ESX Server 3 配置指南

ESX Server 3.5 和 VirtualCenter 2.5

vmware®

ESX Server 3 配置指南
修订时间：20080410
项目：VI-CHS-Q208-491

我们的网站提供最新的技术文档，网址为：

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

此外， VMware 网站还提供最新的产品更新。

如果对本文档有任何意见或建议，请将反馈信息提交至以下地址：

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.
北京办公室 北京市东城区长安街一号东方广场 W2 办公楼 6 层 601 室
邮编：100738 电话：+86-10-8520-0148
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
邮编：200120 电话 : +86-21-6160 -1168
广州办公室 广州市天河北路 233 号中信广场 7401 室
邮编：510613 电话：+86-20-3877-1938
http://www.vmware.com/cn

目录

存储器

安全

关于本书

本手册 （《*ESX Server 3 配置指南*》）提供有关如何为 ESX Server 3 配置网络的信息，其包括如何创建虚拟机交换机和端口以及如何为虚拟机、 VMotion、 IP 存储器和服务控制台创建网络的信息。此外还论述了配置文件系统及各种类型的存储器，例如 iSCSI、光纤通道等等。为帮助保护 ESX Server 3 安装，本指南提供了有关 ESX Server 3 中嵌入的安全功能的论述以及为使其免受攻击而可采取的安全措施。此外，它还包括一个 ESX Server 3 技术支持命令和其 VI Client 等效指令的列表以及一个 `vmkfstools` 实用程序的描述。

《*ESX Server 3 配置指南*》涉及 ESX Server 3.5 的内容。要阅读并了解有关 ESX Server 3i 版本 3.5 的内容，请参见 http://www.vmware.com/support/pubs/vi_pubs.html。

为方便讲解，本书使用以下产品命名约定：

- 对于特定于 ESX Server 3.5 的主题，本书使用术语 “ESX Server 3”。
- 对于特定于 ESX Server 3i 版本 3.5 的主题，本书使用术语 “ESX Server 3i”。
- 对于上述两款产品的共同主题，本书使用术语 “ESX Server”。
- 如果版本对于论述非常重要，则本书将使用带版本号的完整名称指代该产品。
- 当讲解内容适用于 VMware® Infrastructure 3 的所有 ESX Server 版本时，本书使用术语 “ESX Server 3.x”。

目标读者

本手册专供需要安装、升级或使用 ESX Server 3 的用户使用。本手册中信息的目标读者为熟悉虚拟机技术和数据中心操作且经验丰富的 Windows 或 Linux 系统管理员。

文档反馈

VMware 欢迎您提出宝贵建议，以便改进我们的文档。如有任何意见或建议，请将反馈信息发送至：

docfeedback@vmware.com

VMware Infrastructure 文档

VMware Infrastructure 文档由 VMware VirtualCenter 和 ESX Server 文档集组合而成。

图中使用的缩写

本手册中的图片使用表 1 中列出的缩写形式。

表 1. 缩写

缩写	描述
VC	VirtualCenter
VM	虚拟机
VI Client	VMware Infrastructure Client
服务器	VirtualCenter Server
数据库	VirtualCenter 数据库
host*n*	VirtualCenter 管理的主机
VM#	受管主机上的虚拟机
user#	具有访问权限的用户
dsk#	受管主机的存储磁盘
数据存储	受管主机的存储器
SAN	受管主机之间共享的存储区域网络类型数据存储
tmplt	模板

技术支持和教育资源

以下各节介绍提供的技术支持资源。可以通过下列网址访问本手册及其他书籍的最新版本：

http://www.vmware.com/support/pubs

在线支持和电话支持

通过在线支持可提交技术支持请求、查看产品和合同信息，以及注册您的产品。网址为：http://www.vmware.com/cn/support。

具有相应支持合同的客户应通过电话支持获得优先级为 1 的问题的最快响应。网址为：http://www.vmware.com/cn/support/phone_support.html。

支持服务项目

了解 VMware 支持服务项目如何帮助您满足业务需求。网址为：http://www.vmware.com/cn/support/services。

VMware 教育服务

VMware 课程提供了大量实践操作环境、案例研究范例，以及用于作业参考工具的课程材料。有关 VMware 教育服务的详细信息，请访问 http://mylearn1.vmware.com/mgrreg/index.cfm。

1 简介

《*ESX Server 3 配置指南*》介绍了为配置 ESX Server 3 主机网络、存储器和安全所需要完成的任务。此外，它还提供有助于了解这些任务以及如何部署 ESX Server 3 主机以满足需要的概述、建议和概念性论述。在使用《*ESX Server 3 配置指南*》中的信息之前，请仔细阅读 "*Virtual Infrastructure 简介*" 以了解系统架构以及组成 VMware Infrastructure 系统的物理和虚拟设备的概述。

此简介概括了本指南的内容，因此从中可以找到所需信息。本指南论述了以下主题：

- ESX Server 3 网络配置
- ESX Server 3 存储器配置
- ESX Server 3 安全功能
- ESX Server 3 命令参考
- `vmkfstools` 命令

网络

ESX Server 3 网络章节使您物理和虚拟网络概念，介绍完成配置 ESX Server 3 主机的网络连接需要执行的基本任务，并对高级网络主题和任务进行论述。网络一节包含以下章节：

- “网络” - 介绍网络概念并指导您完成在设置 ESX Server 3 主机的网络时需执行的最常见任务。
- “高级网络” - 论述了高级网络任务，例如设置 MAC 地址、编辑虚拟交换机和端口以及 DNS 路由。此外，它还提供了有关使网络配置更有效的提示。
- “网络连接方案和疑难解答” - 介绍常用的网络配置和疑难解答方案。

存储器

ESX Server 3 存储器章节提供有关存储器的基本认识、配置和管理 ESX Server 3 主机存储器需执行的基本任务的描述以及如何设置裸设备映射 (RDM) 的论述。存储器一节包含以下章节：

- “存储器简介” - 介绍可以为 ESX Server 3 主机配置的存储器类型。
- “配置存储器” - 说明如何配置本地 SCSI 存储器、光纤通道存储器和 iSCSI 存储器。它还介绍虚拟机文件系统 (VMFS) 存储和网络附加存储。
- “管理存储器” - 说明如何管理现有的数据存储和由数据存储组成的文件系统。
- “裸设备映射” - 介绍裸设备映射、如何配置此类型的存储器以及如何通过设置多路径、故障切换等方式来管理裸设备映射。

安全

ESX Server 3 安全章节介绍 VMware 已嵌入到 ESX Server 3 中的安全措施以及避免 ESX Server 3 主机受到安全威胁多采用的措施。这些措施包括使用防火墙、利用虚拟交换机的安全功能以及设置用户身份验证和权限。安全一节包含以下章节：

- “ESX Server 3 系统的安全性” - 介绍有助于确保数据环境安全的 ESX Server 3 功能并提供一个与安全相关的系统设计的概述。
- “确保 ESX Server 3 配置的安全性” - 说明如何为 ESX Server 3 主机和 VMware VirtualCenter 配置防火墙端口、如何使用虚拟交换机和 VLAN 来确保虚拟机的网络隔离以及如何确保 iSCSI 存储器的安全。
- “身份验证和用户管理” - 介绍如何设置用户、组、权限和角色以控制对 ESX Server 3 主机和 VirtualCenter 的访问权限。它还介绍了加密和委派用户。
- “服务控制台安全” - 介绍嵌入到服务控制台的安全功能并演示如何配置这些功能。

- “安全部署与建议” - 提供一些样本部署，以便在设置个人的 ESX Server 3 部署时对需要考虑的问题有所了解。本章还介绍进一步确保虚拟机安装需要执行的一些操作。

附录

《ESX Server 3 配置指南》 包括提供专业化信息的附录，这些信息在配置 ESX Server 3 主机时可能会有用。

- “ESX Server 3 技术支持命令” - 论述了可通过诸如安全 shell(SSH) 等命令行 shell 发出的 ESX Server 3 配置命令。尽管有这些命令可供使用，但不要将其视为可在其上生成脚本的 API。这些命令可能有所更改，并且 VMware 不支持依赖于 ESX Server 3 配置命令的应用程序和脚本。此附录提供了对应于这些命令的 VMware Infrastructure Client 等效指令。
- “使用 vmkfstools” - 论述了 `vmkfstools` 实用程序，该程序可用于执行 iSCSI 磁盘的管理和迁移任务。

网络

网络 2

本章将指导您掌握在 ESX Server 3 环境中进行网络连接的基本概念及如何在虚拟基础架构环境中设置和配置网络。

使用 VMware Infrastructure (VI) Client 在下列表示三种网络服务类型的三种类别的基础添加网络：

- 虚拟机
- VMkernel
- 服务控制台

本章将讨论以下主题：

网络概念概述

一些概念对透彻了解虚拟网络至关重要。如果是首次接触 ESX Server 3，VMware 建议阅读本节。

物理网络 是连接在一起以便互相发送和接收数据的物理机所形成的网络。 VMware ESX Server 3 运行于物理机之上。

虚拟网络 是由运行于单台物理机之上的相互进行逻辑连接并互相发送和接收数据的虚拟机之间形成的网络。虚拟机可连接在添加网络步骤中所创建的虚拟网络。每个虚拟网络均有一个虚拟交换机为其提供服务。虚拟网络可通过虚拟网络的虚拟交换机将一个或多个物理以太网适配器 （也称为上行链路适配器）关联在一起，从而连接至物理网络。如果没有上行链路与虚拟交换机相关联，虚拟网络上的所有流量则限制在物理主机之内。如果有一个或多个上行链路适配器与虚拟交换机相关联，连接至此虚拟网络的虚拟机也能访问连接至上行链路适配器的物理网络。

物理以太网交换机 管理物理网络上计算机之间的网络流量。一个交换机可具有多个端口，每个端口都可与网络上的其他计算机或交换机连接。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至其端口的主机，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。

虚拟交换机 *vSwitch* 的运行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 vSwitch 连接至物理交换机，以连接虚拟网络与物理网络。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型的网络。即使 vSwitch 的运行与虚拟交换机大体相似，但它未具有物理交换机所拥有的一些高级功能。请参见“虚拟交换机”（第 21 页）。

端口组 为每个端口指定了诸如宽带限制和 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至 vSwitches。端口组界定通过 vSwitch 连接至网络的方式。在常规使用中，有一个或多个端口组与单一 vSwitch 相关联。请参见 “端口组”（第 23 页）。

当多个上行链路适配器与单一 vSwitch 相关联以形成小组时，就会出现*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。

VLAN 可用于将单一物理分段进一步分段，以便使端口组中处于不同物理分段中上的端口互相隔离。标准是 802.1Q。

VMkernel TCP/IP 网络堆栈 支持 iSCSI、 NFS 和 VMotion。虚拟机运行其自身系统的 TCP/IP 堆栈，并通过虚拟交换机在以太网级别与 VMkernel 连接。ESX Server 3 有两种新的功能：iSCSI 和 NFS，在本章中称为 *IP 存储器*。IP 存储器指将 TCP/IP 网络通信用

作其基础的任何形式的存储器。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 .ISO 文件的直接装载，该文件向虚拟机显示为 CD-ROM。

注意 网络适配器章节论述如何为 iSCSI 和 NFS 设置网络。要配置 iSCSI 和 NFS 的存储器选项，请参见存储器章节。

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。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 报头的调整后副本。请参见 "TCP 分段卸载和巨讯框"（第 56 页）。

借助*通过 VMotion 进行迁移*，可在 ESX Server 3 主机之间转移已启动的虚拟机，而无需关闭虚拟机。 VMotion 功能是可选的需要其自身的许可密钥。

虚拟交换机

借助 VMware Infrastructure ，可使用 Virtual Infrastructure (VI) Client 或直接 SDK API 创建称为虚拟交换机 (vSwitch) 的虚拟网络设置。 vSwitch 可在虚拟机之间进行内部流量路由或链接至外部网络。

注意 最多可在单台主机上创建 127 个 vSwitch。

使用虚拟交换机组合多个网络适配器的带宽并平衡它们之间的通信流量。也可将它们配置为处理物理网卡故障切换。

vSwitch 模拟物理以太网交换机。vSwitch 的默认逻辑端口数量为 56，但在 ESX Server 3 中创建最多具有 1016 个端口的 vSwitch。每个端口均可连接一个虚拟机网络适配器。与 vSwitch 关联的每个上行链路适配器均使用一个端口。vSwitch 的每个逻辑端口都是单一端口组的成员。还可向每个 vSwitch 分配一个或多个端口组。请参见 "端口组"（第 23 页）。

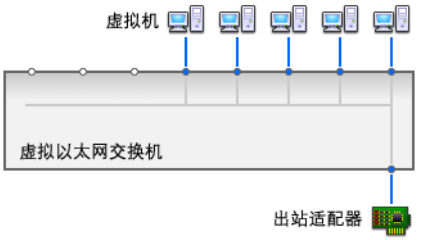
在配置虚拟机以访问网络之前，必须执行以下任务：

1 创建 vSwitch，并将其配置为连接至主机上的物理适配器，以连接至所需的物理网络。

2 创建连接至该 vSwitch 的虚拟机端口组，并为其命名，以便在配置虚拟机期间引用该名称。

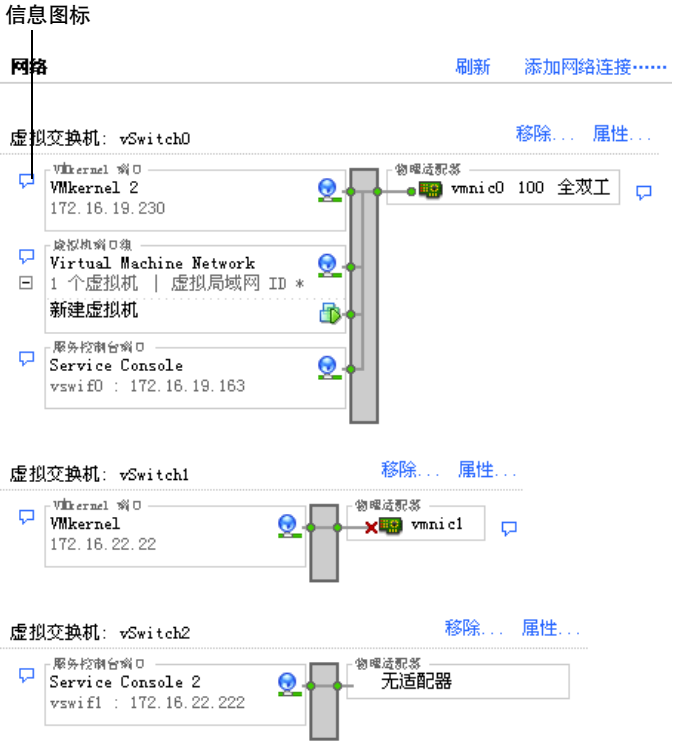
当两个或多个虚拟机连接至同一 vSwitch 时，它们之间的网络流量就会在本地进行路由。如果将上行链路适配器连接至 vSwitch，每台虚拟机均可访问该适配器所连接的外部网络，如图 2-1 中所示。

图 2-1 虚拟交换机连接



在 VI Client 中，选定 vSwitch 的详细信息显示为交互图，如图 2-2 中所示。始终可看到每台 vSwitch 的最重要信息。

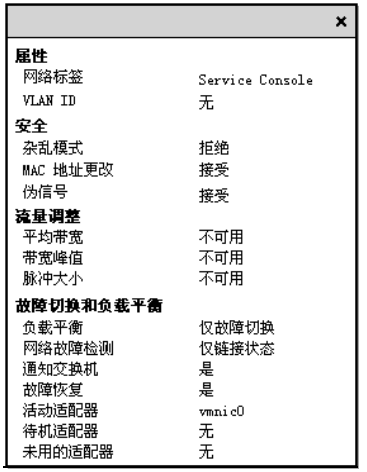
图 2-2 虚拟交换机交互图



单击信息图标，即可选择性地显示次要的和第三级信息。

弹出窗口中显示了详细的属性，如图 2-3 中所示。

图 2-3 虚拟交换机详细属性



端口组

端口组将多个端口聚合在公共配置下，并为连接标定网络的虚拟机提供稳定的定位点。每个端口组都由一个当前主机特有的网络标签标识。

注意 最多可在单台主机上创建 512 个端口组。

VLAN ID 是可选的，它将端口组流量限制在物理网络内的一个逻辑以太网段中。

注意 要使端口组到达其他 VLAN 上的端口组，请将 VLAN ID 设置为 4095。

启用网络服务

需要在 ESX Server 3 中启用两种类型的网络服务：

- 将虚拟机连接至物理网络
- 将 VMkernel 服务 （例如， NFS、 iSCSI 或 VMotion）连接至物理网络

为 ESX Server 3 运行管理服务的服务控制台的网络是在安装期间默认设置的。服务控制台端口是将 ESX Server 3 连接至任何网络或远程服务 （包括 VI Client）所必需的。某些服务可能需要其他服务控制台端口，例如 iSCSI 存储器。有关配置服务控制台端口的信息，请参见 “服务控制台配置”（第 32 页）。

查看 VI Client 中的网络连接信息

VI Client 显示了一般网络信息及网络适配器的特定信息。

查看 VI Client 中的一般网络连接信息

1 登录 VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[网络 (Networking)]**。

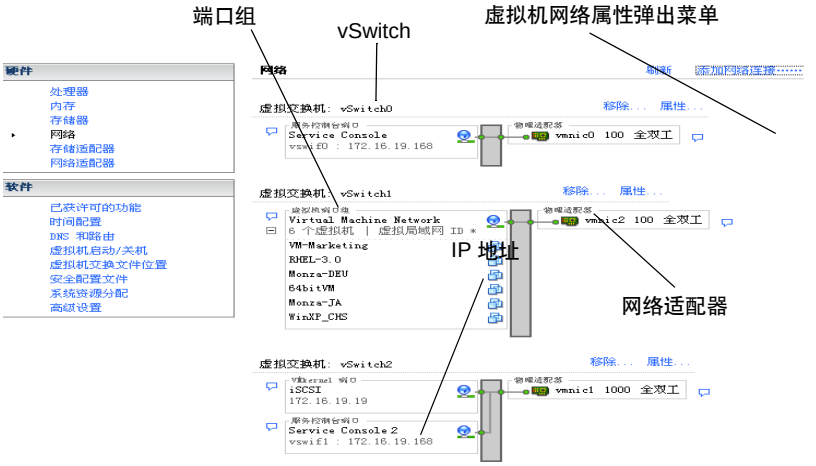
网络面板显示了以下信息，如图 2-4 中所示：

- 虚拟交换机
- 每个适配器的适配器信息
  - 链接状态
  - 显性速度和双工
- 服务控制台和 VMkernel TCP/IP 服务

  IP 地址
- 服务控制台

  虚拟设备名称
- 虚拟机
  - 电源状态
  - 连接状态
- 端口组
  - 网络标签 - 通用于所有三个端口配置类型
  - 已配置虚拟机数量
  - VLAN ID （如有）- 通用于所有三种端口配置类型

图 2-4 一般网络连接信息



查看 VI Client 中的网络适配器信息

1 登录 VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[网络适配器 (Network Adapters)]**。

网络适配器面板显示了以下信息：

- **[设备 (Device)]** - 网络适配器的名称
- **[速度 (Speed)]** - 网络适配器的实际速度和双工
- **[已配置 (Configured)]** - 网络适配器的已配置速度和双工
- **[vSwitch]** - 网络适配器所关联的 vSwitch
- **[观察到的 IP 范围 (Observed IP ranges)]** - 网络适配器可访问的 IP 地址
- **[支持 LAN 唤醒 (Wake on LAN supported)]** - 网络适配器支持 LAN 唤醒的能力。

虚拟机的虚拟网络配置

VI Client 添加网络向导可指导您完成创建虚拟机可连接的虚拟网络的任务。任务包括：

- 设置虚拟机的连接类型
- 将虚拟网络添加到新的或现有的 vSwitch。

- 为网络标签和 VLAN ID 配置连接设置

有关为单一虚拟机配置网络连接的信息，请参见 *《基本系统管理指南》*。

设置虚拟机网络时，需要考虑是否在 ESX Server 3 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 - 即均位于第 2 层同一子网内。

ESX Server 3 不支持在不同的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在其被移至另一个网络后不再可被访问的系统和资源。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的需求的智能交换机，当地址解析协议 (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。如果有一个或多个网络适配器连接到 vSwitch，则 vSwitch 仅可将数据传输至外部网络。当两个或多个适配器连接至一个单一 vSwitch 时，它们便以透明方式进行组合。

为虚拟机创建或添加虚拟网络

1 登录 VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[网络 (Networking)]**。

虚拟机交换机将出现在包括详细布局的概述中。

3 在页面右侧，单击 **[添加网络连接 (Add Networking)]**。

注意 添加网络向导用于添加新的端口和端口组。

4 接受默认的连接类型 **[虚拟机 (Virtual Machines)]**。

通过 **[虚拟机 (Virtual Machines)]**，可添加带标签的网络，以处理虚拟机网络流量。

5 单击 **[下一步 (Next)]**。

6 选择 **[创建虚拟交换机 (Create a virtual switch)]**。

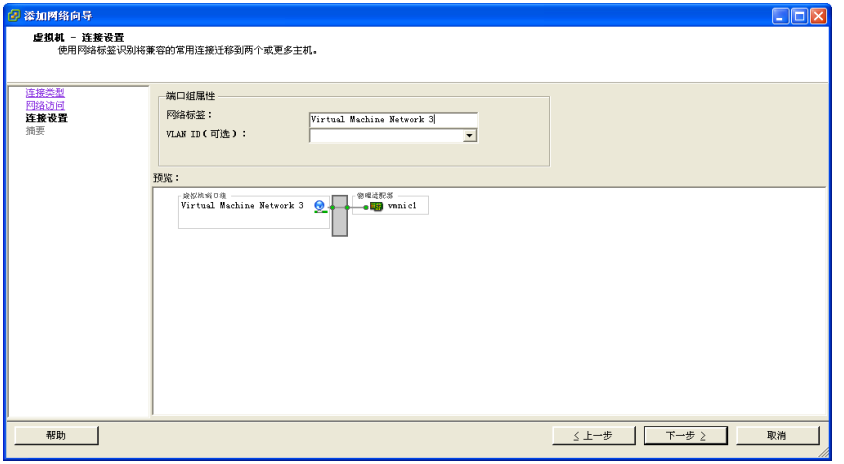
创建新的 vSwitch 不一定要具有以太网适配器。

如果创建的 vSwitch 不带物理网络适配器，则该 vSwitch 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 vSwitch 上的虚拟机均无法通过此 vSwitch 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 vSwitch。

更改将出现在 **[预览 (Preview)]** 窗格中。

7 单击 **[下一步 (Next)]**。

8 在 **[端口组属性 (Port Group Properties)]** 组中，输入用于识别所创建的端口组的网络标签。



使用网络标签识别两台或多台主机共用的迁移兼容连接。

9 如果您使用了 VLAN，则需要在 **[VLAN ID]** 字段中输入一个介于 1 和 4094 之间的数字。

如果不能确定输入的值，请将此字段留空或者询问网络管理员。

如果输入 0 或将此字段留空，端口组仅可检测到未标记的 （非 VLAN）流量。如果输入 4095，端口组可检测到任何 VLAN 上的流量，而 VLAN 标志仍保持原样。

10 单击 **[下一步 (Next)]**。

11 确定 vSwitch 配置正确之后，单击 **[完成 (Finish)]**。

注意 要启用故障切换 （网卡绑定），请将两个或更多适配器绑定到同一交换机。如果某个上行链路适配器出现故障，那么网络流量会路由至交换机所连接的另一个适配器。网卡绑定要求两台以太网设备位于同一以太网广播域中。

VMkernel 网络配置

在主机之间移动虚拟机称为迁移。迁移已启动的虚拟机称为 *VMotion*。使用 VMotion 迁移仅限于高兼容性系统之间的迁移，确保在迁移虚拟机时不会出现停机。必须正确设置 VMkernel 网络连接堆栈，以容纳 VMotion。

IP 存储器 指将 TCP/IP 网络通信用作其基础的任何形式的存储器，包括用于 ESX Server 3 的 iSCSI 和 NFS。由于这些存储器类型都是基于网络的，因此均可使用相同的 VMkernel 接口和端口组。

VMkernel 提供的网络服务（iSCSI、NFS 和 VMotion）使用 VMkernel 中的 TCP/IP 堆栈。此 TCP/IP 堆栈与用于服务控制台中的 TCP/IP 堆栈完全隔离。所有 TCP/IP 堆栈均通过连接至一个或多个 vSwitches 上的一个或多个端口组而访问不同的网络。

VMkernel 级别的 TCP/IP 堆栈

VMware VMkernel TCP/IP 网络连接堆栈已得到扩展，可用以下方式处理 iSCSI、NFS 和 VMotion：

- 作为虚拟机数据存储的 iSCSI
- 用于直接装载 .ISO 文件的 iSCSI， .ISO 文件向虚拟机显示为 CD-ROM
- 作为虚拟机数据存储的 NFS
- 用于直接装载 `.ISO` 文件的 NFS， .ISO 文件向虚拟机显示为 CD-ROM
- 通过 VMotion 进行迁移

注意 ESX Server 3 在 TCP/IP 上仅支持第 3 版本的 NFS。

配置的影响和准则

配置 VMkernel 网络时请参考以下准则：

- 在安装期间分配至服务控制台的 IP 地址必须不同于从 VMware Infrastructure Client 的 **[配置 (Configuration)] > [网络 (Networking)]** 选项卡分配给 VMkernel 的 TCP/IP 堆栈的 IP 地址。
- 与其他 VMkernel 服务不同， iSCSI 配有一个服务控制台组件，因此，用于到达 iSCSI 目标的网络必须可访问服务控制台和 VMkernel TCP/IP 堆栈。
- 为 ESX Server 3 主机配置软件 iSCSI 之前，需要通过启用 iSCSI 软件客户端服务而打开防火墙端口。请参见 “为支持的服务和管理代理打开防火墙端口”（第 171 页）。

设置 VMkernel

1 登录 VMware VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[网络 (Networking)]**。

3 单击 **[添加网络连接 (Add Networking)]**。

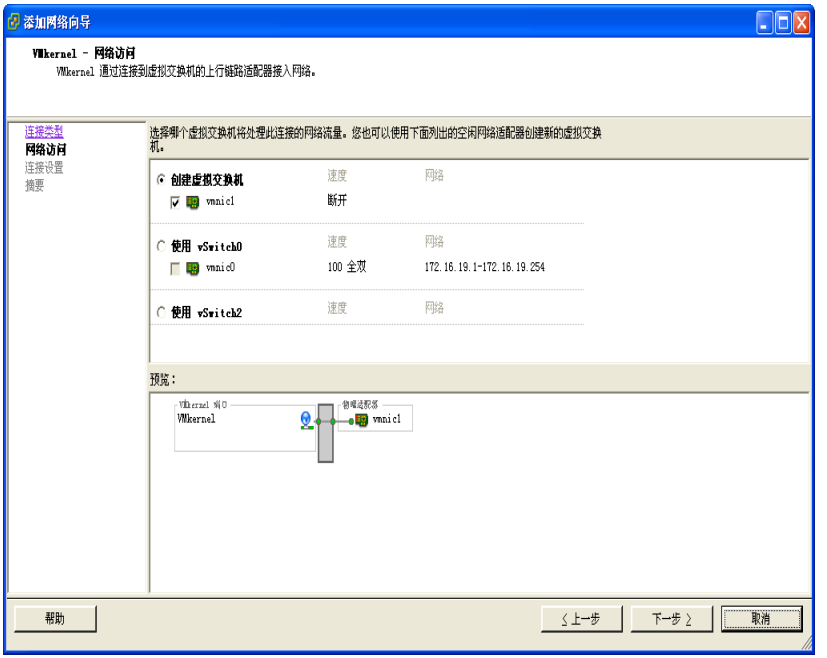
4 选择 **[VMkernel]**，然后单击 **[下一步 (Next)]**。

选择 **[VMotion 和 IP 存储器 (VMotion and IP Storage)]**，即可将为 VMotion 和 IP 存储器 （NFS 或 iSCSI）运行服务的 VMkernel 连接至物理网络。

此时将出现 **[网络访问 (Network Access)]** 页面。

5 选择要使用的 vSwitch，或选择 **[创建虚拟交换机 (Create a virtual switch)]** 以新建 vSwitch。

6 为 vSwitch 将使用的网络适配器选择复选框。



选择将出现在 **[预览 (Preview)]** 窗格中。

为每个 vSwitch 选择适配器，以便使通过适配器连接的虚拟机或其他设备可到达正确的以太网分段。如果 **[创建虚拟交换机 (Create a new virtual switch)]** 下方未出现适配器，则表明系统中所有网络适配器均被现有 vSwitches 占用。可以在不使用网络适配器的情况下创建新的 vSwitch，也可以选择现有 vSwitch 所使用的网络适配器。

有关在 vSwitches 之间移动网络适配器的信息，请参见 “添加上行链路适配器”（第 40 页）。

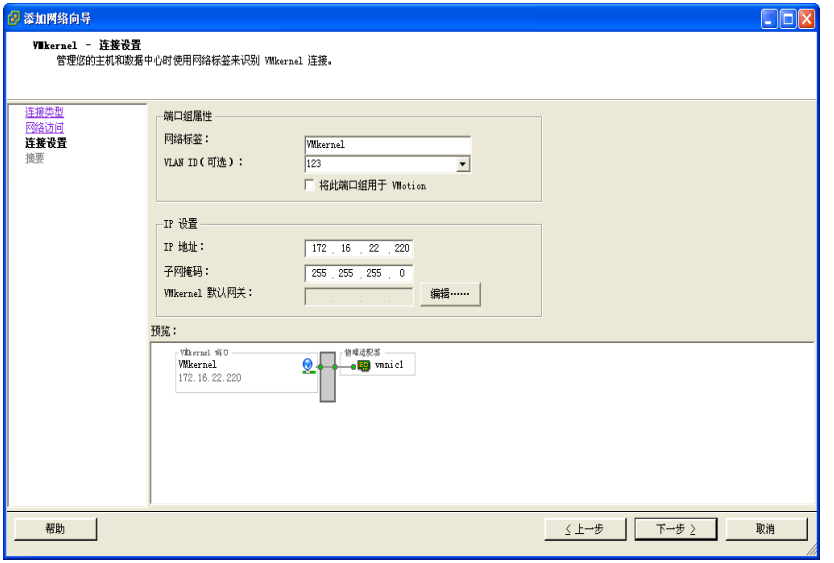
7 单击 **[下一步 (Next)]**。

8 在 **[端口组属性 (Port Group Properties)]** 区域中，选择或输入网络标签和 VLAN ID。

- **[网络标签 (Network Label)]** - 用于识别所创建的端口组的名称。此标签是在配置诸如 VMotion 和 IP 存储器之类的 VMkernel 服务时配置要连接至此端口组的虚拟适配器时指定的。
- **[VLAN ID]** - 用于识别端口组网络流量将使用的 VLAN。

9 选择 **[将此端口组用于 VMotion (Use this port group for VMotion)]** 以启用此端口组，此端口组向另一个 ESX Server 将其本身显示为应在其中发送 VMotion 流量的网络连接。

仅可为每个 ESX Server 3 主机的一个 VMotion 和 IP 存储器端口组启用此属性。如果未为任何端口组启用此属性，则不可通过 VMotion 向此主机进行迁移。



10 在 **[IP 设置 (IP Settings)]** 组中，单击 **[编辑 (Edit)]** 以便为诸如 VMotion、NAS 和 iSCSI 之类的 VMkernel 服务设置 **[VMkernel 默认网关 (VMkernel Default Gateway)]**。

注意 为所创建的端口设置默认网关。VirtualCenter 2 的行为与 VirtualCenter 1.x. 不同。必须使用有效的 IP 地址而不是虚拟的地址来配置 VMkernel IP 堆栈。

在 **[DNS 配置 (DNS Configuration)]** 选项卡上，默认情况下，主机名称输入在名称字段。如同域一样，在安装期间指定的 DNS 服务器地址也已预先选定。

在 **[路由 (Routing)]** 选项卡中，服务控制台和 VMkernel 均需要其自身的网关信息。连接至不在诸如服务控制台或 VMkernel 之类的 IP 子网上的计算机需要网关。

静态 IP 地址为默认值。

11 单击 **[确定 (OK)]**，然后单击 **[下一步 (Next)]**。

12 使用 **[上一步 (Back)]** 按钮进行更改。

13 检查在 **[即将完成 (Ready to Complete)]** 页面上做出的更改，单击 **[完成 (Finish)]**。

服务控制台配置

服务控制台和 VMkernel 均使用了虚拟以太网适配器连接至 vSwitch 并到达 vSwitch 所服务的网络。

基本服务控制台配置任务

两种常见的服务控制台配置更改为：更改网卡及为使用中的现有网卡更改设置。

如果仅出现一个服务控制台连接，则不允许更改服务控制台配置。对于新的连接，请将网络设置更改为使用其他的网卡。在确保新的连接运行正常之后，移除旧的连接。正在切换至新的网卡。

注意 在 ESX Server 3 中最多可创建 16 个服务控制台端口。

配置服务控制台网络

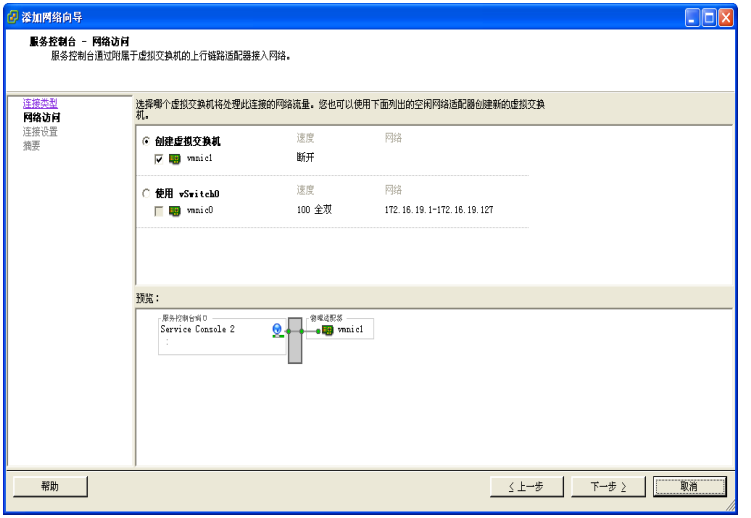
1 登录 VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[网络 (Networking)]**。

3 单击 **[添加网络连接 (Add Networking)]**。

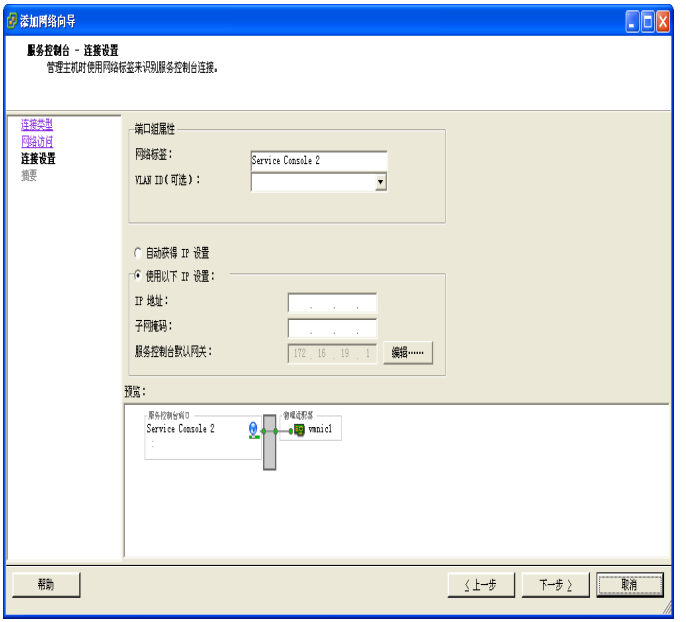
4 选择 **[连接类型 (Connection Types)]** 页面上的 **[服务控制台 (Service Console)]**，然后单击 **[下一步 (Next)]**。



5 选择要用于网络访问的 vSwitch，或选择 **[创建新的 vSwitch (Create a new vSwitch)]** 并单击 **[下一步 (Next)]**。

如果 **[创建虚拟交换机 (Create a new virtual switch)]** 组下方未出现适配器，则表明系统中所有网络适配器均被现有 vSwitch 占用。有关在 vSwitches 之间移动网络适配器的信息，请参见 “添加上行链路适配器”（第 40 页）。

6 在 **[端口组属性 (Port Group Properties)]** 组中，选择或输入 **[网络标签 (Network Label)]** 和 **[VLAN ID]**。



较新的端口和端口组将出现在 vSwitch 图的顶部。

7 输入 **[IP 地址 (IP Address)]** 和 **[子网掩码 (Subnet Mask)]**，或为 IP 地址和子网掩码选择 **[自动获得 IP 设置 (Obtain IP setting automatically)]**。

8 单击 **[编辑 (Edit)]**，设置 **[服务控制台默认网关 (Service Console Default Gateway)]**。

请参见 “设置默认网关”（第 34 页）。

9 单击 **[下一步 (Next)]**。

10 检查信息，并单击 **[完成 (Finish)]**。

配置服务控制台端口

1 登录 VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[网络 (Networking)]**。

3 在页面的右侧，找到要编辑的 vSwitch，然后单击该 vSwitch 的 **[属性 (Properties)]**。

4 在 **[vSwitch 属性 (vSwitch Properties)]** 对话框中，单击 **[端口 (Ports)]** 选项卡。

5 选择 **[服务控制台 (Service Console)]**，然后单击 **[编辑 (Edit)]**。

此时会出现一个警告对话框，说明修改服务控制台连接可能会断开所有管理代理的连接。

6 要继续服务控制台配置，请单击 **[继续修改此连接 (Continue modifying this connection)]**。

7 根据需要编辑端口属性、 IP 设置和有效策略。

8 单击 **[确定 (OK)]**。

每个 TCP/IP 堆栈只能配置一个默认网关。

设置默认网关

1 登录 VMware VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[DNS 和路由 (DNS and Routing)]**。

此时将出现 **[DNS 和路由 (DNS and Routing)]** 面板。

3 单击 **[属性 (Properties)]**。

在 **[DNS 配置 (DNS Configuration)]** 选项卡上，默认情况下，主机名称输入在名称字段。原先在安装期间选定的 DNS 服务器地址和域也预先选定。

在 **[路由 (Routing)]** 选项卡上，服务控制台和 VMkernel 通常并未连接至同一网络，因此需要其各自的网关信息。连接的计算机与服务控制台或 VMkernel 接口位于不同 IP 子网上时需要网关。

注意 所有的 NAS 和 iSCSI 服务器均应可由默认网关访问，或与相关的 vSwitch 处在同一广播域上。

对于服务控制台，仅当两个或多个网络适配器使用同一子网时才需要网关设备。网关设备确定将用于默认路由的网络适配器。

4 单击 **[路由 (Routing)]** 选项卡。

5 设置 VMkernel 默认网关。

小心 错误配置可导致 UI 无法与主机连接，在此情况下，必须从服务控制台的命令行重新对主机进行配置。保存更改之前，请确保网络设置正确。

6 单击 **[确定 (OK)]**。

显示服务控制台信息

1 单击信息图标，以显示服务控制台信息。

2 单击 **[X]**，关闭信息弹出窗口。

对服务控制台使用 DHCP

大多数情况下，应对服务控制台使用静态 IP 地址。如果 DNS 服务器可将服务控制台的主机名称映射至动态生成的 IP 地址，也可将服务控制台设置为使用动态地址 DHCP。

如果 DNS 服务器无法将主机名称映射至其 DHCP 生成的 IP 地址，请确定服务控制台的数字 IP 地址，并在访问主机时使用该数字地址。

当 DHCP 租期到期或系统重启时，数字 IP 地址可能会发生变化。因此，VMware 建议不要将 DHCP 用于服务控制台，除非 DNS 服务器可处理主机名称转换。

3 高级网络

本章指导您学习 ESX Server 3 环境下的高级网络主题并论述如何设置和更改高级网络配置选项。

本章将讨论以下主题：

虚拟交换机属性和策略

本节会指导您配置虚拟交换机属性和在虚拟交换机级别设置的网络策略。

虚拟交换机属性

虚拟交换机设置可控制端口的 vSwitch 层面默认值，而每个 vSwitch 的端口组设置均可替代这些值。

编辑虚拟交换机属性

编辑 vSwitch 属性包括：

- 配置端口
- 配置上行链路网络适配器

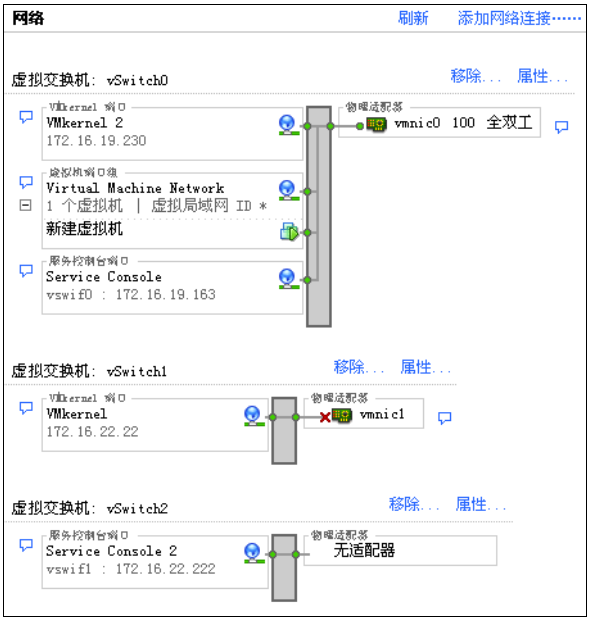
编辑 vSwitch 的端口数量

1 登录 VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[网络 (Networking)]**。

3 在页面的右侧，找到要编辑的 vSwitch。



4 单击该 vSwitch 的 **[属性 (Properties)]**。

5 单击 **[端口 (Ports)]** 选项卡。

6 在 **[配置 (Configuration)]** 列表中选择 vSwitch 项目，然后单击 **[编辑 (Edit)]**。

7 单击 **[常规 (General)]** 选项卡以设置端口数量。

8 从下拉菜单中选择您要使用的端口数量。

9 单击 **[确定 (OK)]**。

通过更改速度来配置上行链路网络适配器

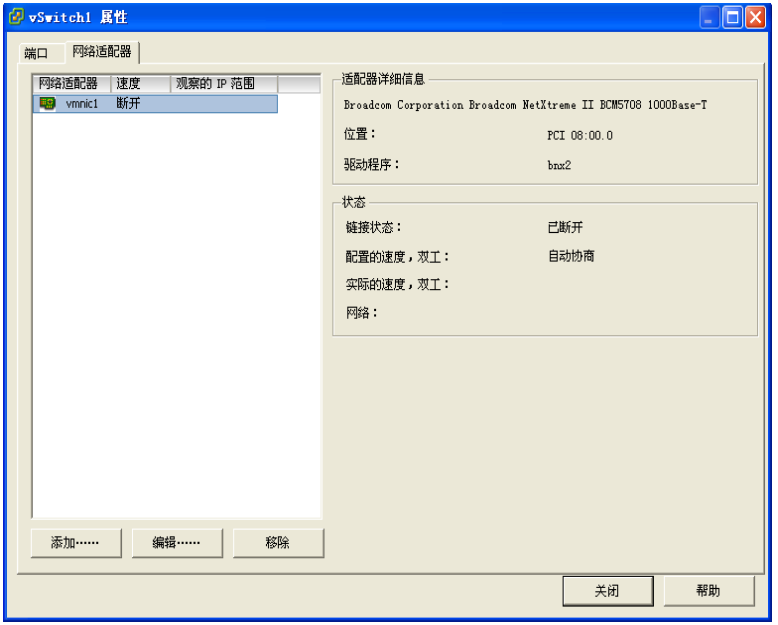
1 登录 VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[网络 (Networking)]**。

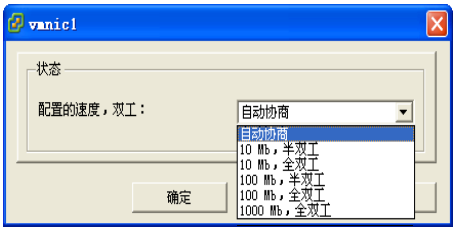
3 选择 vSwitch 并单击 **[属性 (Properties)]**。

4 单击 **[网络适配器 (Network Adapters)]** 选项卡。



5 要更改网络适配器的已配置速度和双工值，请选择网络适配器并单击 **[编辑 (Edit)]**。

此时将显示 **[状态 (Status)]** 对话框。默认值是 **[自动协商 (Autonegotiate)]**，这通常是正确的选择。



6 要手动选择连接速度，请从下拉菜单中选择速度 / 双工。

如果网卡和物理交换机在协商正确的连接速度时可能失败，请手动选择连接速度。速度和双工不匹配的表现包括低带宽，或者根本没有链路连接。

适配器及其连接的物理交换机端口必须设置为相同值，即两者可设置为 ″auto″ 和 ″auto″ 或 ″ND″ 和 ″ND″，其中 ND 表示速度和双工，但两者不能设置为 ″auto″ 和 ″ND″。

7 单击 **[确定 (OK)]**。

添加上行链路适配器

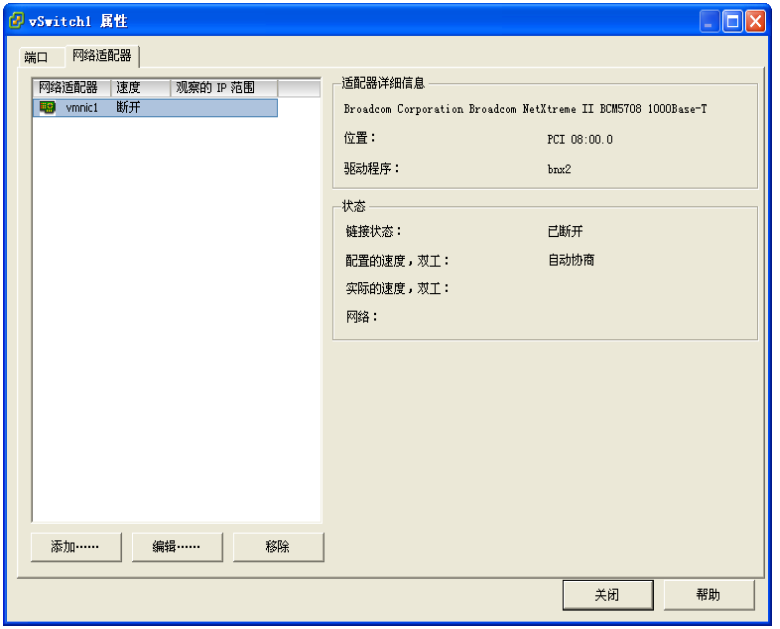
1 登录 VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[网络 (Networking)]**。

3 选择 vSwitch 并单击 **[属性 (Properties)]**。

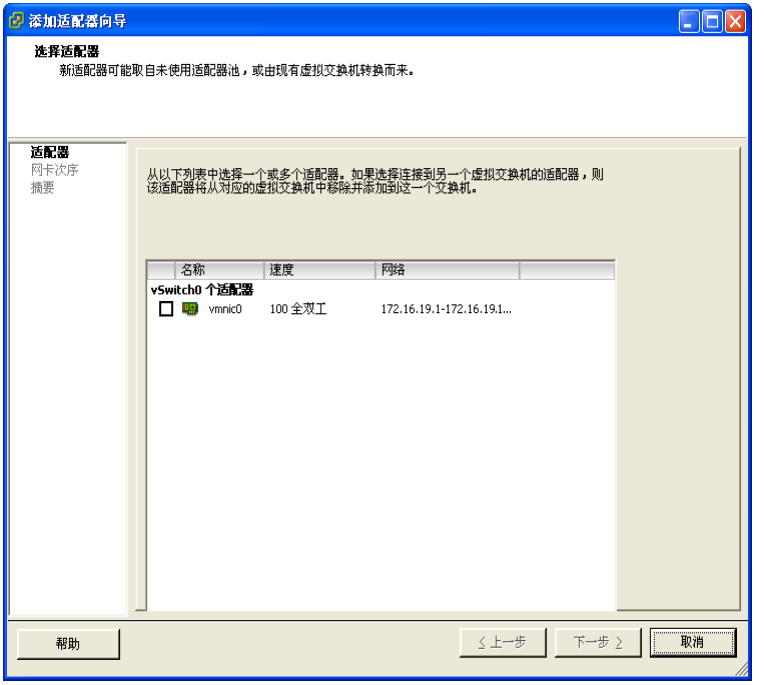
4 在 **[属性 (Properties)]** 对话框中，单击 **[网络适配器 (Network Adapters)]** 选项卡。



5 单击 **[添加 (Add)]** 以启动添加适配器向导。

可以将多个适配器与一个 vSwitch 关联以提供网卡绑定。此组可以共享流量并提供故障切换。

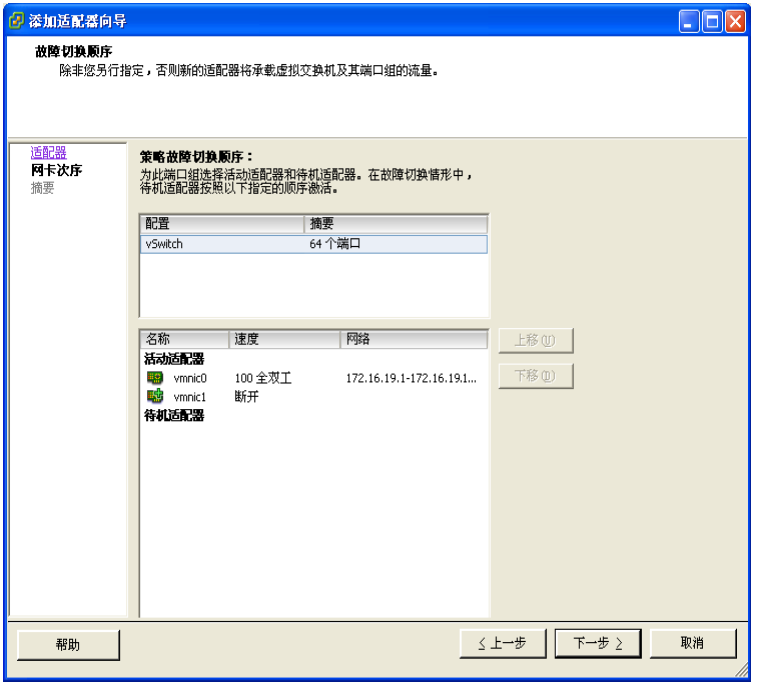
小心 错误配置可导致 VI Client 不能与主机连接。



6 从列表中选择一个或多个适配器，然后单击 **[下一步 (Next)]**。

7 要对网卡排序，请选择网卡，然后单击 **[上移 (Move Up)]** 和 **[下移 (Move Down)]** 将其上移或下移到适当的类别中 （“活动”或 “待机”）。

- **[活动适配器 (Active Adapters)]** - vSwitch 使用的适配器。
- **[待机适配器 (Standby Adapters)]** - 当一个或多个活动适配器出现故障时转为活动状态的适配器。



8 单击 **[下一步 (Next)]**。

9 查看 **[适配器摘要 (Adapter Summary)]** 页上的信息，单击 **[上一步 (Back)]** 以更改条目，然后单击 **[完成 (Finish)]**。

此时将重新出现网络适配器列表，显示 vSwitch 目前要求使用的适配器。

10 单击 **[关闭 (Close)]** 以退出 **[vSwitch 属性 (vSwitch Properties)]** 对话框。

在 **[配置 (Configuration)]** 选项卡的 **[网络 (Networking)]** 部分中将按指定的顺序和类别显示网络适配器。

Cisco 发现协议

Cisco 发现协议 (CDP) 允许 ESX Server 3 管理员决定 Cisco 交换机的哪一个端口与指定的 vSwitch 相连。当特定的 vSwitch 启用了 CDP 时，可以从 VI Client 查看 Cisco 交换机的属性 （例如设备 ID、软件版本和超时）。

可使用服务控制台命令行界面来启用 CDP 。

启用 CDP

1 直接登录 ESX Server 3 主机的控制台。

2 使用命令 `esxcfg-vswitch -b <vSwitch>` 查看 vSwitch 当前的 CDP 模式。

如果禁用了 CDP，则模式将显示为 **[关闭 (down)]**。

3 使用命令 `esxcfg-vswitch -B <mode> <vSwitch>` 来更改 CDP 模式。

可用的 CDP 模式为：

- **[关闭 (down)]** - 禁用 CDP。
- **[监听 (listen)]** - ESX Server 3 检测并显示与关联的 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 vSwitch 的信息。
- **[播发 (advertise)]** - ESX Server 3 将有关 vSwitch 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。
- **[同时 (both)]** - ESX Server 3 检测并显示与关联的 Cisco 交换机相关的信息，且将有关 vSwitch 的信息提供给 Cisco 交换机管理员。

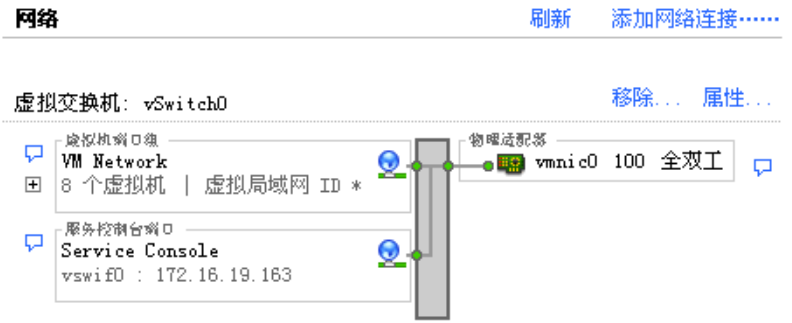
从 VI Client 查看 Cisco 交换机信息

1 将 vSwitch 的 CDP 模式设置为 **[同时 (both)]** 或 **[监听 (listen)]**。

2 登录 VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

3 依次单击 **[配置 (Configuration)]** 选项卡和 **[网络 (Networking)]**。



4 单击 vSwitch 右侧的信息图标。

Cisco 发现协议 ×

属性	
版本	0
超时	0
生存时间	120
例子	4348
设备 ID	emc-server-3
地址	172.16.250.23
端口 ID	FastEthernet0/8
软件版本	Cisco IOS Software,
硬件平台	cisco WS-C2960-24TT-L
IP 前缀	0.0.0.0
IP 前缀长度	0
VLAN	190
全双工	有效
MTU	0
系统名称	
原有系统	
管理地址	172.16.250.23
位置	
CDP 设备功能	
路由器	无效
透明网桥	无效
源路由网桥	无效
网络交换机	有效
主机	无效
IGMP 已启用	有效
中继器	无效

注意 由于 CDP 播发 Cisco 设备信息一般每分钟进行一次，因此从启用 ESX Server 3 的 CDP 到从 VI Client 获得 CDP 数据间可能会有较长延迟。

虚拟交换机策略

通过选择 **[端口 (Ports)]** 选项卡顶部的 vSwitch，然后单击 **[编辑 (Edit)]** 便可以应用一系列 vSwitch 层面的策略。

要替代端口组的任何设置，请选择端口组并单击 **[编辑 (Edit)]**。对于 vSwitch 层面配置的任何更改将应用到该 vSwitch 上的任何端口组，但不包括那些由端口组替代的配置选项。

vSwitch 策略包括：

- 第 2 层安全策略
- 流量调整策略
- 负载平衡和故障切换策略

第 2 层安全策略

第 2 层是数据链接层。第 2 层安全策略的三个元素是杂乱模式、 MAC 地址更改和伪信号。

在非杂乱模式下，客户机适配器将仅侦听其自身 MAC 地址上的流量。在杂乱模式中，它可侦听所有数据包。默认情况下，客户机适配器设置为非杂乱模式。

有关安全的详细信息，请参见 “确保虚拟交换机端口安全”（第 181 页）。

编辑第 2 层安全策略

1 登录 VMware VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

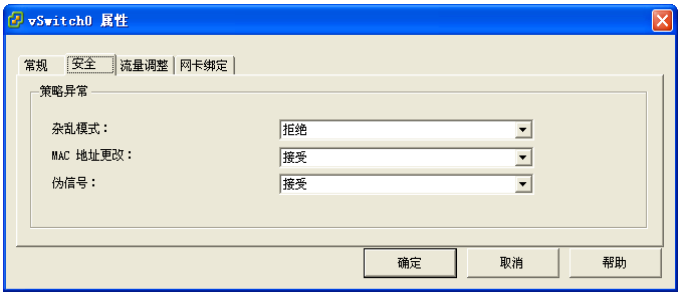
2 依次单击 **[配置 (Configuration)]** 选项卡和 **[网络 (Networking)]**。

3 要编辑 vSwitch 的第二层安全策略，请单击 **[属性 (Properties)]**。

4 在 vSwitch 的 **[属性 (Properties)]** 对话框中，单击 **[端口 (Ports)]** 选项卡。

5 选择 vSwitch 项目，并单击 **[编辑 (Edit)]**。

6 在 vSwitch 的 [属性 (Properties)] 对话框中，单击 **[安全 (Security)]** 选项卡。



默认情况下，**[杂乱模式 (Promiscuous Mode)]** 设置为 **[拒绝 (Reject)]**、**[MAC 地址更改 (MAC Address Changes)]** 和 **[伪信号 (Forced Transmits)]** 设置为 **[接受 (Accept)]**。

此处的策略将应用到 vSwitch 上的所有虚拟适配器，除非虚拟适配器的端口组指定了策略异常。

7 在 **[策略异常 (Policy Exceptions)]** 窗格中，选择是拒绝还是接受第 2 层安全策略异常：

- **[杂乱模式 (Promiscuous Mode)]**
  - **[拒绝 (Reject)]** - 将客户机适配器置于杂乱模式不会对适配器接收哪些帧产生任何影响。
  - **[接受 (Accept)]** - 将客户适配器置于杂乱模式使其检测经过 vSwitch 的所有帧，这些帧是适配器所连端口组的 VLAN 策略所允许的帧。
- **[MAC 地址更改 (MAC Address Changes)]**
  - **[拒绝 (Reject)]** - 如果将 **[MAC 地址更改 (MAC Address Changes)]** 设置为 **[拒绝 (Reject)]**，并且客户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，则将丢失所有入站帧。

    如果客户操作系统将 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。
  - **[接受 (Accept)]** - 从客户操作系统更改 MAC 地址具有特别作用：将接收传入新 MAC 地址的帧。
- **[伪信号 (Forced Transmits)]**
  - **[拒绝 (Reject)]** - 如果具有源 MAC 地址的出站帧与适配器上当前设置的出站帧不同，那么这些出站帧会丢失。

- **[接受 (Accept)]** - 不执行筛选，所有出站帧均可通过。

8 单击 **[确定 (OK)]**。

流量调整策略

ESX Server 3 通过为三个出站流量特性指定参数来调整流量：平均带宽、脉冲大小和带宽峰值。可以通过 VI Client 设置这些特性的值，为每个端口组建立流量调整策略。

- **[平均带宽 (Average Bandwidth)]** 指定在已过去的时间内每秒允许通过 vSwitch 的平均位数，即允许的平均负载。
- **[脉冲大小 (Burst Size)]** 可设置一次脉冲中允许的最大字节数量。如果脉冲超过脉冲大小参数，将对剩余数据包进行排队，等待稍后传输。如果队列已满，将丢弃数据包。指定了这两个特性的值即指明希望 vSwitch 在正常运作期间处理的负载。
- **[带宽峰值 (Peak Bandwidth)]** 是 vSwitch 在不丢失数据包的前提下可负担的最大带宽。如果流量超过指定带宽峰值，将对剩余数据包进行排队，等连接上的流量恢复至平均值且有足够空闲周期处理排队的数据包后再进行传输。如果队列已满，将丢弃数据包。即使由于连接已闲置而获得了空闲带宽，在流量恢复至允许的平均负载之前，带宽峰值参数仍会将传输限制在峰值以下。

编辑流量调整策略

1 登录 VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[网络 (Networking)]**。

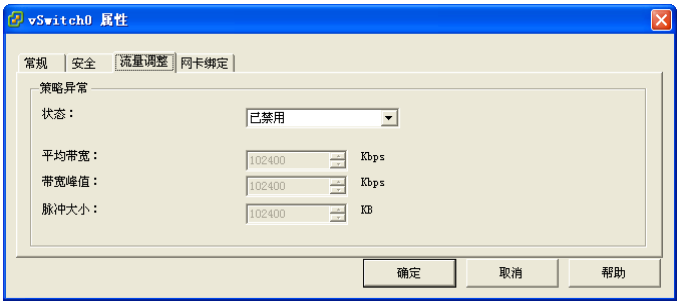
3 选择 vSwitch 并单击 **[属性 (Properties)]**。

4 在 **[vSwitch 属性 (vSwitch Properties)]** 对话框中，单击 **[端口 (Ports)]** 选项卡。

5 选择 vSwitch，并单击 **[编辑 (Edit)]**。

6 单击 **[流量调整 (Traffic Shaping)]** 选项卡。

禁用流量调整时，可调功能将呈灰色。如果启用流量调整，可以选择性地在端口组级别重写所有流量调整功能。



此策略将应用到端口组连接的单个虚拟机适配器，而不是整个 vSwitch。

[状态 (Status)] - 如果在 **[状态 (Status)]** 字段中启用了策略异常，则设置了网络带宽分配量的限值，每个虚拟适配器会将此分配量关联到特定的端口组。如果禁用策略，则在默认情况下，服务将能够自由、顺畅地连接到物理网络。

剩余的字段定义网络流量参数：

- **[平均带宽 (Average Bandwidth)]** 是一段特定时间上的测量值。
- **[带宽峰值 (Peak Bandwidth)]** 是允许的最大带宽值，并且不得小于平均带宽。此参数限制脉冲期间的最大带宽。
- **[脉冲大小 (Burst Size)]** 是指定脉冲大小（以千字节 (KB) 为单位）的值。此参数控制可在一个脉冲内发送的数据量。

负载平衡和故障切换策略

负载平衡和故障切换策略允许您确定如何在适配器之间分配网络流量，以及如何通过配置以下参数，在适配器发生故障时重新路由流量：

- **[负载平衡策略 (Load Balancing policy)]** 确定出站流量在分配给 vSwitch 的网络适配器上的分布方式。

  注意 入站流量由物理交换机上的负载平衡策略控制。

- **[故障切换检测 (Failover Detection)]**：链接状态和信标探测
- **[网络适配器顺序 (Network Adapter Order)]** （活动或待机）

编辑故障切换和负载平衡策略

1 登录 VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[网络 (Networking)]**。

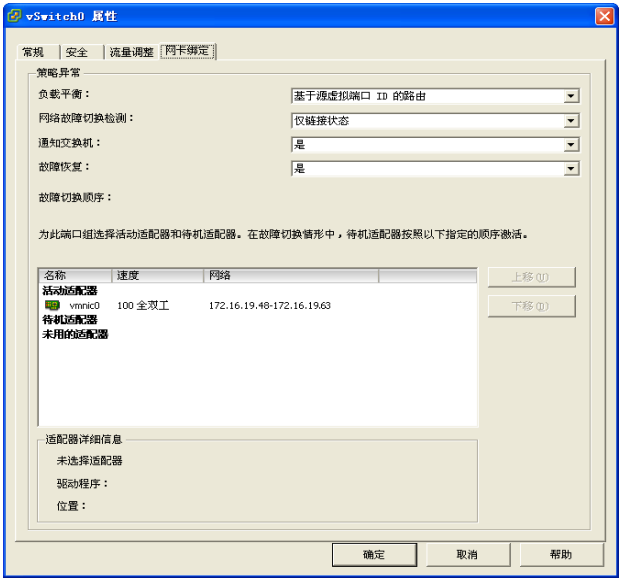
3 选择一台 vSwitch 并单击 **[编辑 (Edit)]**。

4 在 **[vSwitch 属性 (vSwitch Properties)]** 对话框中，单击 **[端口 (Ports)]** 选项卡。

5 要编辑 vSwitch 的 **[故障切换和负载平衡 (Failover and Load Balancing)]** 值，请选择 vSwitch 项目并单击 **[属性 (Properties)]**。

6 单击 **[网卡绑定 (NIC Teaming)]** 选项卡。

可以在端口组级别重写故障切换顺序。默认情况下，新适配器对于所有策略都是活动的。除非另行指定，否则新适配器将承载 vSwitch 及其端口组的流量。



7 在 **[策略异常 (Policy Exceptions)]** 组中：

- **[负载平衡 (Load Balancing)]** - 指定如何选择上行链路。
  - **[基于源端口 ID 的路由 (Route based on the originating port ID)]** - 选择基于虚拟端口的上行链路，流量正是通过此端口进入虚拟交换机。

- **[基于 IP 哈希的路由 (Route based on ip hash)]** - 选择基于每个数据包的源和目标 IP 地址哈希的上行链路。对于非 IP 数据包，偏移量中的任何值都将用于计算哈希值。
- **[基于源 MAC 哈希值的路由 (Route based on source MAC hash)]** - 选择基于源以太网哈希的上行链路。
- **[使用明确故障切换顺序 (Use explicit failover order)]** - 始终使用活动适配器列表中通过故障切换检测标准的最高顺序的上行链路。

注意 基于 IP 的成组要求为物理交换机配置以太通道。对于其他所有选项，应禁用以太通道。

- **[网络故障切换检测 (Network Failover Detection)]** - 为故障切换检测指定使用方法。
  - **[仅链接状态 (Link Status only)]** - 仅依靠网络适配器提供的链接状态。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，配置了错误的 VLAN 中，或者在物理交换机的另一端拔掉线缆）。
  - **[信标探测 (Beacon Probing)]** - 发出并监听组中所有网卡上的信标探测，使用此信息并结合链接状态来确定链接故障。该选项可检测上述许多仅通过链接状态无法检测到的故障。
- **[通知交换机 (Notify Switches)]** - 选择 **[是 (Yes)]** 或 **[否 (No)]** 以确定在故障切换时是否通知交换机。

  如果选择 **[是 (Yes)]**，则每当虚拟网卡连接到 vSwitch 或虚拟网卡的流量因故障切换事件而由小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，为使在出现故障切换以及使用 VMotion 进行迁移时的延迟最短，最好使用此过程。

  注意 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。以多播模式使用网络负载平衡时不存在此问题。

- **[故障恢复 (Failback)]** - 选择 **[是 (Yes)]** 或 **[否 (No)]** 以禁用或启用故障恢复。

  此选项决定物理适配器从故障中恢复后将如何返回到活动任务。如果故障恢复设置为 **[否 (No)]**，则适配器将在恢复后立即返回到活动任务，替换接替其位置的待机适配器 （如果有）。如果故障恢复设置为 **[是 (Yes)]** （默认），则即使发生故障的适配器已经恢复，它仍将保持非活动状态，直到当前有活动的适配器发生故障，要求替换。

- **[故障切换顺序 (Failover Order)]** - 指定如何为适配器分配工作负载。如果只需要使用一部分的适配器，保留另一部分以便应对发生故障时的紧急情况，则可以设置此条件，使用下拉菜单将适配器分为两组：
  - **[活动适配器 (Active Adapters)]** - 当网络适配器连接正常且处于活动状态时继续使用该适配器。
  - **[待机适配器 (Standby Adapters)]** - 当活动适配器的一个连接出现故障时使用该适配器。
  - **[未用的适配器 (Unused Adapters)]** - 不使用的适配器。

端口组配置

可以更改以下端口组配置：

- 端口组属性
- 带标记的网络策略

编辑端口组属性

1 登录 VMware VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[网络 (Networking)]**。

3 在窗口的右侧，单击网络的 **[属性 (Properties)]**。

4 单击 **[端口 (Ports)]** 选项卡。

5 选择端口组并单击 **[编辑 (Edit)]**。

6 在端口组的 **[属性 (Properties)]** 对话框中，单击 **[常规 (General)]** 选项卡以更改：

- **[网络标签 (Network Label)]** - 标识正在创建的端口组。当配置要附加到此端口组的虚拟适配器时，或者当配置虚拟机或 VMkernel 服务 （例如 VMotion 和 IP 存储器）时，请指定此标签。
- **[VLAN ID]** - 用于识别端口组网络流量所使用的 VLAN。

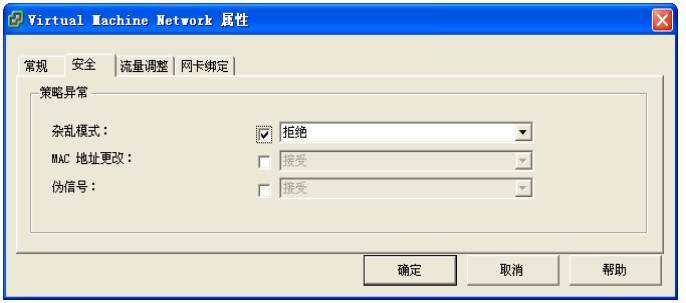
7 单击 **[确定 (OK)]**。

重写带标记的网络策略

1 要重写特定带标签网络的网络策略，请选择该网络，单击 **[编辑 (Edit)]**，然后单击 **[安全 (Security)]** 选项卡。

2 选中要重写的有标记网络策略的复选框。

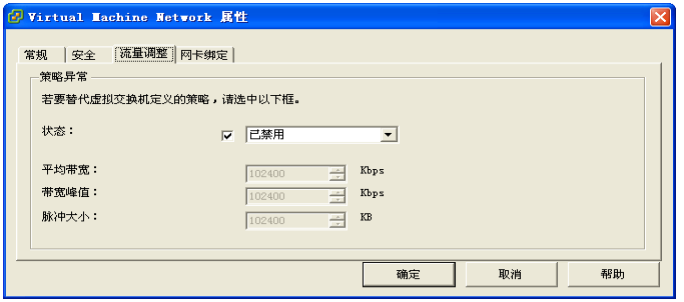
有关这些设置的详细信息，请参见 “第 2 层安全策略”（第 46 页）。



3 单击 **[流量调整 (the Traffic Shaping)]** 选项卡。

4 选择 **[状态 (Status)]** 旁边的复选框，并选择 **[已启用 (Enabled)]** 或 **[已禁用 (Disabled)]**。

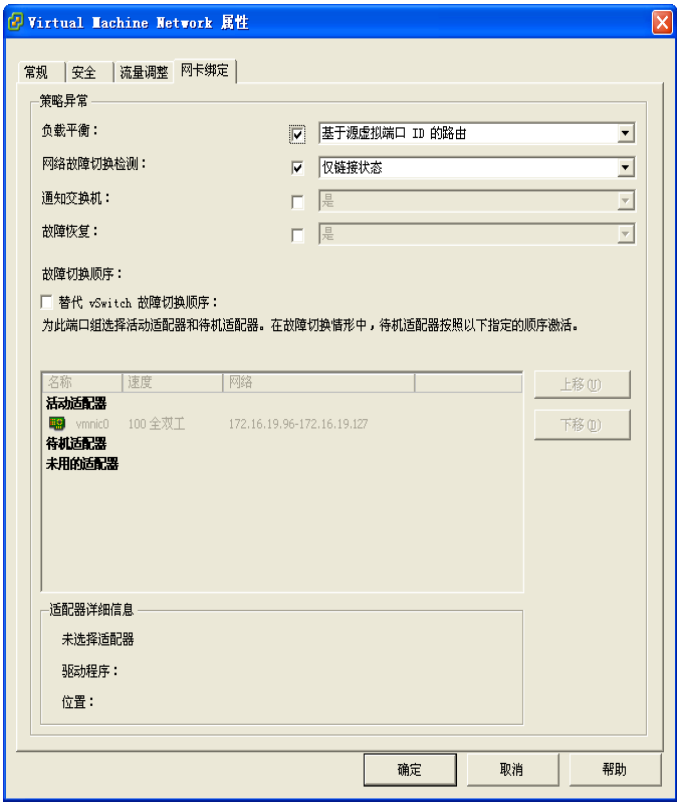
有关 **[状态 (Status)]** 设置的详细信息，请参见 “流量调整策略”（第 48 页）。



5 单击 **[网卡绑定 (NIC Teaming)]** 选项卡。

6 选中相关复选框以重写负载平衡或故障切换策略。

有关这些设置的详细信息，请参见 “负载平衡和故障切换策略”（第 49 页）。



7 单击 **[确定 (OK)]**。

DNS 和路由

通过 VI Client 配置 DNS 和路由

更改 DNS 和路由配置

1 登录 VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[DNS 和路由 (DNS and Routing)]**。

3 在窗口的右侧，单击 **[属性 (Properties)]**。

4 在 **[DNS 配置 (DNS Configuration)]** 选项卡中，为 **[名称 (Name)]** 和 **[域 (Domain)]** 字段输入值。

5 选择是自动获取 DNS 服务器地址，还是使用 DNS 服务器地址。

注意 仅当服务控制台可访问 DHCP 服务器时， DHCP 才是受支持的。换而言之，服务控制台必须配置了虚拟界面 (vswif) 并且连接到 DHCP 服务器驻留的网络。

6 指定用于查找主机的域。

7 在 **[路由 (Routing)]** 选项卡中，根据需要更改默认的网关信息。

只有当将服务控制台配置为连接到多个子网时才选择网关设备。

8 单击 **[确定 (OK)]**。

TCP 分段卸载和巨讯框

TCP 分段卸载 (TSO) 和巨讯框支持已添加至 ESX Server 3 版本 3.5 中的 TCP/IP 堆栈。必须使用命令行界面在服务器级别启用巨讯框才能配置每个 vSwitch 的 MTU 尺寸。TSO 在 Vmkernel 接口上默认启用，但必须在虚拟机级别启用。

启用 TSO

通过增强型 vmxnet 网络适配器实现的 TSO 支持可用于运行以下客户操作系统的虚拟机：

- 带 Service Pack 2 的 Microsoft Windows 2003 Enterprise Edition（32 位和 64 位）
- Red Hat Enterprise Linux 4 （64 位）
- Red Hat Enterprise Linux 5 （32 位和 64 位）
- SuSE Linux Enterprise Server 10 （32 位和 64 位）

要在虚拟机级别启用 TSO，必须将现有 vmxnet 或灵活虚拟网络适配器替换为增强型 vmxnet 虚拟网络适配器。这可能会导致虚拟网络适配器的 MAC 地址发生变化。

对虚拟机启用 TSO 支持。

1 登录 VI Client，从清单面板中选择虚拟机。

此时将出现该服务器的硬件配置页面。

2 单击 **[摘要 (Summary)]** 选项卡，然后单击 **[编辑设置 (Edit Settings)]**。

3 从 **[硬件 (Hardware)]** 列表中选择网络适配器。

4 记录网络适配器使用的网络设置和 MAC 地址。

5 单击 **[移除 (Remove)]**，从虚拟机中移除网络适配器。

6 单击 **[添加 (Add)]**。

7 选择 **[以太网适配器 (Ethernet Adapter)]**，然后单击 **[下一步 (Next)]**。

8 在 **[适配器类型 (Adapter Type)]** 组中，选择 **[增强型 vmxnet (Enhanced vmxnet)]**。

9 选择旧网络适配器使用的网络设置和 MAC 地址并单击 **[下一步 (Next)]**。

10 单击 **[完成 (Finish)]**。

11 单击 **[确定 (OK)]**。

12 如果未将虚拟机设置为在每次开机时升级 VMware Tools，则必须手动升级 VMware Tools。请参见 *《基本系统管理指南》*。

TSO 在 VMkernel 接口上默认启用。如果对特定 VMkernel 接口禁用了 TSO，启用 TSO 的唯一方式是删除此 VMkernel 接口，然后重新创建已启用 TSO 的 VMkernel 接口。

检查是否在 VMkernel 接口上启用了 TSO

1 直接登录 ESX Server 3 主机的控制台。

2 使用 `esxcfg-vmknic -l` 命令显示 VMkernel 接口的列表。

每个 TSO 启用的 VMkernel 接口应出现在将 **TSO MSS** 设置为 40960 的列表上。

如果未对特定 VMkernel 接口启用 TSO，启用 TSO 的唯一方式是删除此 VMkernel 接口，然后重新创建该 VMkernel 接口。请参见 “VMkernel 网络配置”（第 28 页）。

启用巨讯框

巨讯框允许 ESX Server 3 将较大的帧发送到物理网络上。要使巨讯框生效，网络必须端到端支持巨讯框。可支持最大值为 9 KB （9000 字节）的巨讯框。不支持带巨讯框的 iSCSI。

必须在 ESX Server 3 主机上通过命令行界面对每个 vSwitch 或 VMkernel 接口启用巨讯框。在启用巨讯框之前，请与硬件供应商核对，以确保您的物理网络适配器支持巨讯框。

创建已启用巨讯框的 vSwitch

1 直接登录 ESX Server 3 主机的控制台。

2 使用 `esxcfg-vswitch -m <MTU> <vSwitch>` 命令为 vSwitch 设置 MTU 尺寸。

通过此命令，可为此 vSwitch 上的所有上行链路设置 MTU。所设置的 MTU 尺寸应在连接至 vSwitch 的所有虚拟网络适配器中是最大的。

3 使用 `esxcfg-vswitch -l` 命令在主机上显示 vSwitch 列表，检查 vSwitch 的配置是否正确。

创建已启用巨讯框的 VMkernel 接口

1 直接登录 ESX Server 3 主机的控制台

2 使用 `esxcfg-vmknic -a -i <ip address> -n <netmask> -m <MTU> <prot group name>` 命令创建支持巨讯框的 VMkernel 连接。

3 使用 `esxcfg-vmknic -l` 命令显示 VMkernel 接口列表，检查启用了巨讯框的接口的配置是否正确。

注意 ESX Server 3 支持的最大 MTU 尺寸为 9000。

NetQueue 和网络性能

ESX Sever 3 中的 NetQueue 为网络适配器提供多个接收队列。这样可以使处理扩展到多个 CPU，提高网络的接收性能。

NetQueue 仅在运行 Neterion s2io 驱动程序的以下系统上可用：

- Dell 2950
- HP DL 585G2
- IBM 3850
- IBM 3950

在 ESX Server 3 主机上启用 NetQueue

1 登录 VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

2 单击 **[配置 (Configuration)]** 选项卡，然后单击 **[高级设置 (Advanced Settings)]**。

3 选择 **[VMkernel]**。

4 选择 **[VMkernel.Boot.netNetQueueEnable]** 并单击 **[确定 (OK)]**。

5 直接登录 ESX Server 3 主机的控制台。

6 使用 `esxcfg-module -e s2io` 命令来启用 s2io 模块。

7 使用 `esxcfg-module -s "intr_type=2 rx_ring_num=8" s2io` 命令在 s2io 模块上启用 NetQueue。

8 重新引导 ESX Server 3 主机。

在 s2io 模块上禁用 NetQueue 选项

直接登录到 ESX Server 3 主机的控制台并使用 `esxcfg-module -s "" s2io` 命令。

设置 MAC 地址

MAC 地址是为服务控制台、 VMkernel 和虚拟机所使用的虚拟网络适配器而生成的。大多数情况下，这些 MAC 地址都是合适的。但是，可能需要为虚拟网络适配器设置 MAC 地址，如在下列情况：

- 在不同物理服务器上的虚拟网络适配器由于共享同一子网且分配了相同的 MAC 地址而发生冲突时。
- 确保虚拟网络适配器始终拥有相同的 MAC 地址。

以下各节描述了 MAC 地址是如何生成的，以及如何为虚拟网络适配器设置 MAC 地址。

MAC 地址生成

虚拟机上的每个虚拟网络适配器都分配了其自身唯一的 MAC 地址。 MAC 地址是 6 个字节的数字。每一家网络适配器的制造商都分配了唯一的、 3 个字节的前缀，称为 OUI（组织唯一标识符），此标识符可用于生成唯一的 MAC 地址。

VMware 有以下 OUI：

- 一个用于生成 MAC 地址。
- 一个用于手动设置 MAC 地址。
- 还有一个以前用于旧虚拟机，但是 ESX Server 3 已经不再使用。

为每个虚拟网络适配器生成的 MAC 地址的前 3 个字节由该 OUI 组成。此 MAC 地址生成算法将计算其余 3 个字节。此算法保证 MAC 地址在虚拟机中是唯一的，并尝试在虚拟机之间提供唯一的 MAC 地址。

在同一子网中，每个虚拟机的网络适配器都拥有唯一的 MAC 地址。否则，它们将产生不可预知的行为。该算法将在任何服务器上，随时为运行的和已挂起的虚拟机的数量设置一个限值。当不同物理机上的虚拟机共享一个子网时，它也不会处理所有地址。

VMware 通用唯一标识符 (UUID) 生成的 MAC 地址已经通过冲突检查。生成的 MAC 地址是使用三个部分创建的：VMware OUI、物理 ESX Server 3 计算机的 SMBIOS UUID，以及基于 （为其生成 MAC 地址）实体名称的哈希。

在生成 MAC 地址后，除非虚拟机移动到其他位置，例如移动到服务器上的不同路径，否则地址不会更改。虚拟机的配置文件中的 MAC 地址将保存下来。在关闭的特定物理虚拟机上，已分配给运行中和暂停虚拟机的网络适配器的所有 MAC 地址不会对照运行中或暂停虚拟机的 MAC 地址进行检查。虽然虚拟机再次启动后有可能获得不同的 MAC 地址，但机率不大。这种地址的获取是由于该虚拟机再次启动时，与之前在其关闭时启动的虚拟机发生冲突而造成的。

设置 MAC 地址

要规避每台物理机 256 个虚拟网络适配器的限制，以及在虚拟机之间可能发生的 MAC 地址冲突，系统管理员可以手动分配 MAC 地址。 VMware 将此 OUI 用于手动生成的地址：00:50:56.

MAC 地址的范围是

```
00:50:56:00:00:00–00:50:56:3F:FF:FF
```

可以通过将下面的行添加到虚拟机配置文件中设置地址：

```
ethernet <number>.address = 00:50:56:XX:YY:ZZ
```

其中，<number> 表示以太网适配器的数量，XX 是 00 至 3F 间有效的十六进制数字，而 YY 和 ZZ 是 00 和 FF 之间有效的十六进制数字。但 XX 的值不得大于 3F，以避免与 VMware Workstation 和 VMware GSX Server 产品生成的 MAC 地址冲突。对于手动生成的 MAC 地址，其最大值为：

```
ethernet<number>.address = 00:50:56:3F:FF:FF
```

同时，必须在虚拟机配置文件中设置选项：

```
ethernet<number>.addressType="static"
```

由于 VMware ESX Server 3 虚拟机不支持任意 MAC 地址，因此必须使用以上格式。只要从硬编码的地址中为 `XX:YY:ZZ` 选择了唯一值，则在自动分配的 MAC 地址与手动分配的地址之间应该绝不会发生冲突。

使用 MAC 地址

可以更改已关闭虚拟机的虚拟网卡来使用通过 VI Client 静态分配的 MAC 地址。

设置 MAC 地址

1 登录 VI Client，从清单面板中选择虚拟机。

2 单击 **[摘要 (Summary)]** 选项卡，然后单击 **[编辑设置 (Edit Settings)]**。

3 从 **[硬件 (Hardware)]** 列表中选择网络适配器。

4 在 **[MAC 地址 (MAC Address)]** 组中，选择 **[手动 (Manual)]**。

5 输入所需静态 MAC 地址，然后单击 **[确定 (OK)]**。

网络最佳配置方案和提示

本节提供了以下相关信息：

- 网络最佳配置方案
- 网络提示

网络最佳配置方案

在配置网络时，请考虑这些最佳做法：

- 将网络服务彼此分开，以获得更好的安全性或更佳的性能。

  要使一组特定的虚拟机能够发挥最佳性能，请将它们置于单独的物理网卡上。这种分离方法可以使总网络工作负载的一部分更平均地分摊到多部 CPU 上。例如，隔离的虚拟机可更好地服务于来自 Web 客户端的流量。

- 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）可以满足以下建议的操作。

  - 使服务控制台处于其自己的网络中是确保 ESX Server 3 系统安全的一个重要部分。由于服务控制台的安全漏洞将使得攻击者能够完全控制系统上运行的所有

虚拟机，因此服务控制台网络连接与服务器上任何远程访问设备的网络连接具有同等的重要性。

- 保证 VMotion 连接处于专用且单独的网络中是非常重要的，因为使用 VMotion 进行迁移时，客户操作系统内存中的内容将通过网络进行传输。

装载 NFS 卷

在 ESX Server 3 中， ESX Server 3 访问 ISO 映像 （用作虚拟机的虚拟 CD-ROM）的 NFS 存储器的模型与 ESX Server 2.x 中所用的模型是不同的。

ESX Server 3 支持基于 VMkernel 的 NFS 装载。新模型将通过 VMkernel NFS 功能将 NFS 卷与 ISO 映像一起装载。所有以这种方式装载的 NFS 卷均显示为 VI Client 中数据存储。虚拟机配置编辑器允许浏览 ISO 映像的服务控制台文件系统，以便用作虚拟 CD-ROM 设备。

网络提示

请考虑以下网络提示：

- 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 vSwitch。如果无法实现，可以使用不同的 VLAN ID 将网络服务附加到端口组，以便在一个 vSwitch 上将它们彼此分离开来。与此同时，与网络管理员确认所选的网络或 VLAN 与环境中的其它部分是隔离开的，即没有与其相连的路由器。
- 可以在不影响虚拟机或运行于 vSwitch 后端的网络服务的前提下，向 vSwitch 添加或从中移除网卡。如果移除所有运行中的硬件，虚拟机仍可互相通信。而且，如果保留一个网卡原封不动，所有的虚拟机仍然可以与物理网络相连。
- 要将虚拟机分离成组，请按照其成组策略将端口组与不同的活动适配器组配合使用。只要所有的适配器无故障，上述操作就可以使用单独的适合器，但是当出现网络或硬件故障时，仍会回退到共享状态。
- 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的（连接到物理网络）虚拟网络和无上行链路的纯虚拟网络之间路由。

4 网络连接方案和疑难解答

本章描述了网络连接配置和疑难解答方案。

本章将讨论以下主题：

软件 iSCSI 存储器的网络配置

为 ESX Server 3 主机配置的存储器可能包括一个或多个使用 iSCSI 存储器的存储区域网络 (SAN)。iSCSI 是一种使用 TCP/IP 协议通过网络端口（而不是通过直接连接到 SCSI 设备）来访问 SCSI 设备和交换数据记录的方法。在 iSCSI 事务中，原始 SCSI 数据块被封装在 iSCSI 记录中并传送至请求数据的设备或用户。

注意 软件启动的 iSCSI 不可用于 ESX Server 3.5 中的 10GigE 网络适配器。

配置 iSCSI 存储器之前，必须创建 VMkernel 端口以处理 iSCSI 网络及 iSCSI 网络的服务控制台连接。

为软件 iSCSI 创建 VMkernel 端口

1 登录 VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[网络 (Networking)]**。

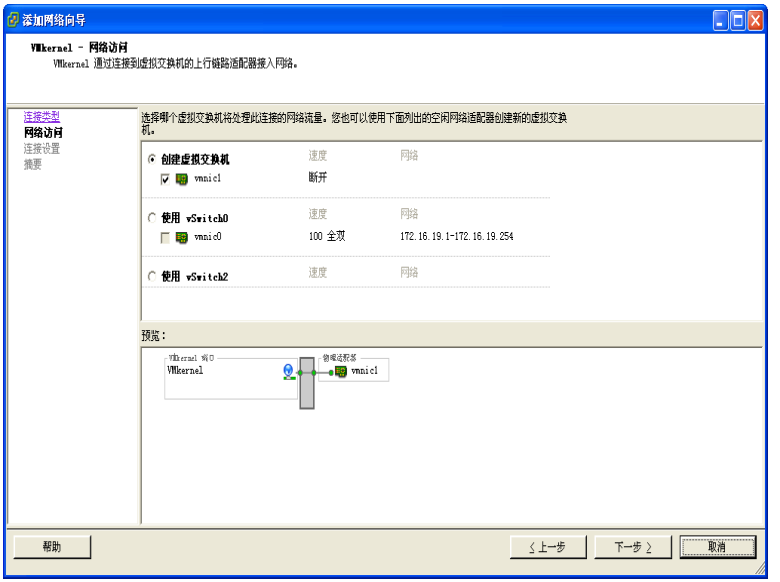
3 单击 **[添加网络连接 (Add Networking)]**。

4 选择 **[VMkernel]**，然后单击 **[下一步 (Next)]**。

此时将出现 **[网络访问 (Network Access)]** 页面。在此页面上，即可将为 iSCSI 存储器运行服务的 VMkernel 连接至物理网络。

5 选择要使用的 vSwitch，或单击 **[创建虚拟交换机 (Create a virtual switch)]**。

6 选择 vSwitch 要使用的网络适配器复选框。



选择将出现在 **[预览 (Preview)]** 窗格中。

为每个 vSwitch 选择适配器，以便使通过适配器连接的虚拟机或其他设备可到达正确的以太网分段。如果 **[创建虚拟交换机 (Create a virtual switch)]** 组中未出现适配器，则表明系统中所有网络适配器均被现有 vSwitch 占用。

有关在 vSwitches 之间移动网络适配器的信息，请参见 “添加上行链路适配器”（第 40 页）。

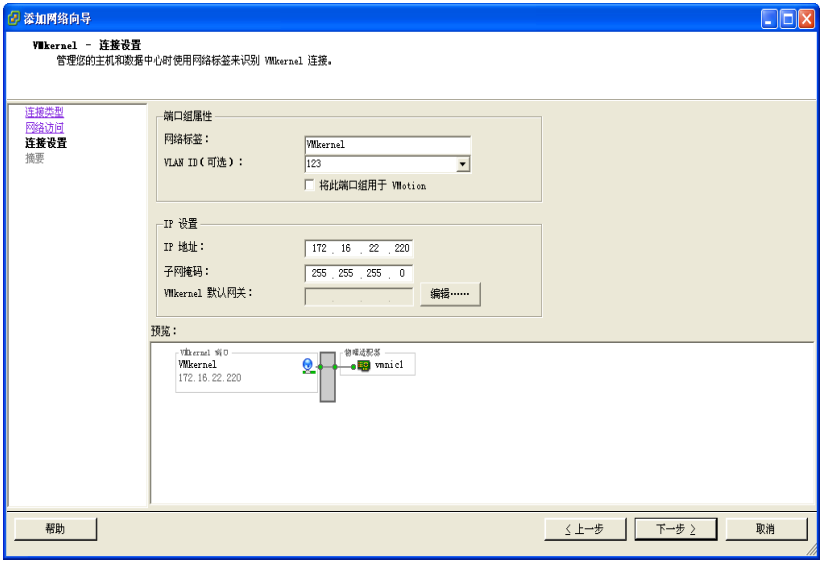
注意 不要在 100 MB 网络适配器上使用 iSCSI。

7 单击 **[下一步 (Next)]**。

8 在 **[端口组属性 (Port Group Properties)]** 组中，选择或输入网络标签和 VLAN ID（可选）。

[网络标签 (Network Label)]。用于识别所创建的端口组的名称。配置 iSCSI 存储器时，请在配置与此端口组连接的虚拟适配器时指定此标签。

[VLAN ID]。用于识别端口组网络流量将使用的 VLAN。不需要 VLAN ID。如果您不确定是否需要它们，请向网络管理员咨询。



9 在 **[IP 设置 (IP Settings)]** 组中，单击 **[编辑 (Edit)]** 以便为 iSCSI 设置 **[VMkernel 默认网关 (VMkernel Default Gateway)]**。

在 **[路由 (Routing)]** 选项卡中，服务控制台和 VMkernel 均需要其自身的网关信息。

注意 为所创建的端口设置默认网关。必须使用有效的静态 IP 地址配置 VMkernel 堆栈。

10 单击 **[确定 (OK)]**。

11 单击 **[下一步 (Next)]**。

12 单击 **[上一步 (Back)]** 进行更改。

13 检查在 **[即将完成 (Ready to Complete)]** 页面上做出的更改，单击 **[完成 (Finish)]**。

为 iSCSI 创建 VMkernel 端口后，创建的服务控制台必须与 VMkernel 端口连接到同一个 vSwitch。

为软件 iSCSI 存储器配置服务控制台连接

1 登录 VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

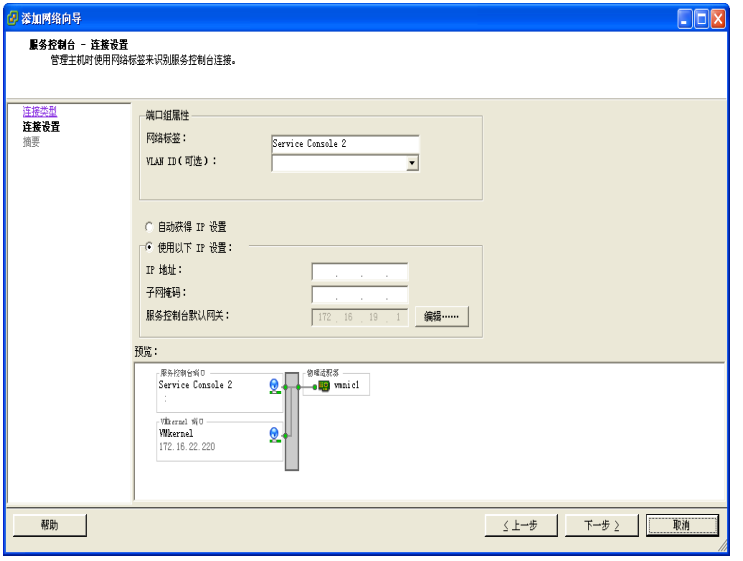
2 依次单击 **[配置 (Configuration)]** 选项卡和 **[网络 (Networking)]**。

3 在页面的右侧，单击与您所创建的 VMkernel 端口相关联的 vSwitch 的 **[属性 (Properties)]**。

4 在 **[端口 (Ports)]** 选项卡上，单击 **[添加 (Add)]**。

5 选择 **[服务控制台 (Service Console)]** 连接类型，单击 **[下一步 (Next)]**。

6 在 **[端口组属性 (Port Group Properties)]** 组中，输入用于识别所创建的端口组的网络标签。



较新的端口和端口组将出现在 vSwitch 图的顶部。

7 输入 **[IP 地址 (IP Address)]** 和 **[子网掩码 (Subnet Mask)]**，或为 IP 地址和子网掩码选择 DHCP 选项 **[自动获得 IP 设置 (Obtain IP setting automatically)]**。请注意，此 IP 必须不同于为 VMkernel 选择的 IP。

8 单击 **[编辑 (Edit)]**，设置 **[服务控制台默认网关 (Service Console Default Gateway)]**。

请参见 “设置默认网关”（第 34 页）。

9 单击 **[下一步 (Next)]**。

10 确定 vSwitch 配置正确之后，单击 **[完成 (Finish)]**。

创建 VMkernel 端口和服务控制台连接后，即可启用和配置软件 iSCSI 存储器。有关配置 iSCSI 适配器和存储器的信息，请参见 “iSCSI 存储器”（第 100 页）。

在刀片服务器上配置网络

由于刀片服务器的网络适配器数量可能是限定值，因此，可能需要使用 VLAN 来分离服务控制台、 VMotion、 IP 存储器和各组虚拟机的流量。为了安全起见， VMware 建议最好为服务控制台和 VMotion 配备各自的网络。如果出于此目的将物理适配器专用于分离 vSwitch，则必须放弃冗余 （组合）连接或停止隔离各个网络客户端，或同时执行。借助 VLAN，不必使用多个物理适配器即可实现网络分段。

要使刀片服务器的网络刀片支持 ESX Server 3 端口组进行 VLAN 标签通信，必须将此刀片配置为支持 802.1Q，将端口配置为标签端口。

将端口配置为标签端口的方法因服务器而异。下表描述如何在三个最为常用的刀片服务器上配置标签端口。

HP 刀片	将端口的 **[VLAN 标记 (VLAN Tagging)]** 设置为 **[已启用 (enabled)]**。
Dell PowerEdge	将端口设置为 **[已标记 (Tagged)]**。
IBM eServer 刀片中心	在端口配置中选择 **[标记 (Tag)]**。

通过刀片服务器上的 VLAN 配置虚拟机端口组

1 登录 VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[网络 (Networking)]**。

3 在页面的右侧，单击与服务控制台相关联的 vSwitch 的 **[属性 (Properties)]**。

4 在 **[端口 (Ports)]** 选项卡上，单击 **[添加 (Add)]**。

5 为连接类型选择 **[虚拟机 (Virtual Machines)]** （默认）。

6 单击 **[下一步 (Next)]**。

7 在 **[端口组属性 (Port Group Properties)]** 组中，输入用于识别所创建的端口组的网络标签。

使用网络标签识别两台或多台主机之间共用的迁移兼容的连接。

8 在 **[VLAN ID]** 字段中，输入一个介于 1 和 4094 之间的数字。

如果不能确定输入的值，请将此处留空或者询问网络管理员。

9 单击 **[下一步 (Next)]**。

10 确定 vSwitch 配置正确之后，单击 **[完成 (Finish)]**。

通过刀片服务器上的 VLAN 配置 VMkernel 端口

1 登录 VI Client，从清单面板中选择服务器。

此时将出现该服务器的硬件配置页面。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[网络 (Networking)]**。

3 在页面的右侧，单击与服务控制台相关联的 vSwitch 的 **[属性 (Properties)]**。

4 在 **[端口 (Ports)]** 选项卡上，单击 **[添加 (Add)]**。

5 选择 **[VMkernel]**，然后单击 **[下一步 (Next)]**。

通过此选项，即可将为 VMotion 和 IP 存储器 （NFS 或 iSCSI）运行服务的 VMkernel 连接至物理网络。

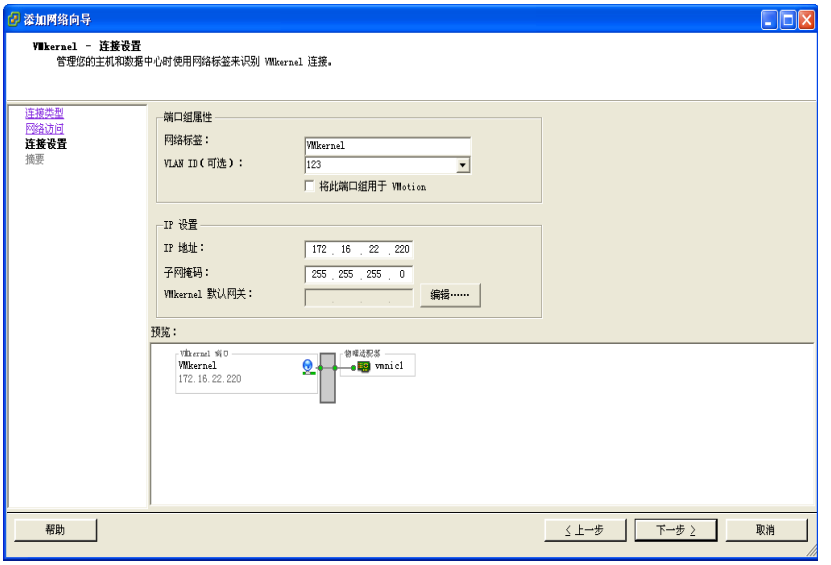
6 在 **[端口组属性 (Port Group Properties)]** 组，选择或输入网络标签和 VLAN ID。

[网络标签 (Network Label)]。用于识别所创建的端口组的名称。此标签是在配置诸如 VMotion 和 IP 存储器之类的 VMkernel 服务时，配置与此端口组连接的虚拟适配器时指定的。

[VLAN ID]。用于识别端口组网络流量将使用的 VLAN。

7 选择 **[将此端口组用于 VMotion (Use this port group for VMotion)]** 以启用此端口组，此端口组向另一个 ESX Server 3 将其本身显示为用于发送 VMotion 流量的网络连接。

仅可为每个 ESX Server 3 主机的其中一个 VMotion 和 IP 存储器端口组启用此属性。如果未为任何端口组启用此属性，则不可通过 VMotion 向此主机进行迁移。



8 在 **[IP 设置 (IP Settings)]** 组中，单击 **[编辑 (Edit)]** 以便为诸如 VMotion、NAS 和 iSCSI 之类的 VMkernel 服务设置 **[VMkernel 默认网关 (VMkernel Default Gateway)]**。

注意 为所创建的端口设置默认网关。VirtualCenter 2 的行为与 VirtualCenter 1.x. 不同。必须使用有效的 IP 地址而不是虚拟的地址来配置 VMkernel IP 堆栈。

在 **[DNS 配置 (DNS Configuration)]** 选项卡下方，默认情况下，主机名称输入在名称字段。在安装期间指定的 DNS 服务器地址和域也预先选定。

在 **[路由 (Routing)]** 选项卡中，服务控制台和 VMkernel 均需要其自身的网关信息。连接不在服务控制台或 VMkernel 等所在同一 IP 子网上的计算机时，需要网关。

静态 IP 地址为默认值。

9 单击 **[确定 (OK)]**。

10 单击 **[下一步 (Next)]**。

11 单击 **[上一步 (Back)]** 进行更改。

12 检查在 **[即将完成 (Ready to Complete)]** 页面上做出的更改，单击 **[完成 (Finish)]**。

疑难解答

本节指导解决常见网络问题。

服务控制台网络的疑难解答

如果服务控制台网络的某些部分配置错误，则无法通过 VI Client 访问 ESX Server 3 主机。如果发生此情况，可直接连接至服务控制台并使用以下服务控制台命令，重新配置网络：

- `esxcfg-vswif -l`

  提供服务控制台的当前网络接口的列表。

  检查是否显示 `vswif0` 及当前 IP 地址和子网掩码是否正确。

- `esxcfg-vswitch -l`

  提供当前虚拟交换机配置列表。

  检查为服务控制台配置的上行链路适配器是否连接至合适的物理网络。

- `exscfg-nics -l`

  提供当前网络适配器列表。

  检查为服务控制台配置的上行链路适配器是否为上行，且其速度和双工是否都正确。

- `esxcfg-nics -s <speed> <nic>`

  可更改网络适配器的速度。

- `esxcfg-nics -d <duplex> <nic>`

  可更改网络适配器的双工。

- `esxcfg-vswif -i <new ip address> vswifX`

  可更改服务控制台的 IP 地址。

- `esxcfg-vswif -n <new netmask> vswifX`

  可更改服务控制台的子网掩码。

- `esxcfg-vswitch -U <old vmnic> <service console vswitch>`

  可移除服务控制台的上行链路。

- `esxcfg-vswitch -L <new vmnic> <service console vswitch>`

  可更改服务控制台的上行链路。

如果使用 esxcfg-* 命令时出现长时间等待现象，则可能表明 DNS 配置错误。esxcfg-* 命令要求配置 DNS，以便使 localhost 名称解析正常运行。这要求 /etc/hosts 文件包含适用于已配置的 IP 地址和 127.0.0.1 localhost 地址的条目。

网络适配器配置疑难解答

在某些情况下，添加新的网络适配器可能导致无法使用 VI Client 对服务控制台进行连接和管理，这是因为网络适配器已重命名。

如果发生此情况，必须使用服务控制台对受影响的网络适配器进行重命名。

使用服务控制台重命名网络适配器

1 直接登录 ESX Server 3 主机的控制台。

2 使用 esxcfg-nics -l 命令查看已分配给网络适配器的名称。

3 使用 esxcfg-vswitch -l 命令查看与不再通过 esxcfg-nics 命令显示的设备名称相关联的 vSwitch （如有）。

4 使用 esxcfg-vswitch -U <old vmnic name> <vswitch> 命令移除已重命名的任何网络适配器。

5 使用 esxcfg-vswitch -L <new vmnic name> <vswitch> 命令重新添加并正确命名网络适配器。

物理交换机配置疑难解答

发生故障切换或故障恢复事件时，有时可能会失去 vSwitch 连接。这可导致与此 vSwitch 相关联的虚拟机所使用的 MAC 地址出现在与之前不同的交换机端口。

为了避免此问题，请将物理交换机置于 portfast 或 portfast 中继模式。

端口组配置疑难解答

更改虚拟机所连接的端口组的名称会导致虚拟机的网络配置 （与端口组连接）无效。

虚拟网络适配器与端口组之间通过名称进行连接，此名称存储在虚拟机配置中。更改端口组的名称不需要重新配置所有与该端口组连接的虚拟机。已启动的虚拟机在关闭之前将继续运行，因为其已与网络之间建立连接。

避免对使用中的网络进行重命名。重命名端口组后，必须使用服务控制台重新配置每一个相关联的虚拟机，以反映新的端口组名称。

存储器

5 存储器简介

存储一节包含了有关 ESX Server 3 可用的存储选项的概述信息，阐述了如何配置 ESX Server 3 系统以便可以使用和管理不同类型的存储器。

有关存储管理员需要在存储阵列执行的特定操作的信息，请参见 *《光纤通道 SAN 配置指南》*和 *《iSCSI SAN 配置指南》*。

本章将讨论以下主题：

存储器概述

ESX Server 3 虚拟机使用虚拟硬盘来存储其操作系统、程序文件，以及与其活动有关的其他数据。虚拟磁盘是一个大型物理文件或一组文件，可以像任何其他文件一样轻松地对其进行复制、移动、存档和备份。为了存储虚拟磁盘文件并且能够操作文件， ESX Server 3 需要专用的存储空间。

ESX Server 3 可以使用各种物理存储设备 （包括主机的内部和外部存储设备或联网的存储设备）上的存储空间。存储设备是专门用于特定任务 （存储和保护数据）的物理磁盘或磁盘阵列。

ESX Server 3 可以发现它有权限访问的存储设备并将设备格式化为数据存储。数据存储是一种特殊的逻辑容器，类似于逻辑卷上的文件系统； ESX Server 3 在其中放置虚拟磁盘文件和封装虚拟机基本组件的其他文件。数据存储部署在不同设备上，它将各个存储产品的特性隐藏起来，并提供一个统一的模型来存储虚拟机文件。

使用 VI Client，可以在 ESX Server 3 发现的任何存储设备上预先设置数据存储。

若要了解如何访问和配置存储设备，以及如何创建和管理数据存储，请参见以下各章：

- “配置存储器”（第 93 页）
- “管理存储器”（第 121 页）

数据存储一经创建，即可用于存储虚拟机文件。有关创建虚拟机的详细信息，请参见*《基本系统管理》*。

物理存储器的类型

ESX Server 3 存储管理过程以存储管理员在不同存储设备上预先分配的存储空间开始。

ESX Server 3 支持下面的存储设备类型：

- **本地** - 在直接连接到 ESX Server 3 主机的内部或外部存储设备或阵列上存储虚拟机文件。
- **联网** - 在位于 ESX Server 3 主机之外的外部共享存储设备或阵列上存储虚拟机文件。主机通过高速网络与联网设备进行通信。

本地存储器

本地存储设备可以是位于 ESX Server 3 主机内部的内部硬盘，也可以是位于主机之外并直接连接到主机的外部存储系统。

本地存储设备不需要存储网络即可与 ESX Server 3 进行通信。所需的只是一根连接到存储设备的电缆；必要时， ESX Server 3 主机中需要有一个兼容的 HBA。

通常，可以将多个 ESX Server 3 主机连接到单个本地存储系统。根据存储设备的类型和使用的拓扑结构，连接的实际主机数可能会有所不同。

许多本地存储系统支持冗余连接路径以确保容错性能。请参见 “管理多路径”（第 125 页）。

当多个 ESX Server 3 主机连接到本地存储单元时，这些主机将以非共享模式访问存储 LUN。非共享模式不允许多个 ESX Server 3 主机同时访问同一个 VMFS 数据存储。但是，一些 SAS 存储系统可对多个 ESX Server 3i 主机提供共享访问。此类型的访问允许多个 ESX Server 3i 主机访问 LUN 上的同一个 VMFS 数据存储。请参见 “在 ESX Server 3 系统间共享 VMFS 卷”（第 83 页）。

ESX Server 3 支持多种内部或外部本地存储设备，包括 SCSI、IDE、SATA 和 SAS 存储系统。无论使用何种存储类型， ESX Server 3 都会向虚拟机隐藏物理存储层。

设置本地存储时，请记住以下几点：

- 无法使用 IDE/ATA 驱动器来存储虚拟机。
- 只能以非共享模式使用内部和外部本地 SATA 存储器。 SATA 存储器不支持多个 ESX Server 3 主机共享相同的 LUN，因此也无法共享同一个 VMFS。

  使用 SATA 存储器时，请确保通过支持的双重 SATA/SAS 控制器连接 SATA 驱动器。
- 某些 SAS 存储系统可以向多个 ESX Server 3 主机提供对相同 LUN （以及相同 VMFS 数据存储）的共享访问。

有关支持的本地存储设备的信息，请参见 *《I/O 兼容性指南》*，网址是 www.vmware.com/support/pubs/vi_pubs.html。

联网的存储器

联网存储设备是 ESX Server 3 主机用来远程存储虚拟机文件的外部存储设备或阵列。 ESX Server 3 主机通过高速存储网络访问这些设备。

ESX Server 3 支持下面的联网存储技术：

- **光纤通道 (FC)** - 在 FC 存储区域网络 (SAN) 上远程存储虚拟机文件。FC SAN 是一种将 ESX Server 3 主机连接到高性能存储设备的专用高速网络。该网络使用光纤通道协议，将 SCSI 流量从虚拟机传输到 FC SAN 设备。

  要连接 FC SAN， ESX Server 3 主机应配有光纤通道主机总线适配器 (HBA)，并且除非使用光纤通道直接连接存储器，否则主机还应配有光纤通道交换机，以帮助路由存储流量。

- **Internet SCSI (iSCSI)** - 在远程 iSCSI 存储设备上存储虚拟机文件。 iSCSI 将 SCSI 存储流量打包在 TCP/IP 协议中，以便通过标准 TCP/IP 网络 （而不是专用 FC 网络）进行传输。通过 iSCSI 连接， ESX Server 3 主机可以充当与位于远程 iSCSI 存储系统的*目标*进行通信的*启动器*。

  ESX Server 3 提供下面的 iSCSI 连接类型：

  - **硬件启动的 iSCSI** - ESX Server 3 主机通过第三方 iSCSI HBA 连接到存储器。
  - **软件启动的 iSCSI** - ESX Server 3 使用 VMkernel 中基于软件的 iSCSI 启动器来连接到存储器。通过这种 iSCSI 连接类型，主机只需要一个标准的网络适配器来进行网络连接。

- **网络附加存储 (NAS)** - 在通过标准 TCP/IP 网络访问的远程文件服务器上存储虚拟机文件。 ESX Server 3 内置的 NFS 客户端使用网络文件系统 (NFS) 协议第 3 版与 NAS/NFS 服务器进行通信。为了进行网络连接， ESX Server 3 主机需要一个标准的网络适配器。

请参见 *《存储器 /SAN 兼容性指南》*，网址是 www.vmware.com/pdf/vi3_san_guide.pdf。

支持的存储适配器

根据可用的存储器类型， ESX Server 3 系统可能需要用来连接特定存储设备或网络的适配器。ESX Server 3 支持不同的适配器类别，包括 SCSI、iSCSI、RAID、光纤通道和以太网。 ESX Server 3 直接通过 VMkernel 中的设备驱动程序访问适配器。

有关 ESX Server 3 支持的适配器类型的详细信息，请参见 *《I/O 兼容性指南》*，网址是 www.vmware.com/support/pubs/vi_pubs.html。

数据存储

可以使用 VI Client 访问 ESX Server 3 主机发现的不同类型的存储设备，并在这些设备上部署数据存储。数据存储是特殊的逻辑容器，类似于文件系统，它将各个存储设备的特性隐藏起来，并提供一个统一的模型来存储虚拟机文件。

数据存储还可以用来存储 ISO 映像、虚拟机模板和软盘映像。请参见 *《基本系统管理》*，网址是 www.vmware.com/support/pubs/。

根据使用的存储器类型， ESX Server 3 数据存储可以具有下面的文件系统格式：

- **虚拟机文件系统 (VMFS)** - 优化的高性能文件系统，用于存储 ESX Server 3 虚拟机。 ESX Server 3 可以将 VMFS 部署在任何基于 SCSI 的本地或联网存储设备上，包括光纤通道和 iSCSI SAN 设备。

除了使用 VMFS 数据存储之外，虚拟机还可以直接访问裸设备并使用映射文件 (RDM) 作为代理。有关 RDM 的详细信息，请参见 “裸设备映射”（第 133 页）。

- **网络文件系统 (NFS)** - NAS 存储设备上的文件系统。 ESX Server 3 支持 TCP/IP 上的 NFS 版本 3。 ESX Server 3 可以访问位于 NFS 服务器上指定的 NFS 卷。 ESX Server 3 装载 NFS 卷并用它来满足存储需求。

如果使用服务控制台访问 ESX Server 3 主机，您会看到 VMFS 和 NFS 数据存储位于 `/vmfs/volumes` 目录下面的单独子目录。有关使用服务控制台命令和实用程序的信息，请参见 “使用 vmkfstools”（第 253 页）。

VMFS 数据存储

ESX Server 3 主机访问基于 SCSI 的存储设备 （例如 SCSI、 iSCSI 或 FC SAN）时，存储空间会以 LUN 形式呈现给 ESX Server 3。*LUN* 是一种逻辑卷，它表示单个物理磁盘或磁盘阵列中聚集的许多磁盘上的存储空间。可以从存储磁盘或阵列上的整个空间或部分空间 （称为*分区*）创建单个 LUN。使用多个物理磁盘或分区上磁盘空间的 LUN 仍然会以单个逻辑卷的形式呈现给 ESX Server 3。

ESX Server 3 可以将 LUN 格式化为 VMFS 数据存储。 VMFS 数据存储主要用作虚拟机的存储库。可以在同一个 VMFS 卷上存储多个虚拟机。封装在一组文件中的各个虚拟机都会占用一个单独的目录目录。对于虚拟机内部的操作系统，VMFS 会保留内部文件系统语义，这样可以确保正确的应用程序行为以及在虚拟机中运行的应用程序的数据完整性。

此外，还可以使用 VMFS 数据存储来存储其他文件，例如虚拟机模板和 ISO 映像。

VMFS 支持下面的文件和块大小，使得虚拟机能够运行数据极其庞大的应用程序，包括虚拟机中的数据库、 ERP 和 CRM：

- 最大虚拟磁盘大小：2 TB （块大小为 8 MB）
- 文件大小上限：2 TB （块大小为 8 MB）
- 块大小：1 MB （默认）、 2 MB、 4 MB 和 8 MB

创建和增加 VMFS 数据存储

可以使用 VI Client 预先在 ESX Server 3 发现的任何基于 SCSI 的存储设备上设置 VMFS 数据存储。ESX Server 3 允许每个系统最多具有 256 个 VMFS 数据存储，这些数据存储的最小卷大小为 1.2 GB。

注意 每个 LUN 始终只具有一个 VMFS 数据存储。

有关在基于 SCSI 的存储设备上创建 VMFS 数据存储的信息，请参见以下各节：

- “添加本地存储器”（第 94 页）
- “添加光纤通道存储器”（第 97 页）
- “添加可通过硬件启动器访问的 iSCSI 存储器”（第 108 页）
- “添加可通过硬件启动器访问的 iSCSI 存储器”（第 108 页）

创建 VMFS 数据存储以后，可以编辑它的属性。请参见 “编辑 VMFS 数据存储”（第 123 页）。

如果 VMFS 数据存储需要更多空间，可以通过添加扩展来动态增加 VMFS 卷 （最多为 64 TB）。*扩展* 是物理存储设备上的 LUN，可以动态添加到任何现有的 VMFS 数据存储。数据存储可以跨越多个扩展，但显示为单个卷。

注意 无法重新格式化远程 ESX Server 3 主机正在使用的 VMFS 卷。如果试图这样做，则会看到一个警告，该警告会指出正在使用的卷的名称以及正在使用该卷的主机网卡的 MAC 地址。此警告也会出现在 VMkernel 和 VMkwarning 日志文件中。

创建 VMFS 数据存储时的注意事项

在使用 VMFS 数据存储格式化存储设备之前，需要规划如何设置 ESX Server 3 系统的存储器。

由于以下原因，可能需要更少、更大的 VMFS 卷：

- 在无需存储管理员提供更多空间的情况下，使虚拟机的创建更具灵活性。
- 能够更灵活地调整虚拟磁盘大小以及执行快照。
- 使要管理的 VMFS 数据存储减少。

由于以下原因，可能需要更多、更小的 VMFS 卷：

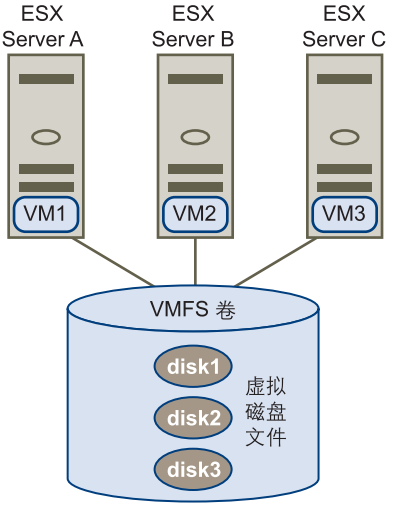
- 降低浪费的存储空间。
- 不同的应用程序可能需要不同的 RAID 特性。
- 每个 LUN 设置多路径策略和磁盘份额时获得更多的灵活性。
- 使用 Microsoft 群集服务要求每个群集磁盘资源位于自己的 LUN 中。
- 性能更佳。

您可能决定配置一些服务器来使用更少、更大的 VMFS 卷，但是其他服务器依然使用容量较小的 VMFS 卷。

在 ESX Server 3 系统间共享 VMFS 卷

作为一个群集文件系统，VMFS 可让多个 ESX Server 3 主机同时访问同一个 VMFS 数据存储。最多可以将 32 个主机连接到单个 VMFS 卷。

图 5-1 在 ESX Server 3 主机间共享 VMFS 卷



为了确保多台服务器不会同时访问同一个虚拟机， VMFS 提供了磁盘锁定。

在多个 ESX Server 3 主机间共享同一个 VMFS 卷具有以下好处：

- 可使用 VMware Distributed Resource Scheduling 和 VMware High Availability。

  可以跨越不同的物理服务器分配虚拟机。这意味着，每个服务器上会运行一组虚拟机，以便所有服务器就不会同时在同一个区域面临很高的需求。

  如果某台服务器发生故障，可以在另一台物理服务器上重新启动虚拟机。万一发生故障，每个虚拟机的磁盘锁会被释放。

  有关 VMware DRS 和 VMware HA 的详细信息，请参见 *《资源管理指南》*，网址是 www.vmware.com/support/pubs/。

- 可以使用 VMotion 对正在运行的虚拟机执行物理服务器间的实时迁移。

  有关 VMotion 的详细信息，请参见 *《基本系统管理》*，网址是 www.vmware.com/support/pubs/。

- 可以使用 VMware Consolidated Backup，它可让一个称为 VCB 代理的代理服务器在虚拟机启动和读写存储器时备份虚拟机的快照。

  有关 Consolidated Backup 的详细信息，请参见 *《虚拟机备份指南》*，网址是 www.vmware.com/support/pubs/。

NFS 数据存储

ESX Server 3 可以访问位于 NAS 服务器上的指定 NFS 卷、装载该卷，以及用它来满足存储需求。可以使用 VMFS 数据存储的相同方式使用 NFS 卷来存储和引导虚拟机。

ESX Server 3 支持 NFS 卷上的以下共享存储功能：

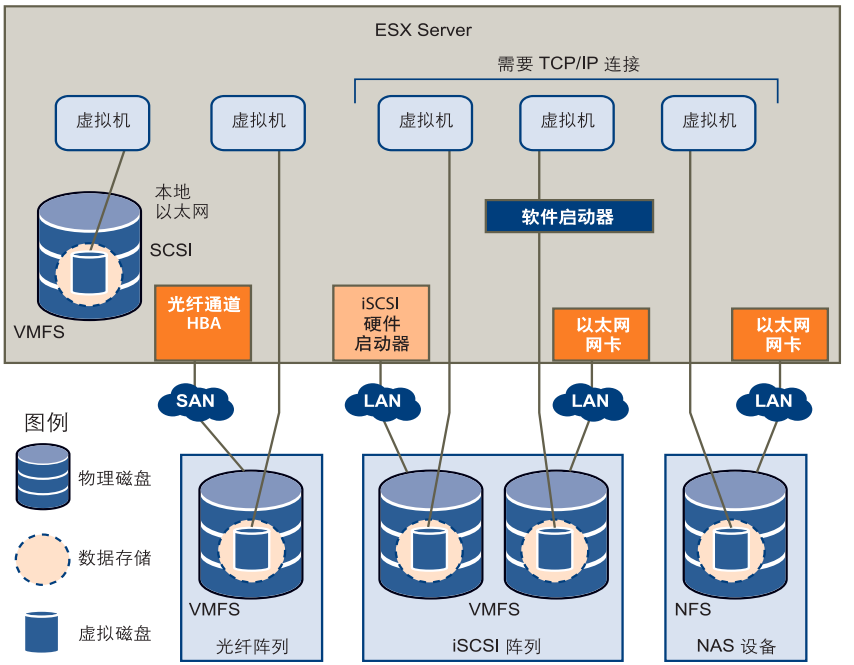
- 使用 VMotion。
- 使用 VMware DRS 和 VMware HA。
- 装载 ISO 映像，该映像以 CD-ROM 形式呈现给虚拟机。
- 创建虚拟机快照。请参见 *《基本系统管理》*，网址是 www.vmware.com/support/pubs/。

虚拟机如何访问存储器

当虚拟机与存储在数据存储上的虚拟磁盘进行通信时，它会发出 SCSI 命令。由于数据存储可以存在于各种类型的物理存储器上，因此，根据 ESX Server 3 系统用来连接存储设备的协议，这些命令会封装成其他形式。ESX Server 3 支持光纤通道 (FC)、Internet SCSI (iSCSI) 和 NFS 协议。无论 ESX Server 3 使用何种类型的存储设备，虚拟磁盘会以装载的 SCSI 设备形式呈现给虚拟机。虚拟磁盘向虚拟机的操作系统隐藏了物理存储层。这样可以在虚拟机内运行未针对特定存储设备 （例如 SAN）而认证的操作系统。

图 5-2 列出了使用不同存储类型的五个虚拟机，以说明各个类型之间的区别。

图 5-2 访问不同存储器类型的虚拟机



注意 此图仅用来解释概念。它并非是建议的配置。

比较存储类型

表 5-1 比较 ESX Server 3 支持的联网存储技术。

表 5-1 ESX Server 3 支持的联网存储

技术	协议	传输	接口
光纤通道	FC/SCSI	数据 /LUN 的块访问	FC HBA
iSCSI	IP/SCSI	数据 /LUN 的块访问	■ iSCSI HBA （硬件启动的 iSCSI） ■ 网卡 （软件启动的 iSCSI）
NAS	IP/NFS	文件 （无直接 LUN 访问）	网卡

表 5-2 比较不同类型存储器支持的 ESX Server 3 功能。

表 5-2 存储器支持的 ESX Server 3 功能

存储器类型	引导虚拟机	VMotion	数据存储	RDM	虚拟机群集	VMware HA 和 DRS	VCB
SCSI	是	否	VMFS	否	否	否	是
光纤通道	是	是	VMFS	是	是	是	是
iSCSI	是	是	VMFS	是	否	是	是
NFS 上的 NAS	是	是	NFS	否	否	是	是

查看 VMware Infrastructure Client 中的存储信息

VI Client 可以显示有关可用数据存储、数据存储使用的存储设备和配置的适配器的详细信息。有关详细信息，请参见以下各节：

- “显示数据存储”（第 86 页）
- “查看存储适配器”（第 88 页）
- “了解显示屏幕中的存储设备命名”（第 89 页）

显示数据存储

可使用以下方式将数据存储添加到 VI Client 中：

- 当主机添加到清单时发现。将主机添加到清单中时， VI Client 显示主机可以使用的任何数据存储。

- 在可用存储设备上创建。可以使用 **[添加存储器 (Add Storage)]** 选项来创建和配置新的数据存储。请参见 “配置存储器”（第 93 页）。

可以查看可用数据存储列表并分析它们的属性。

要显示数据存储，请在主机 **[配置 (Configuration)]** 选项卡上，单击 **[存储器 (Storage)]**。

对于每个数据存储，[存储器 (Storage)] 部分显示摘要信息，包括：

- 数据存储所在的目标存储设备。请参见 “了解显示屏幕中的存储设备命名”（第 89 页）。
- 数据存储使用的文件系统类型。请参见 “数据存储”（第 80 页）。
- 总容量，包括已用空间和可用空间。

若要查看有关特定数据存储的其他详细信息，请从列表中选择数据存储。**[详细信息 (Details)]** 部分显示以下信息：

- 数据存储的位置。
- 数据存储跨越的个别扩展及其容量 （VMFS 数据存储）。
- 用来访问存储设备的路径 （VMFS 数据存储）。

在图 5-3 中，“symm-07”数据存储是从可用数据存储列表中选择的。**[详细信息 (Details)]** 窗格提供有关选定数据存储的信息。

图 5-3 数据存储信息

可以刷新和移除任何现有数据存储，以及更改 VMFS 数据存储的属性。编辑或重新配置 VMFS 数据存储时，可以更改标签、添加扩展、进行升级，或者修改存储设备的路径。请参见 “管理存储器”（第 121 页）。

查看存储适配器

VI Client 可以显示您系统可以使用的任何存储适配器。

要显示存储适配器，请在主机 **[配置 (Configuration)]** 选项卡上，单击 **[存储适配器 (Storage Adapters)]**。

可以查看有关存储适配器的以下信息：

- 现有的存储适配器。
- 存储适配器的类型，例如光纤通道 SCSI 或 iSCSI。
- 每个适配器的详细信息，例如它所连接到存储设备和目标 ID。

若要查看特定适配器的配置属性，请从 **[存储适配器 (Storage Adapters)]** 列表中选择适配器。

在图 5-4 中，已选择 iSCSI 硬件 vmhba0 适配器。**[详细信息 (Details)]** 窗格提供有关适配器所连接的 LUN 数以及所使用的路径。

若要更改路径的配置，可以从列表中选择此路径，再右键单击路径，然后单击 **[管理路径 (Manage Paths)]**，以打开 [管理路径 (Manage Paths)] 对话框。请参见 “管理多路径”（第 125 页）。

图 5-4 存储适配器信息

了解显示屏幕中的存储设备命名

在 VI Client 中，存储设备的名称会显示为三个或四个数字的序列，中间用冒号分隔，例如 `vmhba1:1:3:1`。该名称具有以下含义：

```
<HBA>:<SCSI target>:<SCSI LUN>:<disk partition>
```

缩写 `vmhba` 表示 ESX Server 3 系统上的不同物理 HBA。它也可以表示 ESX Server 3 使用 VMkernel 网络堆栈实现的虚拟 iSCSI 启动器。第四个数字表示磁盘上 VMFS 数据存储占用的分区。

`vmhba1:1:3:1` 示例表示通过 HBA 1 访问的 SCSI 目标 1、 SCSI LUN3 上的第一个分区。

虽然第三个和第四个数字永远不会更改，但前两个数字可以更改。例如，重新引导 ESX Server 3 系统以后， `vmhba1:1:3:1` 会更改为 `vmhba3:2:3:1`，然而，该名称仍然表示同一个物理设备。第一个和第二个数字可能会由于以下原因而更改：

- 第一个数字 (HBA) 会在光纤通道或 iSCSI 网络发生故障时更改。在这种情况下，ESX Server 3 系统必须使用其他 HBA 来访问存储设备。

- 第二个数字 （SCSI 目标）会在 ESX Server 3 主机可见的光纤通道或 iSCSI 目标映射发生任何修改时更改。

配置和管理存储器

本指南的 “配置存储器” 和 “管理存储器” 两章介绍了大多数概念，并且概述了使用存储器时需要执行的任务。

有关配置 SAN 的详细信息，请参见 *《光纤通道 SAN 配置指南》* 和 *《iSCSI SAN 配置指南》*。

有关特定存储器配置任务的详细信息，请参见以下内容：

- 本地存储器配置：

  “在本地 SCSI 磁盘上创建数据存储”（第 94 页）

- 光纤通道 SAN 存储器配置：

  “在光纤通道设备上创建数据存储”（第 98 页）

- 硬件启动的 iSCSI 存储器配置：
  - “查看硬件 iSCSI 启动器属性”（第 102 页）
  - “设置硬件启动器的 iSCSI 名称、别名和 IP 地址”（第 104 页）
  - “使用动态发现设置目标发现地址”（第 105 页）
  - “设置硬件启动器的 CHAP 参数”（第 107 页）
  - “在硬件 iSCSI 设备上创建数据存储”（第 108 页）
- 软件启动的 iSCSI 存储器配置：
  - “查看软件 iSCSI 启动器属性”（第 110 页）
  - “启动软件 iSCSI 启动器”（第 113 页）
  - “设置软件启动器的目标发现地址”（第 113 页）
  - “设置软件启动器的 CHAP 参数”（第 113 页）
  - “在通过软件启动器访问的 iSCSI 设备上创建数据存储”（第 114 页）
- NAS 存储器配置：

  “装载 NFS 卷”（第 118 页）

- 存储器储管理：

- "将 VMFS-2 升级到 VMFS-3"（第 123 页）
- "编辑数据存储的名称"（第 124 页）
- "将一个或多个扩展添加到数据存储"（第 124 页）
- "移除数据存储"（第 122 页）

- 路径管理：
  - "设置多路径策略"（第 131 页）
  - "设置首选路径"（第 132 页）
  - "禁用路径"（第 132 页）

6 配置存储器

本章包含有关配置本地 SCSI 存储设备、光纤通道 SAN 存储器、iSCSI 存储器以及 NAS 存储器的信息。

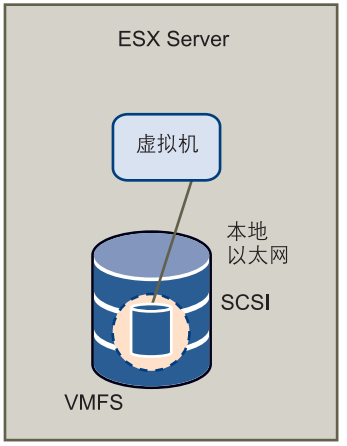
注意 有关配置 SAN 的更多信息，请参见 *《光纤通道 SAN 配置指南》* 和 *《iSCSI SAN 配置指南》*。

本章将讨论以下主题：

本地存储器

本地存储器使用基于 SCSI 的设备，如 ESX Server 3 主机硬盘或任何直接连接至 ESX Server 3 主机的外围专用存储系统。图 6-1 描述了一台使用本地 SCSI 存储器的虚拟机。

图 6-1 本地存储器



在此本地存储器拓扑示例中，ESX Server 3 主机使用单一连接来连接磁盘。可以在该磁盘上创建 VMFS 数据存储，以存储虚拟机磁盘文件。

虽然可以使用这种存储器配置拓扑，但不推荐使用。在存储阵列和 ESX Server 3 主机间使用单一连接会形成*单一故障点 (SPOF)*，在连接不稳定或出现故障时导致中断。为确保一定的容错，部分 DAS 系统支持多个连接路径。请参见 “管理多路径”（第 125 页）。

添加本地存储器

加载本地存储适配器驱动程序时，ESX Server 3 会检测可用的 SCSI 存储设备。在 SCSI 设备上创建新数据存储之前，可能需要重新执行扫描。请参见 “重新执行扫描”（第 115 页）。

在 SCSI 存储设备上创建数据存储时，添加存储器向导将指导您完成所有配置步骤。

在本地 SCSI 磁盘上创建数据存储

1 登录 VI Client，从清单面板中选择服务器。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[硬件 (Hardware)]** 面板下方的 **[存储器 (Storage)]**。

3 单击 **[添加存储器 (Add Storage)]**。

4 选择 **[磁盘 /LUN (Disk/LUN)]** 存储器类型，然后单击 **[下一步 (Next)]**。

5 选择要用于数据存储的 SCSI 设备，然后单击 **[下一步 (Next)]**。

此时将打开 [当前磁盘布局 (Current Disk Layout)] 页面。如果格式化的磁盘是空白磁盘，则 [当前磁盘布局 (Current Disk Layout)] 页面将自动显示整个磁盘空间，以进行存储器配置。

6 如果磁盘不为空，请在 [当前磁盘布局 (Current Disk Layout)] 页面的顶部面板中检查当前磁盘布局，并从底部面板中选择配置选项：

- **[使用整个设备 (Use the entire device)]** - 选择此选项以将整个磁盘或 LUN 专用于单个 VMFS 数据存储。 VMware 建议选择此选项。

警告 如果选择该选项，则先前在此设备上存储的任何文件系统或数据将会被销毁。

- **[使用可用空间 (Use free space)]** - 选择此选项以在剩余的可用磁盘空间中部署 VMFS 数据存储。

7 单击 **[下一步 (Next)]**。

8 在 [磁盘 /LUN- 属性 (Disk/LUN-Properties)] 页面，输入数据存储名称并单击 **[下一步 (Next)]**。

此时会显示 [磁盘 /LUN - 格式化 (Disk/LUN-Formatting)] 页面。

9 如果需要，请调整文件系统和容量值。

默认情况下，存储设备上的全部可用空间均可使用。

10 单击 **[下一步 (Next)]**。

11 在 [即将完成 (Ready to Complete)] 页面，检查数据存储配置信息并单击 **[完成 (Finish)]**。

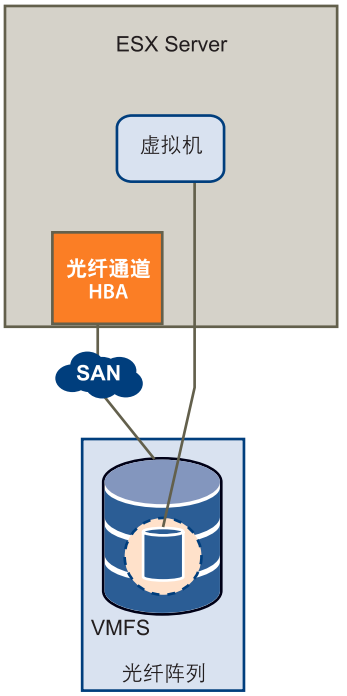
该过程在 ESX Server 3 主机的本地 SCSI 磁盘上创建数据存储。

光纤通道存储器

ESX Server 3 支持光纤通道适配器，可借由该适配器将 ESX Server 3 系统连接至 SAN 并查看其上的磁盘阵列。

图 6-2 描述了使用光纤通道存储器的虚拟机。

图 6-2 光纤通道存储器



在该配置中，ESX Server 3 系统通过光纤通道适配器连接至 SAN Fabric （包括光纤通道交换机及存储阵列）。此时 ESX Server 3 系统可以使用存储阵列的 LUN。可以访问 LUN 并创建用于满足 ESX Server 3 存储需求的数据存储。数据存储采用 VMFS 格式。

其他信息：

- 请参见 “添加光纤通道存储器”（第 97 页）。
- 有关配置 SAN 的详细信息，请参见 *《光纤通道 SAN 配置指南》*。
- 有关 ESX Server 3 支持的 SAN 存储设备的详细信息，请参见 *《存储器 /SAN 兼容性指南》*。
- 有关光纤通道 HBA 的多路径及如何管理路径的详细信息，请参见 “管理多路径”（第 125 页）。

添加光纤通道存储器

在光纤通道设备上创建新数据存储之前，请重新扫描光纤通道适配器，以发现任何新增的 LUN。请参见 “重新执行扫描”（第 115 页）。

在光纤通道存储设备上创建数据存储时，添加存储器向导将指导您完成配置。

在光纤通道设备上创建数据存储

1 登录到 VI Client，然后从清单面板中选择服务器。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[硬件 (Hardware)]** 面板下方的 **[存储器 (Storage)]**。

3 单击 **[添加存储器 (Add Storage)]**。

4 选择 **[磁盘 /LUN (Disk/LUN)]** 存储器类型，然后单击 **[下一步 (Next)]**。

5 选择要用于数据存储的光纤通道设备，然后单击 **[下一步 (Next)]**。

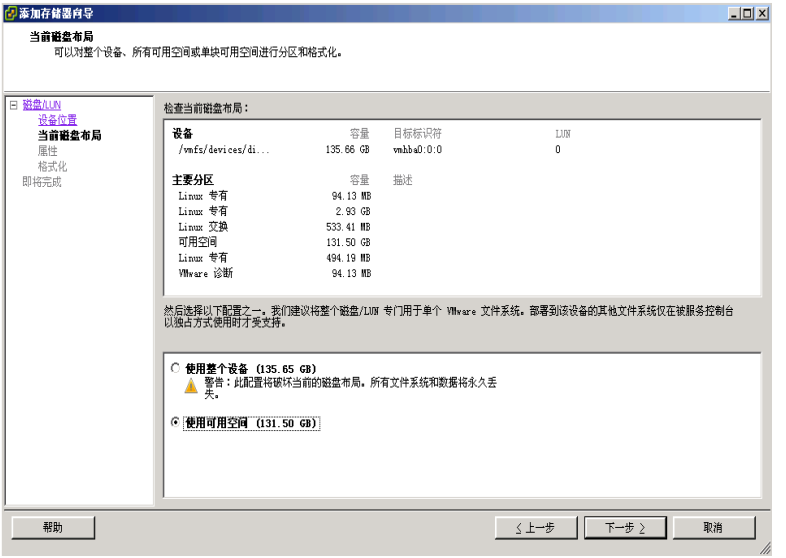
此时将打开 [当前磁盘布局 (Current Disk Layout)] 页面。如果格式化的磁盘是空白磁盘，则 [当前磁盘布局 (Current Disk Layout)] 页面将自动显示整个磁盘空间，以进行存储器配置。

6 如果磁盘不为空，请在 [当前磁盘布局 (Current Disk Layout)] 页面的顶部面板中检查当前磁盘布局，并从底部面板中选择配置选项：

- **[使用整个设备 (Use the entire device)]** - 选择此选项以将整个磁盘或 LUN 专用于单个 VMFS 数据存储。 VMware 建议选择此选项。

警告 如果选择该选项，则先前在此设备上存储的任何文件系统或数据将会被销毁。

- **[使用可用空间 (Use free space)]** - 选择此选项以在剩余的可用磁盘空间中部署 VMFS 数据存储。



7 单击 **[下一步 (Next)]**。

8 在 [磁盘 /LUN- 属性 (Disk/LUN-Properties)] 页面，输入数据存储名称并单击 **[下一步 (Next)]**。

此时会显示 [磁盘 /LUN - 格式化 (Disk/LUN-Formatting)] 页面。

9 如果需要，请调整用于数据存储的文件系统值和容量。

默认情况下，存储设备上的全部可用空间均可使用。

10 单击 **[下一步 (Next)]**。

11 在 [即将完成 (Ready to Complete)] 页面，检查数据存储配置信息并单击 **[完成 (Finish)]**。

该过程在光纤通道磁盘上创建 ESX Server 3 主机数据存储。

12 单击 **[刷新 (Refresh)]**。

有关高级配置 （如使用多路径、掩码以及时区）的信息，请参见 *《光纤通道 SAN 配置指南》*。

iSCSI 存储器

ESX Server 3 支持 iSCSI 技术，通过该技术 ESX Server 3 系统可使用 IP 网络访问远程存储器。借助 iSCSI，可将虚拟机向其虚拟磁盘发出的 SCSI 存储命令转换为 TCP/IP 协议数据包，并将其传输至存储虚拟磁盘的远程设备或目标。对于虚拟机来说，此设备显示为本地附加 SCSI 驱动器。

iSCSI 启动器

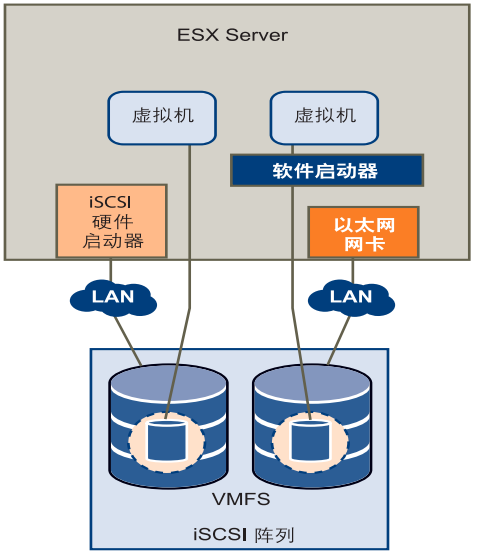
要访问远程目标，ESX Server 3 主机需要使用 iSCSI 启动器。启动器在 IP 网络上的 ESX Server 3 系统和目标存储设备之间传输 SCSI 请求和响应。

ESX Server 3 支持基于硬件和软件的 iSCSI 启动器：

- **硬件 iSCSI 启动器** - iSCSI 超过 TCP/IP 容量的第三方主机总线适配器 (HBA)。此专用 iSCSI 适配器负责所有 iSCSI 处理和管理。
- **软件 iSCSI 启动器** - 嵌入 VMkernel 的代码，可以让 ESX Server 3 系统通过标准网络适配器连接至 iSCSI 存储设备。软件启动器负责 iSCSI 处理，同时通过网络堆栈与网络适配器进行通信。借助软件启动器，无需购买专用硬件即可使用 iSCSI 技术。

图 6-3 描述了两台使用不同类型 iSCSI 启动器的虚拟机。

图 6-3 iSCSI 存储器



在第一个 iSCSI 存储器配置示例中， ESX Server 3 系统采用的是硬件 iSCSI 适配器。该专用 iSCSI 适配器通过 LAN 向磁盘发送 iSCSI 封包。

在第二个示例中，ESX Server 3 系统配置为使用软件 iSCS 启动器。使用软件启动器时，ESX Server 3 系统通过现有网卡连接至 LAN。

命名要求

因为 SAN 可能变得大而复杂，所以使用该网络的所有 iSCSI 启动器和目标均有唯一的、永久的 iSCSI 名称，且分配有访问地址。 iSCSI 名称为特定 iSCSI 设备、启动器或目标提供了正确的标识符，而不管其物理位置如何。

在配置 iSCSI 启动器时，请确保其名称格式正确。启动器可使用以下格式之一：

- **IQN （iSCSI 限定名）** - 最多可包含 255 个字符，格式如下：

  `iqn.<year-mo>.<reversed_domain_name>:<unique_name>`

  其中， `<year-mo>` 代表注册域名时的年份和月份， `<reversed_domain_name>` 为正式域名，而 `<unique_name>` 则为要使用的任意名称，如服务器名称。

  例如：`iqn.1998-01.com.mycompany:myserver`。

- **EUI（扩展的唯一标识符）** - 代表 `eui.` 前缀后跟 16 个字符的名称。对于 IEEE 分配的公司名称，此名称包括 24 位，对于诸如序列号之类的唯一 ID，却包括 40 位。

  例如， `eui.0123456789ABCDEF`。

发现方法

为确定网络上可供访问的存储器资源， ESX Server 3 系统使用以下发现方法：

- **动态发现** - 也称为发送目标发现。每次启动器联系指定的 iSCSI 服务器时，均会将 *发送目标* 请求发送到服务器。服务器通过向启动器提供一个可用目标的列表来做出响应。
- **静态发现** - 启动器不需要执行任何发现。启动器预先知道其将要联系的所有目标，并使用这些目标的 IP 地址和域名与其进行通信。

  静态发现方法仅适用于通过硬件启动器访问 iSCSI 存储器的情况。

iSCSI 安全

由于 iSCSI 技术使用 IP 网络连接远程目标，因此有必要确保连接的安全。 IP 协议本身并不能保护其传输的数据，且不能验证访问网络上目标的启动器的合法性。因此，需要采取特定措施保护 IP 网络安全。

ESX Server 3 支持挑战握手身份验证协议 (CHAP)，iSCSI 启动器可将此协议用于身份验证。当启动器与目标建立初始连接后，CHAP 将对启动器进行身份验证，并检查启动器与目标共享的 CHAP 密码。此操作可在 iSCSI 会话期间定期重复。

配置 ESX Server 3 系统的 iSCSI 启动器时，请核实 iSCSI 存储器是否支持 CHAP，如果支持，应确保为启动器启用 CHAP。请参见 "确保 iSCSI 存储器安全"（第 183 页）。

配置硬件 iSCSI 启动器和存储器

当 ESX Server 3 通过硬件启动器与 iSCSI 存储器通信时，可使用专用的第三方适配器通过 TCP/IP 访问 iSCSI 存储器。此 iSCSI 适配器负责 ESX Server 3 系统的所有 iSCSI 处理和管理。

在设置驻留在 iSCSI 存储器设备上的数据存储之前，请先安装和配置硬件 iSCSI 适配器。

安装和查看 iSCSI 硬件启动器

有关受支持的适配器的详细信息，请参见 VMware 网站 www.vmware.com 上的 *《I/O 兼容性指南》*。

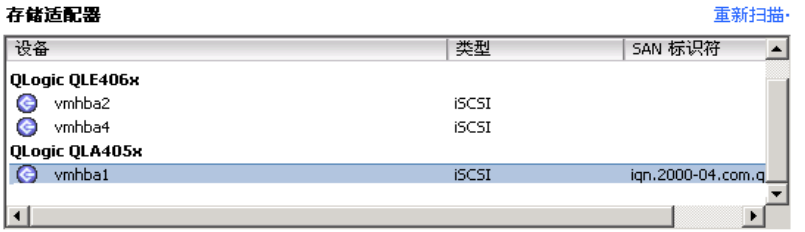
开始配置硬件 iSCSI 启动器之前，请确保 iSCSI HBA 已成功安装并显示在可供配置的适配器列表上。如果启动器已安装，则可查看其属性。

查看硬件 iSCSI 启动器属性

1 登录到 VI Client，然后从清单面板中选择服务器。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[硬件 (Hardware)]** 面板下方的 **[存储适配器 (Storage Adapters)]**。

硬件 iSCSI 启动器显示在存储适配器的列表上。

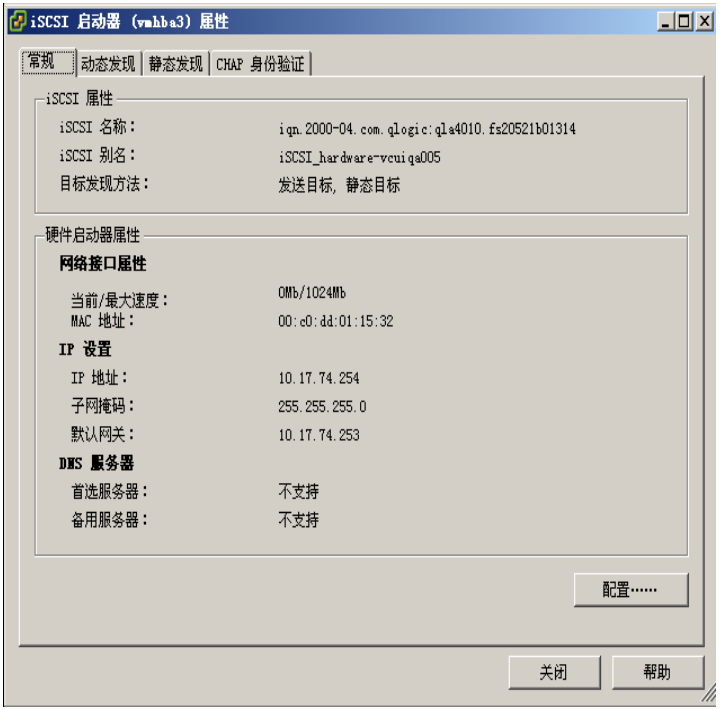


3 选择要配置的启动器。

此时将显示启动器的详细信息，包括型号、IP 地址、iSCSI 名称、发现方法、iSCSI 别名及所发现的任何目标。

4 单击 **[属性 (Properties)]**。

此时会打开 [iSCSI 启动器属性 (iSCSI Initiator Properties)] 对话框。**[常规 (General)]** 选项卡显示了启动器的附加特性。



现在可配置硬件启动器或更改其默认特性。

配置硬件 iSCSI 启动器

配置硬件 iSCSI 启动器时，需要设置启动器的 iSCSI 名称、 IP 地址和发现地址。此外，VMware 建议设置 CHAP 参数。

配置硬件 iSCSI 启动器后，请重新执行扫描，以便该启动器可访问的所有 LUN 均显示在存储设备列表上。请参见 “重新执行扫描”（第 115 页）。

设置命名参数

在配置硬件 iSCSI 启动器时，请确保其名称和 IP 地址的格式正确。

请参见 “命名要求”（第 101 页）。

设置硬件启动器的 iSCSI 名称、别名和 IP 地址

1 在 [iSCSI 启动器属性 (iSCSI Initiator Properties)] 对话框上，单击 **[配置 (Configure)]**。

2 要更改启动器的默认 iSCSI 名称，请输入新的 iSCSI 名称。

可以使用供应商提供的默认名称。如果更改默认名称，要确保输入的新名称具有正确的格式。否则，一些存储设备可能不能识别硬件 iSCSI 启动器。

3 输入 iSCSI 别名。

别名是一种名称，可用于识别硬件 iSCSI 启动器。

4 在 **[硬件启动器属性 (Hardware Initiator Properties)]** 组中输入所有所需的值。

5 单击 **[确定 (OK)]** 以保存更改。

6 重新引导服务器使更改生效。

设置硬件启动器的发现地址

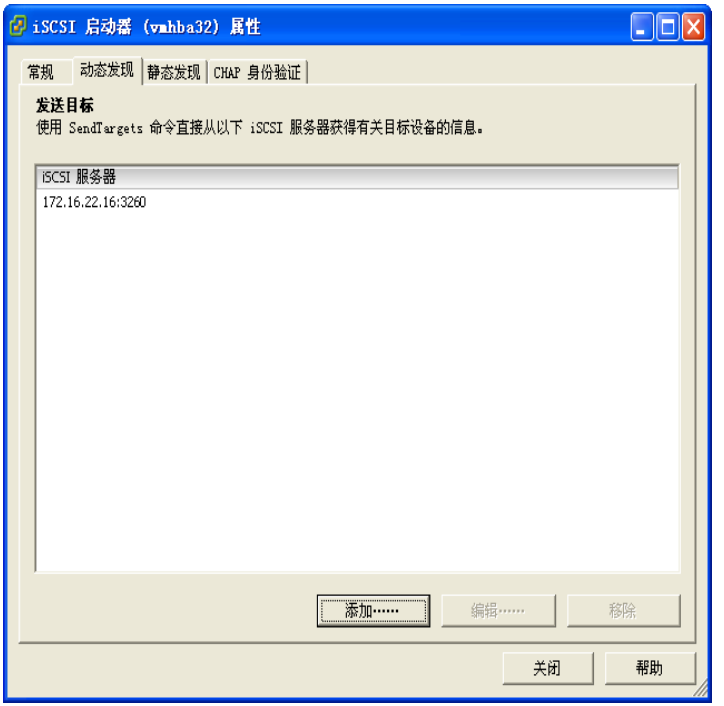
设置目标发现地址，以便硬件启动器确定网络上可供访问的存储器资源。可以通过动态发现或静态发现来进行此设置。

请参见 “发现方法”（第 101 页）。

采用动态发现时，特定的 iSCSI 服务器会向 ESX Server 3 主机提供目标列表。

使用动态发现设置目标发现地址

1 在 [iSCSI 启动器属性 (iSCSI Initiator Properties)] 对话框中，单击 **[动态发现 (Dynamic Discovery)]** 选项卡。



2 要添加新的 iSCSI 服务器以供 ESX Server 3 主机用于动态发现会话，请单击 **[添加 (Add)]**。

3 在 [添加发送目标服务器 (Add Send Targets Server)] 对话框中，输入 iSCSI 服务器的 IP 地址，然后单击 **[确定 (OK)]**。

ESX Server 3 主机与该服务器建立动态发现会话之后，该服务器将做出响应并提供可用于 ESX Server 3 主机的目标列表。这些目标的名称和 IP 地址显示在 **[静态发现 (Static Discovery)]** 选项卡上。

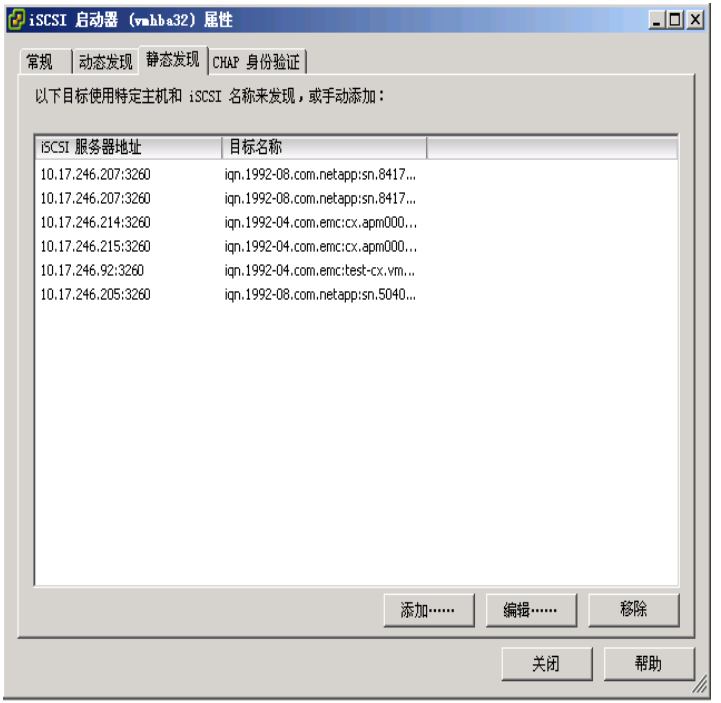
4 要更改 iSCSI 的 IP 地址或移除服务器，请选择 IP 地址并单击 **[编辑 (Edit)]** 或 **[移除 (Remove)]**。

使用硬件启动器时，除了动态发现方法，还可以使用静态发现来手动输入要联系的目标的 IP 地址和 iSCSI 名称。

使用静态发现设置目标发现地址

1 在 [iSCSI 启动器属性 (iSCSI Initiator Properties)] 对话框中，单击 **[静态发现 (Static Discovery)]** 选项卡。

如果先前使用了动态发现方法，则该选项卡会显示 iSCSI 服务器向 ESX Server 3 主机提供的所有目标。



2 要添加目标，可单击 **[添加 (Add)]** 并输入目标的 IP 地址和完全合格的名称。

3 要更改或删除特定目标，请选择目标并单击 **[编辑 (Edit)]** 或 **[移除 (Remove)]**。

注意 如果移除了通过动态发现添加的一个目标，则该目标可在下次进行重新扫描、重置 HBA 或重新引导系统时返加到列表中，

设置硬件启动器的 CHAP 参数

配置硬件 iSCSI 启动器时，应验证是否在 iSCSI 存储器上启用了 CHAP。如果已启用，则需要为启动器启用 CHAP，确保 CHAP 身份验证凭据与 iSCSI 存储器匹配。

请参见 “iSCSI 安全”（第 101 页）。

设置硬件启动器的 CHAP 参数

1 在 [iSCSI 启动器属性 (iSCSI Initiator Properties)] 对话框上，单击 **[CHAP 身份验证 (CHAP Authentication)]** 选项卡。

此时选项卡会显示默认的 CHAP 参数 （如果有）。

2 要对现有 CHAP 参数作出任何更改，请单击 **[配置 (Configure)]**。

3 要使 CHAP 保持启用状态，请选择 **[使用以下 CHAP 凭据 (Use the following CHAP credentials)]**。

4 输入新的 CHAP 名称或选择 **[使用启动器名称 (Use initiator name)]**。

5 如果需要，请指定 CHAP 密码。

所有新目标均将使用此 CHAP 密码对启动器进行身份验证。

6 单击 **[确定 (OK)]** 以保存更改。

注意 如果禁用 CHAP，则现有会话会保持到重新引导 ESX Server 3 主机或存储系统强制注销之时。之后，您不能再连接到需要 CHAP 的目标。

添加可通过硬件启动器访问的 iSCSI 存储器

在可通过硬件启动器访问的 iSCSI 存储设备上创建数据存储时，添加存储器向导将指导您完成配置。

在硬件 iSCSI 设备上创建数据存储

1 登录到 VI Client，然后从清单面板中选择服务器。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[硬件 (Hardware)]** 面板下方的 **[存储器 (Storage)]**。

3 单击 **[添加存储器 (Add Storage)]**。

4 选择 **[磁盘 /LUN (Disk/LUN)]** 存储器类型，然后单击 **[下一步 (Next)]**。

5 选择要用于数据存储的 iSCSI 设备，然后单击 **[下一步 (Next)]**。

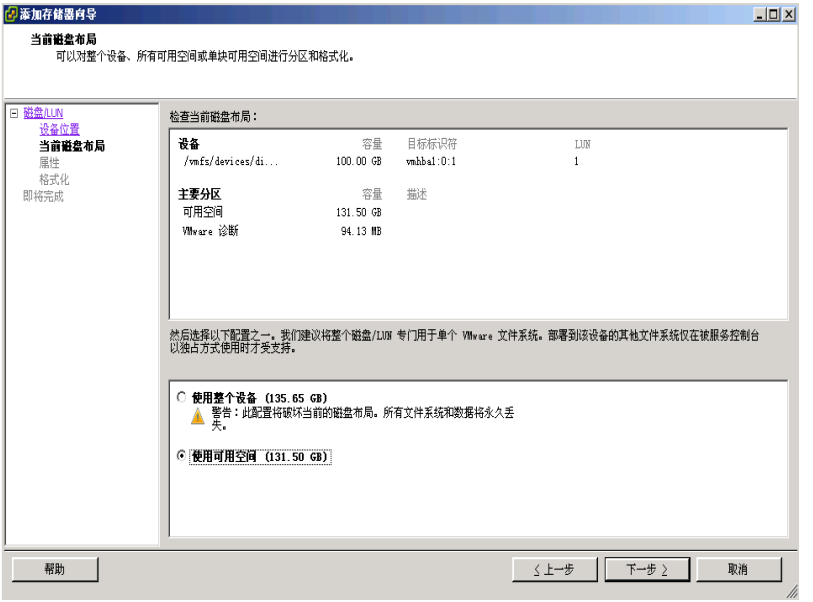
此时将打开 [当前磁盘布局 (Current Disk Layout)] 页面。如果格式化的磁盘是空白磁盘，则 [当前磁盘布局 (Current Disk Layout)] 页面将自动显示整个磁盘空间，以进行存储器配置。

6 如果磁盘不为空，请在 [当前磁盘布局 (Current Disk Layout)] 页面的顶部面板中检查当前磁盘布局，并从底部面板中选择配置选项：

- **[使用整个设备 (Use the entire device)]** - 选择此选项以将整个磁盘或 LUN 专用于单个 VMFS 数据存储。 VMware 建议选择此选项。

警告 如果选择该选项，则先前在此设备上存储的任何文件系统或数据将会被销毁。

- **[使用可用空间 (Use free space)]** - 选择此选项以在剩余的可用磁盘空间中部署 VMFS 数据存储。



7 单击 **[下一步 (Next)]**。

8 在 [磁盘 /LUN- 属性 (Disk/LUN-Properties)] 页面，输入数据存储名称并单击 [下一步 (Next)]。

9 如果需要，请调整用于数据存储的文件系统值和容量。默认情况下，存储设备上的全部可用空间均可使用。

10 单击 **[下一步 (Next)]**。

11 检查数据存储信息，然后单击 **[完成 (Finish)]**。

该过程在硬件启动 iSCSI 设备上创建数据存储。

12 单击 **[刷新 (Refresh)]**。

配置软件 iSCSI 启动器和存储器

借助基于软件的 iSCSI 实施，可使用标准网络适配器将 ESX Server 3 系统连接至 IP 网络上的远程 iSCSI 目标。 VMkernel 中嵌入的 ESX Server 3 软件 iSCSI 启动器为该连接提供了便利，因为其可通过网络堆栈与网络适配器进行通信。

配置使用软件启动器访问 iSCSI 存储器的数据存储之前，请启用网络连接，然后配置软件 iSCSI 启动器。

设置可通过软件启动器访问的 iSCSI 存储器

准备和设置使用软件启动器访问 iSCSI 存储设备的数据存储时，请执行以下步骤。

1 创建 VMkernel 端口以处理 iSCSI 网络。

请参见 “VMkernel 网络配置”（第 28 页）和 “软件 iSCSI 存储器的网络配置”（第 64 页）。

2 为软件 iSCSI 配置服务控制台连接。

请参见 “为支持的服务和管理代理打开防火墙端口”（第 171 页）。

3 配置软件 iSCSI 启动器。

请参见 “配置软件 iSCSI 启动器”（第 112 页）。

4 重新扫描新的 iSCSI LUN。

请参见 “重新执行扫描”（第 115 页）。

5 设置数据存储。

请参见 “添加可通过软件启动器访问的 iSCSI 存储器”（第 114 页）。

查看软件 iSCSI 启动器

ESX Server 3 系统用于访问 iSCSI 存储设备的软件 iSCSI 适配器显示于可用适配器列表中。可使用 VI Client 检查其属性。

查看软件 iSCSI 启动器属性

1 登录到 VI Client，然后从清单面板中选择服务器。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[硬件 (Hardware)]** 面板下方的 **[存储适配器 (Storage Adapters)]**。

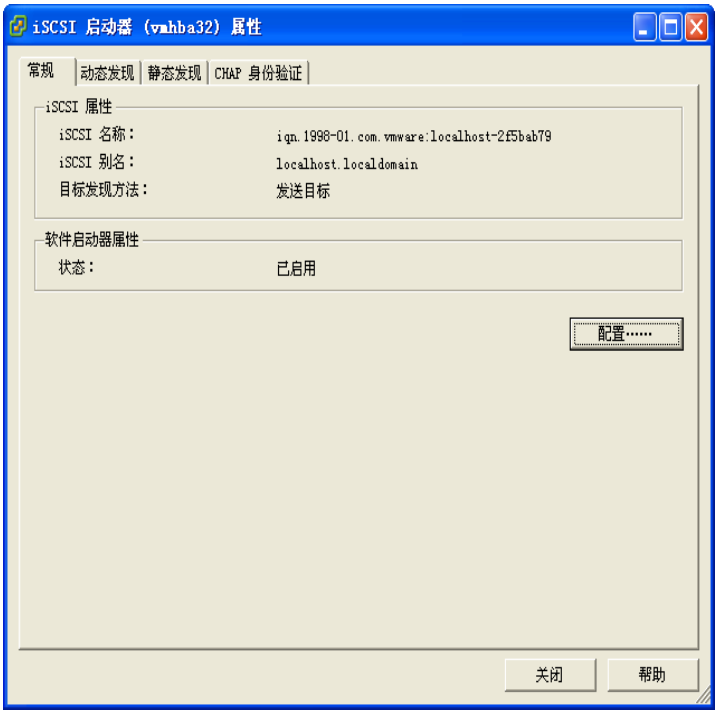
此时会显示可用存储适配器的列表。

3 在 iSCSI 软件适配器下方，选择可用的软件启动器。

如果启用了启动器，[详细信息 (Details)] 面板将显示启动器的型号、 IP 地址、 iSCSI 名称、发现方法、 iSCSI 别名及所发现的任何目标。

4 单击 **[属性 (Properties)]**。

此时会打开 [iSCSI 启动器属性 (iSCSI Initiator Properties)] 对话框。**[常规 (General)]** 选项卡显示了软件启动器的附加特性。



现在可配置软件启动器或更改其默认特性。

配置软件 iSCSI 启动器

配置软件 iSCSI 启动器时，请启用启动器，并设置其目标地址。 VMware 还建议设置 CHAP 参数。配置软件 iSCSI 启动器后，请重新执行扫描，以便该启动器可访问的所有 LUN 均可显示在可用于 ESX Server 3 系统的存储设备列表上。请参见 “重新执行扫描”（第 115 页）。

启用软件 iSCSI 启动器

启用软件 iSCSI 启动器，以便 ESX Server 3 可使用该启动器。

启动软件 iSCSI 启动器

1 在 [iSCSI 启动器属性 (iSCSI Initiator Properties)] 对话框上，单击 **[配置 (Configure)]**。

2 要启用启动器，请选择 **[已启用 (Enabled)]**。

3 要更改启动器的默认 iSCSI 名称，请输入新的名称。

确保输入的名称具有正确的格式。否则，一些存储设备不会识别软件 iSCSI 启动器。请参见 “命名要求”（第 101 页）。

4 单击 **[确定 (OK)]** 保存更改。

设置软件启动器的发现地址

设置目标发现地址，以便软件启动器确定网络上可供访问的存储器资源。

注意 采用软件启动器时，只有动态发现方法可用。

请参见 “发现方法”（第 101 页）。

设置软件启动器的目标发现地址

1 在 [iSCSI 启动器属性 (iSCSI Initiator Properties)] 对话框中，单击 **[动态发现 (Dynamic Discovery)]** 选项卡。

2 要添加 ESX Server 3 主机可用于动态发现会话的新 iSCSI 目标，请单击 **[添加 (Add)]**。

3 输入发送目标服务器 IP 地址，然后单击 **[确定 (OK)]**。

4 要更改或删除发送目标服务器，请选择服务器并单击 **[编辑 (Edit)]** 或 **[移除 (Remove)]**。

设置软件启动器的 CHAP 参数

当配置软件 iSCSI 启动器时，应验证是否已在 iSCSI 存储器上启用 CHAP。如果已启用，则需要为启动器启用 CHAP，确保 CHAP 身份验证凭据与 iSCSI 存储器匹配。

请参见 “iSCSI 安全”（第 101 页）。

设置软件启动器的 CHAP 参数

1 在 [iSCSI 启动器属性 (iSCSI Initiator Properties)] 对话框上，单击 **[CHAP 身份验证 (CHAP Authentication)]** 选项卡。

2 要指定 CHAP 参数，请单击 **[配置 (Configure)]**。

3 要使 CHAP 保持启用状态，请选择 **[使用以下 CHAP 凭据 (Use the following CHAP credentials)]**。

4 输入 CHAP 名称或选择 **[使用启动器名称 (Use initiator name)]**。

5 如果需要，请指定 CHAP 密码。

所有新目标均将使用此 CHAP 密码对启动器进行身份验证。

6 单击 **[确定 (OK)]** 保存更改。

注意 如果禁用 CHAP，则现有会话会保持到重新引导 ESX Server 3 主机或存储系统强制注销之时。之后，您不能再连接到需要 CHAP 的目标。

添加可通过软件启动器访问的 iSCSI 存储器

在可通过软件启动器访问的 iSCSI 存储设备上创建数据存储时，添加存储器向导将指导您完成配置。

在通过软件启动器访问的 iSCSI 设备上创建数据存储

1 登录到 VI Client，然后从清单面板中选择服务器。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[硬件 (Hardware)]** 面板下方的 **[存储器 (Storage)]**。

3 单击 **[添加存储器 (Add Storage)]**。

4 选择 **[磁盘 /LUN (Disk/LUN)]** 存储器类型，然后单击 **[下一步 (Next)]**。

5 选择要用于数据存储的 iSCSI 设备，然后单击 **[下一步 (Next)]**。

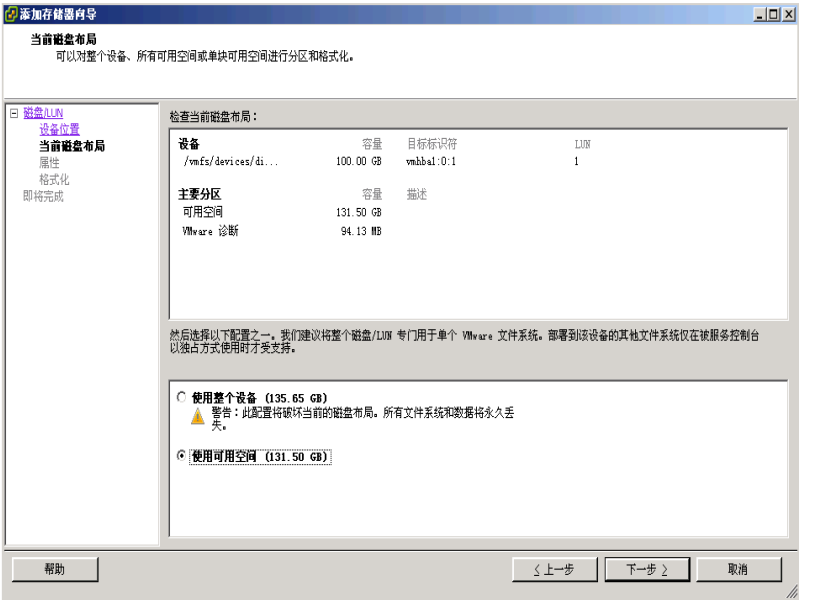
此时将打开 [当前磁盘布局 (Current Disk Layout)] 页面。如果格式化的磁盘是空白磁盘，则 [当前磁盘布局 (Current Disk Layout)] 页面将自动显示整个磁盘空间，以进行存储器配置。

6 如果磁盘不为空，请在 [当前磁盘布局 (Current Disk Layout)] 页面的顶部面板中检查当前磁盘布局，并从底部面板中选择配置选项：

- **[使用整个设备 (Use the entire device)]** - 选择此选项以将整个磁盘或 LUN 专用于单个 VMFS 数据存储。 VMware 建议选择此选项。

警告 如果选择该选项，则先前在此设备上存储的任何文件系统或数据将会被销毁。

- **[使用可用空间 (Use free space)]** - 选择此选项以在剩余的可用磁盘空间中部署 VMFS 数据存储。



7 单击 **[下一步 (Next)]**。

8 在 [磁盘 /LUN- 属性 (Disk/LUN-Properties)] 页面，输入数据存储名称并单击 [下一步 (Next)]。

9 如果需要，请调整用于数据存储的文件系统值和容量。默认情况下，存储设备上的全部可用空间均可使用。

10 单击 **[下一步 (Next)]**。

11 检查数据存储信息，然后单击 **[完成 (Finish)]**。

该过程在软件 iSCSI 存储设备上创建数据存储。

12 单击 **[刷新 (Refresh)]**。

重新执行扫描

如果发生以下任一事件，请重新执行扫描：

- 对可供 ESX Server 3 系统使用的存储磁盘或 LUN 进行了更改。
- 对存储适配器进行了更改。

- 创建新的数据存储或移除现有数据存储。
- 重新配置现有数据存储，例如添加新的扩展。

注意 屏蔽所有指向 LUN 的路径之后，应重新扫描所有提供指向 LUN 的路径的适配器，以便更新配置。

重新执行扫描

1 在 VI Client 中，选择一个主机，然后单击 **[配置 (Configuration)]** 选项卡。

2 选择 [硬件 (Hardware)] 面板中的 **[存储适配器 (Storage Adapters)]**，单击 [存储适配器 (Storage Adapters)] 面板上方的 **[重新扫描 (Rescan)]**。

注意 也可右键单击一个适配器，并单击 **[重新扫描 (Rescan)]** 仅重新扫描该适配器。

3 要发现新的磁盘或 LUN，请选择 **[扫描新的存储设备 (Scan for New Storage Devices)]**。

新发现的 LUN 将出现在磁盘 /LUN 列表上。

4 要发现新的数据存储或在其配置更改后更新数据存储，请选择 **[扫描新的 VMFS 卷 (Scan for New VMFS Volumes)]**。

发现的新数据存储或 VMFS 卷将出现在数据存储列表上。

网络附加存储

本节包含有关网络附加存储 (NAS) 的信息。

ESX Server 3 支持通过 NFS 协议使用 NAS。

虚拟机如何使用 NFS

ESX Server 3 支持的 NFS 协议可启用 NFS 客户端和 NFS 服务器之间的通信。客户端向服务器发送信息请求，并获取服务器回复的结果。

ESX Server 3 中嵌入的 NFS 客户端可让您访问 NFS 服务器和使用 NFS 卷进行存储。ESX Server 3 仅支持 TCP 上的 NFS 版本 3。

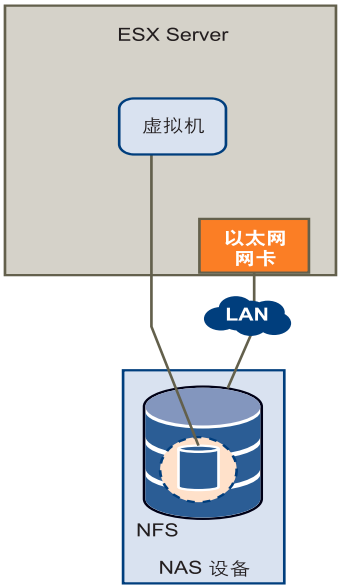
可使用 VI Client 将 NFS 卷配置为数据存储。已配置的 NFS 数据存储会显示在 VI Client 中，可将之用来存储虚拟磁盘文件，使用方式与基于 VMFS 的数据存储相同。

在基于 NFS 的数据存储上创建的虚拟磁盘采用由 NFS 服务器规定的磁盘格式，通常为精简磁盘格式，要求按需分配空间。如果在向该磁盘写入数据时出现虚拟机空间不足，VI Client 会通知您需要更多空间。这时您有以下选择：

- 在卷上释放更多空间，以便虚拟机能继续写磁盘操作。
- 终止虚拟机会话。终止会话将关闭虚拟机。

图 6-4 描述使用 NFS 卷存储其文件的虚拟机。

图 6-4 NFS 存储器



在该配置中， ESX Server 3 连接到存储虚拟磁盘文件的 NFS 服务器。

警告 当 ESX Server 3 访问基于 NFS 的数据存储上的虚拟机磁盘文件时，会在该磁盘文件所驻留的同一目录中生成一个特殊的 `.lck-XXX` 锁定文件，以阻止其他 ESX Server 3 主机访问该虚拟磁盘文件。不要移除 `.lck-XXX` 锁文件，因为如果没有该文件，正在运行的虚拟机将无法访问其虚拟磁盘文件。

NFS 卷和虚拟机委派用户

如果计划在基于 NFS 的数据存储上创建、配置或管理虚拟机，需要为一位特殊用户（叫作委派用户）分配 NFS 访问特权。

默认情况下，ESX Server 3 主机的委派用户为 `root`。但是，使用 `root` 作为委派用户可能不适用于所有 NFS 卷。有时，为使 NFS 卷免遭非授权访问，NFS 管理员会在导出卷时开启 `root squash` 选项。开启 `root squash` 时，NFS 服务器会将超级用户访问视为任何非特权用户访问，并可能拒绝 ESX Server 3 主机访问存储在 NFS 卷上的虚拟机文件。

可通过 ESX Server 3 的试验性功能将委派用户更改为其他身份。该身份必须与 NFS 服务器上目录的所有者匹配，否则 ESX Server 3 主机无法执行文件级操作。

请参见 "NFS 存储器的虚拟机委派"（第 206 页）。

小心 更改 ESX Server 3 主机的委派用户仅为试验性功能，VMware 仅对该功能提供有限支持。

配置 ESX Server 3 访问 NFS 卷

NFS 需要网络连接，以访问存储在远程服务器上的数据。在配置 NFS 之前，必须先为 VMotion 和 IP 存储器配置网络。

有关配置网络的详细信息，请参见 "VMkernel 网络配置"（第 28 页）。

创建基于 NFS 的数据存储

在 NFS 卷上创建数据存储时，添加存储器向导将指导您完成所有配置步骤。

装载 NFS 卷

1 登录到 VI Client，然后从清单面板中选择服务器。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[硬件 (Hardware)]** 面板下方的 **[存储器 (Storage)]**。

3 单击 **[添加存储器 (Add Storage)]**。

4 选择 **[网络文件系统 (Network File System)]** 作为存储器类型，然后单击 **[下一步 (Next)]**。

5 输入服务器名称、装载点文件夹名称以及数据存储名称。

6 单击 **[下一步 (Next)]**。

7 在 [网络文件系统摘要 (Network File System Summary)] 页面中，检查配置选项，然后单击 **[完成 (Finish)]**。

创建诊断分区

要成功运行，您的 ESX Server 3 需要具有用于存储核心转储的诊断分区或转储分区，以提供调试和技术支持。可在本地磁盘和专用或共享的 SAN LUN 上创建诊断分区。

诊断分区不能位于可通过软件启动器访问的 iSCSI LUN 上。

每台 ESX Server 3 主机均必须拥有一个 100 MB 的诊断分区。如果多台 ESX Server 3 主机共享一个 SAN，则请为每台主机配置一个 100 MB 的诊断分区。

注意 如果在安装 ESX Server 3 时选择了 **[建议的分区 (Recommended Partitioning)]**，安装程序将自动为您的主机创建一个诊断分区。**[诊断 (Diagnostic)]** 选项不会在 [选择存储类型 (Select Storage Type)] 页面上出现。如果在安装期间选择了 **[高级分区 (Advanced Partitioning)]** 选项并选择不指定诊断分区，则需要立即配置。有关 ESX Server 3 分区的详细信息，请参见 *《安装指南》*。

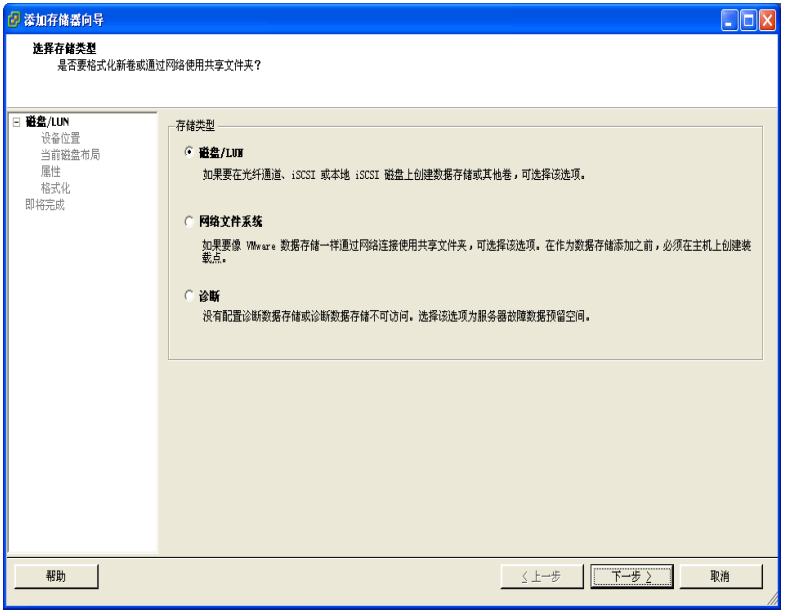
创建诊断分区

1 登录到 VI Client，然后从清单面板中选择服务器。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[硬件 (Hardware)]** 面板下方的 **[存储器 (Storage)]**。

3 单击 **[添加存储器 (Add Storage)]**。

此时 [选择存储类型 (Select Storage Type)] 页面将出现。



4 选择 **[诊断 (Diagnostic)]** 并单击 **[下一步 (Next)]**。

如果看不到 **[诊断 (Diagnostic)]** 选项，则表示 ESX Server 3 主机已拥有诊断分区。可使用 `esxcfg-dumppart` 服务控制台命令查询和扫描主机的诊断分区。请参见"ESX Server 3 技术支持命令"（第 247 页）。

5 指定诊断分区类型：

- **[专用本地存储器 (Private Local)]**- 在本地磁盘上创建诊断分区。此分区将仅存储 ESX Server 3 主机的故障信息。
- **[专用 SAN 存储器 (Private SAN Storage)]** - 在非共享 SAN LUN 上创建诊断分区。此分区将仅存储 ESX Server 3 主机的故障信息。
- **[共享 SAN 存储器 (Shared SAN Storage)]**- 在共享 SAN LUN 上创建诊断分区。此分区将由多个主机访问并且会存储多个主机的故障信息。

单击 **[下一步 (Next)]**。

6 选择要用于诊断分区的设备，然后单击 **[下一步 (Next)]**。

7 检查分区配置信息，然后单击 **[完成 (Finish)]**。

7 管理存储器

本章包含有关管理现有数据存储和包含数据存储的文件系统的信息。本章将讨论以下主题：

管理数据存储

ESX Server 3 系统使用数据存储来存储与其虚拟机关联的所有文件。数据存储是一个逻辑存储单元，它可以使用一个物理设备、一个磁盘分区或若干个物理设备上的磁盘空间。数据存储可以存在于不同类型的物理设备 （包括 SCSI、 iSCSI、光纤通道 SAN 或 NFS）上。

注意 除了使用数据存储之外，虚拟机还可以使用映射文件 (RDM) 作为代理来直接访问裸设备。请参见 “裸设备映射特点”（第 137 页）。

有关数据存储的详细信息，请参见 “数据存储”（第 80 页）。

可使用以下方式之一将数据存储添加到 VI Client 中：

- 当主机添加到清单时发现。将主机添加到清单中时， VI Client 会显示主机可以识别的所有数据存储。
- 在可用存储设备上创建。可以使用 **[添加存储器 (Add Storage)]** 命令来创建和配置新的数据存储。

数据存储一经创建，即可用于存储虚拟机文件。另外，您还可根据需要更改数据存储，如向数据存储中添加扩展，或重命名、移除数据存储。

可以移除不用的数据存储。

小心 从 ESX Server 3 系统移除数据存储会断开系统与保存数据存储的存储设备之间的连接，并停止该存储设备的所有功能。

不能移除目前运行的虚拟机的虚拟磁盘所在的数据存储。

移除数据存储

1 登录到 VI Client，然后从清单面板中选择服务器。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[存储器 (Storage)]**。

3 选择要移除的数据存储，然后单击 **[移除 (Remove)]**。

4 确认要移除数据存储。

5 在可以看到数据存储的所有服务器上执行重新扫描。

编辑 VMFS 数据存储

使用 VMFS 格式的数据存储部署在基于 SCSI 的存储设备上。

创建基于 VMFS 的数据存储以后，可以通过重命名或扩展进行修改。如果有任何 VMFS-2 数据存储，可将其升级到 VMFS-3 格式。

升级数据存储

ESX Server 3 包括 VMFS 版本 3 (VMFS-3)。如果已用 VMFS-2 格式化了数据存储，则可以读取存储在 VMFS-2 中的文件，但不能使用它们。要使用文件，将 VMFS-2 升级为 VMFS-3。

将 VMFS-2 升级到 VMFS-3 时， ESX Server 3 文件锁定机制可以确保没有远程 ESX Server 3 或本地进程正在访问正在转换的 VMFS 卷。ESX Server 3 会保留数据存储上的所有文件。

使用升级选项之前，请考虑以下注意事项：

- 提交或放弃对要升级的 VMFS-2 卷中虚拟磁盘的任何更改。
- 备份要升级的 VMFS-2 卷。
- 确保没有已启动的虚拟机在使用此 VMFS-2 卷。
- 确保无其他 ESX Server 主机在访问此 VMFS-2 卷。

小心 VMFS-2 转换为 VMFS-3 是一种单向进程。将基于 VMFS 的数据存储转换为 VMFS-3 后，不能将其恢复为 VMFS-2。

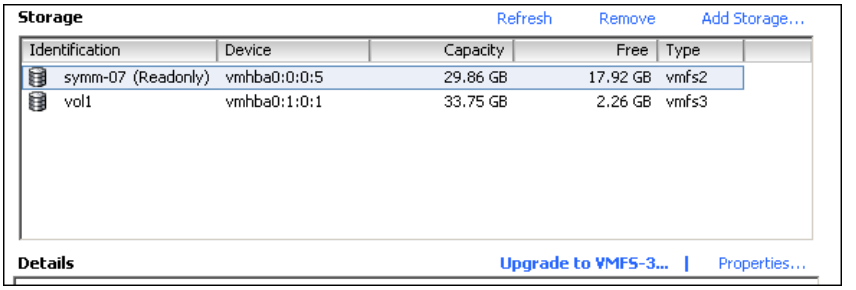
若要升级 VMFS-2 文件系统，其文件块大小不应超过 8 MB。

将 VMFS-2 升级到 VMFS-3

1 登录到 VI Client，然后从清单面板中选择服务器。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[存储器 (Storage)]**。

3 选择使用 VMFS-2 格式的数据存储。



4 单击 **[升级到 VMFS-3 (Upgrade to VMFS-3)]**。

5 在可以看到数据存储的所有主机上执行重新扫描。

更改数据存储的名称

可更改现有的基于 VMFS 的数据库名称。

编辑数据存储的名称

1 登录到 VI Client，然后从清单面板中选择服务器。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[存储器 (Storage)]**。

3 选择要编辑其名称的数据存储，单击 **[属性 (Properties)]** 链接。

4 在 [常规 (General)] 面板中，单击 **[更改 (Change)]**。

5 输入新的数据存储名称，然后单击 **[确定 (OK)]**。

将扩展添加到数据存储

通过附加硬盘分区作为扩展，可以扩展使用 VMFS 格式的数据存储。数据存储可以跨越 32 个物理存储扩展。

当您需要在此数据存储上创建新的虚拟机时，或者当此数据存储上运行的虚拟机需要更多空间时，可以动态地将新的扩展添加到数据存储。

将一个或多个扩展添加到数据存储

1 登录到 VI Client，然后从清单面板中选择服务器。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[存储器 (Storage)]**。

3 选择要扩展的数据存储，然后单击 **[属性 (Properties)]**。

4 在 [扩展 (Extents)] 面板中，单击 **[添加扩展 (Add Extent)]**。

5 选择要作为新扩展添加的磁盘，然后单击 **[下一步 (Next)]**。

6 检查用作扩展的当前磁盘布局，以确保该磁盘未包含任何重要信息。

小心 如果所添加的磁盘或分区先前已格式化，则将对其进行重新格式化，所包含的文件系统和任何数据均将丢失。

7 设置扩展的容量。

默认情况下，存储设备上的全部可用空间均可供使用。

8 单击 **[下一步 (Next)]**。

9 检查建议的扩展布局和数据存储的新配置，然后单击 **[完成 (Finish)]**。

10 在可以看到数据存储的所有服务器上执行重新扫描。

管理多路径

为了维持 ESX Server 3 主机和直接连接或网络连接的存储器之间的持续连接， ESX Server 3 支持多路径。*多路径* 是一种技术，可让您使用路径上的多个物理元素，这些元素负责在 ESX Server 3 主机和外部存储设备之间传输数据。万一路径上的任何元素（HBA、交换机、存储处理器 (SP) 或电缆）发生故障， ESX Server 3 可以使用冗余路径。检测故障路径并切换到另一条路径的过程称为*路径故障切换*。使用故障切换路径的这种做法有助于确保 ESX Server 3 系统和存储设备之间的不间断流量。ESX Server 3 不需要特定的故障切换驱动程序即可支持多路径。

注意 如果指向存储虚拟机磁盘的存储设备的所有路径都不可用，则虚拟机将以无法预知的方式发生故障。

默认情况下，在任何特定时间， ESX Server 3 主机仅使用一个路径 （称为*活动路径*）来与特定存储设备进行通信。

选择活动路径时， ESX Server 3 遵循以下多路径策略：

- **[最近使用 (Most Recently Used)]** - ESX Server 3 主机选择最近使用的路径作为活动路径。如果此路径不可用，则主机会切换到备用路径并继续使用新路径作为活动路径。

  对于*主动 / 被动* 存储阵列，需要使用 [最近使用 (Most Recently Used)] 策略；在这种阵列中，一个存储处理器保持被动状态，等待另一个存储处理器发生故障。

- **[固定的 (Fixed)]** - ESX Server 3 主机始终使用指向存储设备的指定首选路径作为活动路径。如果 ESX Server 3 主机无法通过首选路径访问存储器，它会尝试随后成为活动路径的备用路径。一旦首选路径可用，主机就会自动恢复到首选路径。

VMware 建议将 [固定的 (Fixed)] 策略用于*主动 / 主动*存储阵列；在这种阵列中，所有存储处理器都可以传递存储流量，所有路径都可以一直处于活动状态，除非路径发生故障。大多数 iSCSI 存储系统均为主动 / 主动。

注意 VMware 建议不要手动将 **[最近使用 (Most Recently Used)]** 更改为 **[固定的 (Fixed)]**。系统会自动为有需要的阵列设置此策略。

- **[循环 (Round Robin)]** - ESX Server 3 主机将自动轮流选择所有可用的路径。除了路径故障切换，循环还支持路径间的负载平衡。

  在此版本中，循环负载平衡为试验性功能，不支持供生产使用。请参见 *《循环负载平衡》*白皮书。

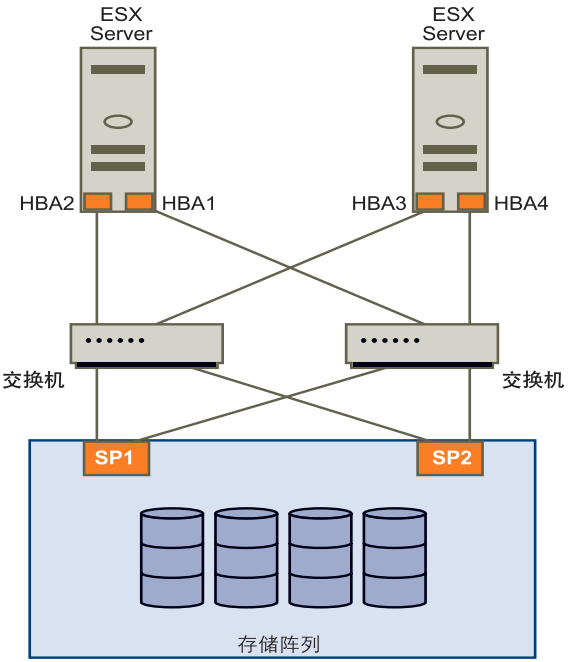
本地存储和光纤通道 SAN 中的多路径

在最简单的多路径本地存储拓扑结构中，可以使用一个具有两个 HBA 的 ESX Server 3 主机。 ESX Server 3 主机通过两根电缆连接到双端口本地存储系统。使用这种配置时，如果 ESX Server 3 主机和本地存储系统之间的某个连接元素发生故障，可以确保容错。

为了支持 FC SAN 中的路径切换，ESX Server 3 主机通常具有两个或更多可用的 HBA ；使用一个或多个交换机可以从这些 HBA 到达存储阵列。或者，设置可以包括一个 HBA 和两个存储处理器，以便 HBA 可以使用不同的路径到达磁盘阵列。

在图 7-1 中，多条路径将每台服务器与存储设备相连。例如，如果 HBA1 或 HBA1 和交换机之间的链路发生故障，HBA2 会取代 HBA1 并提供服务器和交换机之间的连接。一个 HBA 取代另一个 HBA 的过程称为 HBA 故障切换。

图 7-1 光纤通道多路径



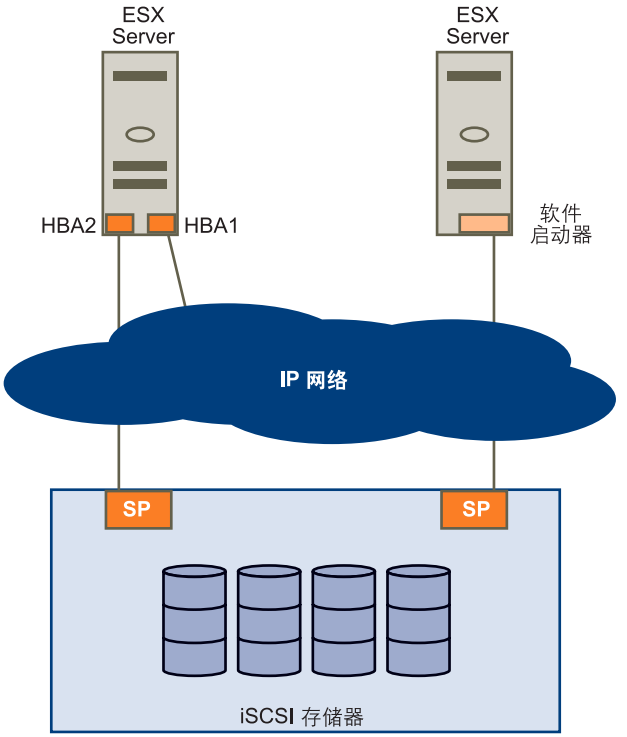
类似地，如果 SP1 或 SP1 和交换机之间的链路中断，SP2 会取代 SP1 并提供交换机和存储设备之间的连接。此过程称为 SP 故障切换。 VMware ESX Server 3 通过多路径功能支持 HBA 和 SP 故障切换。

请参见 *《光纤通道 SAN 配置指南》*。

iSCSI SAN 中的多路径

在 iSCSI 存储中，ESX Server 3 会利用 IP 网络中内置的多路径支持，允许网络执行路由操作，如图 7-2 所示。通过动态发现， iSCSI 启动程序获得目标地址列表，启动程序可以使用这些地址作为通往 iSCSI LUN 的多条路径来实现故障切换目的。

图 7-2 iSCSI 多路径



此外，借助软件启动的 iSCSI，可以使用网卡绑定，以便通过 VMkernel 中的网络层执行多路径操作。请参见 “网络”（第 17 页）。

请参见 *《iSCSI SAN 配置指南》*。

查看当前的多路径状态

可以使用 VI Client 来查看当前的多路径状况。

查看当前的多路径状况

1 登录到 VI Client，然后从清单面板中选择服务器。

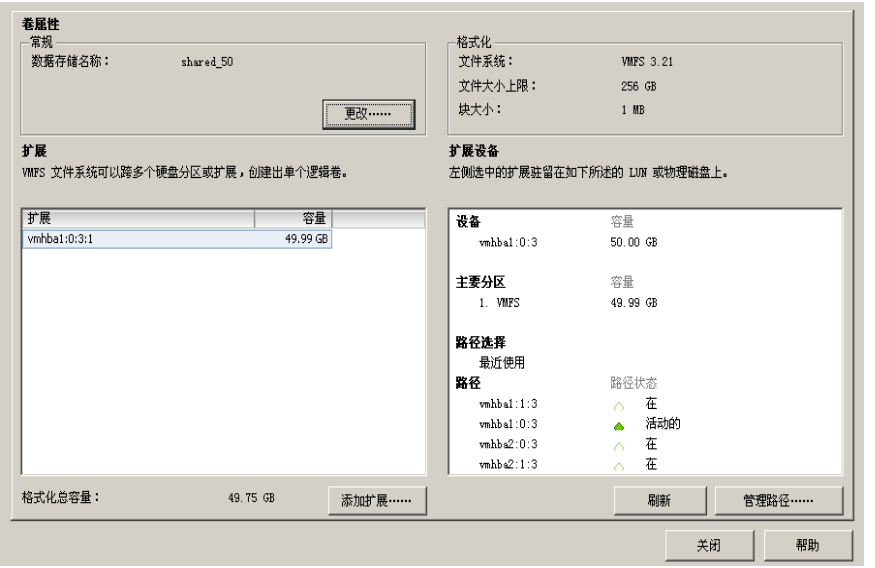
2 依次单击 **[配置 (Configuration)]** 选项卡和 [硬件 (Hardware)] 面板下方的 **[存储器 (Storage)]**。

3 从已配置数据存储列表中，选择要查看或配置其路径的数据存储。

[详细信息 (Details)] 面板显示用来访问数据存储的路径总数，以及是否有任何路径断开或禁用。

4 单击 **[属性 (Properties)]**。

此时会打开选定数据存储的 [卷属性 (Volume Properties)] 对话框。

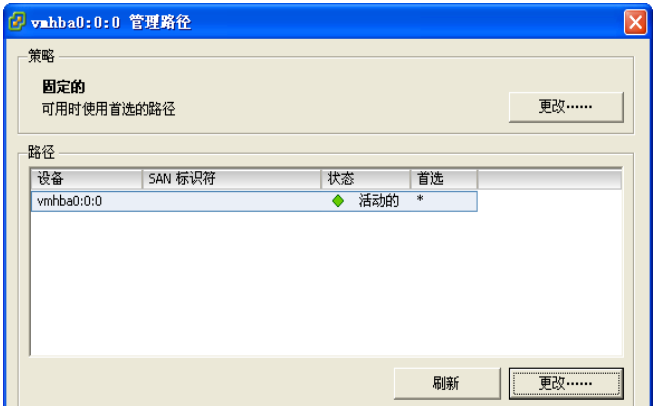


[扩展设备 (Extent Device)] 面板包括的信息涵盖 ESX Server 3 主机用来访问数据存储的多路径策略和每条路径的状态。其中会出现下面的路径信息：

- **[活动 (Active)]** - 路径处于工作状态并且是用来传输数据的当前路径。
- **[已禁用 (Disabled)]** - 路径已禁用，无法传输数据。
- **[待机 (Standby)]** - 路径处于工作状态，但当前并未用来传输数据。
- **[中断 (Broken)]** - 软件无法通过此路径连接到磁盘。

5 单击 **[管理路径 (Manage Paths)]** 打开 [管理路径 (Manage Paths)] 对话框。

如果是使用 **[固定的 (Fixed)]** 路径策略，可以首选路径。首选路径的第四列标有一个星号 (*)。

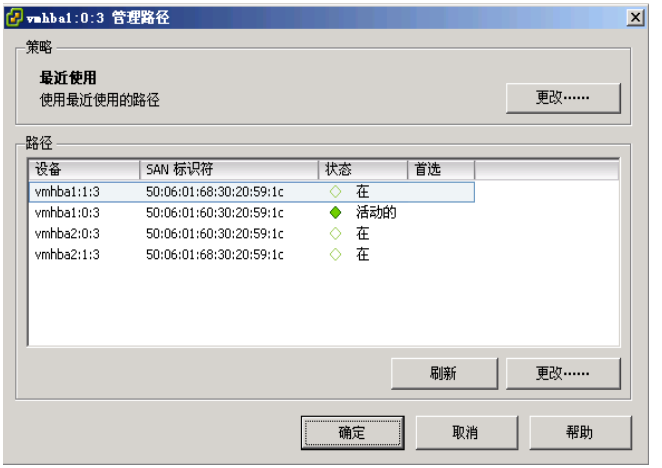


可以使用 [管理路径 (Manage Paths)] 对话框来启用或禁用路径、设置多路径策略，以及指定首选路径。

设置 LUN 的多路径策略

可以使用 [管理路径 (Manage Paths)] 对话框来设置多路径策略，并为 [固定的 (Fixed)] 策略指定首选路径。如果是管理 RDM 的路径，请参见 “管理路径”（第 144 页）。

[管理路径 (Manage Paths)] 对话框会显示通往磁盘的不同路径列表，以及磁盘的多路径策略和每条路径的连接状态。同时还会显示通往磁盘的首选路径。



设置多路径策略

1 在 [策略 (Policy)] 面板中，单击 **[更改 (Change)]**。

2 选择下列选项之一：

- **[固定的 (Fixed)]**
- **[最近使用 (Most Recently Used)]**
- **[循环 （试验性功能） (Round Robin (Experimental))]**

3 单击 **[确定 (OK)]**，然后单击 **[关闭 (Close)]**，以保存设置并返回到 [配置 (Configuration)] 页面。

注意 对于主动 / 被动存储设备，VMware 建议使用 **[最近使用 (Most Recently Used)]**。

如果将路径策略设置为 **[固定的 (Fixed)]**，请指定主机在路径可用时应使用的首选路径。

设置首选路径

1 在 [路径 (Paths)] 面板中，选择要成为首选路径的路径，然后单击 **[更改 (Change)]**。

2 在 [首选项 (Preference)] 窗格中，单击 **[首选 (Preferred)]**。

如果没有显示 **[首选 (Preferred)]** 选项，请确保 **[路径策略 (Path Policy)]** 是 **[固定的 (Fixed)]**。

3 单击 **[确定 (OK)]** 两次，以保存设置并退出对话框。

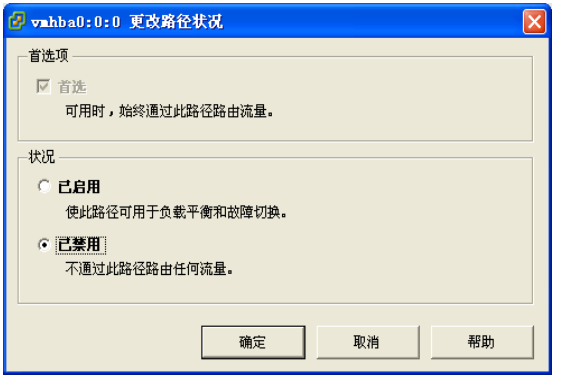
禁用路径

若因维护或其他原因而需要临时禁用路径，请使用 VI Client。

禁用路径

1 在 [路径 (Paths)] 面板中，选择要禁用的路径，然后单击 **[更改 (Change)]**。

2 选择 **[已禁用 (Disabled)]** 以禁用路径。



3 单击 **[确定 (OK)]** 两次，以保存设置并退出对话框。

vmkfstools 命令

除了使用 VI Client 之外，还可以使用 `vmkfstools` 程序来管理物理存储设备，以及在 ESX Server 3 主机上创建和操作 VMFS 数据存储和卷。

有关支持的 `vmkfstools` 命令列表，请参见 “使用 vmkfstools”（第 253 页）。

8 裸设备映射

裸设备映射 (RDM) 为虚拟机提供了一种机制，来直接访问物理存储子系统 （仅限光纤通道或 iSCSI）上的 LUN。本章包含有关 RDM 的信息。

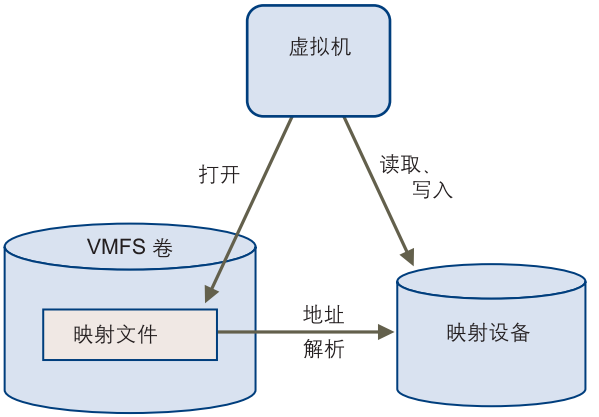
本章将讨论以下主题：

关于裸设备映射

RDM 是独立 VMFS 卷中的映射文件，它可充当裸物理设备的代理，即直接由虚拟机使用的 SCSI 设备。 RDM 包含用于管理和重定向对物理设备进行磁盘访问的元数据。该文件具有直接访问物理设备的一些优点，同时保留了 VMFS 文件系统中虚拟磁盘的一些优点。因此，它完美结合了 VMFS 易管理性与裸设备访问。

可用诸如 “将裸设备映射至数据库”、“映射系统 LUN”或 “将磁盘文件映射至物理磁盘卷”之类的术语描述 RDM。所有这些术语均指 RDM。

图 8-1 裸设备映射



尽管对于大多数虚拟磁盘存储器，我们推荐使用 VMFS 数据存储，但在特定情况下，您可能需要使用原始 LUN，或者位于 SAN 中的逻辑磁盘。

例如，在以下情况下，需要随同 RDM 一起使用原始 LUN：

- 当在虚拟机中运行 SAN 快照或其他分层应用程序时。 RDM 能够更好地启用使用 SAN 内在功能的可扩展备份卸载系统。
- 在任何跨物理主机的 MSCS 群集情况下 - 虚拟到虚拟群集以及物理到虚拟群集。在此情况下，群集数据和仲裁磁盘应配置为 RDM 而非共享 VMFS 上的文件。

将 RDM 视为从 VMFS 卷到原始 LUN 的符号链接（请参见图 8-1）。映射使 LUN 显示为 VMFS 卷中的文件。在虚拟机配置中引用 RDM 而非原始 LUN。 RDM 包含对原始 LUN 的引用。

使用 RDM，可以：

- VMotion 迁移使用原始 LUN 的虚拟机。
- 将原始 LUN 添加到使用 VI Client 的虚拟机。
- 使用分布式文件锁定、权限和命名等文件系统功能。

RDM 有两种可用兼容模式：

- 虚拟兼容模式能够使 RDM 的功能与虚拟磁盘文件完全相同，包括使用快照。
- 物理兼容模式允许直接访问 SCSI 设备，适用于需要较低级别控制的应用程序。

裸设备映射的优点

RDM 具有许多优点，但并非在每种情况下都能使用。通常，对于易管理性而言，虚拟磁盘文件优于 RDM。但是，当需要裸设备时，必须使用 RDM。下表突出说明了 RDM 的优点：

- **用户友好的持久名称** - 为映射设备提供了用户友好的名称。使用 RDM 时，不必通过设备名称引用设备。可以根据映射文件的名称来引用设备，例如：

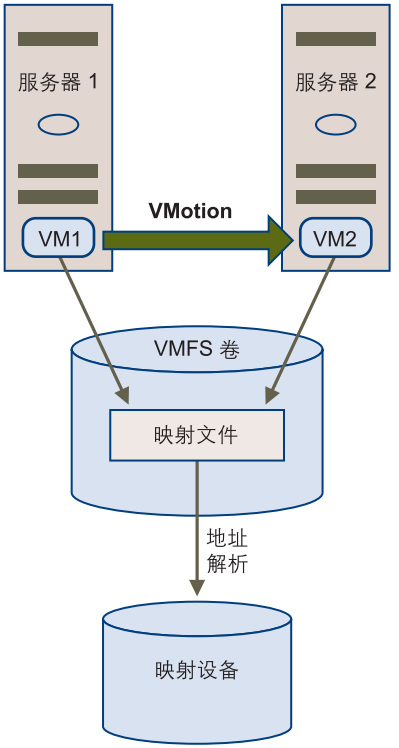
  ```
  /vmfs/volumes/myVolume/myVMDirectory/myRawDisk.vmdk
  ```

- **动态名称解析** - 存储每一映射设备唯一的标识信息。 VMFS 文件系统将每一 RDM 与其当前 SCSI 设备相关联，而不考虑由于适配器硬件更改、路径更改、设备重定位等所引起的服务器物理配置的变化。
- **分布式文件锁定** - 使得有可能使用针对 SCSI 裸设备的 VMFS 分布式锁定。当两台不同服务器上的虚拟机试图访问同一 LUN 时， RDM 上的分布式锁定使其能够安全使用共享原始 LUN 而不会丢失数据。
- **文件权限** - 可以使用文件权限。在文件打开时，强制执行映射文件权限，以保护映射的卷。
- **文件系统操作** - 令使用文件系统实用程序来使用映射的卷，将映射文件用作代理成为可能。对普通文件有效的大部分操作都可应用于映射文件，并且可进行重定向，以便于在映射设备上进行操作。
- **快照** - 可以在映射的卷上使用虚拟机快照。

  注意 当在物理兼容模式下使用 RDM 时，快照不可用。

- **VMotion** - 使您可使用 VMotion 迁移虚拟机。映射文件可充当代理，允许 VirtualCenter 使用与迁移虚拟磁盘文件相同的机制迁移虚拟机。请参见图 8-2。

图 8-2 使用裸设备映射的虚拟机的 VMotion



- **SAN 管理代理** - 可以在虚拟机内运行某些 SAN 管理代理。与此相似，可以在虚拟机内运行需要使用硬件特定 SCSI 命令访问设备的任何软件。这种软件称为基于 SCSI 目标的软件。

  注意 使用 SAN 管理代理时，需要为 RDM 选择物理兼容模式。

- **N-Port ID 虚拟化 (NPIV)** - 可以使用 NPIV 技术，通过该技术，单一光纤通道 HBA 端口可使用多个全球端口名称 (WWPN) 向光纤通道架构注册。通过此功能，HBA 端口就可显示为多个虚拟端口，每个端口均有其自身的 ID 和虚拟端口名称。这样，虚拟机就可声明其中每个虚拟端口，并将其用于所有 RDM 流量。

  注意 NPIV 仅可用于具备 RDM 磁盘的虚拟机。

  请参见 *《光纤通道 SAN 配置指南》*。

VMware 与存储管理软件的供应商合作，确保他们的软件能够在包括 ESX Server 3 的环境下正常工作。此类应用程序包括：

- SAN 管理软件
- 存储资源管理 (SRM) 软件
- 快照软件
- 复制软件

此类软件将物理兼容模式用于 RDM，以便直接访问 SCSI 设备。

各种管理产品都可以以出色的性能集中运行 （不是在 ESX Server 3 计算机上），其他产品则可以在服务控制台或虚拟机中良好运行。 VMware 不正式认可这些应用程序或者提供兼容性矩阵。要了解在 ESX Server 3 环境中是否支持某 SAN 管理应用程序，请与 SAN 管理软件提供商联系。

裸设备映射的局限性

当计划使用 RDM 时，请考虑以下事项：

- **不可用于块设备或某些 RAID 设备** - RDM （在当前实施中）使用 SCSI 序列号识别映射设备。由于块设备和某些直连 RAID 设备不能导出序列号，它们不能与 RDM 一起使用。
- **仅可用于 VMFS-2 和 VMFS-3 卷** - RDM 需要 VMFS-2 或 VMFS-3 格式。在 ESX Server 3 中， VMFS-2 文件系统为只读。要使用 VMFS-2 所存储的文件，将其升级为 VMFS-3。
- **物理兼容模式下无快照** - 如果在物理兼容模式下使用 RDM，则不能使用磁盘快照。物理兼容模式允许虚拟机管理自己的快照或镜像操作。

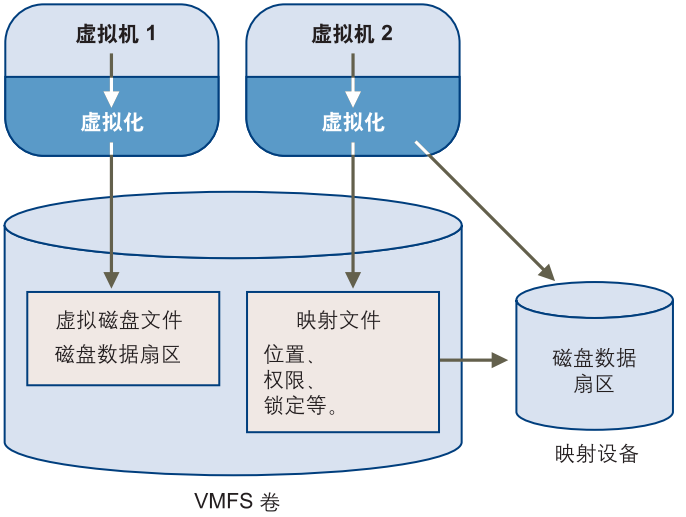
  但是，在虚拟模式下，可以使用快照。请参见 “虚拟兼容模式与物理兼容模式比较”（第 138 页）。
- **无分区映射** - RDM 需要映射设备是完整的 LUN。不支持映射到分区。

裸设备映射特点

RDM 是 VMFS 卷中管理映射设备元数据的一种特殊映射文件。管理软件将映射文件视作普通磁盘文件，适用于常规文件系统操作。对于虚拟机，存储虚拟层将映射设备视作虚拟 SCSI 设备。

映射文件中元数据的主要内容包括映射设备的位置 （名称解析）和映射设备的锁定状况。

图 8-3 映射文件元数据

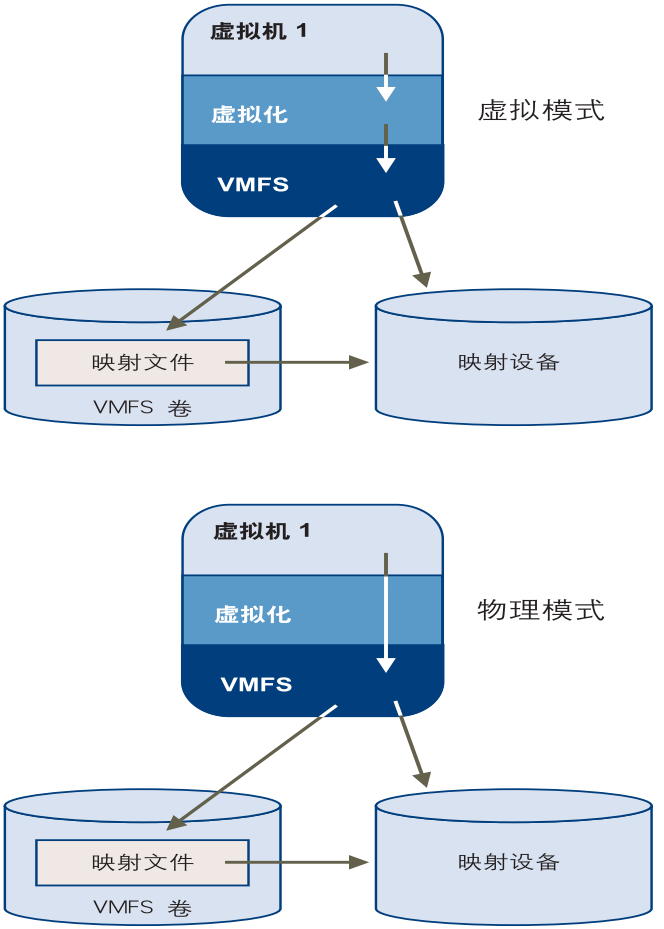


虚拟兼容模式与物理兼容模式比较

RDM 的虚拟模式指定了映射设备的完整虚拟化。客户机操作系统似乎与 VMFS 卷中的虚拟磁盘文件完全相同。真实硬件属性隐藏。虚拟模式使使用裸磁盘的客户能够认识到 VMFS 的优点，例如用于数据保护的高级文件锁定和简化开发流程的快照等。虚拟模式还比物理模式在存储硬件上更具移植性，具有与虚拟磁盘文件相同的属性。

RDM 的物理模式指定了映射设备的最小 SCSI 虚拟化，实现了 SAN 管理软件的最大灵活性。在物理模式下，Vmkernel 将所有 SCSI 命令传递至设备。例外：REPORT LUNs 命令被虚拟化，从而 VMkernel 可以将虚拟机与 LUN 隔离。否则，基础硬件的所有物理特性都将公开。物理模式对于在虚拟机中运行 SAN 管理代理或其他基于 SCSI 目标的软件非常有用。物理模式还允许虚拟到物理群集，实现具有成本效益的高可用性。

图 8-4 虚拟兼容模式和物理兼容模式

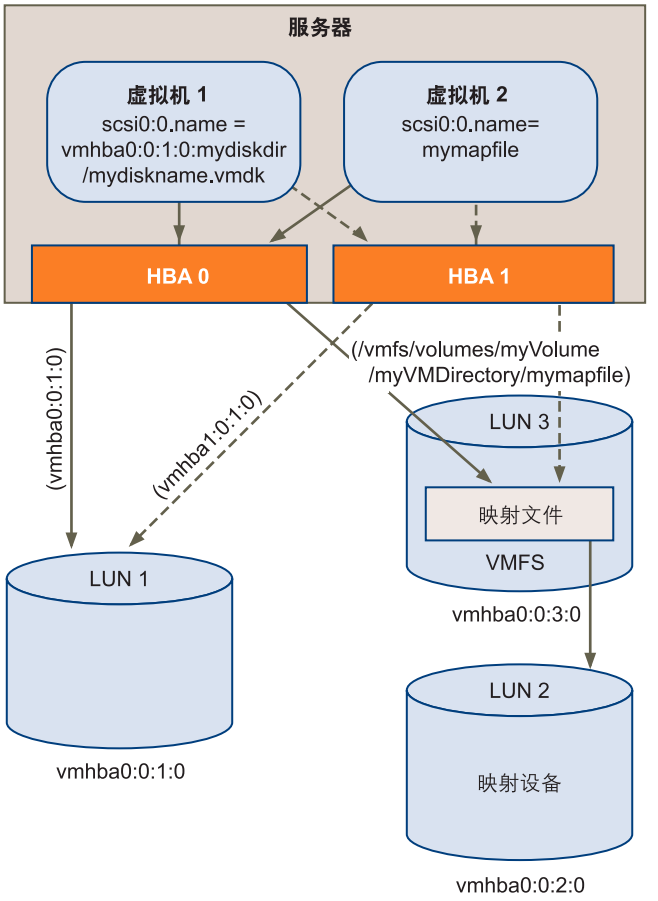


动态名称解析

RDM 通过引用 `/vmfs` 子树中映射文件的名称，使您能够为设备提供永久名称。

图 8-5 中的示例表示三个 LUN。LUN 1 根据其设备名称进行访问，与第一个可见 LUN 相关。LUN 2 是映射设备，由 LUN 3 上的 RDM 进行管理。RDM 根据 `/vmfs` 子树中的名称进行访问，该名称固定不变。

图 8-5 名称解析示例

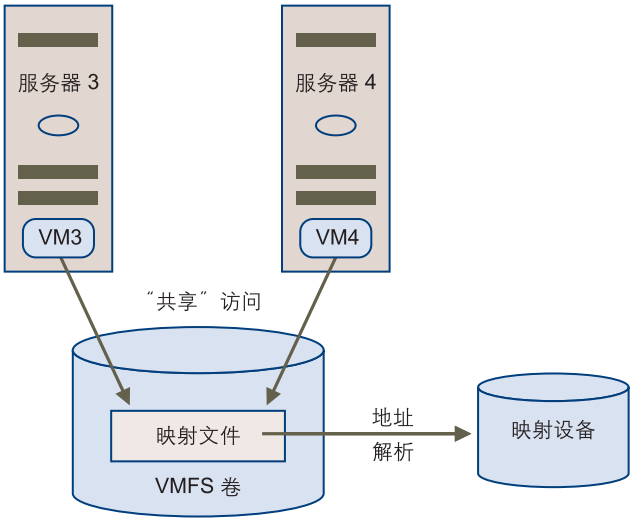


所有映射的 LUN 都由 VMFS 唯一识别，标识存储在其内部数据结构中。SCSI 路径的任何更改，例如光纤通道交换机故障或添加新的主机总线适配器，都可能更改 vmhba 设备名称，因为该名称包括路径标识 （启动器、目标、 LUN）。动态名称解析可通过调整数据结构，使 LUN 与新的设备名称重新对应，从而弥补这些更改。

虚拟机群集的裸设备映射

对于故障切换情况，应与需要访问同一原始 LUN 的虚拟机群集一起使用 RDM。设置与访问同一虚拟磁盘文件的虚拟机群集的设置相同，但 RDM 替换虚拟磁盘文件。

图 8-6 从群集式虚拟机进行访问



请参见 *《资源管理指南》*。

裸设备映射与其他 SCSI 设备访问方法的比较

为了帮助您在 SCSI 设备的多个可用访问模式之间进行选择，表 8-1 提供了对不同模式可用功能的快速比较。

表 8-1 虚拟磁盘和裸设备映射的可用功能

ESX Server 3 功能	虚拟磁盘文件	虚拟模式 RDM	物理模式 RDM
SCSI 命令已传递	否	否	是 不传递 REPORT LUN
VirtualCenter 支持	是	是	是
快照	是	是	否
分步式锁定	是	是	是
群集	仅限机箱内群集	机箱内群集和机箱间群集	N+1 （仅限物理到虚拟群集）
基于 SCSI 目标的软件	否	否	是

VMware 建议将虚拟磁盘文件用于机箱内群集。如果要将机箱内群集重新配置为机箱间群集，则可将虚拟模式 RDM 用于机箱内群集。请参见 *《资源管理指南》*。

管理映射的 LUN

可用于管理映射的 LUN 及其 RDM 的工具，包括 VI Client、 `vmkfstools` 实用程序以及在服务控制台中所使用的普通文件系统实用程序。

VMware Infrastructure Client

使用 VI Client，可以将 SAN LUN 映射到数据存储和管理指向映射的 LUN 的路径。

用 RDM 创建虚拟机

当您授予您的虚拟机对原始 SAN LUN 的直接访问权限时，可创建驻留在 VMFS 数据存储并指向 LUN 的映射文件。尽管映射文件与常规虚拟磁盘文件的扩展名均为 `.vmdk`，但 RDM 文件仅包括映射信息。实际虚拟磁盘数据直接存储在 LUN 上。

您可创建 RDM 作为新虚拟机的初始磁盘或将其添加至现有虚拟机中。创建 RDM 时，您可指定要映射的 LUN 及要存储 RDM 的数据存储。

用 RDM 创建虚拟机

1 遵循创建自定义虚拟机所需的所有步骤。

请参见 *《基本系统管理》*。

2 在 [选择磁盘 (Select a Disk)] 页面中，选择 **[裸设备映射 (Raw Device Mapping)]**，然后单击 **[下一步 (Next)]**。

3 从 SAN 磁盘或 LUN 列表中，选择您的虚拟机可直接访问的原始 LUN。

有关配置 SAN 存储器的更多信息，请参见 *《光纤通道 SAN 配置指南》* 和 *《iSCSI SAN 配置指南》*。

4 为 RDM 映射文件选择数据存储。

可以将 RDM 文件置于虚拟机配置文件驻留的同一数据存储上，或者选择不同的数据存储。

注意 要将 VMotion 用于启用了 NPIV 的虚拟机，请确保该虚拟机的 RDM 文件位于同一数据存储上。启用 NPIV 后，不可在数据存储之间执行 Storage VMotion 或 VMotion。

---

5 选择兼容模式：

- **[物理兼容 (Physical compatibility)]** 模式允许客户操作系统直接访问硬件。如果正在虚拟机中使用 SAN 感知应用程序，则物理兼容模式非常有用。但是，带有物理兼容 RDM 的虚拟机不能克隆，不能制作成模板，或者不能迁移（如果迁移涉及复制磁盘）。
- **[虚拟兼容 (Virtual compatibility)]** 模式允许 RDM 像虚拟磁盘一样工作，因此您可使用诸如快照和克隆之类的功能。

6 选择虚拟设备节点。

7 如果选择 **[独立 (Independent)]** 模式，则选择下列一项：

- **[持久 (Persistent)]** - 更改会立即永久性地写入磁盘。
- **[非持久 (Nonpersistent)]** - 当关闭电源或恢复快照时，对该磁盘的更改会被放弃。

8 单击 **[下一步 (Next)]**。

9 在 [即将完成新建虚拟机 (Ready to Complete New Virtual Machine)] 页面上，检查您所做的选择。

10 单击 **[完成 (Finish)]** 完成虚拟机。

也可将 RDM 添加至现有虚拟机。

将 RDM 添加至虚拟机

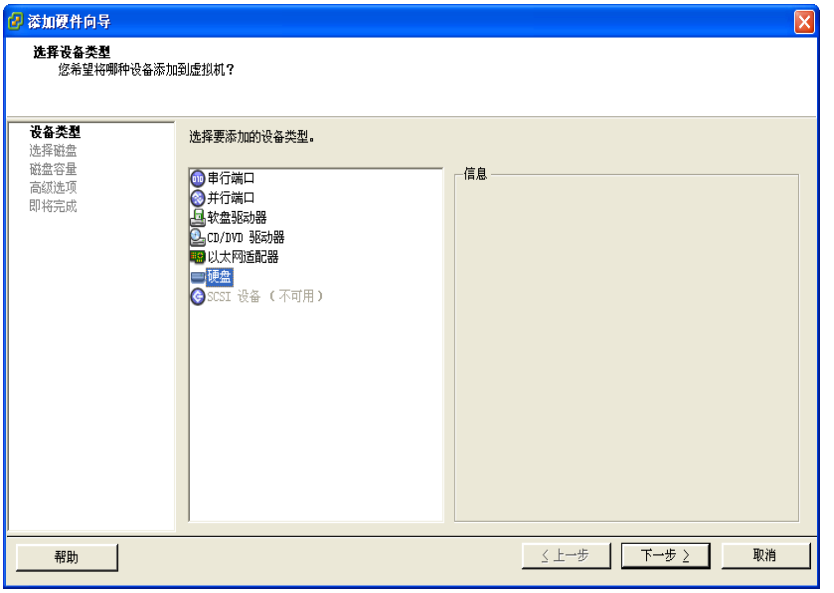
1 从 VI Client 中，单击导航栏中的 **[清单 (Inventory)]**，并在必要时展开清单。

2 从目录面板中选择虚拟机。

3 在 **[摘要 (Summary)]** 选项卡中，单击 **[编辑设置 (Edit Settings)]**。

4 单击 **[添加 (Add)]**。

此时会打开添加硬件向导。



5 选择 **[硬盘 (Hard Disk)]** 作为要添加的设备类型，然后单击 **[下一步 (Next)]**。

6 选择 **[裸设备映射 (Raw Device Mapping)]**，然后单击 **[下一步 (Next)]**。

7 转至前一过程中的步骤 3。

管理映射原始 LUN 的路径

可以使用 [管理路径 (Manage Paths)] 对话框管理映射文件和映射原始 LUN 的路径。

管理路径

1 以管理员或映射磁盘所属于的虚拟机的所有者身份登录。

2 从目录面板中选择虚拟机。

3 在 **[摘要 (Summary)]** 选项卡上，单击 **[编辑设置 (Edit Settings)]** 链接。

此时将打开 [虚拟机属性 (Virtual Machine Properties)] 对话框。

4 在 **[硬件 (Hardware)]** 选项卡上，选择 **[硬盘 (Hard Disk)]**，然后单击 **[管理路径 (Manage Paths)]**。

5 使用 [管理路径 (Manage Paths)] 对话框启用或禁用路径、设置多路径策略和指定优先路径。

请按照以下过程操作：

- "设置多路径策略"（第 131 页）
- "设置首选路径"（第 132 页）
- "禁用路径"（第 132 页）

vmkfstools 实用程序

可以在服务控制台中使用 `vmkfstools` 命令行实用程序执行许多可通过 VI Client 使用的相同操作。适用于 RDM 的典型操作是创建映射文件、查询映射信息 （例如映射设备的名称和标识）以及导入或导出虚拟磁盘的命令。

请参见 "使用 vmkfstools"（第 253 页）。

文件系统操作

在服务控制台中完成的大部分常用文件系统操作都可适用于 RDM。

表 8-2 用于服务控制台的命令

命令	描述
`ls -l`	在显示映射设备长度的同时，显示映射文件的文件名和权限。
`du`	显示映射设备而非映射文件所占用的空间。
`mv`	重命名映射文件，但不会影响映射设备。
`cp`	复制映射设备的内容。不能使用该命令将虚拟磁盘文件复制到映射设备。而只能使用 `vmkfstools` 命令。
`dd`	从映射设备或向映射设备复制数据。但是， VMware 建议使用 `vmkfstools` 导入和导出命令来复制数据。

安全

9 ESX Server 3 系统的安全性

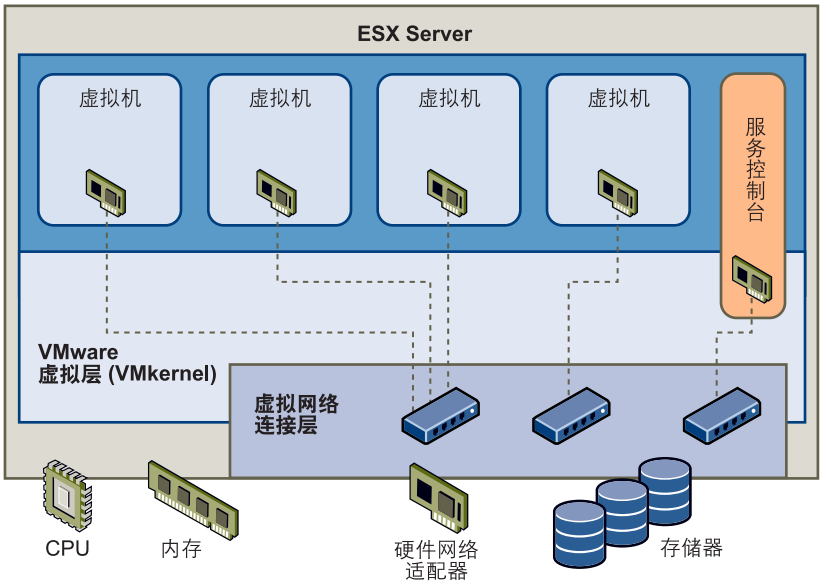
ESX Server 的开发注重于加强安全性。本节概述了 VMware 如何确保 ESX Server 环境中的安全性，从安全角度阐述了系统架构并提供了附加安全资源的列表。

本章包括以下各节：

ESX Server 3 架构和安全功能

从安全角度而言，VMware ESX Server 3 主要由四个组件组成：虚拟层、虚拟机、服务控制台和虚拟网络层。图 9-1 对这些组件进行了概述。

图 9-1 ESX Server 3 架构



每个组件及此全面架构旨在确保 ESX Server 3 系统的整体安全性。

安全性和虚拟层

虚拟层 （或 Vmkernel）是 VMware 设计用来运行虚拟机的内核。它对 ESX Server 主机所使用的硬件进行控制，并调度虚拟机之间的硬件资源分配。由于 VMkernel 专用于支持虚拟机且不用于其他用途，因此其接口严格限定为管理虚拟机所需的 API。

安全性与虚拟机

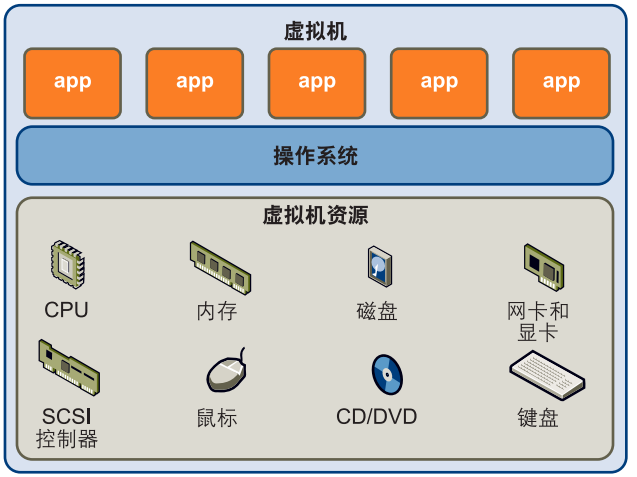
虚拟机是运行应用程序和客户操作系统的容器。所有的 VMware 虚拟机均互相隔离。虚拟机的设计使其包含客户操作系统内的所有用户，无论用户具备什么特权。即使是管理员，也将从其他虚拟机隔离，就像从其他物理机隔离一样。

通过此隔离，多台虚拟机就可在共享硬件的同时安全地运行，既确保能够访问硬件，又保证运行不受干扰。例如，如果虚拟机中运行的一台客户操作系统崩溃，同一 ESX Server 主机上的其他虚拟机还是继续运行。客户机操作系统崩溃不影响：

- 用户访问其他虚拟机的能力
- 操作虚拟机访问其所需资源的能力
- 其他虚拟机的性能

同一硬件上运行的虚拟机互相隔离。当虚拟机共享诸如 CPU、内存及 I/O 设备之类的物理资源时，单一虚拟机上的客户操作系统可检测到的设备仅限于可供其使用的虚拟设备，如图 9-2 中所示。

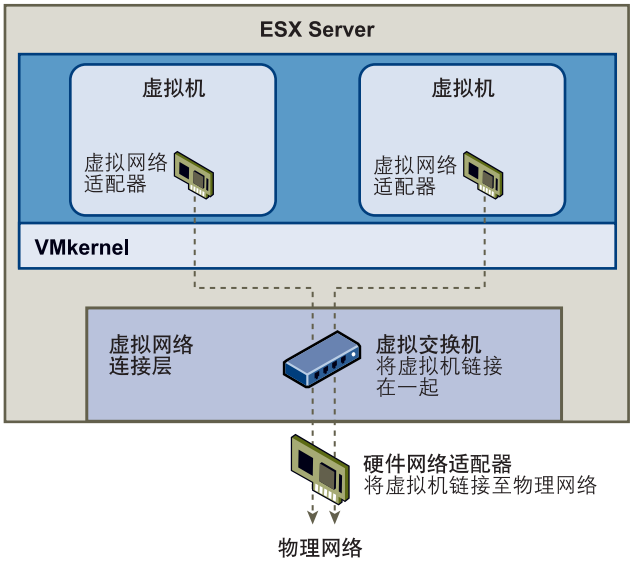
图 9-2 虚拟机隔离



由于 VMkernel 可调节物理资源及通过其对物理硬件进行的所有访问，因此虚拟机无法阻止此层隔离。

如同物理机仅通过网卡就可与网络中其他计算机进行通信一样，虚拟机也仅通过虚拟交换机与同一台 ESX Server 主机上运行的其他虚拟机进行通信。而且，虚拟机可仅通过物理网络适配器与物理网络 （包括其他 ESX Server 主机上的虚拟机）进行通信，如图 9-3 中所示。

图 9-3 通过虚拟交换机进行虚拟网络连接



鉴于虚拟机在网络中互相隔离这一情况，可以应用这些规则：

- 如果某台虚拟机未与任何其他虚拟机共享虚拟交换机，则其与主机中的虚拟网络完全隔离。
- 如果未为某台虚拟机配置物理网络适配器，则该虚拟机与任何物理网络完全隔离。
- 如果使用了与保护物理机相同的保护措施 （防火墙和防毒软件等）来保护网络中的虚拟机，该虚拟机则像物理机一样安全。

在 ESX Server 主机上设置资源预留量和限制量，可进一步保护虚拟机。例如，通过 ESX Server 中可用的详细资源控制，可对虚拟机进行配置，使其获得的 ESX Server 主机 CPU 资源始终不少于 10%，但也决不超过 20%。

资源预留量和限制量可保护虚拟机的性能不会因其他虚拟机尝试消耗共享硬件上的太多资源而降低。例如，如果 ESX Server 主机上的一台虚拟机由于受到拒绝服务 (DoS) 或分布式拒绝服务 (DDoS) 攻击而出现故障，该虚拟机上的资源限制量就会阻止该攻击占据太多硬件资源，否则其他虚拟机也会受到影响。与此相似，每台虚拟机上的资源预留量可在受到 DoS 攻击的虚拟机需要较多资源的情况下确保所有其他虚拟机仍有足够的资源可供使用。

默认情况下， ESX Server 通过应用分布式算法而强制实行一种形式的资源预留量，该分布算法可将可用主机资源均匀分布于虚拟机之中，同时保留一定百分比的资源供诸如服务控制台之类的其他系统组件使用。此默认行为在一定程度上为防止 DoS 和 DDoS

攻击提供了自然保护。要定制默认行为，以避免在虚拟机配置之间均匀分布资源预留量和限制量，可逐一指定资源预留量和限制量。有关如何管理虚拟机资源分配的讨论，请参见 *《资源管理指南》*。

安全性和服务控制台

ESX Server 3 服务控制台是基于 Red Hat Enterprise Linux 3 Update 8 (RHEL 3 U8) 的 Linux 的有限分发版本。服务控制台为监控和管理整个 ESX Server 3 主机提供了执行环境。

如果服务控制台因某种原因上受到损害，与其进行交互的虚拟机也可能受到损害。为了使通过服务控制台进行攻击的风险最小化， VMware 使用了防火墙对服务控制台进行保护。有关此防火墙的信息，请参见 “服务控制台防火墙配置”（第 211 页）。

除了实施服务控制台防火墙， VMware 还采用了以下几种其他方式来缓解服务控制台可能承担的风险。

- ESX Server 3 仅运行管理其功能所不可或缺的服务，分布仅限定于运行 ESX Server 3 所需的功能。
- 默认情况下， ESX Server 3 是用高安全性设置进行安装的，这意味着所有出站端口均已关闭，而仅打开与诸如 VMware Virtual Infrastructure Client 之类的客户端进行交互所需的入站端口。 VMware 建议保留此安全设置，除非服务控制台是连接至可信网络。
- 默认情况下，非专用于服务控制台访问管理的所有端口均已关闭。如果需要其他服务，则必须另外打开特定端口。
- 来自客户端的所有通信在默认情况下均通过 SSL 进行加密。 SSL 连接使用 256 位 AES 分块加密和 1024 位 RSA 密钥加密。
- ESX Server 3 在内部使用 Tomcat Web 服务来支持诸如 Virtual Infrastructure Web Access 之类的 Web 客户端对服务控制台进行的访问。经过修改， Tomcat Web 服务仅运行 Web 客户端进行管理和监控所需的功能。因此， ESX Server 3 不易遇到在广泛使用中所发现的 Tomcat 安全问题。
- VMware 监控可能影响服务控制台安全性的所有安全警示，并在必要时提供安全修补程序，就如同为可能影响 ESX Server 3 主机的任何其他安全漏洞提供该安全修补程序一样。 VMware 为 RHEL 3 U6 提供了安全修补程序，并可在以后尽量提供该修补程序。
- 未安装诸如 FTP 和 Telnet 之类的不安全服务，且这些服务所要使用的端口在默认情况下也是关闭的。由于易于获取诸如 SSH 和 SFTP 之类较为安全的服务，因此，请始终避免使用这些不安全的服务，以支持更为安全的替代方案。如果必须使用不

安全的服务，且已为服务控制台实施了充分的保护措施，则必须明确为其打开相应端口。

- 使用 `setuid` 或 `setgid` 标记的应用程序的数量已最小化，可以禁用 ESX Server 3 操作不一定需要的 `setuid` 或 `setgid` 应用程序。有关必要的和可选的 `setuid` 和 `setgid` 应用程序的信息，请参见 “setuid 和 setgid 应用程序”（第 221 页）。

有关这些安全措施及其他服务控制台安全建议的详细信息，请参见 “服务控制台安全”（第 209 页）。

尽管可以在服务控制台上安装和运行专用于 RHEL 3 U6 的某些类型的程序，但这种使用可能带来非常严重的后果且不受支持，除非 VMware 另有明确说明。如果在受支持的配置中发现安全漏洞， VMware 会主动通知已签署有效的支持和订购合同的所有客户，并提供所有必要的修补程序。

注意 Red Hat 提出的某些安全建议并不适用于 ESX Server 3 环境。在这些情况下，VMware 不会发出通知或提供修补程序。

要进一步了解 VMware 有关受支持程序的安全修补程序及不受支持的软件的策略，请参见 “安全资源和信息”（第 159 页）。

安全性和虚拟网络连接层

虚拟网络层由虚拟网络设备组成，通过这些设备，虚拟机和服务控制台可与其他网络连接。 ESX Server 依赖于虚拟网络层来支持虚拟机与其用户之间的通信。此外， ESX Server 主机可使用虚拟网络层与 iSCSI SAN 和 NAS 存储器等进行通信。虚拟网络连接层包括虚拟网络适配器和虚拟交换机。

可确保虚拟机网络安全的方法取决于所安装的客户操作系统、虚拟机是否运行于可信环境及各种其他因素。通常与其他常见安全措施相结合 （例如，安装防火墙），虚拟交换机的保护作用大大加强。 ESX Server 也支持可用于为虚拟机网络、服务控制台或存储器配置提供进一步保护的 IEEE 802.1q VLAN。可通过 VLAN 对物理网络进行分段，以便使同一物理网络中的两台计算机无法互相发送或接收数据包，除非它们位于同一 VLAN 上。

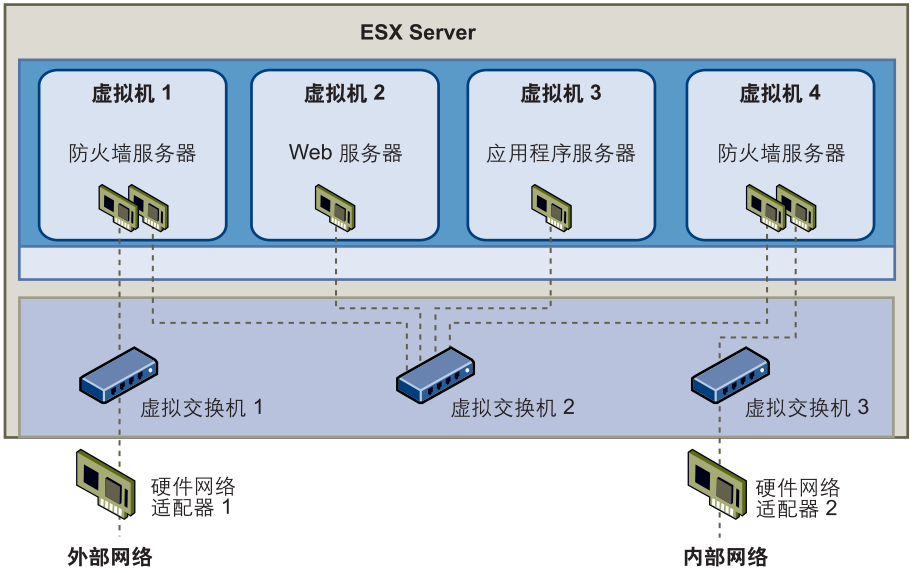
可参考以下示例，以了解如何使用虚拟交换机实施诸如 DMZ 之类的安全工具并在同台 ESX Server 主机内的不同网络上配置虚拟机。

注意 有关虚拟交换机和 VLAN 如何有助于保护虚拟机网络的特定讨论及针对虚拟机网络提出的其他安全建议的讨论，请参见 “通过 VLAN 确保虚拟机安全”（第 176 页）。

示例：在单台 ESX Server 主机上创建网络 DMZ

使用 ESX Server 隔离和虚拟网路功能配置安装环境的一个示例是：在单台 ESX Server 主机上创建无戒备区网络 (DMZ)，如 图 9-4 所示

图 9-4 在单台 ESX Server 主机上配置的 DMZ



此配置包括将四个虚拟机配置为在虚拟交换机 2 上创建虚拟 DMZ。虚拟机 1 和虚拟机 4 运行防火墙，并通过虚拟交换机连接到虚拟适配器上。这两个虚拟机都是多址的。在剩余的两个虚拟机当中，虚拟机 2 运行 Web 服务器，虚拟机 3 作为应用程序服务器运行。这两个虚拟机都是单址的。

Web 服务器和应用程序服务器占用两个防火墙之间的 DMZ。这两个元素之间的媒介为连接防火墙与服务器的虚拟交换机 2。此交换机未与 DMZ 之外的任何元素进行直接连接，并通过两个防火墙与外部流量相隔离。

从运行角度来看，外部流量通过硬件网络适配器 1 （由虚拟交换机 1 路由）从 Internet 进入虚拟机 1，并由此虚拟机上安装的防火墙进行验证。如经防火墙授权，流量可路由至 DMZ 中的虚拟交换机，即虚拟交换机 2。由于 Web 服务器和应用程序服务器也连接至此交换机，因此，它们可以满足外部请求。

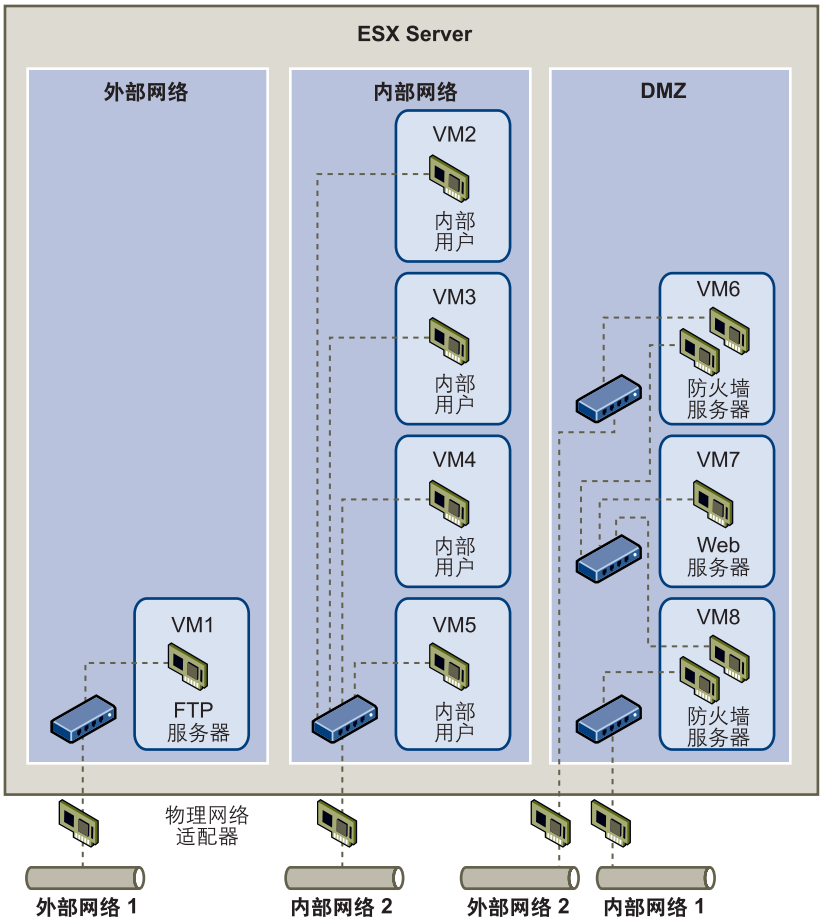
虚拟交换机 2 也连接至虚拟交换机 4。此虚拟机在 DMZ 和内部企业网络之间提供了防火墙。此防火墙对 Web 服务器和应用程序服务器的数据包进行筛选。验证后的数据包将通过虚拟交换机 3 路由至硬件网络适配器 2。硬件网络适配器 2 连接至内部企业网络。

在单台 ESX Server 上创建 DMZ 时，可使用轻量防火墙。虽然此配置中的虚拟机无法直接控制另一台虚拟机或访问其内存，但所有虚拟机仍通过虚拟网络连接，而此网络可能成为病毒传播的介质或成为其他类型攻击的目标。 DMZ 中虚拟机的安全性类似于连接至同一网络中的独立物理机。

示例：在单台 ESX Server 主机中创建多个网络

ESX Server 系统的设计可让您将一些虚拟机组连接至内部网络，将一些虚拟机组连接至外部网络，再将另一些虚拟机组同时连接至外部网络和内部网络 - 这一切都在同一 ESX Server 主机上进行。此功能是由于对虚拟机的基本隔离及对虚拟网络功能的有计划使用而生成的，如图 9-5 中所示。

图 9-5 单台 ESX Server 主机内已配置的外部网络、内部网络和 DMZ



系统管理员在此处将 ESX Server 主机配置到三个不同的虚拟机区域，每个区域的功能各不相同：

- **FTP 服务器** - 虚拟机 1 是用 FTP 软件配置的，它可用作从外部资源（例如，由供应商本地化的表单和辅助材料）发出及向其发送的数据的存储区域。

  此虚拟机仅与外部网络相关联。它自身拥有可用来与外部网络 1 相连接的虚拟交换机和物理网络适配器。此网络专用于公司用来接收外部来源数据的服务器。例如，公司使用外部网络 1 从供应商接收 FTP 流量，并允许供应商通过 FTP 访问存储在外部可用服务器上的数据。除了服务于虚拟机 1，外部网络 1 也服务于在整个站点的不同 ESX Server 主机上配置的 FTP 服务器。

  由于虚拟机 1 不与主机中的任何虚拟机共享虚拟交换机或物理网络适配器，因此，其他驻留的虚拟机无法通过虚拟机 1 网络收发数据包。此限制可防止嗅探攻击（嗅探攻击需向受害者发送网络流量）。更为重要的是，攻击者再也无法使用 FTP 自然漏洞访问任何主机的其他虚拟机。

- **内部虚拟机** - 虚拟机 2 - 5 仅供内部使用。这些虚拟机处理和存储公司机密数据（例如，医疗记录、法律裁决和欺诈调查）因此，系统管理员必须确保这些虚拟机提供最高程度的保护。

  这些虚拟机通过其自身的虚拟交换机和网络适配器连接至内部网络 2。内部网络 2 仅供内部人员使用 （例如，索赔专员、内部律师或调解员）。

  虚拟机 2 - 5 可通过虚拟交换机与另一台虚拟机进行通信，或通过物理网络适配器与内部网络 2 上其他位置的内部虚拟机进行通信。它们不能与对外计算机进行通信。如同 FTP 服务器一样，这些虚拟机不能从其他的虚拟机网络接收 / 发送数据包。与此相似，主机的其他虚拟机不能从虚拟机 2 - 5 接收或向其发送数据包。

- **DMZ** - 虚拟机 6 - 8 被配置为可供营销小组用于发布公司外部网站的 DMZ。

  此虚拟机组与外部网络 2 和内部网络 1 相关联。公司使用外部网络 2 来支持营销部门和财务部门用来托管公司网站的 Web 服务器及公司向外部用户托管的其他 Web 设施。内部网络 1 是营销部门用于向公司网站发布网页、张贴下载及维护服务（例如，用户论坛）的媒介。

  由于这些网络与外部网络 1 和内部网络 2 相隔离，因此虚拟机无任何共享联络点（交换机或适配器）， FTP 服务器或内部虚拟机组也不存在任何攻击风险。

  有关如何使用虚拟机配置 DMZ 的示例，请参见 “示例：在单台 ESX Server 主机上创建网络 DMZ”（第 155 页）。

通过利用虚拟机隔离、正确配置虚拟交换机及维护网络独立，系统管理员可在同一 ESX Server 主机上容纳所有三个虚拟机区，并完全不用担心数据或资源流失。

公司使用了多个内部和外部网络，并确保每组的虚拟交换机和物理网络适配器与其他组的虚拟交换机和物理网络适配器完全独立，从而在虚拟机组中强制实施隔离。

由于没有任何虚拟交换机横跨虚拟机区，因此系统管理员可成功地消除虚拟机区之间的数据包泄漏风险。虚拟机本身无法向另一个虚拟交换机直接泄露数据包。仅在以下情况下，数据包才会在虚拟交换机之间移动：

- 虚拟交换机连接至同一物理 LAN。
- 虚拟交换机连接至可用于传输数据包的公用虚拟机。

这些条件均未出现在样本配置中。如果系统管理员想要确保不存在公用虚拟交换机路径，可查看 VI Client 或 VI Web Access 中的网络布局，以检查是否可能存在共享联络点。有关虚拟交换机布局的信息，请参见 “虚拟交换机”（第 21 页）。

为了保护虚拟机的资源，系统管理员为每个虚拟机配置了资源预留量和限制量，从而降低了 DoS 和 DDoS 攻击的风险。系统管理员在 DMZ 的前后端安装了软件防火墙，确保 ESX Server 主机受到物理防火墙的保护，并配置了服务控制台和联网的存储器资源以便使每个服务控制台均有其自身的虚拟交换机，从而为 ESX Server 主机和虚拟机提供了进一步保护。

安全资源和信息

通过下列资源，可找到有关安全性主题的其他信息。

表 9-1 Web 上的 VMware 安全资源

主题	资源
VMware 安全策略，最新安全预警、安全下载及安全主题重点讨论	www.vmware.com/security/communities.vmware.com/community/vmtn/general/security
公司安全响应策略	http://www.vmware.com/support/policies/security_response.html VMware 致力于帮助维护安全的环境。为保证能及时地解决所有安全问题，VMware 在 “VMware 安全响应策略” 中作出了致力于解决其产品中可能存在的漏洞之承诺。
第三方软件支持策略	http://www.vmware.com/support/policies VMware 支持各种存储系统、软件代理 （例如，备份代理）及系统管理代理等。在 http://www.vmware.com/vmtn/resources 上搜索《ESX Server 3 兼容性指南》，可找到支持 ESX Server 3 的代理、工具和其他软件的列表。 VMware 不可能对此行业中的所有产品和配置进行测试。如果 VMware 未在兼容性指南中列出某种产品或配置，其技术支持人员将试图帮助解决任何相关问题，但不能保证该产品或配置的可用性。请始终不要忘记对不受支持的产品或配置的任何风险进行评估。

确保 ESX Server 3 配置的安全性

10

本章介绍一些可用来为 ESX Server 3 主机、虚拟机和 iSCSI SAN 创造安全环境的措施。讨论重点围绕从安全角度而言的网络配置计划及可以用来保护配置中的组件免遭攻击的措施。

本章将讨论以下主题：

用防火墙确保网络安全

安全管理员使用防火墙保护网络或网络中的选定组件免遭侵袭。防火墙可控制对其保护范围内设备的访问，方法是关闭除管理员显式或隐式指定的授权路径之外的所有通信路径，从而防止对设备进行未授权使用。管理员在防火墙打开的路径或端口允许防火墙内外设备间的流量。

在虚拟机环境中，可在为以下两者间的防火墙规划布局：

- 物理机 （例如 VirtualCenter Management Server 主机）与 ESX Server 3 主机。
- 虚拟机之间 （例如在作为外部 Web 服务器的虚拟机与连接到公司内部网络的虚拟机之间）。
- 物理机与虚拟机 （例如在物理网络适配器卡和虚拟机之间设立防火墙）。

如何在 ESX Server 3 配置中使用防火墙取决于如何计划使用网络以及确保给定组件的安全性。例如，如果在您创建的虚拟网络中的每台虚拟机专用于运行同一部门的不同基准测试套件，那么从一台虚拟机对另一台虚拟机进行不利访问的风险极小。因此，不必将为虚拟机之间配置防火墙。但是，为防止外部主机测试运行的干扰，可在虚拟网络的入口点配置防火墙以保护整组虚拟机。

本节介绍配置 VirtualCenter 和未配置 VirtualCenter 时防火墙的安装位置。

- “配置了 VirtualCenter Server 网络的防火墙”（第 163 页）
- “未配置 VirtualCenter Server 网络的防火墙”（第 165 页）
- “用于管理访问的 TCP 和 UDP 端口”（第 166 页）
- “通过防火墙连接到 VirtualCenter Server”（第 168 页）
- “通过防火墙连接到虚拟机控制台”（第 168 页）
- “通过防火墙连接 ESX Server 3 主机”（第 170 页）
- “为支持的服务和管理代理打开防火墙端口”（第 171 页）

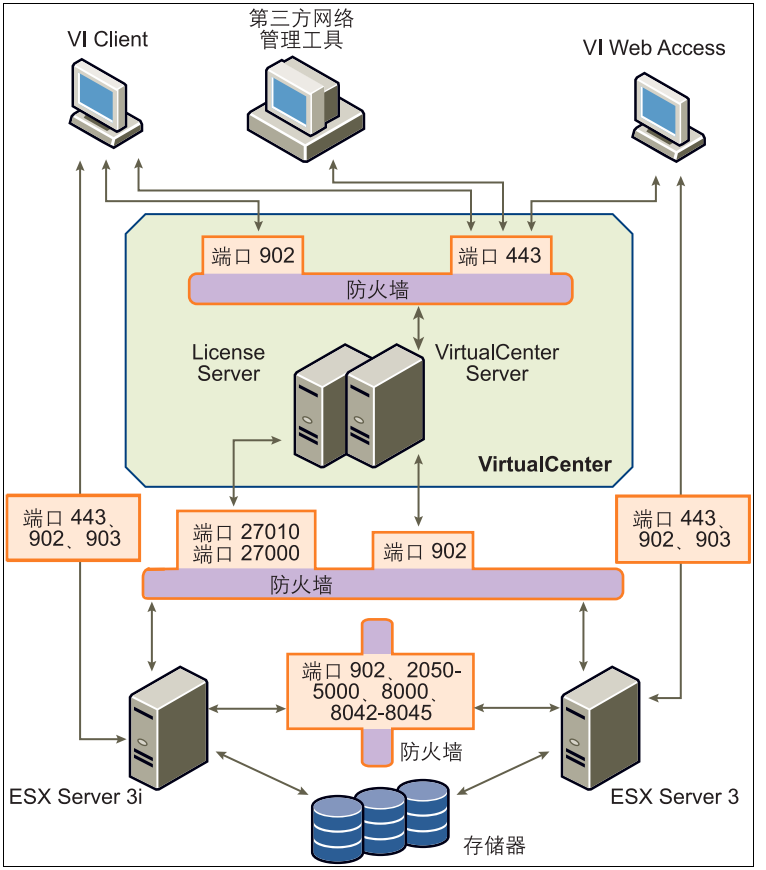
有关服务控制台防火墙的信息，请参见 “服务控制台防火墙配置”（第 211 页）。要在安装过程中配置防火墙和端口设置，请参见 *《设置指南》*。

配置了 VirtualCenter Server 网络的防火墙

若使用 VirtualCenter Server，可在图 10-1 中所示的任何位置安装防火墙。

注意 根据配置不同，可能无需图中所有防火墙，也可能需在未显示的位置安装防火墙。

图 10-1 Virtual Infrastructure 网络配置和流量流程



配置了 VirtualCenter Server 的网络可通过几种客户端接收通信：VI Client、 VI Web Access 或使用 SDK 与主机相连接的第三方网络管理客户端。在正常操作期间，VirtualCenter 在指定端口侦听受管主机和客户端的数据。 VirtualCenter 还假设其受管主机在指定端口侦听 VirtualCenter 的数据。如果这些元素之间有防火墙，必须确保防火墙中有打开的端口以支持数据传输。

若通过 VirtualCenter Server 访问 ESX Server 3 主机，则通常使用防火墙保护 VirtualCenter Server。该防火墙可为网络提供基本保护。该防火墙是位于客户端和 VirtualCenter Server 之间还是 VirtualCenter Server 和客户端均位于防火墙之后取决于您的部署。重点是确保在作为整个网络入口点处安装防火墙。

您可能要在网络中的其他访问点安装防火墙，具体取决于网络使用规划以及各种设备的安全级别。根据为网络配置确定的安全风险选择防火墙位置。以下是 ESX Server 3 实施常用的防火墙位置列表。列表和图 10-1 中的许多防火墙位置都是可选的。

- Web 浏览器与 VI Web Access HTTP 和 HTTPS 代理服务器之间。
- VI Client、VI Web Access Client 或第三方网络管理客户端与 VirtualCenter Server 之间。
- VI Client 与 ESX Server 3 主机之间 （若用户通过 VI Client 访问虚拟机）。此连接附加在 VI Client 与 VirtualCenter Server 间的连接之上，且需要一个不同端口。
- Web 浏览器与 ESX Server 3 主机之间 （若用户通过 Web 浏览器访问虚拟机）。此连接附加在 VI Web Access Client 与 VirtualCenter Server 间的连接之上，且需要不同端口。
- License Server 与 VirtualCenter Server 或 ESX Server 3 主机之间。在包括 VirtualCenter Server 的配置中， License Server 与 VirtualCenter Server 通常在同一台物理机上运行。在这种情况下，License Server 通过防火墙连接到 ESX Server 3 网络，与 VirtualCenter Server 并行运行，但使用不同端口。

  在有些配置中可能使用外部 License Server，例如您的公司需通过一个专用设备控制所有许可证。为此，应通过 License Server 和 VirtualCenter Server 之间的防火墙连接这两个服务器。

  无论如何设置 License Server 连接，用于许可证流量的端口均相同。有关许可信息，请参见 *《设置指南》*。
- VirtualCenter Server 与 ESX Server 3 主机之间。
- 网络中的 ESX Server 3 主机之间。尽管 ESX Server 3 主机之间的流量通常被认为是可信的，但如果担心计算机之间的安全性遭到破坏，可在 ESX Server 3 主机间添加防火墙。

  若在 ESX Server 3 主机间添加防火墙并打算在服务器间迁移虚拟机、执行克隆操作或使用 Vmotion，还必须在将源主机和目标主机隔开的防火墙中打开端口，以便两者进行通信。
- ESX Server 3 主机和网络存储器（例如 NFS 或 iSCSI 存储器）之间。这些端口并非专用于 VMware，可根据网络规范进行配置。

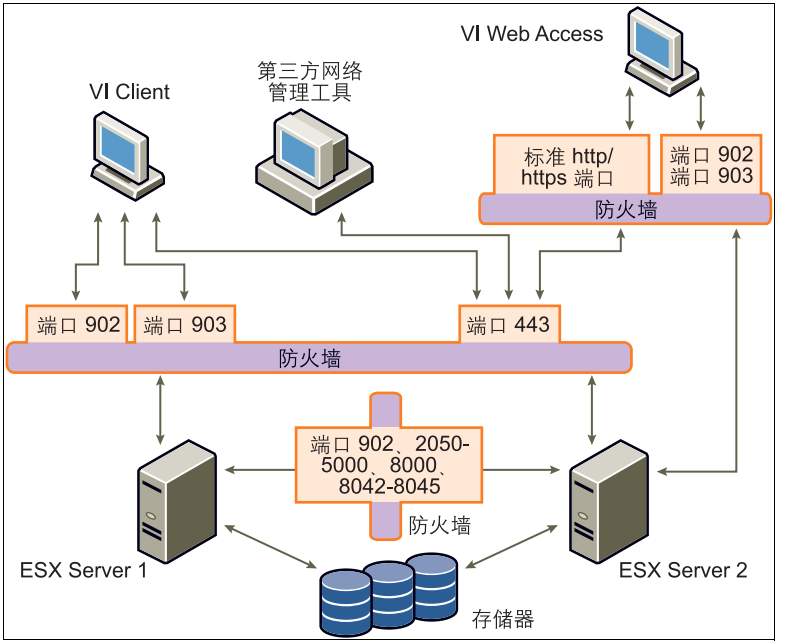
有关端口打开以用于这些通信路径的信息，请参见 ″用于管理访问的 TCP 和 UDP 端口″（第 166 页）。

未配置 VirtualCenter Server 网络的防火墙

若将客户端直接连接到 ESX Server 3 网络，而不是使用 VirtualCenter Server，则防火墙配置略为简单。可在 图 10-2 中显示的任何位置安装防火墙。

注意 根据配置不同，可能无需图 10-2 中所有防火墙，也可能需在未显示的位置安装防火墙。

图 10-2 针对客户端直接管理的 ESX Server 3 网络的防火墙配置



无论网络有没有配置 VirtualCenter Server，均通过相同类型的客户端接收通信：VI Client、VI Web Access Client 或第三方网络管理客户端。防火墙需求通常相同，但有一些重要区别：

- 与包含 VirtualCenter Server 的配置一样，应确保有防火墙保护 ESX Server 3 层，或保护客户端及 ESX Server 3 层，具体取决于您的配置。该防火墙可为网络提供基本保护。所使用的防火墙端口与配置了 VirtualCenter Server 的情况相同。

- 此类配置中的许可是您在每台 ESX Server 3 主机上安装的 ESX Server 3 包的一部分。由于许可证驻留在服务器上，因此无需安装单独的 License Server。这就免除了在 License Server 与 ESX Server 3 间设立防火墙的需要。

  注意 有时可能需要将许可证集中起来。可选择维护单独的 License Server，或将 License Server 寄存在网络中的一台 ESX Server 3 主机上。无论使用哪种方法，均通过防火墙使用通常为虚拟机许可预留的端口将 License Server 连接到 ESX Server 3 网络，这与配置了 VirtualCenter Server 的情况是一样的。若使用 License Server，而不是使用在 ESX Server 3 主机上自动安装的许可证，需对配置进行额外设置。有关许可信息，请参见 *《设置指南》*。

用于管理访问的 TCP 和 UDP 端口

本节列出了用于对 VirtualCenter Server、ESX Server 3 主机和其他网络组件进行管理访问的预定 TCP 和 UDP 端口。若要从防火墙外管理网络组件，可能需重新配置防火墙以允许在适当端口的访问。

注意 表 10-1 中列出的端口均通过服务控制台界面连接，除非另有指定。

表 10-1 TCP 和 UDP 端口

端口	用途	流量类型
80	HTTP 访问。 默认的非安全 TCP Web 端口，通常与端口 443 一起用作从 Web 访问 ESX Server 3 网络的访问前端。端口 80 将流量重定向至 HTTPS 登录页面 （端口 443），您将从这里启动虚拟机控制台。 将端口 80 用于从 Web 到 VI Web Access 的连接。 WS 管理使用端口 80。	入站 TCP
427	CIM 客户端使用服务位置协议版本 2 (SLPv2) 来查找 CIM 服务器。	入站和出站 UDP

表 10-1 TCP 和 UDP 端口 （续）

端口	用途	流量类型
443	HTTPS 访问。 默认的 SSL Web 端口。将端口 443 用于： ■ 从 Web 到 VI Web Access 的连接。 ■ VI Web Access 和第三方网络管理客户端到 VirtualCenter Server 的连接。 ■ VI Web Access 和第三方网络管理客户端对 ESX Server 3 主机的直接访问。 ■ VI Client 对 VirtualCenter Server 的访问。 ■ VI Client 对 ESX Server 3 主机的直接访问。 ■ WS 管理。 ■ VMware Update Manager。 ■ VMware Converter。	入站 TCP
902	ESX Server 3 的身份验证流量。将端口 902 用于 ESX Server 3 主机在迁移和置备过程中对其他 ESX Server 3 主机的访问。	入站 TCP，出站 UDP
903	用户在特定 ESX Server 3 主机上访问虚拟机时生成的远程控制台流量。 将端口 903 用于： ■ VI Client 对虚拟机控制台的访问。 ■ VI Web Access Client 对虚拟机控制台的访问。	入站 TCP
2049	来自 NFS 存储设备的事务。 此端口用于 VMkernel 界面，而不是服务控制台界面。	入站和出站 TCP
2050-2250	ESX Server 3 主机之间的流量，用于 VMware High Availability (HA) 和 EMC 自动启动管理器。这些端口由 VMKernel 接口管理。	出站 TCP，入站和出站 UDP
3260	来自 iSCSI 存储设备的事务。 此端口用于 VMkernel 界面和服务控制台界面。	出站 TCP
5900-5906	由 VNC 等管理工具使用的 RFB 协议。	入站和出站 TCP
5988	通过 HTTPS 的 CIM XML 事务。	入站和出站 TCP
5989	通过 HTTP 的 CIM XML 事务。	入站和出站 TCP
8000	来自 Vmotion 的输入请求。 此端口用于 VMkernel 界面，而不是服务控制台界面。	入站和出站 TCP

表 10-1 TCP 和 UDP 端口 （续）

端口	用途	流量类型
8042-8045	ESX Server 3 主机之间的流量，用于 HA 和 EMC 自动启动管理器。	出站 TCP，入站和出站 UDP
27000	从 ESX Server 3 到 License Server (lmgrd.exe) 的许可证事务	入站和出站 TCP
27010	从 ESX Server 3 到 License Server (vmwarelm.exe) 的许可证事务	入站和出站 TCP

除上述 TCP 和 UDP 端口外，还可根据需要配置其他端口：

- 可使用 VI Client 为已安装的管理代理及支持的服务 （例如 SSH、 NFS 等等）打开端口。有关为这些服务配置附加端口的信息，请参见 “为支持的服务和管理代理打开防火墙端口”（第 171 页）。
- 可以通过运行命令行脚本在服务控制台防火墙中为网络所需的其他服务和代理打开端口。请参见 “服务控制台防火墙配置”（第 211 页）。

通过防火墙连接到 VirtualCenter Server

如表 10-1 中所示，VirtualCenter Server 使用端口 443 侦听其客户端的数据传输。如果 VirtualCenter Server 及其客户端之间设有防火墙，则必须配置一个连接，以便 VirtualCenter Server 接收客户端的数据。

要使 VirtualCenter Server 能够接收客户端的数据，请打开端口 443。有关配置防火墙端口的其他信息，请联系防火墙系统管理员。

如果正在使用 VI Client 且不希望将端口 443 用作 VI Client 与 VirtualCenter Server 的通信端口，可通过更改 VI Client 的 VirtualCenter 设置切换到另一个端口。要了解如何更改这些设置，请参见 *《基本系统管理指南》*。

通过防火墙连接到虚拟机控制台

无论是通过 VirtualCenter Server 将客户端连接到 ESX Server 3 主机，还是将其直接连接到 ESX Server 3 主机，用户和管理员与虚拟机控制台的通信都需要某些端口。这些端口支持不同客户端功能，与 ESX Server 3 内的不同层相连接，并使用不同身份验证协议。它们是：

- **端口 902** - VirtualCenter Server 使用此端口向 VirtualCenter 受管主机发送数据。端口 902 是 VirtualCenter Server 向 ESX Server 3 主机发送数据时假设可用的端口。VMware 不支持为此连接配置不同端口。

  端口 902 通过 VMware 授权守护进程 (`vmware-authd`) 将 VirtualCenter Server 连接到 ESX Server 3 主机。此守护进程随后将端口 902 的数据分多路传输到适当的接收方进行处理。

- **端口 443** - VI Client、VI Web Access Client 和 SDK 使用此端口向 VirtualCenter 受管主机发送数据。当直接连接到 ESX Server 3 主机时，VI Client、VI Web Access Client 和 SDK 还使用此端口支持与服务器及其虚拟机相关的任何管理功能。端口 443 是客户端向 ESX Server 3 主机发送数据时假设可用的端口。VMware 不支持为这些连接配置不同端口。

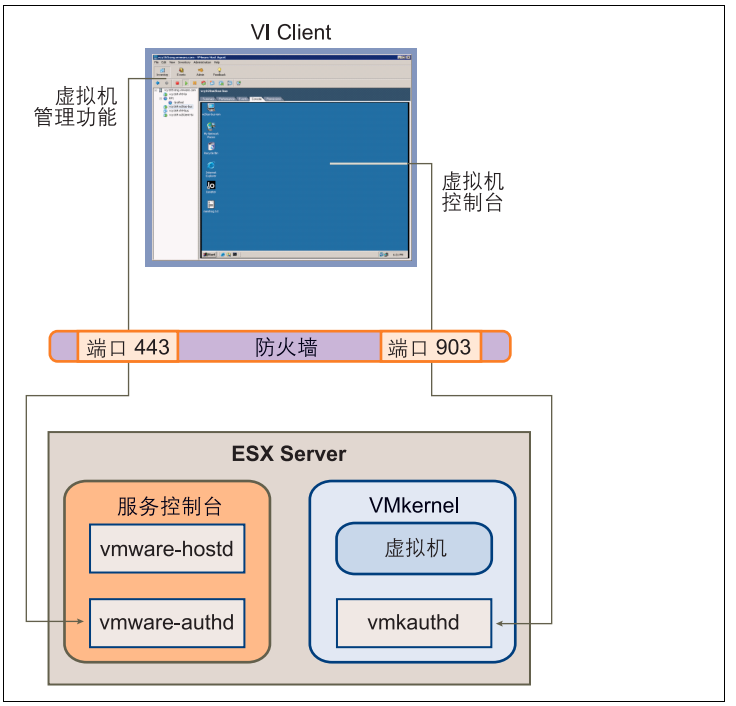
  端口 443 通过 Tomcat Web 服务或 SDK 将客户端连接到 ESX Server 3 主机。`vmware-hostd` 将端口 443 的数据分多路传输到适当的接收方进行处理。

- **端口 903** - VI Client 和 VI Web Access 使用此端口为虚拟机上的客户操作系统鼠标 - 键盘 - 屏幕 (MKS) 活动提供连接。用户正是通过此端口与虚拟机的客户操作系统及应用程序交互。端口 903 是 VI Client 和 VI Web Access 与虚拟机交互时假设可用的端口。 VMware 不支持为此功能配置不同端口。

  端口 903 将 VI Client 连接到在 ESX Server 3 上配置的指定虚拟机。

图 10-3 说明了 VI Client 功能、端口及 ESX Server 3 进程间的关系。 VI Web Access Client 使用相同的基本映射与 ESX Server 3 主机交互。

图 10-3 VI Client 与 ESX Server 3 通信时的端口使用情况



如果在 VirtualCenter Server 和 VirtualCenter 受管主机间设有防火墙，打开防火墙中的端口 443 和 903 可允许：

- 从 VirtualCenter Server 到 ESX Server 3 主机的数据传输。
- 从 VI Client 和 VI Web Access 直接到 ESX Server 3 主机的数据传输。

有关配置端口的其他信息，请咨询防火墙系统管理员。

通过防火墙连接 ESX Server 3 主机

如果在两个 ESX Server 3 主机间设有防火墙，并希望允许主机间的事务或使用 VirtualCenter 执行任何源或目标操作 （例如 VMware High Availability (HA) 流量、迁移、克隆或 Vmotion），则必须配置一个连接，以便受管主机接收数据。可以通过打开下列端口实现这一点：

- 443 （服务器到服务器的迁移和置备流量）
- 2050-5000 （用于 HA 流量）

- 8000 （用于 Vmotion）
- 8042-8045 （用于 HA 流量）

有关配置端口的其他信息，请咨询防火墙系统管理员。有关这些端口的方向和协议的更详细信息，请参见 “用于管理访问的 TCP 和 UDP 端口”（第 166 页）。

为支持的服务和管理代理打开防火墙端口

使用 VI Client 将服务器控制台防火墙配置为接受普遍支持的服务和已安装的管理代理。在 VirtualCenter 中配置 ESX Server 3 主机安全配置文件时，添加或移除这些服务或代理会自动打开或关闭防火墙中的预定端口以允许或禁止与服务或代理的通信。以下是可以添加或移除的服务和代理列表：

- NIS 客户端
- NFS 客户端 （不安全服务）
- SMB 客户端 （不安全服务）
- FTP 客户端 （不安全服务）
- SSH 客户端
- Telnet 客户端 （不安全服务）
- NTP 客户端
- iSCSI 软件客户端
- SSH 服务器
- Telnet 服务器 （不安全服务）
- FTP 服务器 （不安全服务）
- NFS 服务器 （不安全服务）
- CIM HTTP 服务器 （不安全服务）
- CIM HTTPS 服务器
- SNMP 服务器
- Syslog 客户端
- 您安装的其他受支持管理代理

注意 此列表可能更改，因此您可能会发现 VI Client 提供此列表中未提到的服务和代理。此外，并非列表中的所有服务都将默认安装。可能需要执行其他任务来配置和启用这些任务。

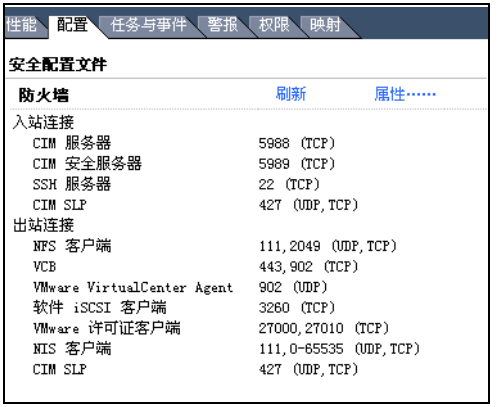
如果列表中不包括安装的设备、服务或代理，请从命令行打开服务控制台防火墙中的端口。请参见 “服务控制台防火墙配置”（第 211 页）。

允许服务或管理代理访问 ESX Server 3

1 登录 VI Client，从清单面板中选择服务器。

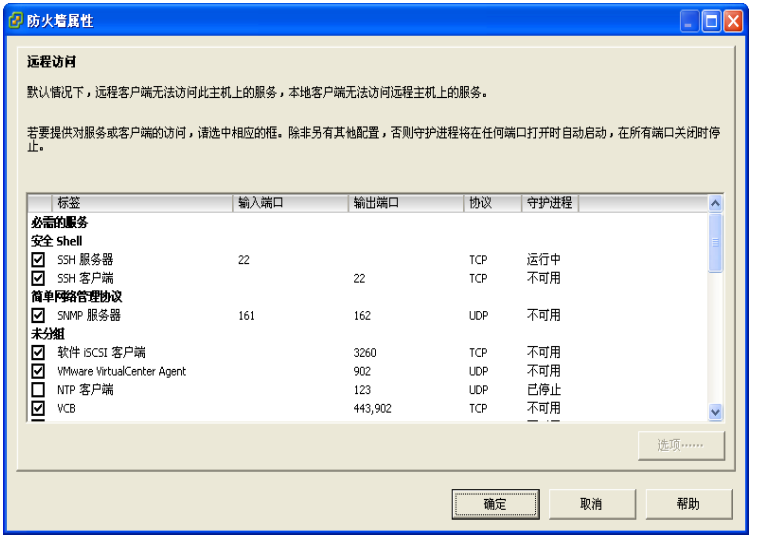
2 依次单击 **[配置 (Configuration)]** 选项卡和 **[安全配置文件 (Security Profile)]**。

VI Client 将显示相应防火墙端口当前活动的输入和输出连接列表。



3 单击 **[属性 (Properties)]**，打开 **[防火墙属性 (Firewall Properties)]** 对话框。

[防火墙属性 (Firewall Properties)] 对话框列出了可为主机配置的所有服务和管理代理。



4 选择要启用的服务和代理。

[入站端口 (Incoming Ports)] 和 **[出站端口 (Outgoing Ports)]** 列表示 VI Client 为该服务打开的端口，**[协议 (Protocol)]** 列表示该服务使用的协议，**[守护进程 (Daemon)]** 列表示与该服务关联的守护进程状态。

5 单击 **[确定 (OK)]**。

根据防火墙设置自动执行服务行为

ESX Server 3 可对服务是否随防火墙端口状态启动的行为进行自动化。该自动化功能有助于确保当环境配置为启用服务功能时启动服务。例如，仅当某些端口打开时启动某网络服务可帮助避免这样的情况，即服务已启动，但无法完成实现预定目的所需的通信。

例如，某些协议 （如 Kerberos）要求获取有关当前时间的准确信息。 NTP 服务是获取准确时间信息的一种方式，但此服务只能在所需防火墙端口打开的情况下运作。因此，若所有端口均处于关闭状态，此服务将无法实现其目标。 NTP 服务提供一个选项，可配置启动或停止此服务的条件。此配置包括一些选项，指定是否打开防火墙端口，然后是否根据这些条件启动或停止 NTP 服务。有多个可能的配置选项，所有选项均同时适用于 SSH 服务器。

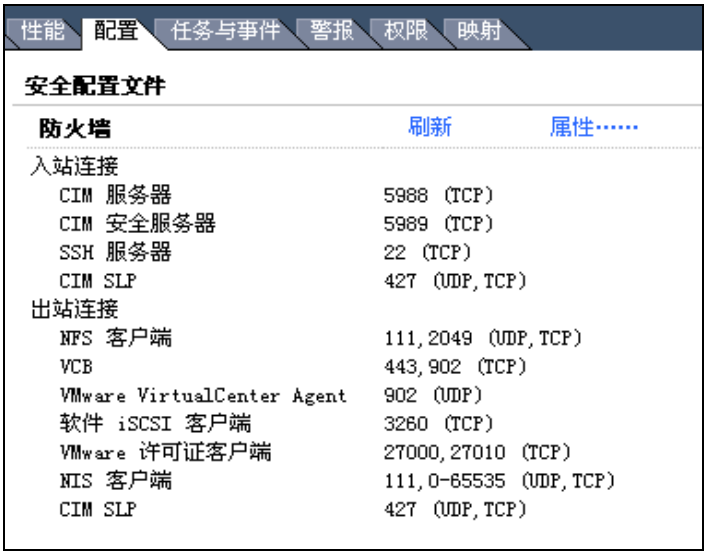
注意 本节中说明的设置仅适用于通过 VI Client 或用 VMware Infrastructure SDK 创建的应用程序配置的服务设置。通过其他方式 （例如 esxcfg-firewall 实用程序或 /etc/init.d/ 中的配置文件）进行的配置不会受这些设置的影响。

- **[如果任何端口打开则自动启动，如果所有端口关闭则停止 (Start automatically if any ports are open, and stop when all ports are closed)]** - 这是这些服务的默认设置，也是 VMware 推荐的设置。如果任何端口打开，则客户端尝试联系与相关服务有关的网络资源。如果某些端口打开，但特定服务的端口关闭，则此尝试将失败，但几乎不会对此类情况造成障碍，当适用的出站端口打开时，此服务将开始完成其任务。
- **[与主机一起启动和停止 (Start and stop with host)]** - 服务在主机启动后立即启动，并在主机关机之前不久关闭。此选项与 **[如果任何端口打开则启动，如果所有端口关闭则停止 (Start automatically if any ports are open, and stop when all ports are closed)]** 非常相似，都意味着此服务经常尝试完成其任务 （例如 NTP 服务尝试连接到指定的 NTP 服务器。）。如果端口之前是关闭的，但随后打开了，客户端将在此后立即开始完成其任务。
- **[手动启动和停止 (Start and stop manually)]** - 主机保留用户指定的服务设置，无论端口打开与否。当用户启动 NTP 服务后，只要主机仍然开启，该服务会一直运行。如果服务已启动且主机已关闭，该服务将作为关机程序的一部分停止，但当主机一启动，该服务将再次启动，保留用户指定的状态。

配置服务启动与防火墙配置的关系

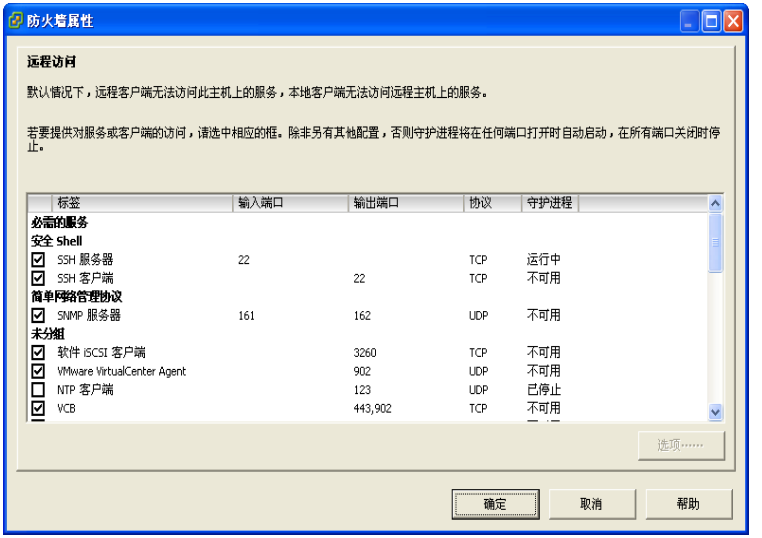
1 登录 VI Client，从清单面板中选择服务器。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[安全配置文件 (Security Profile)]**。VI Client 将显示相应防火墙端口当前活动的输入和输出连接列表。



3 单击 **[属性 (Properties)]**。

[防火墙属性 (Firewall Properties)] 对话框列出了可为主机配置的所有服务和管理代理。



4 选择要配置的服务，然后单击 **[选项 (Options)]**。

[启动策略 (Startup Policy)] 决定服务启动的条件。此对话框还提供有关服务当前状态的信息，并提供手动启动、停止或重新启动服务的界面。

5 从 **[启动策略 (Startup Policy)]** 选项中选择一项。

6 单击 **[确定 (OK)]**。

通过 VLAN 确保虚拟机安全

网络可能是任何系统中最脆弱的环节之一。与物理网络一样，虚拟机网络也需要保护。如果将虚拟机网络与物理网络连接，则其遭到破坏的风险不亚于由物理机组成的网络。即使虚拟机网络已与任何物理网络隔离，虚拟机也可能遭到网络中的其他虚拟机的攻击。用于确保虚拟机安全的要求通常与物理机相同。

虚拟机是相互独立的。一台虚拟机无法读取或写入另一台虚拟机的内存、访问其数据、使用其应用程序等等。但在网络中，任何虚拟机或虚拟机组仍可能遭到其他虚拟机的未授权访问，因此可能需要通过外部手段加强保护。可通过以下方式增加这层保护：

- 为虚拟网络增加防火墙保护，方法是在其中的部分或所有虚拟机上安装和配置软件防火墙。

  为提高效率，可设置专用虚拟机以太网或*虚拟网络*。有了虚拟网络，可在网络最前面的虚拟机上安装软件防火墙。这可以充当物理网络适配器和虚拟网络中剩余虚拟机之间的保护性缓存。

  在虚拟网络最前面的虚拟机上安装软件防火墙是一项不错的安全措施。但是，软件防火墙会降低性能，因此请先对安全需求和性能进行权衡，然后再决定在虚拟网络中的其他虚拟机上安装软件防火墙。请参见 “网络概念概述”（第 20 页）。

- 将主机中的不同虚拟机区域置于不同网络段上。如果将虚拟机区域隔离在自己的网络段中，可以大大降低虚拟机区域间泄漏数据的风险。分段可防止多种威胁，包括地址解析协议 (ARP) 欺骗，即攻击者操作 ARP 表以重新映射 MAC 和 IP 地址，从而访问进出主机的网络流量。攻击者使用 ARP 欺骗生成拒绝服务，劫持目标系统并以其他方式破坏虚拟网络。

  精细分段可降低虚拟机区域间传送数据包的几率，从而防止探查攻击 （此类攻击需向受害者发送网络流量）。此外，攻击者无法使用一个虚拟机区域中的不安全服务访问主机中的其他虚拟机区域。可以使用两种方法之一实施分段，每种方法具有不同优势。

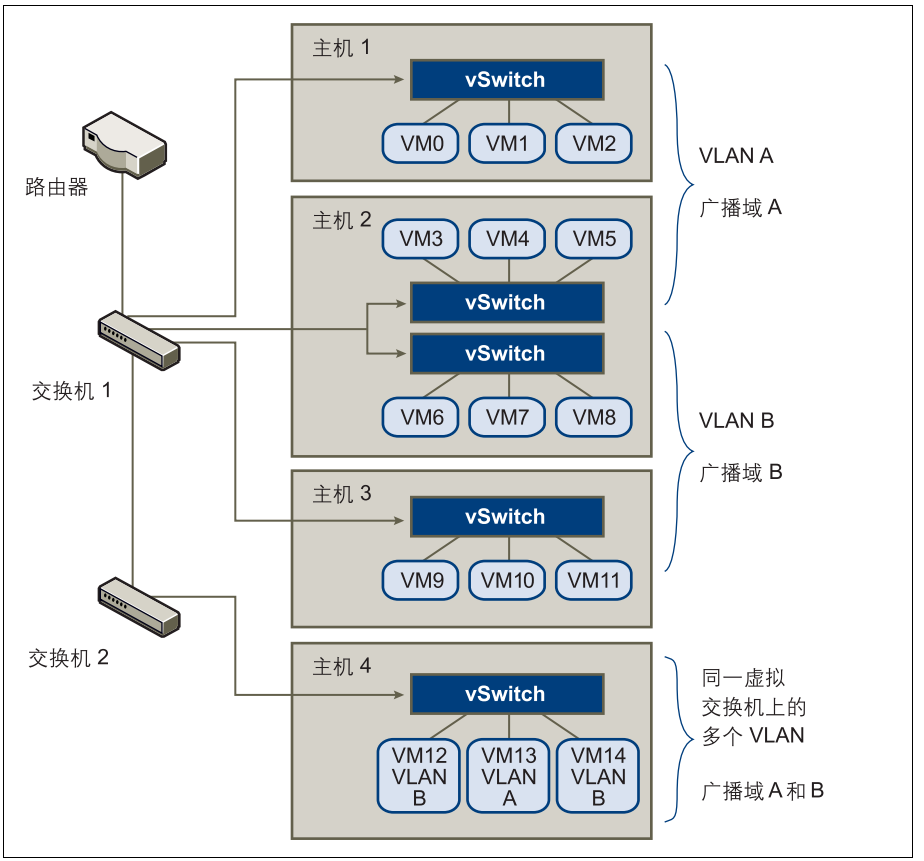
  - 将单独的物理网络适配器用于虚拟机分区，以确保各分区处于隔离状态。将单独的物理网络适配器用于虚拟机分区可能是最安全的方法，并且在初次创建段之后不易出现配置错误。

- 设置虚拟局域网 (VLAN) 以帮助保护网络。 VLAN 几乎能够提供以物理方式实施单独网络所具有的所有安全优势，但省去了硬件开销，可为您节省部署和维护附加设备、线缆等硬件的成本，是一种可行的解决方案。

VLAN 是一种 IEEE 标准的网络方案，通过特定的标记方法将数据包的传送限制在 VLAN 中的端口内。若配置正确， VLAN 将是您保护一组虚拟机免遭意外或恶意侵袭的可靠方法。

VLAN 可让您对物理网络进行分段，以便只有属于相同 VLAN 的网络中的两台虚拟机才能相互传送数据包。例如，会计记录和会计帐务是一家公司最敏感的内部信息。如果公司的销售、货运和会计员工均使用同一物理网络中的虚拟机，可按图 10-4 所示设置 VLAN 以保护会计部门的虚拟机。

图 10-4 VLAN 布局示例



在此配置中，会计部门的所有员工均使用 VLAN A 中的虚拟机，销售部门的员工使用 VLAN B 中的虚拟机。

路由器将包含会计数据的数据包转发至交换机。这些数据包将被标记为仅分发至 VLAN A。因此，数据将被局限在广播域 A 内，无法传送到广播域 B，除非对路由器进行此配置。

该 VLAN 配置可防止销售人员截取传至会计部门的数据包。还可防止会计部门接收传至销售组的数据包。一个虚拟交换机可为不同 VLAN 中的虚拟机服务。

vSwitch 和 VLAN 安全注意事项

ESX Server 3 配备完整的符合 IEEE 802.1q 的 VLAN 实施。如何设置 VLAN 以确保网络组件安全取决于您安装的客户操作系统、网络设备的配置方式等因素。 VMware 不能对如何设置 VLAN 提出具体建议，但当您使用 VLAN 部署作为安全执行策略一部分时，应考虑以下因素：

- **将 VLAN 视作更广的安全实施的一部分** - VLAN 能够有效地控制数据在网络中的传送位置和范围。如果攻击者可以访问网络，其攻击行为可能仅限于用作入口点的 VLAN，从而降低了攻击整个网络的风险。

  VLAN 之所以能够提供保护，只是因为它可以控制数据在通过交换机并进入网络后的传送和包含方式。VLAN 可帮助确保网络架构的第 2 层（数据链接层）安全。但是，配置 VLAN 不能保护网络模型的物理层或任何其他层。即使创建 VLAN，也应通过确保硬件 （路由器、集线器等等）安全和加密数据传送来提供额外保护。

  VLAN 不能代替虚拟机配置中的防火墙。大多数包括 VLAN 的网络配置也同时包括防火墙。如果虚拟网络中包括 VLAN，请确保安装的所有防火墙是 VLAN 可识别的。

- **确保正确配置 VLAN** - 设备配置错误及网络、硬件、固件或软件缺陷会导致 VLAN 容易遭到 VLAN 跳转攻击。如果有权访问一个 VLAN 的攻击者创建了一些数据包，并用欺骗手段致使物理交换机将这些数据包传送到其无权访问的另一个 VLAN，则将发生 VLAN 跳转。容易受到此类攻击的原因通常是由于对本机 VLAN 操作进行了错误的交换机配置，从而导致交换机可以接收和传送未标记数据包。

  为帮助防止 VLAN 跳转，请及时安装硬件和固件更新以确保设备是最新的。同时请在配置设备时遵照供应商的最佳做法准则。

  VMware 虚拟交换机不支持本机 VLAN 的概念。通过这些交换机的所有数据都会被适当地标记。但是，网络中可能有其他为本机 VLAN 操作配置的交换机，因此配置了虚拟交换机的 VLAN 仍然容易遭受 VLAN 跳转。

如果计划使用 VLAN 执行网络安全，VMware 建议为所有交换机禁用本机 VLAN 功能，除非必须在本机模式中操作某些 VLAN。如果需要使用本机 VLAN，请注意交换机供应商就此功能提供的配置准则。

- **为管理工具和服务控制台之间的通信创建单独的 VLAN 或虚拟交换机** - 无论是使用管理客户端还是命令行， ESX Server 3 的所有配置任务均通过服务控制台来执行，包括配置存储器、控制虚拟机行为的各个方面及设置虚拟交换机或虚拟网络。服务控制台是 ESX Server 3 的控制点，确保它免遭误用非常关键。

  VMware ESX Server 3 管理客户端使用身份验证和加密方法来防止对服务控制台进行未授权访问，而其他服务可能不提供相同保护。如果攻击者可以访问服务控制台，便可以自由地重新配置 ESX Server 3 主机的许多属性，例如更改整个虚拟交换机配置、更改授权方法等等。

  服务控制台的网络连接通过虚拟交换机建立。要为这个关键的 ESX Server 3 组件提供更好的保护， VMware 建议使用以下任一方法隔离服务控制台：

  - 为管理工具与服务控制台之间的通信创建单独的 VLAN。
  - 配置网络访问，以便通过一个虚拟交换机及一个或多个上行链路端口连接管理工具和控制台。

  两种方法均可防止任何无法访问服务控制台 VLAN 或虚拟交换机的用户看到进出服务控制台的流量，还可防止攻击者向服务控制台发送数据包。您也可以选择在单独的物理网络段上配置服务控制台。物理分段可提供一层额外的安全保护，因为以后不易出现配置错误。

  除了为管理工具与服务控制台之间的通信设置单独的 VLAN 或虚拟交换机外，还应为 VMotion 及网络附加存储器设置单独的 VLAN 或虚拟交换机。

  如果您的配置包含一个直接通过主机而不是通过硬件适配器配置的 iSCSI SAN，应为服务控制台和 iSCSI 创建一个单独的虚拟交换机以提供共享网络连接。第二个网络连接附加在用于管理工具通信的主服务控制台网络连接之上。第二个服务控制台网络连接仅支持 iSCSI 活动，不应将其用于任何管理活动或管理工具通信。

虚拟交换机保护和 VLAN

通过 VMware 虚拟交换机可阻止某些威胁 VLAN 安全的行为。虚拟交换机的设计方式使其可以防御各种攻击，其中多种攻击均涉及 VLAN 跳转。有了这层保护并不能保证您的虚拟机配置不会遭受其他类型的攻击。例如，虚拟交换机只能保护虚拟网络免遭这些攻击，但不能保护物理网络。

以下列表将介绍一些虚拟交换机和 VLAN 可以防御的攻击。

- **MAC 洪水** - 使交换机充满大量数据包，其中包含标记为来自不同来源的 MAC 地址。许多交换机使用内容可寻址内存 (CAM) 表了解和存储每个数据包的源地址。当此表填满时，交换机可能进入完全打开状况，此时将在所有端口广播每个输入数据包，致使攻击者看到交换机的所有流量。此状况可能导致 VLAN 间的数据包泄漏。

  VMware 虚拟交换机虽存储 MAC 地址表，但不获取来自显著流量的 MAC 地址，因此不容易受到此类攻击。

- **802.1q 和 ISL 标记攻击** - 强制交换机将帧从一个 VLAN 重定向至另一个 VLAN，方法是通过欺骗手段致使交换机充当干线并向其他 VLAN 广播流量。

  VMware 虚拟交换机不执行此类攻击所需的动态中继，因此不会遭到攻击。

- **双重封装攻击** - 出现的情形为：攻击者创建一个双重封装数据包，其内部标记中的 VLAN 标识符与外部标记中的 VLAN 标识符不同。为实现向后兼容性，本机 VLAN 将去除传送数据包的外部标记，除非进行其他配置。当本机 VLAN 交换机去除外部标记后，只剩下内部标记，它将把数据包传送到与所去除外部标记中标识的 VLAN 不同的 VLAN。

  VMware 虚拟交换机会丢弃虚拟机尝试通过为特定 VLAN 配置的端口发送的任何双重封装帧。因此它们不容易遭到此类攻击。

- **多播暴力攻击** - 涉及将大量多播帧几乎同时发送到已知 VLAN，以期使交换机过载，从而错误地允许向其他 VLAN 广播一些帧。

  VMware 虚拟机不允许帧离开其正确的广播域 (VLAN)，因此不容易遭到此类攻击。

- **跨树攻击** - 目标是跨树协议 (STP)，此协议用于控制 LAN 组件间的桥接。攻击者发送网桥协议数据单元 (BPDU) 数据包，尝试更改网络拓扑同时将这些封包设置为根网桥。作为根网桥，攻击者可以探查传送帧的内容。

  VMware 虚拟交换机不支持 STP，因此不容易受到此类攻击。

- **随机帧攻击** - 涉及发送大量数据包，这些数据包的源地址和目标地址保持不变，但字段的长度、类型或内容会随机变化。此类攻击的目标是强制交换机错误地将数据包发送到不同 VLAN。

  VMware 虚拟交换机不容易遭到此类攻击。

将来还会不断有新的安全威胁出现，因此请勿将此视作有关攻击的详尽列表。请定期查看网站 (http://www.vmware.com/support/security.html) 上的 VMware 安全资源，了解安全警示、近期安全警示及 VMware 安全策略。

确保虚拟交换机端口安全

与物理网络适配器一样，虚拟网络适配器也可以发送看上去来自不同机器的帧或模拟另一台机器，以便可以接收传至该机器的网络帧。此外，虚拟网络适配器也可以像物理网络适配器一样进行配置以接收传至其他机器的帧。

当您为网络创建虚拟交换机时，会添加端口组，为附加到交换机的虚拟机、存储系统等组件强加策略配置。可通过 VI Client 创建虚拟端口。

在向虚拟交换机添加端口或端口组的过程中， VI Client 会为端口配置安全配置文件。此安全配置文件可用来确保 ESX Server 3 阻止其虚拟机的客户操作系统模拟网络上的其他机器。实施此安全功能的目的在于使负责模拟的客户操作系统检测不到模拟行为已被阻止。

安全配置文件决定您对虚拟机执行的防模拟和截断攻击保护强度。为正确使用安全配置文件中的设置，需了解一些虚拟网络适配器如何控制传送及此级别的攻击如何进行的基础知识。

创建每个虚拟网络适配器时，都将向其分配自己的 MAC 地址。此地址称为初始 MAC 地址。尽管可以从客户操作系统外部重新配置初始 MAC 地址，但不能由客户操作系统进行更改。此外，每个适配器具有一个有效 MAC 地址，可过滤目标 MAC 地址与该有效 MAC 不同的输入网络流量。客户操作系统负责设置有效 MAC 地址，并通常将有效 MAC 地址与初始 MAC 地址保持一致。

发送数据包时，操作系统通常将其网络适配器的有效 MAC 地址输入以太网帧的源 MAC 地址字段。它还将接收网络适配器的 MAC 地址输入目标 MAC 地址字段。接收网络适配器仅在数据包的目标 MAC 地址与其自己的有效 MAC 地址匹配时才接受数据包。

网络适配器创建后，其有效 MAC 地址与初始 MAC 地址相同。虚拟机的操作系统可随时将有效 MAC 地址更改为其他值。如果操作系统更改了有效 MAC 地址，其网络适配器将接收传至新 MAC 地址的网络流量。操作系统可随时发送带有模拟源 MAC 地址的帧。这样，操作系统便可通过模拟经接收网络授权的网络适配器对网络中的设备进行恶意攻击。

可以使用 ESX Server 3 主机上的虚拟交换机安全配置文件设置以下选项以防止此类攻击：

- **[MAC 地址更改 (MAC Address Changes)]** - 默认情况下，此选项设置为 **[接受 (Accept)]**，这意味着 ESX Server 3 主机接受将有效 MAC 地址更改为非初始 MAC 地址的请求。**[MAC 地址更改 (MAC Address Changes)]** 选项设置将影响虚拟机接收的流量。

为防止 MAC 模拟，可将此选项设置为 **[拒绝 (Reject)]**。如果执行此操作 ESX Server 3 主机将不允许将有效 MAC 地址更改为非初始 MAC 地址的请求，而是禁用虚拟适配器用于发送请求的端口。这样一来，虚拟适配器必须在它将有效 MAC 地址更改为初始 MAC 地址后才能再接收帧。客户操作系统检测不到 MAC 地址更改已被拒绝。

注意 有时您可能确实需要多个适配器在网络中使用同一 MAC 地址 （例如在单播模式中使用 Microsoft 网络负载平衡）。在标准多播模式下使用 Microsoft 网络负载平衡时，适配器不能共享 MAC 地址。

- **[伪信号 (Forged Trasmits)]** - 默认情况下，此选项设置为 **[接受 (Accept)]**，这意味着 ESX Server 3 主机不比较源 MAC 地址和有效 MAC 地址。 **[伪信号 (Forged Trasmits)]** 选项设置将影响从虚拟机传送的流量。

  为防止 MAC 模拟，可将此选项设置为 **[拒绝 (Reject)]**。如此， ESX Server 3 主机将对操作系统传送的源 MAC 地址与其适配器的有效 MAC 地址进行比较，以确认是否匹配。如果地址不匹配， ESX Server 3 将丢弃数据包。

  客户操作系统检测不到其虚拟网络适配器无法使用模拟 MAC 地址发送数据包。ESX Server 3 主机会在带有模拟地址的任何数据包递送之前将其截断，而客户操作系统可能假设数据包已被丢弃。

- **[杂乱模式运行 (Promiscuous mode operation)]**- 默认情况下，此选项设置为 **[拒绝 (Reject)]**，这意味着虚拟网络适配器不能在杂乱模式中运行。杂乱模式会清除虚拟网络适配器执行的任何接收筛选，以便客户操作系统接收在线观察到的所有流量。

  尽管杂乱模式对于跟踪网络活动很有用，但它是一种不安全的运作模式，因为杂乱模式中的任何适配器均可访问各种数据包，无论某些数据包是否仅应由特定网络适配器接收。这意味着虚拟机中的管理员或根用户可以查看传至其他客户机或主机操作系统的流量。

  注意 有时您可能确实需要将虚拟交换机配置为在杂乱模式中运行 （例如运行网络入侵检测软件或数据包探查器时）。

若要为端口更改上述任何默认设置，应在 VI Client 通过编辑虚拟交换机设置来修改安全配置文件。有关编辑这些设置的信息，请参见 “虚拟交换机策略”（第 46 页）。

确保 iSCSI 存储器安全

为 ESX Server 3 主机配置的存储器可能包括一个或多个使用 iSCSI 的存储区域网络 (SAN)。iSCSI 是一种使用 TCP/IP 协议通过网络端口（而不是通过直接连接到 SCSI 设备）来访问 SCSI 设备和交换数据记录的方法。在 iSCSI 事务中，原始 SCSI 数据块被封装在 iSCSI 记录中并传送至请求数据的设备或用户。

iSCSI SAN 可让您有效地利用现有以太网架构为 ESX Server 3 主机提供对其可动态共享的资源的访问。iSCSI SAN 可为依赖公用存储池服务多个用户的环境提供经济的存储解决方案。与任何网络系统一样，iSCSI SAN 也可能遭到安全破坏。在 ESX Server 3 主机上配置 iSCSI 时，可采取几种措施降低安全风险。

注意 用于确保 iSCSI SAN 安全的要求和程序与可用于 ESX Server 3 主机的 iSCSI 硬件适配器和通过 ESX Server 3 主机直接配置的 iSCSI 相同。有关配置 iSCSI 适配器和存储器的信息，请参见 “iSCSI 存储器”（第 100 页）。

通过身份验证确保 iSCSI 设备的安全

确保 iSCSI 免遭不利侵袭的一种方法就是每当 ESX Server 3 主机尝试访问目标 LUN 上的数据时都要求 iSCSI 设备（或称*目标*）对主机（或称*启动器*）进行身份验证。身份验证的目的是证明启动器具有访问目标的权利，这是在您配置身份验证时授予的权利。

为 ESX Server 3 主机上的 iSCSI SAN 设置身份验证时有两个选项可选：

- **[挑战握手身份验证协议 (CHAP) (Challenge Handshake Authentication Protocol(CHAP))]** - 可将 iSCSI SAN 配置为使用 CHAP 身份验证。在 CHAP 身份验证中，当启动器联系 iSCSI 目标时，目标向启动器发送一个预定义 ID 值和一个随机值（或称*密钥*）。启动器随后创建一个单向哈希值，并将其发送给目标。此哈希值包含三个元素：目标发送的预定义 ID 值、随机值和一个由启动器和目标共享的专用值（或称 *CHAP 密码*）。当目标收到启动器的哈希值后，将使用相同的元素创建自己的哈希值并将其与启动器的哈希值进行比较。如果结果匹配，目标对启动器进行身份验证。

  ESX Server 3 对 iSCSI 支持单向 CHAP 身份验证，不支持双向 CHAP。在单向 CHAP 身份验证中，目标需验证启动器，但启动器无需验证目标。启动器仅有一组凭据，所有 iSCSI 目标均使用这组凭据。

  ESX Server 3 仅支持 HBA 级别的 CHAP 身份验证，不支持每个目标的 CHAP 身份验证，后者可让您为每个目标配置不同凭据以实现更好的目标优化。

- **[禁用 (Disabled)]** - 可将 iSCSI SAN 配置为不使用身份验证。启动器与目标间的通信仍需经过初步身份验证，因为 iSCSI 目标设备通常会设置为仅与特定启动器通信。

如果您的 iSCSI 存储器位于一个位置，并创建一个专用网络或 VLAN 为所有 iSCSI 设备提供服务，那么选择不执行更严格的身份验证可能有意义。 iSCSI 配置是安全的，因为它与任何不利访问隔离，这与光纤通道 SAN 很相似。

通常，除非您愿意冒 iSCSI SAN 被攻击的风险，或需处理因人为错误而造成的问题，否则请勿禁用身份验证。

ESX Server 3 不对 iSCSI 支持 Kerberos、安全远程协议 (SRP) 或公用密钥身份验证方法。此外，它也不支持 IPsec 身份验证和加密。

使用 VI Client 确定当前是否在执行身份验证并配置身份验证方法。

检查身份验证方法

1 登录 VI Client，从清单面板中选择服务器。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[存储适配器 (Storage Adapters)]**。

3 选择要检查的 iSCSI 适配器，然后单击 **[属性 (Properties)]** 以打开 **[iSCSI 启动器属性 (iSCSI Initiator Properties)]** 对话框。

4 单击 **[CHAP 身份验证 (CHAP Authentication)]**。

若 **[CHAP 名称 (CHAP Name)]** 显示一个名称 （通常是 iSCSI 启动器名称），则表示 iSCSI SAN 正在使用 CHAP 身份验证。

注意 如果 **[CHAP 名称 (CHAP Name)]** 显示 **[未指定 (Not Specified)]**，则表示 iSCSI SAN 未使用 CHAP 身份验证。

5 单击 **[关闭 (Close)]**。

配置 iSCSI 以用于 CHAP 身份验证

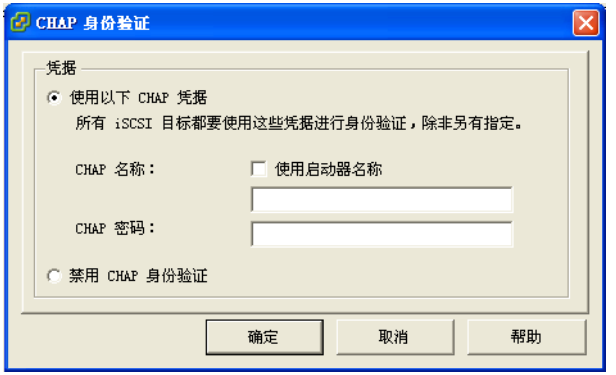
1 登录 VI Client，从清单面板中选择服务器。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[存储适配器 (Storage Adapters)]**。

3 选择 iSCSI 适配器，然后单击 **[属性 (Properties)]** 以打开 **[iSCSI 启动器属性 (iSCSI Initiator Properties)]** 对话框。

4 单击 **[CHAP 身份验证 (CHAP Authentication)]**> **[配置 (Configure)]** 以打开 **[CHAP 身份验证 (CHAP Authentication)]** 对话框。

5 单击 **[使用以下 CHAP 凭据 (Use the following CHAP credentials)]**。



6 执行下列操作之一：

- 要将 CHAP 名称设置为 iSCSI 适配器名称，请选中 **[使用启动器名称 (Use initiator name)]**。
- 要将 CHAP 名称设置为除 iSCSI 适配器名称之外的任何其他名称，请取消选中 **[使用启动器名称 (Use initiator name)]**，并在 **[CHAP 名称 (CHAP Name)]** 字段中输入不超过 255 个字母数字字符的名称。

7 输入 CHAP 密码以用作身份验证的一部分。

您输入的密码是一个文本字符串。

VI Client 未对您输入的 CHAP 密码施加长度限制。但是，某些 iSCSI 设备要求密码必须超过某一最少字符数，或对您可使用的字符类型有所限制。要确定具体要求，请查看制造商的文档。

8 单击 **[确定 (OK)]**。

禁用 iSCSI 身份验证

1 登录 VI Client，从清单面板中选择服务器。

2 依次单击 **[配置 (Configuration)]** 选项卡和 **[存储适配器 (Storage Adapters)]**。

3 选择 iSCSI 适配器，然后单击 **[属性 (Properties)]** 以打开 **[iSCSI 启动器属性 (iSCSI Initiator Properties)]** 对话框。

4 单击 **[CHAP 身份验证 (CHAP Authentication)]**> **[配置 (Configure)]** 以打开 **[CHAP 身份验证 (CHAP Authentication)]** 对话框。

5 选中 **[禁用 CHAP 身份验证 (Disable CHAP authentication)]**。

6 单击 **[确定 (OK)]**。

保护 iSCSI SAN

计划 iSCSI 配置时，应采取一些措施提高 iSCSI SAN 的整体安全。 iSCSI 配置是否安全取决于 IP 网络，因此在设置网络时执行良好的安全标准可帮助保护 iSCSI 存储器。

以下是一些具体建议：

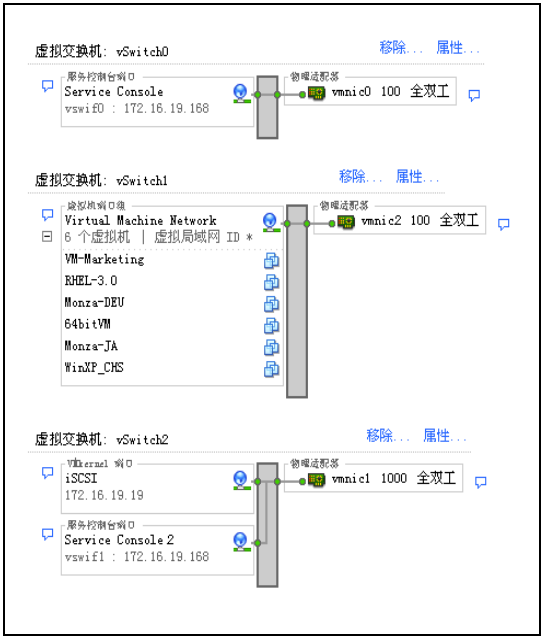
- **保护传送的数据** - iSCSI SAN 中的一个主要安全风险便是攻击者可能探查传送的存储数据。

  VMware 建议您采取额外措施使攻击者不易看到 iSCSI 数据。无论是 iSCSI 硬件适配器还是 ESX Server 3 主机 iSCSI 启动器，均不会对其传送至目标或从目标接收的数据进行加密，从而造成数据更易遭到探查攻击。

  通过 iSCSI 配置允许虚拟机共享虚拟交换机和 VLAN 可能导致 iSCSI 流量暴露，从而遭到虚拟机攻击者误用。为帮助确保入侵者无法侦听 iSCSI 传送数据，请确保任何虚拟机都无法看到 iSCSI 存储网络。

  如果使用硬件 iSCSI 适配器，可通过以下方式来实现：请确保 iSCSI 适配器和 ESX Server 3 物理网络适配器未由于共享交换机或某种其他方式而无意地在主机外部连接。如果直接通过 ESX Server 3 主机配置 iSCSI，可通虚拟机未使用的另一个虚拟机交换机配置 iSCSI 存储器，如图 10-5 中所示。

图 10-5 单独虚拟交换机上的 iSCSI 存储器



若直接通过主机而不是硬件适配器配置 iSCSI，必须在虚拟网络设置中为服务控制台创建两个网络连接。第一个服务控制台网络连接在其虚拟交换机上配置并以独占方式用于管理工具连接 （图中的 vSwitch0）。配置第二个服务控制台网络连接是为了共享用于 iSCSI 连接的虚拟交换机 （图中的 vSwitch2）。第二个服务控制台网络连接仅支持 iSCSI 活动。不应将其用于任何管理活动或管理工具通信。若要在共享虚拟交换机上对 iSCSI 和服务控制台进行一定程度的分离，可在不同 VLAN 上对它们进行配置。

注意 不要在用于 iSCSI 连接的虚拟交换机上为服务控制台配置默认网关，而是应在用于管理工具连接的虚拟交换机上配置默认网关。

除了通过提供专用虚拟交换机来保护 iSCSI SAN 外，还可考虑在 iSCSI SAN 自己的 VLAN 上对其进行配置。将 iSCSI 配置放在单独的 VLAN 上可确保只有 iSCSI 适配器可以看到 iSCSI SAN 内的传送数据。

- **确保 iSCSI 端口安全** - 当您运行 iSCSI 设备时， ESX Server 3 主机不会打开任何侦听网络连接的端口。此措施可降低入侵者通过空闲端口侵入 ESX Server 3 主机并控制主机的几率。因此，运行 iSCSI 时不会在连接的 ESX Server 3 主机端产生任何额外安全风险。

  您运行的任何 iSCSI 目标设备都必须具有一个或多个用于侦听 iSCSI 连接的开放 TCP 端口。如果 iSCSI 设备软件中存在任何安全漏洞，则数据遭遇的风险并非 ESX Server 3 所造成。要降低此风险，请安装存储设备制造商提供的所有安全修补程序并对连接到 iSCSI 网络的设备进行限制。

11 身份验证和用户管理

本章说明 ESX Server 3 如何处理用户身份验证并显示如何设置用户和组权限。此外，它讨论如何加密 VI Client、 SDK 和 VI Web Access 的连接，以及如何配置委派用户名以处理与 NFS 存储器进行的事务。

本章将讨论以下主题：

通过身份验证和权限确保 ESX Server 3 的安全

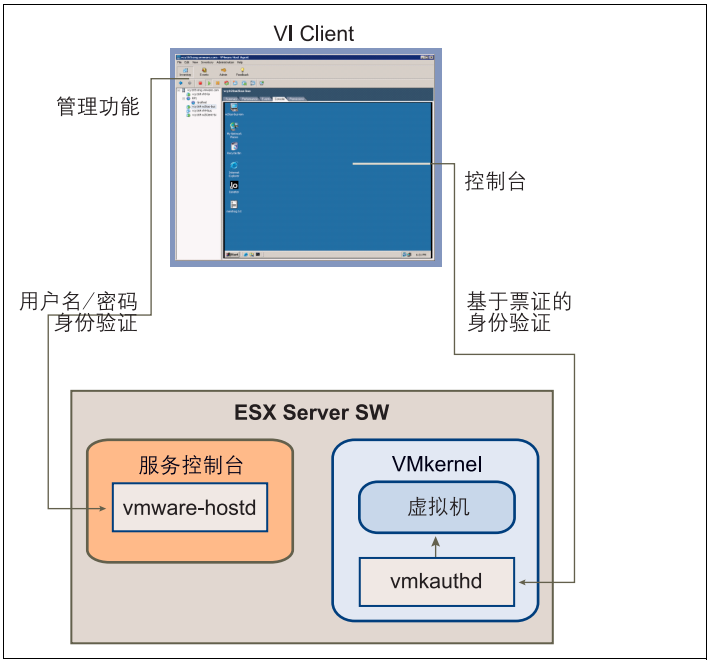
ESX Server 3 使用了“可插入认证模块 (PAM)”结构对使用 VI Client、VI Web Access 或服务控制台访问 ESX Server 3 主机的用户进行身份验证。VMware 服务的 PAM 配置位于 `/etc/pam.d/vmware-authd`，其中存储了身份验证模块的路径。

如同 Linux 一样， ESX Server 3 的默认安装使用了 `/etc/passwd` 身份验证，但可对 ESX Server 3 进行配置以使用另一个分布式身份验证机制。如果要使用第三方身份验证工具，而不使用 ESX Server 3 默认实施，请参考供应商文档以查看说明。在进行第三方身份验证的过程中，可能需要使用新的模块信息来更新 `/etc/pam.d/vmware-authd` 文件。

每当 VI Client 或 VirtualCenter 用户连接至 ESX Server 3 主机时， `xinetd` 进程即会连接“VMware 主机代理 (`vmware-hostd`)”进程。`vmware-hostd` 进程从客户端接收用户名和密码，并将它们转发至 PAM 模块以执行身份验证。

图 11-1 说明了 ESX Server 3 如何从 VI Client 对事务进行身份验证的一个基本示例。

图 11-1 对 VI Client 与 ESX Server 3 之间的通信进行身份验证



通过 VI Web Access 和第三方网络管理客户端进行的 ESX Server 身份验证事务以相似的方式与 `vmware-hostd` 进程直接进行交互。

要确保为您的站点有效地进行身份验证，您可能需要执行一些基本任务，例如，设置用户、组、权限和角色，配置用户属性、添加自己的证书及确定是否要使用 SSL 等。

关于用户、组、权限和角色

当具有相应权限的已知用户使用为用户存储的密码登录主机时，可以向其授予对 ESX Server 主机及其资源的访问权限。 VirtualCenter 在确定是否授予用户访问权限时，使用了相似的方法 VirtualCenter 和 ESX Server 主机根据分配给用户的权限确定用户的访问级别。例如，某用户可能具有在主机上创建虚拟机的权限，另一位用户可能具有启动虚拟机的权限但不具有创建虚拟机的权限。

VirtualCenter 和 ESX Server 3 主机凭借用户名、密码和权限组合这一机制对用户的访问权限进行验证并授予其执行操作的权限。为了支持这一机制， VirtualCenter 和 ESX Server 主机保留了授权用户、其密码及向每个用户分配的权限列表。 VirtualCenter 和 ESX Server 主机在下列情况下拒绝授予访问权限：

- 非用户列表上的用户尝试登录。
- 用户输入的密码不正确。
- 用户在列表上但未分配权限。
- 已成功登录的用户尝试执行其不具有相应权限的操作。

在管理 ESX Server 主机和 VirtualCenter 的过程中，需要制定用户和权限模型。通过这些模型，可对要如何处理特定类型的用户及如何设计权限进行基本规划。在制定用户名和权限模型时，请注意：

- ESX Server 3 和 VirtualCenter 使用了一组特权或*角色* 来控制每个用户或组可执行的操作。 ESX Server 3 和 VirtualCenter 提供了一组预定的角色，但也可自行创建新的角色。
- 分配组的用户更易于管理。如果创建了组，则可将角色应用至组，这样组中的所有用户将均继承此角色。

了解用户

用户是经过授权可登录 ESX Server 3 主机或 VirtualCenter 的个人。 ESX Server 3 用户分为两类：可通过 VirtualCenter 访问 ESX Server 3 主机的用户及通过 VI Client、 VI Web Access、第三方客户端或命令 shell 程序直接登录主机访问 ESX Server 3 主机的用户。这两个类别提取不同来源的用户。

- **授权的 VirtualCenter** - 包括在 VirtualCenter 引用的 Windows 域列表中，或者是 VirtualCenter 主机上的本地 Windows 用户。

不能使用 VirtualCenter 手动创建、移除或以其他方式更改用户。要操作用户列表或更改用户密码，必须通过用于管理 Windows 域的工具执行此操作。

对 Windows 域作出的任何更改均反映在 VirtualCenter 中。但由于不能直接在 VirtualCenter 中管理用户，因此用户界面不会提供用户列表以供查看。仅在角色分配期间选择用户和组时，才可使用用户和组列表。只有在选择配置权限的用户时才会看到这些更改。

- **直接访问用户** - 经授权直接在 ESX Server 3 主机上工作，已在安装 ESX Server 3 时默认添加至或由系统管理员在安装后添加至内部用户列表。

  如果以管理员身份登录主机，则可为这些用户执行各种管理操作，例如，更改密码、组成员资格和权限等。也可添加和移除用户。

VirtualCenter 保留的用户列表与 ESX Server 3 主机保留的用户列表完全独立。即使主机和 VirtualCenter 保留的列表似乎有共同的用户 （例如，称为 *devuser* 的用户），也应将这些用户视为碰巧拥有相同名称的独立用户。 VirtualCenter 中的 devuser 属性（包括权限和密码等）与 ESX Server 3 主机上的 devuser 属性相互独立。如果以 devuser 用户身份登录 VirtualCenter，则可能具有从数据存储查看和删除文件的权限，但是，如果以 devuser 用户身份登录 ESX Server 3 主机，则不具有这样的权限。

由于名称重复可能造成混乱， Vmware 建议您在创建 ESX Server 3 主机用户之前对 VirtualCenter 用户列表进行检查，以避免名称重复。要检查 VirtualCenter 用户，请查看 Windows 域列表。

了解组

通过创建组，可更有效地管理某些用户属性。组由通过一组公用的规则和权限进行管理的一组用户组成。向某个组分配权限时，该组中的所有用户都将继承这些权限，而不必逐个处理用户配置文件。因此，使用组可大大节省设置权限模型所需的时间，并提高未来可扩展性。

管理员需要决定如何建立组结构，以达到安全和使用目标。例如，三位兼职销售小组成员的工作时间各不相同，要他们共享一台虚拟机但不想使用销售经理的虚拟机。在这种情况下，可创建称为 *SalesShare* 的组，该组包括三个销售人员：Mary、 John 和 Tom。然后，可向 SalesShare 组授予仅与一个对象 （虚拟机 A）交互的权限。Mary、John 和 Tom 将继承这些权限，并可启动虚拟机 A，在虚拟机 A 上开始控制台会话。他们不能在销售经理的虚拟机上执行这些操作：虚拟机 B、 C 和 D。

VirtualCenter 和 ESX Server 3 主机上的组列表的来源与其各自用户列表的来源相同。如果通过 VirtualCenter 进行操作，则从 Windows 域调用组列表。如果直接登录至 ESX Server 3 主机，则从该主机保留的表格中调用组列表。建议以同样的方式处理组列表和用户列表。

了解权限

对于 ESX Server 3 和 VirtualCenter，将权限定义为访问角色，访问角色由用户及为对象 （例如，虚拟机或 ESX Server 3 主机）分配的用户角色组成。权限授予用户在 ESX Server 3 主机上执行特定操作和管理特定对象 （或者，如果用户从 VirtualCenter 进行操作，则指 VirtualCenter 管理的所有对象）的权利。例如，要配置 ESX Server 3 主机的内存，您必须拥有已授予主机配置特权的权限。

大多数 VirtualCenter 和 ESX Server 3 用户操作与主机相关联的对象的能力很有限。但是，管理员角色的用户则对诸如数据存储、主机、虚拟机和资源池之类的所有虚拟对象拥有充分的访问权利和权限。在默认情况下，将向超级用户授予管理员角色，如果由 VirtualCenter 管理主机，则 vpxuser 也是管理员用户。管理员用户具有以下权限：

- **超级用户** - 超级用户可在所登录的特定 ESX Server 3 主机上执行一系列完整的控制操作，包括操作权限、创建组和用户及处理事件等。已登录 ESX Server 3 主机的超级用户不能在更广泛的 ESX Server 3 部署中控制任何其他主机的活动。

  为了确保安全性起见，可能不想以管理员角色使用超级用户。在此情况下，可在安装后更改权限，以便使超级用户不再拥有管理特权，也可通过 VI Client 一起删除超级用户的访问权限，请参见 *《基本系统管理》* 中的 “管理用户、组、权限和角色” 章节。如果执行了此操作，首先必须创建超级用户级别的、可向另一个用户分配管理员角色的另一种权限。

  向另一个用户分配管理员角色，有助于通过可跟踪性维护安全。 VI Client 将管理员角色用户启动的所有操作记录为事件，使您能对其进行审计跟踪可使用此功能加强充当主机管理员的各个用户的责任心。如果所有管理员均以超级用户身份登录主机，则不能分辨某项操作是哪一个管理员执行的。相反，如果创建了超级用户级别的多个权限 （每一个权限均与不同的用户或用户组相关联），则可对每个管理员或管理组的操作进行跟踪。

  创建备用管理员用户后，就可以安全地删除超级用户的权限或更改其角色以限制其特权。如果删除或更改了超级用户的权限，则在将主机置于 VirtualCenter 的管理之中时，必须使用所创建的新用户作为主机身份验证点。请参见 “了解角色” （第 194 页）。

  注意 通过命令行界面运行的配置命令 （`esxcfg` 命令）不能执行访问检查。因此，即使限制超级用户的特权，也不会影响用户可使用命令行界面命令执行的操作。

- **vpxuser** - 此用户是在 ESX Server 3 主机上充当具有管理员权限的 VirtualCenter 的实体，它可为该主机管理活动。 vpxuser 是在将 ESX Server 3 主机连接至 VirtualCenter 时创建的。除非是通过 VirtualCenter 对 ESX Server 3 主机进行了管理，否则它不会显示在该主机上。

如果通过 VirtualCenter 对 ESX Server 3 主机进行管理，VirtualCenter 则在该主机上具有管理员特权。例如， VirtualCenter 可将虚拟机移至和移离主机，并执行支持虚拟机所必需的配置更改。

VirtualCenter 管理员可通过 vpxuser 在主机上执行超级用户可执行的大多数任务，并调度任务和处理模板等。但是，不能以 VirtualCenter 管理员身份执行某些操作。这些操作包括为 ESX Server 3 主机直接创建、删除或编辑用户和组，它仅可由具有管理员权限的用户直接在每个 ESX Server 3 主机上执行。

小心 不要以任何方式更改 vpxuser 及其权限。如果执行了此操作，在通过 VirtualCenter 操作 ESX Server 主机时可能会出现问题。

如果在 ESX Server 3i 主机上担当管理员角色，则可向该主机上的各个用户和组授予权限；如果在 VirtualCenter 中担当管理员角色，则可向 VirtualCenter 引用的 Windows 域列表中包含的任何用户或组授予权限。

VirtualCenter 通过分配权限这一流程对任何选定的 Windows 域用户或组进行注册。默认情况下，向属于 VirtualCenter Server 上本地 Windows 管理员组的所有用户授予与分配至管理员角色的任何用户相同的访问权利。属于管理员组的用户可以个人身份登录并具有充分访问权限。

为安全起见，可考虑从管理员角色中移除 Windows Administrators 组。可在安装后更改权限，以使 Windows Administrators 组不具备管理特权。也可使用 VI Client 删除 Windows Administrators 组访问权限。如果删除 Windows Administrators 访问权限，首先必须创建超级用户级别的、可向另一个用户分配管理员角色的另一种权限。

直接在 ESX Server 3i 主机上配置权限的方法与在 VirtualCenter 中配置权限的方法相同。而且， ESX Server 3i 和 VirtualCenter 的特权列表也相同。

如欲获取有关配置权限的信息且了解可分配的特权，请参见 *《基本系统管理》*。

了解角色

VirtualCenter 和 ESX Server 仅向分配了对象权限的用户授予对象访问权限。向用户或组分配对象权限时，可按角色对用户或组进行配对。角色是一组预定义的特权。

ESX Server 主机可提供三种默认的角色，与这些角色相关联的特权不可更改。每个后续的默认角色均包括前一个角色的特权。例如，管理员角色继承只读角色的特权。您本人创建的角色不继承任何默认角色的特权。默认的角色为：

- **无权访问** - 分配有此角色的对象用户不能以任何方式查看或更改对象。例如，拥有对特定虚拟机的**无权访问**角色的用户在登录 ESX Server 主机时无法看到 VI Client 清单中的虚拟机。拥有对特殊对象的**无权访问**角色的用户，可选择与**无权访问**的对象相关联的 VI Client 选项卡，但该选项卡不显示任何内容。例如，如果用户对任

何虚拟机都不具有访问权限，则他们可选择 **[虚拟机 (Virtual Machines)]** 选项卡，但不会看到列在此选项卡上的虚拟机或任何状态信息 - 表格为空白。

默认情况下，在 ESX Server 3 主机上创建的任何用户或组均分配有**无权访问**角色。可按每个对象提升或降低新创建的用户或组的角色。

默认情况下，超级用户和 vpxuser 是未分配有**无权访问**角色的唯一用户。相反，它们分配有管理员角色。

如果首先使用管理员角色创建了超级用户级别的替代权限并将此角色与另一个用户相关联，则可一起删除超级用户的权限或将其角色更改为无权访问。如果删除或更改了超级用户的权限，则在将主机置于 VirtualCenter 的管理之中时，必须使用所创建的新用户作为主机身份验证点。

- **只读** - 分配有此角色的对象用户，可查看对象的状况和详细信息。

  具有此角色的用户可查看虚拟机、主机和资源池属性。该用户不能查看主机的远程控制台。所有通过菜单和工具栏执行的操作均被禁止。

- **管理员** - 分配了此对象角色的用户可在对象上查看和执行所有操作。此角色也包括只读角色固有的所有权限。

可使用 VI Client 中的角色编辑设施创建自定义角色，以创建符合用户需求的特权组。如果使用了连接至 VirtualCenter 的 VI Client 来管理 ESX Server 3 主机，则可在 VirtualCenter 中选择其他角色。同样，在 VirtualCenter 中不可访问在 ESX Server 3 主机上直接创建的角色。仅当您直接从 VI Client 登录主机时，才可使用这些角色。

如果通过 VirtualCenter 管理 ESX Server 3 主机，则在主机和 VirtualCenter 中维护自定义角色可能会引起混淆和误用。在此类型配置中， VMware 建议仅在 VirtualCenter 中维护自定义角色。有关创建、更改和删除角色的信息及 VirtualCenter 中可用的其他角色的讨论，请参见 *《基本系统管理》*。

处理 ESX Server 3 主机上的用户和组

如果通过 VI Client 直接连接至 ESX Server 3 主机，则可创建、编辑和删除用户和组。只要登录 ESX Server 3 主机，就会看到这些用户和组，但在登录 VirtualCenter 时看不见。

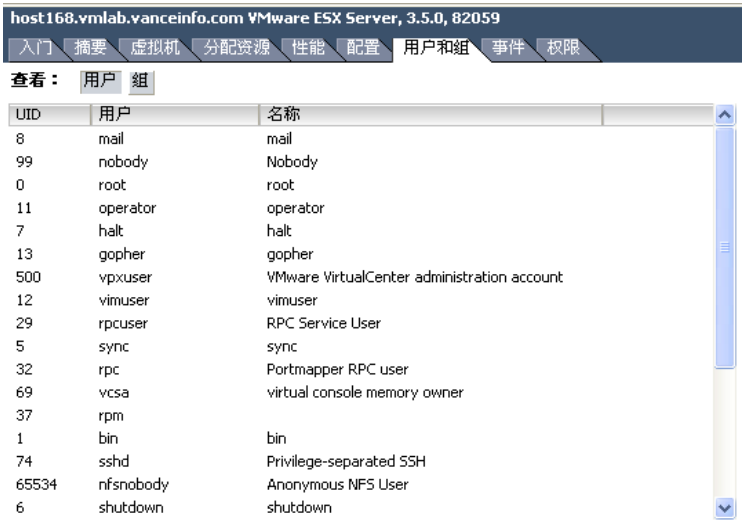
查看并导出用户和组信息

可通过 VI Client 中的 **[用户和组 (Users & Groups)]** 选项卡来处理用户和组。根据您单击的是 **[用户 (Users)]** 还是 **[组 (Groups)]**，该选项卡将显示 **[用户 (Users)]** 表或 **[组 (Groups)]** 表。

也可通过直接连接至 ESX Server 3 主机来创建角色并设置权限。由于这些任务在 VirtualCenter 中使用的更广泛，因此请参见 *《基本系统管理》* 获得有关处理权限和角色的信息。

图 11-2 显示了 **[用户 (Users)]** 表。**[组 (Groups)]** 表与其相似。

图 11-2 用户表



UID	用户	名称
8	mail	mail
99	nobody	Nobody
0	root	root
11	operator	operator
7	halt	halt
13	gopher	gopher
500	vpxuser	VMware VirtualCenter administration account
12	vimuser	vimuser
29	rpcuser	RPC Service User
5	sync	sync
32	rpc	Portmapper RPC user
69	vcsa	virtual console memory owner
37	rpm	
1	bin	bin
74	sshd	Privilege-separated SSH
65534	nfsnobody	Anonymous NFS User
6	shutdown	shutdown

可按列来对列表排序，显示或隐藏列，以及以准备报告或在 Web 上发布用户或组列表时可使用的格式来导出列表。

查看和排序 ESX Server 3 用户或组

1 通过 ESX Server 3 主机登录 VI Client。

2 从清单面板中选择服务器。

3 单击 **[用户和组 (Users & Groups)]** 选项卡或单击 **[用户 (Users)]** 或 **[组 (Groups)]**。

4 必要时执行以下任何操作：

- 要按任意列对表进行排序，请单击列标题。
- 要显示或隐藏列，请右键单击任何列标题，并选择或取消选择要隐藏的列名称。

从 ESX Server 3 用户或组表中导出数据

1 通过 ESX Server 3 主机登录 VI Client。

2 从清单面板中选择服务器。

3 单击 **[用户和组 (Users & Groups)]** 选项卡，然后单击 **[用户 (Users)]** 或 **[组 (Groups)]**。

4 根据要在已导出文件中看到的信息，确定如何排序表及隐藏或显示列。

5 右键单击用户表中的任何位置，然后单击 **[导出 (Export)]** 以打开 **[另存为 (Save As)]** 对话框。

6 选择路径，输入文件名，然后选择文件类型。

7 单击 **[确定 (OK)]**。

处理用户表

可向 ESX Server 3 主机 **[用户 (Users)]** 表添加用户、移除用户以及更改各种用户属性，例如密码和组成员资格。执行这些操作时，即正在更改 ESX Server 3 主机保留的内部用户列表。

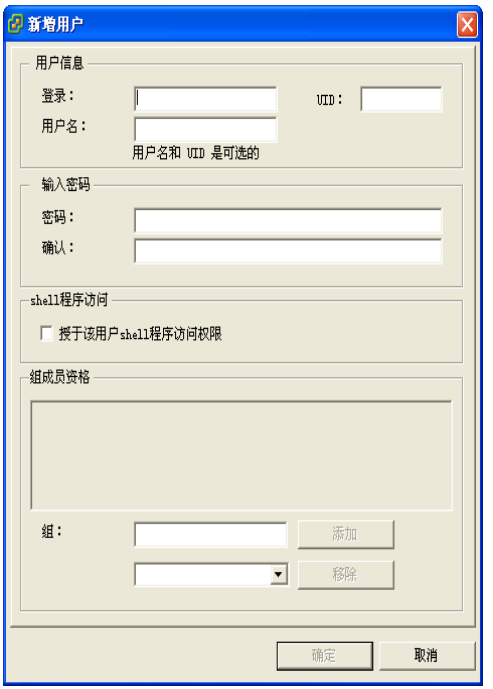
向 ESX Server 3 用户表添加用户

1 通过 ESX Server 3 主机登录 VI Client。

2 从清单面板中选择服务器。

3 单击 **[用户和组 (Users & Groups)]** 选项卡，然后单击 **[用户 (Users)]**。

4 右键单击 **[用户 (Users)]** 表中的任何位置，然后单击 **[添加 (Add)]** 以打开 **[新增用户 (Add New User)]** 对话框。



5 输入登录名、用户名、数字用户 ID (UID) 和密码。

指定用户名和 UID 是可选的。如果未指定 UID， VI Client 则分配下一个可用的 UID。

密码的长度和复杂性应符合 “密码限制”（第 214 页）中所述要求。但是， ESX Server 3 主机仅在您已切换至 `pam_passwdqc.so` 插件以进行身份验证时才检查密码的符合性。并不强制执行默认身份验证插件 `pam_cracklib.so` 中的密码设置。

6 如果要用户能通过命令 shell 程序访问 ESX Server 3 主机，请选择 **[授予该用户 shell 程序访问权限 (Grant shell access to this user)]**。

一般而言，不要向 ESX Server 3 主机用户授予 shell 程序访问权限，除非您确定有必要通过 shell 程序而不是通过 VI Client 访问主机。仅通过 VI Client 访问主机的用户不需要具有 shell 程序访问权限。

7 对于要用户所属的每个现有组，输入组名称，然后单击 **[添加 (Add)]**。

如果键入的组名称不存在，VI Client 会发出警告，且不将该组添加至 **[组成员资格 (Group membership)]** 列表。

8 单击 **[确定 (OK)]**。

输入的登录和用户名显示在 **[用户 (Users)]** 表中。

修改用户设置

1 通过 ESX Server 3 主机登录 VI Client。

2 从清单面板中选择服务器。

3 单击 **[用户和组 (Users & Groups)]** 选项卡，然后单击 **[用户 (Users)]**。

4 右键单击要修改的用户，然后单击 **[编辑 (Edit)]** 以打开 **[编辑用户 (Edit User)]** 对话框。

5 要更改用户 ID，请在 **[UID]** 字段中输入数字用户 ID。

VI Client 在您首次创建用户时分配 UID。大多数情况下，并不需要更改此分配。

6 请输入新的用户名。

7 要更改用户密码，请选择 **[更改密码 (Change Password)]**，然后输入新密码。

密码的长度和复杂性应符合 “密码限制”（第 214 页）中所述要求。但是， ESX Server 3 主机仅在您已切换至 `pam_passwdqc.so` 插件以进行身份验证时才检查密码的符合性。并不强制执行默认身份验证插件 `pam_cracklib.so` 中的密码设置。

8 要更改用户通过命令 shell 程序访问 ESX Server 3 主机的能力，请选择或取消选择 **[授予该用户 shell 程序访问权限 (Grant shell access to this user)]**。

9 要将此用户添加到其他组，请输入组名称，然后单击 **[添加 (Add)]**。

如果键入的组名称不存在，VI Client 会发出警告，且不将该组添加至 **[组成员资格 (Group membership)]** 列表。

10 要从组中移除用户，请从列表中选择组名称，然后单击 **[移除 (Remove)]**。

11 单击 **[确定 (OK)]**。

从 ESX Server 3 用户表移除用户

1 通过 ESX Server 3 主机登录 VI Client。

2 从清单面板中选择服务器。

3 单击 **[用户和组 (Users & Groups)]** 选项卡，然后单击 **[用户 (Users)]**。

4 右键单击要移除的用户，然后单击 **[移除 (Remove)]**。

小心 *不要* 移除超级用户。

处理组表

可向 ESX Server 3 的 **[组 (Groups)]** 表添加组，移除组以及添加或移除组成员。执行这些操作时，即正在更改 ESX Server 3 主机保留的内部组列表。

向 ESX Server 3 组表添加组

1 通过 ESX Server 3 主机登录 VI Client。

2 从清单面板中选择服务器。

3 依次单击 **[用户和组 (Users & Groups)]** 选项卡和 **[组 (Groups)]**。

4 右键单击 **[组 (Groups)]** 表中的任何位置，然后单击 **[添加 (Add)]** 打开 **[新增组 (Create New Group)]** 对话框。

5 在 **[组 ID (Group ID)]** 字段中输入组名称和数字组 ID (GID)。

指定 GID 是可选的。如果未指定 GID， VI Client 则分配下一个可用的组 ID。

6 对于想作为组成员的每个用户，输入用户名并单击 **[添加 (Add)]**。

如果键入的用户名不存在，VI Client 会发出警告，且不会将该用户添加至 **[此组中用户 (Users in this group)]** 列表。

7 单击 **[确定 (OK)]**。

输入的组 ID 和组名称现已显示在 **[组 (Groups)]** 表中。

在组中添加或移除用户

1 通过 ESX Server 3 主机登录 VI Client。

2 从清单面板中选择服务器。

3 依次单击 **[用户和组 (Users & Groups)]** 选项卡和 **[组 (Groups)]**。

4 右键单击要修改的组，然后单击 **[编辑 (Edit)]** 打开 **[编辑组 (Edit Group)]** 对话框。

5 要向该组中添加用户，请键入用户名，然后单击 **[添加 (Add)]**。

如果键入的用户名不存在，VI Client 会发出警告，且不将该用户添加至 **[此组中用户 (Users in this group)]** 列表。

6 要从组中移除用户，请从列表中选择用户名，然后单击 **[移除 (Remove)]**。

7 单击 **[确定 (OK)]**。

从 ESX Server 3 组表移除组

1 通过 ESX Server 3 主机登录 VI Client。

2 从清单面板中选择服务器。

3 依次单击 **[用户和组 (Users & Groups)]** 选项卡和 **[组 (Groups)]**。

4 右键单击要移除的组，然后单击 **[移除 (Remove)]**。

小心 *不要* 移除超级用户。

ESX Server 3 加密和安全证书

ESX Server 支持 SSL v3 和 TLS v1 （此处统称为 SSL）。SSL 有助于保障通信安全。如果启用了 SSL，则数据将是专用的，并受到保护，因此这些数据无法读取，并且只要在传输过程中对其进行修改，就将被检测到。只要以下条件成立，所有网络流量都会进行加密。

- 未对 Web 代理服务作出更改以允许未加密的流量通过端口。
- 服务控制台防火墙的安全性已配置为中级和高级。有关配置服务控制台防火墙的信息，请参见 “服务控制台防火墙配置”（第 211 页）。

默认情况下不启用 SSL，因此，如果不采取操作，将不会对网络流量加密。SSL 会保护 VI Client 和 VirtualCenter 之间的初始连接，但不会对后续通信加密。要完全启用 ESX Server 3 中的证书提供的安全功能，必须启用证书检查并安装新证书。

启用证书检查

1 使用 VI Client 登录到 VirtualCenter server。

2 单击 **[管理 (Administration)]** > **[Virtual Center Management Server 配置 (Virtual Center Management Server Configuration)]**。

此时会出现 **[Virtual Center Management Server 配置 (Virtual Center Management Server Configuration)]** 对话框。

3 在左窗格中单击 **[SSL 设置 (SSL Settings)]**，然后启用 **[检查主机证书 (Check host certificates)]** 复选框。

4 单击 **[确定 (OK)]**。

要利用证书检查的全部优点，请安装新证书。初始证书由 ESX Server 创建并存储在主机上。用于确保 VirtualCenter 和 VI Web Access 会话安全的证书未经可信证书颁发机构签署，因此，它不能提供您在生产环境中可能需要的身份验证安全性。例如，自签署证书易于受到中间人攻击。如果要在外部使用加密的连接，则需要向可信证书颁发机构购买证书，或使用您本人的安全证书进行 SSL 连接。如果使用了自签署证书，客户端就会收到关于证书的警告。

要解决此问题，请安装由公认的证书颁发机构签署的证书。

证书的默认位置是 ESX Server 3 主机上的 `/etc/vmware/ssl/`。证书由两个文件组成：证书本身 (`rui.crt`) 和专用密钥文件 (`rui.key`)。

添加证书并修改 ESX Server 3 Web 代理设置

在添加 ESX Server 3 证书并考虑加密和用户安全性，请注意以下事项：

- 避免使用口令设置证书。 ESX Server 3 并不处理口令 （也称为加密的密钥）。如果设置口令， ESX Server 3 进程将无法正常启动。
- 可配置 Web 代理，以使其搜索非默认位置中的证书。对于倾向于将其证书集中在单台计算机上以便使多台主机可使用证书的公司而言，此功能相当有用。

小心 如果证书的存储位置不是 ESX Server 3 主机，当主机丢失网络连接时，证书将无法使用。如果启用了证书检查，将无法与客户机建立安全连接。

- 为了支持对用户名、密码和数据包进行加密，将为 VI Web Access 和 VMware Infrastructure SDK 连接启用 SSL。要配置这些连接以使它们不对传输进行加密，请为 VI Web Access 连接或 VMware Infrastructure SDK 连接禁用 SSL，方法是将连接从 HTTPS 切换至 HTTP，如 “更改 Web 代理服务的安全设置”（第 203 页）中所述。仅当为这些客户端创建了充分可信的环境时才可考虑禁用 SSL，此环境中安装了防火墙且完全隔离与主机间的传输。禁用 SSL 可提高性能，因为避免了执行加密所需的开销。
- 为了防止误用 ESX Server 3 服务 （例如，托管 VI Web Access 的内部 Web 服务器），仅可通过用于 HTTPS 传输的端口 443 才能访问大多数内部 ESX Server 3 服务。端口 443 充当 ESX Server 3 的反向代理。通过 HTTP 欢迎页面即可看到 ESX Server 3 上的服务列表，但如果未经适当授权，则不能直接访问这些服务。可对此设置进行更改，以便可通过 HTTP 连接直接访问各种服务。 VMware 建议您不要作出此更改，除非是在充分可信的环境中使用 ESX Server 3。
- 在升级 VirtualCenter 和 VI Web Access 时，证书仍然不变。如果移除 VirtualCenter 和 VI Web Access，证书目录不会从服务控制台中移除。

配置 Web 代理以在非默认位置中搜索证书

1 以超级用户身份登录服务控制台。

2 将目录更改为 /etc/vmware/hostd/。

3 使用文本编辑器打开 proxy.xml 文件，并找到以下 XML 分段：

```
<ssl>
  <!-- The server private key file-->
  <privateKey>/etc/vmware/ssl/rui.key</privateKey>
  <!-- The server side certificate file-->
  <certificate>/etc/vmware/ssl/rui.crt</certificate>
</ssl>
```

4 使用从可信证书颁发机构接收的专用密钥文件的绝对路径来替换 /etc/vmware/ssl/rui.key。

此路径可能位于 ESX Server 3 主机上，也可能位于存储公司的证书和密钥的集中式计算机上。

注意 保持 <privateKey> 和 </privateKey> XML 标记不变。

5 使用从可信证书颁发机构接收的证书文件的绝对路径来替换 /etc/vmware/ssl/rui.crt。

小心 不要删除原始 rui.key 和 rui.crt 文件。ESX Server 主机会使用这些文件。

6 保存更改并关闭文件。

7 输入以下命令以重新启动 vmware-hostd 进程：

```
service mgmt-vmware restart
```

更改 Web 代理服务的安全设置

1 以超级用户身份登录服务控制台。

2 将目录更改为 /etc/vmware/hostd/。

3 使用文本编辑器打开 proxy.xml 文件。文件内容通常如下所示：

```
<ConfigRoot>
   <EndpointList>
      <_length>6</_length>
      <_type>vim.ProxyService.EndpointSpec[]</_type>
      <e id="0">
         <_type>vim.ProxyService.NamedPipeServiceSpec</_type>
```

```
            <accessMode>httpsWithRedirect</accessMode>
            <pipeName>/var/run/vmware/proxy-webserver</pipeName>
            <serverNamespace>/</serverNamespace>
         </e>
         <e id="1">
            <_type>vim.ProxyService.NamedPipeServiceSpec</_type>
            <accessMode>httpsWithRedirect</accessMode>
            <pipeName>/var/run/vmware/proxy-sdk</pipeName>
            <serverNamespace>/sdk</serverNamespace>
         </e>
         <e id="2">
            <_type>vim.ProxyService.LocalServiceSpec</_type>
            <accessMode>httpsWithRedirect</accessMode>
            <port>8080</port>
            <serverNamespace>/ui</serverNamespace>
         </e>
         <e id="3">
            <_type>vim.ProxyService.NamedPipeServiceSpec</_type>
            <accessMode>httpsOnly</accessMode>
            <pipeName>/var/run/vmware/proxy-vpxa</pipeName>
            <serverNamespace>/vpxa</serverNamespace>
         </e>
         <e id="4">
            <_type>vim.ProxyService.NamedPipeServiceSpec</_type>
            <accessMode>httpsWithRedirect</accessMode>
            <pipeName>/var/run/vmware/proxy-mob</pipeName>
            <serverNamespace>/mob</serverNamespace>
         </e>
         <e id="5">
            <_type>vim.ProxyService.LocalServiceSpec</_type>
            <!--Use this mode for "secure" deployment-->
            <!-- <accessMode>httpsWithRedirect</accessMode> -->
            <!-- Use this mode for "insecure" deployment-->
            <accessMode>httpAndHttps</accessMode>
            <port>8889</port>
            <serverNamespace>/wsman</serverNamespace>
         </e>
      </EndpointList>
   </ConfigRoot>
```

4 根据需要更改安全设置。例如，您可能要修改使用 HTTPS 的服务的条目，以添加 HTTP 访问的选项。

   - *e id* 是服务器 ID XML 标记的 ID 编号。ID 编号在 HTTP 区域中必须是唯一的。

- *_type* 为所移动的服务的名称，例如 /sdk 或 /mob。
- *accessmode* 是服务允许的通信形式。可接受的值包括：
  - httpOnly - 只能通过纯文本 HTTP 连接访问服务。
  - httpsOnly - 只能通过 HTTPS 连接访问服务。
  - httpsWithRedirect - 只能通过 HTTPS 连接访问服务。通过 HTTP 发出的请求将被重定向至相应的 HTTPS URL。
  - httpAndHttps - 可通过 HTTP 和 HTTPS 两种连接访问服务。
- *port* 是分配给该服务的端口号。可将不同的端口编号分配至服务。
- *namespace* 是提供此服务的服务器的命名空间。

5 保存更改并关闭文件。

6 输入以下命令以重新启动 vmware-hostd 进程：

```
service mgmt-vmware restart
```

示例：设置 VI Web Access 以通过不安全的端口进行通信

VI Web Access 通常通过安全端口 (HTTPS, 443) 与 ESX Server 3 主机进行通信。如果处在完全可信的环境中，则可决定可以允许不安全的端口 （例如， HTTP, 80）。要执行此操作，请在 proxy.xml 文件中更改 webserver 的 accessMode 属性，如 "更改 Web 代理服务的安全设置"（第 203 页）中所述。结果如下。 accessMode 从 httpsWithRedirect 更改为 httpAndHttps。

```
<_type>vim.ProxyService.LocalServiceSpec</_type>
<accessMode>httpAndHttps</accessMode>
<port>8080</port>
<serverNamespace>/ui</serverNamespace>
```

重新生成证书

在安装后首次启动主机时， ESX Server 3 主机会生成证书。此后，只要重新启动 vmware-hostd 进程， mgmt-vmware 脚本就会搜索现有的证书文件 （rui.crt 和 rui.key），如果它不能找到这些文件，就会生成新的证书文件。

在某些情况下，可能需要强制 ESX Server 3 主机生成新的证书。通常只有在下列情况下，才需要生成新的证书：

- 更改了主机名。
- 意外删除了证书。

为 ESX Server 3 主机生成新的证书

1 将目录更改为 /etc/vmware/ssl。

2 执行以下命令，为任何现有证书创建备份：

```
mv rui.crt orig.rui.crt
mv rui.key orig.rui.key
```

注意 如果由于意外删除了证书而生成新证书，则不必完成备份步骤。

3 输入以下命令以重新启动 vmware-hostd 进程：

```
service mgmt-vmware restart
```

4 通过执行以下命令将新证书文件的时戳与 orig.rui.crt 和 orig.rui.key 进行对比，以确认 ESX Server 3 主机已生成了新的证书：

```
ls -la
```

NFS 存储器的虚拟机委派

要在虚拟机上执行大多数操作， ESX Server 3 需要访问虚拟机文件。例如，为了启动和关闭虚拟机， ESX Server 3 必须能创建、操作和删除虚拟磁盘文件的存储卷上的文件。

要在 NFS 数据存储上创建、配置或管理虚拟机，可以使用委派用户。 ESX Server 3i 使用委派用户的身份来识别向基本文件系统发出的所有 I/O 请求。委派用户是试验性的，不受正式支持。

默认情况下，ESX Server 3 主机的委派用户为 root 用户。但是，将 root 用户用作委派用户可能不适用于所有 NFS 数据存储。 NFS 管理员可在启用根权限压缩的情况下导出卷。 root squash 功能将超级用户权限映射至 NFS 服务器上不具有重要特权的用户，从而限制超级用户的能力。此功能通常用于防止对 NFS 卷上的文件进行未授权的访问。如果在已启用 root squash 的情况下导出 NFS 卷，NFS 服务器则可能拒绝对 ESX Server 3 主机进行的访问。为了确保您可从主机创建和管理虚拟机，NFS 管理员必须关闭 root squash 功能，或将 ESX Server 3 主机的物理网络适配器添加至可信服务器的列表中。

如果 NFS 管理员不愿采取任何这些行动，可通过试验性的 ESX Server 3 功能将委派用户更改为另一个身份。该身份必须与 NFS 服务器上目录的所有者匹配，否则 ESX Server 3 主机无法执行文件级操作。要为委派用户设置另一个身份，请获取以下信息：

- 使用目录所有者的名称
- 使用目录所有者的 ID (UID)
- 使用目录所有者的组 ID (GID)

使用此信息更改 ESX Server 3 主机的委派用户设置，以便使其与目录所有者相匹配，使 NFS 数据存储能正确地识别 ESX Server 3 主机。委派用户的配置是全局性的，同样的身份可用于访问每个卷。

在 ESX Server 3 主机上设置委派用户需要完成以下操作：

- 从直接在 ESX Server 3 主机上运行的 VI Client 的 **[用户和组 (Users & Groups)]** 选项卡：
  - 编辑用户命名的 `vimuser` 以添加正确的 UID 和 GID。`vimuser` 是为了便于您设置委派用户而向您提供的 ESX Server 3 主机用户。默认情况下，`vimuser` 的 UID 为 12， GID 为 20。
  - 用委派用户名、 UID 和 GID 将一个全新的用户添加至 ESX Server 3 主机。

  无论是通过直接连接还是通过 VirtualCenter Server 管理主机，都必须执行这些步骤。同时，请确保委派用户 （所创建的 `vimuser` 或委派用户）在使用 NFS 数据存储的所有 ESX Server 3 主机上均是相同的。有关添加用户的信息，请参见 “处理用户表”（第 197 页）。
- 按以下步骤中所述，将虚拟机委派配置为主机安全配置文件的一部分。需要通过 VirtualCenter 或直接在 ESX Server 3 主机上运行的 VI Client 配置安全配置文件。

警告 更改 ESX Server 3 主机的委派用户仅为试验性操作， VMware 目前并不支持此实施。使用此功能可能导致意外的行为。

更改虚拟机委派

1 通过 ESX Server 3 主机登录 VI Client。

2 从清单面板中选择服务器。

  此服务器的硬件配置页面与 **[摘要 (Summary)]** 选项卡一起显示。

3 单击 **[进入维护模式 (Enter Maintenance Mode)]**。

4 依次单击 **[配置 (Configuration)]** 选项卡和 **[安全配置文件 (Security Profile)]**。

5 单击 **[虚拟机委派 (Virtual Machine Delegate)] > [编辑 (Edit)]** 以打开 **[虚拟机委派 (Virtual Machine Delegate)]** 对话框。

6 输入委派用户的用户名。

7 单击 **[确定 (OK)]**。

8 重新引导 ESX Server 3 主机。

重新引导主机后，就可在直接运行于 ESX Server 3 主机上的 VirtualCenter 和 VI Client 中看到委派用户设置。

12 服务控制台安全

本章提供了使用服务控制台的基本安全建议，阐述了服务控制台内置的一些安全功能。服务控制台是 ESX Server 3 的管理界面，因此其安全很关键。为了避免服务控制台遭到未经授权侵入和误用，VMware 对几个服务控制台参数、设置和活动施加了一些限制。

这些限制旨在提高 ESX Server 3 的安全级别。可以为了满足特定的配置需求而放宽这些限制，但是这样做之前，要确保在受信任的环境中工作且已经采取了足够的其他安全措施，以便保护整个网络和连接到 ESX Server 3 主机的设备。

本章将讨论以下主题：

常规安全建议

评估服务控制台安全和管理服务控制台时请考虑以下建议：

- **限制用户访问。**

  为了改进安全性，可限制用户访问服务控制台，实施设置密码限制等访问安全策略，例如字符长度、密码时效限制及使用 grub 密码引导主机。

  服务控制台有特权访问 ESX Server 3 的某些领域。因此，应仅向受信任的用户提供登录访问权。默认情况下，系统通过禁止以超级用户身份进行安全壳 (SSH) 登录来限制根访问，且强烈建议您保持此默认设置。应要求 ESX Server 3 系统管理员作为常规用户登录，且使用 sudo 命令来执行需要超级用户特权的特定任务。

  另外，请尝试在服务控制台上运行尽可能少的进程。理想情况下，应力争只运行必需的进程、服务和代理，例如病毒检查器、虚拟机备份等等。

- **使用 VI Client 管理 ESX Server 3 主机。**

  尽可能用 VI Client、VI Web Access 或第三方网络管理工具来管理 ESX Server 3 主机，而不是以超级用户身份通过命令行界面工作。使用 VI Client 可限制有服务控制台访问权的帐户，安全地委派职责，并设置角色以防止管理员和用户使用不必要的功能。

- **仅使用 VMware 源来升级在服务控制台上运行的 ESX Server 3 组件。**

  服务控制台运行各种第三方软件包 （例如 Tomcat Web 服务）来支持管理界面或需要执行的任务。 VMware 不支持从 VMware 源以外的任何其他源升级这些软件包。如果使用来自另一个源的下载文件或修补程序，就可能危及服务控制台的安全或功能。定期查看第三方供应商站点和 VMware 知识库，以获知安全警示。

登录服务控制台

尽管您是通过 VI Client 执行大多数 ESX Server 3 配置活动，但在配置某些安全功能时也需使用服务控制台命令行界面。使用命令行界面需登录主机。如果具有 ESX Server 3 主机的直接访问权，可登录这台计算机上的物理控制台。为此，请按 Alt+F2 打开登录页面。对于远程连接，可使用 SSH 或其他远程控制台连接在主机上开始会话。

不管是从本地还是通过 SSH 等远程连接访问服务控制台，均必须使用 ESX Server 3 主机可识别的用户名和密码登录。有关 ESX Server 3 主机的用户名和密码的信息，请参见“处理 ESX Server 3 主机上的用户和组”（第 195 页）。

如果登录主机后要执行需根特权的活动，则应作为可识别的用户登录服务控制台并通过 su 命令 （最好是 sudo 命令）获得根特权。 sudo 命令可增强安全性，因为该命令仅向选定活动授予根特权，相比而言， su 命令则向所有活动授予根特权。使用 sudo 还将提

供详细说明，因为所有 sudo 活动都会记录下来，而如果使用 su， ESX Server 3 仅记录用户通过 su 的方式切换为根这一事实。

除了特定于 ESX 的命令外，还可以使用服务控制台命令行界面执行许多 Linux 和 Unix 命令。有关服务控制台命令的详细使用说明，可使用 man <command_name> 命令查看手册页。

服务控制台防火墙配置

ESX Server 3 在服务控制台和网络之间设有防火墙。为了确保服务控制台的完整性，VMware 已经减少了默认情况下打开的防火墙端口数目。安装时，服务控制台防火墙配置为阻止除端口 902、80、443 和 22 流量之外的所有输入和出站流量，这四个端口用于与 ESX Server 3 进行基本通信。此设置确保了 ESX Server 3 主机的高安全级别。

注意 此防火墙还允许 Internet 控制消息协议 (ICMP) ping 及与 DHCP 和 DNS （仅 UDP）客户端的通信。

在受信任的环境中，您可能认为可以接受较低的安全级别。此时，可将防火墙设置为中等安全或低安全级别：

- **中等安全级别** - 除了默认端口 （902、 433、 80 和 22）以及明确打开的任何端口外，阻止其他所有入站流量。不阻止出站流量。
- **低安全级别** - 不阻止入站或出站流量。该设置等同于移除防火墙。

由于默认情况下打开的端口受到严格的限制，因此安装之后可能需要打开其他端口。有关可能需要打开的常用端口列表，请参见 “用于管理访问的 TCP 和 UDP 端口”（第 166 页）。

当添加有效操作 ESX Server 3 所需的支持服务和管理代理时，需要打开服务控制台防火墙中的其他端口。您可以通过 VirtualCenter 添加服务和管理代理，如 “为支持的服务和管理代理打开防火墙端口”（第 171 页）中所述。

除了为这些服务和代理打开的端口之外，当配置某些设备、服务或代理 （如存储设备、备份代理和管理代理等）时也可能需要打开其他端口。例如，如果正将 Veritas NetBackup™ 4.5 用作备份代理，则需要打开端口 13720、 13724、 13782 和 13783，NetBackup 将这些端口用于客户端媒体事务、数据库备份、用户备份或恢复等。若要确定要打开哪些端口，请参见设备、服务或代理的供应商规范。

更改服务控制台安全级别

更改服务控制台的安全级别的过程分为两步：确定服务控制台防火墙安全级别和重置服务控制台防火墙设置。为了避免不必要的步骤，请始终在更改防火墙设置之前对其进行检查。

每次降低安全设置或打开其他端口时，都会提高网络中的入侵风险。应在访问需求和网络安全控制程度之间寻求平衡。

确定服务控制台防火墙安全级别

1 登录服务控制台并获取超级用户特权。

2 执行以下两条命令，以确定目前是阻止还是允许入站和出站流量：

```
esxcfg-firewall -q incoming
esxcfg-firewall -q outgoing
```

3 按如下方式解释结果：

表 12-1 服务控制台安全级别

命令行响应	安全级别
默认情况下阻止入站端口。 默认情况下阻止出站端口。	高
默认情况下阻止入站端口。 默认情况下不阻止出站端口。	中等
默认情况下不阻止入站端口。 默认情况下不阻止出站端口。	低

设置服务控制台防火墙安全级别

1 登录服务控制台并获取超级用户特权。

2 根据需要执行以下命令之一：

- 将服务控制台防火墙设置为中等安全级别：

  ```
  esxcfg-firewall --allowOutgoing --blockIncoming
  ```

- 将虚拟防火墙设置为低安全级别：

  ```
  esxcfg-firewall --allowIncoming --allowOutgoing
  ```

小心 使用上述命令将禁用所有防火墙保护。

- 将服务控制台防火墙还原为高安全级别：

  ```
  esxcfg-firewall --blockIncoming --blockOutgoing
  ```

3 执行下列命令可重新启动 vmware-hostd 进程：

```
service mgmt-vmware restart
```

更改服务控制台防火墙安全级别不会影响现有连接。例如，如果防火墙设置为低安全级别且有备份运行在未明确打开的端口上，则将防火墙设置提升为高安全级别不会终止此备份。相反，由于防火墙配置为可针对先前建立的连接传递数据包，因此备份将完成，然后释放此连接，且此端口不再接受任何其他连接。

打开和关闭服务控制台防火墙中端口

安装第三方设备、服务和代理时，可以打开服务控制台防火墙端口。打开端口以支持正安装的项目之前，请参见供应商规范以确定必需的端口。

如果关闭一个端口，则关闭该端口时，不会自动断开与该端口关联的服务的活动会话。例如，如果正在执行备份而您关闭了备份代理的端口，则备份将继续，直到备份完成及代理释放连接。

只有当您为不能通过 VI Client 明确配置的服务或代理打开或关闭端口时，才执行下列程序。有关在 VirtualCenter 中配置其他端口的信息，请参见 “为支持的服务和管理代理打开防火墙端口”（第 171 页）。

小心 VMware 支持仅通过 VI Client 或 esxcfg-firewall 命令打开和关闭防火墙端口，如下所述。使用任何其他方法或脚本打开和关闭防火墙端口可能会导致意外行为。

打开服务控制台防火墙中的特定端口

1 登录服务控制台并获取超级用户特权。

2 执行下列命令：

```
esxcfg-firewall --openPort <prot number>,tcp|udp,in|out,<prot name>
```

其中：

- 端口号是供应商指定的端口号。
- tcp|udp 是协议。为 TCP 流量选择 tcp，为 UDP 流量选择 udp。
- in|out 是流量方向。选择 in 为入站流量打开端口，选择 out 为出站流量打开端口。
- 端口名称是描述性名称。该名称不必唯一，但是应有意义，帮助标识使用端口的服务或代理。

例如：

```
esxcfg-firewall --openPort 6380,tcp,in,Navisphere
```

3 执行下列命令可重新启动 vmware-hostd 进程：

```
service mgmt-vmware restart
```

关闭服务控制台防火墙中的特定端口

1 登录服务控制台并获取超级用户特权。

2 执行下列命令：

```
esxcfg-firewall -closePort <port_number>,tcp|udp,in|out,<port name>
```

端口名称参数对 -closePort 是可选的。

例如：

```
esxcfg-firewall --closePort 6380,tcp,in
```

3 执行下列命令可重新启动 vmware-hostd 进程：

```
service mgmt-vmware restart
```

使用 -closePort 选项只能关闭用 -openPort 选项打开的端口。如果使用了不同方法打开端口，则需使用等效方法关闭该端口。例如，只能通过在 VI Client 中禁用 SSH 服务器输入连接和 SSH 客户端传输连接来关闭 SSH 端口 (22)。有关通过 VI Client 打开和关闭端口的信息，请参见 “为支持的服务和管理代理打开防火墙端口”（第 171 页）。

密码限制

攻击者可以登录 ESX Server 3 主机的难易程度取决于是否可找到合法用户名 / 密码组合。恶意用户可以用许多方式获得密码。例如，攻击者可以探查不安全的网络流量（例如 Telnet 和 FTP 传输）以尝试成功登录。

另一种常见方法是通过运行密码生成器来破解密码。密码生成器对装载各种密码攻击非常有用，包括暴力攻击 （生成器尝试不超过某个密码长度的每个字符组合）和字典式攻击 （生成器尝试实际单词和实际单词的简单变种）。

实施管理长度、字符集和密码持续时间的限制可让密码生成器启动的攻击变得更加困难。密码越长越复杂，攻击者就越难发现密码。用户更改密码越频繁，就越难找到反复奏效的密码。

注意 在决定如何实施密码限制时，要始终考虑到人的因素。如果这些限制使得密码难以记住或强制进行频繁的密码更改，用户可能倾向于写下自己的密码，导致事与愿违。

为了避免密码数据库遭到误用， ESX Server 3 启用了密码遮蔽，以便隐藏密码哈希，使其无法访问。此外， ESX Server 3 使用 MD5 密码哈希，可提供更强的密码安全并让您将最小长度要求设置为八个字符以上。

ESX Server 3 在两个级别上提供密码控制，以帮助实施针对用户的密码策略并限制密码破解风险：

- **密码时效** - 这些控制措施可规定用户密码处于活动状态多长时间后即需用户进行更改。这可帮助确保用户频繁更改密码，致使攻击者即使通过探查或社会工程获得了密码，也不能无限期地访问 ESX Server 3。
- **密码复杂度** - 这些控制措施确保用户选择密码生成器难以确定的密码。

密码时效

为了确保密码不会长期保持活动状态， ESX Server 3 默认情况下对用户登录施加了下列密码时效限制：

- **最大天数** - 用户在需要更改密码之前可以保持密码的天数。 ESX Server 3 的默认设置为 90 天。默认情况下， `root` 帐户和其他服务帐户可免除 90 天到期的限制。
- **最小天数** - 两次密码更改之间相隔的最小天数。默认设置为 0，意味着用户可以随时更改其密码。
- **警告时间** - ESX Server 3 注意到密码到期之前预先发出密码更改提醒的天数。默认设置为七天。只有直接登录服务控制台或使用 SSH 时才会显示警告。

通过执行 `esxcfg-auth` 命令选项可以相应调整上述任何设置。若要对个别用户重写默认密码时效设置，可使用 `chage` 命令。

更改 ESX Server 3 的默认密码时效限制

1 登录服务控制台并获取超级用户特权。

2 根据需要执行以下一条或多条命令。

- 更改用户可以保持密码的最大天数：

  ```
  esxcfg-auth --passmaxdays=<days>
  ```

  其中， `<days>` 是密码到期之前的最大天数。

- 更改两次密码更改之间相隔的最小天数：

  ```
  esxcfg-auth --passmindays=<days>
  ```

  其中， `<days>` 是两次密码更改之间相隔的最小天数。

- 更改密码更改之前的警告时间：

  ```
  esxcfg-auth --passwarnage=<days>
  ```

  其中， `<days>` 是密码更改到期之前用户预先收到警告的天数。

重写个别用户或组的默认密码时效限制

1 登录服务控制台并获取超级用户特权。

2 根据需要执行以下一条或多条命令：

- 指定新的天数最大值：

  ```
  chage –M <days> <username>
  ```

- 指定新的天数的最小值：

  ```
  chage –m <days> <username>
  ```

- 指定新的警告时间值：

  ```
  chage –W <days> <username>
  ```

  若要了解其他 chage 选项，可使用 man chage 命令。

密码复杂度

默认情况下， ESX Server 3 使用 pam_cracklib.so 插件来设置用户创建密码时必须遵守的规则并在创建过程中检查密码强度。

pam_cracklib.so 插件可让您确定所有密码必须达到的基本标准。默认情况下， ESX Server 3 不对根密码施加任何限制。但是，当非超级用户尝试更改密码时，所选择的密码必须符合 pam_cracklib.so 设定的基本标准。此外，非超级用户只能尝试特定次数的密码更改，此后 pam_cracklib.so 将开始发出消息并最终关闭密码更改页面。 ESX Server 3 对 pam_cracklib.so 密码标准和重试限制的默认设置如下：

- **最小长度** - ESX Server 3 系统的 pam_cracklib.so 最小长度参数设置为 9。这意味着如果用户仅使用一个字符类别 （小写、大写、数字或其他），则必须输入至少八个字符。

  如果用户输入字符类别的组合，则密码长度算法允许更短的密码。为了计算用户为针对给定最小长度设置形成有效密码而需输入的实际字符长度，按如下方式应用密码长度算法：

  M - CC = E

  其中：

  - M 是最小长度参数。
  - CC 是用户在密码中包括的字符类别数。
  - E 是用户必须输入的字符数。

表 12-2 显示假定用户至少输入一个小写字符作为密码一部分时此算法的运作方式。 pam_cracklib.so 插件不允许密码少于 6 个字符。因此，尽管从算术角度而言，对于由 4 种字符组成的密码，其准确的字符要求是 5 个字符，但有效的要求是 6 个字符。

表 12-2 密码复杂度算法结果

有效密码的字符数	密码尝试中的字符类型			
	小写字符	大写字符	数字	其他字符
8	是			
7	是	是		
	是		是	
	是			是
6	是	是	是	
	是	是		是
	是		是	是
5	是	是	是	是

- **重试次数** - ESX Server 3 系统的 pam_cracklib.so 重试次数参数设置为 3。如果用户未在 3 次尝试中输入足够可靠的密码， pam_cracklib.so 将关闭密码更改对话框。用户必须打开新的密码更改会话重试。

pam_cracklib.so 插件会检查所有密码更改尝试以确保密码满足下列强度标准：

- 新密码不得是回文，即密码字符围绕某个中心字母互相对称，例如 radar 或 civic。
- 新密码不得是旧密码的逆序。
- 新密码不得通过旋转形成，即旧密码的一种变体，将旧密码的一个或多个字符旋转到密码字符串的前面或后面。
- 新密码与旧密码的差异不能只是更改了大小写。
- 新密码必须与旧密码的区别不能只是几个字符不同。
- 新密码不得在过去已经用过。只有在配置了密码重用规则的情况下，pam_cracklib.so 插件才会应用此标准。

  默认情况下， ESX Server 3 不强制实施任何密码重用规则，因此 pam_cracklib.so 插件通常决不会以这些理由拒绝密码更改尝试。但是，您可以配置重用规则以确保用户不是轮流使用几个密码。

  如果配置重用规则，旧密码会存储到 pam_cracklib.so 插件在每次密码更改尝试期间引用的文件内。重用规则将确定 ESX Server 3 保留的旧密码数目。当用户创建

的密码达到了重用规则指定的值时，旧密码将按照新旧顺序从文件中移除。若要了解如何配置重用规则，请参见 “配置密码重用规则”（第 218 页）。

- 新密码必须具有足够的长度和复杂度。通过用 esxcfg-auth 命令更改 pam_cracklib.so 复杂度参数可配置这些要求，此命令可让您设置重试次数、最小密码长度和各种字符信用。字符信用可让用户在密码中包括更多字符类型时输入更短的密码。若要了解如何配置密码长度和复杂度，请参见 “更改 pam_cracklib.so 插件的默认密码复杂度”（第 219 页）。

有关 pam_cracklib.so 插件的更多信息，请参见 Linux 文档。

注意 用于 Linux 的 pam_cracklib.so 插件提供的参数多于 ESX Server 3 支持的参数。您无法在 esxcfg-auth 中指定这些额外参数。

配置密码重用规则

1 登录服务控制台并获取超级用户特权。

2 通过在命令提示符中输入 cd /etc/pam.d/ 更改目录。

3 使用文本编辑器来打开 system-auth 文件。

4 查找以下列字符开头的行：

```
password    sufficient    /lib/security/$ISA/pam_unix.so
```

5 将下列参数添加到行尾：

```
remember=X
```

其中 X 是为每个用户存储的旧密码数。在 remember=X 和前面的参数之间使用空格作为分隔符。

6 保存更改并关闭文件。

7 将目录更改为 /etc/security/，并发出以下命令生成文件名为 opasswd 的零长度文件：

```
touch opasswd
```

8 输入下列命令：

```
chmod 0600 opasswd
chown root:root /etc/security/opasswd
```

更改 pam_cracklib.so 插件的默认密码复杂度

1 登录服务控制台并获取超级用户特权。

2 输入下列命令：

```
esxcfg-auth --usecrack=<retries> <minimum length> <le_credit> <un_credit>
<d_credit> <oc_credit>
```

其中：

- 重试是 ESX Server 3 对用户锁定密码更改模式之前允许用户重试的次数。
- 最小长度是用户为形成可接受密码必须输入的最少字符数。该数值是应用任何长度信用之前的总长度。

  更改密码时始终会应用一个长度信用，因此密码长度实际上比指定的最小长度参数少一个字符。由于 pam_cracklib.so 插件不接受少于六个字符的密码，因此计算最小长度参数时应使用户无法通过减去长度信用将密码长度减至六以下。
- 小写字符信用是用户在密码中至少包括一个小写字符时最小长度参数要减少的数值。
- 大写字符信用是用户在密码中至少包括一个大写字符时最小长度参数要减少的数值。
- 数字字符是用户在密码中至少包括一个数字时最小长度参数要减少的数值。
- 其他字符信用是用户在密码中至少包括一个特殊字符时最小长度参数要减少的数值，例如下划线或短划线。

可将字符信用参数输入为正数，如果不希望插件为包括这种字符提供用户信用，可将其输入为零 (0)。字符信用是可以叠加的。用户输入的字符的不同类型越多，形成有效密码所需的字符就越少。例如，您发出以下命令：

```
esxcfg-auth --usecrack=3 11 1 1 1 2
```

实行此设置时，如果用户创建一个包含小写字符和一个下划线的密码，将需要八个字符才能创建有效密码。如果用户决定包括所有类型的字符 （小写、大写、数字和特殊字符），则只需要六个字符。

更改密码插件

pam_cracklib.so 插件可对大多数环境实施足够的密码强度。但是，如果 pam_cracklib.so 插件的严格程度不足以满足需求，可以改用 pam_passwdqc.so 插件。可以通过 esxcfg-auth 命令来更改插件。

pam_passwdqc.so 插件与 pam_cracklib.so 插件测试相同的密码特性。但是此插件提供了用于微调密码强度的更多选项，且为包括超级用户在内的所有用户执行密码强度测试。 pam_passwdqc.so 插件的使用方法也比 pam_cracklib.so 插件略为复杂。有关此插件的更多信息，请参见 Linux 文档。

注意 用于 Linux 的 pam_passwdqc.so 插件提供的参数多于 ESX Server 3 支持的参数。您无法在 esxcfg-auth 中指定这些额外参数。

切换为 pam_passwdqc.so 插件

1 登录服务控制台并获取超级用户特权。

2 输入下列命令：

```
esxcfg-auth --usepamqc=<N0> <N1> <N2> <N3> <N4> <match>
```

其中：

- N0 是仅使用一种字符时密码所需的字符数。
- N1 是使用两种字符时密码所需的字符数。
- N2 用于密码短语。 ESX Server 3 要求密码短语由三个单词组成。
- N3 是使用三种字符时密码所需的字符数。
- N4 是使用全部四种字符时密码所需的字符数。
- 匹配是允许从旧密码中重用的字符串的字符数。如果 pam_passwdqc.so 插件找到此长度或更长的重用字符串，将认定此字符串无法通过强度测试并仅使用剩余的字符。

将上述任何选项设置为 -1 可指示 pam_passwdqc.so 插件忽略此要求。将上述任何选项设置为 disabled 可指示 pam_passwdqc.so 插件认定具有关联特性的密码不符合要求。除 -1 和 disabled 之外，使用的这些值必须是递减顺序。

例如，您发出以下命令：

```
esxcfg-auth --usepamqc=disabled 18 -1 12 8
```

如果实行此设置，用户创建密码时不能设置仅包含一种字符的密码。用户需要对两种字符组成的密码使用至少 18 个字符，对三种字符组成的密码使用至少 12 个字符，对四种字符组成的密码使用至少 8 个字符。创建密码短语的尝试将被忽略。

密码强度

通过不安全的连接传输数据会带来安全风险，因为数据通过网络传输时，恶意用户可能会扫描这些数据。作为一项安全措施，网络组件通常对数据加密，以防止他人轻松读取这些数据。为了加密数据，发送组件（如网关或重定向程序）会应用算法或*密码*在传输数据之前改变这些数据。接收组件使用密钥解密这些数据，将其还原为原始形式。

目前有几种不同的常用密码，每种密码提供的安全级别也有所差异。密码保护数据的能力的一种衡量方法是其*密码强度*，即加密密钥的位数。位数越大，密码越安全。

为了确保对外部网络连接之间的数据传输进行保护，ESX Server 3 采用了目前可用的最强大的块密码之一，即 256 位 AES 块加密。ESX Server 3 还将 1024 位 RSA 用于密钥交换。这些加密算法默认用于下列连接：

- VI Client 通过服务控制台与 VirtualCenter Server 和 ESX Server 3 主机的连接。
- VI Web Access 通过服务控制台与 ESX Server 3 主机的连接。

  注意 由于 VI Web Access 的密码使用情况由正使用的 Web 浏览器决定，因此该管理工具可能使用其他密码。

- SDK 与 VirtualCenter Server 和 ESX Server 3 的连接。
- 服务控制台通过 VMkernel 与虚拟机的连接。
- SSH 通过服务控制台与 ESX Server 3 主机的连接。有关详细信息，请参见“SSH 安全”（第 225 页）。

setuid 和 setgid 应用程序

`setuid` 标记允许应用程序通过将有效用户 ID 设置为程序所有者用户 ID 以临时更改运行应用程序的用户的权限。`setgid` 标记允许应用程序将有效组 ID 设置为程序所有者的组 ID 以临时更改运行应用程序的组的权限。

ESX Server 3 安装期间，默认情况下将安装若干包括 `setuid` 和 `setgid` 标记的应用程序。这些应用程序通过服务控制台启动。其中一些应用程序提供了正确运行 ESX Server 3 主机所需的设施。另一些则是可选的，但是它们可以简化 ESX Server 3 主机和网络的维护和故障排除。

默认 setuid 应用程序

表 12-3 列出了默认的 setuid 应用程序，并指示应用程序是必需的还是可选的。

表 12-3 默认 setuid 应用程序

应用程序	用途和路径	必需或可选
crontab	允许个别用户添加 cron 作业。 **路径**：/usr/bin/crontab	可选
pam_timestamp_check	支持密码身份验证。 **路径**：/sbin/pam_timestamp_check	必需
passwd	支持密码身份验证。 **路径**：/usr/bin/passwd	必需
ping	发送和侦听网络接口上的控制数据包。可用于调试网络。 **路径**：/bin/ping	可选
pwdb_chkpwd	支持密码身份验证。 **路径**：/sbin/pwdb_chkpwd	必需
ssh-keysign	对 SSH 执行基于主机的身份验证。 **路径**：/usr/libexec/openssh/ssh-keysign	如果使用基于主机的身份验证，则为必需。 否则为可选。
su	通过更改用户让普通用户成为根用户。 **路径**：/bin/su	必需
sudo	仅针对特定操作让普通用户充当根用户。 **路径**：/usr/bin/sudo	可选
unix_chkpwd	支持密码身份验证。 **路径**：/sbin/unix_chkpwd	必需
vmkload_app	执行运行虚拟机所需的任务。该应用程序安装在两个位置中：一个用于标准用途，一个用于调试。 **标准用途的路径**： /usr/lib/vmware/bin/vmkload_app **调试的路径**： /usr/lib/vmware/bin-debug/vmkload_app	两个路径均为必需

表 12-3 默认 setuid 应用程序 （续）

应用程序	用途和路径	必需或可选
vmware-authd	对使用 VMware 特定服务的用户进行身份验证。 **路径**：/usr/sbin/vmware-authd	必需
vmware-vmx	执行运行虚拟机所需的任务。该应用程序安装在两个位置中：一个用于标准用途，一个用于调试。 **标准用途的路径**：/usr/lib/vmware/bin/vmware-vmx **调试的路径**：/usr/lib/vmware/bin-debug/vmware-vmk	两个路径均为必需

禁用任何必需的应用程序都将使 ESX Server 3 身份验证和虚拟机运行出现问题，但您可以禁用任何可选应用程序。

禁用可选的 setuid 应用程序

1 登录服务控制台并获取超级用户特权。

2 执行下列命令：

```
chmod a-s <path_to_executable>
```

默认 setgid 应用程序

默认情况下将安装两个包括 setgid 标记的应用程序。表 12-4 列出了默认的 setgid 应用程序，并指示应用程序是必需的还是可选的。

表 12-4 默认 setgid 应用程序

应用程序	用途和路径	必需或可选
wall	提醒所有终端某个操作即将发生。该应用程序由 shutdown 和其他命令调用。 **路径**：/usr/bin/wall	可选
lockfile	执行 Dell OM 管理代理的锁定。 **路径**：/usr/bin/lockfile	对于 Dell OM 是必需的，否则是可选的

禁用必需的应用程序将使 ESX Server 3 身份验证和虚拟机运行出现问题，但您可以禁用任何可选应用程序。

禁用可选的 setgid 应用程序

1 登录服务控制台并获取超级用户特权。

2 执行下列命令：

```
chmod a-g <path_to_executable>
```

SSH 安全

SSH 是常用的 UNIX 和 Linux 命令 shell，可让您远程登录服务控制台并为 ESX Server 3 执行某些管理和配置任务。SSH 用于安全登录和数据传输，因为它可提供比其他命令 shell 更强大的保护。在此 ESX Server 3 版本中， SSH 配置得到了增强，能够提供更高的安全级别。此次增强的关键功能包括：

- **禁用第 1 版 SSH 协议** - VMware 不再支持第 1 版 SSH 协议，而是以独占方式使用第 2 版协议。第 2 版消除了第 1 版中存在的某些安全问题，且提供了更安全的与服务控制台相连的通信接口。
- **提高了加密强度** - SSH 目前对连接仅支持 256 位和 128 位 AES 密码。
- **限制以超级用户进行远程登录** - 不能再以超级用户远程登录，而是以可识别的用户登录，并使用 `sudo` 命令执行需要超级用户特权的特定操作，或输入 `su` 命令成为根用户。

注意 `sudo` 命令具有安全优势，因为它可限制根活动，并通过对用户执行的任何根活动生成审核记录来帮助您检查可能存在的根特权误用情况。

这些设置旨在为通过 SSH 传输到服务控制台的数据提供可靠保护。如果此配置对您的需求而言过于严格，可以降低安全参数。

更改默认的 SSH 配置

1 登录服务控制台并获取超级用户特权。

2 通过在命令提示符中输入 **`cd /etc/ssh`** 更改目录。

3 根据需要使用文本编辑器来执行以下任意或全部操作。

- 若要允许远程根登录，可在 `sshd_config` 文件的下列行中将设置更改为 `yes`：

  ```
  PermitRootLogin no
  ```

- 若要恢复为默认 SSH 协议 （第 1 版和第 2 版），可在 `sshd_config` 文件中注释掉以下行：

  ```
  Protocol 2
  ```

- 若要恢复为 3DES 密码或其他密码，可在 `sshd_config` 文件中注释掉以下行：

  ```
  Ciphers aes256-cbc,aes128-cbc
  ```

- 若要禁用 SSH 上的安全 FTP (SFTP)，可在 `sshd_config` 文件中注释掉以下行：

  ```
  Subsystem ftp /usr/libexec/openssh/sftp-server
  ```

4 保存更改并关闭文件。

5 执行下列命令可重新启动 SSHD 服务：

```
service sshd restart
```

安全修补程序和安全漏洞扫描软件

如果 VMware 将某个支持 LINUX 的软件包作为服务控制台组件 （例如服务、设施或协议）提供，而目前有该软件包的修补程序可用， VMware 将提供 ″RPM 软件包管理器 (RPM)″ 包，用于在 ESX Server 3 上更新该软件包。尽管可以从其他源获得这些修补程序，但请始终使用 VMware 生成的 RPM，而不是使用第三方 RPM。

当向软件包提供修补程序时， VMware 的策略是将此修补程序反向移植到已知为稳定的软件版本中。这种方法减少了在软件中引发新问题和不稳定性的几率。因为修补程序是添加到现有版本的软件中，因此软件的版本号保持不变，但会添加修补程序编号作为后缀。

某些安全扫描程序 （如 Nessus）在搜索安全漏洞时会检查版本号，但不检查修补程序后缀。因此，这些扫描程序可能误报软件安全级别低且没有包括最新的安全修补程序（即使已经包括）。此问题在业界较常见，不是 VMware 特有的。

注意 一些安全扫描程序能够正确处理这种情形，但通常滞后一个版本或多个版本。例如， Red Hat 修补程序之后发布的 Nessus 版本通常不会报告这些错误情况。

以下举例说明了此问题是如何出现的：

1 您最初安装了含 OpenSSL 0.9.7a 版本 （其中 0.9.7a 是不含修补程序的原始版本）的 ESX Server 3。

2 OpenSSL 发布了修复 0.9.7 版本中安全漏洞的修补程序。此版本称为 0.9.7x。

3 VMware 将 OpenSSL 0.9.7x 修补程序反向移植到原始版本，更新修补程序编号，并创建 RPM。 RPM 中的 OpenSSL 版本为 0.9.7a-1，表示原始版本 (0.9.7a) 现在包含第 1 个修补程序。

4 您安装 RPM。

5 安全扫描程序未能注意到 -1 后缀，误报 OpenSSL 的安全级别不是最新的。

如果扫描程序报告软件包的安全级别较低，请执行以下检查：

- 查看修补程序后缀以确定是否需要进行更新。

- 阅读 VMware RPM 文档，了解有关修补程序内容的信息。
- 使用以下命令从 RPM 更改日志的安全警示中查找通用漏洞披露 (CVE) 号：

  ```
  rpm– q ––changelog openssl | grep <CVE_number>
  ```

  如果存在此 CVE 号，则指定的软件包将修补该漏洞。

13 安全部署与建议

本章重点讲述如何确保 ESX Server 3 在特定环境中的安全，在讲解时会提出一系列 ESX Server 3 部署方案，供您在规划部署的某些安全功能时参考。本章还提出了若干基本的安全建议，供您在创建和配置虚拟机时参考。

本章包括以下主题：

常用 ESX Server 3 部署的安全措施

根据公司规模、数据及资源与外界共享的方式、有多个数据中心还是只有一个数据中心等因素， ESX Server 3 部署的复杂度会有极大差异。

以下部署的实质在于用户访问、资源共享及安全级别的策略。通过对比这些部署，您可以了解在规划 ESX Server 3 部署安全时需面临的问题。

单客户部署

在此类部署中， ESX Server 3 主机由一家公司拥有并在一个数据中心进行维护。 ESX Server 3 资源不与外部用户共享。 ESX Server 3 主机由一名网站管理员维护，其上运行多台虚拟机。

此类部署不允许存在客户管理员，维护众多虚拟机的工作由网站管理员独自负责。公司配备一组不具有 ESX Server 3 主机帐户的系统管理员，他们无法访问 VirtualCenter 或主机命令行 shell 等任何 ESX Server 3 工具。这些系统管理员可以通过虚拟机控制台访问虚拟机，因此可以加载软件和执行虚拟机内部的其他维护任务。

表 13-1 显示了如何处理您为 ESX Server 3 主机配置的所用组件的共享。

表 13-1 单客户部署中的组件共享

功能	配置	备注
服务控制台与虚拟机共享同一个物理网络？	否	通过为服务控制台配置其专用物理网络来隔离服务控制台。
服务控制台与虚拟机共享同一个 VLAN？	否	通过为服务控制台配置其专用 VLAN 来隔离服务控制台。虚拟机及其他系统设施 （如 VMotion）都不应使用该 VLAN。
虚拟机共享同一个物理网络？	是	将虚拟机配置在同一个物理网络中。
网络适配器共享？	局部	通过为服务控制台配置其专用虚拟交换机和虚拟网络适配器来隔离服务控制台。虚拟机及其他系统设施都不应使用该交换机或适配器。 但是，您可以在该虚拟交换机和网络适配器上配置虚拟机。
VMFS 共享？	是	所有 `.vmdk` 文件均应驻留在同一个 VMFS 分区中。
安全级别	高	逐个打开 FTP 等所需服务的端口。有关安全级别的信息，请参见 “服务控制台防火墙配置”（第 211 页）。
虚拟机内存过量使用？	是	为虚拟机配置的总内存多于总物理内存。

表 13-2 显示了设置 ESX Server 3 主机用户帐户的方式。

表 13-2 单客户部署中的用户帐户设置

用户类别	帐户总数
网站管理员	1
客户管理员	0
系统管理员	0
商业用户	0

表 13-3 显示了每个用户的访问级别。

表 13-3 单客户部署中的用户访问

访问级别	网站管理员	系统管理员
访问根？	是	否
通过 SSH 进行服务控制台访问？	是	否
VirtualCenter 与 VI Web Access？	是	否
创建和修改虚拟机？	是	否
通过控制台进行虚拟机访问？	是	是

多客户限制部署

在此类部署中，ESX Server 3 主机位于同一个数据中心内，用于为多名客户提供应用程序。ESX Server 3 主机由一名网站管理员维护，其上运行多台客户专用的虚拟机。属于不同客户的虚拟机可以位于同一台 ESX Server 3 主机上，但网站管理员限制资源共享，以避免欺诈性交互。

虽然只有一名网站管理员，但有多名客户管理员维护分配给其客户的虚拟机。此类部署还包括一些客户系统管理员，它们没有 ESX Server 3 帐户，但可以通过虚拟机控制台访问虚拟机以加载软件和执行虚拟机内部的其他维护任务。

表 13-4 显示了如何处理您为 ESX Server 3 主机配置的所用组件的共享。

表 13-4 多客户限制部署中的组件共享

功能	配置	备注
服务控制台与虚拟机共享同一个物理网络？	否	通过为服务控制台配置其专用物理网络来隔离服务控制台。
服务控制台与虚拟机共享同一个 VLAN？	否	通过为服务控制台配置其专用 VLAN 来隔离服务控制台。虚拟机及其他系统设施 （如 VMotion）都不应使用该 VLAN。
虚拟机共享同一个物理网络？	局部	将每位客户的虚拟机放置到不同的物理网络中。所有物理网络均相互独立。
网络适配器共享？	局部	通过为服务控制台配置其专用虚拟交换机和虚拟网络适配器来隔离服务控制台。虚拟机及其他系统设施都不应使用该交换机或适配器。 将一位客户的多台虚拟机配置为可共享同一台虚拟交换机和同一块网络适配器。但是，它们不与任何其他客户共享交换机和适配器。
VMFS 共享？	否	每位客户都有自己的 VMFS 分区，而且其虚拟机的 `.vmdk` 文件以独占方式驻留于该分区。该分区可跨多个 LUN。
安全级别	高	根据需要打开 FTP 等服务的端口。
虚拟机内存过量使用？	是	为虚拟机配置的总内存多于总物理内存。

表 13-5 显示了设置 ESX Server 3 主机用户帐户的方式。

表 13-5 多客户限制部署中的用户帐户设置

用户类别	帐户总数
网站管理员	1
客户管理员	10
系统管理员	0
商业用户	0

表 13-6 显示了每个用户的访问级别。

表 13-6 多客户限制部署中的用户访问

访问级别	网站管理员	客户管理员	系统管理员
访问根？	是	否	否
通过 SSH 进行服务控制台访问？	是	是	否
VirtualCenter 与 VI Web Access？	是	是	否
创建和修改虚拟机？	是	是	否
通过控制台进行虚拟机访问？	是	是	是

多客户开放部署

在此类部署中，ESX Server 3 主机位于同一个数据中心内，用于为多名客户提供应用程序。ESX Server 3 主机由一名网站管理员维护，其上运行多台客户专用的虚拟机。属于不同客户的虚拟机可以位于同一台 ESX Server 3 主机上，但存在更少的资源共享限制。

虽然只有一名网站管理员，但有多名客户管理员维护分配给其客户的虚拟机。此类部署还包括一些客户系统管理员，它们没有 ESX Server 3 帐户，但可以通过虚拟机控制台访问虚拟机以加载软件和执行虚拟机内部的其他维护任务。最后，一组没有帐户的商业用户可以使用虚拟机运行其应用程序。

表 13-7 显示了如何处理您为 ESX Server 3 主机配置的所用组件的共享。

表 13-7 多客户开放部署中的组件共享

功能	配置	备注
服务控制台与虚拟机共享同一个物理网络？	否	通过为服务控制台配置其专用物理网络来隔离服务控制台。
服务控制台与虚拟机共享同一个 VLAN？	否	通过为服务控制台配置其专用 VLAN 来隔离服务控制台。虚拟机及其他系统设施 （如 VMotion）都不应使用该 VLAN。
虚拟机共享同一个物理网络？	是	将虚拟机配置在同一个物理网络中。
网络适配器共享？	局部	通过为服务控制台配置其专用虚拟交换机和虚拟网络适配器来隔离服务控制台。虚拟机及其他系统设施都不应使用该交换机或适配器。 但是，您可以在该虚拟交换机和网络适配器上配置所有虚拟机。
VMFS 共享？	是	虚拟机可以共享 VMFS 分区，且其虚拟机 `.vmdk` 文件可以驻留在共享分区上。虚拟机不共享 `.vmdk` 文件。

表 13-7 多客户开放部署中的组件共享 （续）

功能	配置	备注
安全级别	高	根据需要打开 FTP 等服务的端口。
虚拟机内存过量使用？	是	为虚拟机配置的总内存多于总物理内存。

表 13-8 显示了设置 ESX Server 3 主机用户帐户的方式。

表 13-8 多客户开放部署中的用户帐户设置

用户类别	帐户总数
网站管理员	1
客户管理员	10
系统管理员	0
商业用户	0

表 13-9 显示了每个用户的访问级别。

表 13-9 多客户开放部署中的用户访问

访问级别	网站管理员	客户管理员	系统管理员	商业用户
访问根？	是	否	否	否
通过 SSH 进行服务控制台访问？	是	是	否	否
VirtualCenter 与 VI Web Access？	是	是	否	否
创建和修改虚拟机？	是	是	否	否
通过控制台进行虚拟机访问？	是	是	是	是

虚拟机建议

在评估虚拟机安全和管理虚拟机时，请考虑以下安全预防措施。

安装防病毒软件

由于每台虚拟机都承载着标准操作系统，因此，应考虑安装防病毒软件，保护其免遭病毒感染。根据虚拟机的使用方式，可能还需要安装软件防火墙。

注意 软件防火墙和防病毒软件需占用大量虚拟化资源。如果确信虚拟机处于可完全信任的环境中，则可以在这两条安全措施的必要性与虚拟机的性能之间寻求平衡。

禁用客户操作系统与远程控制台之间的复制和粘贴操作

在虚拟机下运行 VMware Tools 时，可以在客户操作系统和远程控制台之间进行复制和粘贴操作。控制台窗口获得焦点时，虚拟机中运行的非特权用户和进程均可以访问虚拟机控制台的剪贴板。如果用户在使用控制台前将敏感信息复制到剪贴板中，就可能在无意中向虚拟机暴露敏感数据。

要避免该问题，可以考虑禁用客户操作系统的复制和粘贴操作。

禁用客户操作系统和远程控制台之间的复制和粘贴操作

1 登录 VI Client，从清单面板中选择虚拟机。

此时会显示该虚拟机的配置页面的 **[摘要 (Summary)]** 选项卡。

2 单击 **[编辑设置 (Edit Settings)]**。

3 单击 **[选项 (Options)]**> **[高级 (Advanced)]**> **[配置参数 (Configuration Parameters)]**，打开 **[配置参数 (Configuration Parameters)]** 对话框。

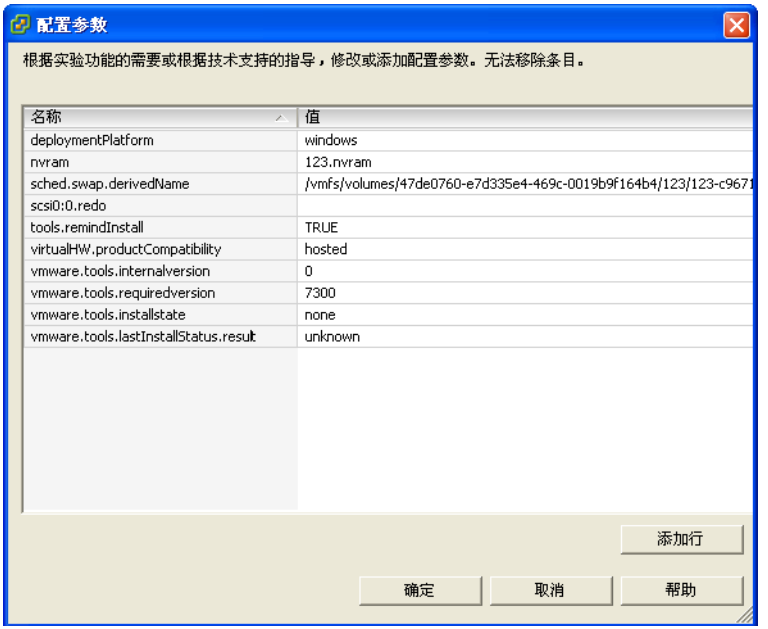
4 单击 **[添加 (Add)]** 按钮。

5 在 **[名称 (Name)]** 字段和 **[值 (Value)]** 列中键入下列值。

表 13-10 配置参数设置

名称字段	值字段
isolation.tools.copy.disable	true
isolation.tools.paste.disable	true
isolation.tools.setGUIOptions.enable	false

结果显示如下。



注意 这些选项将替代在客户操作系统的 VMware Tools 控制面板中做出的任意设置。

6 单击 **[确定 (OK)]** 关闭 **[配置参数 (Configuration Parameters)]** 对话框，然后再次单击 **[确定 (OK)]** 关闭 **[虚拟机属性 (Virtual Machine Properties)]** 对话框。

移除不必要的硬件设备

虚拟机内的非特权用户和进程可以连接或断开网络适配器和 CD-ROM 驱动器等硬件设备。攻击者可利用该能力以多种方式破坏虚拟机的安全。例如，默认情况下，可以访问虚拟机的攻击者能够：

- 连接已断开的 CD-ROM 驱动器并访问留在驱动器中的媒体上的敏感信息。
- 断开网络适配器，使虚拟机与网络隔离，造成拒绝服务故障。

作为常规安全预防措施，可以使用 [VI Client 配置 (VI Client Configuration)] 选项卡上的命令移除所有不需要或无用的硬件设备。虽然此举可提高虚拟机的安全性，但对于需要稍后恢复当前未使用的设备以提供服务的情况来说，这并非一个好的解决方案。

如果不希望永久移除设备，可以阻止虚拟机用户或进程在客户操作系统中连接或断开设备。

阻止虚拟机用户或进程断开设备

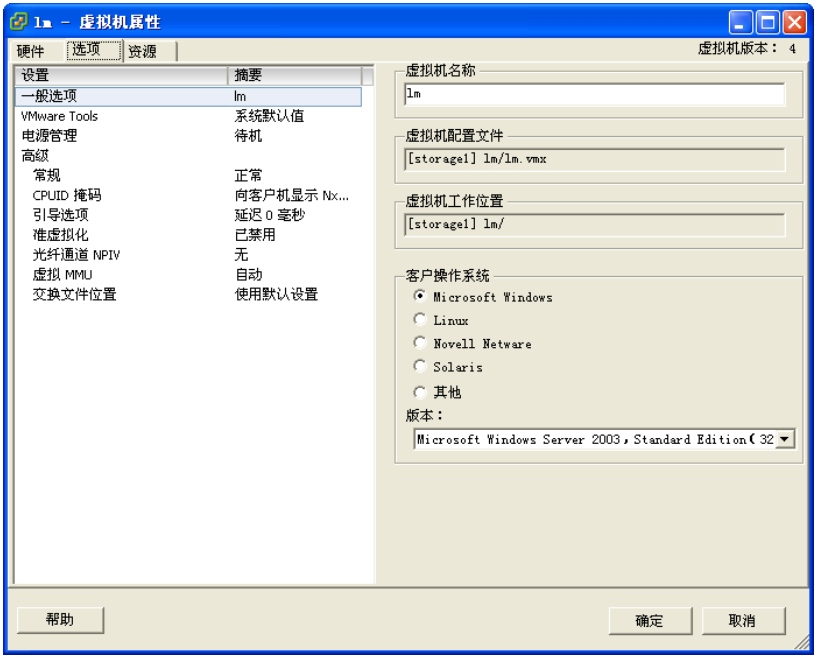
1 登录 VI Client，从清单面板中选择虚拟机。

此时会显示该虚拟机的配置页面的 **[摘要 (Summary)]** 选项卡。

2 单击 **[编辑设置 (Edit Settings)]**。

此时会显示 **[虚拟机属性 (Virtual Machine Properties)]** 对话框。

3 单击 **[选项 (Options)] >[常规 (General)]**，记下 **[虚拟机配置文件 (Virtual Machine Configuration File)]** 字段中显示的路径。



4 登录服务控制台并获取超级用户特权。

5 更改目录以访问虚拟机配置文件 （在步骤 3 中记录了其路径）。

虚拟机配置文件位于 /vmfs/volumes/<datastore> 目录中，其中，<datastore> 是虚拟机文件驻留的存储设备的名称。例如，如果从 **[虚拟机属性 (Virtual Machine Properties)]** 对话框获取的虚拟机配置文件为 [vol1]vm-finance/vm-finance.vmx，请按照以下方式更改目录：

```
cd /vmfs/volumes/vol1/vm-finance/
```

6 使用 nano 或其他文本编辑器将下面的行添加到 .vmx 文件中。

```
<device_name>.allowGuestConnectionControl = "false"
```

其中， <device_name> 为需要保护设备的名称，例如 ethernet1。

注意 默认情况下，以太网 0 配置为不允许断开设备。除非以前的管理员将 <device_name>.allowGuestConnectionControl 设置为真，否则无需更改该设置。

---

7 保存更改并关闭文件。

8 返回至 VI Client 并重启虚拟机。操作步骤为：右键单击清单面板中的虚拟机，单击 **[关闭 (Power Off)]**，然后单击 **[启动 (Power On)]**。

限制客户操作系统写入主机内存

客户操作系统进程会通过 VMware Tools 向 ESX Server 3 主机发送信息消息。这种消息叫作 `setinfo` 消息，通常包含定义虚拟机特性的名称 / 值对或主机存储的标识符，例如 `ipaddress=10.17.87.224`。

如果不限制主机存储这些消息的数据量，则无限的数据流会使攻击者有机可乘，他们可编写模仿 VMware Tools 的程序以使用任意配置数据填写主机内存，从而占用虚拟机所需的空间，发动一起 DOS 攻击。

为避免该问题，请将包含这些名称 / 值对的配置文件限制为 1 MB 大小。1 MB 大小可满足大多数使用情况，但也可以根据需要更改该值。如果向配置文件中存储的自定义信息较多，可以增加该值。

要修改 GuestInfo 内存限制，请设置 .vmx 文件的 tools.setInfo.sizeLimit 属性。默认限制为 1 MB，即使 `sizeLimit` 属性不存在，该限制仍起作用。

修改客户操作系统的变量内存限制

1 登录 VI Client，从清单面板中选择虚拟机。

此时会显示该虚拟机的配置页面的 **[摘要 (Summary)]** 选项卡。

2 单击 **[编辑设置 (Edit Settings)]**。

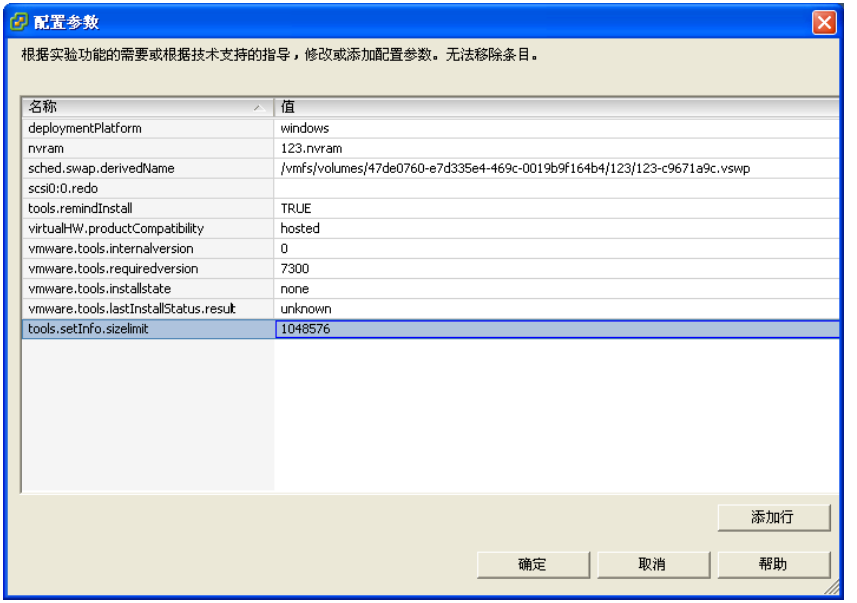
3 单击 **[选项 (Options)]> [高级 (Advanced)]> [配置参数 (Configuration Parameters)]**，打开 **[配置参数 (Configuration Parameters)]** 对话框。

4 如果大小限制属性不存在，则请单击 **[添加行 (Add Row)]** 并键入以下内容：

- **名称字段 - `tools.setInfo.sizeLimit`**
- **值字段 – `<Number of Bytes>`**

如果大小限制属性存在，请将该属性修改为所需限制。

下图所示为将 GuestInfo 大小限制为 1048576 字节 （1 MB）的配置：



5 单击 **[确定 (OK)]** 关闭 **[配置参数 (Configuration Parameters)]** 对话框，然后再次单击 **[确定 (OK)]** 关闭 **[虚拟机属性 (Virtual Machine Properties)]** 对话框。

您也可选择完全阻止客户操作系统将任何名称 / 值对写入配置文件。该选择适合必须阻止客户操作系统修改配置设置的情况。

阻止客户操作系统进程向主机发送配置消息

1 登录 VI Client，从清单面板中选择虚拟机。

此时会显示该虚拟机的配置页面的 **[摘要 (Summary)]** 选项卡。

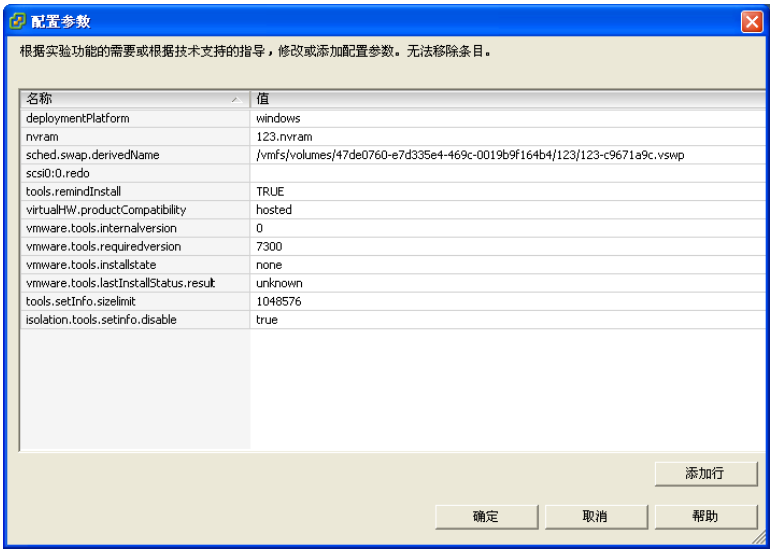
2 单击 **[编辑设置 (Edit Settings)]**。

3 单击 **[选项 (Options)]**> **[高级 (Advanced)]**> **[配置参数 (Configuration Parameters)]**，打开 **[配置参数 (Configuration Parameters)]** 对话框。

4 单击 **[添加 (Add)]** 按钮并键入以下内容：

- **名称字段 - `isolation.tools.setinfo.disable`**
- **值字段 - `true`**

结果显示如下。



5 单击 **[确定 (OK)]** 关闭 **[配置参数 (Configuration Parameters)]** 对话框，然后再次单击 **[确定 (OK)]** 关闭 **[虚拟机属性 (Virtual Machine Properties)]** 对话框。

配置客户操作系统的日志记录级别

虚拟机可以将故障排除信息写入存储在 VMFS 卷上的虚拟机日志文件中。虚拟机用户和进程可能会有意或无意地误用日志记录，导致大量数据淹没日志记录文件。随时间的推移，日志文件会占用大量的文件系统空间，造成拒绝服务故障。

为避免该问题，请考虑修改虚拟机客户操作系统的日志记录设置。这些设置可以限制日志文件的总大小和数量。通常，主机会在每次重启时创建新的日志文件，因此，文件会变得非常大，但可以通过限制日志文件大小的上限来确保更频繁地创建新日志文件。如果要限制日志记录数据的总大小，VMware 建议保存 10 个日志文件，每个文件限制为 100 KB。这样大小的日志文件不会占用过量的主机磁盘空间，而存储的数据量又足以捕捉到调试可能出现的大多数问题的充足信息。

客户操作系统会在每次向日志写入条目时检查日志的大小，如果大小超出限制，则将下一个条目写入到新日志中。如果已经存在最大数量的日志文件，则在创建新日志时删除最旧的日志。通过写入超大的日志条目可以尝试发动避免这些限制的拒绝服务攻击，但由于每个日志条目的大小限制在 4 KB 以下，因此，日志文件的大小不会比配置限制大 4 KB 以上。

限制日志文件的数量和大小

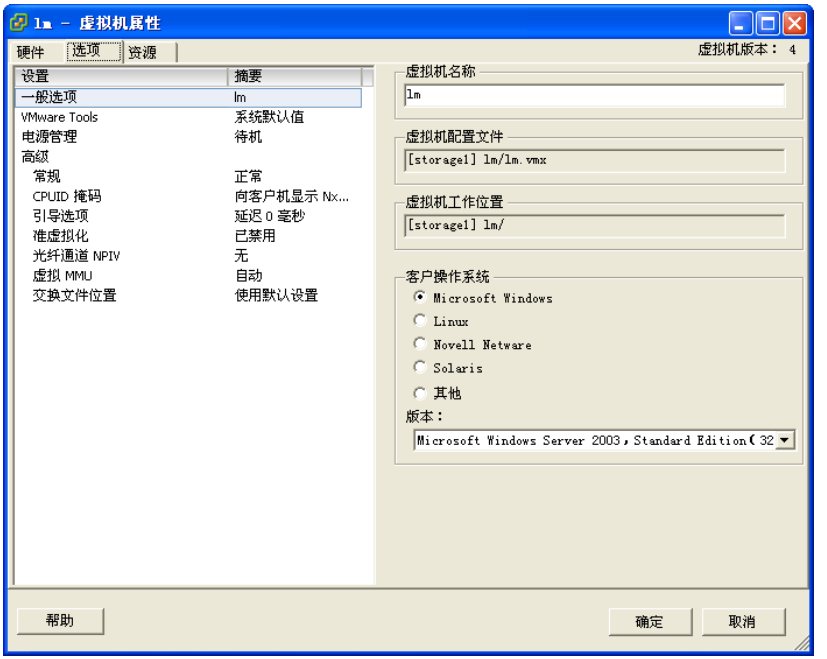
1 登录 VI Client，从清单面板中选择虚拟机。

此时会显示该虚拟机的配置页面的 **[摘要 (Summary)]** 选项卡。

2 单击 **[编辑设置 (Edit)]**。

此时会显示 [虚拟机属性 (Virtual Machine Properties)] 对话框。

3 单击 **[选项 (Options)]**> **[常规 (General)]**，记下 **[虚拟机配置文件 (Virtual Machine Configuration File)]** 字段中显示的路径。



4 登录服务控制台并获取超级用户特权。

5 更改目录以访问虚拟机配置文件 （在步骤 3 中记录了其路径）。

虚拟机配置文件位于 `/vmfs/volumes/<datastore>` 目录中，其中，`<datastore>` 是虚拟机文件驻留的存储设备的名称。例如，如果从 **[虚拟机属性 (Virtual Machine Properties)]** 对话框获取的虚拟机配置文件为 `[vol1]vm-finance/vm-finance.vmx`，请按照以下方式更改目录：

```
cd /vmfs/volumes/vol1/vm-finance/
```

6 要限制日志大小，请使用 nano 或其他文本编辑器在 `.vmx` 文件中添加或编辑下面的行。

```
log.rotateSize=<maximum size>
```

其中，`<maximum size>` 是文件大小的上限 （以字节为单位）。例如，要将大小限制为
100 KB 左右，可以输入 **`100000`**。

7 要保留限制数量的日志文件，请使用 nano 或其他文本编辑器在 `.vmx` 文件中添加或编辑下面的行。

```
log.keepOld=<number of files to keep>
```

其中，`<number of files to keep>` 是服务器保留的文件数量。例如，要保留 10 个日志文件 （达到 10 个文件后，在创建新文件时删除最旧的文件），可以输入 **`10`**。

也可以完全停止日志记录。请注意，如果做出该决定，可能无法收集充足的日志，以进行故障排除。而且，如果在禁用日志后出现虚拟机问题， VMware 不提供技术支持。

禁用客户操作系统的日志记录

1 登录 VI Client，从清单面板中选择虚拟机。

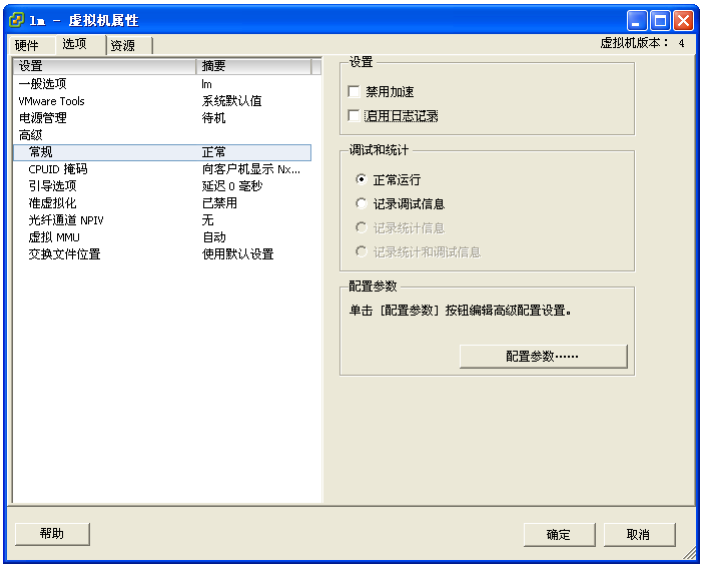
此时会显示该虚拟机的配置页面的 **[摘要 (Summary)]** 选项卡。

2 单击 **[编辑设置 (Edit Settings)]**。

3 单击 **[选项 (Options)]**> **[高级 (Advanced)]** > **[常规 (General)]**。

4 取消选择 **[启用日志记录 (Enable logging)]** 复选框。

结果显示如下。



5 单击 **[确定 (OK)]** 关闭 **[虚拟机属性 (Virtual Machine Properties)]** 对话框。

附录

ESX Server 3 技术支持命令 A

本附录列出了用于配置 ESX Server 3 的服务控制台命令。其中大多数命令专供技术支持使用并仅供参考。但在少数情况下，这些命令也提供为 ESX Server 3 主机执行配置任务的唯一方式。此外，如果丢失了与主机的连接，则通过命令行界面执行某一命令可能是您唯一可以求助的方式 - 例如，如果网络不起作用，则 VI Client 也因此不可用。

注意 如果使用此附录中的命令，则必须执行 `service mgmt-vmware restart` 命令重新启动 `vmware-hostd` 进程，同时警示 VI Client 及其他管理工具，通知其配置已更改。一般而言，如果主机当前由 VI Client 或 VirtualCenter Server 管理，则不要执行此附录中的命令。

VI Client 图形用户界面提供了此附录中所述的执行配置任务的首选方式。可以使用此附录来判断应使用什么 VI Client 命令来代替服务控制台命令。此附录提供在 VI Client 中执行的操作的概述，但不给出完整的说明。有关使用命令和通过 VI Client 执行配置任务的详细信息，请参见联机帮助。

登录服务控制台并使用 `man <esxcfg_command_name>` 命令显示手册页，可找到有关多个 ESX Server 3 命令的详细信息。

表 A- 1 列出了为 ESX Server 3 提供的技术支持命令，概括了每个命令的用途并提供了一个备用 VI Client。只有在从清单面板中选定 ESX Server 3 主机并单击 **[配置 (Configuration)]** 选项卡之后，才可以执行表中列出的大多数 VI Client 操作。除非另有声明，否则这些操作即为下述任一过程的预备步骤。

表 A-1 ESX Server 3 技术支持命令

服务控制台命令	命令用途和 VI Client 过程
`esxcfg-advcfg`	为 ESX Server 3 配置高级选项。 要在 VI Client 中配置高级选项，请单击 **[高级设置 (Advanced Settings)]**。**[高级设置 (Advanced Settings)]** 对话框打开时，使用左侧的列表选择要使用的设备类型或活动，然后输入适当的设置。
`esxcfg-auth`	配置身份验证。可使用此命令在 `pam_cracklib.so` 和 `pam_passwdqc.so` 插件之间切换，以便实施密码更改规则。也可使用此命令来重置这两个插件的选项。有关详细信息，请参见 “密码复杂度”（第 216 页）。 在 VI Client 中无法配置这些功能。
`esxcfg-boot`	配置引导程序设置。此命令适用于引导程序进程，并仅供 VMware 技术支持使用。除非得到 VMware 技术支持代表指示，否则不得发出此命令。 在 VI Client 中无法配置这些功能。
`esxcfg-dumppart`	配置诊断分区或搜索现有诊断分区。 在安装 ESX Server 3 时，将自动创建诊断分区，用于在发生系统故障时存储调试信息。除非确定主机没有诊断分区，否则无需手动创建此分区。 可对 VI Client 中的诊断分区执行以下管理行为： ■ **确定是否有诊断分区** - 单击 **[存储器 (Storage)] > [添加 (Add)]**，然后查看 **[添加存储器 (Add Storage)]** 向导的第一个页面以确定其是否包括 **[诊断 (Diagnostic)]** 选项。如果没有 **[诊断 (Diagnostic)]** 选项，则 ESX Server 3 已具有一个诊断分区。 ■ **配置诊断分区** - 单击 **[存储器 (Storage)] > [添加 (Add)] > [诊断 (Diagnostic)]**，然后一步步完成向导。
`esxcfg-firewall`	配置服务控制台防火墙端口。 要在 VI Client 中为支持的服务和代理配置防火墙端口，请选择 Internet 服务。可通过该服务访问 ESX Server 3 主机。单击 **[安全配置文件 (Security Profile)] > [防火墙 (Firewall)] > [属性 (Properties)]**，然后使用 **[防火墙属性 (Firewall Properties)]** 对话框添加服务。有关添加支持的服务和配置防火墙的详细信息，请参见 “为支持的服务和管理代理打开防火墙端口”（第 171 页）。 不可通过 VI Client 配置不受支持的服务。对于这些服务，请使用如 “服务控制台防火墙配置”（第 211 页）中所述的 `esxcfg-firewall` 命令。
`esxcfg-info`	打印有关服务控制台、 VMkernel、虚拟网络中各种子系统以及存储资源硬件的状况信息。 VI Client 不提供打印此信息的方法，但可以通过用户界面中的不同选项卡和功能获得尽可能多的信息。例如，通过检查 **[虚拟机 (Virtual Machines)]** 选项卡上的信息，可以查看虚拟机的状态。
`esxcfg-init`	执行内部初始化例程。此命令适用于引导程序进程，不得在任何情况下使用此命令。使用此命令可能导致 ESX Server 3 主机出现问题。 此命令不存在 VI Client 等效指令。

表 A-1 ESX Server 3 技术支持命令 （续）

服务控制台命令	命令用途和 VI Client 过程
`esxcfg-linuxnet`	引导 ESX Server 3 进入仅服务控制台模式而不是进入 ESX 模式时，将 `vswif` 转换为 `eth`。此命令适用于引导程序进程，并仅供 VMware 技术支持使用。除非得到 VMware 技术支持代表指示，否则不得发出此命令。 此命令不存在 VI Client 等效指令。
`esxcfg-module`	设置驱动程序参数和修改在启动时加载的驱动程序。此命令适用于引导程序进程，并仅供 VMware 技术支持使用。除非得到 VMware 技术支持代表指示，否则不得发出此命令。 此命令不存在 VI Client 等效指令。
`esxcfg-mpath`	为光纤通道或 iSCSI 磁盘配置多路径设置。 要为 VI Client 中的存储器配置多路径设置，请单击 **[存储器 (Storage)]**。选择数据存储或映射的 LUN，然后单击 **[属性 (Properties)]**。 **[属性 (Properties)]** 对话框打开时，根据需要选择所需的扩展。然后单击 **[扩展设备 (Extent Device)]** > **[管理路径 (Manage Paths)]**，然后使用 **[管理路径 (Manage Path)]** 对话框配置路径。
`esxcfg-nas`	管理 NAS 装载。使用此命令可添加、删除、列出和更改 NAS 设备的属性。 要查看 VI Client 中的 NAS 设备，请单击 **[存储器 (Storage)]**，然后滚动查看存储器列表。也可以从 **[存储器 (Storage)]** 视图执行以下活动： ■ **显示 NAS 设备的属性** - 单击设备并查看 **[详细信息 (Details)]** 下的信息。 ■ **添加 NAS 设备** - 单击 **[添加存储器 (Add Storage)]**。 ■ **删除 NAS 设备** - 单击 **[移除 (Remove)]**。 ■ **更改 NAS 设备的属性** - 单击设备，然后单击 **[详细信息 (Details)]** > **[属性 (Properties)]**。 有关如何创建和配置 NAS 数据存储的完整说明，请参见 “配置 ESX Server 3 访问 NFS 卷”（第 118 页）。
`esxcfg-nics`	打印物理网络适配器的列表以及有关驱动程序、 PCI 设备和每个网卡的链接状况的信息。也可使用此命令来控制物理网络适配器的速度和双工模式。 要查看有关 VI Client 中主机的物理网络适配器的信息，请单击 **[网络适配器 (Network Adapters)]**。 要更改 VI Client 中物理网络适配器的速度和双工模式，请单击 **[网络 (Networking)]** > **[属性 (Properties)]** 以更改与物理网络适配器关联的虚拟交换机。在 **[属性 (Properties)]** 对话框中，单击 **[网络适配器 (Network Adapters)]** > **[编辑 (Edit)]**，然后选择速度和双工模式组合。有关如何更改速度和双工模式的完整说明，请参见 “通过更改速度来配置上行链路网络适配器”（第 39 页）。
`esxcfg-resgrp`	恢复资源组设置并允许您执行基本资源组管理。 从清单面板选择一个资源池，然后单击 **[摘要 (Summary)]** 选项卡上的 **[编辑设置 (Edit Settings)]** 以更改资源组设置。

表 A-1 ESX Server 3 技术支持命令 （续）

服务控制台命令	命令用途和 VI Client 过程
esxcfg-route	设置或检索默认 VMkernel 网关路由以及添加、移除或列出静态路由。 要查看 VI Client 中的默认 VMkernel 网关路由，请单击 **[DNS 和路由 (DNS and Routing)]**。要更改默认的路由，请单击 **[属性 (Properties)]**，然后同时更新 **[DNS 和路由配置 (DNS and Routing Configuration)]** 对话框中这两个选项卡的信息。
esxcfg-swiscsi	配置软件 iSCSI 软件适配器。 要配置 VI Client 中的软件 iSCSI 系统，请单击 **[存储适配器 (Storage Adapters)]**，选择要配置的 iSCSI 适配器，然后单击 **[属性 (Properties)]**。使用 **[iSCSI 启动程序属性 (iSCSI Initiator Properties)]** 对话框配置适配器。 有关如何创建和配置 iSCSI 数据存储的完整说明，请参见 “iSCSI 存储器”（第 100 页）。
esxcfg-upgrade	将 ESX Server 从 ESX Server 2.*x* 升级为 ESX Server 3。该命令不用于一般用途。 从 2.*x* 升级到 3.*x* 时完成以下三个任务。以下任务可在 VI Client 中执行： ■ **升级主机** - 升级二进制数据，从 ESX Server 2.*x* 转换为 ESX Server 3。不可从 VI Client 执行此步骤。有关执行此升级的信息，请参见 *《安装与升级指南》*。 ■ **升级文件系统** - 要将 VMFS-2 升级到 VMFS-3，请挂起或关闭虚拟机，然后单击 **[清单 (Inventory)] > [主机 (Host)] >[进入维护模式 (Enter Maintenance Mode)]**。单击 **[存储器 (Storage)]**，选择存储设备，然后单击 **[升级到 VMFS-3 (Upgrade to VMFS-3)]**。必须为要升级的每个存储设备执行此步骤。 ■ **升级虚拟机** - 要将虚拟机从 VMS-2 升级到 VMS-3，请右键单击清单面板中的虚拟机，然后选择 **[升级虚拟机 (Upgrade Virtual Machine)]**。
esxcfg-vmhbadevs	打印 VMkernel 存储设备至服务控制台设备的映射。此命令不存在 VI Client 等效指令。
esxcfg-vmknic	创建和更新 VMotion、 NAS 和 iSCSI 的 VMkernel TCP/IP 设置。 要设置 VI Client 中的 VMotion、 NFS 或 iSCSI 网络连接，请单击 **[网络 (Networking)] > [添加网络连接 (Add Networking)]**。选择 **[VMkernel]**，然后一步步完成 **[添加网络向导 (Add Network Wizard)]**。在 **[连接设置 (Connection Settings)]** 步骤中定义 IP 地址子网掩码和 VMkernel 默认网关。 要查看设置，请单击 VMotion、 iSCSI 或 NFS 端口左侧的蓝色图标。要编辑任何这些设置，请单击交换机的 **[属性 (Properties)]**。从交换机 **[属性 (Properties)]** 对话框上的列表中选择端口，然后单击 **[编辑 (Edit)]** 以打开端口 **[属性 (Properties)]** 对话框，然后更改端口的设置。 有关如何创建和更新 VMotion、 NFS 或 iSCSI 网络连接的完整说明，请参见 “VMkernel 网络配置”（第 28 页）。

表 A-1 ESX Server 3 技术支持命令 （续）

服务控制台命令	命令用途和 VI Client 过程
esxcfg-vswif	创建和更新服务控制台网络设置。如果因网络配置问题无法通过 VI Client 管理 ESX Server 3 主机，则使用此命令。有关详细信息，请参见 “服务控制台网络的疑难解答”（第 72 页）。 要设置 VI Client 中的服务控制台连接，请单击 **[网络 (Networking)] > [添加网络连接 (Add Networking)]**。选择 **[服务控制台 (Service Console)]**，然后一步步完成 **[添加网络向导 (Add Network Wizard)]**。在 **[连接设置 (Connection Settings)]** 步骤中定义 IP 地址子网掩码和服务控制台默认网关。 要查看设置，请单击服务控制台端口左侧的蓝色图标。要编辑任何这些设置，请单击交换机的 **[属性 (Properties)]**。从交换机 **[属性 (Properties)]** 对话框上的列表中选择服务控制台端口。单击 **[编辑 (Edit)]** 以打开端口 **[属性 (Properties)]** 对话框，然后更改端口设置。 有关如何创建和更新服务控制台连接的完整说明，请参见 “服务控制台配置”（第 32 页）。
esxcfg-vswitch	创建和更新虚拟机网络设置。 要设置 VI Client 中的虚拟机连接，请单击 **[网络 (Networking)] > [添加网络连接 (Add Networking)]**。选择 **[虚拟机 (Virtual Machine)]**，然后一步步完成 **[添加网络向导 (Add Network Wizard)]**。 要查看设置，请单击虚拟机端口组左侧的语言泡状图标。要编辑这些设置，请单击交换机的 **[属性 (Properties)]**。从交换机 **[属性 (Properties)]** 对话框上的虚拟机列表中选择端口，然后单击 **[编辑 (Edit)]** 以打开端口 **[属性 (Properties)]** 对话框，然后更改端口的设置。 有关如何创建和更新虚拟机的完整说明，请参见 “虚拟机的虚拟网络配置”（第 25 页）。

其他命令

为了支持特定的内部操作，ESX Server 3 安装包括标准 Linux 配置命令的子集，例如网络和存储器配置命令。使用这些命令执行配置命令可能导致严重的配置冲突并造成部分 ESX Server 3 功能不可用。除非 VMware Infrastructure 文档中另有说明或者得到 VMware 技术支持人员指示，否则在配置 ESX Server 3 时始终通过 VI Client 工作。

使用 vmkfstools

B

可以使用 vmkfstools 实用程序来创建和操作 VMware ESX Server 主机上的虚拟磁盘、文件系统、逻辑卷和物理存储设备。使用 vmkfstools 可以在磁盘的物理分区上创建和管理 virtual machine file system (VMFS)。还可以使用此命令操作文件，例如存储在 VMFS-2、 VMFS-3 和 NFS 上的虚拟磁盘文件。

可使用 VI Client 执行大多数 vmkfstools 操作。有关使用 VI Client 操作存储器的信息，请参见 “配置存储器”（第 93 页）。

本附录包括以下各节：

vmkfstools 命令语法

一般而言，不需以超级用户的身份登录来运行 vmkfstools 命令。但是，某些命令，例如文件系统命令，可能需要以超级用户身份登录。

以下是与 vmkfstools 命令配合使用的参数：

- <option> 为一个或多个命令行选项及相关联的参数，用于指定 vmkfstools 要执行的活动 - 例如，在创建新的虚拟磁盘时选择磁盘格式。

  输入选项以后，通过在 /vmfs 层次结构中输入相对或绝对文件路径名，指定要在其中执行操作的文件或 VMFS 文件系统。

- <partion> 用于指定文件分区。此参数使用 vmhbaA:T:L:P 格式，其中 A、 T、 L 和 P 是分别代表着适配器、目录、 LUN 和分区编号的整数。分区数字必须大于零 (0)，并对应于类型为 fb 的有效 VMFS 分区。

  例如， vmhba0:2:3:1 表示在 LUN 3、目标 2 和 HBA 0 上第一个分区。

- <device> 用于指定设备或逻辑卷。此参数使用 ESX Server 3 设备文件系统中的路径名。路径名以 /vmfs/devices 开头，这是设备文件系统的装载点。

  指定不同类型的设备时，请使用以下格式：

  - /vmfs/devices/disks 适用于本地或基于 SAN 的磁盘。
  - /vmfs/devices/lvm 适用于 ESX Server 3 逻辑卷。
  - /vmfs/devices/generic 适用于通用 SCSI 设备，例如磁带驱动器。

- <path> 用于指定 VMFS 文件系统或文件。此参数是对目录符号链接、裸设备映射或 /vmfs 下的文件进行命名的绝对或相对路径。

  - 要指定 VMFS 文件系统，请使用此格式：

    /vmfs/volumes/<file_system_UUID>

    或

    /vmfs/volumes/<file_system_label>

  - 要指定 VMFS 文件，请使用此格式：

    /vmfs/volumes/<file system label|file system UUID>/[dir]/myDisk.vmdk

    如果当前的工作目录是 myDisk.vmdk 的父目录，则不必输入完整路径。

  例如，

  /vmfs/volumes/datastore1/rh9.vmdk

vmkfstools 选项

本节包括了一个可以与 vmkfstools 命令一同使用的选项的列表。本节中某些任务所包含的选项仅建议高级用户使用。

长格式与短格式 （单个字母）的选项表示相同含义。例如，下面的命令是一样的：

```
vmkfstools --createfs vmfs3 --blocksize 2m vmhba1:3:0:1
vmkfstools -C vmfs3 -b 2m vmhba1:3:0:1
```

-v 子选项

该 -v 子选项表示命令输出的详细级别。该子选项的格式如下：

```
-v --verbose <number>
```

可以指定 <number> 的值，范围是从 1 到 10 的整数。

使用任何 vmkfstools 选项都可以指定 -v 子选项。如果选项的输出不适合于 -v 子选项，则 vmkfstools 将忽略 -v。

注意 由于可以将 -v 子选项包含在任何 vmkfstools 命令行中，因此 -v 不作为子选项纳入选项描述中。

文件系统选项

文件系统选项可用于创建 VMFS 文件系统。这些选项不适用于 NFS。这些任务中有许多是可以通过 VI Client 执行的。

创建 VMFS 文件系统

```
-C --createfs vmfs3
-b --blocksize <block_size>kK|mM
-S --setfsname <fsName>
```

本选项将在指定的 SCSI 分区，例如 vmhba1:0:0:1 上创建 VMFS-3 文件系统。该分区将成为文件系统的主分区。

在任何 ESX Server 3 主机上， VMFS-2 文件系统都是只读的。您不可创建或修改 VMFS-2 文件系统，但可读取 VMFS-2 文件系统上存储的文件。 VMFS-3 文件系统不能从 ESX 2.x 主机进行访问。

小心 一个 LUN 只有一个 VMFS 卷。

可以与 -C 选项一同指定以下子选项：

- –b ––blocksize - 定义 VMFS-3 文件系统的块大小。默认的块大小为 1 MB。指定的 <block_size> 值必须是 128 kb 的倍数，最小值为 128 kb。输入大小值时，请加上后缀 m 或 M 以表明单位类型。单位类型不区分大小写 - vmkfstools 将 m 或 M 的含义理解为兆字节，将 k 或 K 的含义理解为千字节。
- –S ––setfsname - 为正在创建的 VMFS-3 文件系统定义 VMFS 卷的卷标。此子选项只与 –C 选项连用。指定的卷标最多为 128 个字符，并且在开头和结尾不能包含空格。

  定义了卷标后，则在为 vmkfstools 命令指定 VMFS 卷时可随时使用此卷标。卷标将出现在为 Linux ls –l 命令生成的列表中，并且作为指向 /vmfs/volumes 目录下 VMFS 卷的符号链接。

  要更改 VMFS 卷标，请使用 Linux ln –sf 命令。可参考以下示例：

  ```
  ln –sf /vmfs/volumes/<UUID> /vmfs/volumes/<fsName>
  ```

  <fsName> 是用于 <UUID> VMFS 的新卷标。

创建 VMFS 文件系统的示例。

```
vmkfstools –C vmfs3 –b 1m –S my_vmfs /vmfs/devices/disks/vmhba1:3:0:1
```

此示例说明如何在 vmhba 适配器 1 的 LUN 0、目标 3 的第一个分区上创建名称为 my_vmfs 的新 VMFS-3 文件系统。文件块大小为 1 MB。

扩展现有的 VMFS-3 卷

```
–Z ––extendfs <extention–device> <existing–VMFS–volume>
```

此选项将为以前创建的 VMFS 卷 <existing–VMFS–volume> 添加另一个扩展。您必须指定路径全名，例如 /vmfs/devices/disks/vmhba0:1:2:1，而不仅是短名称 vmhba0:1:2:1。每次使用此选项时都用新扩展扩展 VMFS-3 卷，因此该卷将跨多个分区。逻辑 VMFS-3 卷最多可以包含 32 个物理扩展。

小心 运行此选项时，则之前在 <extension–device> 中指定的 SCSI 设备上保存的所有数据均将丢失。

扩展 VMFS-3 卷的示例

```
vmkfstools –Z /vmfs/devices/disks/vmhba0:1:2:1
            /vmfs/devices/disks/vmhba1:3:0:1
```

此示例允许逻辑文件系统跨到新分区，以对其进行扩展。扩展后的文件系统跨两个分区 - vmhba1:3:0:1 和 vmhba0:1:2:1. 在此示例中， vmhba1:3:0:1 是主分区的名称。

列出 VMFS 卷的属性

`-P --queryfs`
`-h --human-readable`

当此选项用于任何驻留在 VMFS 卷上的文件或目录时，它将列出指定的卷的属性。列出的属性包括 VMFS 版本号 （VMFS-2 或 VMFS-3）、指定的 VMFS 卷所包含的扩展的个数、卷标 （如果有）、 UUID 以及各个扩展所驻留的设备名称列表。

注意 如果任何设备备用 VMFS 文件系统脱机，则扩展的数量以及可用的空间也将相应更改。

可以在使用 `-P` 选项时指定 `-h` 子选项。如果这样，则 `vmkfstools` 将以更易理解的形式列出卷容量，例如， `5k`、 `12.1M` 或 `2.1G`。

将 VMFS-2 升级至 VMFS-3

可以将 VMFS-2 文件系统升级至 VMFS-3。

小心 VMFS-2 至 VMFS-3 的转换是一种单向进程。将 VMFS-2 卷转换为 VMFS-3 后，则不能再转换回 VMFS-2 卷。

仅当 VMFS-2 文件系统的文件块大小未超过 8 MB 时，才可对其进行升级。

升级文件系统时，请使用以下选项：

- `-T --tovmfs3 -x --upgradetype [zeroedthick|eagerzeroedthick|thin]`

  该选项将 VMFS-2 文件系统转换为 VMFS-3，同时保留文件系统中的所有文件。转换之前，请使用模块选项 `fsauxFunction=upgrade` 卸载 `vmfs2` 和 `vmfs3` 驱动程序并加载辅助文件系统驱动程序 `fsaux`。

  您必须使用 `-x --upgradetype` 子选项将升级类型指定为以下任一种：

  - `-x zeroedthick`（默认）- 保留 VMFS-2 厚文件的属性。通过 `zeroedthick` 文件格式，磁盘空间将分配至文件以备将来使用，并且未使用的数据块也不会置零。
  - `-x eagerzeroedthick` - 转换时将厚文件中的未使用数据块置零。如果使用此子选项，则升级过程会比使用其它选项耗时更长。
  - `-x thin` - 将 VMFS-2 厚文件转换为自动精简配置的 VMFS-3 文件。与 `thick` 文件格式相反，自动精简配置的格式不允许为文件分配额外空间以备将来使用，它采用的是按需使用空间。在转换时将放弃 `thick` 文件中未使用的块。

在转换期间，ESX Server 3 文件锁定机制将确保没有其他本地进程访问正在转换的 VMFS 卷，同时也必须确保没有远程的 ESX Server 主机正在访问此卷。转换可能需时几分钟，完成后将返回命令提示符。

转换后，卸载 `fsaux` 驱动程序并加载 `vmfs3` 和 `vmfs2` 驱动程序，以继续正常操作。

- `-u --upgradefinish`

  此选项可完成升级。

虚拟磁盘选项虚拟磁盘选项可用于设置、迁移和管理存储在 VMFS-2、 VMFS-3 和 NFS 文件系统中的虚拟磁盘。这些任务中有许多也可以通过 VI Client 执行。

受支持的磁盘格式

创建或克隆虚拟磁盘时，可以使用 `-d --diskformat` 子选项来指定磁盘格式。从以下格式中选择：

- `zeroedthick` （默认） - 在创建时为虚拟磁盘分配所需的空间。创建时不会擦除物理设备上保留的任何数据，但是以后从虚拟机首次执行写操作时会按需要将其置零。虚拟机不从磁盘读取陈旧数据。
- `eagerzeroedthick` - 在创建时为虚拟磁盘分配所需的空间。与 `zeroedthick` 格式相比，在创建时会将物理设备上保留的数据置零。创建这种格式的磁盘可能比创建其他类型的磁盘耗时更长。
- `thick` - 在创建时为虚拟磁盘分配所需的空间。这种格式化类型不会将可能存在于该分配空间中的任何旧数据置零。非超级用户不允许创建此格式。
- `thin` - 自动精简配置的虚拟磁盘。与 `thick` 格式不同，它在创建时不会为虚拟磁盘分配所需的空间，只会在将来需要时再提供或置零。
- `rdm` - 虚拟兼容模式裸磁盘映射。
- `rdmp` - 物理兼容模式 （传递）裸磁盘映射。
- `raw` - 裸设备。
- `2gbsparse` - 最大扩展为 2 GB 的稀疏磁盘。可将此格式的磁盘用于其他 VMware 产品，但是，除非先利用 `vmkfstools` 以兼容的格式 （例如 `thick` 或 `thin`）重新导入磁盘，否则无法在 ESX Server 主机上启动稀疏磁盘，
- `monosparse` - 单片式稀疏磁盘。可将此格式的磁盘用于其他 VMware 产品。
- `monoflat` - 单片式平面磁盘。可将此格式的磁盘用于其他 VMware 产品。

注意 仅可用于 NFS 的磁盘格式是 thin、 thick、 zerodthick 和 2gbsparse。

thick、zeroedthick 和 thin 通常具有相同的意义，因为决定分配策略的是 NFS 服务器而非 ESX Server 主机。大多数 NFS 服务器上的默认分配策略是 thin。

创建虚拟磁盘

```
-c --createvirtualdisk <size>[kK|mM|gG]
      -a --adaptertype [buslogic|lsilogic] <srcfile>
      -d --diskformat [thin|zeroedthick|eagerzeroedthick]
```

此选项将在 VMFS 卷上按指定的路径创建虚拟磁盘。指定虚拟磁盘的容量。为 <size> 输入值时，可以加上 k （千字节）、 m （兆字节）或 g （千兆字节）等后缀以指明其单位类型。单位类型不区分大小写 - vmkfstools 将 k 或 K 的含义理解为千字节。如果不指定单位类型， vmkfstools 将默认为字节。

可以与 -c 选项一同指定以下子选项：

- -a 指定用于与虚拟磁盘进行通信的设备驱动程序。可以在 BusLogic 和 LSI Logic SCSI 这两个驱动程序间选择。
- -d 用于指定磁盘格式。有关磁盘格式的详细描述，请参见 “受支持的磁盘格式”（第 258 页）。

创建虚拟磁盘的示例

```
vmkfstools -c 2048m /vmfs/volumes/myVMFS/rh6.2.vmdk
```

此示例说明了如何在名称为 myVMFS 的 VMFS 文件系统中创建一个名为 rh6.2.vmdk、大小为 2 GB 的虚拟磁盘文件。此文件表示虚拟机可访问的空虚拟磁盘。

初始化虚拟磁盘

```
-w --writezeros
```

此选项将在虚拟磁盘的所有数据上写入零数据，以将其清空。完成此命令的时间可能较长，具体取决于虚拟磁盘的大小以及连接至托管虚拟磁盘的设备的 I/O 带宽。

小心 使用此命令时将丢失虚拟磁盘上的现有数据。

填充精简虚拟磁盘

```
-j --inflatedisk
```

此选项将 thin 虚拟磁盘转换为 eagerzeroedthick，并保留所有现有数据。此选项对尚未分配的任何块进行分配和置零。

请参见 "受支持的磁盘格式"（第 258 页）。

删除虚拟磁盘

```
-U --deletevirtualdisk
```

此选项将删除与虚拟磁盘 （它是在 VMFS 卷上指定路径中列出的虚拟磁盘）相关联的文件。

重命名虚拟磁盘

```
-E --renamevirtualdisk <oldName> <newName>
```

此选项将重命名与虚拟磁盘 （它是在命令行的路径规范部分中列出的虚拟磁盘）相关联的文件。您必须指定原始文件名或文件路径 <oldName>，以及新文件名或文件路径 <newName>。

克隆虚拟或原始磁盘

```
-i --importfile <srcfile> -d --diskformat
   [rdm:<device>|rdmp:<device>|
      raw:<device>|thin|2gbsparse|monosparse|monoflat]
```

此选项将创建指定虚拟磁盘或裸磁盘的副本。

可以将 -d 子选项与 -i 选项一起使用。此子选项将为创建的副本指定磁盘格式。请参见 "受支持的磁盘格式"（第 258 页）。非超级用户不允许克隆虚拟磁盘或裸磁盘。

注意 要克隆 ESX Server 3 重做日志，同时保留其层次结构，请使用 cp 命令。

克隆虚拟磁盘的示例

```
vmkfstools -i /vmfs/volumes/templates/gold-master.vmdk
              /vmfs/volumes/myVMFS/myOS.vmdk
```

此示例说明了如何将主虚拟磁盘的内容从 templates 存储库克隆到 myVMFS 文件系统上名为 myOS.vmdk 的虚拟磁盘文件中。可以通过向虚拟机配置文件添加配置行来配置虚拟机使用此虚拟磁盘，如下例所示：

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/myOS.vmdk
```

迁移 VMware Workstation 和 VMware GSX Server 虚拟机

不能使用 VI Client 将通过 VMware Workstation 或 VMware GSX Server 创建的虚拟机迁移到 ESX Server 3 系统中。但是，可使用 vmkfstools -i 命令将虚拟磁盘导入 ESX Server 3 系统，然后将此磁盘连接到在 ESX Server 3 中创建的新虚拟机上。您必须首先导入虚拟磁盘，因为您无法启动在 ESX Server 主机上以 2gbsparse 格式导出的磁盘。

迁移 VMware Workstation 和 GSX Server 虚拟机

1 将 Workstation 或 GSX Server 磁盘导入 /vmfs/volumes/myVMFS/ 目录或任何子目录。

2 在 VI Client 中，使用 **[自定义 (Custom)]** 配置选项创建新虚拟机。

3 配置磁盘时，选择 **[使用现有虚拟磁盘 (Use an existing virtual disk)]** 选项并连接导入的 Workstation 或 GSX Server 磁盘。

扩展虚拟磁盘

`-X --extendvirtualdisk <new size>[kK|mM|gG]`

此选择可在创建虚拟机后，扩展分配至虚拟机的磁盘大小。输入此命令之前，必须关闭使用此磁盘文件的虚拟机。必须更新磁盘上的文件系统，以便使客户操作系统识别和使用新的磁盘大小，并利用额外的空间。

通过分别添加 k （千字节）、 m （兆字节）或 g （千兆字节）等后缀，可以将 newSize 参数指定为千字节、兆字节或千兆字节。单位类型不区分大小写 - vmkfstools 将 k 或 K 的含义理解为千字节。如果不指定单位类型， vmkfstools 将默认为千字节。

上述 newSize 参数将重新定义整个磁盘的大小，而不是定义给磁盘增加的大小。

例如，要给 4 G 的虚拟磁盘增加 1 G，则输入：

`vmkfstools -X 5g <disk name>.dsk`

注意 请勿在虚拟机中对有快照与其关联的基础磁盘进行扩展。否则，您再也不能提交快照或将基础磁盘转换回原始大小。

将 VMFS-2 虚拟磁盘迁移至 VMFS-3

`-M --migratevirtualdisk`

此选项可以将指定的虚拟磁盘文件从 ESX Server 2 格式转换为 ESX Server 3 格式。

创建虚拟兼容模式裸设备映射

`-r --createrdm <device>`

此选项将在 VMFS-3 卷上创建裸设备映射 (RDM) 文件，并将裸磁盘映射至该文件。在建立映射后，便可以像访问正常 VMFS 虚拟磁盘那样访问原始磁盘。映射的文件长度与其所指的原始磁盘的大小相同。

当指定 <device> 参数时，为分区输入 0，这表示整个原始磁盘均已使用。使用以下格式：

`/vmfs/devices/disks/vmhbaA:T:L:0`

有关详细信息，请参见 “vmkfstools 命令语法”（第 254 页）。

有关配置和使用 RDM 的详细信息，请参见 “裸设备映射”（第 133 页）。

注意 所有 VMFS-3 文件锁定机制均适用于 RDM。

创建虚拟兼容模式 RDM 的示例

```
vmkfstools –r /vmfs/devices/disks/vmhba1:3:0:0 my_rdm.vmdk
```

创建名为 `my_rdm.vmdk` 的 RDM 文件，并将 `vmhba1:3:0:0` 裸磁盘映射到该文件。通过将以下行添加到虚拟机配置文件中，可以配置虚拟机使用 `my_rdm.vmdk` 映射文件：

```
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/myVMFS/my_rdm.vmdk
```

创建物理兼容模式裸设备映射

```
–z ––createrdmpassthru <device>
```

此选项允许将传递裸设备映射到 VMFS 卷上的文件。该映射使虚拟机在访问其虚拟磁盘时能够规避 ESX Server 3 SCSI 命令的筛选。当虚拟机需要发送专用的 SCSI 命令时，例如当 SAN 感知软件在虚拟机中运行时，此类映射将非常有用。

在建立了此类映射后，便可以使用该映射像访问任何其它 VMFS 虚拟磁盘一样访问原始磁盘了。

当指定 `<device>` 参数时，为分区输入 `0`，这表示整个裸设备均已使用。使用以下格式：

```
/vmfs/devices/disks/vmhbaA:T:L:0
```

请参见 “vmkfstools 命令语法”（第 254 页）。

列出 RDM 的属性

```
–q ––queryrdm
```

此选项可列出原始磁盘映射的属性。

此选项将打印原始磁盘 RDM 的 vmhba 名称。此选项还将打印原始磁盘的其他标识信息，例如磁盘 ID。

显示虚拟磁盘几何结构

```
–g ––geometry
```

此选项可获得有关虚拟磁盘几何结构的信息。

输入信息的形式如下：几何结构信息 C/H/S，其中 C 代表磁道的数量，H 代表磁头的数量，以及 S 代表扇区的数量。

注意 在将 VMware Workstation 虚拟磁盘导入 ESX Server 3 主机时，可能会看到磁盘几何结构不匹配的错误消息。磁盘几何结构不匹配也可能是因为加载客户操作系统或运行新创建的虚拟机时出现了问题。

管理 LUN 的 SCSI 预留

–L 选项可用于为物理存储设备执行管理任务。这些任务中有大部分是可以通过 VI Client 执行的。

```
–L --lock [reserve|release|lunreset|targetreset|busreset]<device>
```

该选项允许保留 SCSI LUN 以便由 ESX Server 3 主机专用；解除保留以便其他主机能够访问 LUN ；还允许重置保留，以强制从目标解除所有保留。

小心 使用 –L 选项可以中断 SAN 中其他服务器的操作。仅在排除群集设置故障时使用 –L 选项。

除非得到 VMware 的特别通知，否则决不要在托管 VMFS 卷的 LUN 上使用此选项。

可以通过几种方式指定 –L 选项：

- –L reserve - 保留指定的 LUN。保留后，仅有指定的服务器可以访问 LUN。如果其他服务器尝试访问 LUN，将导致保留错误。
- –L release - 解除在指定 LUN 上的保留。其他服务器可再次访问 LUN。
- –L lunreset - 重置指定的 LUN，方法是清除 LUN 上的所有保留，并使 LUN 再次对所有服务器可用。重置对设备上的其它 LUN 没有影响。如果保留了设备上的另一个 LUN，则它将仍然是保留的。
- –L targetreset - 重置整个目标。重置将清除与该目标关联的所有 LUN 上的保留，并使 LUN 再次对所有服务器可用。
- –L busreset - 重置总线上所有可访问的目标。重置将清除可通过总线访问的所有 LUN 上的任何保留，并使其再次对所有服务器可用。

当输入 <device> 参数时，请使用以下格式：

```
/vmfs/devices/disks/vmhbaA:T:L:P
```

请参见 “vmkfstools 命令语法”（第 254 页）。

索引

K

L

M

N

P

Q

W

X

Y

Z