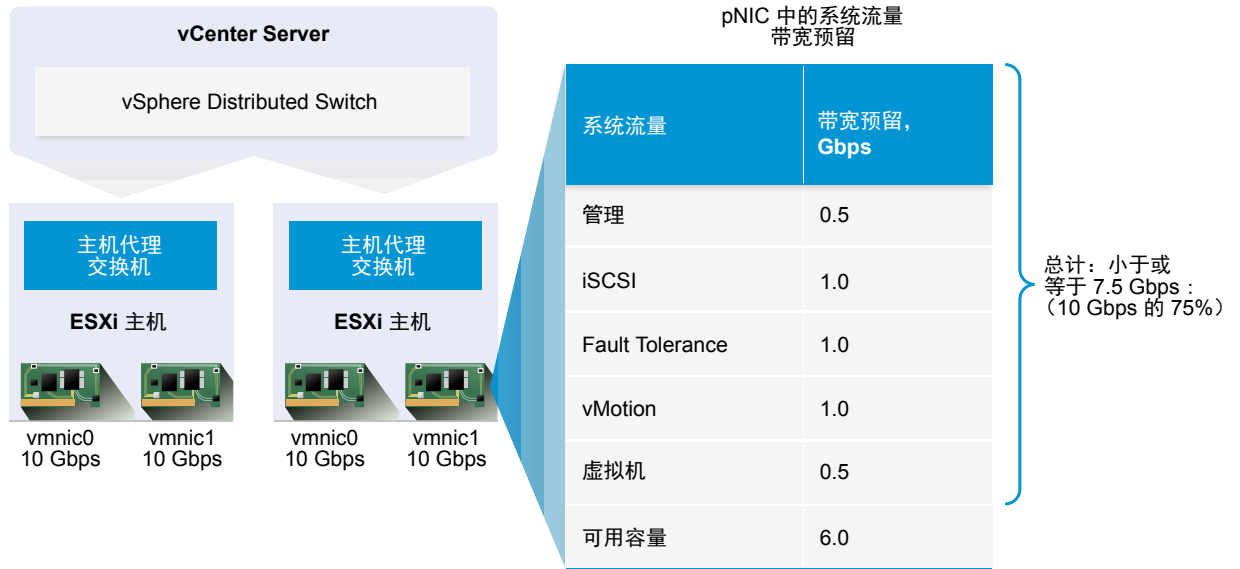
系统流量的带宽预留示例

物理适配器的容量决定要保证的带宽。根据此容量，可保证用于某个系统功能进行其最佳操作的带宽最小值。

例如，在已连接到具有 10 GbE 网络适配器的 ESXi 主机的 Distributed Switch 上，可以配置预留以保证 1 Gbps 用于通过 vCenter Server 进行管理，1 Gbps 用于 iSCSI 存储器，1 Gbps 用于 vSphere Fault Tolerance，1 Gbps 用于 vSphere vMotion 流量，以及 0.5 Gbps 用于虚拟机流量。Network I/O Control 在每个物理网络适配器上分配请求的带宽。可以预留不超过物理网络适配器带宽的 75%，即不超过 7.5 Gbps。

可以将更多容量保留为未预留，以使主机可根据份额、限制和使用来动态分配带宽，并且仅预留足够系统功能运行的带宽。

图 11-1 10 GbE 物理网络适配器上系统流量的带宽预留示例



## 配置系统流量的带宽分配

为连接到 vSphere Distributed Switch 的物理适配器上的主机管理、iSCSI 存储器、NFS 存储器、vSphere vMotion、vSphere Fault Tolerance、Virtual SAN 和 vSphere Replication 分配带宽。

要使用 Network I/O Control 启用虚拟机的带宽分配，可配置虚拟机系统流量。虚拟机流量的带宽预留也用在接入控制中。打开虚拟机电源时，接入控制会验证是否有充足带宽可用。

### 前提条件

- 确认 vSphere Distributed Switch 为 6.0.0 及更高版本。
- 确认交换机上的 Network I/O Control 为版本 3。
- 确认已启用 Network I/O Control。请参见第 148 页，“在 vSphere Distributed Switch 上启用 Network I/O Control”。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在配置选项卡上，展开资源分配。
- 3 单击系统流量。  
查看系统流量类型的带宽分配。
- 4 选择要置备的根据 vSphere 功能确定的流量类型，然后单击编辑。  
此时将显示该流量类型的网络资源设置。
- 5 从份额下拉菜单中，编辑流经物理适配器的总流量份额。  
Network I/O Control 在物理适配器达到饱和时会应用已配置的份额。  
可以选择一个选项设置预定义的值，也可以选择自定义，然后键入从 1 到 100 的数值设置其他份额。
- 6 在预留对话框中，输入必须为该流量类型提供的带宽最小值。  
系统流量的总预留不得超过连接到 Distributed Switch 的所有适配器中容量最小的适配器所支持带宽的 75%。
- 7 在限制文本框中，设置所选类型的系统流量可使用的带宽最小值。

8 单击**确定**应用分配设置。

vCenter Server 将 Distributed Switch 的分配传播到连接到该交换机的主机物理适配器。

## 虚拟机流量的带宽分配

Network I/O Control 版本 3 允许为单个虚拟机配置带宽要求。还可以使用可在其中为虚拟机流量分配聚合预留的带宽配额的网络资源池，然后将池的带宽分配给单个虚拟机。

### 关于为虚拟机分配带宽

Network I/O Control 使用两种模型为虚拟机分配带宽：基于承载虚拟机流量的物理适配器上的网络资源池和分配在整个 vSphere Distributed Switch 上分配。

#### 网络资源池

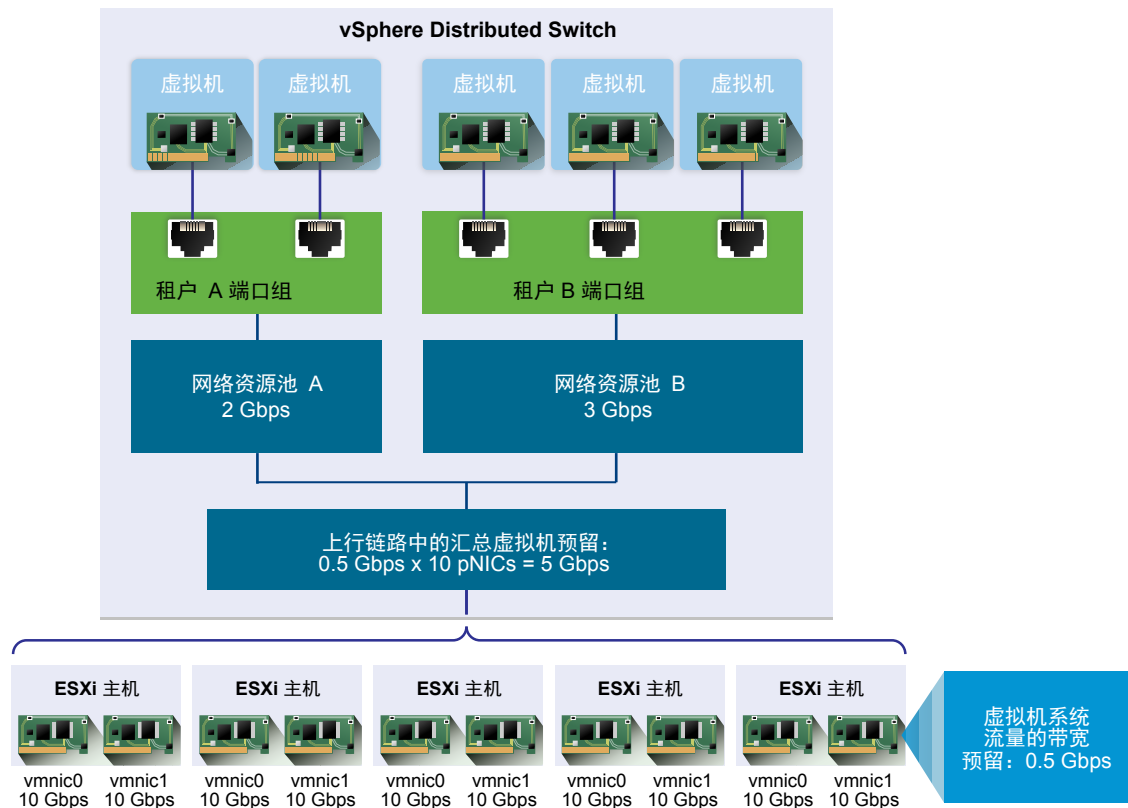
网络资源池代表为所有连接到 Distributed Switch 的物理适配器上的虚拟机系统流量预留的聚合带宽的一部分。

例如，如果虚拟机系统流量在具有 10 个上行链路的 Distributed Switch 上为每个 10 GbE 上行链路预留了 0.5 Gbps，那么此交换机上虚拟机预留可用的总聚合带宽为 5 Gbps。每个网络资源池可预留此 5 Gbps 容量的配额。

带宽配额专用于网络资源池，由与该池关联的分布式端口组共享。虚拟机通过该虚拟机连接到的分布式端口组从池接收带宽。

默认情况下，交换机上的分布式端口组分配至叫做“默认”的网络资源池，其配额未配置。

图 11-2 vSphere Distributed Switch 的上行链路间的网络资源池带宽聚合





## 定义虚拟机的带宽要求

为单个虚拟机分配带宽类似于分配 CPU 和内存资源。Network I/O Control 版本 3 根据在虚拟机硬件设置中为网络适配器定义的份额、预留和限制为虚拟机置备带宽。预留代表一种保证，保证虚拟机的流量可以消耗最低指定带宽。如果物理适配器有更大容量，则虚拟机可根据指定的份额和限制使用额外带宽。

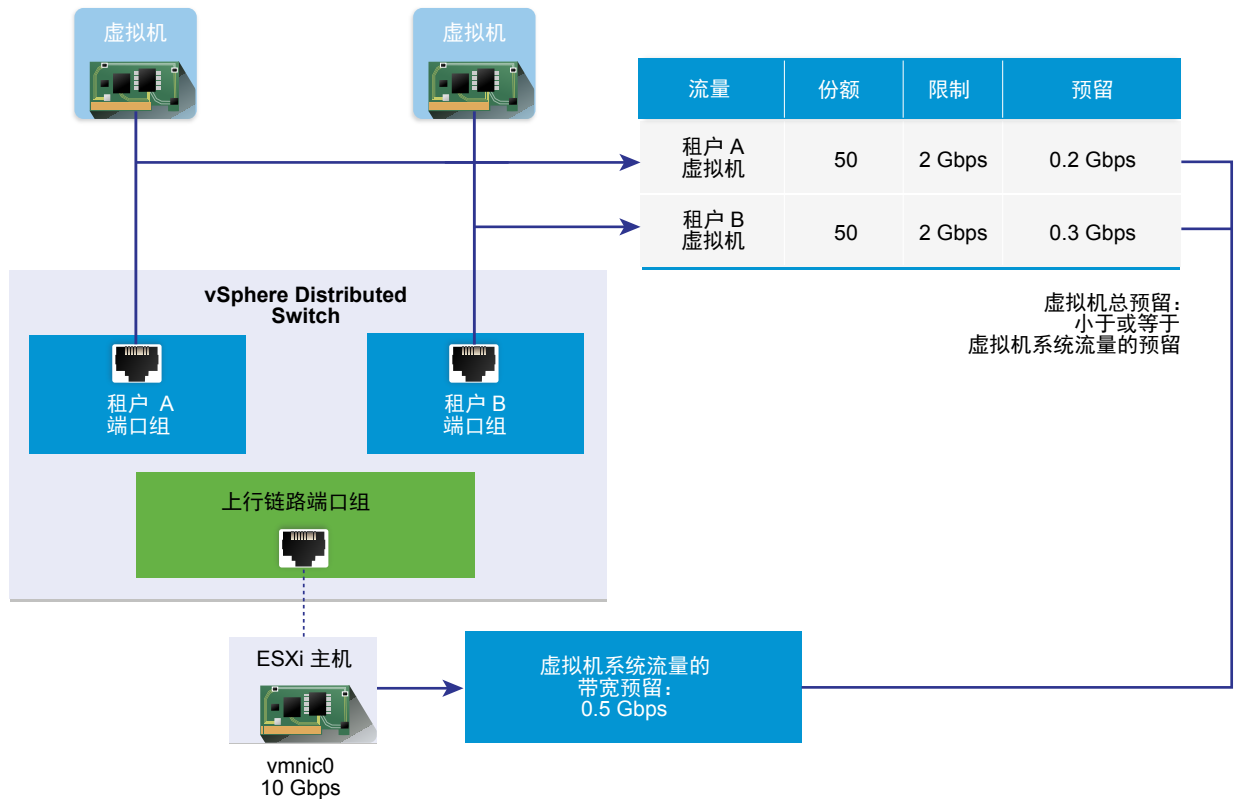
## 置备给主机上虚拟机的带宽

在虚拟机已配置带宽预留的情况下，为保证带宽，Network I/O Control 会实施变为活跃流量引擎。**Distributed Switch** 尝试将虚拟机网络适配器的流量放置于可提供所需带宽且在活动成组策略范围之内的物理适配器。

主机上虚拟机的总带宽预留不能超过为虚拟机系统流量配置的预留带宽。

实际限制和预留还取决于适配器连接到的分布式端口组的流量调整策略。例如，如果一个虚拟机网络适配器要求的带宽限制为 200 Mbps 且在流量调整策略中配置的平均带宽为 100 Mbps，则有效限制将变为 100 Mbps。

图 11-3 单个虚拟机的带宽分配配置





## 虚拟机流量的带宽分配参数

Network I/O Control 版本 3 基于在虚拟机硬件设置中为网络适配器配置的份额、预留和限制向单个虚拟机分配带宽。

**表 11-4 虚拟机网络适配器的带宽分配参数**

带宽分配参数	描述
份额	流量通过虚拟机网络适配器的相对优先级（从 1 到 100），依据承载此虚拟机与网络之间流量的物理适配器的容量确定。
预留	虚拟机网络适配器在物理适配器上必须收到的最低带宽 (Mbps)。
限制	在虚拟机网络适配器上流量传输至同一主机或其他主机上的其他虚拟机所需的最大带宽。

## 虚拟机带宽的接入控制

为保证虚拟机有足够的带宽可用，vSphere 会依据带宽预留和成组策略在主机级别和群集级别实施接入控制。

### vSphere Distributed Switch 中的带宽接入控制

打开虚拟机电源时，Distributed Switch 上的 Network I/O Control 功能会验证主机是否满足以下条件。

- 主机上有一个物理适配器可以依据成组策略和预留为虚拟机网络适配器提供最低带宽。
- 虚拟机网络适配器的预留少于网络资源池中的可用配额。

如果更改正在运行的虚拟机的网络适配器预留，Network I/O Control 会重新验证关联的网络资源池是否能够容纳新预留。如果该池的空闲配额不足，则不会应用更改。

要在 vSphere Distributed Switch 中使用接入控制，请执行以下任务：

- 为 Distributed Switch 上的虚拟机系统流量配置带宽分配。
- 使用为虚拟机系统流量配置的带宽预留配额配置网络资源池。
- 将该网络资源池和连接虚拟机与交换机的分布式端口组进行关联。
- 为连接到该端口组的虚拟机配置带宽要求。

### vSphere DRS 中的带宽接入控制

如果您打开一台位于群集中的虚拟机的电源，vSphere DRS 会将该虚拟机放置在其容量依据活动成组策略足以保证为虚拟机提供预留带宽的主机上。

在以下情况下，vSphere DRS 会将虚拟机迁移到其他主机，以满足该虚拟机的带宽预留要求：

- 预留更改为初始主机无法再满足的值。
- 承载虚拟机流量的物理适配器处于脱机状态。

要在 vSphere DRS 中使用接入控制，请执行以下任务：

- 为 Distributed Switch 上的虚拟机系统流量配置带宽分配。
- 为连接到 Distributed Switch 的虚拟机配置带宽要求。

有关根据虚拟机带宽要求管理资源的详细信息，请参见 *vSphere 资源管理* 文档。

### vSphere HA 中的带宽接入控制

当主机发生故障或被隔离时，vSphere HA 会依据带宽预留和成组策略在群集中的其他主机上打开虚拟机电源。

要在 vSphere HA 中使用接入控制，请执行以下任务：

- 为虚拟机系统流量分配带宽。
- 为连接到 Distributed Switch 的虚拟机配置带宽要求。

有关 vSphere HA 根据虚拟机带宽要求提供故障切换的详细信息，请参见 *vSphere 可用性* 文档。

## 创建网络资源池

在 vSphere Distributed Switch 上创建网络资源池以为一组虚拟机预留带宽。

网络资源池为虚拟机提供预留配额。配额表示为已连接到 Distributed Switch 的物理适配器上的虚拟机系统流量预留的一部分带宽。可以从与该池关联的虚拟机配额中留出部分带宽。已打开电源、与该池关联的虚拟机的网络适配器中的预留不得超过该池的配额。请参见第 151 页，“关于为虚拟机分配带宽”。

### 前提条件

- 确认 vSphere Distributed Switch 为 6.0.0 及更高版本。
- 确认交换机上的 Network I/O Control 为版本 3。
- 确认已启用 Network I/O Control。请参见第 148 页，“在 vSphere Distributed Switch 上启用 Network I/O Control”。
- 确认虚拟机系统流量包括已配置的带宽预留。请参见第 150 页，“配置系统流量的带宽分配”。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在配置选项卡上，展开资源分配。
- 3 单击网络资源池。
- 4 单击添加图标。
- 5 （可选）键入网络资源池的名称和描述。
- 6 根据为虚拟机系统流量预留的可用带宽，为预留配额输入一个值，以 Mbps 为单位。

可分配给该池的最大配额根据以下公式来确定：

$$\text{max reservation quota} = \text{aggregated reservation for vm system traffic} - \text{quotas of the other resource pools}$$

而且

- 虚拟机系统流量的汇总预留 = 每个 pNIC 上虚拟机系统流量已配置的带宽预留 \* 已连接到 Distributed Switch 的 pNIC 数量
- 其他池的配额 = 其他网络资源池预留配额的总和

- 7 单击确定。

### 下一步

将一个或多个分布式端口组添加到网络资源池，以便可以从该池的配额中为单个虚拟机分配带宽。请参见第 154 页，“向网络资源池中添加分布式端口组”。

## 向网络资源池中添加分布式端口组

向网络资源池添加分布式端口组，从而可向连接到该端口组的虚拟机分配带宽。

要立即向多个分布式端口组分配网络资源池，可以使用管理分布式端口组向导中的资源分配策略。请参见第 109 页，“管理 vSphere Distributed Switch 上的多个端口组的策略”。

Network I/O Control 根据在 Distributed Switch 上活动的 Network I/O Control 版本中实施的模型，向与分布式端口组关联的虚拟机分配带宽。请参见第 145 页，“关于 vSphere Network I/O Control 版本 3”。

#### 前提条件

- 确认 vSphere Distributed Switch 为 5.1 及更高版本。
- 确认已启用 Network I/O Control。请参见第 148 页，“在 vSphere Distributed Switch 上启用 Network I/O Control”。

#### 步骤

- 1 在 vSphere Web Client 中找到分布式端口组。
    - a 选择 Distributed Switch，然后单击**网络**选项卡。
    - b 单击**分布式端口组**。
  - 2 选择分布式端口组，然后单击**编辑分布式端口组设置**。
  - 3 在“编辑设置”对话框中，单击**常规**。
  - 4 从**网络资源池**下拉菜单中，选择该网络资源池，然后单击**确定**。
- 如果 Distributed Switch 不包含网络资源池，则下拉菜单中仅会显示**(默认)**选项。

## 为虚拟机配置带宽分配

可以为已连接到分布式端口组的单个虚拟机配置带宽分配。可以使用带宽的份额、预留和限制设置。

#### 前提条件

- 确认 vSphere Distributed Switch 为 6.0.0 及更高版本。
- 确认交换机上的 Network I/O Control 为版本 3。
- 确认已启用 Network I/O Control。请参见第 148 页，“在 vSphere Distributed Switch 上启用 Network I/O Control”。
- 确认虚拟机系统流量包括已配置的带宽预留。请参见第 150 页，“配置系统流量的带宽分配”。

#### 步骤

- 1 在 vSphere Web Client 中找到虚拟机。
    - a 选择数据中心、文件夹、群集、资源池或主机，然后单击**虚拟机**选项卡。
    - b 单击**虚拟机**，然后从列表中双击虚拟机。
  - 2 在虚拟机的**配置**选项卡上，展开**设置**，然后选择**虚拟机硬件**。
  - 3 单击**编辑**。
  - 4 展开虚拟机网络适配器的网络适配器 X 部分。
  - 5 如果要为新虚拟机网络适配器配置带宽分配，请从**新设备**下拉菜单中选择**网络**，然后单击**添加**。  
“新网络”部分会显示带宽分配及其他网络适配器设置的选项。
  - 6 如果虚拟机网络适配器未连接到分布式端口组，请从网络适配器 X 或“新网络”标签旁边的下拉菜单中选择端口组。
- 此时即显示虚拟机网络适配器的**份额、预留和限制**设置。

- 7 从**份额**下拉菜单中，将此虚拟机中流量的相对优先级设置为连接的物理适配器容量中的份额。  
Network I/O Control 在物理适配器达到饱和时会应用已配置的份额。  
可以选择一个选项设置预定义的值，也可以选择**自定义**，然后键入从 1 到 100 的数值设置其他份额。
- 8 在**预留**文本框中，预留虚拟机打开电源后必须可供虚拟机网络适配器使用的最小带宽。  
如果使用网络资源池置备带宽，与该池相关联的已打开电源虚拟机的网络适配器中的预留值不得超过该池的配额。  
如果已启用 vSphere DRS，要打开虚拟机的电源，请确保主机上所有虚拟机网络适配器中的预留不超过为主机物理适配器上的虚拟机系统流量预留的带宽。
- 9 在**限制**文本框中，对虚拟机网络适配器可以占用的带宽设置限制。
- 10 单击**确定**。

网络

I/O Control 会分配从网络资源池的预留配额中为虚拟机网络适配器预留的带宽。

## 在多个虚拟机上配置带宽分配

只需一次操作，即可在连接到特定网络资源池的多个虚拟机上配置带宽分配，例如，将 Network I/O Control 升级到版本 3 后。

### 前提条件

- 确认 vSphere Distributed Switch 为 6.0.0 及更高版本。
- 确认交换机上的 Network I/O Control 为版本 3。
- 确认已启用 Network I/O Control。请参见第 148 页，“在 vSphere Distributed Switch 上启用 Network I/O Control”。
- 确认虚拟机系统流量包括已配置的带宽预留。请参见第 150 页，“配置系统流量的带宽分配”。
- 验证虚拟机是否通过连接的分布式端口组与特定网络资源池关联。请参见第 154 页，“向网络资源池中添加分布式端口组”。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在**配置**选项卡上，展开**资源分配**。
- 3 单击**网络资源池**。
- 4 选择一个网络资源池。
- 5 单击**虚拟机**。  
此时将显示连接到所选网络资源池的虚拟机网络适配器的列表。
- 6 选择要配置其设置的虚拟机网络适配器，然后单击**编辑**。
- 7 从**份额**下拉菜单中，设置处于物理适配器的范围之内且承载流量的那些虚拟机的流量的相对优先级。  
Network I/O Control 在物理适配器达到饱和时会应用已配置的份额。
- 8 在**预留**文本框中，预留打开虚拟机电源时必须提供给每个虚拟机网络适配器的最低带宽。  
如果使用网络资源池置备带宽，与该池相关联的已打开电源虚拟机的网络适配器中的预留值不得超过该池的配额。
- 9 在**限制**文本框中，设置每个虚拟机网络适配器可占用的带宽的限制。

- 10 单击**确定**。

## 更改网络资源池的配额

更改可为连接到一组分布式端口组的虚拟机预留的带宽配额。

### 前提条件

- 确认 vSphere Distributed Switch 为 6.0.0 及更高版本。
- 确认交换机上的 Network I/O Control 为版本 3。
- 确认已启用 Network I/O Control。请参见第 148 页，“在 vSphere Distributed Switch 上启用 Network I/O Control”。
- 确认虚拟机系统流量包括已配置的带宽预留。请参见第 150 页，“配置系统流量的带宽分配”。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在**配置**选项卡上，展开**资源分配**。
- 3 单击**网络资源池**。
- 4 从列表中选择网络资源池，然后单击**编辑**。
- 5 在**预留配额**对话框中，输入为交换机上所有物理适配器的虚拟机系统流量预留的可用带宽聚合中虚拟机的带宽配额。
- 6 单击**确定**。

## 从网络资源池中移除分布式端口组

要停止向虚拟机分配网络资源池的预留配额中的带宽，可移除虚拟机连接到的端口组与该池之间的关联。

### 步骤

- 1 在 vSphere Web Client 中找到分布式端口组。
  - a 选择 Distributed Switch，然后单击**网络**选项卡。
  - b 单击**分布式端口组**。
- 2 选择分布式端口组，然后单击**编辑分布式端口组设置**。
- 3 在端口组的“编辑设置”对话框中，单击**常规**。
- 4 从**网络资源池**下拉菜单中，选择**(默认)**，然后单击**确定**。

分布式端口组即与默认虚拟机网络资源池相关联。

## 删除网络资源池

删除不再使用的网络资源池。

### 前提条件

将网络资源池从所有关联的分布式端口组中分离出来。请参见第 157 页，“从网络资源池中移除分布式端口组”。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在**配置**选项卡上，展开**资源分配**。

- 3 单击**网络资源池**。
- 4 选择一个网络资源池，然后单击**移除**。
- 5 单击**是删除资源池**。

## 将物理适配器移到 Network I/O Control 的范围之外

在某些情况下，您可能需要从 Network I/O Control 版本 3 的带宽分配模型中排除容量小的物理适配器。

例如，如果 vSphere Distributed Switch 上的带宽分配在 10 GbE 网卡上进行量身定制，则您可能无法向交换机添加 1 GbE 网卡，因为其无法满足在 10 GbE 网卡上配置的更高分配要求。

### 前提条件

- 验证主机正在运行 ESXi 6.0 和更高版本。
- 确认 vSphere Distributed Switch 为 6.0.0 及更高版本。
- 确认交换机上的 Network I/O Control 为版本 3。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在 **配置** 选项卡上，展开 **系统**，然后选择 **高级系统设置**。
- 3 以逗号分隔列表形式将需要在 Network I/O Control 范围之外运行的物理适配器设置为 `Net.IOControlPnicOptOut` 参数。

例如：`vmnic0,vmnic3`

- 4 单击**确定**应用更改。

## 使用 Network I/O Control 版本 2

在 vSphere Distributed Switch 5.x 上，以及在已升级到 6.0、但未将 Network I/O Control 增强到版本 3 的 vSphere Distributed Switch 上，您可确保系统流量和虚拟机可以使用 Network I/O Control 版本 2 的资源池模型收到所需的操作带宽。

### Network I/O Control 版本 2 中的网络资源池

在 Network I/O Control 版本 2 中，Distributed Switch 流量支持两类网络资源池：

- 系统网络资源池。提供给主要系统流量类型的用于控制网络带宽的预定义池：**Fault Tolerance** 流量、**iSCSI** 流量、**vMotion** 流量、**管理流量**、**vSphere Replication** 流量、**NFS** 流量和**虚拟机流量**。
- 用户定义的网络资源池。用于虚拟机流量的自定义池。用户自定义的资源池中的设置在关联该池与分布式端口组后应用到虚拟机。

## Network I/O Control 版本 2 中网络资源池的带宽分配参数

带宽分配参数	描述
份额	<p>当物理适配器饱和时，使用该适配器的虚拟机或 VMkernel 适配器会根据在网络资源池上配置的份额将带宽接收到外部网络中。</p> <p>分配给某个网络资源池的物理适配器份额确定提供给与该网络资源池关联的流量的总可用带宽份额。提供给某个网络资源池的出站流量的实际带宽份额是由网络资源池的份额以及其他网络资源池正在主动传输的内容来确定的。</p> <p>例如，您向 vSphere FT 流量和 iSCSI 流量分配 100 个份额，而每个其他网络资源池有 50 个份额。配置了一个物理适配器用于发送 vSphere Fault Tolerance、iSCSI 和管理流量。在某一时刻，vSphere Fault Tolerance 和 iSCSI 是该物理适配器上的活动流量类型，并且用光了其容量。每个流量会收到 50% 的可用带宽。在另一时刻，所有三个流量类型使该适配器呈饱和状态。在这种情况下，vSphere FT 流量和 iSCSI 流量可分别获得 40% 的适配器容量，vMotion 则可获得 20%。</p> <p><b>注意</b> iSCSI 流量资源池份额不适用于从属硬件 iSCSI 适配器的 iSCSI 流量。</p>
限制	网络资源池的主机限制是与该网络资源池关联的流量可在物理适配器上占用的最大带宽。
QoS 标记	向网络资源池分配 QoS 优先级标记会将 802.1p (CoS) 标记应用到与该网络资源池关联的所有出站数据包。如此便可标记特定流量，以便交换机等网络设备可以视为更高优先级处理。

## 在 Network I/O Control 版本 2 中创建网络资源池

当流经物理网络适配器的流量变得密集时，创建用户定义的网络资源池以对带宽分配进行自定义。

### 前提条件

- 确认 vSphere Distributed Switch 为 5.1 或更高版本。
- 确认 Distributed Switch 上的 Network I/O Control 为版本 2。
- 在 Distributed Switch 上启用 Network I/O Control。请参见第 148 页，“在 vSphere Distributed Switch 上启用 Network I/O Control”。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在配置选项卡上，展开资源分配。
- 3 单击新建。
- 4 输入网络资源池的名称和可选描述。
- 5 在限制文本框中，对与主机上连接的物理适配器有关的网络资源池输入带宽限制（以 Mbps 为单位）。默认情况下，不会应用任何流量限制。
- 6 从物理适配器份额下拉菜单中，输入与网络资源池关联的虚拟机或 VMkernel 适配器拥有的物理适配器容量的份额。  
Network I/O Control 在连接的物理适配器变成饱和状态时会应用已配置的份额。  
可以选择一个选项设置预定义的值，也可以选择自定义，然后输入从 1 到 100 的数值设置其他份额。
- 7 （可选）从 CoS 优先级标记下拉菜单中，选择用于标记与网络资源池关联的系统或虚拟机流量的 QoS 标记，然后单击确定。  
QoS 优先级标记表示一个 IEEE 802.1p (CoS) 标记，用于定义网络协议堆栈的第 2 层中与资源池关联的虚拟机的流量优先级。

## 下一步

将一个或多个分布式端口组与网络资源池关联，以在虚拟机上应用带宽控制设置。请参见第 154 页，“[向网络资源池中添加分布式端口组](#)”。

## 在 Network I/O Control 版本 2 中编辑网络资源池的设置

在 Network I/O Control 版本 2 中，编辑系统设置或用户定义的网络资源池的设置可更改与池关联的流量的优先级。

### 前提条件

- 确认 vSphere Distributed Switch 为 5.1 及更高版本。
- 确认 Distributed Switch 上的 Network I/O Control 为版本 2。
- 在 Distributed Switch 上启用 Network I/O Control。请参见第 148 页，“[在 vSphere Distributed Switch 上启用 Network I/O Control](#)”。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在配置选项卡上，展开资源分配。
- 3 从列表中选择网络资源池，然后单击编辑。
- 4 在限制文本框中，对虚拟机网络适配器可以占用的带宽设置限制。
- 5 从物理适配器份额下拉菜单中，输入与网络资源池关联的虚拟机或 VMkernel 适配器拥有的物理适配器容量的份额。

Network I/O Control 在连接的物理适配器变成饱和状态时会应用已配置的份额。

可以选择一个选项设置预定义的值，也可以选择自定义，然后输入从 1 到 100 的数值设置其他份额。

- 6 （可选）从 CoS 优先级标记下拉菜单中，选择用于标记与网络资源池关联的系统或虚拟机流量的 QoS 标记，然后单击确定。

QoS 优先级标记表示一个 IEEE 802.1p (CoS) 标记，用于定义网络协议堆栈的第 2 层中与资源池关联的虚拟机的流量优先级。

Network I/O Control 版本 2 将新的带宽控制设置应用到与网络资源池关联的分布式端口组上的 VMkernel 和虚拟机适配器。



## MAC 地址管理

---

MAC 地址用于网络协议堆栈的第 2 层（数据链路层），可将帧传输到收件人。在 vSphere 中，vCenter Server 会生成虚拟机适配器和 VMkernel 适配器的 MAC 地址，您也可以手动分配上述地址。

每一家网络适配器的制造商都分配了一个唯一的名为组织唯一标识符 (OUI) 的 3 字节前缀，此标识符可用于生成唯一的 MAC 地址。

VMware 支持多种地址分配机制，每种机制具有不同的 OUI：

- 生成的 MAC 地址
  - 由 vCenter Server 分配
  - 由 ESXi 主机分配
- 手动设置 MAC 地址
- 为旧虚拟机生成，但不再与 ESXi 一起使用

如果重新配置已关闭虚拟机电源的网络适配器（例如，通过更改自动 MAC 地址分配类型或设置静态 MAC 地址），则 vCenter Server 会在适配器重新配置生效前解决所有 MAC 地址冲突。

本章讨论了以下主题：

- [第 161 页，“从 vCenter Server 的 MAC 地址分配”](#)
- [第 164 页，“在 ESXi 主机上生成 MAC 地址”](#)
- [第 165 页，“为虚拟机设置静态 MAC 地址”](#)

### 从 vCenter Server 的 MAC 地址分配

vSphere 5.1 及更高版本提供多种方案用于在 vCenter Server 中自动分配 MAC 地址。可以选择最能满足您的 MAC 地址重复要求以及本地管理或通用管理地址的 OUI 要求等的方案。

以下 MAC 地址生成的方案在 vCenter Server 中可用：

- VMware OUI 分配（默认分配）
- 基于前缀的分配
- 基于范围的分配

在生成 MAC 地址后，除非虚拟机具有与其他已注册虚拟机冲突的 MAC 地址，否则地址不会更改。MAC 地址将保存在虚拟机的配置文件中。

---

**注意** 如果您使用了基于前缀或基于范围的无效分配值，则将在 `vpxd.log` 文件中记录一条错误。vCenter Server 将不会在置备虚拟机期间分配 MAC 地址。

---

## 防止出现 MAC 地址冲突

已关闭电源的虚拟机的 MAC 地址不会对照运行中或已挂起虚拟机的地址进行检查。

重新打开虚拟机的电源时，虚拟机可能会获取一个不同的 MAC 地址。这种变化可能是由与其他虚拟机的地址冲突引起的。在关闭了此虚拟机的电源时，其 MAC 地址已分配给打开电源的其他虚拟机。

如果重新配置已关闭电源的虚拟机的网络适配器（例如，通过更改自动 MAC 地址分配类型或设置静态 MAC 地址），则 vCenter Server 会在适配器重新配置生效前解决 MAC 地址冲突。

有关解析 MAC 地址冲突的信息，请参见 *vSphere 故障排除* 文档。

## VMware OUI 分配

VMware 组织唯一标识符 (OUI) 分配根据默认的 VMware OUI 00:50:56 和 vCenter Server ID 分配 MAC 地址。

VMware OUI 分配是虚拟机的默认 MAC 地址分配模式。分配适用于多达 64 个 vCenter Server 实例，每个 vCenter Server 可以分配多达 64000 个唯一 MAC 地址。VMware OUI 分配方案适用于小规模部署。

### MAC 地址格式

根据 VMware OUI 分配方案，MAC 地址采用 00:50:56:XX:YY:ZZ 格式，其中 00:50:56 表示 VMware OUI，XX 的计算方法为 (80 + vCenter Server ID)，YY 和 ZZ 是随机两位十六进制数字。

通过 VMware OUI 分配创建的地址的范围为 00:50:56:80:YY:ZZ - 00:50:56:BF:YY:ZZ。

## 基于前缀的 MAC 地址分配

在 ESXi 主机 5.1 及更高版本上，可以使用基于前缀的分配来指定除 VMware 默认 OUI 00:50:56 以外的其他 OUI，或引入本地管理 MAC 地址 (LAA) 以获取更大的地址空间。

基于前缀的 MAC 地址分配解决了默认 VMware 分配的限制，可在较大规模部署中提供唯一地址。引入 LAA 前缀可获得很大的 MAC 地址空间（2 的 46 次方），而通用唯一地址 OUI 只能提供 1600 万 MAC 地址空间。

确认在同一个网络中为不同 vCenter Server 实例提供的前缀是唯一的。vCenter Server 依靠这些前缀来避免 MAC 地址重复问题。请参见 *vSphere 故障排除* 文档。

## 基于范围的 MAC 地址分配

在 ESXi 主机 5.1 及更高版本中，您可以使用基于范围的分配来包含或排除本地管理地址 (LAA) 的范围。

您可使用起始 MAC 地址和结束 MAC 地址指定一个或多个范围，例如 (02:50:68:00:00:02, 02:50:68:00:00:FF)。MAC 地址仅在指定的范围内生成。

您可以指定多个 LAA 范围，并且 vCenter Server 会跟踪每个范围内的已使用地址数。vCenter Server 将从第一个仍包含可用地址的范围分配 MAC 地址。vCenter Server 会检查其范围内的 MAC 地址是否冲突。

在使用基于范围的分配时，必须为 vCenter Server 的不同实例提供不重叠的范围。vCenter Server 不会检测可能会与其他 vCenter Server 实例相冲突的范围。有关解决 MAC 地址重复问题的详细信息，请参见 *vSphere 故障排除* 文档。

## 分配 MAC 地址

使用 vSphere Web Client 启用基于前缀或基于范围的 MAC 地址分配，以及调整分配参数。

如果您正从一种分配类型更改为另一种类型（例如，从 VMware OUI 分配更改为基于范围的分配），请使用 vSphere Web Client。但是，如果方案是基于前缀或基于范围的并且您希望更改为其他分配方案，则必须手动编辑 vpxd.cfd 文件并重新启动 vCenter Server。

更改为或调整基于范围或基于前缀的分配

通过在 vSphere Web Client 中从默认 VMware OUI 切换为基于范围或基于前缀的 MAC 地址分配，可以避免和解决 vSphere 部署中 MAC 地址重复冲突问题。

使用 vSphere Web Client 中的 vCenter Server 实例可用的**高级设置**将分配方案从默认的 VMware OUI 更改为基于范围或基于前缀的分配。

要从基于范围或基于前缀的分配切换回 VMware OUI 分配，或在基于范围与基于前缀的分配之间切换，请手动编辑 vpxd.cfg 文件。请参见第 163 页，“设置或更改分配类型”。

**注意** 在 vCenter Server 5.1 和 ESXi 5.1 及更高版本的主机中，应使用基于前缀的 MAC 地址分配。

如果 vCenter Server 5.1 实例管理运行低于 ESXi 5.1 的 ESXi 版本的主机，应使用 VMware OUI 基于前缀的 MAC 地址分配。分配了非 VMware OUI 前缀 MAC 地址的虚拟机将无法在低于 5.1 版本的主机上打开电源。这些主机以显式方式检查所分配的 MAC 地址是否使用 VMware OUI 00:50:56 前缀。

步骤

- 1 在 vSphere Web Client 中，导航到 vCenter Server 实例。
- 2 在**配置**选项卡上，展开**设置**，然后选择**高级设置**。
- 3 单击**编辑**。
- 4 添加或编辑目标分配类型的参数。

仅使用一种分配类型。

- 更改为基于前缀的分配。

键	示例值
config.vpxd.macAllocScheme.prefixScheme.prefix	005026
config.vpxd.macAllocScheme.prefixScheme.prefixLength	23

prefix 和 prefixLength 确定新添加的 vNIC 所具有的 MAC 地址前缀的范围。prefix 是与 vCenter Server 实例关联的 MAC 地址的起始 OUI，prefixLength 则确定前缀长度的位数。

例如，表中的设置使 VM NIC MAC 地址以 00:50:26 或 00:50:27 开头。

- 更改为基于范围的分配。

键	示例值
config.vpxd.macAllocScheme.rangeScheme.range[X].begin	005067000000
config.vpxd.macAllocScheme.rangeScheme.range[X].end	005067ffff

range[X] 中的 x 代表范围序号。例如，range[0] 中的 0 表示 MAC 地址分配的第一个范围的分配设置。

- 5 单击**确定**。

设置或更改分配类型

如果要将基于范围或基于前缀的分配更改为 VMware OUI 分配，必须在 vpxd.cfd 文件中设置分配类型，然后重新启动 vCenter Server。

前提条件

请在更改 vpxd.cfg 文件之前确定分配类型。有关分配类型的信息，请参见第 161 页，“从 vCenter Server 的 MAC 地址分配”

**步骤**

- 1 在 vCenter Server 的主机上，导航到包含配置文件的目录：
  - 在 Windows Server 操作系统上，目录的位置为 C:\ProgramData\VMware\CIS\cfg\vmware-vpx。
  - 在 vCenter Server Appliance 上，目录的位置为 /etc/vmware-vpx。
- 2 打开 vpxd.cfg 文件。
- 3 决定要使用的分配类型，然后在文件中输入相应的 XML 代码来配置该分配类型。

以下是要使用的 XML 代码的示例。

---

**注意** 仅使用一种分配类型。

---

◆ VMware OUI 分配

```
<vpxd>
<macAllocScheme>
<VMwareOUI>true</VMwareOUI>
</macAllocScheme>
</vpxd>
```

◆ 基于前缀的分配

```
<vpxd>
<macAllocScheme>
<prefixScheme>
<prefix>005026</prefix>
<prefixLength>23</prefixLength>
</prefixScheme>
</macAllocScheme>
</vpxd>
```

◆ 基于范围的分配

```
<vpxd>
<macAllocScheme>
<rangeScheme>
<range id="0">
<begin>005067000001</begin>
<end>005067000001</end>
</range>
</rangeScheme>
</macAllocScheme>
</vpxd>
```

- 4 保存 vpxd.cfg。
- 5 重新启动 vCenter Server 主机。

## 在 ESXi 主机上生成 MAC 地址

当 ESXi 主机未连接到 vCenter Server 时，会为虚拟机适配器生成 MAC 地址。此类地址具有单独的 VMware OUI，以避免发生冲突。

在以下任一情况下，ESXi 主机会为虚拟机适配器生成 MAC 地址：

- 主机未连接到 vCenter Server。
- 虚拟机配置文件不包含 MAC 地址和有关 MAC 地址分配类型的信息。

## MAC 地址格式

主机生成的 MAC 地址由 VMware OUI 00:0C:29 和最后三个八位字节（采用十六进制格式的虚拟机 UUID）组成。虚拟机 UUID 基于哈希值，该哈希值使用 ESXi 物理机的 UUID 和虚拟机配置文件（.vmx）的路径计算得出。

## 防止出现 MAC 地址冲突

系统将跟踪特定物理机上已分配给运行中和已挂起虚拟机的网络适配器的所有 MAC 地址，以防止出现冲突。

如果将具有主机生成的 MAC 地址的虚拟机从一个 vCenter Server 导入到另一个，请在打开虚拟机电源重新生成地址时选择**我已复制**选项，从而避免在目标 vCenter Server 中或在 vCenter Server 系统之间出现潜在冲突。

## 为虚拟机设置静态 MAC 地址

在大多数网络部署中，生成的 MAC 地址都是合适的。但是，可能需要为虚拟机适配器设置唯一的静态 MAC 地址。

以下情况可能需要设置静态 MAC 地址：

- 不同物理主机上的虚拟机适配器由于共享同一子网且分配了相同的 MAC 地址而发生冲突。
- 确保虚拟机适配器始终拥有同一个 MAC 地址。

默认情况下，VMware 将组织唯一标识符 (OUI) 00:50:56 用于手动生成的地址，但支持所有唯一的手动生成的地址。

---

**注意** 确保没有其他非 VMware 设备使用分配给 VMware 组件的地址。例如，同一子网中可能有物理服务器使用 11:11:11:11:11:11、22:22:22:22:22:22 作为静态 MAC 地址。由于物理服务器不属于 vCenter Server 清单，因此 vCenter Server 无法检查是否存在地址冲突。

---

## 静态 MAC 地址的 VMware OUI

默认情况下，静态 MAC 地址以 VMware 组织唯一标识符 (OUI) 作为前缀。但是，受 VMware OUI 提供的可用地址范围限制。

如果决定使用 VMware OUI，则部分范围已经预留，可供 vCenter Server、主机物理网卡和虚拟网卡使用，以及供将来使用。

可以设置符合以下格式的包含 VMware OUI 前缀的静态 MAC 地址：

00:50:56:XX:YY:ZZ

其中，XX 是 00 至 3F 之间有效的十六进制数字，而 YY 和 ZZ 是 00 至 FF 之间有效的十六进制数字。为避免与 vCenter Server 生成的或分配到适用于基础架构流量的 VMkernel 适配器的 MAC 地址冲突，XX 的值不能大于 3F。

对于手动生成的 MAC 地址，其最大值如下。

00:50:56:3F:FF:FF

为避免生成的 MAC 地址与手动分配的 MAC 地址冲突，请从硬编码的地址中为 XX:YY:ZZ 选择唯一值。

## 通过使用 vSphere Web Client 分配静态 MAC 地址

可以使用 vSphere Web Client 将静态 MAC 地址分配给已关闭电源的虚拟机的虚拟网卡。

### 步骤

- 1 在 vSphere Web Client 中找到虚拟机。
  - a 选择数据中心、文件夹、群集、资源池或主机，然后单击**虚拟机**选项卡。
  - b 单击**虚拟机**，然后从列表中双击虚拟机。
- 2 关闭虚拟机电源。
- 3 在虚拟机的**配置**选项卡上，展开**设置**，然后选择**虚拟机硬件**。
- 4 单击**编辑**，然后在显示设置的对话框中选择**虚拟硬件**选项卡。
- 5 在**虚拟硬件**选项卡中，展开网络适配器部分。
- 6 在 MAC 地址下，从下拉菜单中选择**手动**。
- 7 键入静态 MAC 地址，然后单击**确定**。
- 8 打开虚拟机电源。

## 在虚拟机配置文件中分配静态 MAC 地址

要为虚拟机设置静态 MAC 地址，可以使用 vSphere Web Client 编辑虚拟机的配置文件。

### 步骤

- 1 在 vSphere Web Client 中找到虚拟机。
  - a 选择数据中心、文件夹、群集、资源池或主机，然后单击**虚拟机**选项卡。
  - b 单击**虚拟机**，然后从列表中双击虚拟机。
- 2 关闭虚拟机电源。
- 3 在虚拟机的**配置**选项卡上，展开**设置**，然后选择**虚拟机选项**。
- 4 单击**编辑**，并从显示该设置的对话框内的**虚拟机选项**选项卡中展开**高级**。
- 5 单击**编辑配置**。
- 6 要分配静态 MAC 地址，请根据需要添加或编辑参数。

参数	值
ethernetX.addressType	静态
ethernetX.address	MAC_address_of_the_virtual_NIC

ethernet 旁边的 X 表示虚拟机中虚拟网卡的序列号。

例如，ethernet0 中的 0 表示第一个添加到虚拟机的虚拟网卡设备的设置。

- 7 单击**确定**。
- 8 打开虚拟机电源。

## 针对 IPv6 配置 vSphere

对于更大的地址空间和改进的地址分配，请配置 ESXi 主机和 vCenter Server 以便在纯 IPv6 环境中操作。

IPv6 被 Internet 工程任务组 (IETF) 指定为 IPv4 的继承者，提供了以下优势：

- 增加了地址长度。增加的地址空间可解决地址耗尽问题并消除网络地址转换的需要。与 IPv4 使用的 32 位地址相比较，IPv6 使用 128 位地址。
- 能够改进节点地址的重新配置。

本章讨论了以下主题：

- [第 167 页，“vSphere IPv6 连接”](#)
- [第 168 页，“在 IPv6 中部署 vSphere”](#)
- [第 170 页，“在主机上启用或禁用 IPv6 支持”](#)
- [第 171 页，“在 ESXi 主机上设置 IPv6”](#)
- [第 171 页，“在 vCenter Server 上设置 IPv6”](#)

### vSphere IPv6 连接

在基于 vSphere 6.0 及更高版本的环境中，节点和功能可以通过支持静态和自动地址配置的 IPv6 以透明方式进行通信。

#### vSphere 节点之间进行通信时使用的 IPv6

vSphere 部署中的节点可以使用 IPv6 进行通信，并根据网络配置接收分配的地址。

**表 13-1** vSphere 环境中节点的 IPv6 支持

连接类型	IPv6 支持	vSphere 节点的地址配置
ESXi 到 ESXi	是	<ul style="list-style-type: none"> <li>■ 静态</li> <li>■ 自动：AUTOCONF/DHCPv6</li> </ul>
vCenter Server 计算机到 ESXi	是	<ul style="list-style-type: none"> <li>■ 静态</li> <li>■ 自动：AUTOCONF/DHCPv6</li> </ul>
vCenter Server 计算机到 vSphere Web Client 计算机	是	<ul style="list-style-type: none"> <li>■ 静态</li> <li>■ 自动：AUTOCONF/DHCPv6</li> </ul>
ESXi 到 vSphere Client 计算机	是	<ul style="list-style-type: none"> <li>■ 静态</li> <li>■ 自动：AUTOCONF/DHCPv6</li> </ul>
虚拟机到虚拟机	是	<ul style="list-style-type: none"> <li>■ 静态</li> <li>■ 自动：AUTOCONF/DHCPv6</li> </ul>

**表 13-1** vSphere 环境中节点的 IPv6 支持（续）

连接类型	IPv6 支持	vSphere 节点的地址配置
ESXi 到 iSCSI 存储	是	<ul style="list-style-type: none"> <li>■ 静态</li> <li>■ 自动: AUTOCONF/DHCPv6</li> </ul>
ESXi 到 NFS 存储	是	<ul style="list-style-type: none"> <li>■ 静态</li> <li>■ 自动: AUTOCONF/DHCPv6</li> </ul>
ESXi 到 Active Directory	否 使用 LDAP 通过 vCenter Server 将 ESXi 连接到 Active Directory 数据库	-
vCenter Server Appliance 到 Active Directory	否 使用 LDAP 将 vCenter Server Appliance 连接到 Active Directory 数据库	-

## vSphere 功能的 IPv6 连接

某些 vSphere 功能不支持 IPv6:

- Auto Deploy
- 通过智能平台管理界面 (IPMI) 和 Hewlett-Packard Integrated Lights-Out (iLO) 的 vSphere DPM。vSphere 6.0 仅支持通过 LAN 唤醒 (WOL) 使主机退出待机模式。
- Virtual SAN
- Authentication Proxy
- 使用基于 AUTH\_SYS 验证方式的 NFS 4.1。
- 连接到 Active Directory 的 vSphere Management Assistant 和 vSphere Command-Line Interface。  
使用 LDAP 将 vSphere Management Assistant 或 vSphere Command-Line Interface 连接到 Active Directory 数据库。

## 虚拟机的 IPv6 连接

虚拟机可以通过 IPv6 在网络中交换数据。vSphere 支持为虚拟机静态和自动分配 IPv6 地址。

自定义虚拟机的客户机操作系统时，也可以配置一个或多个 IPv6 地址。

## FQDN 和 IPv6 地址

在 vSphere 中，应使用映射到 DNS 服务器上的 IPv6 地址的完全限定域名 (FQDN)。如果 DNS 服务器上存在有效 FQDN 以供反向查找，则可以使用 IPv6 地址。

要在纯 IPv6 环境中部署 vCenter Server，只能使用 FQDN。

## 在 IPv6 中部署 vSphere

在纯 IPv6 环境中运行 vSphere 以使用扩展地址空间和可变地址分配。

如果计划在 IPv6 网络中部署 vCenter Server 和 ESXi 主机，还必须执行额外步骤。

- 在 [vSphere 安装中启用 IPv6](#) 第 169 页，  
如果您拥有 IPv6 网络中的 vSphere 6.0 的绿地部署，请通过在部署节点上配置 IPv6 并连接这些节点为纯 IPv6 管理连接配置 ESXi 和 vCenter Server。



- 在升级的 vSphere 环境中启用 IPv6 第 169 页，  
在包含已安装或已升级 vCenter Server 和已升级 ESXi 的 vSphere 6.0 的 IPv4 部署中，配置用于纯 IPv6 管理连接的 ESXi 和 vCenter Server，方法是在已部署节点上启用 IPv6，并重新连接。

在 vSphere 安装中启用 IPv6

如果您拥有 IPv6 网络中的 vSphere 6.0 的绿地部署，请通过在部署节点上配置 IPv6 并连接这些节点为纯 IPv6 管理连接配置 ESXi 和 vCenter Server。

前提条件

- 验证是否已将 vCenter Server、ESXi 主机和外部数据库的 IPv6 地址（如果使用）映射到 DNS 服务器上的完全限定域名 (FQDN)。
- 验证网络基础架构是否为 ESXi 主机、vCenter Server 和外部数据库提供了 IPv6 连接。
- 验证是否已使用映射到 IPv6 地址的 FQDN 安装 vCenter Server 的 6.0 版本。请参见 *vSphere 安装和设置* 文档。
- 验证是否主机已安装 ESXi 6.0。请参见 *vSphere 安装和设置* 文档。

步骤

- 1 在直接控制台用户界面 (DCUI) 中，将每个 ESXi 主机配置为纯 IPv6 节点。
  - a 在 DCUI 中，按 F2，然后登录到主机。
  - b 在配置管理网络菜单中，选择 IPv6 配置，然后按 Enter。
  - c 将 IPv6 地址分配给主机。

地址分配选项	描述
使用 DHCPv6 自动分配地址	1 选择使用动态 IPv6 地址和网络配置选项，然后选择使用 DHCPv6。 2 按 Enter 保存更改。
静态地址分配	1 选择设置静态 IPv6 地址和网络配置选项，然后输入主机的 IPv6 地址和默认网关。 2 按 Enter 保存更改。

- d 在配置管理网络菜单中，选择 IPv4 配置，然后按 Enter。
  - e 选择禁用管理网络的 IPv4 配置，然后按 Enter。
- 2 在 vSphere Web Client 中，将主机添加到清单。

在升级的 vSphere 环境中启用 IPv6

在包含已安装或已升级 vCenter Server 和已升级 ESXi 的 vSphere 6.0 的 IPv4 部署中，配置用于纯 IPv6 管理连接的 ESXi 和 vCenter Server，方法是在已部署节点上启用 IPv6，并重新连接。

前提条件

- 验证网络基础架构是否为 ESXi 主机、vCenter Server 和外部数据库提供了 IPv6 连接。
- 验证是否已将 vCenter Server、ESXi 主机和外部数据库的 IPv6 地址（如果使用）映射到 DNS 服务器上的完全限定域名 (FQDN)。
- 验证是否已安装或升级版本 6.0 的 vCenter Server。请参见 *vSphere 安装和设置* 和 *vSphere 升级* 文档。
- 验证是否所有主机已升级到版本 6.0 ESXi。请参见 *vSphere 升级* 文档。

**步骤**

- 1 在 vSphere Web Client 中，从 vCenter Server 断开主机的连接。
- 2 在直接控制台用户界面 (DCUI) 中，将每个 ESXi 主机配置为纯 IPv6 节点。
  - a 在 DCUI 中，按 F2，然后登录到主机。
  - b 在**配置管理网络**菜单中，选择 **IPv6 配置**，然后按 Enter。
  - c 将 IPv6 地址分配给主机。

地址分配选项	描述
<b>使用 DHCPv6 自动分配地址</b>	<ol style="list-style-type: none"> <li>1 选择<b>使用动态 IPv6 地址和网络配置</b>选项，然后选择<b>使用 DHCPv6</b>。</li> <li>2 按 Enter 保存更改。</li> </ol>
<b>静态地址分配</b>	<ol style="list-style-type: none"> <li>1 选择<b>设置静态 IPv6 地址和网络配置</b>选项，然后输入主机的 IPv6 地址和默认网关。</li> <li>2 按 Enter 保存更改。</li> </ol>

- d 在**配置管理网络**菜单中，选择 **IPv4 配置**，然后按 Enter。
  - e 选择**禁用管理网络的 IPv4 配置**，然后按 Enter。
- 3 如果 vCenter Server 使用外部数据库，请将数据库配置为 IPv6 节点。
- 4 将 vCenter Server 配置为纯 IPv6 节点，并将其重新启动。
- 5 在数据库服务器上禁用 IPv4。
- 6 在 vSphere Web Client 中，将主机添加到清单。
- 7 在网络基础架构中禁用 IPv4。

**在主机上启用或禁用 IPv6 支持**

vSphere 中的 IPv6 支持可使主机能够在具有地址空间大、增强型多播、简化路由等特征的 IPv6 网络环境中正常运行。

在 ESXi 5.1 及更高版本中，默认启用 IPv6。

**步骤**

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在**配置选项卡**上，展开**网络**并选择**高级**。
- 3 单击**编辑**。
- 4 从 **IPv6 支持**下拉菜单中启用或禁用 IPv6 支持。
- 5 单击**确定**。
- 6 重新引导主机来应用 IPv6 支持中的更改。

**下一步**

在主机上配置 VMkernel 适配器（例如管理网络）的 IPv6 设置。请参见第 171 页，“在 ESXi 主机上设置 IPv6”。

## 在 ESXi 主机上设置 IPv6

要通过 IPv6 将 ESXi 主机连接到管理网络、vSphere vMotion、共享存储器、vSphere Fault Tolerance 等，请编辑主机上的 VMkernel 适配器的 IPv6 设置。

### 前提条件

验证 ESXi 主机上是否启用了 IPv6。请参见第 170 页，“在主机上启用或禁用 IPv6 支持”。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开网络，然后选择 VMkernel 适配器。
- 3 选择目标 Distributed Switch 或标准交换机上的 VMkernel 适配器，然后单击编辑。
- 4 在“编辑设置”对话框中，单击 IPv6 设置。
- 5 配置 VMkernel 适配器的地址分配。

IPv6 地址选项	描述
通过 DHCP 自动获取 IPv6 地址	从 DHCPv6 服务器接收 VMkernel 适配器的 IPv6 地址。
通过路由器公告自动获取 IPv6 地址	通过路由器公告从路由器接收 VMkernel 适配器的 IPv6 地址。
静态 IPv6 地址	设置一个或多个地址。对于每个地址条目，输入适配器的 IPv6 地址、子网前缀长度和默认网关的 IPv6 地址。

可以根据网络配置选择多个分配选项。

- 6 （可选）从“IPv6 设置”的“高级设置”部分中，移除通过路由器公告分配的某些 IPv6 地址。  
可以删除主机通过路由器公告获取的某些 IPv6 地址以停止这些地址上的通信。可以删除所有自动分配的地址以强制执行 VMkernel 上已配置的静态地址。
- 7 单击确定在 VMkernel 适配器上应用更改。

## 在 vCenter Server 上设置 IPv6

配置 vCenter Server 以便与 IPv6 网络中的 ESXi 主机和 vSphere Web Client 进行通信。

### 在 vCenter Server Appliance 上设置 IPv6

使用 vSphere Web Client 配置 vCenter Server Appliance 以便与 IPv6 网络中的 ESXi 主机进行通信。

### 步骤

- 1 在 vSphere Web Client 主页中，单击系统配置。
- 2 在“系统配置”下，单击节点。
- 3 在“节点”下选择一个节点，然后单击管理选项卡。
- 4 选择“通用”下面的网络并单击编辑。
- 5 展开网络接口名称以编辑 IP 地址设置。

## 6 编辑 IPv6 设置。

选项	描述
通过 DHCP 自动获取 IPv6 设置	使用 DHCP 自动将网络的 IPv6 地址分配给设备。
通过路由器通告自动获取 IPv6 设置	使用路由器通告自动将网络的 IPv6 地址分配给设备。
静态 IPv6 地址	<p>使用手动设置的静态 IPv6 地址。</p> <ol style="list-style-type: none"> <li>1 单击<b>添加</b>图标。</li> <li>2 输入 IPv6 地址和子网前缀长度。</li> <li>3 单击<b>确定</b>。</li> <li>4 （可选）编辑默认网关。</li> </ol>

可以将设备配置为通过 DHCP 和路由器通告自动获取 IPv6 设置。可以同时分配静态 IPv6 地址。

7 （可选）要移除通过路由器公告自动分配的 IPv6 地址，请单击 **移除地址**，然后删除地址。

您可能希望删除 vCenter Server Appliance 通过路由器公告获取的某些 IPv6 地址，以停止这些地址上的通信或强制执行已配置的静态地址。

**下一步**

使用其 FQDN 通过 IPv6 将 ESXi 主机连接到 vCenter Server。

**使用 IPv6 在 Windows 中设置 vCenter Server**

要使用 IPv6 将 ESXi 主机或 vSphere Web Client 连接到在 Windows 主机上运行的 vCenter Server，请在 Windows 中配置 IPv6 地址设置。

**步骤**

- ◆ 在 Windows 控制面板的“网络和共享中心”文件夹中，为主机配置用于“局域网连接”的 IPv6 地址设置。

**下一步**

使用其 FQDN 通过 IPv6 将 ESXi 主机连接到 vCenter Server。

## 监控网络连接和流量

---

监控通过 vSphere 标准交换机或 vSphere Distributed Switch 的端口的网络连接和网络数据包，以分析虚拟机和主机之间的流量。

本章讨论了以下主题：

- 第 173 页，“使用 `pktcap-uw` 实用程序捕获和跟踪网络数据包”
- 第 185 页，“配置 vSphere Distributed Switch 的 NetFlow 设置”
- 第 186 页，“使用端口镜像”
- 第 192 页，“vSphere Distributed Switch 运行状况检查”
- 第 193 页，“交换机发现协议”

### 使用 `pktcap-uw` 实用程序捕获和跟踪网络数据包

监控流经物理网络适配器、VMkernel 适配器和虚拟机适配器的流量，并使用诸如 Wireshark 的网络分析工具的图形用户界面分析数据包信息。

在 vSphere 5.5 或更高版本中，可以使用 `pktcap-uw` 控制台实用程序监控主机上的数据包。该实用工具无需在 ESXi 主机上进行额外安装便可使用。`pktcap-uw` 提供主机网络堆栈中许多可以监控流量的监控点。

要对捕获的数据包进行详细分析，可以通过 `pktcap-uw` 实用程序将数据包内容保存为 PCAP 或 PCAPNG 格式的文件，然后在 Wireshark 中打开这些文件。您也可以对丢弃的数据包进行故障排除，以及跟踪数据包在网络堆栈中的路径。

---

**注意** `pktcap-uw` 实用程序在 vSphere 各个版本中并不完全支持向后兼容。实用程序的选项将来可能有变。

---

### 用于捕获数据包的 `pktcap-uw` 命令语法

使用 `pktcap-uw` 实用程序可在数据包遍历 ESXi 主机上的网络堆栈时检查数据包的内容。

#### 用于捕获数据包的 `pktcap-uw` 语法

`pktcap-uw` 命令使用以下语法捕获网络堆栈中某个位置的数据包：

```
pktcap-uw switch_port_arguments capture_point_options filter_options output_control_options
```

---

**注意** `pktcap-uw` 实用程序的某些选项仅供 VMware 内部使用，您只有在 VMware 技术支持部门的督导下才能使用这些选项。《vSphere 网络连接》指南中并未介绍这些选项。

---

**表 14-1** 用于捕获数据包的 pktcap-uw 参数

参数组	参数	描述
<i>switch_port_arguments</i>	<code>--uplink vmnicX</code>	捕获与物理适配器相关的数据包。 您可以组合使用 <code>--uplink</code> 和 <code>--capture</code> 选项来监控物理适配器与虚拟交换机之间路径中的某个位置的数据包。 请参见第 177 页，“捕获到达物理适配器的数据包”。
	<code>--vmk vmkX</code>	捕获与 VMkernel 适配器相关的数据包。 您可以组合使用 <code>vmk</code> 和 <code>--capture</code> 选项来监控 VMkernel 适配器与虚拟交换机之间路径中的某个位置的数据包。 请参见第 180 页，“为 VMkernel 适配器捕获数据包”。
	<code>--switchport {vmxnet3_port_ID   vmkernel_adapter_port_ID}</code>	捕获与 VMXNET3 虚拟机适配器相关或与连接到特定虚拟交换机端口的 VMkernel 适配器相关的数据包。您可以在 <code>esxtop</code> 实用程序的网络面板中查看端口的 ID。 您可以组合使用 <code>switchport</code> 和 <code>capture</code> 选项来监控 VMXNET3 适配器或 VMkernel 适配器与虚拟交换机之间路径中的某个位置的数据包。 请参见第 178 页，“为 VMXNET3 虚拟机适配器捕获数据包”。
<i>capture_point_options</i>	<code>--capture capture_point</code>	捕获网络堆栈中特定位置的数据包。例如，可以在接收到来自物理适配器的数据包之后立即对其进行监控。
	<code>--dir {0 1}</code>	根据流量相对于虚拟交换机的方向捕获数据包。 0 代表入站流量，1 代表出站流量。 默认情况下， <code>pktcap-uw</code> 实用程序捕获输入的流量。 使用 <code>--dir</code> 选项连同 <code>--uplink</code> 、 <code>--vmk</code> 或 <code>--switchport</code> 选项。
	<code>--stage {0 1}</code>	捕获更靠近其源或目标的数据包。使用此信息可检查数据包在遍历堆栈中各个点时的变化情况。 0 表示更靠近源的流量，1 表示更靠近目标的流量。 使用 <code>--stage</code> 选项连同 <code>--uplink</code> 、 <code>--vmk</code> 、 <code>--switchport</code> 或 <code>--dvfilter</code> 选项。
	<code>--dvfilter filter_name --capture PreDVFilter PostDVFilter</code>	在 vSphere Network Appliance (DVFilter) 拦截数据包之前或之后对其进行捕获。请参见第 182 页，“在 DVFilter 级别捕获数据包”。

表 14-1 用于捕获数据包的 pktcap-uw 参数（续）

参数组	参数	描述
	-A   --availpoints	查看 <b>pktcap-uw</b> 实用程序支持的所有捕获点。
		有关 <b>pktcap-uw</b> 实用程序的捕获点的详细信息，请参见第 183 页，“ <b>pktcap-uw 实用程序的捕获点</b> ”。
<i>filter_options</i>		根据源或目标的地址、VLAN ID、VXLAN ID、第 3 层协议和 TCP 端口筛选捕获的数据包。请参见第 176 页，“ <b>用于筛选数据包的 pktcap-uw 选项</b> ”。
<i>output_control_options</i>		将数据包的内容保存到文件、仅捕获一定数量的数据包、捕获数据包开头一定数量的字节等等。请参见第 175 页，“ <b>用于输出控制的 pktcap-uw 选项</b> ”。

竖线 | 代表替换值，与竖线一起使用的大括号 {} 用于指定参数或选项的选择列表。

用于跟踪数据包的 pktcap-uw 命令语法

使用 **pktcap-uw** 实用程序可查看数据包在 ESXi 主机上的网络堆栈中的路径，以便进行滞后时间分析。

用于跟踪数据包的 pktcap-uw 语法

**pktcap-uw** 实用程序的命令使用以下语法跟踪网络堆栈中的数据包：

```
pktcap-uw --trace filter_options
                    output_control_options
```

用于跟踪数据包的 pktcap-uw 实用程序选项

使用 **pktcap-uw** 实用程序跟踪数据包时，支持使用以下选项：

表 14-2 用于跟踪数据包的 pktcap-uw 选项

参数	描述
<i>filter_options</i>	根据源或目标的地址、VLAN ID、VXLAN ID、第 3 层协议和 TCP 端口筛选跟踪的数据包。请参见第 176 页，“ <b>用于筛选数据包的 pktcap-uw 选项</b> ”。
<i>output_control_options</i>	将数据包内容保存到文件以及仅跟踪一定数量的数据包。请参见第 175 页，“ <b>用于输出控制的 pktcap-uw 选项</b> ”。

用于输出控制的 pktcap-uw 选项

使用 **pktcap-uw** 实用程序的输出控制选项可将数据包内容保存到文件，从每个数据包捕获最多一定数量的字节，以及限制捕获的数据包数量。

用于输出控制的 pktcap-uw 选项

**pktcap-uw** 实用程序的输出控制选项在捕获和跟踪数据包时有效。有关 **pktcap-uw** 实用程序命令语法的信息，请参见第 173 页，“**用于捕获数据包的 pktcap-uw 命令语法**”和第 175 页，“**用于跟踪数据包的 pktcap-uw 命令语法**”。

表 14-3 pktcap-uw 实用程序支持的输出控制选项

选项	描述
{-o   --outfile} <i>pcap_file</i>	将捕获或跟踪的数据包保存在数据包捕获 (PCAP) 格式的文件中。使用此选项可在可视化分析器工具（如 Wireshark）中检查数据包。
-P   --ng	将数据包内容保存在 PCAPNG 格式的文件中。可将此选项与 -o 或 --outfile 选项一起使用。
--console	将数据包详细信息和内容打印到控制台输出内容中。默认情况下， <b>pktcap-uw</b> 实用程序会在控制台输出内容中显示数据包信息。
{-c   --count} <i>number_of_packets</i>	捕获前若干个数据包（ <i>number_of_packets</i> 用于指定数据包个数）。
{-s   --snaplen} <i>snapshot_length</i>	从每个数据包中仅捕获前若干长度的字节（ <i>snapshot_length</i> 用于指定字节长度）。如果主机上的流量很大，可使用此选项减少 CPU 和存储器的负载。 要限制捕获内容的大小，请设置一个大于 24 的值。 要捕获完整的数据包，请将此选项设置为 0。
-h	查看有关 <b>pktcap-uw</b> 实用程序的帮助信息。

竖线 | 代表替换值，与竖线一起使用的大括号 {} 用于指定参数或选项的选择列表。

## 用于筛选数据包的 pktcap-uw 选项

通过使用 **pktcap-uw** 实用程序为源地址和目标地址、VLAN、VXLAN 和占用数据包负载的下一级别协议应用筛选选项，可缩小监控的数据包范围。

### 筛选选项

**pktcap-uw** 的筛选选项在捕获和跟踪数据包时有效。有关 **pktcap-uw** 实用程序命令语法的信息，请参见第 173 页，“用于捕获数据包的 **pktcap-uw** 命令语法”和第 175 页，“用于跟踪数据包的 **pktcap-uw** 命令语法”。

表 14-4 pktcap-uw 实用程序的筛选选项

选项	描述
--srcmac <i>mac_address</i>	捕获或跟踪具有特定源 MAC 地址的数据包。使用冒号分隔其中的八位字节。
--dstmac <i>mac_address</i>	捕获或跟踪具有特定目标 MAC 地址的数据包。使用冒号分隔其中的八位字节。
--mac <i>mac_address</i>	捕获或跟踪具有特定源 MAC 地址或目标 MAC 地址的数据包。使用冒号分隔其中的八位字节。
--ethtype 0x <i>EtherType</i>	根据占用数据包负载的下一级别协议捕获或跟踪位于第 2 层的数据包。 <i>EtherType</i> 对应于以太网帧中的 <i>EtherType</i> 字段。它表示占用帧负载的下一级别协议的类型。 例如，要监控链路层发现协议 (LLDP) 的流量，请键入 <b>--ethtype 0x88CC</b> 。
--vlan <i>VLAN_ID</i>	捕获或跟踪属于 VLAN 的数据包。
--srcip <i>IP_address IP_address/subnet_range</i>	捕获或跟踪具有特定源 IPv4 地址或子网的数据包。
--dstip <i>IP_address IP_address/subnet_range</i>	捕获或跟踪具有特定目标 IPv4 地址或子网的数据包。
--ip <i>IP_address</i>	捕获或跟踪具有特定源 IPv4 地址或目标 IPv4 地址的数据包。



表 14-4 pktcap-uw 实用程序的筛选选项（续）

选项	描述
<code>--proto 0xIP_protocol_number</code>	根据占用负载的下一级别协议捕获或跟踪位于第 3 层的数据包。 例如，要监控 UDP 协议的流量，请键入 <code>--proto 0x11</code> 。
<code>--srcport source_port</code>	根据数据包的源 TCP 端口对其进行捕获或跟踪。
<code>--dstport destination_port</code>	根据数据包的目标 TCP 端口对其进行捕获或跟踪。
<code>--tcpport TCP_port</code>	根据数据包的源 TCP 端口或目标 TCP 端口对其进行捕获或跟踪。
<code>--vxlان VXLAN_ID</code>	捕获或跟踪属于 VXLAN 的数据包。

竖线 | 表示替代值。

使用 pktcap-uw 实用程序捕获数据包

通过 pktcap-uw 实用程序捕获虚拟交换机与物理适配器、VMkernel 适配器和虚拟机适配器之间的路径中的数据包，可对 ESXi 主机上的网络堆栈中的数据传输进行故障排除。

捕获到达物理适配器的数据包

通过捕获 vSphere 标准交换机或 vSphere Distributed Switch 与物理适配器之间路径中的某些点的数据包，监控与外部网络相关的主机流量。

您可以指定虚拟交换机与物理适配器之间的数据路径中的某个捕获点，也可以根据相对于交换机的流量方向以及与数据包源位置或目标位置的邻近程度来确定捕获点。有关支持的捕获点的信息，请参见第 183 页，“pktcap-uw 实用程序的捕获点”。

步骤

- 1（可选）在主机适配器列表中查找要监控的物理适配器的名称。
  - 在 vSphere Web Client 中，在主机的配置选项卡上展开网络，然后选择物理适配器。
  - 在主机的 ESXi Shell 中，要查看物理适配器列表及检查适配器状态，运行以下 ESXCLI 命令：

```
esxcli network nic list
```

每个物理适配器都以 vmnicX 的形式表示。X 是 ESXi 分配给物理适配器端口的编号。
- 2在主机的 ESXi Shell 中，运行带有 --uplink vmnicX 参数和相应选项的 pktcap-uw 命令，监控特定点的数据包，筛选捕获的数据包并将结果保存到文件。

```
pktcap-uw --uplink vmnicX [--capture capture_point|--dir 0|1] [filter_options] [--outfile pcap_file_path [--ng]] [--count number_of_packets]
```

其中方括号 [] 中所括的是 `pktcap-uw --uplink vmnicX` 命令的选项，竖线 | 表示替代值。

如果运行不带选项的 `pktcap-uw --uplink vmnicX` 命令，您将在控制台输出中获得在交换点传入标准交换机或 Distributed Switch 的数据包的内容。

- a 使用 `--capture` 选项检查另一捕获点的数据包或使用 `--dir` 选项检查另一流量方向的数据包。

pktcap-uw 命令选项	目标
<code>--capture UplinkSnd</code>	在数据包进入物理适配器设备前一刻对其进行监控。
<code>--capture UplinkRcv</code>	在数据包从物理适配器被接收到网络堆栈后立即对其进行监控。
<code>--dir 1</code>	监控离开虚拟交换机的数据包。
<code>--dir 0</code>	监控进入虚拟交换机的数据包。

- b 使用 `filter_options` 可根据源和目标地址、VLAN ID、VXLAN ID、第 3 层协议和 TCP 端口筛选数据包。

例如，要监控来自 IP 地址为 192.168.25.113 的源系统的数据包，请使用 `--srcip 192.168.25.113` 筛选选项。

- c 使用相应选项可将每个数据包的内容或部分数据包的内容保存到 `.pcap` 或 `.pcapng` 文件中。

- 要将数据包保存到 `.pcap` 文件中，请使用 `--outfile` 选项。
- 要将数据包保存到 `.pcapng` 文件中，请使用 `--ng` 和 `--outfile` 选项。

可以在 Wireshark 等网络分析器工具中打开该文件。

默认情况下，`pktcap-uw` 实用程序会将数据包文件保存到 ESXi 文件系统的根文件夹。

- d 使用 `--count` 选项可监控一定数量的数据包。

- 3 如果未使用 `--count` 选项限制数据包的数量，请按 `Ctrl+C` 停止捕获或跟踪数据包。

### 示例：捕获 vmnic0 从 IP 地址 192.168.25.113 接收的数据包

要捕获 `vmnic0` 从源系统（分配的 IP 地址为 192.168.25.113）接收的前 60 个数据包并将它们保存到名为 `vmnic0_rcv_srcip.pcap` 的文件，请运行以下 `pktcap-uw` 命令：

```
pktcap-uw --uplink vmnic0 --capture UplinkRcv --srcip 192.168.25.113 --outfile
vmnic0_rcv_srcip.pcap --count 60
```

### 下一步

如果已将数据包的内容保存到某个文件中，请将该文件从 ESXi 主机复制到运行图形分析器工具（如 Wireshark）的系统上，然后在该工具中将其打开以检查数据包详细信息。

## 为 VMXNET3 虚拟机适配器捕获数据包

使用 `pktcap-uw` 实用程序可监控虚拟交换机与 VMXNET3 虚拟机适配器之间的流量。

您可以指定虚拟交换机与虚拟机适配器之间的数据路径中的某个捕获点。还可以根据相对于交换机的流量方向以及与数据包源位置或目标位置的邻近程度来确定捕获点。有关支持的捕获点的信息，请参见第 183 页，“`pktcap-uw` 实用程序的捕获点”。

### 前提条件

确认虚拟机适配器是 VMXNET3 类型。

步骤

- 1 在主机上，使用 `esxstop` 实用程序查看虚拟机适配器的端口 ID。
  - a 在主机 ESXi Shell 中，运行 `esxstop` 启动实用程序。
  - b 按下 N 切换到实用程序的网络面板。
  - c 在 USED-BY 列中，找到虚拟机适配器，并记下它的 PORT-ID 值。  
USED-BY 字段包含虚拟机名称和虚拟机适配器连接的端口。
  - d 按下 Q 退出 `esxstop`。
- 2 在主机 ESXi Shell 中，运行 `pktcap-uw --switchport port_ID`。  
`port_ID` 是 `esxstop` 实用程序在 PORT-ID 列中显示的虚拟机适配器的 ID。
- 3 在主机 ESXi Shell 中，运行带有 `--switchport port_ID` 参数和相应选项的 `pktcap-uw` 命令，监控特定点的数据包，筛选捕获的数据包并将结果保存到文件。

```
pktcap-uw
    --switchport
    port_ID [--capture
    capture_point|--dir 0|1 --stage 0|1] [filter_options] [--outfile
pcap_file_path [--ng]] [--count
    number_of_packets]
```

其中方括号 [] 中所括的是 `pktcap-uw --switchport port_ID` 命令的选项，竖线 | 表示替代值。

如果运行不带选项的 `pktcap-uw --switchport port_ID` 命令，您将在控制台输出中获得在交换点传入标准交换机或 Distributed Switch 的数据包的内容。

- a 要检查客户机操作系统与虚拟交换机之间路径中的另一捕获点或方向上的数据包，请使用 `--capture` 选项，或者组合使用 `--dir` 和 `--stage` 选项的值。

pktcap-uw 命令选项	目标
<code>--capture Vmxnet3Tx</code>	在数据包从虚拟机传递到交换机时对其进行监控。
<code>--capture Vmxnet3Rx</code>	在数据包到达虚拟机时对其进行监控。
<code>--dir 1 --stage 0</code>	在数据包离开虚拟交换机后立即对其进行监控。
<code>--dir 1</code>	在数据包进入虚拟机前一刻对其进行监控。
<code>--dir 0 --stage 1</code>	在数据包进入虚拟交换机后立即对其进行监控。

- b 使用 `filter_options` 可根据源和目标地址、VLAN ID、VXLAN ID、第 3 层协议和 TCP 端口筛选数据包。  
例如，要监控来自 IP 地址为 192.168.25.113 的源系统的数据包，请使用 `--srcip 192.168.25.113` 筛选选项。
  - c 使用相应选项可将每个数据包的内容或部分数据包的内容保存到 `.pcap` 或 `.pcapng` 文件中。
    - 要将数据包保存到 `.pcap` 文件中，请使用 `--outfile` 选项。
    - 要将数据包保存到 `.pcapng` 文件中，请使用 `--ng` 和 `--outfile` 选项。可以在 Wireshark 等网络分析器工具中打开该文件。  
默认情况下，`pktcap-uw` 实用程序会将数据包文件保存到 ESXi 文件系统的根文件夹。
  - d 使用 `--count` 选项可监控一定数量的数据包。
- 4 如果未使用 `--count` 选项限制数据包的数量，请按 `Ctrl+C` 停止捕获或跟踪数据包。

**示例：捕获虚拟机从 IP 地址 192.168.25.113 接收的数据包**

要在来源系统（分配的 IP 地址为 192.168.25.113）的前 60 个数据包到达端口 ID 为 33554481 的虚拟机适配器时捕获这些数据包，并将它们保存到名为 `vmxnet3_rcv_srcip.pcap` 的文件，请运行以下 `pktcap-uw` 命令：

```
pktcap-uw --switchport 33554481 --capture Vmxnet3Rx --srcip 192.168.25.113 --outfile
vmxnet3_rcv_srcip.pcap --count 60
```

**下一步**

如果已将数据包的内容保存到某个文件中，请将该文件从 ESXi 主机复制到运行图形分析器工具（如 Wireshark）的系统上，然后在该工具中将其打开以检查数据包详细信息。

**为 VMkernel 适配器捕获数据包**

使用 `pktcap-uw` 实用程序可监控 VMkernel 适配器与虚拟交换机之间交换的数据包。

您可以捕获虚拟交换机与 VMkernel 适配器之间流量中的某个捕获点的数据包。还可以根据相对于交换机的流量方向以及与数据包源位置或目标位置的邻近程度来确定捕获点。有关支持的捕获点的信息，请参见第 183 页，“`pktcap-uw` 实用程序的捕获点”。

**步骤**

- 1 （可选）在 VMkernel 适配器列表中查找要监控的 VMkernel 适配器的名称。

- 在 vSphere Web Client 中，在主机的配置选项卡上展开网络，然后选择 VMkernel 适配器。
- 在主机的 ESXi Shell 中，要查看物理适配器列表，运行以下控制台命令：

```
esxcli network ip interface list
```

每个 VMkernel 适配器以 `vmkX` 的形式表示，其中 X 是 ESXi 分配给适配器的序号。

- 2 在主机的 ESXi Shell 中，运行带有 `--vmk vmkX` 参数和相应选项的 `pktcap-uw` 命令，监控特定点的数据包，筛选捕获的数据包并将结果保存到文件。

```
pktcap-uw --vmk vmkX [--capture capture_point|--dir 0|1 --stage 0|1] [filter_options]
[--outfile pcap_file_path [--ng]] [--count number_of_packets]
```

其中方括号 [] 中所括的是 `pktcap-uw --vmk vmkX` 命令的选项，竖线 | 表示替代值。

您可以将 `--vmk vmkX` 选项替换为 `--switchport vmkernel_adapter_port_ID`，其中 `vmkernel_adapter_port_ID` 是 `esxtop` 实用程序的网络面板中显示的该适配器的 PORT-ID 值。

如果运行不带选项的 `pktcap-uw --vmk vmkX` 命令，您将获得离开 VMkernel 适配器的数据包的内容。

- a 要检查特定位置和方向上传输或接收的数据包，请使用 `--capture` 选项，或者组合使用 `--dir` 和 `--stage` 选项的值。

pktcap-uw 命令选项	目标
<code>--dir 1 --stage 0</code>	在数据包离开虚拟交换机后立即对其进行监控。
<code>--dir 1</code>	在数据包进入 VMkernel 适配器前一刻对其进行监控。
<code>--dir 0 --stage 1</code>	在数据包进入虚拟交换机前一刻对其进行监控。

- b 使用 `filter_options` 可根据源和目标地址、VLAN ID、VXLAN ID、第 3 层协议和 TCP 端口筛选数据包。  
例如，要监控来自 IP 地址为 192.168.25.113 的源系统的数据包，请使用 `--srcip 192.168.25.113` 筛选选项。

- c 使用相应选项可将每个数据包的内容或部分数据包的内容保存到 `.pcap` 或 `.pcapng` 文件中。
    - 要将数据包保存到 `.pcap` 文件中，请使用 `--outfile` 选项。
    - 要将数据包保存到 `.pcapng` 文件中，请使用 `--ng` 和 `--outfile` 选项。

可以在 Wireshark 等网络分析器工具中打开该文件。

默认情况下，`pktcap-uw` 实用程序会将数据包文件保存到 ESXi 文件系统的根文件夹。
  - d 使用 `--count` 选项可监控一定数量的数据包。
- 3 如果未使用 `--count` 选项限制数据包的数量，请按 `Ctrl+C` 停止捕获或跟踪数据包。

### 下一步

如果已将数据包的内容保存到某个文件中，请将该文件从 ESXi 主机复制到运行图形分析器工具（如 Wireshark）的系统上，然后在该工具中将其打开以检查数据包详细信息。

## 捕获丢弃的数据包

通过使用 `pktcap-uw` 实用程序捕获丢弃的数据包，可对失去连接问题进行故障排除。

数据包可能会在网络流中的某个点被丢弃。导致这一问题的原因很多，例如防火墙规则、IOChain 和 DVfilter 中使用了过滤功能、VLAN 不匹配、物理适配器故障、校验和错误等等。您可以使用 `pktcap-uw` 实用程序检查丢弃数据包的位置以及丢包的原因。

### 步骤

- 1 在主机的 ESXi Shell 中，运行带有相应选项的 `pktcap-uw --capture Drop` 命令，监控特定点的数据包，筛选捕获的数据包并将结果保存到文件。

```
pktcap-uw --capture Drop [filter_options] [--outfile pcap_file_path [--ng]] [--count number_of_packets]
```

其中方括号 [] 中所括的是 `pktcap-uw --capture Drop` 命令的选项，竖线 | 表示替代值。

- a 使用 `filter_options` 可根据源和目标地址、VLAN ID、VXLAN ID、第 3 层协议和 TCP 端口筛选数据包。
 

例如，要监控来自 IP 地址为 192.168.25.113 的源系统的数据包，请使用 `--srcip 192.168.25.113` 筛选选项。
- b 使用相应选项可将每个数据包的内容或部分数据包的内容保存到 `.pcap` 或 `.pcapng` 文件中。

- 要将数据包保存到 `.pcap` 文件中，请使用 `--outfile` 选项。
- 要将数据包保存到 `.pcapng` 文件中，请使用 `--ng` 和 `--outfile` 选项。

可以在 Wireshark 等网络分析器工具中打开该文件。

默认情况下，`pktcap-uw` 实用程序会将数据包文件保存到 ESXi 文件系统的根文件夹。

---

**注意** 只有将捕获的数据包输出到控制台后，才能查看丢弃数据包的原因和位置。`pktcap-uw` 实用程序仅将数据包的内容保存到 `.pcap` 或 `.pcapng` 文件。

---

- c 使用 `--count` 选项可监控一定数量的数据包。
- 2 如果未使用 `--count` 选项限制数据包的数量，请按 `Ctrl+C` 停止捕获或跟踪数据包。

除了丢弃的数据包的内容，`pktcap-uw` 实用程序的输出内容中还显示丢包原因和网络堆栈中最后处理该数据包的功能。

## 下一步

如果已将数据包的内容保存到某个文件中，请将该文件从 ESXi 主机复制到运行图形分析器工具（如 Wireshark）的系统上，然后在该工具中将其打开以检查数据包详细信息。

## 在 DVFilter 级别捕获数据包

查看数据包在通过 vSphere Network Appliance (DVFilter) 时的变化情况。

DVFilter 是驻留在虚拟机适配器与虚拟交换机之间的流量中的一种代理。它们可以拦截数据包，以保护虚拟机免受安全攻击和避免不需要的流量。

## 步骤

- 1 （可选）要查找想要监控的 DVFilter 的名称，请在 ESXi Shell 中运行 `summarize-dvfilter` 命令。

该命令的输出内容中包含主机上部署的 DVFilter 的快速通道和慢速通道代理。

- 2 运行带有 `--dvfilter dvfilter_name` 参数和相应选项的 `pktcap-uw` 实用程序，监控特定点的数据包，筛选捕获的数据包并将结果保存到文件。

```
pktcap-uw
        --dvFilter
        dvfilter_name
        --capture PreDVFilter|PostDVFilter [filter_options] [--outfile
        pcap_file_path [--ng]] [--count
        number_of_packets]
```

其中方括号 [] 中所括的是 `pktcap-uw --dvFilter vmnicX` 命令的可选项，竖线 | 表示替代值。

- a 使用 `--capture` 选项监控 DVFilter 拦截数据包之前或之后的数据包。

pktcap-uw 命令选项	目标
<code>--capture PreDVFilter</code>	捕获进入 DVFilter 之前的数据包。
<code>--capture PostDVFilter</code>	捕获离开 DVFilter 之后的数据包。

- b 使用 `filter_options` 可根据源和目标地址、VLAN ID、VXLAN ID、第 3 层协议和 TCP 端口筛选数据包。

例如，要监控来自 IP 地址为 192.168.25.113 的源系统的数据包，请使用 `--srcip 192.168.25.113` 筛选选项。

- c 使用相应选项可将每个数据包的内容或部分数据包的内容保存到 `.pcap` 或 `.pcapng` 文件中。

- 要将数据包保存到 `.pcap` 文件中，请使用 `--outfile` 选项。

- 要将数据包保存到 `.pcapng` 文件中，请使用 `--ng` 和 `--outfile` 选项。

可以在 Wireshark 等网络分析器工具中打开该文件。

默认情况下，`pktcap-uw` 实用程序会将数据包文件保存到 ESXi 文件系统的根文件夹。

- d 使用 `--count` 选项可监控一定数量的数据包。

- 3 如果未使用 `--count` 选项限制数据包的数量，请按 `Ctrl+C` 停止捕获或跟踪数据包。

## 下一步

如果已将数据包的内容保存到某个文件中，请将该文件从 ESXi 主机复制到运行图形分析器工具（如 Wireshark）的系统上，然后在该工具中将其打开以检查数据包详细信息。

## 使用 pktcap-uw 实用程序的捕获点

当某个功能在主机上的网络堆栈中的特定位置处理数据包时，可使用 `pktcap-uw` 实用程序的捕获点来监控这些数据包。

### 捕获点概述

`pktcap-uw` 实用程序中的捕获点表示一端的虚拟交换机与另一端的物理适配器、VMkernel 适配器或虚拟机适配器之间的路径中的某个位置。

您可以将某些捕获点与适配器选项组合在一起使用。例如，捕获上行链路流量时使用 `UplinkRcv` 点。另外，可以单独处理其他点。例如，使用 `Drop` 点可检查所有丢弃的数据包。

---

**注意** `pktcap-uw` 实用程序的某些捕获点仅供 VMware 内部使用，您只有在 VMware 技术支持部门的督导下才能使用这些捕获点。*vSphere 网络连接指南*中并未介绍这些捕获点。

---

### 有关在 pktcap-uw 实用程序中使用捕获点的选项

要查看某个捕获点的数据包状态或内容，请将 `--capturecapture_point` 选项添加到 `pktcap-uw` 实用程序。

### 自动选择捕获点

对于与物理适配器、VMkernel 适配器或 VMXNET3 适配器相关的流量，通过组合使用 `--dir` 和 `--stage` 选项，可以自动选择和切换捕获点来检查数据包在某点前后的变化情况。

### pktcap-uw 实用程序的捕获点

`pktcap-uw` 实用程序支持仅在监控上行链路、VMkernel 或虚拟机流量时可以使用的捕获点，以及代表堆栈中与适配器类型无关的特殊位置的捕获点。

#### 与物理适配器流量相关的捕获点

`pktcap-uw --uplink vmnicX` 命令支持在物理适配器与虚拟交换机之间路径中的特定位置和方向上处理流量的功能对应的捕获点。

捕获点	描述
UplinkRcv	该功能接收来自物理适配器的数据包。
UplinkSnd	该功能向物理适配器发送数据包。
PortInput	该功能将来自 UplinkRcv 的一系列数据包传递至虚拟交换机上的某个端口。
PortOutput	该功能将来自虚拟交换机上某个端口的一系列数据包传递至 UplinkSnd 点。

#### 与虚拟机流量相关的捕获点

`pktcap-uw --switchport vmxnet3_port_ID` 命令支持在 VMXNET3 适配器与虚拟交换机之间路径中的特定位置和方向上处理流量数据包的功能对应的捕获点。

捕获点	描述
Vmxnet3Rx	该功能在 VMXNET3 后端接收来自虚拟交换机的数据包。
Vmxnet3Tx	该功能在 VMXNET3 后端将来自虚拟机的数据包发送至虚拟交换机。
PortOutput	该功能将来自虚拟交换机上某个端口的一系列数据包传递至 Vmxnet3Rx。
PortInput	该功能将来自 Vmxnet3Tx 的一系列数据包传递至虚拟交换机上的某个端口。这是与 VMXNET3 适配器相关的流量的默认捕获点。

### 与 VMkernel 适配器流量相关的捕获点

`pktcap-uw --vmk vmkX` 和 `pktcap-uw --switchport vmkernel_adapter_port_ID` 命令支持在 VMkernel 适配器与虚拟交换机之间路径中的特定位置和方向上处理流量的功能对应的捕获点。

捕获点	描述
PortOutput	该功能将来自虚拟交换机上某个端口的一系列数据包传递至 VMkernel 适配器。
PortInput	该功能将来自 VMkernel 适配器的一系列数据包传递至虚拟交换机上的某个端口。这是与 VMkernel 适配器相关的流量的默认捕获点。

### 与分布式虚拟筛选器相关的捕获点

`pktcap-uw --dvfilter divfilter_name` 命令需要一个捕获点来指示是在数据包进入 DVFilter 时进行捕获还是在数据包离开 DVFilter 时进行捕获。

捕获点	描述
PreDVFilter	在 DVFilter 拦截数据包之前进行捕获的点。
PostDVFilter	在 DVFilter 拦截数据包之后进行捕获的点。

### 独立捕获点

某些捕获点直接映射到网络堆栈而不是物理适配器、VMkernel 适配器或 VMXNET3 适配器。

捕获点	描述
丢弃	捕获丢弃的数据包并显示发生丢包的位置。
TcpipDispatch	当功能在虚拟交换机与 VMkernel 的 TCP/IP 堆栈之间来回分派流量时，捕获功能所在位置的数据包。
PktFree	在数据包被释放的前一刻对其进行捕获。

### 列出 pktcap-uw 实用程序的捕获点

查看 `pktcap-uw` 实用程序的所有捕获点，可找出用于对 ESXi 主机上的网络堆栈中某个位置的流量进行监控的捕获点的名称。

有关 `pktcap-uw` 实用程序的捕获点的信息，请参见第 183 页，“[pktcap-uw 实用程序的捕获点](#)”。

### 步骤

- ◆ 在主机的 ESXi Shell 中，运行 `pktcap-uw -A` 命令查看 `pktcap-uw` 实用程序支持的所有捕获点。

## 使用 pktcap-uw 实用程序跟踪数据包

使用 `pktcap-uw` 实用程序可跟踪数据包遍历网络堆栈时的路径，以进行延迟时间分析和定位数据包损坏或被丢弃时所在的点。

`pktcap-uw` 实用程序会显示数据包的路径连时间戳，时间戳记录了 ESXi 上的网络连接功能处理数据包的时间。该实用程序将在堆栈释放数据包前一刻报告数据包的路径。

要查看数据包的完整路径信息，必须将 `pktcap-uw` 实用程序的结果打印到控制台输出内容中，或将结果保存到 PCAPNG 文件。



## 步骤

- 1 在主机 ESXi Shell 中，运行带有相应选项的 `pktcap-uw --trace` 命令，可筛选跟踪的数据包、将结果保存到文件以及限制跟踪的数据包的数量。

```
pktcap-uw
           --trace [filter_options] [--outfile
           pcap_file_path [--ng]] [--count
           number_of_packets]
```

其中方括号 [] 中所括的是 `pktcap-uw --trace` 命令的可选项，竖线 | 表示替代值。

- a 使用 `filter_options` 可根据源和目标地址、VLAN ID、VXLAN ID、第 3 层协议和 TCP 端口筛选数据包。

例如，要监控来自 IP 地址为 192.168.25.113 的源系统的数据包，请使用 `--srcip 192.168.25.113` 筛选选项。

- b 使用相应选项可将每个数据包的内容或部分数据包的内容保存到 `.pcap` 或 `.pcapng` 文件中。

- 要将数据包保存到 `.pcap` 文件中，请使用 `--outfile` 选项。

- 要将数据包保存到 `.pcapng` 文件中，请使用 `--ng` 和 `--outfile` 选项。

可以在 Wireshark 等网络分析器工具中打开该文件。

默认情况下，`pktcap-uw` 实用程序会将数据包文件保存到 ESXi 文件系统的根文件夹。

---

**注意** `.pcap` 文件仅包含跟踪的数据包的内容。要收集除数据包内容以外的数据包路径，请将输出内容保存到 `.pcapng` 文件。

---

- c 使用 `--count` 选项可监控一定数量的数据包。

- 2 如果未使用 `--count` 选项限制数据包的数量，请按 `Ctrl+C` 停止捕获或跟踪数据包。

## 下一步

如果已将数据包的内容保存到某个文件中，请将该文件从 ESXi 主机复制到运行图形分析器工具（如 Wireshark）的系统上，然后在该工具中将其打开以检查数据包详细信息。

# 配置 vSphere Distributed Switch 的 NetFlow 设置

通过向 NetFlow 收集器发送报告分析流经 vSphere Distributed Switch 的虚拟机 IP 流量。

5.1 版及更高版本的 vSphere Distributed Switch 支持 IPFIX（NetFlow 版本 10）。

## 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 从操作菜单中，选择 **设置 > 编辑 Netflow**。
- 3 键入 NetFlow 收集器的 **收集器 IP 地址** 和 **收集器端口**。  
您可以通过 IPv4 或 IPv6 地址连接 NetFlow 收集器。
- 4 设置用于标识交换机相关信息的 **观察域 ID**。
- 5 要仅在一个网络设备下而不是在交换机上每个主机的单独设备下的 NetFlow 收集器中查看 Distributed Switch 的信息，请在 **交换机 IP 地址** 文本框中键入 IPv4 地址。
- 6 （可选）在 **活动流导出超时** 和 **闲置流导出超时** 文本框中，设置流启动后发送消息需等待的时间（秒）。

- 7 （可选）要更改交换机收集的数据部分，请配置**采样率**。

采样率表示 NetFlow 在每次收集数据包后丢弃的数据包数。采样率为  $x$  指示 NetFlow 按收集的数据包:丢弃的数据包比率 1: $x$  来丢弃数据包。如果比率为 0，则 NetFlow 每个数据包采样一次，即，收集一个数据包后不丢弃任何数据包。如果比率为 1，则 NetFlow 采样一个数据包，然后丢弃下一个数据包，依此类推。

- 8 （可选）要收集同一主机上虚拟机之间的网络活动中的数据，请启用**仅处理内部流**。

如果物理网络设备上启用了 NetFlow，“仅处理内部流”可避免重复发送 Distributed Switch 和物理网络设备的信息。

- 9 单击**确定**。

### 下一步

为连接到分布式端口组或端口的虚拟机的流量启用 NetFlow 报告。请参见第 95 页，“[在分布式端口组或分布式端口上启用或禁用 NetFlow 监控](#)”。

## 使用端口镜像

通过端口镜像，可将分布式端口流量镜像到其他分布式端口或特定物理交换机端口。

可在交换机上使用端口镜像将一个交换机端口（或整个 VLAN）上的一份数据包发送到另一个交换机端口上的监控连接。端口镜像用于分析和调试数据或诊断网络上的错误。

### 端口镜像版本兼容性

vSphere 5.1 及更高版本中的特定端口镜像功能取决于您使用的 vCenter Server、vSphere Distributed Switch 和主机的版本，以及您如何结合使用 vSphere 的各个方面。

**表 14-5 端口镜像兼容性**

vCenter Server 版本	vSphere Distributed Switch 版本	主机版本	vSphere 5.1 端口镜像功能
vSphere 5.1 及更高版本	vSphere 5.1 及更高版本	vSphere 5.1 及更高版本	可以使用 vSphere 5.1 端口镜像。vSphere 5.0 及早期版本未提供端口镜像功能。
vSphere 5.1 及更高版本	vSphere 5.1 及更高版本	vSphere 5.0 及早期版本	vSphere 5.0 及早期版本的主机可以添加到 vSphere 5.1 vCenter Server，但是不能添加到 Distributed Switch 版本 5.1 及更高版本。
vSphere 5.1 及更高版本	vSphere 5.0	vSphere 5.0	vSphere vCenter Server 版本 5.1 及更高版本可以在 vSphere 5.0 Distributed Switch 上配置端口镜像。
vSphere 5.1 及更高版本	vSphere 5.0	vSphere 5.1 及更高版本	运行 vSphere 5.1 的主机可以添加到 vSphere 5.0 Distributed Switch 并支持 vSphere 5.0 端口镜像。
vSphere 5.1 及更高版本	vSphere 5.0 之前的版本	vSphere 5.5 及早期版本	不支持端口镜像。
vSphere 5.0 及早期版本	vSphere 5.0 及早期版本	vSphere 5.1	vSphere 5.1 主机无法添加到 vCenter Server 5.0 及早期版本。

如果您将主机配置文件与端口镜像设置一起使用，则主机配置文件必须改写为 vSphere 5.1 及更高版本中的新端口镜像版本。

## 端口镜像互操作性

将 vSphere 端口镜像与 vSphere 的其他功能配合使用时，有一些互操作性问题需要考虑。

### vMotion

根据您选择的 vSphere 端口镜像会话类型，vMotion 的功能会有所不同。在进行 vMotion 期间，镜像路径会暂时无效，但完成 vMotion 后会还原。

**表 14-6 vMotion 与端口镜像的互操作性**

端口镜像会话类型	源和目标	可与 vMotion	功能互操作
分布式端口镜像	非上行链路分布式端口源和目标	是	分布式端口之间的端口镜像只能为本地。如果源和目标因 vMotion 而位于不同的主机上，则两者之间的镜像将不会正常工作。但是，如果源和目标移到同一主机上，则端口镜像将正常工作。
远程镜像源	非上行链路分布式端口源	是	将源分布式端口从主机 A 移到主机 B 时，会在主机 A 上删除从源端口到主机 A 的上行链路的原始镜像路径，并在主机 B 上创建从源端口到主机 B 的上行链路的新镜像路径。通过在会话中指定的上行链路名称确定使用哪一个上行链路。
	上行链路端口目标	否	无法通过 vMotion 移动上行链路。
远程镜像目标	VLAN 源	否	
	非上行链路分布式端口目标	是	将目标分布式端口从主机 A 移到主机 B 时，从源 VLAN 到目标端口的所有原始镜像路径都将从 A 移到 B。
已封装远程镜像 (L3) 源	非上行链路分布式端口源	是	将源分布式端口从主机 A 移到主机 B 时，从源端口到目标 IP 的所有原始镜像路径都将从 A 移到 B。
	IP 目标	否	
分布式端口镜像 (传统)	IP 源	否	
	非上行链路分布式端口目标	否	将目标分布式端口从主机 A 移到主机 B 时，从源 IP 到目标端口的所有原始镜像路径都将无效，因为端口镜像会话源在 A 上仍可以看到目标。

### TSO 和 LRO

TCP 分段卸载 (TSO) 和大型接收卸载 (LRO) 可能会导致正在镜像的数据包数量与已镜像数据包数量不相等。

在 vNIC 上启用 TSO 后，vNIC 可能会向 Distributed Switch 发送大数据包。在 vNIC 上启用 LRO 后，发送到 vNIC 的小数据包可能会合并成大数据包。

源	目标	描述
TSO	LRO	来自源 vNIC 的数据包可能是大数据包，是否对其进行拆分取决于其大小是否超过目标 vNIC LRO 限制。
TSO	任意目标	来自源 vNIC 的数据包可能是大数据包，在目标 vNIC 中会将其拆分成标准数据包。
任意源	LRO	来自源 vNIC 的数据包是标准数据包，在目标 vNIC 中可能会将其合并成大数据包。

## 创建端口镜像会话

使用 vSphere Web Client 创建端口镜像会话，将 vSphere Distributed Switch 流量镜像到端口、上行链路和远程 IP 地址。

### 前提条件

验证 vSphere Distributed Switch 的版本是否为 5.0.0 或更高的版本。

### 步骤

- 1 [选择端口镜像会话类型](#)第 188 页，  
要开始端口镜像会话，必须指定端口镜像会话的类型。
- 2 [指定端口镜像名称和会话详细信息](#)第 189 页，  
要继续创建端口镜像会话，请指定新端口镜像会话的名称、说明和会话详细信息。
- 3 [选择端口镜像源](#)第 189 页，  
要继续创建端口镜像会话，请为新端口镜像会话选择源和流量方向。
- 4 [选择端口镜像目标并验证设置](#)第 189 页，  
要完成端口镜像会话的创建，请选择端口或上行链路作为端口镜像会话的目标。

## 选择端口镜像会话类型

要开始端口镜像会话，必须指定端口镜像会话的类型。

### 步骤

- 1 在 vSphere Web Client 导航器中，浏览到分布式交换机。
- 2 单击 **配置** 选项卡并展开 **设置**。
- 3 选择 **端口镜像** 选项并单击 **新建**。
- 4 选择端口镜像会话的会话类型。

选项	描述
<b>分布式端口镜像</b>	将数据包从多个分布式端口镜像到同一主机上的其他分布式端口。如果源和目标在不同主机上，则该会话类型不起作用。
<b>远程镜像源</b>	将数据包从多个分布式端口镜像到相应主机上的特定上行链路端口。
<b>远程镜像目标</b>	将数据包从大量 VLAN 镜像到分布式端口。
<b>已封装远程镜像 (L3) 源</b>	将数据包从多个分布式端口镜像到 远程代理的 IP 地址。虚拟机的流量会通过 IP 通道镜像到远程物理目标。
<b>分布式端口镜像 (传统)</b>	将数据包从多个分布式端口镜像到相应主机上的多个分布式端口和/或上行链路端口。

- 5 单击 **下一步**。

指定端口镜像名称和会话详细信息

要继续创建端口镜像会话，请指定新端口镜像会话的名称、说明和会话详细信息。

步骤

- 1 设置会话属性。根据选择的会话类型，会有不同的选项可供配置。

选项	描述
名称	您可为端口镜像会话输入唯一名称，也可接受自动生成的会话名称。
状态	使用下拉菜单启用或禁用会话。
会话类型	显示您选择的会话的类型。
目标端口上的正常 I/O	使用下拉菜单允许或禁止目标端口上的正常 I/O。只有编辑上行链路和分布式端口目标时，才会提供该属性。 如果不允许此选项，将允许镜像流量在目标端口上流出，而不允许任何流量流入。
镜像数据包长度 (字节)	使用该复选框可启用以字节为单位的镜像数据包长度。这会限制镜像帧的大小。如果选择了此选项，则所有镜像帧都将被截断为指定的长度。
采样率	选择对数据包采样的速度。默认情况下，会为除传统会话之外的所有端口镜像会话启用该选项。
描述	您可输入端口镜像会话配置的描述。

- 2 单击下一步。

选择端口镜像源

要继续创建端口镜像会话，请为新端口镜像会话选择源和流量方向。

您可在未设置源和目标的情况下创建端口镜像会话。如果未设置源和目标，则创建的端口镜像会话没有镜像路径。这样一来，您便可创建属性集正确的端口镜像会话。设置属性后，您可编辑端口镜像会话来添加源和目标信息。

步骤

- 1 选择要镜像的流量源和流量方向。

根据所选端口镜像会话的类型，会提供不同的配置选项。

选项	描述
从列表中添加现有端口	单击 <b>选择分布式端口</b> 。此时将打开一个对话框，其中显示了现有端口列表。选中分布式端口旁边的复选框，然后单击 <b>确定</b> 。您可选择多个分布式端口。
按端口号添加现有端口	单击 <b>添加分布式端口</b> ，输入端口号，然后单击 <b>确定</b> 。
设置流量方向	添加端口后，在列表中选择端口，然后单击“输入”、“输出”或“输入/输出”按钮。您的选择会显示在“流量方向”列中。
指定源 VLAN	如果选择了远程镜像目标会话类型，则必须指定源 VLAN。单击 <b>添加添加 VLAN ID</b> 。编辑 ID - 使用上下箭头，或在字段中单击来手动输入 VLAN ID。

- 2 单击下一步。

选择端口镜像目标并验证设置

要完成端口镜像会话的创建，请选择端口或上行链路作为端口镜像会话的目标。

您可在未设置源和目标的情况下创建端口镜像会话。如果未设置源和目标，则创建的端口镜像会话没有镜像路径。这样一来，您便可创建属性集正确的端口镜像会话。设置属性后，您可编辑端口镜像会话来添加源和目标信息。

根据 VLAN 转发策略对端口镜像进行检查。如果原始帧的 VLAN 不等于目标端口或由目标端口中继，则不镜像这些帧。

### 步骤

- 1 选择端口镜像会话的目标。

根据所选会话的类型，会提供不同的选项。

选项	描述
<b>选择目标分布式端口</b>	单击 <b>选择分布式端口</b> 从列表中选择端口，或单击 <b>添加分布式端口</b> 按端口号添加端口。您可添加多个分布式端口。
<b>选择上行链路</b>	从列表中选择现有上行链路，然后单击 <b>添加</b> 将上行链路添加到端口镜像会话中。您可选择多条上行链路。
<b>选择端口或上行链路</b>	单击 <b>选择分布式端口</b> 从列表中选择端口，或单击 <b>添加分布式端口</b> 按端口号添加端口。您可添加多个分布式端口。 单击 <b>添加上行链路</b> 添加上行链路作为目标。从列表中选择上行链路，然后单击 <b>确定</b> 。
<b>指定 IP 地址</b>	单击 <b>添加</b> 。新列表条目即已创建。选择该条目，然后单击 <b>编辑</b> 输入 IP 地址，或直接在“IP 地址”字段中单击来键入 IP 地址。如果 IP 地址无效，会显示一条警告。

- 2 单击**下一步**。
- 3 在**即将完成**页面上，检查为端口镜像会话输入的信息。
- 4 （可选）使用**上一步**按钮编辑信息。
- 5 单击**完成**。

新端口镜像会话即会显示在**设置**选项卡的“端口镜像”部分中。

## 查看端口镜像会话详细信息

查看端口镜像会话详细信息，包括状态、源和目标。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在**配置**选项卡上，展开**设置**，并单击**端口镜像**。
- 3 从列表中选择端口镜像会话，以在屏幕底部显示更多详细信息。使用选项卡可以查看配置详细信息。
- 4 （可选）单击**新建**以添加新的端口镜像会话。
- 5 （可选）单击**编辑**编辑所选端口镜像会话的详细信息。
- 6 （可选）单击**移除**移除所选端口镜像会话。

## 编辑端口镜像会话详细信息、源和目标

编辑端口镜像会话的详细信息（包括名称、描述和状态）、源和目标。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在**配置**选项卡上，展开**设置**，并单击**端口镜像**。
- 3 从列表中选择端口镜像会话，然后单击**编辑**。

4 在**属性**页面上，编辑会话属性。

根据所编辑端口镜像会话的类型，会提供不同的配置选项。

选项	描述
<b>名称</b>	您可为端口镜像会话输入唯一名称，也可接受自动生成的会话名称。
<b>状态</b>	使用下拉菜单启用或禁用会话。
<b>目标端口上的正常 I/O</b>	使用下拉菜单允许或禁止目标端口上的正常 I/O。只有编辑上行链路和分布式端口目标时，才会提供该属性。 如果未选择此选项，将只允许镜像流量在目标端口上流出，而不允许任何流量流入。
<b>封装 VLAN ID</b>	在字段中输入有效的 VLAN ID。对于远程镜像源端口镜像会话，必须输入该信息。 选中 <b>保留原始 VLAN</b> 旁边的复选框，创建在目标端口封装所有帧的 VLAN ID。如果原始帧中包含 VLAN 并且未选择“保留原始 VLAN”，则封装 VLAN 会替换原始 VLAN。
<b>镜像数据包长度 (字节)</b>	使用该复选框可启用以字节为单位的镜像数据包长度。这会限制镜像帧的大小。如果选择了此选项，则所有镜像帧都将被截断为指定的长度。
<b>描述</b>	您可输入端口镜像会话配置的描述。

5 在**源**页面上，编辑端口镜像会话的源。

根据所编辑端口镜像会话的类型，会提供不同的配置选项。

选项	描述
<b>从列表中添加现有端口</b>	单击 <b>选择分布式端口...</b> 按钮。此时将打开一个对话框，其中显示了现有端口列表。选中分布式端口旁边的复选框，然后单击 <b>确定</b> 。您可选择多个分布式端口。
<b>按端口号添加现有端口</b>	单击 <b>添加分布式端口...</b> 按钮，输入端口号，然后单击 <b>确定</b> 。
<b>设置流量方向</b>	添加端口后，在列表中选择端口，然后单击“输入”、“输出”或“输入/输出”按钮。您的选择会显示在“流量方向”列中。
<b>指定源 VLAN</b>	如果选择了远程镜像目标会话类型，则必须指定源 VLAN。单击 <b>添加</b> 按钮添加 VLAN ID。编辑 ID - 使用上下箭头，或在字段中单击来手动输入 VLAN ID。

6 在**目标**部分中，编辑端口镜像会话的目标。

根据所编辑端口镜像会话的类型，会提供不同的配置选项。

选项	描述
<b>选择目标分布式端口</b>	单击 <b>选择分布式端口...</b> 按钮从列表中选择端口，或单击 <b>添加分布式端口...</b> 按钮按端口号添加端口。您可添加多个分布式端口。
<b>选择上行链路</b>	从列表中选择现有上行链路，然后单击 <b>添加 &gt;</b> 将上行链路添加到端口镜像会话中。您可选择多条上行链路。
<b>选择端口或上行链路</b>	单击 <b>选择分布式端口...</b> 按钮从列表中选择端口，或单击 <b>添加分布式端口...</b> 按钮按端口号添加端口。您可添加多个分布式端口。 单击 <b>添加上行链路...</b> 按钮添加上行链路作为目标。从列表中选择上行链路，然后单击 <b>确定</b> 。
<b>指定 IP 地址</b>	单击 <b>添加</b> 按钮。新列表条目即已创建。选择该条目，然后单击“编辑”按钮输入 IP 地址，或直接在“IP 地址”字段中单击来输入 IP 地址。如果 IP 地址无效，将打开一个警告对话框。

7 单击**确定**。

## vSphere Distributed Switch 运行状况检查

vSphere Distributed Switch 5.1 及更高版本中支持的运行状况检查有助于标识 vSphere Distributed Switch 中的配置错误并进行故障排除。

vSphere 会运行定期运行状况检查以检查分布式和物理交换机上的某些设置，从而标识网络连接配置中的常见错误。两次运行状况检查之间的默认时间间隔为 1 分钟。

配置错误	运行状况检查	Distributed Switch 上的所需配置
Distributed Switch 上配置的 VLAN 中继范围与物理交换机上的中继范围不匹配。	检查 Distributed Switch 上的 VLAN 设置是否与已连接的物理交换机端口上的中继端口配置匹配。	至少两个活动的物理网卡
物理网络适配器、Distributed Switch 和物理交换机端口上的 MTU 设置不匹配。	检查基于每一 VLAN 的物理接入交换机端口 MTU 巨帧设置是否与 vSphere Distributed Switch MTU 设置匹配。	至少两个活动的物理网卡
端口组上配置的绑定策略与物理交换机端口通道上的策略不匹配。	检查加入以太通道的物理交换机的已连接访问端口是否与绑定策略为 IP 哈希的分布式端口配对。	至少两个活动的物理网卡和两台主机

运行状况检查仅限于 Distributed Switch 上行链路连接的接入交换机端口。

## 启用或禁用 vSphere Distributed Switch 健康状况检查

运行状况检查可监控 vSphere Distributed Switch 配置更改。您必须启用 vSphere Distributed Switch 运行状况检查，才能在 Distributed Switch 配置中执行检查。

### 前提条件

确认 vSphere Distributed Switch 为 5.1 或更高版本。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 从操作菜单中，选择 **设置 > 编辑运行状况检查**。
- 3 使用下拉菜单启用或禁用健康状况检查选项。

选项	描述
<b>VLAN 和 MTU</b>	报告分布式上行链路端口状态和 VLAN 范围。
<b>绑定和故障切换</b>	检查在成组策略中使用的 ESXi 主机和物理交换机之间是否存在任何配置不匹配。

- 4 单击 **确定**。

### 下一步

当更改 vSphere Distributed Switch 的配置时，您可以在 vSphere Web Client 中的 **监控** 选项卡中查看关于更改的信息。请参见第 193 页，[“查看 vSphere Distributed Switch 健康状况”](#)。



### 查看 vSphere Distributed Switch 健康状况

在 vSphere Distributed Switch 上启用健康状况检查后，可以在 vSphere Web Client 中查看连接的主机的网络健康状况。

**前提条件**

验证 vSphere Distributed Switch 上 VLAN 和 MTU 以及成组策略的健康状况检查是否已启用。请参见第 192 页，“启用或禁用 vSphere Distributed Switch 健康状况检查”。

**步骤**

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 在 **监控** 选项卡上，单击 **运行状况**。
- 3 在“健康状况详细信息”部分中，查看连接到交换机的主机的整体状况、VLAN、MTU 以及成组运行状况。

### 交换机发现协议

交换机发现协议帮助 vSphere 管理员确定连接到 vSphere 标准交换机或 vSphere Distributed Switch 的物理交换机端口。

vSphere 5.0 及更高版本支持 Cisco 发现协议 (CDP) 和链路层发现协议 (LLDP)。CDP 对于连接到 Cisco 物理交换机的 vSphere 标准交换机和 vSphere Distributed Switch 可用。LLDP 对于版本 5.0.0 及更高版本的 vSphere Distributed Switch 可用。

当特定 vSphere Distributed Switch 或 vSphere 标准交换机启用了 CDP 或 LLDP 时，可以通过 vSphere Web Client 查看同级物理交换机的属性（如设备 ID、软件版本和超时）。

### 在 vSphere Distributed Switch 上启用 Cisco 发现协议

通过 Cisco 发现协议 (CDP)，vSphere 管理员可以确定物理 Cisco 交换机上连接到 vSphere 标准交换机或 vSphere Distributed Switch 的端口。如果为 vSphere Distributed Switch 启用了 CDP，则可以查看 Cisco 交换机的属性（例如，设备 ID、软件版本和超时）。

**步骤**

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 从 **操作** 菜单中，选择 **设置 > 编辑设置**。
- 3 在“编辑设置”对话框中，单击 **高级**。
- 4 在“发现协议”部分中，从 **类型** 下拉菜单中选择 **Cisco 发现协议**。
- 5 从 **操作** 下拉菜单中，选择连接到该交换机的 ESXi 主机的操作模式。

选项	描述
侦听	ESXi 检测并显示与关联 Cisco 交换机端口相关的信息，但并不向 Cisco 交换机管理员提供有关 vSphere Distributed Switch 的信息。
通知	ESXi 将有关 vSphere Distributed Switch 的信息提供给 Cisco 交换机管理员，但不检测和显示 Cisco 交换机的相关信息。
二者	ESXi 检测并显示与关联 Cisco 交换机相关的信息，并向 Cisco 交换机管理员提供有关 vSphere Distributed Switch 的信息。

- 6 单击 **确定**。

## 在 vSphere Distributed Switch 上启用链路层发现协议

通过链路层发现协议 (LLDP)，vSphere 管理员可以确定连接到给定 vSphere Distributed Switch 的物理交换机端口。为特定分布式交换机启用了 LLDP 时，您可通过 vSphere Web Client 查看物理交换机的属性（例如机箱 ID、系统名称和描述以及设备功能）。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 从操作菜单中，选择**设置 > 编辑设置**。
- 3 在“编辑设置”对话框中，单击**高级**。
- 4 在“发现协议”部分中，从**类型**下拉菜单中选择**链路层发现协议**。
- 5 从操作下拉菜单中，选择连接到该交换机的 ESXi 主机的操作模式。

操作	描述
<b>侦听</b>	ESXi 检测并显示与关联物理交换机端口相关的信息，但不向交换机管理员提供有关 vSphere Distributed Switch 的信息。
<b>通知</b>	ESXi 将有关 vSphere Distributed Switch 的信息提供给交换机管理员，但不检测和显示物理交换机的相关信息。
<b>二者</b>	ESXi 检测并显示与关联物理交换机相关的信息，并向交换机管理员提供有关 vSphere Distributed Switch 的信息。

- 6 单击**确定**。

## 查看交换机信息

当 Distributed Switch 上的 Cisco 发现协议 (CDP) 或链路层发现协议 (LLDP) 已启用且连接到交换机的主机处于“侦听”或“二者”操作模式时，可以从 vSphere Web Client 查看物理交换机信息。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在**配置**选项卡上，展开**网络**，然后单击**物理适配器**。
- 3 从列表选择一个物理适配器以查看其详细信息。

根据已启用的交换机发现协议，交换机的属性将显示在 **CDP** 或 **LLDP** 选项卡下。如果在网络中提供了相关信息，则可以在对等设备功能下查看交换机的系统功能。

## 配置用于虚拟机网络连接的协议配置文件

网络协议配置文件中包含 vCenter Server 分配给 vApp 或具有 vApp 功能的虚拟机的 IPv4 和 IPv6 地址的池，这些地址连接到与配置文件关联的端口组。

网络协议配置文件中还包含 IP 子网、DNS 和 HTTP 代理服务器的设置。

要使用网络协议配置文件配置虚拟机的网络连接设置，请执行以下操作：

- 在数据中心级别或 vSphere Distributed Switch 级别创建网络配置文件。
- 将协议配置文件与 vApp 虚拟机的端口组相关联。
- 从 vApp 的设置或虚拟机的 vApp 选项中启用暂时或静态 IP 分配策略。

---

**注意** 在将从协议配置文件中检索网络设置的 vApp 或虚拟机移至另一个数据中心时，若要开机，则必须在目标数据中心为已连接的端口组分配一个协议配置文件。

---

- [添加网络协议配置文件](#) 第 195 页，  
网络协议配置文件包含 IPv4 和 IPv6 地址池。vCenter Server 可将这些资源分配给 vApp 或具有 vApp 功能的虚拟机，这些 vApp 或虚拟机会连接到与该配置文件关联的端口组。
- [将端口组与网络协议配置文件关联](#) 第 197 页，  
要将网络协议配置文件中的 IP 地址范围应用到属于 vApp 或启用了 vApp 功能的虚拟机，可将配置文件与控制虚拟机网络的端口组关联。
- [配置虚拟机或 vApp 以使用网络协议配置文件](#) 第 198 页，  
在将协议配置文件与标准交换机或 Distributed Switch 的端口组关联后，能够在连接到该端口组并且与 vApp 关联或已启用 vApp 选项的虚拟机上使用配置文件。

### 添加网络协议配置文件

网络协议配置文件包含 IPv4 和 IPv6 地址池。vCenter Server 可将这些资源分配给 vApp 或具有 vApp 功能的虚拟机，这些 vApp 或虚拟机会连接到与该配置文件关联的端口组。

网络协议配置文件中还包含 IP 子网、DNS 和 HTTP 代理服务器的设置。

---

**注意** 将从协议配置文件中检索网络设置的 vApp 或虚拟机移动到另一个数据中心时，若要打开该 vApp 或虚拟机的电源，则必须为目标数据中心上的已连接端口组分配协议配置文件。

---

#### 步骤

- 1 导航到与 vApp 关联的数据中心，然后单击**配置**选项卡。

## 2 单击网络协议配置文件

将列出现有网络协议配置文件。

## 3 单击“添加”图标 (+) 以添加新网络协议配置文件。

## 选择网络协议配置文件的名称和网络

为网络协议配置文件命名，然后选择应使用它的网络。

### 步骤

#### 1 键入网络协议配置文件的名称。

#### 2 选择使用该网络协议配置文件的网络。

网络一次可与一个网络协议配置文件关联。

#### 3 单击 下一步。

## 指定网络协议配置文件中的 IPv4 配置

网络协议配置文件包含可供 vApps 使用的 IPv4 和 IPv6 地址池。创建网络协议配置文件时，可以设置其 IPv4 配置。

可以为 IPv4、IPv6 或这两者配置网络协议配置文件范围。如果将 vApp 设置为使用暂时 IP 分配，则 vCenter Server 将使用这些范围为虚拟机动态分配 IP 地址。

### 步骤

#### 1 在其相应字段中输入 IP 子网和网关。

#### 2 选择 DHCP 存在以指示 DHCP 服务器在此网络中可用。

#### 3 输入 DNS 服务器信息。

用以逗号、分号或空格分隔的 IP 地址指定服务器。

#### 4 选中启用 IP 池复选框以指定 IP 池范围。

#### 5 如果启用 IP 池，请在 IP 池范围字段中输入逗号分隔的主机地址范围列表。

范围由 IP 地址、井字号 (#) 和指定范围长度的数字组成。

网关和范围必须位于子网内。在 IP 池范围字段中输入的范围不能包含网关地址。

例如，**10.20.60.4#10**，**10.20.61.0#2** 表示 IPv4 地址的范围可以从 10.20.60.4 到 10.20.60.13 和从 10.20.61.0 到 10.20.61.1。

#### 6 单击 下一步。

## 指定网络协议配置文件的 IPv6 配置

网络协议配置文件包含可供 vApps 使用的 IPv4 和 IPv6 地址池。创建网络协议配置文件时，可以设置其 IPv6 配置。

可以为 IPv4、IPv6 或这两者配置网络协议配置文件范围。如果将 vApp 设置为使用暂时 IP 分配，则 vCenter Server 将使用这些范围为虚拟机动态分配 IP 地址。

### 步骤

#### 1 在其相应字段中输入 IP 子网和网关。

#### 2 选择 DHCP 存在以指示 DHCP 服务器在此网络中可用。

- 3 输入 DNS 服务器信息。  
用以逗号、分号或空格分隔的 IP 地址指定服务器。
- 4 选中**启用 IP 池**复选框以指定 IP 池范围。
- 5 如果启用 IP 池，请在 **IP 池范围** 字段中输入逗号分隔的主机地址范围列表。  
范围由 IP 地址、井字号 (#) 和指定范围长度的数字组成。例如，假定您指定以下 IP 池范围：  
`fe80:0:0:0:2bff:fe59:5a:2b#10,fe80:0:0:0:2bff:fe59:5f:b1#2`  
则地址位于以下范围中：  
`fe80:0:0:0:2bff:fe59:5a:2b - fe80:0:0:0:2bff:fe59:5a:34`  
和  
`fe80:0:0:0:2bff:fe59:5f:b1 - fe80:0:0:0:2bff:fe59:5f:b2`  
网关和范围必须位于子网内。在 **IP 池范围** 字段中输入的范围不能包含网关地址。
- 6 单击 **下一步**。

## 指定网络协议配置文件的 DNS 和其他配置

创建网络协议配置文件时，可以指定 DNS 域、DNS 搜索路径、主机前缀和 HTTP 代理。

### 步骤

- 1 输入 DNS 域。
- 2 输入主机前缀。
- 3 输入 DNS 搜索路径。  
搜索路径被指定为以逗号、分号或空格分隔的 DNS 域的列表。
- 4 输入代理服务器的服务器名称和端口号。  
服务器名称可以包含冒号和端口号。  
例如，`web-proxy:3912` 是有效的代理服务器。
- 5 单击 **下一步**。

## 完成网络协议配置文件的创建

### 步骤

- ◆ 检查设置，然后单击**完成**完成添加网络协议配置文件。

## 将端口组与网络协议配置文件关联

要将网络协议配置文件中的 IP 地址范围应用到属于 vApp 或启用了 vApp 功能的虚拟机，可将配置文件与控制虚拟机网络的端口组关联。

可以使用相应端口组的设置将标准交换机的端口组或 Distributed Switch 的分布式端口组与网络协议配置文件关联。

**步骤**

- 1 在 vSphere Web Client 的“网络”视图中，导航到 vSphere Distributed Switch 的分布式端口组或 vSphere 标准交换机的端口组。  
标准交换机的端口组在数据中心的下面。vSphere Web Client 在父 Distributed Switch 对象的下面显示分布式端口组。
- 2 在配置选项卡上，展开**更多**，然后单击**网络协议配置文件**。
- 3 单击右上角的**将网络协议配置文件与选定的网络关联**按钮。
- 4 在关联网络协议配置文件向导的“设置关联类型”页面上，选择**使用现有网络协议配置文件**，然后单击**下一步**。  
如果现有网络协议配置文件不包含适合端口组中的 vApp 虚拟机的设置，则必须创建新的配置文件。
- 5 选择网络协议配置文件，然后单击**下一步**。
- 6 检查网络协议配置文件的关联和设置，然后单击**完成**。

**配置虚拟机或 vApp 以使用网络协议配置文件**

在将协议配置文件与标准交换机或 Distributed Switch 的端口组关联后，能够在连接到该端口组并且与 vApp 关联或已启用 vApp 选项的虚拟机上使用配置文件。

**前提条件**

确认虚拟机已连接到与网络协议配置文件关联的端口组。

**步骤**

- 1 在 vSphere Web Client 中，导航到虚拟机或 vApp。
- 2 打开 vApp 的设置或虚拟机的 **vApp 选项** 选项卡。
  - 右键单击某个 vApp，然后选择**编辑设置**。
  - 右键单击某个虚拟机，选择**编辑设置**，然后在“编辑设置”对话框中，单击 **vApp 选项** 选项卡。
- 3 单击**启用 vApp 选项**。
- 4 在“编写”下，展开 **IP 分配**，并将 IP 分配方案设置为 **OVF 环境**。
- 5 在“部署”下，展开 **IP 分配** 并将 IP 分配设置为 **暂时 - IP 池** 或 **静态 - IP 池**。  
**静态 - IP 池** 和 **暂时 - IP 池** 选项都会从与端口组关联的网络协议配置文件中的范围内分配 IP 地址。如果选择 **静态 - IP 池**，则会在首次打开虚拟机或 vApp 的电源时分配 IP 地址，并且该地址不受重新启动的影响。如果选择 **暂时 - IP 池**，则在每次打开虚拟机或 vApp 的电源时分配 IP 地址。
- 6 单击**确定**。

打开虚拟机电源后，连接到端口组的适配器将接收协议配置文件中指定范围内的 IP 地址。关闭虚拟机电源后，将释放 IP 地址。

## 多播筛选

在 vSphere 6.0 及更高版本中，vSphere Distributed Switch 支持与单个多播组相关的多播数据包筛选的基本和侦听模式。根据交换机上虚拟机订阅的多播组数量选择模式。

- [多播筛选模式](#)第 199 页，  
除了用于筛选多播流量的默认基本模式外，vSphere Distributed Switch 6.0.0 及更高版本还支持多播侦听。多播侦听可以根据虚拟机中的 Internet 组管理协议 (IGMP) 和多播侦听器发现 (MLD) 消息以更精确的方式转发多播流量。
- [在 vSphere Distributed Switch 上启用多播侦听](#)第 200 页，  
使用 vSphere Distributed Switch 上的多播侦听，根据虚拟机发送以订阅多播流量的 Internet 组管理协议 (IGMP) 或多播侦听器发现 (MLD) 成员资格信息以精确的方式转发流量。
- [编辑多播侦听的查询时间间隔](#)第 200 页，  
如果已在 vSphere Distributed Switch 6.0 上启用 IGMP 或 MLD 多播侦听，则交换机会发送有关虚拟机成员资格的常规查询，以防未在物理交换机上配置侦听查询器。在已连接到 Distributed Switch 的 ESXi 6.0 主机上，可以编辑交换机发送常规查询的时间间隔。
- [编辑 IGMP 和 MLD 的源 IP 地址数量](#)第 200 页，  
在 vSphere Distributed Switch 6.0 上启用 IGMP 或 MLD 多播侦听时，可以编辑多播组成员从中接收数据包的最大 IP 源数。

### 多播筛选模式

除了用于筛选多播流量的默认基本模式外，vSphere Distributed Switch 6.0.0 及更高版本还支持多播侦听。多播侦听可以根据虚拟机中的 Internet 组管理协议 (IGMP) 和多播侦听器发现 (MLD) 消息以更精确的方式转发多播流量。

### 基本多播筛选

在基本多播筛选模式下，vSphere Standard Switch 或 vSphere Distributed Switch 根据多播组的目标 MAC 地址转发虚拟机的多播流量。加入多播组时，客户机操作系统会通过交换机将该组的多播 MAC 地址向下推送到网络。交换机会将端口和目标多播 MAC 地址之间的映射保存在本地转发表中。

交换机不会解释虚拟机发送以加入或离开组的 IGMP 消息。交换机会将这些消息直接发送至本地多播路由器，后者随后会解释这些消息以加入虚拟机或将虚拟机从组中移除。

基本模式具有以下限制：

- 虚拟机可能会从未订阅的组中接收数据包，因为交换机会根据多播组的目标 MAC 地址转发数据包，这可能会映射到多达 32 个 IP 多播组。
- 从超过 32 个多播 MAC 地址订阅流量的虚拟机会由于转发模式限制而接收未订阅的数据包。

- 交换机不会根据 IGMP 版本 3 中定义的源地址筛选数据包。

## 多播侦听

在多播侦听模式下，vSphere Distributed Switch 按照 RFC 4541 提供 IGMP 和 MLD 侦听。通过使用 IP 地址，交换机可以更精确地分派多播流量。此模式支持 IGMPv1、IGMPv2 和 IGMPv3（对于 IPv4 多播组地址）以及 MLDv1 和 MLDv2（对于 IPv6 多播组地址）。

交换机可动态检测虚拟机的成员资格。虚拟机通过交换机端口发送包含 IGMP 或 MLD 成员资格信息的数据包时，交换机会创建一条组目标 IP 地址的记录；如果是 IGMPv3，则会创建一条虚拟机首选从中接收流量的源 IP 地址的记录。如果虚拟机在某段时间内不续订某个组的成员资格，则交换机会从查找记录中移除该组的条目。

在 Distributed Switch 的多播侦听模式下，虚拟机在单个交换机端口上最多可接收 256 个组和 10 个源的多播流量。

## 在 vSphere Distributed Switch 上启用多播侦听

使用 vSphere Distributed Switch 上的多播侦听，根据虚拟机发送以订阅多播流量的 Internet 组管理协议 (IGMP) 或多播侦听器发现 (MLD) 成员资格信息以精确的方式转发流量。

如果交换机上的虚拟化工作负载订阅超过 32 个多播组或必须从特定源节点接收流量，请使用多播侦听。有关 vSphere Distributed Switch 的多播筛选模式的信息，请参见第 199 页，“多播筛选模式”。

### 前提条件

确认 vSphere Distributed Switch 为 6.0.0 及更高版本。

### 步骤

- 1 在 vSphere Web Client 中，导航到 Distributed Switch。
- 2 从操作菜单中，选择设置 > 编辑设置。
- 3 在显示交换机设置的对话框中，单击高级。
- 4 在多播筛选模式下拉菜单中，选择 IGMP/MLD 侦听，然后单击确定。

多播侦听在 ESXi 6.0 及更高版本的主机上处于活动状态。

## 编辑多播侦听的查询时间间隔

如果已在 vSphere Distributed Switch 6.0 上启用 IGMP 或 MLD 多播侦听，则交换机会发送有关虚拟机成员资格的常规查询，以防未在物理交换机上配置侦听查询器。在已连接到 Distributed Switch 的 ESXi 6.0 主机上，可以编辑交换机发送常规查询的时间间隔。

发送侦听查询的默认时间间隔为 125 秒。

### 步骤

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在配置选项卡上，展开系统，然后选择高级系统设置。
- 3 找到 Net.IGMPQueryInterval 系统设置。
- 4 单击编辑，然后为该设置输入新值（以秒为单位）。

## 编辑 IGMP 和 MLD 的源 IP 地址数量

在 vSphere Distributed Switch 6.0 上启用 IGMP 或 MLD 多播侦听时，可以编辑多播组成员从中接收数据包的最大 IP 源数。



**步骤**

- 1 在 vSphere Web Client 中，导航到主机。
- 2 在**配置**选项卡上，展开**系统**，然后选择**高级系统设置**。
- 3 要编辑源 IP 地址的数量，请找到 **Net.IGMPV3MaxSrcIPNum** 或 **Net.MLDV2MaxSrcIPNum** 系统设置。
- 4 单击**编辑**，然后为该设置输入一个介于 1 和 32 之间的新值。
- 5 单击**确定**。



## 无状态网络部署

无状态是一种执行模式，适用于不具有以前本应保存配置或状态的本地存储的 ESXi 主机。配置抽象化至主机配置文件中，作为适用于某类别计算机的模板。无状态允许轻松替换、移除和添加故障硬件，从而简化扩展硬件部署。

每个无状态 ESXi 引导都像是第一次引导。ESXi 主机借助内置标准交换机实现与 vCenter Server 的网络连接，从而进行引导。如果主机配置文件指定了分布式交换机成员资格，那么 vCenter Server 会将 ESXi 主机加入 VMware 分布式交换机或第三方交换机解决方案。

当计划无状态 ESXi 主机的网络设置时，您应该尽可能地保持配置的通用性，并避免特定于主机的项目。当部署新主机时，目前设计未涉及重新配置物理交换机。任何此类要求都需要特殊处理。

要设置无状态部署，必须采用标准方式安装一台 ESXi 主机。然后，查找并记录以下网络相关信息，以保存到主机配置文件中：

- vSphere 标准交换机实例和设置（端口组、上行链路、MTU，等等）
- 分布式交换机实例（VMware 和第三方）
- 针对上行链路和上行链路端口或端口组的选择规则
- vNIC 信息：
  - 地址信息（IPv4 或 IPv6、静态或 DHCP、网关）
  - 分配给物理网络适配器的端口组和分布式端口组 (vmknics)
  - 如果有分布式交换机，请记录 VLAN、绑定到 vmknics 的物理网卡和以太通道（如果已配置）

记录的信息将用作主机配置文件的模板。主机配置文件虚拟交换机信息一经提取和放置在主机配置文件中后，您即有机会更改任意信息。在以下部分中提供了针对标准交换机和分布式交换机的修改：上行链路选择策略（基于 vmnic 名称或设备编号）以及自动发现（基于 VLAN ID）。信息（可能已修改）由无状态引导基础架构存储，并在无状态 ESXi 主机下次引导时进行应用。在网络初始化期间，通用网络插件将解释记录的主机配置文件设置并执行以下操作：

- 加载合适的物理网卡驱动程序。
- 随端口组一起创建所有标准交换机实例。它基于策略选择上行链路。如果策略是基于 VLAN ID，则将启动一个探测进程以收集相关信息。
- 对于连接到标准交换机的 VMkernel 网络适配器，它将创建 VMkernel 网络适配器并将其连接到端口组。
- 对于每个连接到分布式交换机的 VMkernel 网络适配器，它将创建具有绑定到 VMkernel 网络适配器的上行链路的临时标准交换机（根据需要）。它将基于记录的信息创建具有 VLAN 和成组策略的临时端口组。具体来说，如果在分布式交换机中使用了以太通道，则将使用 IP 哈希。
- 配置所有 VMkernel 网络适配器设置（分配地址、网关、MTU，等等）。

基本连接将正常工作，并且网络设置即已完成（如果不存在分布式交换机）。

如果存在分布式交换机，那么系统将处于维护模式下，直至分布式交换机修复完成。此时不会启动任何虚拟机。因为分布式交换机需要 **vCenter Server**，所以引导过程将继续，直至建立 **vCenter Server** 连接性，并且 **vCenter Server** 会发现主机应该是分布式交换机的一部分。它将发出分布式交换机主机加入，在主机上创建分布式交换机代理标准交换机，选择相应的上行链路，然后将 **vmknic** 从标准交换机迁移到分布式交换机。此操作完成后，它将删除临时标准交换机和端口组。

在修复过程结束时，**ESXi** 主机将退出维护模式，然后 **HA** 或 **DRS** 可以在主机上启动虚拟机。

如果缺少主机配置文件，则将通过“默认网络连接”逻辑创建临时标准交换机，以创建其上行链路与 **PXE** 引导 **vNIC** 相对应的管理网络交换机（不具有 **VLAN** 标记）。将在管理网络端口组上创建 **vmknic**，其 **MAC** 地址与 **PXE** 引导 **vNIC** 相同。该逻辑以前用于 **PXE** 引导。如果有主机配置文件，但是网络连接主机配置文件处于禁用状态或者具有致命的不完整性，则 **vCenter Server** 将回退到默认网络连接，以便可以远程管理 **ESXi** 主机。这将触发合规性故障，因此 **vCenter Server** 之后会启动恢复操作。

## 网络最佳做法

在配置网络时，请考虑这些最佳做法。

- 为了确保 vCenter Server 与 ESXi 以及其他产品和服务之间连接稳定，请不要在产品之间设置连接限制和超时。设置限制和超时可影响数据包流量，导致服务中断。
- 与用于主机管理、vSphere vMotion、vSphere FT 等的网络相互隔离，从而提高安全性和性能。
- 将单独的物理网卡专用于一组虚拟机，或使用 Network I/O Control 和流量调整以确保虚拟机的带宽。这种分离方法还可以使总网络工作负载的一部分分布到多个 CPU 上。例如，隔离的虚拟机可更好地处理应用程序流量（例如来自 Web Client 的流量）。
- 要以物理方式分离网络服务并且专门将一组特定的网卡用于特定的网络服务，请为每种服务创建 vSphere 标准交换机或 vSphere Distributed Switch。如果此操作无法实现，可以通过将网络服务附加到具有不同 VLAN ID 的端口组，以便在一个交换机上将它们分离开。在这两种情况下，都与网络管理员确认所选的网络或 VLAN 是否与环境中的其他部分隔离，即没有与其相连的路由器。
- 在单独的网络上保持 vSphere vMotion 连接。在进行 vMotion 迁移时，客户机操作系统内存的内容将通过该网络传输。通过使用 VLAN 对单个物理网络分段，或者使用单独的物理网络（后者为首选），可以实现这一点。

为进行跨 IP 子网的迁移和使用单独的缓冲区和插槽池，请将 vMotion 的流量放置在 vMotion TCP/IP 堆栈上，将已关闭电源虚拟机和克隆的迁移的流量放置在置备 TCP/IP 堆栈上。请参见第 50 页，“VMkernel 网络层”。

- 可以在不影响虚拟机或在交换机后端运行的网络服务的前提下，向标准或 Distributed Switch 添加或从中移除网络适配器。如果移除所有正在运行的硬件，虚拟机仍可互相通信。如果保留一个网络适配器原封不动，则所有的虚拟机仍然可以与物理网络相连。
- 为了保护大部分敏感的虚拟机，请在虚拟机中部署防火墙，以便在带有上行链路（连接物理网络）的虚拟网络和无上行链路的纯虚拟网络之间路由。
- 为获得最佳性能，请使用 VMXNET 3 虚拟机网卡。
- 连接到同一 vSphere 标准交换机或 vSphere Distributed Switch 的物理网络适配器还应该连接到同一物理网络。
- 在 vSphere Distributed Switch 中配置所有 VMkernel 网络适配器的相同 MTU。如果多个 VMkernel 网络适配器连接到 vSphere Distributed Switch 但配置了不同的 MTU，您可能会遇到网络连接问题。



# 索引

## 符号

### 标准交换机

- Dump Collector 支持 14
- 安全策略 19
- 绑定和故障切换策略 19
- 查看网络适配器信息 51
- 带宽峰值 92
- 第 2 层安全策略 90
- 端口组 18, 19
- 端口组的 VLAN ID 19
- 端口组的网络标签 19
- Fault Tolerance 日志记录 52, 55
- 负载均衡 85
- 管理流量 52, 55
- 故障切换 85
- 恢复 75
- 回滚 75
- 混杂模式 90
- IPv4 52, 55
- IPv6 52, 55
- 链路状态 85
- 流量调整策略 19, 92
- MAC 地址更改 90
- MTU 55
- MTU 配置 20
- 配置 20
- 平均带宽 92
- 使用 15
- 属性 20
- 突发大小 92
- VMkernel 网络适配器 52
- VMKernel 网络适配器 55
- vMotion 52, 55
- 网卡绑定 85
- 网络适配器 52, 55
- 伪传输 90
- 物理网络适配器 20
- 物理网络适配器的速度和双工 20
- 无状态 203
- 信标探测 85
- 新建标准交换机 18
- 虚拟网络适配器 39

### Distributed Switch

- Dump Collector 支持 14
- 恢复 75, 77
- 编辑 IP 源数 200
- 编辑常规查询时间间隔 200
- CDP 193, 194
- 查看网络适配器信息 51
- 创建 VMkernel 适配器 54

Cisco 发现协议 193

代理交换机 37

导出配置 71

导入配置 71, 72

端口镜像 188

多播侦听

编辑查询时间间隔 200

常规查询 200

Fault Tolerance 流量 33

管理流量 33

管理员联系信息 29

管理主机网络 30

还原配置 71

回滚 75

IP 存储流量 33

健康状况检查 192

健康状况检查启用或禁用 192

交换机发现协议 29

LACP 69

链路层发现协议 194

LLDP 194

名称 29

模板主机 36

MTU 29

Network I/O Control, version 2 160

配置虚拟网络 30

迁移 VMkernel 适配器 33

迁移虚拟机 45

迁移虚拟机网络连接 36

迁移虚拟机网络适配器 36

上行链路 29

升级 28

设置 29

添加 27

添加 VMkernel 适配器 33

添加上行链路适配器 39

添加网卡 39

添加网络适配器 39

添加主机 30

Virtual SAN 流量 33

VLAN 116

VMkernel 适配器 33

VMkernel 网络连接 33

VMkernel 网络适配器 34

vMotion 流量 33

网络适配器 34

网络资源池 154

物理网络适配器 38

虚拟机的带宽保证 153

虚拟机网络连接 36



- 虚拟机网络连接适配器 36
- 虚拟机网络适配器 38
- 移除上行链路适配器 39
- 移除网卡 39
- 移除网络适配器 39
- 移除主机 37
- 运行状况检查 192
- 专用 VLAN 116
- Dump Collector 14
- 管理网络 77
- 恢复, Distributed Switch 77
- netdump 14
- A**
- 安全策略
  - 策略异常 90
  - 分布式端口组 109
  - 混杂模式 90
  - MAC 地址更改 90
  - vSphere 标准交换机 90
  - 伪信号 90
- B**
- 绑定策略
  - 分布式端口组 109
  - 健康状况检查 193
  - 运行状况检查 192
- 被阻止的端口, 分布式端口组 109
- 捕获一定数量的数据包 175
- C**
- CDP 193
- 测试 134
- 创建 LAG 65
- 创建 TCP/IP 堆栈 58
- 创建 vSphere 标准交换机 17
- 创建链路聚合组 65
- Cisco 发现协议 193
- Cisco 交换机 193
- D**
- 带宽
  - 峰值 92
  - 平均 92
- 带宽保证, Distributed Switch 153
- 带宽峰值, 标准交换机 92
- 带宽分配 151
- 单根 I/O 虚拟化
  - 在主机物理适配器上启用 127
  - 另请参见 SR-IOV
- 导出配置
  - distributed switch 71
  - Distributed Switch 71
  - 分布式端口组 73
- 导入配置
  - Distributed Switch 71
  - 分布式端口组 73
- 大型接收卸载, 请参见 LRO
- DCUI, 还原 vDS 77
- 第 2 层安全 90
- 第 2 层安全策略, 分布式端口组 91
- DirectPath I/O
  - 启用 121
  - vMotion 121
  - 虚拟机 121
- 第三方交换机 24
- distributed switch
  - 导出配置 71
  - 还原配置 72
- distributed switch, 编辑网络资源池 157
- DNS, 配置 57
- 端口策略, 分布式端口组 109
- 端口镜像
  - 版本兼容性 186
  - 编辑 VLAN 190
  - 编辑目标 190
  - 编辑源 190
  - 编辑状态 190
  - 采样率 189
  - 功能兼容性 186
  - 会话类型 187, 188
  - I/O 189
  - IP 地址 189
  - 流量方向 189
  - LRO 187
  - 名称 189
  - 目标 189, 190
  - 使用 vSphere Web Client 创建 188
  - 添加端口 189
  - 添加上行链路 189
  - TSO 187
  - VLAN 189, 190
  - vMotion 187
  - 验证设置 189, 190
  - 源 189, 190
  - 状态 190
- 端口组, 定义 13
- 端口阻止 79
- 多播, 筛选 199
- E**
- EST 115
- ESXi 主机
  - LRO 141

- LRO, 检查状态 **140**
- LRO, 启用 **140**
- LRO, VMkernel 的缓冲区大小 **141**
- LRO, VMXNET 3 适配器的缓冲区大小 **141**
- NetQueue **143**
- TSO, 检查状态 **138**
- TSO, 启用 **137**

## F

- 防火墙规则, PVRDMA **133**

- Fault Tolerance 流量 **50**

- Fault Tolerance 日志记录 **52, 55**

- 分布式端口

- 编辑名称 **45**

- 编辑设置 **45**

- 查看流量规则 **104**

- 打开流量规则进行编辑 **105**

- 定义流量规则 **104**

- 端口镜像 **188**

- 端口状况 **44**

- 更改规则优先级 **105**

- 监控端口状况 **44**

- 禁用流量筛选和标记 **106**

- 流量筛选和标记 **101**

- 其他策略 **113**

- 启用流量筛选和标记 **101**

- 删除规则 **106**

- 使用 CoS 和 DSCP 标记流量 **102**

- 授予或拒绝对流量的访问 **103**

- 网络资源池 **94**

- 阻止 **113**

- 阻止所有端口 **113**

- 分布式端口组

- 安全策略 **40, 109**

- 绑定策略 **86, 109**

- 绑定和故障切换策略 **40**

- 备份 **71**

- 被阻止的端口 **109**

- 查看流量规则 **99**

- 常规设置 **43**

- 大规模配置 **109**

- 打开流量规则进行编辑 **99**

- 导出配置 **71, 73**

- 导入配置 **71, 73**

- 第 2 层安全策略 **91**

- 定义流量规则 **99**

- 断开连接时重置 **43, 81**

- 端口绑定 **40, 43**

- 端口策略 **109**

- 端口分配 **40, 43**

- 端口阻止 **40**

- 峰值带宽 **109**

- 分配网络资源池 **154**

- 负载均衡 **109**

- 高级设置 **43, 81**

- 更改规则优先级 **100**

- 故障切换策略 **86, 109**

- 故障切换顺序 **86, 109**

- 还原 **71**

- 还原配置 **71, 73, 74**

- 混杂模式 **109**

- 监控策略 **95**

- 禁用流量筛选和标记 **100**

- 连接到虚拟机 **46**

- 流量筛选和标记 **109**

- 流量调整 **109**

- 流量调整策略 **40, 93**

- MAC 地址更改 **109**

- NetFlow **40, 109**

- NetFlow 策略 **95**

- Network I/O Control **109**

- 配置流量筛选和标记 **96**

- 平均带宽 **109**

- PVLAN **109**

- 其他策略 **109, 113**

- 启用流量筛选和标记 **96**

- QOS 策略 **109**

- 删除规则 **100**

- 删除流量规则 **100**

- 使用 CoS 和 DSCP 标记来标记流量 **96**

- 授予或拒绝对流量的访问 **98**

- 添加新的 **40**

- 替代端口策略 **43, 81**

- 通知交换机 **109**

- 突发大小 **109**

- VLAN **40, 43**

- VLAN 策略 **88, 109**

- VLAN 中继 **109**

- 网络资源池 **40, 43, 94, 109**

- 伪信号 **109**

- 移除 **44**

- 阻止所有端口 **113**

- 分布式交换机

- 无状态 **203**

- 虚拟机 **45**

- 峰值带宽 **109**

- 分配 PVRDMA 适配器, 虚拟机 **134**

- 负载均衡

- 标准交换机 **85**

- 端口 ID 绑定 **83**

- 分布式端口组 109
  - IP 哈希 83
    - 基于 IP 哈希的路由 83
    - 基于负载的成组 84
    - 基于物理网卡负载的路由 84
    - 基于源 MAC 哈希的路由 83
    - 基于源虚拟端口的路由 83
    - MAC 哈希 83
    - 明确故障切换顺序 85
    - 使用明确故障切换顺序 85
    - 虚拟端口 ID 绑定 83
    - 源 MAC 哈希 83
  - 负载均衡策略 82
  - 负载均衡算法
    - IP 哈希负载均衡 82
    - 基于物理网卡负载的路由 82
    - 基于源 MAC 哈希的路由 82
    - 基于源虚拟端口的路由 82
    - 使用明确故障切换顺序 82
- ## G
- 管理流量 50, 52, 55
  - 管理主机网络 31
  - 故障恢复 109
  - 故障切换, 标准交换机 85
  - 故障切换策略, 分布式端口组 86, 109
  - 故障切换顺序, 分布式端口组 86, 109
- ## H
- HCA 132, 133
  - 还原配置
    - distributed switch 72
    - Distributed Switch 71
    - 分布式端口组 73, 74
  - 回滚
    - 标准交换机 75
    - Distributed Switch 75
    - 禁用 76
    - vpxd.cfg 文件 76
    - 主机网络 75
  - 混杂模式 90, 109
- ## I
- IGMP 侦听
    - 多播侦听 199
    - 概览 199
    - 启用 200
  - IOMMU 122, 127
  - IP 存储流量 50
  - IP 地址配置 196
  - IP 哈希负载均衡 83
  - IPv4 52, 55
  - IPv6
    - 概览 167
    - 配置 167
    - vCenter Server 171
    - VMkernel 57
    - vSphere 安装 169
    - vSphere 升级 169
    - 在 vCenter Server 上启用 171, 172
    - 在 VMkernel 上启用 171
    - 在主机上禁用 170
    - 在主机上启用 170
  - iSCSI 流量 50
- ## J
- 健康状况检查
    - 查看信息 193
    - 启用或禁用 192
  - 监控策略, 分布式端口组 95
  - 交换机拓扑, SR-IOV 129
  - 静态 MAC 地址 165
  - 禁用回滚 76
  - 基于 IP 哈希的路由 82
  - 基于范围的 MAC 地址分配 163
  - 基于前缀的 MAC 地址分配 162, 163
  - 巨帧
    - 在 vSphere 标准交换机上启用 135
    - 在 vSphere 标准交换机中启用 136
    - 在 vSphere Distributed Switch 中启用 135
    - 在虚拟机中启用 136
  - 巨帧, 启用 135
- ## K
- 客户机操作系统, 移除网卡 40
- ## L
- LACP
    - Distributed Switch 69
    - IP 哈希负载均衡 69
    - iSCSI 69
    - 上行链路端口组 69
    - 升级 63
    - 限制 69
    - 增强型支持 63
    - 转换为增强型 LACP 63
    - 主机 69
  - LACP 支持 61
  - LAG
    - 绑定和故障切换顺序 67
    - 创建 64, 65
    - 分配物理适配器 66
    - 分配物理网卡 66

- 故障切换顺序 66
- 活动 67
- 配置 64
- 迁移网络流量 64
- 设置为备用 66
- 未使用 66
- 中间配置 66
- 链路层发现协议 193, 194
- 链路聚合组
  - 编辑设置 68
  - 负载均衡算法 68
  - 更改配置 68
  - 添加端口 68
  - VLAN 和 NetFlow 策略 68
- 链路状态, 标准交换机 85
- 流量
  - 查看规则 99
  - 筛选和标记 95, 107, 109
  - 筛选和标记, 按 MAC 地址 107
  - 筛选和标记, 按 VLAN ID 107
  - 筛选和标记, 按数据链路层属性 107
  - 使用 CoS 标记 96
  - 使用 DSCP 标记 96
- 流量规则, 添加 99, 105
- 流量筛选和标记
  - 按 IP 地址 108
  - 按 MAC 地址 107
  - 按第 2 层属性 107
  - 按第 3 层属性 107
  - 按数据链路层属性 107
  - 按网络层属性 108
  - 按系统数据类型 107
  - 查看端口上的流量规则 104
  - 查看流量规则 99
  - 打开端口上的规则进行编辑 105
  - 打开规则进行编辑 99
  - 定义流量规则 99
  - 更改端口上的规则优先级 105
  - 更改规则优先级 100
  - 禁用 100
    - 流量筛选和标记
      - 按 VLAN ID 107
      - 按传输协议和端口 108
  - 删除端口上的规则 106
  - 使用 CoS 和 DSCP 来标记端口流量 102
  - 授予或拒绝对流量的访问 103
  - 允许或丢弃操作 103
  - 在端口上定义流量规则 104
  - 在端口上禁用 106
  - 在端口上启用 101
  - 在端口组上启用 96

- 流量筛选, 授予或拒绝对流量的访问 98
- 流量调整, 分布式端口组 109
- 流量调整策略
  - 标准交换机 92
  - 带宽峰值 92
  - 分布式端口组 93
  - 平均带宽 92
  - 突发大小 92
- LLDP 193, 194
- LRO
  - ESXi 主机 140
  - ESXi 主机, 启用 140
  - 检查状态 140
  - Linux 虚拟机 141
  - 启用 141
  - VMkernel 的缓冲区大小 141
  - VMXNET 3 适配器的缓冲区大小 141
  - Windows 虚拟机, 启用 142
  - 硬件 LRO 140

## M

- MAC 地址
  - 本地管理地址 (LAA) 162
  - 分配 MAC 地址 162
  - 静态 166
  - 静态 MAC 地址 165
  - 静态, VMware OUI 165
  - 基于范围的分配 162, 163
  - 基于前缀的分配 162, 163
  - 配置 161, 166
  - 生成 161, 162
  - 生成, 主机 164
  - 设置分配类型 163
  - 手动分配 MAC 地址 165
  - 调整分配参数 163
  - vCenter Server 161
  - VMware OUI 162
  - VMware OUI 分配 163
- MAC 地址冲突 162
- MAC 地址更改 90, 109
- MLD 侦听
  - 概览 199
  - 启用 200
- MTU
  - 健康状况检查 193
  - 运行状况检查 192
- MTU 配置 20

## N

- NetFlow
  - 分布式端口组 109
  - 禁用 95, 109, 185

- 配置 185
- 启用 95, 109, 185
- 收集器设置 185
- NetFlow 策略, 分布式端口组 95
- netqueue 143
- NetQueue
  - 禁用 144
  - 启用 143
- Network I/O Control
  - 版本 145
  - version 2 94, 158, 159
  - 版本 2, 网络资源池配置 160
  - 带宽, 管理流量分配 150
  - 带宽, iSCSI 分配 150
  - 带宽, NFS 分配 150
  - 带宽, Virtual SAN 分配 150
  - 带宽, vMotion 分配 150
  - 带宽, 系统流量分配 150
  - 带宽, 虚拟机分配 151, 153
  - 概览 145
  - 将带宽分配给虚拟机 155
  - 启用 148
  - 升级 146
  - 网络资源池 154
  - 为虚拟机预留带宽 155
  - 向多个虚拟机分配带宽 156
  - 系统流量, 带宽分配 148
  - 系统流量, 带宽分配参数 149
  - 系统流量, 带宽预留 149
  - 虚拟机的带宽保证 153
  - 移除与网络资源池的关联 157
  - 预留配额 154, 157
  - 在物理适配器上禁用 158
- NETWORK I/O CONTROL 94
- NFS 流量 50

## P

- PCI, 虚拟机 120
- PCIe 设备 122, 127
- 配置
  - 导入 72
  - Distributed Switch 72
- 配置 LACP 65
- PFC 134
- 平均带宽, 标准交换机 92
- pktcap-uw
  - 捕获点 183, 184
  - 捕获数据包 177, 178, 180–182
  - 查看所有捕获点 184
  - 跟踪数据包 184
  - 跟踪选项 175

- 跟踪语法 175
- 选项 175, 176
- 用于捕获数据包的选项 173
- 用于捕获数据包的语法 173

## PVRDMA

- ESXi 133
- 防火墙 133
- 防火墙规则 133
- VMkernel 适配器 133
- 要求 132
- 支持 132, 133
- PVRDMA 网络适配器 134

## Q

- 其他策略
  - 分布式端口 113
  - 分布式端口组 109, 113
- QOS 策略, 分布式端口组 109

## R

- RDMA, 聚合以太网 RDMA 134
- RoCe, 网络要求 134

## S

- 上行链路端口
  - 查看流量规则 104
  - 打开流量规则进行编辑 105
  - 定义流量规则 104
  - 更改规则优先级 105
  - 禁用流量筛选和标记 106
  - 流量筛选和标记 101
  - 启用流量筛选和标记 101
  - 删除规则 106
  - 使用 CoS 和 DSCP 标记流量 102
  - 授予或拒绝对流量的访问 103
- 上行链路端口组
  - 备份 71
  - 查看流量规则 99
  - 打开流量规则进行编辑 99
  - 定义流量规则 99
  - 更改规则优先级 100
  - 还原 71
  - 禁用流量筛选和标记 100
  - LACP 69
  - 配置流量筛选和标记 96
  - 启用流量筛选和标记 96
  - 删除流量规则 100
  - 使用 CoS 和 DSCP 标记来标记流量 96
    - 使用 CoS 和 DSCP 标记流量, 端口组 96
  - 授予或拒绝对流量的访问 98
  - VLAN 策略 89

- 上行链路适配器
  - 从 Distributed Switch 中移除 39
  - 添加到 Distributed Switch 39
- 升级
  - Distributed Switch 28
  - vSphere Distributed Switch 28
- 设置 MAC 地址分配类型 163
- 使用 vpxd.cfg 禁用回滚 76
- 数据包捕获
  - 捕获到文件中 175
  - 捕获点 183, 184
  - 查看所有捕获点 184
  - 丢弃的数据包 181
  - DVFilter 182
  - 跟踪数据包 184
  - 仅捕获数据包的前若干个字节 175
  - 控制台命令 173, 175–178, 180–184
  - pktcap-uw 173, 177, 178, 180–184
  - 筛选数据包 176
  - 上行链路 177
  - VMkernel 180
  - VMXNET3 178
  - 物理适配器 177
- 数据包跟踪
  - 控制台命令 175
  - pktcap-uw 175
- SR-IOV
  - 安全策略 129
  - 备份模式 129
  - ESXCLI 命令 130
  - 概览 124
  - 可用 VF 数 126
  - 控制路径 124
  - 启用 130
  - 使用 vCLI 命令启用 130
  - 使用主机配置文件启用 130
  - 数据路径 124
  - VF 126
  - VF 速率控制 126
  - VLAN 策略 129
  - 网络选项 129
  - 物理功能 126
  - 物理网卡交互 126
  - 虚拟功能 126
  - 虚拟机 127
  - 与虚拟机关联作为网络适配器 128
  - 在主机物理适配器上启用 127
  - 中断向量已耗尽 131
  - 主机配置文件 130
  - 组件 124
- SR-IOV, 已关闭虚拟机电源 131

## T

- TCP 分段清除, , 请参见 TSO
- 添加
  - Distributed Switch 27
  - vSphere Distributed Switch 27
- 调整 MAC 地址分配参数 163
- 通用唯一标识符 (UUID) 162
- 通知交换机 109
- TSO
  - ESXi 主机, 检查状态 138
  - ESXi 主机, 启用 137
  - Linux 虚拟机 138
  - 启用 137
  - Windows 虚拟机, 启用 139
  - 物理网络适配器, 检查状态 137
  - 物理网络适配器, 启用 137
- 突发大小, 标准交换机 92

## V

- vApp
  - 配置 IPv4 196
  - 配置 IPv6 196
  - 网络协议配置文件 198
  - 选择网络关联 196
- VDS
  - 分配 vmnic 33
  - 分配物理网卡 33
  - 迁移 vmnic 33
  - 迁移物理网卡 33
  - 添加主机 31
- VGT 115
- Virtual SAN 流量 50
- VLAN
  - 定义 13
  - 端口镜像 190
  - 辅助 117
  - 健康状况检查 193
  - 类型 116
  - 运行状况检查 192
  - 专用 116, 117
- VLAN 策略
  - 分布式端口组 88, 109
  - 上行链路端口组 89
- SR-IOV 129
- VLAN ID
  - 辅助 116
  - 主 116
- VLAN 中继, 分布式端口组 109
- VMkernel
  - 定义 13
  - DNS 57
  - IPv6 57

- 配置 49
- 启用 LRO 141
- 网关 57
- VMkernel 适配器, 查看信息 51
- VMkernel 适配器, PVRDMA 133
- VMkernel 网络连接
  - 创建 VMkernel 适配器 54
  - 使用 ESXCLI 替代默认网关 57
  - 替代默认网关 56
- VMkernel 网络适配器 52
- VMKernel 网络适配器 55–57
- vMotion
  - 定义 13
  - 端口镜像 187
  - 兼容性 119
  - 网络配置 49
- vMotion 流量 50
- VMware OUI
  - MAC 地址, 静态 165
  - MAC 地址, 主机 164
  - vCenter Server 分配 162
- VMware OUI 分配 162
- vpd.cfg 76, 163
- vSphere, 在 IPv6 中部署 168, 169
- vSphere 标准交换机
  - 安全策略 90
  - 第 2 层安全策略 90
  - 定义 13
  - 防止 MAC 地址模拟 90
  - 防止流量扫描 90
  - 混杂模式 90
  - MAC 地址更改 90
  - MTU 配置 20
  - 配置 20
  - 启用巨帧 136
  - 使用 15
  - 属性 20
  - 拓扑图 21
  - 伪传输 90
- vSphere Distributed Switch
  - 安全策略 90
  - 备份 71
  - CDP 193
  - Cisco 发现协议 193
  - 第三方 24
  - 端口镜像 186
  - 对端口进行流量筛选和标记 101
  - 多播 199
  - 防止 MAC 地址模拟 90
  - 防止流量扫描 90
  - 还原 71
  - 将虚拟机迁入或迁出 45
  - 镜像 186
  - 巨帧, 启用 135
  - 链路层发现协议 194
  - 流量筛选和标记 95
  - LLDP 194
  - Network I/O Control 145, 146, 148, 149
  - 升级 28
  - 添加 27
  - 拓扑图 46
  - 拓扑图, 所有主机 47
  - 拓扑图, 主机代理交换机 48
  - 虚拟机 45
  - 在端口组上配置流量筛选和标记 96
  - 另请参见 Distributed Switch
  - 另请参见 Distributed Switch Network I/O Control
- VST 115
- W**
- 外部交换机标记 115
- 网卡
  - 从 Distributed Switch 中移除 39
  - 从 vSphere Distributed Switch 中移除 40
  - 从活动虚拟机中移除 40
  - 客户机操作系统 40
  - 添加到 Distributed Switch 39
- 网卡绑定
  - 标准交换机 21, 85
  - 定义 13
- 网络
  - 分布式端口 44
  - IP 地址配置 196
  - 简介 13
  - 性能 143
  - 资源池 145
- 网络策略
  - 标准交换机 80
  - Distributed Switch 80
- 网络关联设置 196
- 网络流量, 监控 173
- 网络协议配置文件
  - 关联端口组 197
  - 配置 vApp 198
  - 配置虚拟机 198
  - 另请参见 协议配置文件
- 网络资源池
  - 创建 154
  - 分布式端口 94
  - 分布式端口组 94, 109
  - 移除 157

- 预留配额 **154, 157**
  - 在多个虚拟机上分配带宽 **156**
- 网络资源管理 **119**
- 网络最佳做法 **205**
- 为 Distributed Switch 添加主机 **31**
- 伪信号 **90, 109**
- Windows 虚拟机
  - LRO **143**
  - LRO, 启用 **142**
  - 启用 **143**
  - 全局启用 **143**
  - TSO, 启用 **139**
- 物理网络适配器
  - 标准交换机 **20**
    - 从 Distributed Switch 中移除 **39**
  - 故障切换 **21**
  - 添加到 Distributed Switch **39**
  - 添加到标准交换机 **21**
  - TSO, 检查状态 **137**
  - TSO, 启用 **137**
- 无状态分布式交换机 **203**
- 无状态引导 **203**

**X**

- 协议配置文件, 配置 **195**
- 信标探测, 标准交换机 **85**
- 系统流量, 分配带宽 **150**
- 虚拟 LAN, 另请参见 VLAN
- 虚拟机
  - 带宽份额 **155, 156**
  - 带宽分配, 参数 **153**
  - 带宽分配, 概览 **151**
  - 带宽限制 **155, 156**
  - 带宽预留 **155, 156**
  - 静态 MAC 地址 **165**
  - 连接到分布式端口组 **46**
  - 迁入和迁出 vSphere Distributed Switch **45**
  - 迁入或迁出 Distributed Switch **45**
  - 启用巨帧 **136**
  - SR-IOV **127**
  - 网络 **45**
  - 网络协议配置文件 **198**
  - 移除与网络资源池的关联 **157**
- 虚拟交换机标记 **115**
- 虚拟机的带宽保证
  - vSphere DRS **153**
  - vSphere HA **153**
- 虚拟机网络连接 **14, 18**
- 虚拟客户机标记 **115**

- 虚拟网络适配器
  - 标准交换机 **39**
    - 从 Distributed Switch 中移除 **58**

## Y

- 移除标准端口组 **20**
- 移除端口组 **20**
- 移除分布式端口组 **44**
- 已关闭虚拟机电源, SR-IOV **131**
- 应用网络策略 **80**
- 远程直接内存访问 **132**
- 运行状况检查 **192**

## Z

- 直接控制台用户界面 (DCUI), 还原 vDS **77**
- 直通设备
  - 添加到主机 **120**
    - 虚拟机 **120**
- 专用 VLAN
  - 创建 **116**
  - 辅助 **116, 117**
  - 移除 **117**
  - 主 **116, 117**
- 主机
  - 禁用 IPv6 **170**
  - 启用 IPv6 **170**
  - 启用 SR-IOV **130**
- 主机配置文件
  - 启用 SR-IOV **130**
  - SR-IOV **130**
- 主机通道适配器 **132, 133**
- 主机网络, 查看网络适配器信息 **51**
- 主机网络连接, 回滚 **75**
- 准虚拟化 RDMA **132**
- 自定义 TCP/IP 堆栈 **58**
- 资源池, 网络 **145**
- 阻止所有端口
  - 分布式端口 **113**
  - 分布式端口组 **113**