ESX Server 3i 配置指南

ESX Server 3i 版本 3.5 和 VirtualCenter 2.5

vmware®

ESX Server 3i 配置指南
修订时间：20080410
项目：VI-CHS-Q208-527

我们的网站将提供最新技术文档，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

附录

关于本书

本手册 （《*ESX Server 3i 配置指南*》）提供有关如何为 ESX Server 3i 配置网络的信息，包括如何创建虚拟交换机和端口以及如何为虚拟机、 VMotion 和 IP 存储器设置网络的信息。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 3i，本指南提供了有关 ESX Server 3i 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 3i 技术支持命令及其 VMware Infrastructure Client (VI Client) 等效指令的列表以及一个 `vmkfstools` 实用程序的描述。

《ESX Server 3i 配置指南》 涉及 ESX Server 3i 版本 3.5 的内容。要阅读并了解有关 ESX Server 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通用主题，本书使用术语 “ESX Server”。
- 如果讲解内容需要指定某特定版本，本书将使用带版本号的完整名称指代该产品。
- 如果讲解内容适用于 VMware Infrastructure 3 的所有 ESX Server 版本，则本书使用术语 “ESX Server 3.x”。

目标读者

本手册专供需要使用 ESX Server 3i 的用户使用。本手册中信息的目标读者为对 Windows 或 Linux 系统具有丰富经验且熟悉虚拟机技术和数据中心操作的管理员。

文档反馈

VMware 欢迎您提出宝贵建议，以便改进我们的文档。如有意见，请将反馈发送到：

docfeedback@vmware.com

VMware Infrastructure 文档

VMware Infrastructure 文档包括 VMware VirtualCenter 和 ESX Server 文档集。

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
数据库	VirtualCenter 数据库
数据存储	受管主机的存储
dsk#	受管主机的存储磁盘
host*n*	VirtualCenter 管理的主机
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
user#	具有访问权限的用户
VC	VirtualCenter
VM#	受管主机上的虚拟机

技术支持和培训资源

下面各节介绍为您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 培训服务

VMware 课程提供了大量实践操作环境、案例研究示例，以及作为作业参考工具的课程材料。有关 VMware 培训服务的详细信息，请访问 http://mylearn1.vmware.com/mgrreg/index.cfm。

1 简介

《*ESX Server 3i 配置指南*》介绍了为配置 ESX Server 3i 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 3i 主机以满足需要的概述、建议和概念性论述。在使用《*ESX Server 3i 配置指南*》中的信息之前，请仔细阅读《*VMware Infrastructure 简介*》以了解系统架构以及组成 VMware Infrastructure 系统的物理设备和虚拟设备的概述。

此简介概括了本指南的内容，因此从中可以找到所有所需信息。本指南论述了以下主题：

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

网络

ESX Server 3i 网络章节使您了解物理网络和虚拟网络的概念，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 3i 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。
- "网络故障排除" - 介绍常用的网络疑难解答方案。

存储器

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

- "存储器简介" - 介绍可以用来为 ESX Server 3i 主机配置存储器的存储设备类型。它还介绍了可以针对存储需求部署的 VMFS 和 NFS 数据存储。
- "配置存储器" - 说明如何配置本地存储器、光纤通道存储器、 iSCSI 存储器和 NAS 存储器。
- "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 3i 安全章节介绍 VMware 已嵌入到 ESX Server 3i 中的安全措施以及避免 ESX Server 3 主机受到安全威胁所采取的措施。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 3i 系统的安全" - 介绍有助于确保数据环境安全的 ESX Server 3i 功能并提供一个与安全相关的系统设计的概述。
- "确保 ESX Server 3i 配置的安全性" - 说明如何为 ESX Server 3i 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 3i 主机和 VirtualCenter 的访问权限。它还介绍了加密和委派用户。
- "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 3i 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全需要执行的一些操作。

附录

《ESX Server 3i 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 3i 主机时可能会有用。

- "使用远程命令行界面" - 说明如何安装和使用远程命令行界面 (Remote Command-Line Interface, Remote CLI)。它还包括一个所有支持的 Remote CLI 和指向论述每个命令位置的指示器的列表。
- "远程命令行界面参考" - 是在使用 Remote CLI 配置 ESX Server 3i 主机时，或者为快速配置准备运行于多个主机的脚本时，可以使用的命令的参考。附录首先介绍了一些常见的使用情况，然后提供了每条可用命令的参考信息。
- "使用 vmkfstools Remote CLI" - 是 `vmkfstools` 实用程序参考，您可以使用该实用程序来创建和操作与 VMware ESX Server 3i 主机关联的虚拟磁盘、文件系统、逻辑卷和物理存储设备。

网络

网络 2

本章将介绍在 ESX Server 3i 环境中进行网络连接的基本概念，并指导您如何在虚拟基础架构环境中设置和配置网络。

根据可反映两种类型网络服务的两种类别使用 VMware Infrastructure (VI) Client 添加网络连接：

- 虚拟机
- VMkernel

本章将讨论以下主题：

网络概念

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 3i，VMware 建议阅读本节。

概念概述

物理网络 是连接物理机的网络，用于在物理机间收发数据。 VMware ESX Server 3i 运行于物理机之上。

虚拟网络 是逻辑连接运行于单台物理机上的虚拟机的网络，用于在虚拟机间收发数据。虚拟机可连接在添加网络连接步骤中创建的虚拟网络。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，连接此虚拟网络的虚拟机也能访问连接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。一台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。交换机会了解连接其端口的主机，并使用该信息向正确的物理机转发流量。交换机是物理网络的核心，可将多个交换机连接在一起，以形成较大的网络。

虚拟交换机 *vSwitch* 的运行方式与物理以太网交换机十分相似。它检测与其虚拟端口进行逻辑连接的虚拟机，并使用该信息向正确的虚拟机转发流量。可使用物理以太网适配器 （也称为上行链路适配器）将 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 的运行方式与虚拟交换机大体相似，但它不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 23 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 vSwitch。端口组定义通过 vSwitch 的网络连接方式。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 25 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*网卡成组*。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 LAN 段进一步分段，以便使端口组中处于不同物理段上的端口互相隔离。 802.1Q 是标准。

VMkernel TCP/IP 网络堆栈 为 ESX Server 3i 主机提供网络连接并且支持 iSCSI、NFS 和 VMotion。虚拟机运行其自身系统的 TCP/IP 堆栈，并通过虚拟交换机连接以太网级别的 VMkernel。

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 (TCP Segmentation Offload, *TSO*) 可使 TCP/IP 堆栈发出非常大的帧（达到 64 k），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 分段卸载和巨型帧"（第 45 页）。

借助*通过 VMotion 迁移*，可在 ESX Server 3i 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，可通过 VMware Infrastructure (VI) Client 或直接 SDK API 创建称为虚拟交换机 (Virtual Switch, vSwitch) 的虚拟网络设备。 vSwitch 可在虚拟机之间进行内部流量路由或外部网络链接。

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 个。但在 ESX Server 3i 中，可为 vSwitch 创建多达 1016 个端口。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 25 页）。

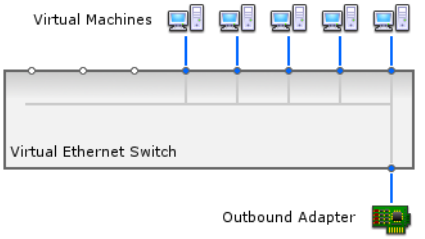
在配置虚拟机以访问网络之前，必须执行以下步骤：

1 创建 vSwitch，并将其配置为连接主机上的物理适配器，以连接物理网络。

2 创建连接该 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



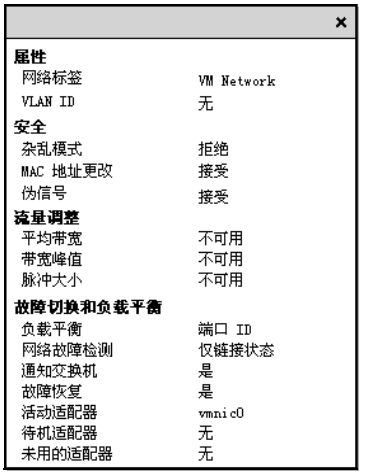
在 VI Client 中，选定 vSwitch 的详细信息显示为交互图，如图 2-2 中所示。始终可看到每台 vSwitch 的最重要信息。

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信息和第三级信息。

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。

使用网络标签，可以在主机之间移植虚拟机配置。对于数据中心中物理连接同一网络的所有端口组 （即每组都可以接收其他组的广播），应赋予同一标签。反过来，如果两个端口组无法接收对方的广播，则应赋予不同的标签。

如果使用 VLAN ID，则需要一起更改端口组标签和 VLAN ID，以便标签仍然能够适当表示连接性。

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

网络服务

需要在 ESX Server 3i 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

查看 VI Client 中的网络连接信息

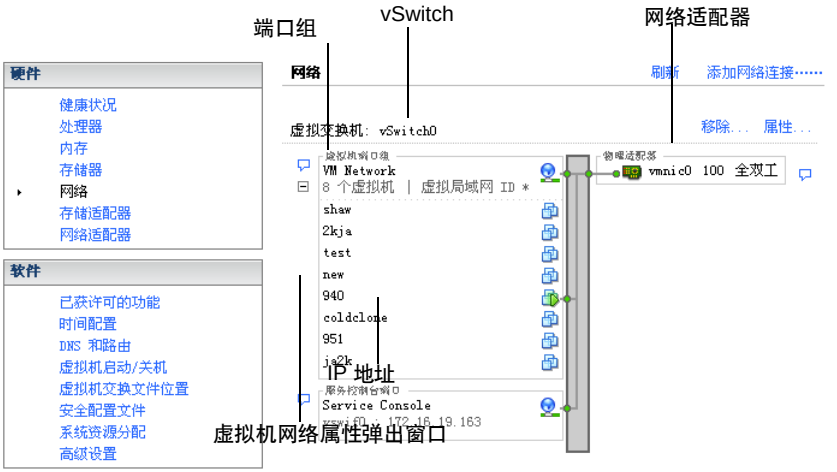
VI Client 显示了一般网络信息及网络适配器的特定信息。

查看 VI Client 中的一般网络连接信息

1 登录 VMware 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 **[网络 (Networking)]**。

图 2-4. 一般网络信息



查看 VI Client 中的一般网络适配器信息

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 唤醒功能。

虚拟机的虚拟网络配置

VI Client 添加网络连接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，需要考虑是否需要在 ESX Server 3i 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 - 即第 2 层的同一子网内。

ESX Server 3i 不支持在不同广播域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使用在其被移至另一个网络后不再可访问的系统和资源。即使网络配置设置为高可用性环境或包括可解决不同网络中虚拟机的需求的智能交换机，当 ARP 表格为虚拟机进行更新并恢复网络流量时，仍会遇到网络延迟。

虚拟机通过上行链路适配器接入物理网络。如果有一个或多个网络适配器连接 vSwitch，它只能将数据传输至外部网络。当两个或多个适配器连接一个单一 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 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)]**。

虚拟交换机以概览加详细信息布局显示。

3 在屏幕右侧，单击 **[添加网络连接 (Add Networking)]**。

此时会出现添加网络连接向导。

注意 添加网络连接向导可重复用于新端口和端口组。

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。

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)]** 下，输入用于识别所创建的端口组的网络标签。

使用网络标签识别常用于两个或多个主机的兼容迁移的连接。

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。

如果不能确定输入内容，请将此处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 （网卡成组），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，网络流量则路由至连接交换机的另一个适配器。网卡成组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 ESX Server 3i 中，VMkernel 网络接口为 ESX Server 3i 主机以及处理 VMotion 和 IP 存储器提供网络连接。

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。 VMotion 迁移可让您在不停机的情况下迁移虚拟机。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 网络通信用作其任何形式的基础存储器，包括用于 ESX Server 3i 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 接口端口组。

VMkernel（iSCSI、NFS 和 VMotion）提供的网络服务使用 VMkernel 中的 TCP/IP 堆栈。每个 TCP/IP 堆栈均通过连接一个或多个 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。
- 用于直接安装 .ISO 文件的 iSCSI， .ISO 文件对于虚拟机显示为 CD-ROM。
- 作为虚拟机数据存储的 NFS。
- 用于直接安装 `.ISO` 文件的 NFS， .ISO 文件对于虚拟机显示为 CD-ROM。
- 基于 VMotion 的迁移。

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

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)]** 链接。

此时将出现添加网络连接向导。

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。

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

6 选择 vSwitch 要使用的网络适配器的复选框。

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 **[新建虚拟交换机 (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，也可以选择现有的 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 35 页）。

7 单击 **[下一步 (Next)]**。

此时将出现 **[连接设置 (Connection Settings)]** 页面。

8 在 **[端口组属性 (Port Group Properties)]** 下，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)]** 复选框以启用此端口组，此端口组对于另一个 ESX Server 3i 显示为用于发送 VMotion 流量的网络连接。

仅可为每个 ESX Server 3i 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。

10 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)]**。

11 单击 **[编辑 (Edit)]**，设置 **[VMkernel 默认网关 (VMkernel Default Gateway)]**。

此时将出现 **[DNS 和路由配置 (DNS and Routing Configuration)]** 对话框。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。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)]** 选项卡下，输入 VMkernel 的网关信息。如果连接的计算机与 VMkernel 没有位于同一 IP 子网内，需要使用网关。

静态 IP 地址为默认值。

12 单击 **[确定 (OK)]** 以保存更改并关闭 **[DNS 配置和路由 (DNS Configuration and Routing)]** 对话框。

13 单击 **[下一步 (Next)]**。

14 使用 **[上一步 (Back)]** 按钮进行更改。

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

3 高级网络

本章指导您学习 ESX Server 3i 环境下的高级网络主题以及如何设置和更改高级网络配置选项。

本章将讨论以下主题：

虚拟交换机配置

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 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，找到要编辑的 vSwitch，然后单击该 vSwitch 的 **[属性 (Properties)]**。

4 单击 **[端口 (Ports)]** 选项卡。

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

6 单击 **[常规 (General)]** 选项卡以设置端口数量。

7 从下拉菜单中选择您要使用的端口数量。

8 单击 **[确定 (OK)]**。

通过更改其速度来配置上行链路网络适配器

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

4 在 **[vSwitch 属性 (vSwitch Properties)]** 对话框中，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。

如果网络适配器和物理交换机无法协商正确的连接速度，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" / "auto" 或 "ND" / "ND"，其中 ND 表示某个速度和双工，但两者不能设置为 "auto" / "ND"。

7 单击 **[确定 (OK)]**。

添加上行链路适配器

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

4 在 vSwitch 的 **[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。

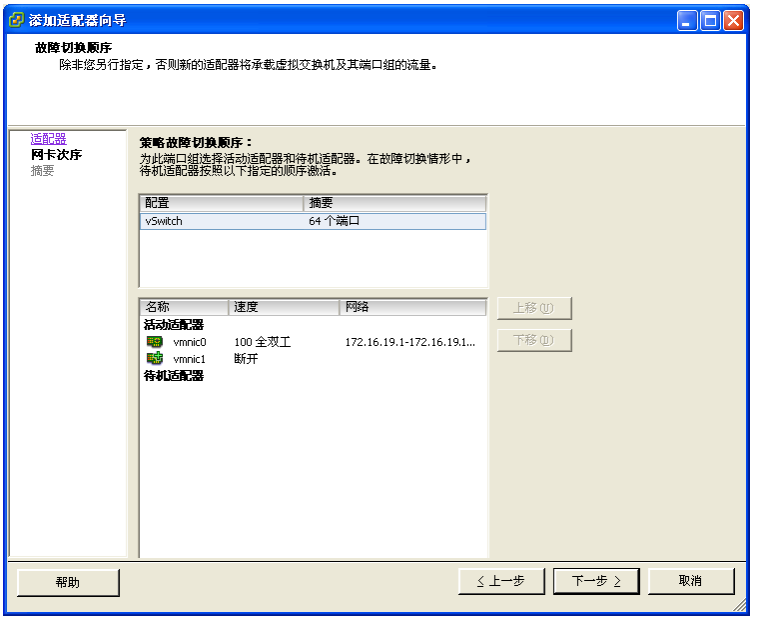
可以将多个适配器与一个 vSwitch 关联以提供网卡成组。此组可以共享流量并提供故障切换。

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 要对网络适配器排序，请选择网络适配器，然后单击按钮，将其上移或下移到所属的类别 （“活动的”或 “备用”）中。

- **[活动适配器 (Active Adapters)]** - vSwitch 当前使用的适配器。
- **[备用适配器 (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 检查信息，并使用 **[上一步 (Back)]** 按钮更改条目，然后单击 **[完成 (Finish)]** 以退出添加适配器向导。

此时将重新出现网络适配器列表，显示 vSwitch 现在需使用的适配器。

10 单击 **[关闭 (Close)]**。

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 3i 管理员决定与指定 vSwitch 相连的 Cisco 交换机端口。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）。

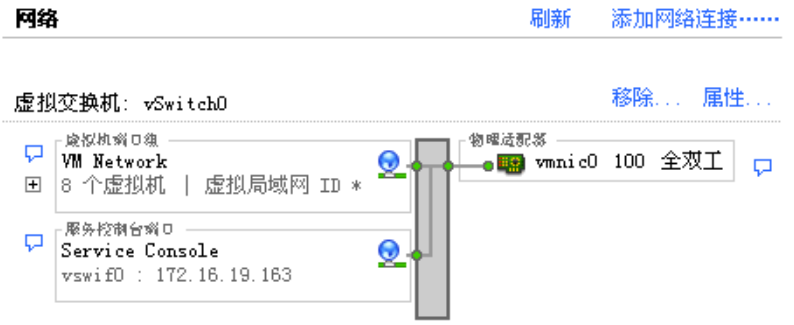
在 ESX Server 3i 中， CDP 设置为侦听，这表示 ESX Server 3i 检测并显示与关联的 Cisco 交换机端口相关的信息，但并不向 Cisco 交换机管理员提供有关 vSwitch 的信息。

从 VI Client 查看 Cisco 交换机信息

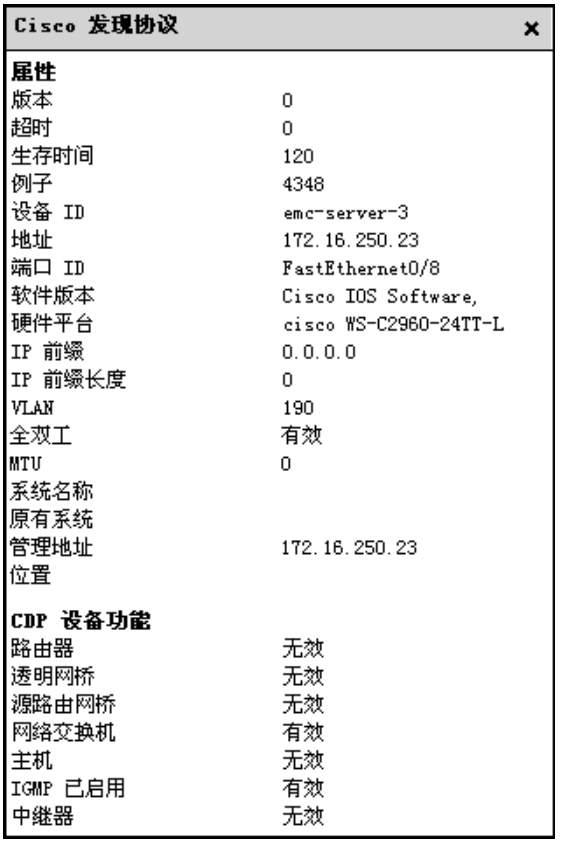
1 登录 VMware VI Client，从清单面板中选择服务器。

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 vSwitch 右侧的信息图标。



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。

要替代端口组的此类设置，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 (Promiscuous Mode)]**、**[MAC 地址更改 (MAC Address Changes)]** 和 **[伪信号 (Forged Transmits)]**。

在非杂乱模式中，客户机适配器仅侦听自己的 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。

请参见 “确保虚拟交换机端口安全”（第 145 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 对于要更改其第 2 层安全策略的 vSwitch，单击其 **[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（除了指定了策略异常的虚拟适配器的端口组所在的 vSwitch ）上的所有虚拟适配器。

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**
  - **[拒绝 (Reject)]** - 不会对适配器接收哪些帧产生任何影响。
  - **[接受 (Accept)]** - 使适配器检测经过 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**
  - **[拒绝 (Reject)]** - 如果设置为 **[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，入站帧将再次通过。
  - **[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**
  - **[拒绝 (Reject)]** - 源 MAC 地址不同于适配器上所设置地址的任何出站帧都会丢失。
  - **[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 3i 通过为三个出站流量特性指定参数来调整流量：**[平均带宽 (Average Bandwidth)]**、**[脉冲大小 (Burst Size)]** 和 **[带宽峰值 (Peak Bandwidth)]**。可以通过 VI Client 设置这些特性的值，为每个端口组设置流量调整策略。

- **[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 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 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)]**。

此时将显示选定 vSwitch 的 **[属性 (Properties)]** 对话框。

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

此时将出现 **[策略异常 (Policy Exceptions)]** 窗格。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。

这些是每个端口组异常将应用到的策略。

此处的策略适用于连接端口组的每个虚拟适配器，而不是整个 vSwitch。

状态 - 如果在 **[状态 (Status)]** 字段中启用了策略异常，则是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)]** - 一段特定时间内的测量值。
- **[带宽峰值 (Peak Bandwidth)]** - 该值为允许的最大带宽，且决不能小于平均带宽。此参数限制脉冲期间的最大带宽。
- **[脉冲大小 (Burst Size)]** - 该值指定脉冲大小 （以千字节 (KB) 为单位）。此参数控制超过平均速率后一次脉冲中可发送的数据量。

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间分布网络流量，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

  负载平衡策略确定了输出流量是如何在分配给 vSwitch 的网络适配器上分布的。

  注意 输入流量由物理交换机上的负载平衡策略控制。

- 故障切换检测：链接状态 / 信标探测
- 网络适配器顺序 （活动 / 备用）

编辑故障切换和负载平衡策略

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 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)]**。

此时将显示 vSwitch 的 **[属性 (Properties)]** 对话框。

6 单击 **[网卡成组 (NIC Teaming)]** 选项卡。

此时将出现 **[策略异常 (Policy Exceptions)]** 区域。可以在端口组级别覆盖故障切换顺序。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)]** 窗格中：

- **[负载平衡 (Load Balancing)]** - 指定如何选择上行链路。
  - **[基于源虚拟端口 ID 的路由 (Route based on the originating port ID)]** - 根据流量进入虚拟交换机的虚拟端口选择上行链路。
  - **[基于 IP哈希值路由 (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 哈希值路由 (Route based on source MAC hash)]** - 根据源以太网的哈希值选择上行链路。
  - **[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信道。对于其他所有选项，应禁用以太信道。

- **[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，或者配置到了错误的 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络适配器上的信标探测，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)]**，则每当虚拟网络适配器连接 vSwitch 时或虚拟网络适配器的流量因故障切换而由小组中的其他物理网络适配器路由时，都将通过网络发送通知以更新物理交换机的查看表。故障切换和 VMotion 迁移的滞后时间极小，因此该选项几乎适用于所有情况。

  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，替换接替其位置的备用适配器 （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。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情况，可以使用下拉菜单设置此条件，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。
  - **[备用适配器 (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)]** - 未使用的适配器。

端口组配置

可以更改以下端口组配置：

- 端口组属性
- 带标签的网络策略

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)]**。

此时将显示 **[vSwitch 属性 (vSwitch Properties)]** 对话框。

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)]** - 识别正在创建的端口组。当配置与此端口组连接的虚拟适配器时，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将使用的 VLAN。

7 单击 **[确定 (OK)]** 以退出 **[vSwitch 属性 (vSwitch Properties)]** 对话框。

覆盖带标记的网络策略

1 要覆盖特定的带标签网络的此类设置，请选择网络。

2 单击 **[编辑 (Edit)]**。

3 单击 **[安全 (Security)]** 选项卡。

4 选中要覆盖的带标签网络策略的复选框。

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

6 选中复选框以覆盖启用或禁用 **[状态]**。

7 单击 **[网卡成组 (NIC Teaming)]** 选项卡。

8 选中相关复选框以覆盖负载平衡或故障切换策略。

9 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 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)]**。

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 选择是获取 DNS 服务器地址，还是使用 DNS 服务器地址。

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。

8 单击 **[确定 (OK)]**。

TCP 分段卸载和巨型帧

TCP 分段卸载 (TCP Segmentation Offload, TSO) 和巨型帧支持已添加到 ESX Server 3i 中。必须使用 Remote CLI 在服务器级别启用巨型帧才能配置每个 vSwitch 的 MTU 大小。 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启动时升级 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。请参见 “VMkernel 网络配置”（第 29 页）。

启用巨型帧

巨型帧允许 ESX Server 3i 将较大的帧发送到物理网络上。要使巨型帧生效，网络必须端到端支持巨型帧。最大可支持 9KB （9000 字节）的巨型帧。 ESX Server 3i 中的 VMkernel 网络接口不支持巨型帧。

必须在 ESX Server 3i 主机上通过 Remote CLI 对每个 vSwitch 启用巨型帧。在启用巨型帧之前，请与硬件供应商核对，以确保您的物理网络适配器支持巨型帧。

创建已启用巨型帧的 vSwitch

1 登录到 ESX Server 3i Remote CLI。

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

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 大小应在连接 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。

注意 ESX Server 3 支持的最大 MTU 大小为 9000。

设置 MAC 地址

MAC 地址是为 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，如在下列情况下：

- 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。
- 希望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 有三个 OUI：

- 一个用于生成 MAC 地址。
- 一个用于手动设置 MAC 地址。
- 一个用于 ESX 3 以前的虚拟机，但是 ESX Server 3i 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 个字节具有该值。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表现。该算法将在任何服务器上，随机地同时为运行的和已挂起的虚拟机的数量设置一个限制。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 3i 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，例如移至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。在特定物理机上，已分配给运行中和暂停虚拟机的网络适配器的所有 MAC 地址不会被跟踪。

已关闭虚拟机的 MAC 地址不会对照运行中或暂停虚拟机的 MAC 地址进行检查。虚拟机再次启动后，有可能获得不同的 MAC 地址。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来设置地址：

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

其中， < 编号 > 表示以太网适配器的编号， 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 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< 编号 >.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< 编号 >.addressType="static"
```

由于 VMware ESX Server 3i 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 输入符合要求的静态 MAC 地址，然后单击 **[确定 (OK)]**。

网络提示和最佳做法

本节提供了以下相关信息：

- 网络最佳做法
- 网络提示

网络最佳做法

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络适配器上。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。

- 在专用于 VMotion 的单独网络上保持 VMotion 连接。在进行 VMotion 迁移时，客户操作系统内存的内容将通过该网络传输。通过使用 VLAN 对单个物理网络分段，或者使用单独的物理网络 （后者为首选），可以实现这一点

装载 NFS 卷

在 ESX Server 3i 中， ESX Server 3i 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 3i 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。以这种方式装载的所有 NFS 卷均显示为 VI Client 中的数据存储。虚拟机配置编辑器允许浏览 ISO 映像的 ESX Server 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络适配器用于特定的网络服务，最轻松的方式是为每种服务创建 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 与环境中的其他部分是隔离开的，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，在 vSwitch 中添加或移除网络适配器。如果移除所有运行中的硬件，虚拟机仍可互相通信。而且，如果保留一个网络适配器原封不动，所有虚拟机仍然可以与物理网络相连。
- 要将虚拟机分组，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。只要所有的适配器正常运行，上述操作也可以使用单独的适配器，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（连接物理网络）的虚拟网络和无上行链路的纯虚拟网络之间路由。

网络疑难解答

本节指导解决常见网络问题。

解决物理交换机配置问题

发生故障切换或故障恢复事件时，有时可能会失去 vSwitch 连接。这会导致与该 vSwitch 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 (portfast trunk)]** 模式。

解决端口组配置问题

更改虚拟机所连接的端口组的名称可能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，因为它已与网络之间建立连接。

最好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 Remote CLI 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

4 存储器简介

存储器一节包含了有关 ESX Server 3i 可用的存储器选项的概述信息，阐述了如何配置 ESX Server 3i 系统以便可以使用和管理不同类型的存储器。

有关存储器管理员可能需要在存储器一侧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》*。

本章包括以下主题：

存储器概述

ESX Server 3i 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 3i 需要专用的存储空间。

ESX Server 3i 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网络连接的存储设备）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 3i 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 3i 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 3i 发现的任何存储设备上预先设置数据存储。

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 69 页）
- “管理存储器”（第 95 页）

数据存储创建后，即可用于存储虚拟机文件。有关创建虚拟机的信息，请参见 *《基本系统管理》*。

物理存储器的类型

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

ESX Server 3i 支持下面的存储设备类型：

- **本地** - 在直接连接 ESX Server 3i 主机的内部或外部存储设备或阵列上存储虚拟机文件。
- **网络连接** - 在位于 ESX Server 3i 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网络连接设备进行通信。

本地存储器

本地存储设备可以是位于 ESX Server 3i 主机内部的内部硬盘，也可以是位于主机之外并直接连接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 3i 进行通信。所需的只是一根连接存储设备的电缆；必要时，ESX Server 3i 主机中需要有一个兼容的 HBA。

通常，可以将多个 ESX Server 3i 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。

许多存储系统支持冗余连接路径以确保容错性能。有关多路径的详细信息，请参见“管理多路径”（第 99 页）。

当多个 ESX Server 3i 主机连接本地存储单元时，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 3i 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 3i 系统间共享 VMFS 卷”（第 59 页）。

ESX Server 3i 支持各种内部或外部本地存储设备，包括 SCSI、 IDE、 SATA 和 SAS 存储系统。无论使用何种存储器类型， ESX Server 3i 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 3i 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 3i 主机提供对相同 LUN （以及相同 VMFS 数据存储）的共享访问。有关信息，请参见 *《ESX Server 3.x 存储器 /SAN 兼容性指南》*，网址是 www.vmware.com/support/pubs/vi_pubs.html。

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。

网络连接的存储器

网络连接的存储设备是 ESX Server 3i 用来远程存储虚拟机文件的外部存储设备或阵列。ESX Server 3i 主机通过高速网络访问这些设备。

ESX Server 3i 支持下面的网络连接存储技术：

- **光纤通道 (FC) SAN** - 在 FC 存储区域网络 (Storage Area Network, SAN) 上远程存储虚拟机文件。FC SAN 是一种将 ESX Server 3i 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 3i 主机应配有光纤通道主机总线适配器 (Host Bus Adapter, HBA)。此外，主机还需要使用帮助路由存储器流量的光纤通道交换机。

- **Internet SCSI (iSCSI) SAN** - 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 3i 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 3i 提供下面的 iSCSI 连接类型：

  - **硬件启动的 iSCSI** - ESX Server 3i 主机通过专用的第三方 HBA （带有基于 TCP/IP 的 iSCSI 功能）连接存储器。
  - **软件启动的 iSCSI** - ESX Server 3i 使用 VMkernel 中基于软件的 iSCSI 代码来连接存储器。通过这种 iSCSI 连接类型，主机只需要使用一个标准的网络适配器来进行网络连接。

- **网络附加存储 (Network-Attached Storage, 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 3i 中内置的 NFS 客户端使用*网络文件系统 (Network File System, NFS)* 协议第 3 版来与 NAS/NFS 服务器进行通信。为了进行网络连接， ESX Server 3i 主机需要使用一个标准的网络适配器。

有关支持的网络连接存储设备的详细信息，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 3i 系统可能需要使用用来连接特定存储设备或网络的适配器。 ESX Server 3i 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 3i 直接通过 VMkernel 中的设备驱动程序访问适配器。

有关 ESX Server 3i 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 来访问 ESX Server 3i 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。有关详细信息，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 3i 数据存储可以具有下面的文件系统格式：

- **VMware 文件系统 (VMware File System, VMFS)** - 针对存储 ESX Server 3i 虚拟机而优化过的特殊高性能文件系统。 ESX Server 3i 可以将 VMFS 部署在任何基于 SCSI 的本地或网络连接存储设备上，包括光纤通道和 iSCSI SAN 设备。

  除了使用 VMFS 数据存储之外，虚拟机还可以使用映射文件 (RDM) 作为代理来直接访问裸设备。有关 RDM 的详细信息，请参见 “裸设备映射”（第 107 页）。

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

VMFS 数据存储

ESX Server 3i 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 3i。*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 3i。

ESX Server 3i 可以将 LUN 格式化为 VMFS 数据存储。VMFS 数据存储主要充当虚拟机的存储库。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。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
- 文件大小上限：2TB
- 块大小：1 MB 到 8 MB

创建和增加 VMFS 数据存储

可以使用 VI Client 预先在 ESX Server 3i 发现的任何基于 SCSI 的存储设备上设置 VMFS 数据存储。ESX Server 3i 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 应始终只具有一个 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 70 页）
- “添加光纤通道存储器”（第 73 页）
- “添加可通过硬件启动器访问的 iSCSI 存储器”（第 83 页）
- “添加可通过软件启动器访问的 iSCSI 存储器”（第 88 页）

创建 VMFS 数据存储以后，可以编辑它的属性。有关详细信息，请参见 “编辑 VMFS 数据存储”（第 97 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 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 3i 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 3i 系统的存储器。

由于以下原因，可能需要数量较少、容量较大的 VMFS 卷：

- 在不向存储器管理员要求更多空间的情况下，使创建虚拟机的灵活性更大。
- 更灵活地调整虚拟磁盘大小、执行快照等等。
- 使要管理的 VMFS 数据存储变得更少。

由于以下原因，可能需要数量较多、容量较小的 VMFS 卷：

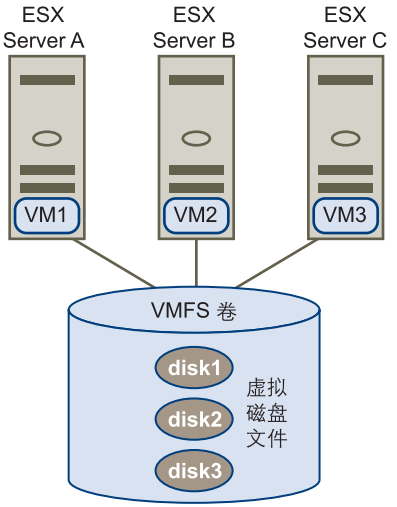
- 由于锁定和 SCSI 预留的问题，对每个 VMFS 数据存储的争用更少。
- 减少浪费的存储空间。
- 不同的应用程序可能需要不同的 RAID 特性。
- 按 LUN 设置多路径策略和磁盘份额时获得更多的灵活性。
- 使用 Microsoft 群集服务要求每个群集磁盘资源位于自己的 LUN 中。

您可能决定将一些服务器配置为使用数量较少、容量较大的 VMFS 卷，而将一些服务器配置为使用数量较多、容量较小的 VMFS 卷。

在 ESX Server 3i 系统间共享 VMFS 卷

作为一个群集文件系统， VMFS 可让多个 ESX Server 3i 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 4-1. 在 ESX Server 3i 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 3i 主机间共享同一个 VMFS 卷具有以下好处：

- 可以使用 VMware DRS 和 VMware HA。

  可以跨越不同的物理服务器分配虚拟机。这意味着，每个特定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。如果发生故障，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 3i 可以访问位于 NAS 服务器上的特定 NFS 卷、装载该卷，以及用它来满足存储需求。可以使用 NFS 卷来存储和引导虚拟机，方式与使用 VMFS 数据存储的方式相同。

ESX Server 3i 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。有关快照的详细信息，请参见 *《基本系统管理》*，网址是 www.vmware.com/support/pubs/。

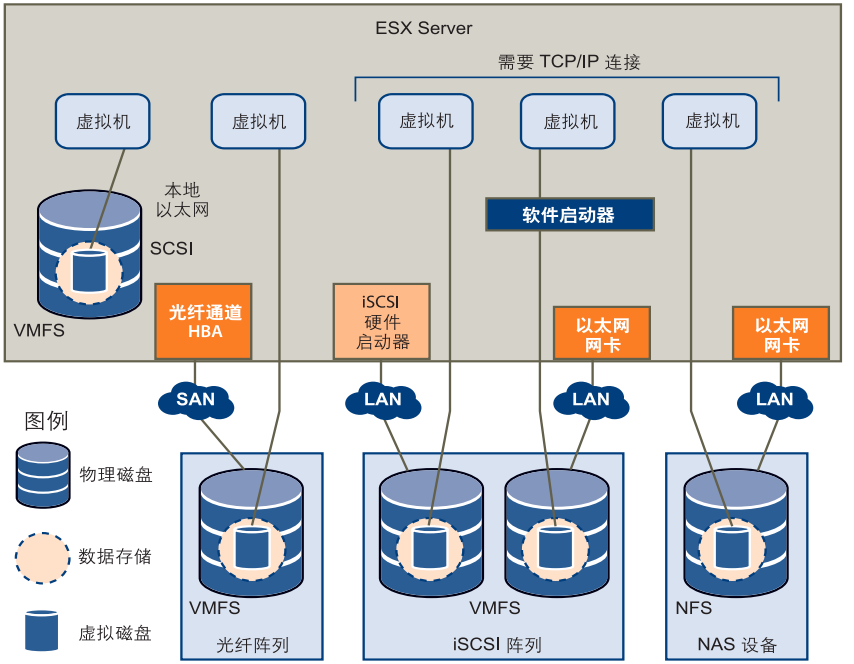
虚拟机如何访问存储器

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 3i 主机用来连接到存储设备的协议，这些命令会封装成其他形式。 ESX Server 3i 支持光纤通道 (Fibre Channel, FC)、 Internet SCSI (iSCSI) 和 NFS 协议。

无论 ESX Server 3i 使用何种类型的存储设备，虚拟磁盘始终会以装载的 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 4-2 中的插图描绘了使用不同存储类型的五个虚拟机，以说明各种类型之间的区别。

图 4-2. 访问不同存储器类型的虚拟机



注意 此插图仅用于对概念进行解释。它并非是建议的配置。

比较存储器类型

表 4-1 比较了 ESX Server 3i 支持的不同网络连接存储技术。

表 4-1. ESX Server 3i 支持的网络连接存储器

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 4-2 比较了不同存储器类型支持的 ESX Server 3i 功能。

表 4-2. 存储器支持的 ESX Server 3i 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 [1]
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 [1]

1 不提供通过光纤通道或 iSCSI SAN 运行的 VCB 卸载功能。

查看 VMware Infrastructure Client 中的存储器信息

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。

显示数据存储

可使用以下方式之一将数据存储添加到 VI Client 中：

- ESX Server 3i 主机首次引导时默认创建 - 首次启动 ESX Server 3i 主机时，软件使用 VMFS 数据存储格式化任何可见的空白本地磁盘或分区，以便在数据存储上创建虚拟机。

  例如，如果您的策略是使用共享存储设备，而不是本地存储器，则可以覆盖此默认行为。为了防止自动格式化磁盘，请在首次启动主机之前，将本地存储设备与主机断开连接。如果已经出现自动格式化磁盘的情况，而您希望覆盖 VMFS 格式，请移除数据存储。

- 当主机添加到清单时发现 - 将新的主机添加到清单中时，VI Client 会显示主机上已经创建的所有数据存储。

- 在可用存储设备上创建 - 可以使用 **[添加存储器 (Add Storage)]** 选项来创建和配置新的数据存储。有关详细信息，请参见 “配置存储器”（第 69 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)]** 链接。

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 64 页）。
- 数据存储使用的文件系统类型。请参见 “数据存储”（第 57 页）。
- 数据存储格式化后的总容量和可用空间。

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 4-3 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)]** 窗格提供有关路径策略、路径数和可用扩展的信息。

图 4-3. 数据存储信息

要查看每个扩展的详细信息，请单击 **[属性 (Properties)]**，然后在 **[扩展 (Extents)]** 面板中进行选择。

可以刷新和移除任何现有的数据存储，以及更改 VMFS 数据存储的属性。编辑 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。有关详细信息，请参见 “管理存储器”（第 95 页）。

了解显示屏幕中的存储设备命名

在 VI Client 中，呈现给 ESX Server 3i 主机的存储设备名称会显示为三个数字的序列，中间用冒号分隔，例如 `vmhba0:0:49`。该名称具有以下含义：

`<HBA>:<SCSI 目标>:<SCSI LUN>`

缩写 `vmhba` 表示 ESX Server 3i 系统上的不同物理 HBA。它也可以表示 ESX Server 3i 使用 VMkernel 网络堆栈实现的软件 iSCSI 启动器。

`vmhba0:0:49` 示例表示，通过 HBA0，ESX Server 3i 主机可以访问 SCSI 目标 0 并使用 VMFS 格式化 LUN49。

在存储设备上创建数据存储之后，设备名称具有下面的格式：

<HBA>:<SCSI 目标 >:<SCSI LUN>:< 磁盘分区 >

第四个数字表示 LUN 上 VMFS 数据存储占用的分区。

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 3i 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 3i 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 3i 主机可见的光纤通道或 iSCSI 目标映射被修改时发生更改。

查看存储适配器

VI Client 可以显示您的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)]** 链接。

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，例如它所连接的存储设备和目标 ID。

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 4-4 中，已选择 iSCSI 存储适配器 “vmhba0”。**[详细信息 (Details)]** 视图提供有关适配器所连接的 LUN 数量以及所使用路径的信息。

如果要更改路径的配置，可以从列表中选择此路径，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。有关管理路径的信息，请参见 “管理多路径”（第 99 页）。

图 4-4. 存储适配器信息

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》*。

请通过以下链接阅读有关特定存储器配置任务的详细信息：

- 本地存储器配置任务：

  “在本地 SCSI 磁盘上创建数据存储”（第 71 页）

- 光纤通道 SAN 存储器配置任务：

  “在光纤通道设备上创建数据存储”（第 73 页）

- 硬件启动的 iSCSI 存储器配置任务：

  - “查看硬件 iSCSI 启动器属性”（第 77 页）
  - “设置硬件启动器的 iSCSI 名称、别名和 IP 地址”（第 79 页）
  - “使用动态发现设置目标发现地址”（第 80 页）
  - “设置硬件启动器的 CHAP 参数”（第 82 页）

5 配置存储器

本章包含有关配置本地存储设备、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*》。

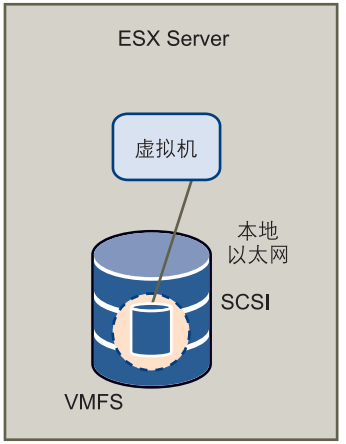
本章包括以下主题：

本地存储器

本地存储器使用基于 SCSI 的设备，如 ESX Server 3i 主机硬盘或任何直接连接 ESX Server 3i 主机的外部专用存储系统。这些外部存储系统称为直接连接存储器 (Direct Attached Storage, DAS)。

图 5-1 描述了使用本地存储器的虚拟机。

图 5-1. 基于 SCSI 的本地存储器



在此本地存储器拓扑示例中，ESX Server 3i 主机使用单一连接来连接存储磁盘。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 3i 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。为确保故障容错，许多本地存储系统支持多个连接路径。有关多路径和 ESX Server 3i 配合使用的详细信息，请参见 “管理多路径”（第 99 页）。

添加本地存储器

加载存储适配器驱动程序后，ESX Server 3i 会立即检测可用的 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 89 页）。

在 SCSI 存储设备上创建数据存储时，**[添加存储器 (Add Storage)]** 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供使用。

10 单击 **[下一步 (Next)]**。

此时将显示 [即将完成 (Ready to Complete)] 页面。

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)]**。

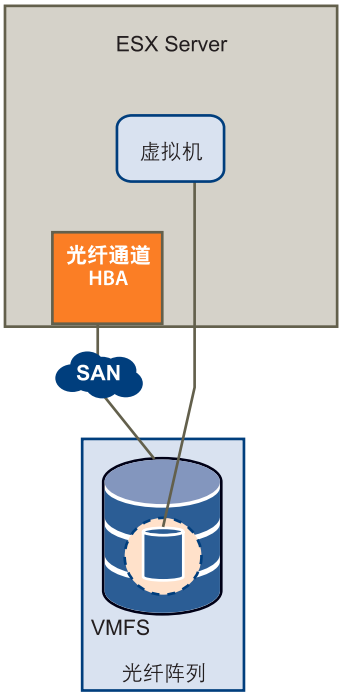
该过程在 ESX Server 3i 主机的基于 SCSI 的本地磁盘上创建数据存储。

光纤通道存储器

ESX Server 3i 支持光纤通道适配器，可通过该适配器将 ESX Server 3i 系统连接至 SAN 并查看 SAN 上的磁盘阵列。

图 5-2 描述了使用光纤通道存储器的虚拟机。

图 5-2. 光纤通道存储器



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

其他信息：

- 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 3i 支持的 SAN 存储设备的详细信息，请参见 *《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 99 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 89 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 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供使用。

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 3i 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 3i 支持 iSCSI 技术，通过该技术 ESX Server 3i 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 3i 主机需要使用 iSCSI 启动器。启动器在 IP 网络上的 ESX Server 3i 系统和目标存储设备之间传输 SCSI 请求和响应。

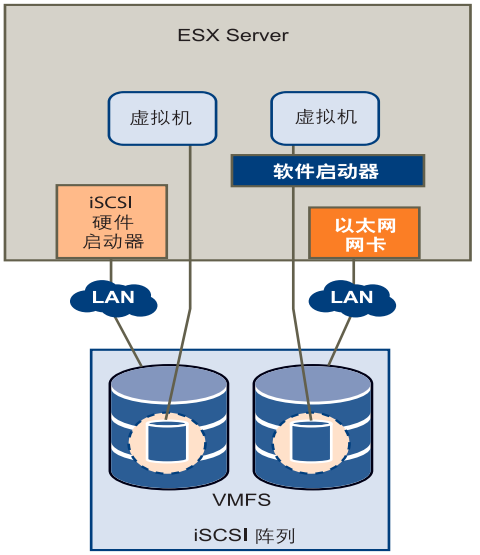
ESX Server 3i 支持基于硬件和软件的 iSCSI 启动器：

- **硬件 iSCSI 启动器** - 带有基于 TCP/IP 的 iSCSI 功能的第三方主机总线适配器 (Host Bus Adapter, 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 3i 系统通过标准网络适配器连接 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。

注意 虚拟机中的客户操作系统无法直接查看 iSCSI 存储器。对客户操作系统而言，可以通过 SCSI HBA 使用连接 ESX Server 3i 系统的 iSCSI 存储器。

图 5-3 描述了两台使用不同类型 iSCSI 启动器的虚拟机。

图 5-3. iSCSI 存储器



在第一个 iSCSI 存储器配置示例中， ESX Server 3i 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 3i 系统配置了软件 iSCS 启动器。使用软件启动器时，ESX Server 3i 系统通过现有网卡连接 LAN。

命名要求

使用 iSCSI 网络的所有 iSCSI 启动器和目标均有唯一的、永久的 iSCSI 名称，并分配有访问地址。 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.<年 – 月>.<转换 _ 域 _ 名>:<唯一 _ 名称>`

  其中， <年 – 月> 代表注册域名时的年份和月份， <转换 _ 域 _ 名> 为正式域名，而 <唯一 _ 名称> 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，此名称为 24 位，对于诸如序列号之类的唯一 ID，却为 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 3i 系统使用以下发现方法：

- **动态发现** - 使用这种方法 （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** - 使用这种方法，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 3i 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 3i 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 147 页）。

配置硬件 iSCSI 启动器和存储器

ESX Server 3i 主机通过硬件启动器访问 iSCSI 存储器时，使用能够通过 TCP/IP 访问 iSCSI 存储器的专用第三方适配器。此 iSCSI 适配器负责 ESX Server 3i 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信息，请参见 VMware 网站 www.vmware.com/cn 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 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 89 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 75 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，一些存储设备不能识别硬件 iSCSI 启动器。

3 输入 iSCSI 别名。

别名是用于识别硬件 iSCSI 启动器的名称。

4 在 [硬件启动器属性 (Hardware Initiator Properties)] 组中输入所有需要的值。

5 单击 **[确定 (OK)]** 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

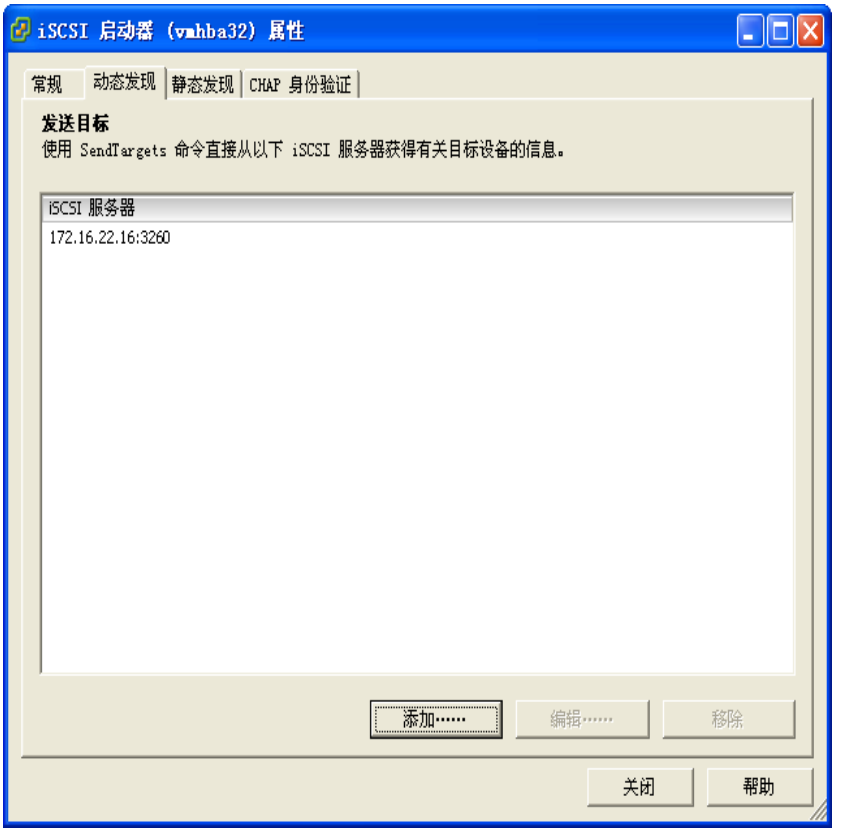
设置目标发现地址，以便硬件启动器确定网络上可供访问的存储器资源。可以通过动态发现或静态发现来进行此设置。

请参见 “发现方法”（第 76 页）

采用动态发现时，特定的 iSCSI 服务器会向 ESX Server 3i 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 3i 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 3i 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 3i 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。

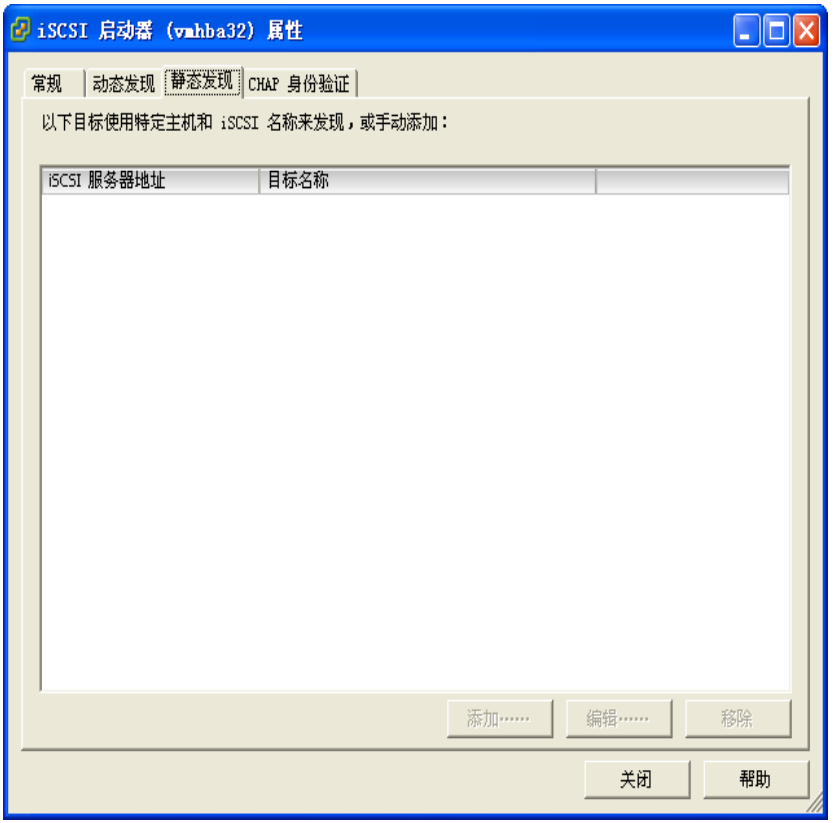
4 要更改 iSCSI 的 IP 地址或移除服务器，请选择 IP 地址并单击 **[编辑 (Edit)]** 或 **[移除 (Remove)]**。

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 3i 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 地址和完全限定名称。

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

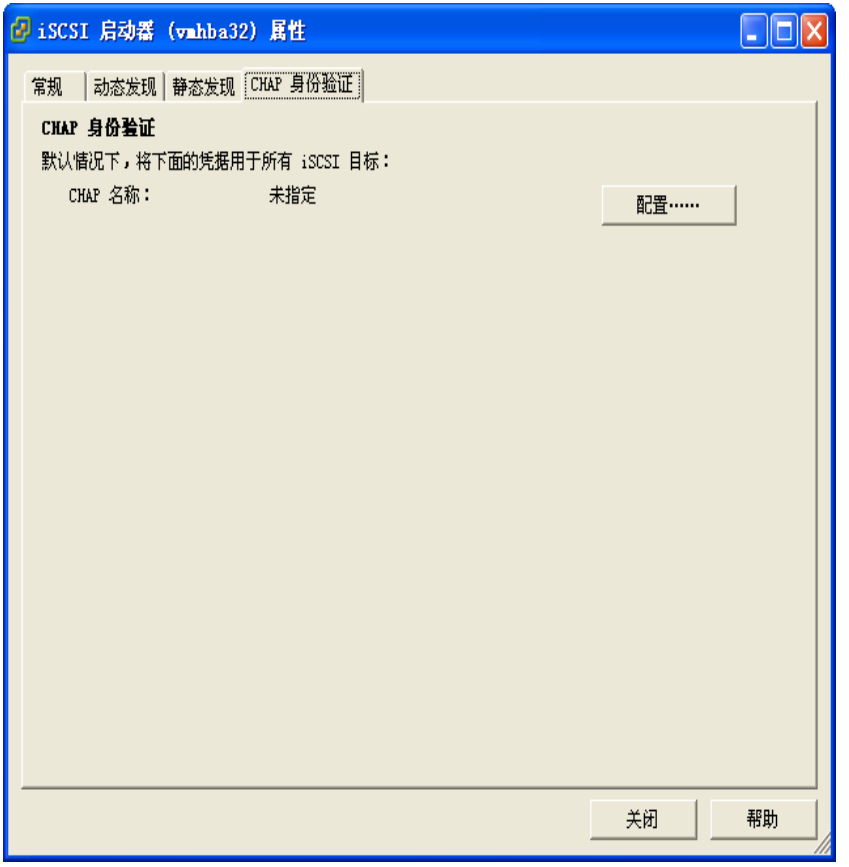
配置硬件 iSCSI 启动器时，应验证是否在 iSCSI 存储器上启用了 CHAP。如果已启用，则需要为启动器启用 CHAP，确保 CHAP 身份验证凭据与 iSCSI 存储器匹配。

请参见 “iSCSI 安全”（第 76 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)]** 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 3i 主机或存储系统强制注销时。之后，您不能再连接需要 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 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 3i 系统连接至 IP 网络上的远程 iSCSI 目标。VMkernel 中嵌入的 ESX Server 3i 软件 iSCSI 启动器为该连接提供了便利，因为它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，然后安装并配置软件 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 29 页）。

2 配置软件 iSCSI 启动器。

请参见 “配置软件 iSCSI 启动器”（第 86 页）。

3 重新扫描新的 iSCSI LUN。

请参见 “重新执行扫描”（第 89 页）。

4 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 88 页）。

查看软件 iSCSI 启动器

ESX Server 3i 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 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)]**。

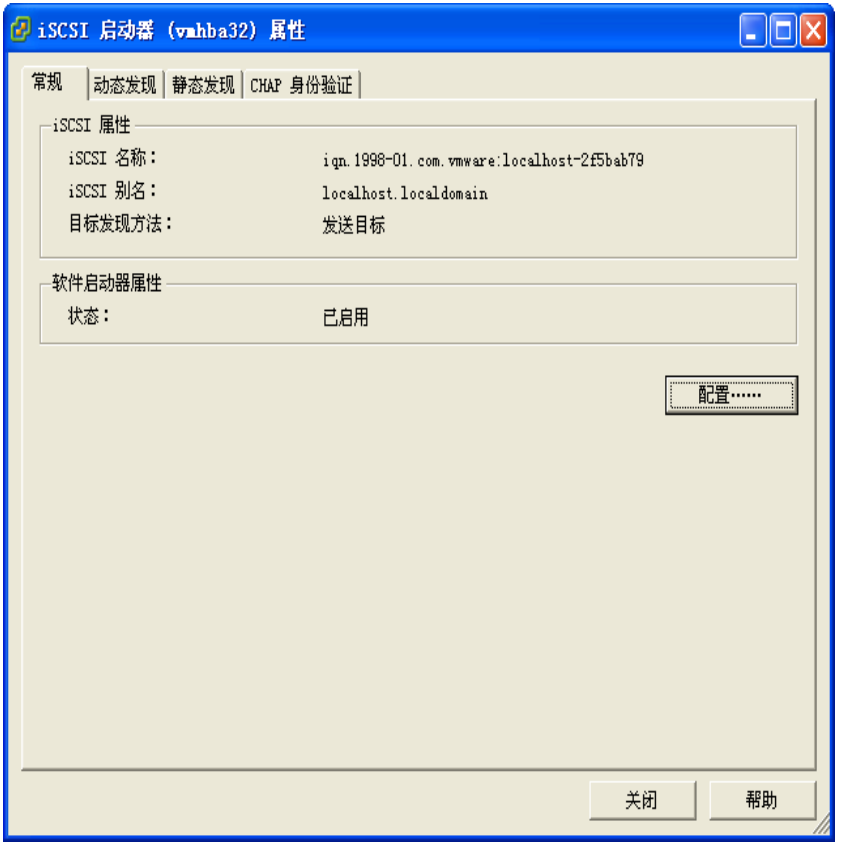
此时会显示可用存储适配器的列表。

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 3i 的存储设备列表上。请参见 “重新执行扫描”（第 89 页）。

启用软件 iSCSI 启动器

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

启用软件 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启动器。请参见“命名要求”（第 75 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 76 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 要添加新的 iSCSI 服务器以供 ESX Server 3i 主机用于动态发现会话，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，应验证是否在 iSCSI 存储器上已启用 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 76 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 3i 主机或存储系统强制注销时。之后，您不能再连接需要 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 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)]**。

此时将显示 [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)]**。

该操作在通过软件启动器访问的 iSCSI 存储设备上创建数据存储。

12 单击 **[刷新 (Refresh)]**。

重新执行扫描

如果发生以下事件，请重新执行扫描：

- 对可供 ESX Server 3i 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，应重新扫描所有具有指向 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 panel)] 面板上方的 **[重新扫描 (Rescan)]**。

注意 也可右键单击单个适配器，并单击 **[重新扫描 (Rescan)]** 以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 将显示在磁盘 /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)]**。

新发现的数据存储将显示在数据存储列表上。

网络附加存储

本节包含有关网络附加存储 (NAS) 的信息。

ESX Server 3i 支持通过 NFS 协议使用 NAS。

虚拟机如何使用 NFS

ESX Server 3i 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 3i 中嵌入的 NFS 客户端可让您访问 NFS 服务器和使用 NFS 卷来存储虚拟机磁盘。 ESX Server 3i 仅支持 TCP 上的 NFS 版本 3。

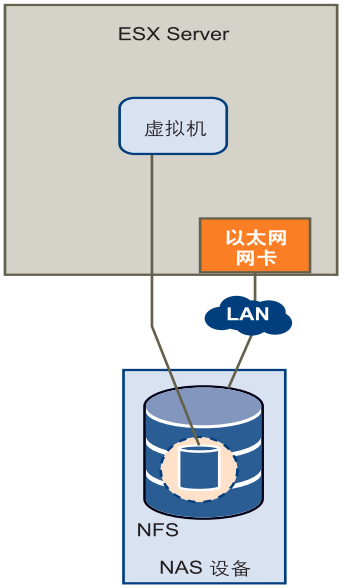
可使用 VI Client 将 NFS 卷配置为数据存储。已配置的 NFS 数据存储会显示在 VI Client 中，可用来存储虚拟磁盘文件，使用方式与基于 VMFS 的数据存储相同。

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，关闭虚拟机。

图 5-4 描述使用 NFS 卷存储其文件的虚拟机。

图 5-4. NFS 存储器



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

警告 当 ESX Server 3i 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，以防止其他 ESX Server 3i 主机访问该虚拟磁盘文件。不要移除 `.lck-XXX` 锁文件，否则，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（称为委派用户）分配 NFS 访问特权。

默认情况下， ESX Server 3i 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，并且会拒绝 ESX Server 3i 主机访问存储在 NFS 卷上的虚拟机文件。

可通过 ESX Server 3i 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 3i 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 168 页）。

警告 更改 ESX Server 3i 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 3i 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 29 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 (Add Storage)]** 向导将指导您完成所有配置步骤。

装载 NFS 卷

1 登录 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

要运行 ESX Server 3i，需要配置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 3i 主机均必须拥有 100 MB 的诊断分区。如果多个 ESX Server 3i 主机共享一个 SAN，请为每个主机配置一个内存为 100 MB 的诊断分区。

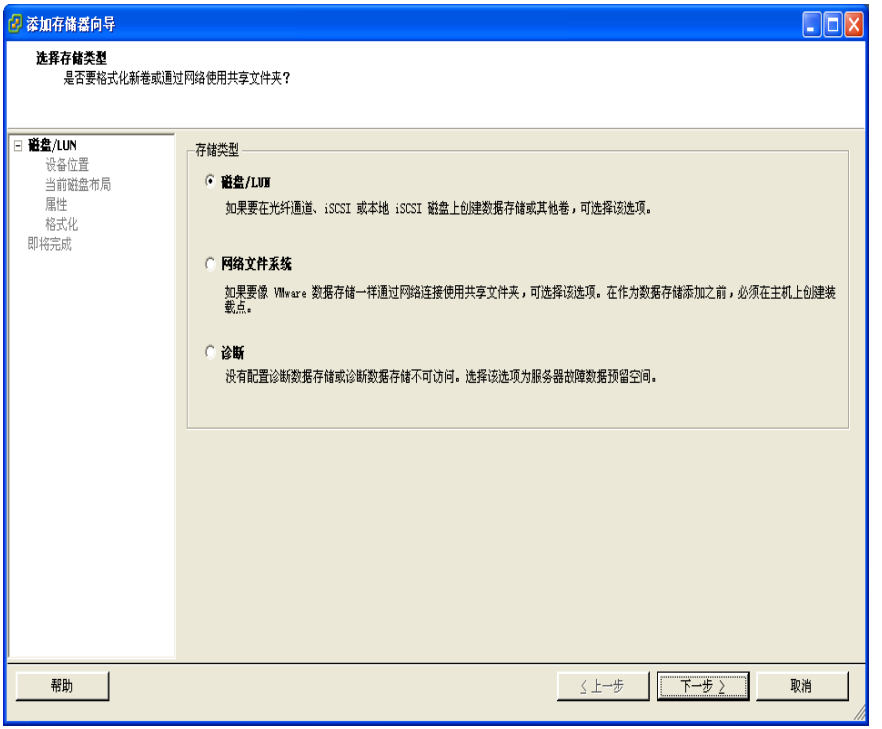
创建诊断分区

1 登录 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)]**。

此时将显示 [选择存储类型 (Select Storage Type)] 页面。



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 3i 主机已拥有诊断分区。可使用命令行界面中的 `vicfg-dumppart` 命令对主机的诊断分区进行查询和扫描。请参见 “使用 vicfg-dumppart 管理诊断分区”（第 206 页）。

5 指定诊断分区类型：

- **专用本地存储器** - 在本地磁盘上创建诊断分区。此分区将仅存储 ESX Server 3i 主机的故障信息。

- **专用 SAN 存储器** - 在非共享 SAN LUN 上创建诊断分区。此分区将仅存储 ESX Server 3i 主机的故障信息。
- **共享 SAN 存储器** - 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可以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)]**。

6 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。本章包括以下各节：

管理数据存储

ESX Server 3i 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 NAS）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。有关 RDM 的详细信息，请参见 “裸设备映射”（第 107 页）。

有关数据存储的详细信息，请参见 “数据存储”（第 57 页）。

可使用以下两种方式之一将数据存储添加到 VI Client 中：

- ESX Server 3i 主机首次引导时默认创建 - 首次启动 ESX Server 3i 主机时，软件使用 VMFS 数据存储格式化任何可见的空白本地磁盘或分区，以便在数据存储上创建虚拟机。
- 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。

数据存储创建后，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。

可移除不使用的数据存储。

小心 从 ESX Server 3i 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 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 VMFS-2 数据存储，可将其升级到 VMFS-3 格式。

升级数据存储

ESX Server 3i 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 升级为 VMFS-3 时， ESX Server 3i 文件锁定机制可确保无远程 ESX Server 或本地进程访问转换中的 VMFS 卷。 ESX Server 3i 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 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。

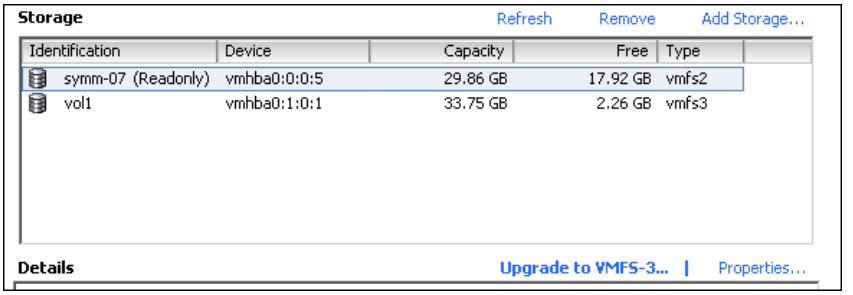
要升级 VMFS-2 文件系统，其文件块大小不应超过 8 MB。

将 VMFS-2 升级到 VMFS-3

1 登录 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 单击使用了 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 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)]**。

此时将打开 [属性 (Properties)] 对话框。

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 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，并释放它包含的文件系统和任何数据。

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 3i 主机和直接连接或网络连接的存储器之间的不间断连接， ESX Server 3i 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 3i 主机和外部存储设备之间传输数据。在路径上的任何元素（HBA、交换机、存储处理器 (SP) 或电缆）发生故障时， ESX Server 3i 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*。使用故障切换路径有助于确保 ESX Server 3i 系统和存储设备之间的不间断流量。 ESX Server 3i 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 3i 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 3i 遵循以下多路径策略：

- **[最近使用 (Most Recently Used)]** - ESX Server 3i 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”策略；在此类阵列中，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 3i 主机始终使用指向存储设备的特定首选路径作为活动路径。如果 ESX Server 3i 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。首选路径可用后，主机就会自动恢复到首选路径。

  VMware 建议将 “固定的”策略用于*主动 / 主动*存储阵列；在此类阵列中，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 3i 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。

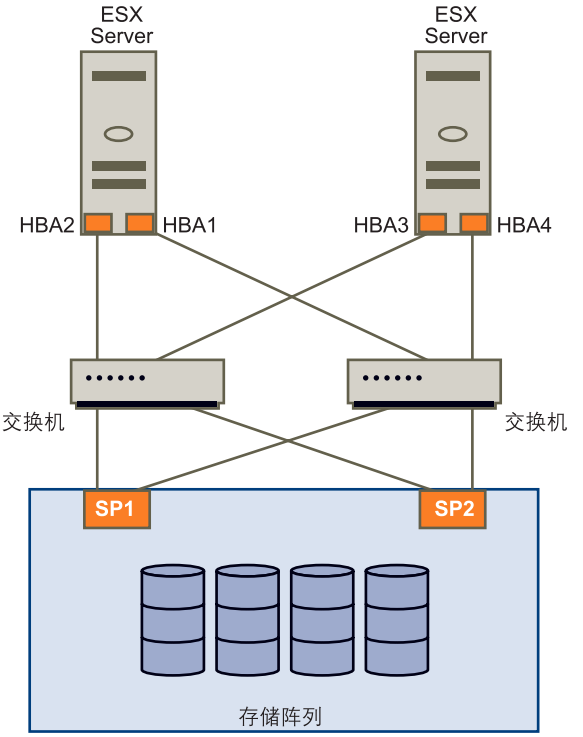
本地存储和光纤通道 SAN 中的多路径

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 3i 主机。ESX Server 3i 主机通过两根电缆连接双端口本地存储系统。使用该配置时，如果 ESX Server 3i 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 3i 主机通常具有两个或更多个可用的 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 6-1 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 会替代 HBA1 并提供服务器和交换机之间的连接。一个 HBA 替代另一个 HBA 的过程称为 HBA 故障切换。

图 6-1. 光纤通道多路径



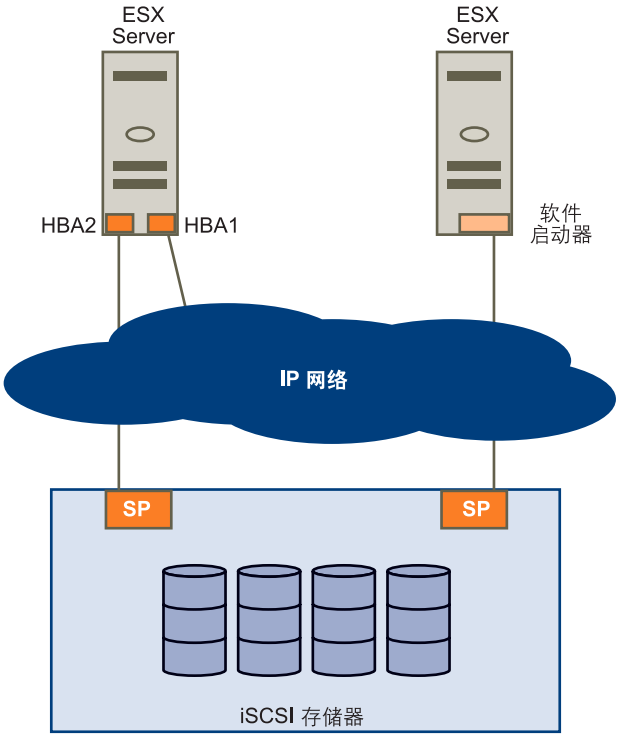
类似地，如果 SP1 或 SP1 和交换机之间的链路中断，SP2 会替代 SP1 并提供交换机和存储设备之间的连接。此过程称为 SP 故障切换。ESX Server 3i 通过多路径功能支持 HBA 和 SP 故障切换。

有关光纤通道存储器中多路径的详细信息，请参见 *《光纤通道 SAN 配置指南》*。

iSCSI SAN 中的多路径

在 iSCSI 存储器中， ESX Server 3i 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 6-2 所示。通过动态发现， iSCSI 启动器获得目标地址列表，启动器可以使用这些地址作为指向 iSCSI LUN 的多条路径来实现故障切换。

图 6-2. iSCSI 多路径



此外，借助软件启动的 iSCSI，可以使用网卡成组，以便通过 VMkernel 中的网络层执行多路径操作。有关详细信息，请参见 “网络”（第 19 页）。

有关 iSCSI 中多路径的详细信息，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 VMware 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的总数，以及是否有任何路径已断开或已禁用。

4 单击 **[属性 (Properties)]**。

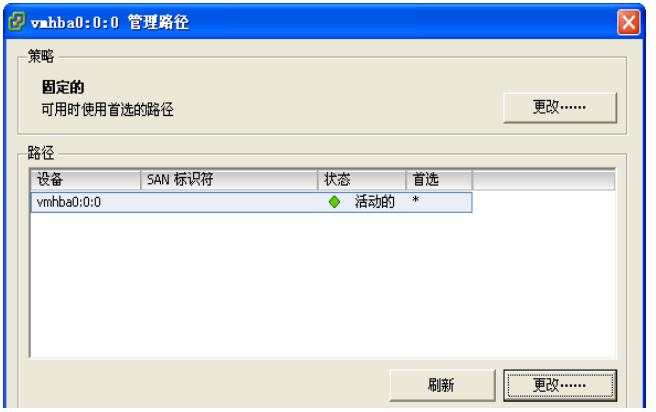
此时会打开选定数据存储的 [卷属性 (Volume Properties)] 对话框。

[扩展设备 (Extent Device)] 面板包括的信息涵盖 ESX Server 3i 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当前用于传输数据的路径。
- **[已禁用 (Disabled)]** - 路径已禁用，无法传输数据。
- **[备用 (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磁盘。

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

如果使用 **[固定的 (Fixed)]** 路径策略，可以看到哪一条路径是首选路径。首选路径的第四列标有一个星号 (*)。

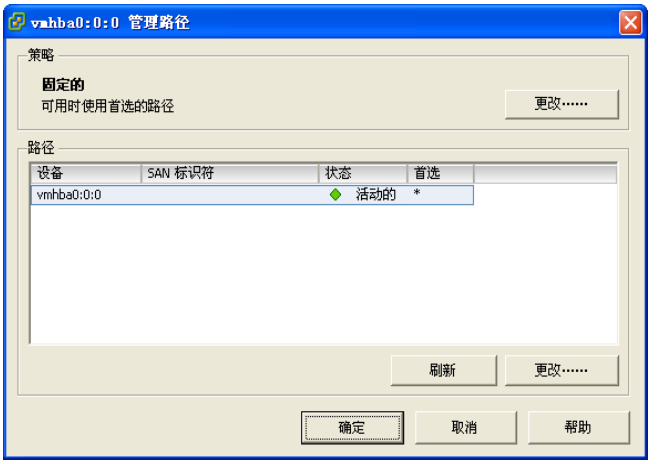


可以使用 [管理路径 (Manage Paths)] 对话框来启用或禁用路径、设置多路径策略，以及指定首选路径。

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。

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



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 (Round Robin)]**

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 （用于 “固定的”多路径策略）

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

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

5 选择 **[已禁用 (Disabled)]** 以禁用路径。

6 单击 **[确定 (OK)]** 两次，以保存更改并退出对话框。

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 3i 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 Remote CLI”（第 221 页）。

7 裸设备映射

裸设备映射 (Raw Device Mapping, 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。

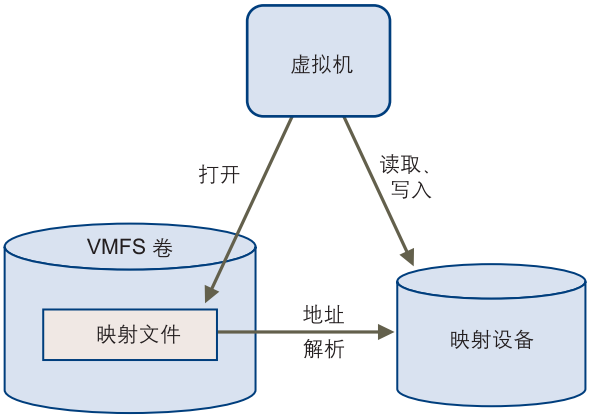
本章将讨论以下主题：

关于裸设备映射

RDM 是 VMFS 卷中的映射文件，它可充当原始物理设备的代理，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存储”、“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 7-1. 裸设备映射



尽管对于大多数虚拟磁盘存储器，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 7-1）。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：

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

RDM 有两种可用兼容性模式：

- 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** - RDM 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：

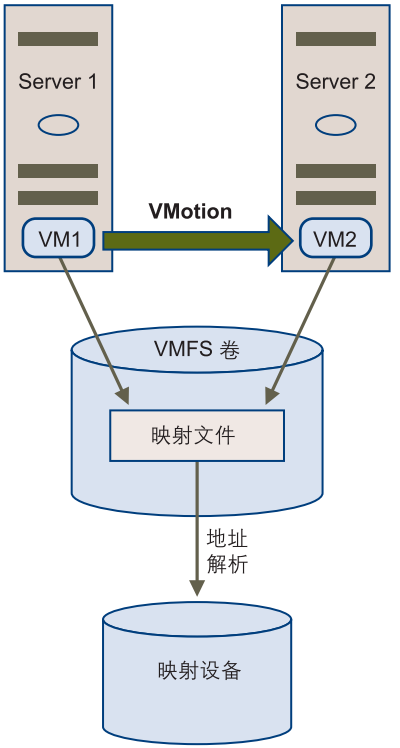
  `/vmfs/volumes/myVolume/myVMDirectory/myRawDisk.vmdk`

- **动态名称解析** - RDM 存储每一映射设备唯一的标识信息。 VMFS 文件系统将每一个 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** - RDM 使得有可能使用针对原始 SCSI 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** - RDM 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** - RDM 可以实现将文件系统实用程序与映射的卷配合使用，将映射文件用作代理。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** - RDM 可以实现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** - RDM 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 7-2。

图 7-2 使用裸设备映射的虚拟机的 VMotion



- **SAN 管理代理** - RDM 令在虚拟机内运行某些 SAN 管理代理成为可能。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 (N-Port ID Virtualization, NPIV)** - RDM 可使用 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，单个 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 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 3i 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，以便能够直接访问 SCSI 设备。

各种管理产品都可以集中 （而非在 ESX Server 3i 计算机上）运行，其他产品则可以在虚拟机中良好运行。 VMware 不正式认可这些应用程序或者提供兼容性列表。要了解在 ESX Server 3i 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：

- **不可用于块设备或特定 RAID 设备** - RDM 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，因此它们不能与 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。 ESX Server 3i 使用 VMFS-3 文件系统。如果有 VMFS-2，需要将其升级到 VMFS-3 才能使用它所存储的文件。
- **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。

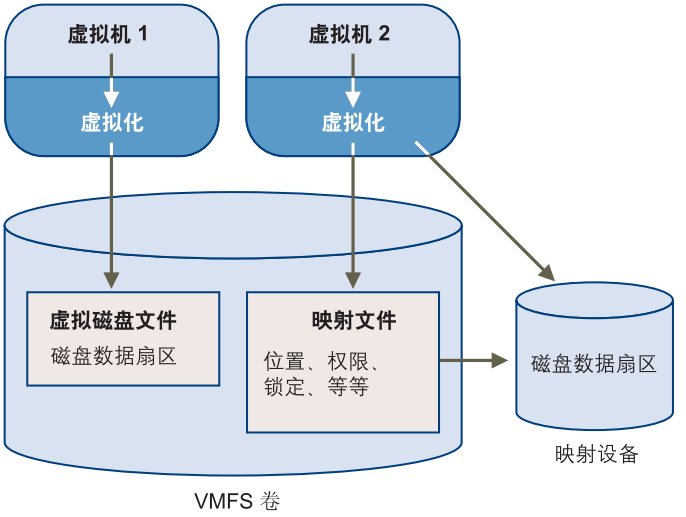
  但是，在虚拟模式下，可以使用快照。有关兼容模式的详细信息，请参见 “虚拟兼容模式与物理兼容模式比较”（第 112 页）。
- **无分区映射** - RDM 需要映射设备是完整的 LUN。不支持映射到分区。

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 7-3. 映射文件元数据

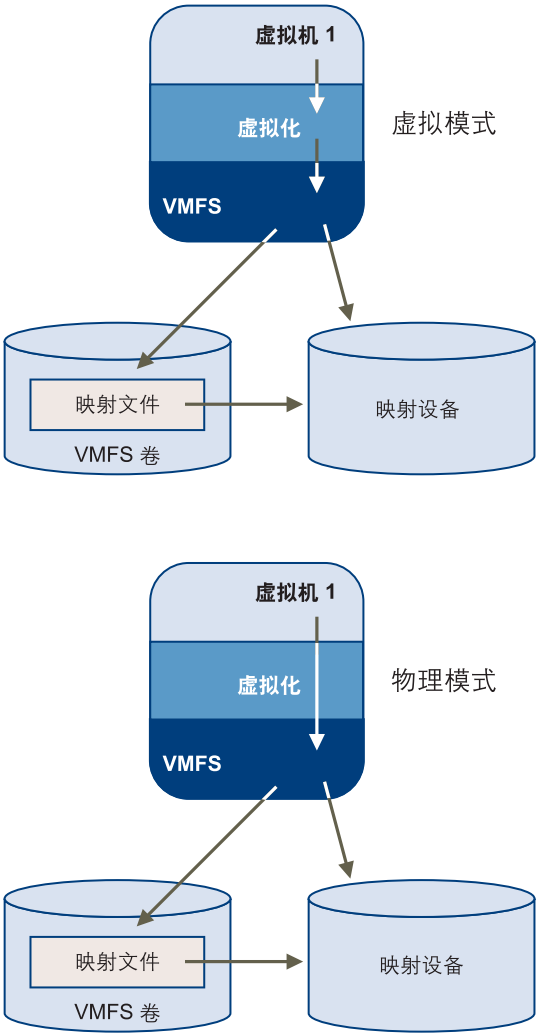


虚拟兼容模式与物理兼容模式比较

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 7-4. 虚拟兼容模式和物理兼容模式

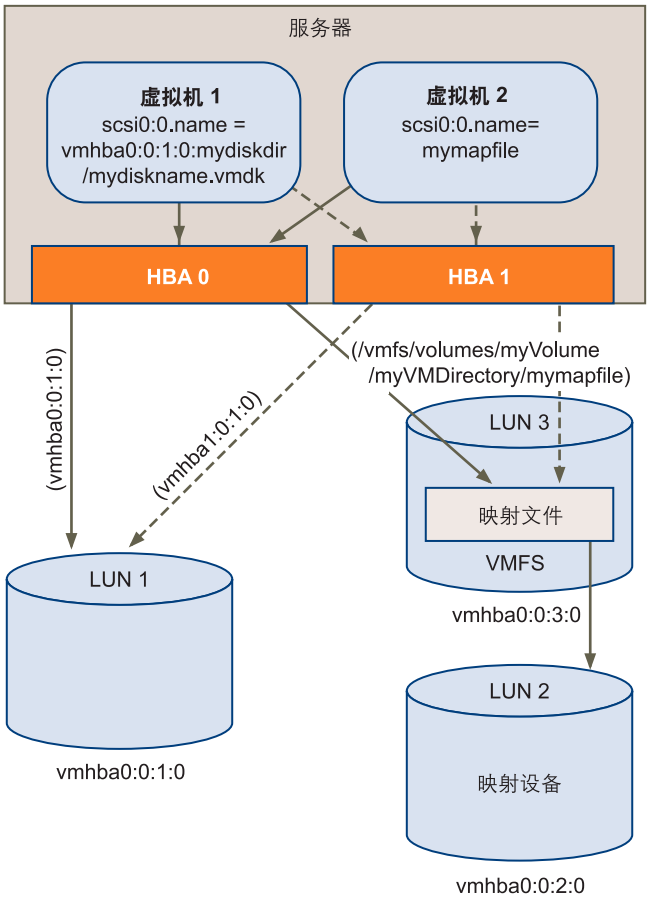


动态名称解析

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

图 7-5 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 7-5. 名称解析示例

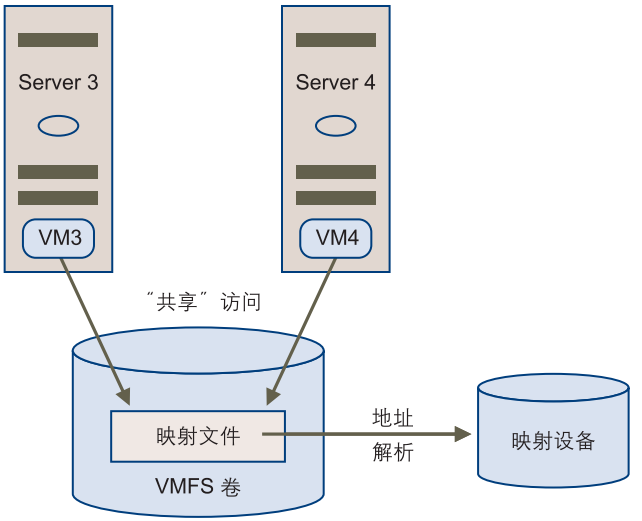


所有映射的 LUN 都由 VMFS 唯一识别，标识存储在其内部数据结构中。SCSI 路径的任何更改，例如光纤通道交换机故障或添加新的主机总线适配器，都可能更改 vmhba 设备名称，因为该名称包括路径标识 （启动器、目标、 LUN）。动态名称解析可通过调整数据结构，使 LUN 与新的设备名称重新对应，从而弥补这些更改。

虚拟机群集的裸设备映射

对于故障切换情况，必须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 7-6. 从群集式虚拟机进行访问



有关配置群集的详细信息，请参见 *《Microsoft 群集服务的设置》*和 *《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 7-1 提供了对不同模式可用功能的快速比较。

表 7-1. 虚拟磁盘和裸设备映射的可用功能

ESX Server 3i 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[1]
VirtualCenter 支持	是	是	是
快照	是	是	否
分布式锁定	是	是	是
群集	仅 CIB[2]	CIB、CAB[3、4]	CAB 和 N+1[5]

表 7-1. 虚拟磁盘和裸设备映射的可用功能

ESX Server 3i 功能	虚拟磁盘文件	虚拟模式 RDM	物理模式 RDM
基于 SCSI 目标的软件	否	否	是

1 不传递 REPORT LUNS

2 CIB = 机箱内群集

3 CAB = 跨机箱的群集

4 VMware 建议使用 CIB 的虚拟磁盘文件。如果 CIB 群集将重新配置为 CAB 群集，请使用 CIB 的虚拟模式 RDM。有关群集的详细信息，请参见 *《Microsoft 群集服务的设置》* 和 *《资源管理指南》*。

5 N+1 = 物理到虚拟群集

管理映射的 LUN

可用于管理映射的 LUN 及其 RDM （映射文件）的工具包括 VI Client 和 `vmkfstools` 实用程序。

VMware Infrastructure Client

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

用 RDM 创建虚拟机

当您授予虚拟机对原始 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映射的 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 存储器的详细信息，请参见 *《光纤通道 SAN 配置指南》* 或 *《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，也可以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：物理或虚拟。

- **[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，也不能迁移 （如果迁移需复制磁盘）。
- **[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，对该磁盘的更改会丢弃。

8 单击 **[下一步 (Next)]**。

9 在 [即将完成新虚拟机 (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 从清单面板中选择虚拟机。

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

4 单击 **[添加 (Add)]**。

5 在添加硬件向导中，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，以完成 RDM 创建工作。

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 从清单面板中选择虚拟机。

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

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)]**。

此时将打开 [管理路径 (Manage Paths)] 对话框。

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 105 页）
- “设置首选路径 （用于 “固定的” 多路径策略）”（第 105 页）
- “禁用路径”（第 105 页）

vmkfstools 实用程序

可以使用 `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。

有关详细信息，请参见 “使用 vmkfstools Remote CLI”（第 221 页）。

安全

8 ESX Server 3i 系统的安全

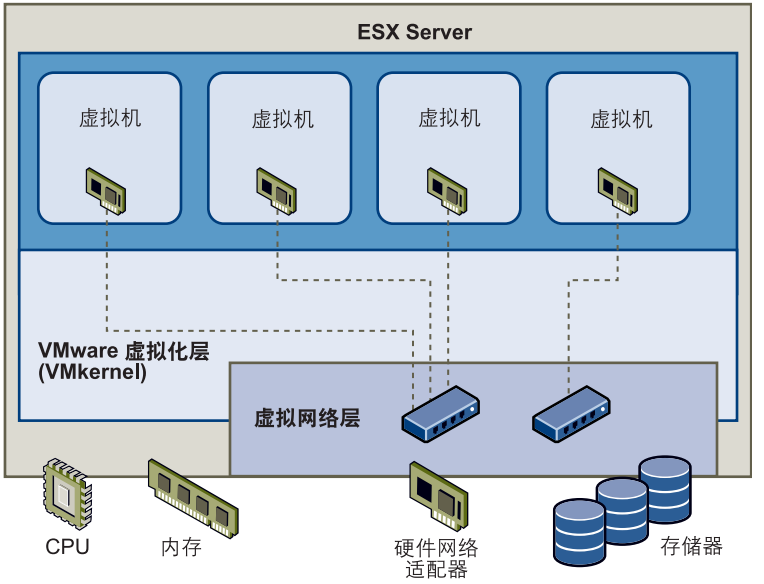
ESX Server 3i 的开发注重于加强安全。本节概述了 VMware 如何确保 ESX Server 3i 环境中的安全，从安全角度阐述了系统架构并提供了附加安全资源的列表。

本章将讨论以下主题：

ESX Server 3i 架构和安全功能

从安全角度而言， VMware ESX Server 3i 主要由三个组件组成：虚拟化层、虚拟机和虚拟网络层。图 8-1 对这些组件进行了概述。

图 8-1. ESX Server 3i 架构



每个组件及此全面架构旨在确保 ESX Server 3i 系统的整体安全。

安全和虚拟化层

虚拟化层 (VMkernel) 是完全由 VMware 设计用来运行虚拟机的内核。它对 ESX Server 3i 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

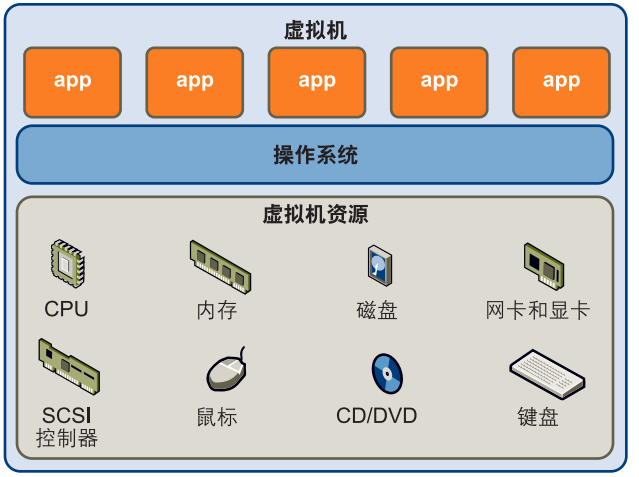
虚拟机是运行应用程序和客户操作系统的容器。所有的 VMware 虚拟机均需设计为互相隔离。如果没有 ESX Server 3i 系统管理员明确授予的特权，则即使是在虚拟机客户操作系统上具有系统管理员特权的用户，也无法突破该隔离层来访问另一台虚拟机。

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，又保证性能不受干扰。例如，如果虚拟机中运行的客户操作系统崩溃，同一 ESX Server 3i 主机上的其他虚拟机还会继续运行。客户机操作系统崩溃不影响：

- 用户访问其他虚拟机的能力
- 运行的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，单个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 8-2 中所示。

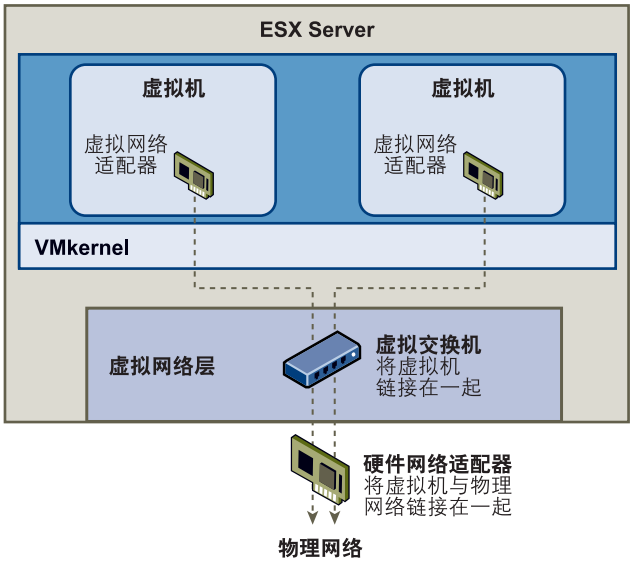
图 8-2. 虚拟机隔离



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该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 3i 主机上运行的其他虚拟机进行通信。而且，虚拟机仅通过物理网络适配器与物理网络 （包括其他 ESX Server 3i 主机上的虚拟机）进行通信，如图 8-3 中所示。

图 8-3. 通过虚拟交换机建立的虚拟网络



鉴于虚拟机在网络中互相隔离的情况，可以应用下列规则：

- 如果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。
- 如果未为虚拟机配置物理网络适配器，则该虚拟机与所有物理网络完全隔离。
- 如果使用了与保护物理机相同的安全措施 （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 3i 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 3i 中可用的精细资源控制，来对虚拟机进行配置，使其获得的 ESX Server 3i 主机 CPU 资源始终不少于 10%，但也决不超过 20%。

资源预留和限制可防止虚拟机的性能因其他虚拟机消耗过多的共享硬件资源而降低。例如，如果 ESX Server 3i 主机上的一台虚拟机由于受到拒绝服务 (Denial-Of-Service, DOS) 攻击而出现故障，该虚拟机上的资源限制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 3i 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其他系统组件使用。此默认行为在一定程度上为防止 DOS 攻击提供了自然保护。如果要定制默认行为，以避免在虚拟机配置之间均匀分布资源预留量和限制量，可逐一设置特定的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》*。

安全和虚拟网络层

虚拟网络层由虚拟网络设备组成，虚拟机可通过这些设备与其他网络连接。ESX Server 3i 通过虚拟网络层来支持虚拟机与其用户之间的通信。此外，ESX Server 3i 主机可使用虚拟层与 iSCSI SAN 和 NAS 存储器等进行通信。虚拟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 3i 还支持可用于为虚拟机网络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接收 / 发送数据包，除非它们位于同一 VLAN 上。

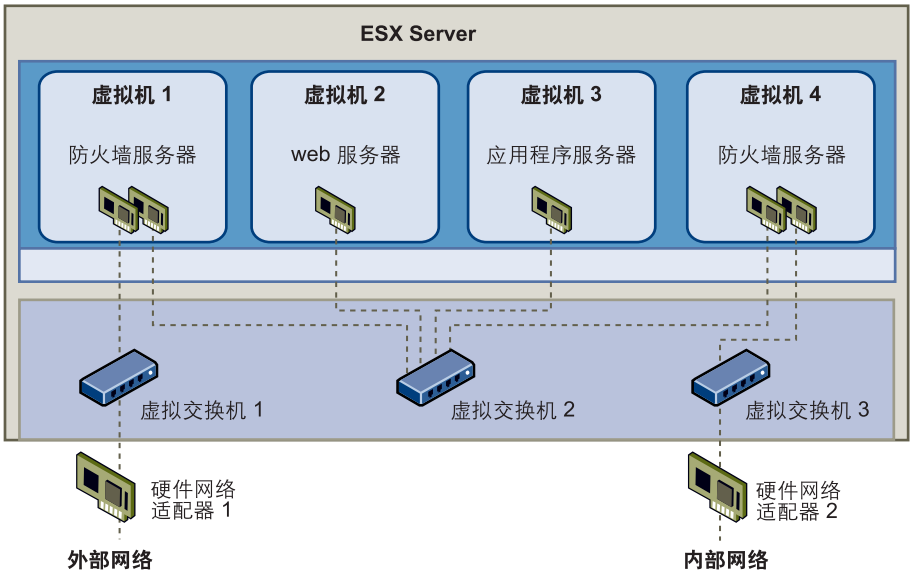
可参考以下示例，以了解如何使用虚拟交换机实施诸如 DMZ 之类的安全工具并在同一 ESX Server 3i 主机内的不同网络上配置虚拟机。

有关虚拟交换机和 VLAN 如何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 140 页）。

示例：在单台 ESX Server 3i 主机内创建网络 DMZ

如何利用 ESX Server 3i 隔离和虚拟网络功能来配置安全环境的一个示例是，在单台 ESX Server 3i 主机上创建网络隔离带 (Demilitarized Zone, DMZ)，如 图 8-4 中所示。

图 8-4. 在单台 ESX Server 3i 主机内配置的 DMZ



此配置包括为在*虚拟交换机 2* 上创建一个虚拟 DMZ 的而创建的四个虚拟机。*虚拟机 1* 和*虚拟机 4* 运行防火墙并通过虚拟交换机连接虚拟适配器。这两个虚拟机都是多址的。在其他两个虚拟机当中，*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。如果防火墙认可流量，则流量路由到 DMZ 中的虚拟交换机 （*虚拟交换机 2*）。由于 Web 服务器和应用程序服务器也连接此交换机，因此它们可以为外部请求提供服务。

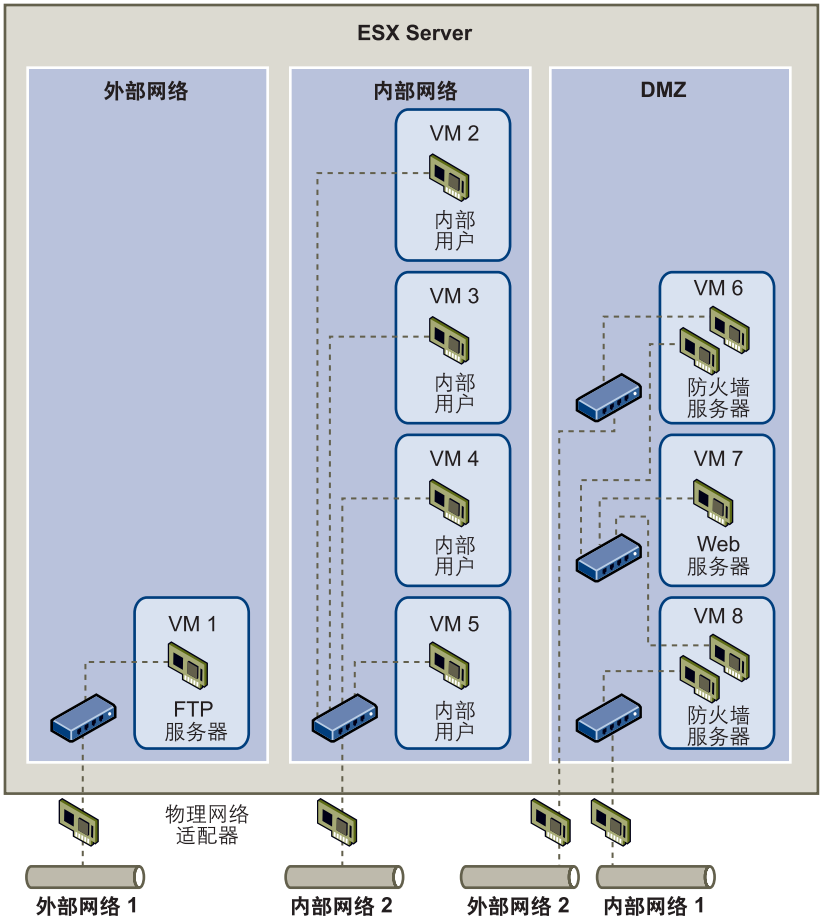
虚拟交换机 2 也连接*虚拟机 4*。此虚拟机在 DMZ 和内部企业网络之间提供了防火墙。此防火墙对 Web 服务器和应用程序服务器的数据包进行筛选。验证后的数据包将通过*虚拟交换机 3* 路由至*硬件网络适配器 2*。*硬件网络适配器 2* 连接内部企业网络。

在单台 ESX Server 3i 内创建 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媒介或成为其他类型攻击的目标。可以认为 DMZ 中虚拟机的安全等同于连接同一网络中的独立物理机。

示例：在单台 ESX Server 3i 主机中创建多个网络

ESX Server 3i 系统的设计可让您将一些虚拟机组连接内部网络，将一些虚拟机组连接外部网络，再将另一些虚拟机组同时连接外部网络和内部网络 - 这一切都在同一 ESX Server 3i 主机内进行。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 8-5 中所示。

图 8-5. 单台 ESX Server 3i 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 3i 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* 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的数据的服务器。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 3i 主机上配置的 FTP 服务器。

由于*虚拟机 1* 没有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。这样可防止嗅探攻击（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给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*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，这些虚拟机不能通过其他的虚拟机网络收发数据包。与此相似，主机的其他虚拟机不能在*虚拟机 2 - 5* 内收发数据包。

- **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。

  有关使用虚拟机配置 DMZ 的示例，请参见 “示例：在单台 ESX Server 3i 主机内创建网络 DMZ”（第 125 页）。

通过利用虚拟机隔离、正确配置虚拟交换机及保持网络隔离，系统管理员可在同一 ESX Server 3i 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的风险。虚拟交换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：

- 虚拟交换机连接同一物理 LAN。
- 虚拟交换机连接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 中的网络交换机布局，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 23 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 的前后和后端安装了软件防火墙，确保 ESX Server 3i 主机受到物理防火墙的保护，并配置了联网的存储器资源以便使每个资源均有其自身的虚拟交换机，从而为 ESX Server 3i 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，可找到有关安全主题的其他信息。

表 8-1. 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	http://www.vmware.com/vmtn/technology/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”中作出了解决其产品中可能存在的漏洞之承诺。
VMware 产品认证	http://www.vmware.com/security/ 在该网站上搜索 “VMware”一词，以查看特定 VMware 产品的认证状态。
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 3i 兼容性指南》，可找到 ESX Server 3i 支持的代理、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。请牢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 3i 配置的安全性

9

本章介绍一些为 ESX Server 3i 主机、虚拟机和 iSCSI SAN 创造安全环境的应采取的措施。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。

本章包括以下主题：

用防火墙确保网络安全

安全管理员使用防火墙防止网络或网络中的选定组件受到侵袭。防火墙根据一套标准，允许或拒绝消息通过，从而控制网络流量。例如，某些防火墙只允许流量通过指定的一组端口。对运行许多服务以及发送和接收大量不同网络流量的服务器而言，防火墙特别有用。

某些版本的 ESX Server 包括防火墙，但 ESX Server 3i 不包括防火墙。这是因为， ESX Server 3i 运行一组限制的已知服务，并且 ESX Server 3i 会阻止添加其他服务。这样的限制使得需要防火墙的因素大为减少。

由于 ESX Server 3i 中没有集成防火墙，因此 VMware 建议部署一套满足需求的安全技术。例如，可以选择安装防火墙来筛选进入和离开安装有 ESX Server 3i 的网络段的流量。

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 3i 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 3i 配置中使用防火墙取决于计划如何使用网络以及任何给定组件所需的安全度。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，那么两台虚拟机间进行不利访问的风险极小。因此，不需要将配置设置为虚拟机之间有防火墙。但是，为防止外部主机测试运行的干扰，可将配置设置为在虚拟网络的入口点有防火墙以保护整组虚拟机。

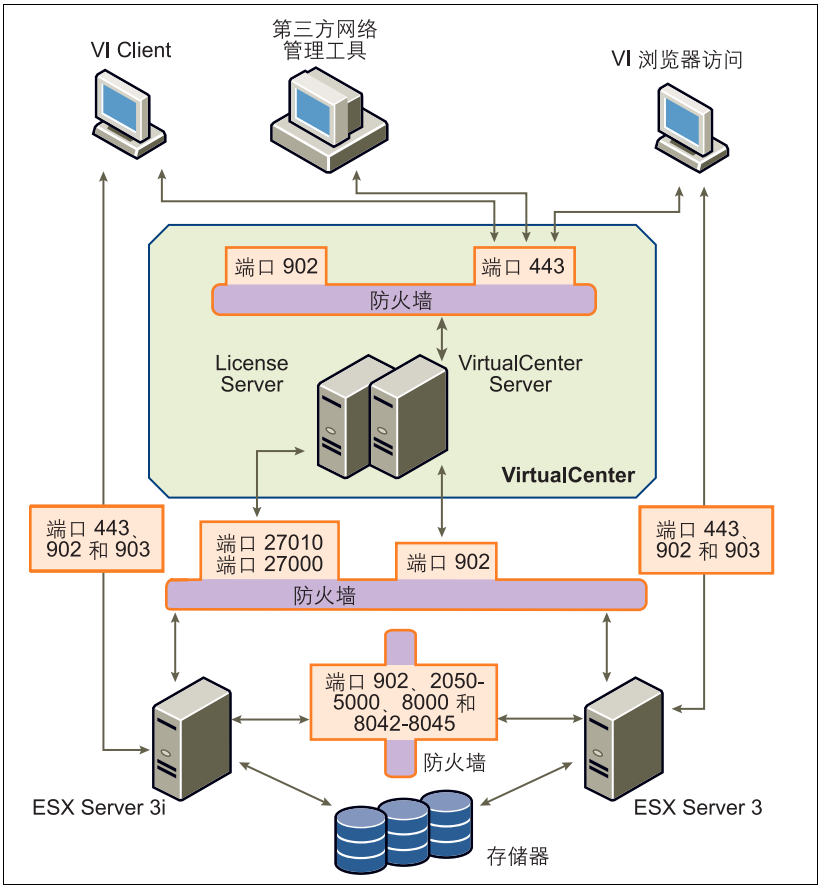
本节介绍配置 VirtualCenter 和未配置 VirtualCenter 时防火墙的安装位置。同时提供了 ESX Server 3i 系统所需防火墙端口的信息。

针对有 VirtualCenter Server 的配置设立防火墙

如果使用 VirtualCenter Server，可在图 9-1 中所示的任何位置安装防火墙。

注意 根据您的配置，可能不需要设立图中的所有防火墙，也可能需在未显示的位置安装防火墙。

图 9-1. Virtual Infrastructure 网络配置和流量示例



配置了 VirtualCenter Server 的网络可通过几种客户端接收通信: VI Client 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。如果任何元素之间有防火墙，必须确保防火墙中有打开的端口以支持数据传输。

如果通过 VirtualCenter Server 访问 ESX Server 3i 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 和客户端均受该防火墙保护取决于您的部署。重点是确保在作为整个系统的入口点处设立防火墙。

根据计划如何使用网络及各种设备所需安全程度，可能还需要在网络中的许多其他访问点设立防火墙。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 3i 实施常用的防火墙位置列表。列表和插图中的许多防火墙位置都是可选的。

- VI Client 或第三方网络管理客户端与 VirtualCenter Server 之间。
- VI Client 与 ESX Server 3i 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。
- License Server 与 VirtualCenter Server 或 ESX Server 3i 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 3i 网络，与 VirtualCenter Server 并行运行，但使用不同端口。

  在某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。在此处应通过 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。有关许可的信息，请参见 *《安装和升级指南》*。
- VirtualCenter Server 与 ESX Server 3i 主机之间。
- 网络中的 ESX Server 3i 主机之间。尽管 ESX Server 3i 主机之间的流量通常被认为是可信的，但如果担心主机之间会引起安全破坏，可在 ESX Server 3i 主机间添加防火墙。

  如果在 ESX Server 3i 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 3i 主机和网络存储设备 （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。

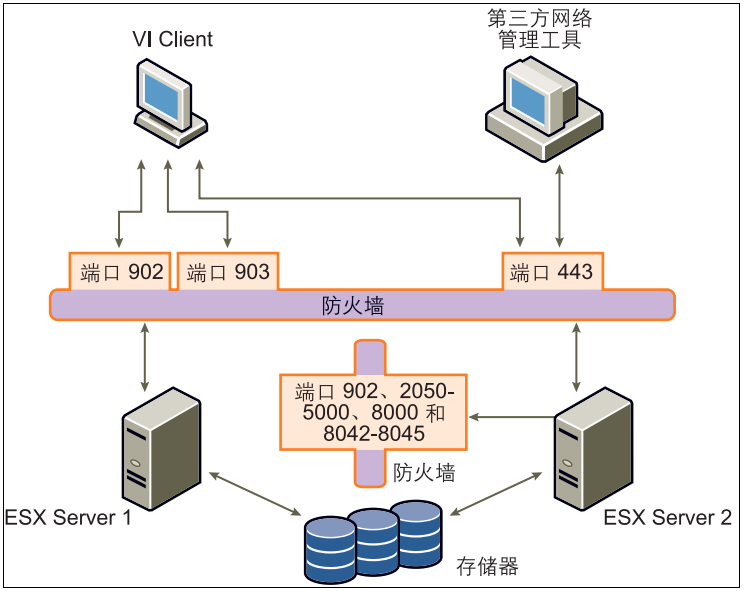
有关为这些通信路径打开的端口的信息，请参见 “用于管理访问的 TCP 和 UDP 端口”（第 136 页）。

针对没有 VirtualCenter Server 的配置设立防火墙

如果客户端直接连接 ESX Server 3i 网络，而不是使用 VirtualCenter Server，则防火墙配置略为简单。可在 图 9-2 中显示的任何位置安装防火墙。

注意 根据您的配置，可能不需要设立图中的所有防火墙，也可能需在未显示的位置安装防火墙。

图 9-2. 针对客户端直接管理的 ESX Server 3i 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 或第三方网络管理客户端。

与包含 VirtualCenter Server 的配置一样，应确保有防火墙保护 ESX Server 3i 层，或保护客户端及 ESX Server 3i 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。

此类型配置中的许可是您在每台 ESX Server 3i 主机上安装的 ESX Server 3i 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。因此，无需在 License Server 与 ESX Server 3i 间设立防火墙。

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 3i 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 3i 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 3i 主机上自动安装的许可证，需对配置进行额外设置。

用于管理访问的 TCP 和 UDP 端口

本节列出了用于对 VirtualCenter Server、 ESX Server 3i 主机和其他网络组件进行管理访问的预定 TCP 和 UDP 端口。如果需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。

表 9-1. 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 3i 网络的访问前端。端口 80 将流量重定向至 HTTPS 登陆页面 （端口 443），您将从这里启动虚拟机控制台。 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
443	HTTPS 访问。 默认的 SSL Web 端口。将端口 443 用于： ■ VI Client 对 VirtualCenter Server 的访问。 ■ VI Client 对 ESX Server 3i 主机的直接访问。 ■ WS 管理。 ■ VMware Update Manager。 ■ VMware Converter。	入站 TCP
902	流量和远程控制台流量的身份验证。 将端口 902 用于： ■ VirtualCenter Server 对 ESX Server 3i 主机的访问。VirtualCenter Server 在端口 902 上发送 ESX Server 3i 主机的 UDP 消息。 ■ ESX Server 3i 主机对其他 ESX Server 3i 主机的访问，以进行迁移和置备。ESX Server 3i 在端口 902 上将 UDP 消息发送到 VirtualCenter Server。 ■ VI Client 对虚拟机控制台的访问。	入站和出站 TCP、出站 UDP
2049	来自 NFS 存储设备的事务。 此端口用于 VMKernel 接口。	入站和出站 TCP
2050 - 2250	ESX Server 3i 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

表 9-1. TCP 和 UDP 端口 （续）

端口	用途	流量类型
3260	来自 iSCSI 存储设备的事务。 此端口用于 VMKernel 接口。	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。	入站和出站 TCP
8042 - 8045	ESX Server 3i 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 3i 到 License Server (lmgrd.exe) 的许可证事务	出站 TCP
27010	从 ESX Server 3i 到 License Server (vmwarelm.exe) 的许可证事务	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配置防火墙”（第 140 页）。

通过防火墙连接 VirtualCenter Server

如表 9-1 中所示，VirtualCenter Server 用来侦听客户端的数据传输的端口为 443。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 接收来自于 VI Client 的数据，请在防火墙中打开 443 端口，以允许数据从 VI Client 传输到 VirtualCenter Server。有关在防火墙中配置端口的其他信息，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》*。

通过防火墙连接虚拟机控制台

无论是通过 VirtualCenter Server 将客户端连接到 ESX Server 3i 主机，还是将其直接连接到 ESX Server 3i 主机，用户和管理员与虚拟机控制台的通信都需要使用端口。这些端口支持不同客户端功能，与 ESX Server 3i 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** - 端口 902 是 VirtualCenter Server 假设可用来从 ESX Server 3i 主机接收数据的端口。 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 3i 主机。此守护进程随后将端口 902 的数据分多路传输到相应的接收方进行处理。

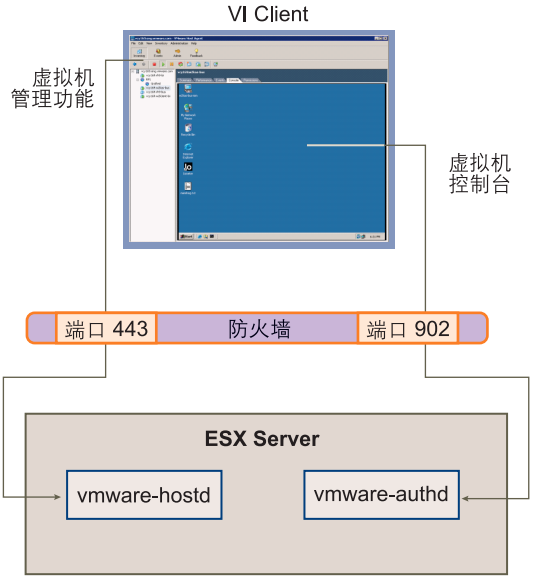
  VI Client 使用此端口为虚拟机上的客户操作系统鼠标 / 键盘 / 屏幕 (Mouse/Keyboard/Screen, MKS) 活动提供连接。用户正是通过此端口与虚拟机的客户操作系统及应用程序交互。端口 902 是 VI Client 与虚拟机交互时假设可用的端口。 VMware 不支持为此功能配置不同端口。

- **端口 443** - VI 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 3i 主机时，VI Client 和 SDK 也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 3i 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 SDK 将客户端连接到 ESX Server 3i 主机。`vmware-hostd` 将端口 443 的数据分多路传输到相应的接收方进行处理。

图 9-3 说明了 VI Client 功能、端口及 ESX Server 3i 进程间的关系。

图 9-3. VI Client 与 ESX Server 3i 的通信中的端口使用情况



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 902 可允许：

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

如果在两个 ESX Server 3i 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 / 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：

- 902 （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 136 页）。

为支持的服务和管理代理配置防火墙

由于 ESX Server 3i 本身没有防火墙，因此您必须在环境中配置任何其他防火墙，以接受普遍支持的服务和已安装的管理代理。以下是 Virtual Infrastructure 环境中常见的服务和代理列表：

- NFS 客户端 （不安全服务）
- NTP 客户端
- iSCSI 软件客户端
- CIM HTTP 服务器 （不安全服务）
- CIM HTTPS 服务器
- Syslog 客户端

注意 此列表可能更改，因此您可能会发现此列表中未提到的服务和代理。可能需要执行其他操作来配置和启用这些任务。

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此层保护：

- 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。

  注意 为提高效率，可设置专用虚拟机以太网或*虚拟网络*。通过虚拟网络，可在虚拟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，然后再决定是否在虚拟网络中的其他虚拟机上安装软件防火墙。

- 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。

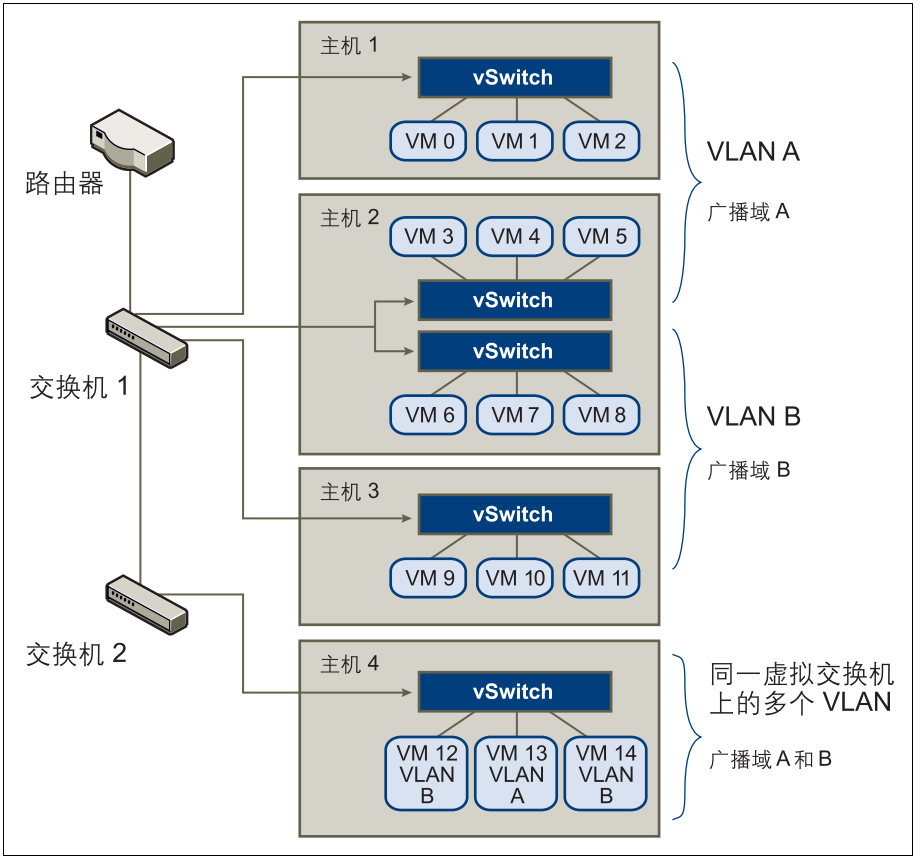
  仔细计划分段可降低虚拟机区域间传送数据包的几率，从而防止探查攻击 （此类攻击需向受害者发送网络流量）。此外，攻击者无法利用一个虚拟机区域中的不安全服务访问主机中的其他虚拟机区域。可以使用两种方法之一实施分段，每种方法具有不同优势。

  - 将单独的物理网络适配器用于虚拟机分区，确保将区域隔离。为虚拟机分区使用单独的物理网络适配器可能是最安全的方法，并且更不容易在初次创建段之后出现配置错误。
  - 设置虚拟局域网 (Virtual Local Area Network, 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。如果配置正确， VLAN 将是您防止一组虚拟机遭受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，以便只有属于同一 VLAN 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 9-4 所示设置 VLAN 以保护会计部门的虚拟机。

图 9-4. 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，无法路由到*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。请注意，一个虚拟交换机可用于不同 VLAN 中的虚拟机。

下节为通过虚拟交换机和 VLAN 保护网络提供了一些建议。

VLAN 安全注意事项

ESX Server 3i 具有的功能完全符合 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，下面的主题介绍了使用 VLAN 部署作为安全执行策略一部分时要考虑的一些因素。

将 VLAN 视为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作为入口点的 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。可使用 VLAN 以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 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，请务必在配置设备时遵照供应商的最佳做法准则。

请注意， 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，由于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对某些 VLAN 执行操作。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。

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。

以下主题将介绍一些虚拟交换机和 VLAN 可加以防御的攻击。

MAC 洪水

这些攻击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 (Content-Addressable Memory, 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

这些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中继线并向其他 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

这些攻击出现的情形为：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

这些攻击涉及将大量多播帧几乎同时发送到已知 VLAN，以使交换机负载过重，从而错误地允许向其他 VLAN 广播一些帧。

VMware 虚拟交换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

这些攻击以跨树协议 (Spanning-Tree Protocol, STP) 为目标，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，将攻击者自己建立成为根网桥。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

这些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计算机的帧或模拟另一台计算机，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计算机的帧。

在为网络创建虚拟交换机时，会添加端口组，为连接交换机的虚拟机、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 3i 阻止其虚拟机的客户操作系统模拟网络上的其他计算机。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 地址输入在以太网帧的源 MAC 地址字段中。它还将接收网络适配器的 MAC 地址输入在目标 MAC 地址字段中。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。

创建后，网络适配器的有效 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。因此，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 3i 主机上的虚拟交换机安全配置文件设置下列三种选项以防止此类攻击。

MAC 地址更改

默认情况下，此选项设置为 **[接受 (Accept)]**，这意味着 ESX Server 3i 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)]**。如此， ESX Server 3i 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）。请注意，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。

MAC 地址更改设置会影响离开虚拟机的流量。如果允许发送者更改 MAC 地址，则即使 vSwitch 或接收虚拟机不允许 MAC 地址更改，也会出现 MAC 地址更改的情况。

伪信号

默认情况下，此选项设置为 **[接受 (Accept)]**，这意味着 ESX Server 3i 主机不会对源 MAC 地址和有效 MAC 地址进行比较。**[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)]**。如果选择该选项， ESX Server 3i 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 3i 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 3i 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

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行模式，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）。

如果需要为端口更改上述任何默认设置，必须在 VI Client 中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 38 页）。

确保 iSCSI 存储器安全

为 ESX Server 3i 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 (Storage Area Network, 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 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 可有效地利用现有以太网架构为 ESX Server 3i 主机提供对其可动态共享的资源的访问。同样地，iSCSI SAN 可为依赖公用存储池为多个用户提供服务的环境提供经济的存储解决方案。与所有网络系统一样，iSCSI SAN 也可能遭到安全破坏。在 ESX Server 3i 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 3i 主机的 iSCSI 硬件适配器和通过 ESX Server 3i 主机直接配置的 iSCSI 相同。

下节介绍如何为 iSCSI SAN 配置身份验证，并且提供了一些用来保护 iSCSI SAN 的建议。该节涵盖以下主题：

- “通过身份验证确保 iSCSI 设备的安全”（第 148 页）
- “保护 iSCSI SAN”（第 151 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 3i 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 3i 主机上的 iSCSI SAN 设置身份验证时有两个选项。

挑战握手身份验证协议 (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 3i 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，目标需对启动器进行身份验证，但启动器无需对目标进行身份验证。启动器仅有一组凭据，所有 iSCSI 目标均使用这些凭据。

ESX Server 3i 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，这使您能够为每个目标配置不同凭据以实现更好的目标优化。

禁用

可将 iSCSI SAN 配置为不使用身份验证。请注意，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 iSCSI 存储器位于一个位置，并创建一个专用网络或 VLAN 以用于所有 iSCSI 设备，那么选择不执行更严格的身份验证可能有意义。这里的前提是 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。

对于 iSCSI， ESX Server 3i 不支持 Kerberos、安全远程协议 (Secure Remote Protocol, 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)]**。

如果 **[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 使用 CHAP 身份验证，如下所示。

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)]**。

为 CHAP 身份验证配置 iSCSI

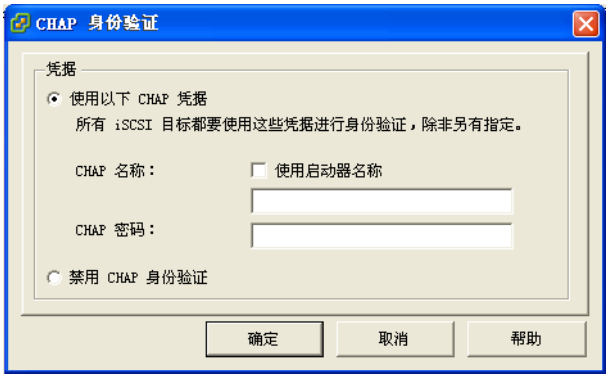
1 登录 VI Client，从清单面板中选择服务器。

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。

注意 VI Client 不对您输入的 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。请查看制造商的文档，以确定要求。

8 单击 **[确定 (OK)]**。

禁用 iSCSI 身份验证

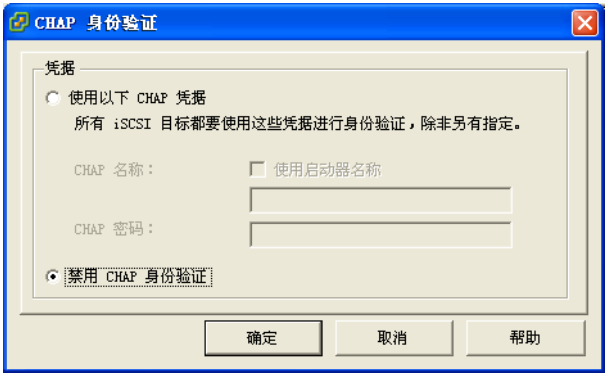
1 登录 VI Client，从清单面板中选择服务器。

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。

保护传送数据

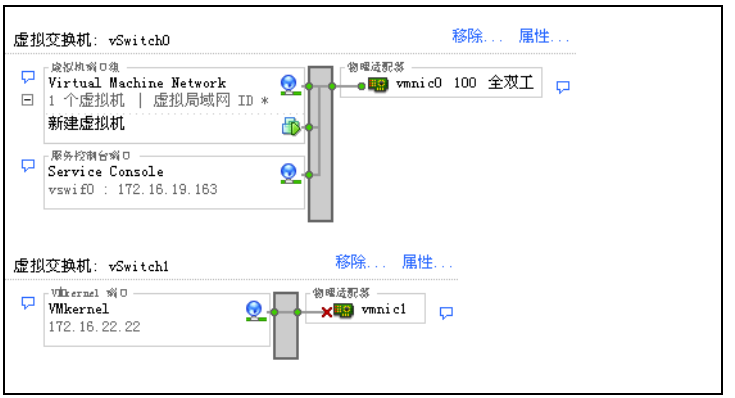
iSCSI SAN 中的一个主要安全风险便是攻击者可能探查传送的存储数据。

VMware 建议您采取其他措施防止攻击者轻松看到 iSCSI 数据。无论是 iSCSI 硬件适配器还是 ESX Server 3i 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，请确保所有虚拟机都无法看到 iSCSI 存储网络。

如果使用 iSCSI 硬件适配器，要实现这一目的，您需执行的操作是：确保 iSCSI 适配器和 ESX 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 3i 主机配置 iSCSI，可通过虚拟机未使用的另一个虚拟机交换机配置 iSCSI 存储器，如图 9-5 中所示。

图 9-5. 单独虚拟交换机上的 iSCSI 存储器



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

运行 iSCSI 设备时，ESX Server 3i 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 3i 主机并控制主机的几率。因此，运行 iSCSI 时不会在连接的 ESX Server 3i 主机端产生任何额外安全风险。

请注意，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 连接的已打开 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 3i 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。

10 身份验证和用户管理

本章说明 ESX Server 3i 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，它还讨论了如何加密 VI Client 和 SDK 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。

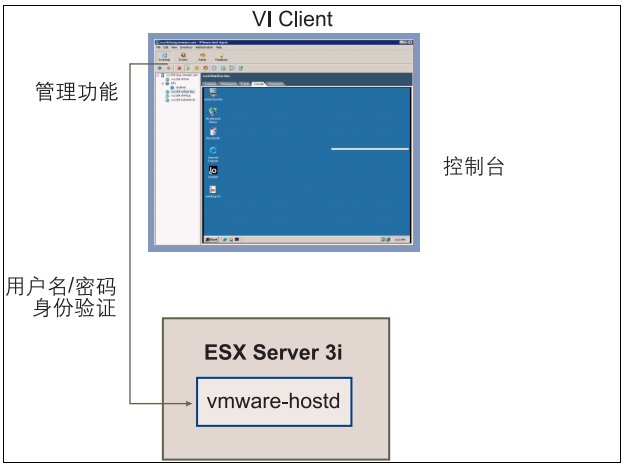
本章将讨论以下主题：

通过身份验证和权限确保 ESX Server 3i 的安全

ESX Server 3i 会对使用 VI Client 或 SDK 访问 ESX Server 3i 主机的用户进行验证。ESX Server 3i 的默认安装使用本地密码数据库来进行身份验证。每当 VI Client 或 VirtualCenter 用户连接 ESX Server 3i 主机时，都会连接 VMware Host Agent (`vmware-hostd`) 进程。`vmware-hostd` 使用用户名和密码来进行验证。

图 10-1 显示 ESX Server 3i 如何验证来自 VI Client 的事务。

图 10-1. 对 VI Client 与 ESX Server 3i 之间的通信进行身份验证



通过第三方网络管理客户端进行的 ESX Server 3i 身份验证事务以相似的方式与 `vmware-hostd` 进程直接进行交互。

要确保为网站有效地进行身份验证，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通过与为用户存储的密码相匹配的密码登录到主机时，可以向其授予对 ESX Server 3i 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 3i 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 3i 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身份验证并授予用户执行操作的权限。为了支持这一机制， VirtualCenter 和 ESX Server 3i 主机保留了授权用户、密码及向每个用户分配的权限的列表。

VirtualCenter 和 ESX Server 3i 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有权限。
- 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 3i 主机和 VirtualCenter 的过程中，需要开发用户和权限模型。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。在开发用户名和权限模型时，请注意：

- ESX Server 3i 和 VirtualCenter 使用了一组特权或*角色*来控制单个用户或组可执行的操作。 ESX Server 3i 和 VirtualCenter 提供了一组预定的角色，但也可自行创建新的角色。
- 分配至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 3i 主机或 VirtualCenter 的个人。ESX Server 3i 用户分为两类：可通过 VirtualCenter 访问 ESX Server 3i 主机的用户及通过从 VI Client、第三方客户端或命令 Shell 程序直接登录主机访问 ESX Server 3i 主机的用户。这两个类别提取不同来源的用户。

- **VirtualCenter 用户** - VirtualCenter 引用的 Windows 域列表中包括的 VirtualCenter 授权用户或 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。要对用户列表进行操作或更改用户密码，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。只有在选择用户以配置权限时才会发现这些更改。

- **直接访问用户** - 经授权直接在 ESX Server 3i 主机上工作的用户是系统管理员添加至内部用户列表的用户。

  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 3i 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，一个名为 *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 *devuser* 的属性（包括权限和密码等），与 ESX Server 3i 主机上 *devuser* 的属性相独立。如果以 *devuser* 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* 身份登录 ESX Server 3i 主机，则可能不具有这样的权限。

由于名称重复可能造成混乱， Vmware 建议您在创建 ESX Server 3i 主机用户之前对 VirtualCenter 用户列表进行检查，以避免创建名称与 VirtualCenter 用户相同的主机用户。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。组由要通过一组公用的规则和权限对其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，您可能会赋予 *SalesShare* 组只与一个对象（*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* 上开始控制台会话等等。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 3i 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 ESX Server 3i 主机，则从该主机维护的表中调用组列表。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 3i 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 3i 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 3i 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 3i 用户对主机相关联的对象执行操作的能力很有限。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主题中所述的权限。

根

超级用户可在其已登录的特定 ESX Server 3i 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 3i 主机的超级用户不能在更广泛的 ESX Server 3i 部署中控制任何其他主机的活动。

为了安全起见，可能不需要使用管理员角色中的超级用户。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，首先必须创建处于超级用户级别、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。

注意 通过命令行界面运行的配置命令 （`vicfg` 命令）不能执行访问检查。因此，即使限制超级用户的特权，也不会影响用户使用命令行界面命令执行的操作。

vpxuser

此用户是在 ESX Server 3i 主机上充当具有管理员权限的实体的 VirtualCenter，它可管理该主机的活动。 vpxuser 是在将 ESX Server 3i 主机连接至 VirtualCenter 时创建的。除非是通过 VirtualCenter 对 ESX Server 3i 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 3i 主机进行管理，VirtualCenter 则在该主机上具有管理员特权。例如， VirtualCenter 可使虚拟机在主机之间移动，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 3i 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 3i 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 对 ESX Server 3i 主机执行操作时可能会出现问题。

dcui

dcui 用户用管理员权限在主机上操作。此用户的主要目的是从直接控制台配置锁定模式的主机。此用户将用作直接控制台的代理，不应由交互式用户来修改或使用。

小心 不要以任何方式更改 dcui 用户及其权限。如果进行了更改，在通过本地 UI 对 ESX Server 3i 主机执行操作时可能会出现问题。

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，首先必须创建处于超级用户级别、可向另一个用户分配管理员角色的另一种权限。

如果未分配有管理员角色的用户不是本地管理员组的成员，则无法登录到本地控制台。要授予本地控制台的访问权限，请使用下面的命令，其中 username 是要向其授予访问权限的用户名称：

```
usermod –G localadmin username
```

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 3i 仅向分配了对象权限的用户授予对象访问权限。向用户或组分配与对象相关的权限时，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 3i 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。以下主题论述了默认的角色。

无权访问

分配此对象角色的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 3i 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，

则可选择 [虚拟机 (Virtual Machines)] 选项卡，但不会看到有虚拟机列出在此选项卡上，也不会看到任何状态信息 - 表为空白。

默认情况下，在 ESX Server 3i 主机上创建的任何用户或组均分配有无权访问角色。可按对象提升或降低新创建的用户或组的角色。

注意 默认情况下，超级用户、dcui 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

分配有此对象角色的用户，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

分配有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 中的角色编辑功能创建自定义角色，以创建符合用户需求的特权组。如果使用了连接 VirtualCenter 的 VI Client 来管理 ESX Server 3i 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 3i 主机上直接创建的角色。仅当直接从 VI Client 登录主机时，才可使用这些角色。

如果通过 VirtualCenter 管理 ESX Server 3i 主机，请注意，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 3i 主机上的用户和组

如果通过 VI Client 直接连接 ESX Server 3i 主机，则可创建、编辑和删除用户和组。只要登录 ESX Server 3i 主机，就会在 VI Client 中看到这些用户和组，但在登录 VirtualCenter 时看不见。

下节介绍如何在直接连接 ESX Server 3i 主机的 VI Client 中处理用户和组。该节介绍可以对用户和组执行的基本任务，例如查看信息、对信息排序和导出报告。它还介绍了如何创建、删除以及编辑用户和组。

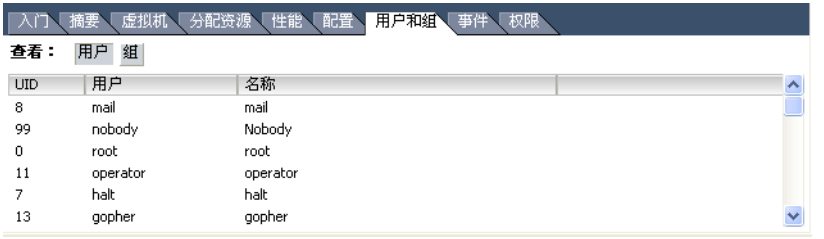
注意 也可通过直接连接 ESX Server 3i 主机来创建角色并设置权限。由于这些任务在 VirtualCenter 中使用的更广泛，因此请参见 *《基本系统管理》* 获得有关处理权限和角色的信息。

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)]** 按钮还是 **[组 (Groups)]** 按钮，该选项卡将显示 **[用户 (Users)]** 表或 **[组 (Groups)]** 表。

图 10-2 显示了 **[用户 (Users)]** 表。 **[组 (Groups)]** 表与其相似。

图 10-2. 用户表



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 3i 用户或组

1 通过 ESX Server 3i 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 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 3i 用户或组表中导出数据

1 通过 ESX Server 3i 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 根据要在导出文件中看到的信息，确定如何对表进行排序以及隐藏或显示列。

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 选择路径并输入文件名。

7 选择文件类型。

可通过以下任一格式导出用户或组表：

- HTML （纯 HTML 或具有与 CSS 样式表配合使用格式的 HTML）
- XML
- Microsoft Excel
- CSV （逗号分隔值）

8 单击 **[确定 (OK)]**。

处理用户表

可向 ESX Server 3i 主机的 **[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，即正在更改由 ESX Server 3i 主机维护的内部用户列表。

向 ESX Server 3i 用户表添加用户

1 通过 ESX Server 3i 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，然偶单击 **[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。

6 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。

7 单击 **[确定 (OK)]**。

输入的登录名和用户名显示在 **[用户 (Users)]** 表中。

修改用户设置

1 通过 ESX Server 3i 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。

密码应有足够的长度和复杂度，以防常见的暴力攻击。

8 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。

9 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)]**。

10 单击 **[确定 (OK)]**。

从 ESX Server 3i 用户表移除用户

1 通过 ESX Server 3i 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 请勿移除超级用户。

处理组表

可向 ESX Server 3i 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，即正在更改由 ESX Server 3i 主机维护的内部组列表。

向 ESX Server 3i 组表添加组

1 通过 ESX Server 3i 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 输入组名称和数字组 ID (Group 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 3i 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 3i 组表移除组

1 通过 ESX Server 3i 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 请勿移除超级用户。

ESX Server 3i 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 SSL，则只要以下条件成立，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。

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 VirtualCenter server。

2 单击 **[管理 (Administration)]** > **[Virtual Center Management Server 配置 (Virtual Center Management Server Configuration)]**。

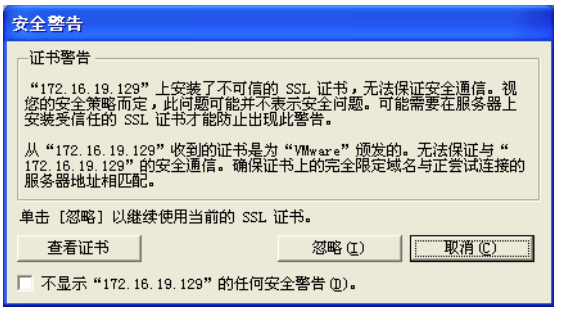
此时会出现 **[Virtual Center Management Server 配置 (Virtual Center Management Server Configuration)]** 对话框。

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 会话安全的证书未经可信证书颁发机构签署，因此，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远程连接，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。

图 10-3. 安全警告



要解决此问题，请添加由公认的证书颁发机构签署的证书。该证书由两个文件组成：证书本身 (`.crt`) 和私钥文件 (`rui.key`)。

修改 ESX Server 3i Web 代理设置

在考虑加密和用户安全时，请注意以下几点：

- ESX Server 3i 并不处理口令（也称为加密的密钥）。如果设置了密码短语，则 ESX Server 3i 进程将无法正常启动，因此请避免使用密码短语设置证书。
- 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 VMware Infrastructure SDK 连接启用 SSL。如果要配置这些连接以使它们不对传输进行加密，请为 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 165 页）中所述。仅当为客户端创建了充分可信的环境 （这意味着此环境中安装了防火墙且完全隔离与主机间的传输）时才可考虑禁用 SSL。禁用 SSL 可提高性能，因为省却了执行加密所需的开销。
- 为了防止误用 ESX Server 3i 服务，仅可通过用于 HTTPS 传输的端口 443 才能访问大多数内部 ESX Server 3i 服务。端口 443 充当 ESX Server 3i 的反向代理。通过 HTTP 欢迎页面即可看到 ESX Server 3i 上的服务列表，但如果未经适当授权，则不能直接访问存储适配器服务。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 3i。
- 在升级 VirtualCenter 时，证书仍然不变。

更改 Web 代理服务的安全设置

1 使用 `vifs` 命令获取 `proxy.xml` 文件副本来进行编辑。此命令采用的格式为：

```
vifs --server hostname --username username --get /host/proxy.xml
                proxy.xml
```

有关使用 `vifs` 的详细信息，请参见“使用 vifs 执行文件系统操作”（第 216 页）。

小心 如果将此文件更改为错误的配置，则系统可能会进入一种难以管理的状况。这样的状况只能使用 DCUI 执行恢复原厂设置才能得以解决。

2 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>
         <!-- 将此模式用于 "安全" 部署 -->
         <!-- <accessMode>httpsWithRedirect</accessMode> -->
         <!-- 将此模式用于 "不安全" 部署 -->
         <accessMode>httpAndHttps</accessMode>
         <port>8889</port>
         <serverNamespace>/wsman</serverNamespace>
      </e>
   </EndpointList>
</ConfigRoot>
```

3 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。

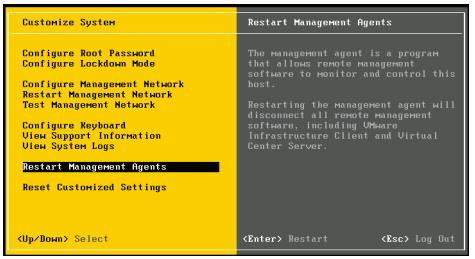
- *e id* 是服务器 ID XML 标记的 ID 编号。ID 编号在 HTTP 区域中必须是唯一的。
- *_type* 为所移动的服务的名称，例如 /sdk 或 /mob。
- *accessmode* 是服务允许的通信形式。可接受的值包括：
  - httpOnly - 只能通过纯文本 HTTP 连接访问服务。
  - httpsOnly - 只能通过 HTTPS 连接访问服务。
  - httpsWithRedirect - 只能通过 HTTPS 连接访问服务。通过 HTTP 发出的请求将被重定向至相应的 HTTPS URL。
  - httpAndHttps - 可通过 HTTP 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。

4 保存更改并关闭文件。

5 使用 vifs 命令将 proxy.xml 文件副本放回 ESX Server。此命令采用的格式为：

```
vifs --server hostname --username username --put /host/proxy.xml
                proxy.xml
```

6 通过本地控制台使用 “重新启动管理代理”操作来使设置生效。重新启动管理代理显示如下：



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 3i 需要访问虚拟机文件。例如，为了启动和关闭虚拟机， ESX Server 3i 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 3i 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 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 服务器会拒绝对 ESX Server 3i 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 3i 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操作，可通过试验性的 ESX Server 3i 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 3i 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)

然后，使用此信息更改 ESX Server 3i 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 3i 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 3i 主机上设置委派用户需要完成以下操作：

- 在直接在 ESX Server 3i 主机上运行的 VI Client 的 [用户和组 (Users & Groups)] 选项卡中：
  - 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 3i 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 3i 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，需要确保委派用户 （所创建的 `vimuser` 或委派用户）在使用 NFS 数据

存储的所有 ESX Server 3i 主机上均是相同的。请参见 “处理用户表”（第 161 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 3i 主机上运行的 VI Client 配置安全配置文件。

小心 更改 ESX Server 3i 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 3i 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 3i 主机。

重新引导主机后，就可在直接运行于 ESX Server 3i 主机上的 VirtualCenter 和 VI Client 中看到委派用户设置。

11 安全部署与建议

本章重点讲述如何确保 ESX Server 3i 在特定环境中的安全，在讲解时会提出一系列 ESX Server 3i 部署方案，供您在规划部署的某些安全功能时参考。本章还提出了基本的安全建议，供您在创建和配置虚拟机时参考。

本章将讨论以下主题：

常用 ESX Server 3i 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 3i 部署的复杂性会有极大差异。

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。通过对部署进行比较，您可以了解在规划 ESX Server 3i 部署安全时需面临的问题。

单客户部署

在此类部署中， ESX Server 3i 主机由一家公司拥有并在一个数据中心进行维护。 ESX Server 3i 资源不与外部用户共享。ESX Server 3i 主机由一名网站管理员维护，并且这些主机运行多台虚拟机。

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 3i 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 3i 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 11-1 显示了如何处理为 ESX Server 3i 主机配置的所用组件的共享。

表 11-1. 单客户部署中的组件共享

功能	配置	备注
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。
VMFS 共享？	是	所有 `.vmdk` 文件均应驻留在同一个 VMFS 分区中。
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 11-2 显示了设置 ESX Server 3i 主机用户帐户的方式。

表 11-2. 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 11-3 显示了每个用户的访问级别。

表 11-3. 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
根访问？	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 3i 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 3i 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 3i 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 3i 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 11-4 显示了如何处理为 ESX Server 3i 主机配置的所用组件的共享。

表 11-4. 多客户限制部署中的组件共享

功能	配置	备注
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。
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。
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 11-5 显示了设置 ESX Server 3i 主机用户帐户的方式。

表 11-5. 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 11-6 显示了每个用户的访问级别。

表 11-6. 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
根访问？	是	否	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 3i 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 3i 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 3i 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 3i 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 11-7 显示了如何处理为 ESX Server 3i 主机配置的所用组件的共享。

表 11-7. 多客户开放部署中的组件共享

功能	配置	备注
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。
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。
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 11-8 显示了设置 ESX Server 3i 主机用户帐户的方式。

表 11-8. 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 11-9 显示了每个用户的访问级别。

表 11-9. 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
根访问？	是	否	否	否
创建和修改虚拟机？	是	是	否	否

ESX Server 3i 锁定模式

要提高 ESX Server 3i 主机的安全性，可以选择将其置于锁定模式。锁定模式仅可用于已添加到 VirtualCenter 的 ESX Server 3i 主机。启用锁定模式会禁用对 ESX Server 3i 计算机进行的所有直接的根访问。对主机随后的任何本地更改，必须：

- 在 VI Client 会话或 RCLI 命令中，使用具有完全编辑权限的 Active Directory 帐户对 VirtualCenter 进行更改。
- 在 VI Client 会话或 RCLI 命令中，使用主机上定义的本地用户帐户直接对 ESX Server 3i 系统进行更改。默认情况下，ESX Server 3i 系统上不存在本地用户帐户。

此类帐户只能在 VI Client 会话中启用锁定模式之前，直接在 ESX Server 3i 系统上创建。对主机的更改限于在该主机上本地授予该用户的特权。

使用添加主机向导将 ESX Server 3i 添加到 VirtualCenter，或者使用 VI Client 管理属于 VirtualCenter 的主机时，可以启用锁定模式。

使用 VI Client 为 ESX Server 3i 启用锁定模式

1 登录 VI Client，从清单面板中选择 ESX Server。

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

3 在 [锁定模式 (Lockdown mode)] 下，单击 **[编辑 (Edit)]**。

此时会显示 [锁定模式 (Lockdown Mode)] 对话框。

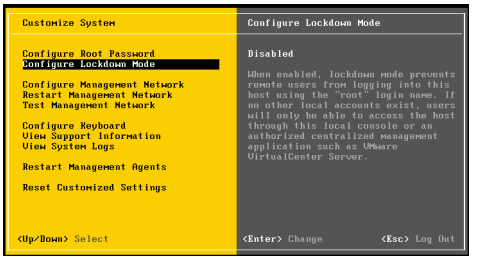
4 选择 **[启用锁定模式 (Enable Lockdown Mode)]** 复选框，以启用锁定模式。

5 单击 **[确定 (OK)]** 关闭 **[锁定模式 (Lockdown Mode)]** 对话框。

也可以通过本地控制台 (DCUI) 启用或禁用锁定。

从本地控制台启用锁定模式

切换 [配置锁定模式 (Configure Lockdown Mode)] 设置，如下图所示。



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

由于每台虚拟机都托管标准操作系统，因此，应考虑安装防病毒软件，使其免遭病毒感染。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

在虚拟机上运行 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)]**。

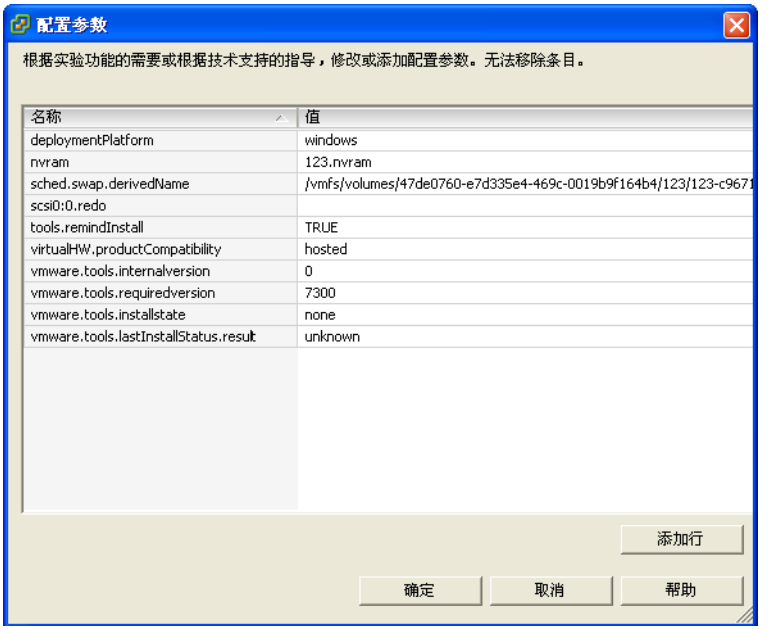
3 单击 **[选项 (Options)]** > **[高级 (Advanced)]** > **[配置参数 (Configuration Parameters)]**，打开 **[配置参数 (Configuration Parameters)]** 对话框。

4 单击 **[添加行 (Add Row)]** 按钮。

5 在 **[名称 (Name)]** 字段和 **[值 (Value)]** 列中键入下列值。

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 控制面板中制定的任意设置。

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。攻击者可利用该功能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。虽然此措施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。

防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)] >[一般选项 (General)]**，记录 **[虚拟机配置文件 (Virtual Machine Configuration File)]** 字段中显示的路径。

4 使用 `vifs` 命令，从步骤 3 中记录的位置获取虚拟机配置文件副本。有关使用 vifs 的详细信息，请参见 “使用 vifs 执行文件系统操作”（第 216 页）。

5 将下面一行添加到 `.vmx` 文件。

```
< 设备名称 >.allowGuestConnectionControl = "false"
```

其中， < 设备名称 > 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 < 设备名称 >`.allowGuestConnectionControl` 设置为 真，否则无需更改该设置。

6 保存更改并关闭文件。使用 `vifs`，将已修改的文件副本放到步骤 3 中记录的位置。

7 右键单击清单面板中的虚拟机，依次单击 **[关闭 (Power Off)]** 和 **[启动 (Power On)]**。

虚拟机关闭，然后启动。

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 3i 主机发送信息消息。这种消息（简称为 `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 的软件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，对 DOS 进行攻击。

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。如果在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 文件内存限制，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)]**。

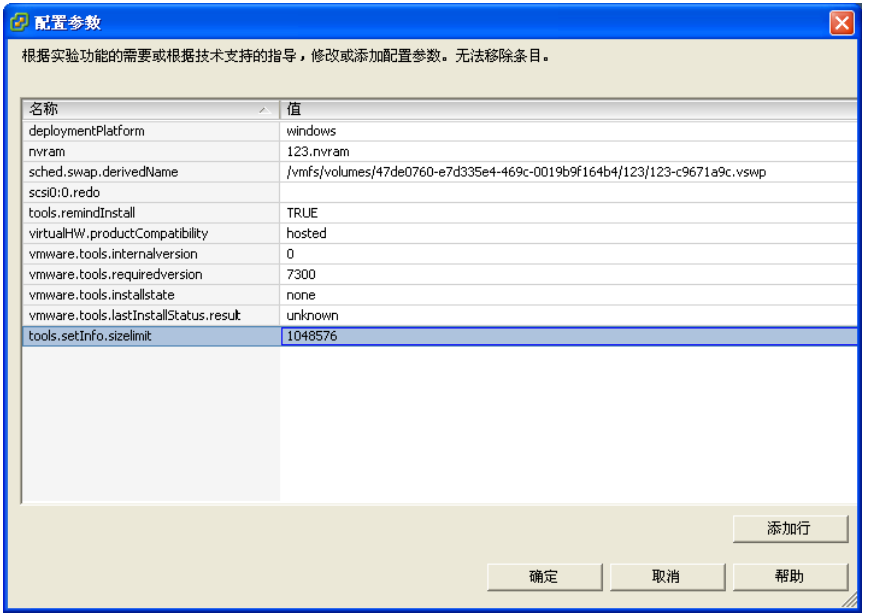
3 单击 **[选项 (Options)]** > **[高级 (Advanced)]** > **[配置参数 (Configuration Parameters)]**，打开 **[配置参数 (Configuration Parameters)]** 对话框。

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 - < 字节数 >**

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。

您也可选择完全禁止客户操作系统将任何名称 / 值对写入配置文件。该选择适合必须禁止客户操作系统修改配置设置的情况。

防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。

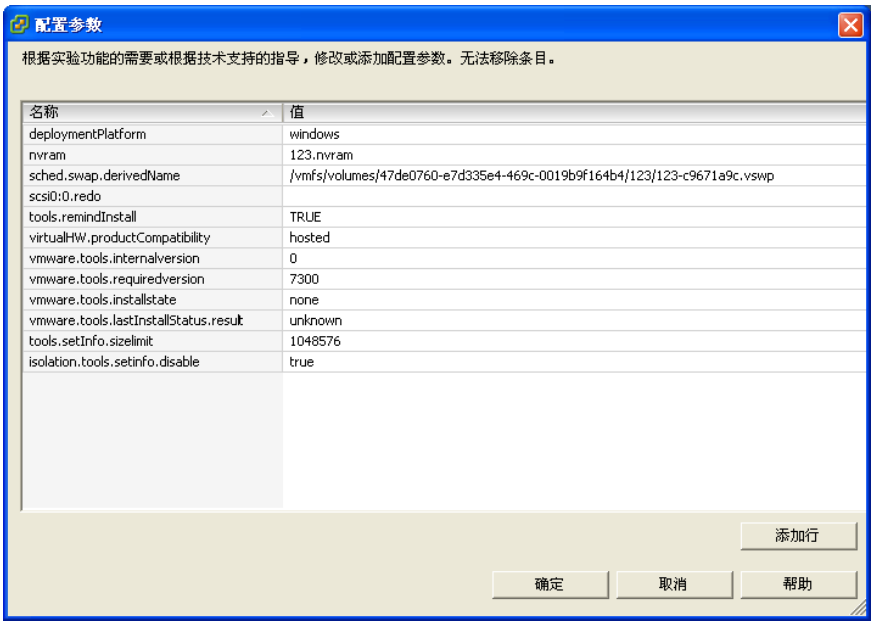
2 单击 **[编辑设置 (Edit Settings)]**。

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

虚拟机可以将疑难解答信息写入存储在 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，主机会在每次重新引导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。此类日志文件不会占用过量的主机磁盘空间，而存储的数据扩展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

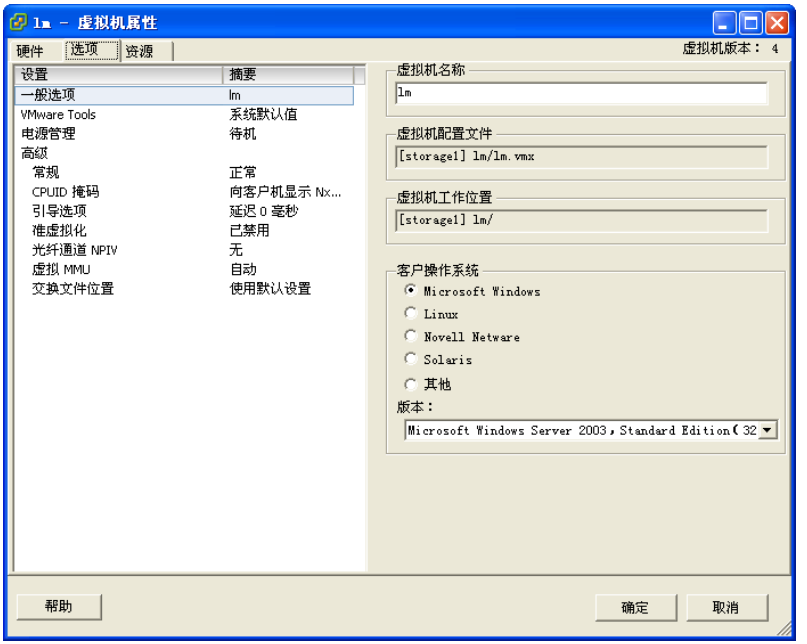
1 登录 VI Client，从清单面板中选择虚拟机。

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 Settings)]**。

此时会显示 [虚拟机属性 (Virtual Machine Properties)] 对话框。

3 单击 **[选项 (Options)] > [一般选项 (General)]**，记录 **[虚拟机配置文件 (Virtual Machine Configuration File)]** 字段中显示的路径。



4 使用 `vifs` 命令获取 `.vmx` 文件副本。有关使用 vifs 的详细信息，请参见 "使用 vifs 执行文件系统操作"（第 216 页）。

5 使用编辑器，在 `.vmx` 文件中添加或编辑下行内容：

```
log.rotateSize=< 上限 >
```

其中，< 上限 > 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`**。

6 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=< 保留文件数 >
```

其中，< 保留文件数 > 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`**。

7 保存更改并关闭文件。使用 `vifs`，将服务器上的副本覆盖为已修改的副本。

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，来解决该问题。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。

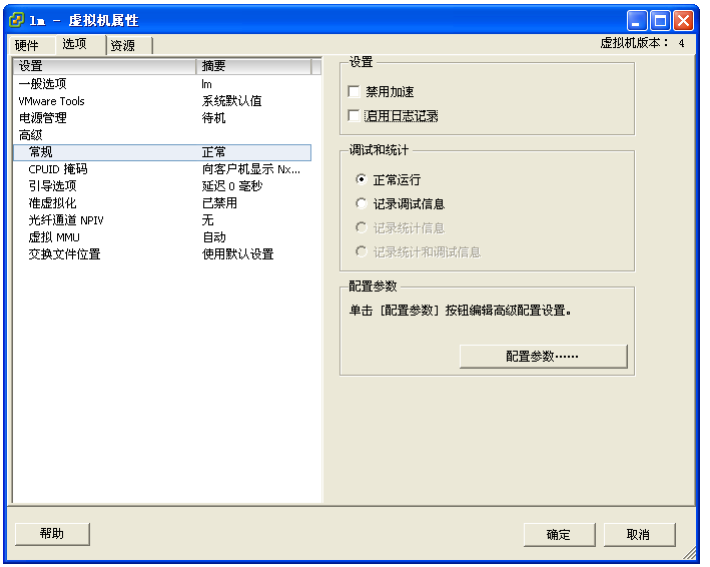
此时会显示该虚拟机的配置页面的 **[摘要 (Summary)]** 选项卡。

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。



单击 **[确定 (OK)]** 关闭 **[虚拟机属性 (Virtual Machine Properties)]** 对话框。

附录

使用远程命令行界面 A

本附录说明如何安装和使用 Remote CLI（Remote Command Line Interface，远程命令行界面）。它还包括一个所有支持的 Remote CLI 和指向论述每个命令位置的指示器的列表。

本附录讨论以下主题：

远程命令行界面概述

通常使用 VI Client 来配置 ESX Server 3i 主机，因为 ESX Server 3i 不包括服务控制台。但是，如果要将相同的配置设置用于多台 ESX Server 3i 主机，或者如果由于其他原因而需要进行命令行访问，则可以使用 Remote CLI（Remote Command Line Interface，远程命令行界面）。

Remote CLI 基于 Virtual Infrastructure Perl Toolkit (VI Perl Toolkit)，后者依赖于 Perl 和许多其他库。可以使用安装软件包或 Remote CLI 设备来访问 Remote CLI 命令。

虚拟设备是预先配置的虚拟机，其中已安装了一些应用程序及所需的操作系统。启动设备时，Linux shell 提示符可让您在远程连接的 ESX Server 3i 主机上运行命令。该 shell 是精简 Debian Linux 环境中的 Linux bash Shell 程序。本附录中列出的所有命令均受支持。

表 A-1 列出了所有的 Remote CLI，每一项均指向本文档中的 Remote CLI 论述或论述 Remote CLI 的另一个文档。

表 A-1. ESX Server 3i 版本 3.5 支持 Remote CLI

命令	描述
resxtop	可让您实时监控 ESX Server 主机使用资源的情况。*《资源管理指南》*中有相关论述。
svmotion	可让您在虚拟机运行时将虚拟机及其磁盘文件从一个数据存储迁移到另一个数据存储。*《基本系统管理》*手册中有相关论述。
vicfg-advcfg	请参见 “在特殊情况下使用 vicfg-advcfg”（第 216 页）。
vicfg-cfgbackup	可让您备份和恢复 ESX Server 3i 主机的配置数据。*《ESX Server 3i 安装指南》*中有相关论述。
vicfg-dumppart	请参见 “使用 vicfg-dumppart 管理诊断分区”（第 206 页）。
vicfg-mpath	请参见 “使用 vicfg-mpath 配置多路径设置”（第 204 页）。
vicfg-nas	请参见 “使用 vicfg-nas 管理 NAS 文件系统”（第 202 页）。
vicfg-nics	请参见 “使用 vicfg-nics 管理物理网络适配器”（第 208 页）。
vicfg-ntp	请参见 “使用 vicfg-ntp 指定 NTP 服务器”（第 213 页）。
vicfg-rescan	请参见 “使用 vicfg-rescan 重新扫描”（第 206 页）。
vicfg-route	请参见 “使用 vicfg-route 操作路由条目”（第 213 页）。

表 A-1. ESX Server 3i 版本 3.5 支持 Remote CLI （续）

命令	描述
vicfg-snmp	ESX Server 3i 包括一个不同于 ESX Server 3 所用代理的 SNMP 管理代理。目前，此 SNMP 代理仅支持 SNMP 陷阱，而不支持 GETS。该代理默认处于关闭状态。要使用此代理，必须启用 SNMP 服务，至少指定一个团体，以及使用 `vicfg-snmp` Remote CLI 配置一个陷阱目标。*《基本系统管理》*手册中有相关论述。
vicfg-syslog	请参见 “使用 vicfg-syslog 指定 syslog 服务器”（第 216 页）。*《ESX Server 3i 安装指南》*详细论述了系统日志并且说明了如何使用 VI Client 来设置系统日志。
vicfg-vmhbadevs	请参见 “使用 vicfg-vmhbadevs 查找可用的 LUN”（第 203 页）。
vicfg-vmknic	请参见 “使用 vicfg-vmknic 管理 VMkernel 网卡”（第 209 页）。
vicfg-vswitch	请参见 “使用 vicfg-vswitch 管理虚拟交换机”（第 210 页）。
vihostupdate	请参见 “使用 vihostupdate 进行性能维护”（第 214 页）。*《ESX Server 3i 安装指南》*中有详细论述。
vifs	请参见 “使用 vifs 执行文件系统操作”（第 216 页）。
vmkfstools	请参见 “使用 vmkfstools Remote CLI”

使用 VMware Remote CLI

可以安装一个包括 Remote CLI 和所有先决条件软件的虚拟设备，或者将 Remote CLI 软件包安装在 Linux 或 Microsoft Windows 中。

- **Remote CLI 虚拟设备** - 下载 Remote CLI 虚拟设备并将其添加到 VirtualCenter Server 或 ESX Server 主机。Remote CLI 虚拟设备是预先安装了精简 Linux 操作系统、VI Perl Toolkit 和所有 Remote CLI 的虚拟机。当 ESX Server 主机上可以使用 Remote CLI 虚拟设备时，可以从虚拟设备的服务控制台运行 Remote CLI 命令。请参见 “安装和使用 Remote CLI 虚拟设备”（第 194 页）。
- **Remote CLI 软件包** - 可以将 Remote CLI 软件包安装在一台服务器上，使其成为所有 ESX Server 3i 主机的管理服务器。请参见 “在 Linux 上安装和使用 Remote CLI”（第 191 页）和 “在 Windows 上安装和使用 Remote CLI”（第 193 页）。

  安装软件包（其中包括 VI Perl Toolkit）以后，可以从操作系统命令行运行 Remote CLI 命令或调用脚本。每次运行命令时，请直接或间接指定连接参数。请参见 “指定 Remote CLI 的必要参数”（第 196 页）。

可以交互使用 Remote CLI 命令，也可以在脚本中使用。

- 在虚拟设备上打开服务控制台并在其中输入 Remote CLI 命令。
- 在安装有 Remote CLI 的 Linux 或 Windows 系统上，使用命令提示符并在其中输入命令。
- 使用若干组 Remote CLI 命令准备脚本，然后从安装有安装软件包的管理服务器或 Remote CLI 虚拟设备服务控制台运行脚本。请参见 “在脚本中使用 Remote CLI”（第 199 页）。

执行命令时，请务必指定要在其上运行命令的服务器以及用户名和密码，如 “指定 Remote CLI 的必要参数”（第 196 页）中所述。

小心 以纯文本方式指定密码存在着将密码泄露给该系统上其他用户的风险。该系统的备份文件也有可能泄露密码。因此，只应在您认为安全可靠的客户端系统上提供纯文本密码。不建议在生产系统上提供纯文本密码。

有两个选择办法。

- 如果交互使用 Remote CLI 并且不指定密码，则系统会提示您输入密码。键入的内容不会在屏幕上显示出来。
- 对于非交互使用，可以使用 VI Perl Toolkit `samples/session` 目录中包含的 `save_session.pl` 脚本，创建一个会话文件。请参见 “使用会话文件”（第 197 页）。

在 Linux 上安装和使用 Remote CLI

下列 Linux 版本的默认安装支持 Remote CLI 的 Perl 安装脚本。

- Fedora Core 7
- SUSE Enterprise Server 10 (SP1)
- Ubuntu Desktop 7.04

许多先决条件库都包含在每个支持的 Linux 版本的基本 （默认）安装中。

Remote CLI 软件包安装程序会安装 Remote CLI 脚本和完整的 VI Perl Toolkit，包括 Perl 和先决条件库。

打开并安装 Remote CLI 软件包

下载并打开 Remote CLI 软件包

1 从 http://www.vmware.com/go/remotecli 下载安装程序软件包 `VMware-RCLI-3.5.0-<date>.i386.tar.gz`。

2 打开 shell 提示符并导航到已下载软件包的目录。

3 打开下载的软件包。

安装 Remote CLI 软件包

1 启动安装程序 (`vmware-install-rcli.pl`)。

安装程序会提示您接受许可协议条款。

2 在提示符下键入 **`yes`** 以接受许可条款并按 Enter 继续。

注意 如果没有键入 `yes` 并按 Enter，则安装程序无法继续。

安装程序会提示您提供安装位置或接受默认位置 `/usr/bin`。

3 指定安装目录，或者按 Enter 接受默认目录。

安装程序会搜索必要的 Perl 库，并记下必要版本级别和安装版本级别之间的任何差异。如果安装程序发现早于必要版本的版本，安装程序会显示下面的消息。

```
The following Perl modules were found on the system but may be too old
to work with VIPerl:
```

在这种情况下，建议安装正确版本的库。

安装程序还会检查 VI Perl 1.0 是否已安装在系统上，并提议替换。

如果覆写 VI Perl Toolkit 的现有安装，则脚本将无法使用。将 RCLI 软件包安装在不同的系统上。

安装过程完成时：

- 会显示成功消息。
- 安装程序会列出必要模块 （如果有的话）的不同版本号。
- 提示符会恢复为 shell 提示符。

现在即可运行 Remote CLI，如 “执行 Remote CLI”中所述。安装过程中同时还会包括许多 VI Perl 实用程序和示例脚本。有关详细信息，请参见 VI Perl 文档。

执行 Remote CLI

安装 Remote CLI 以后，可以从 Linux 命令提示符执行命令。

从 Linux 命令提示符执行 Remote CLI 命令

1 打开命令提示符。

2 传递连接参数并执行命令。可以在命令行上使用配置文件或传递连接参数。扩展名 `.pl` *不是* 必需的。例如：

```
vicfg-ntp --server <server_address> --username <user> --password
<user_password> --help
```

注意 如果未指定用户名和密码，系统会提示。

有关连接参数的完整列表，请参见 “指定 Remote CLI 的必要参数”（第 196 页）。

卸载 Remote CLI

在 Linux 系统上卸载 Remote CLI

1 连接安装 Remote CLI 的目录。

2 执行 `vmware-uninstall-rcli.pl` 脚本。

注意 执行此脚本时，*只会* 卸载 Remote CLI。如果还要卸载 VI Perl Toolkit，则还要执行 `vmware-uninstall-viperl.pl`。

在 Windows 上安装和使用 Remote CLI

将 RCLI 软件包安装在 Windows 上

1 从 http://www.vmware.com/go/remotecli 下载 Remote CLI Windows 安装程序。

2 启动安装程序。此时可能会显示一条有关安装程序数字签名的警告消息。

3 单击 **[是 (Yes)]** 以忽略警告消息并继续安装。

- 如果有以前版本的 VI Perl Toolkit 或 Remote CLI 软件包存在于目标 Windows 系统上，则安装新版本之前，安装程序会提示您卸载该版本。使用 Windows **[添加 / 删除程序 (Add or Remove Programs)]** 控制面板来移除现有的 VI Perl Toolkit 或 Remote CLI 软件包。
- 如果 Perl 的版本存在于目标 Windows 系统上，安装程序会提示您卸载该版本。

小心 默认情况下， RCLI 安装向导会使用 ActivePerl 覆写任何现有的 Perl 安装。如果要保留现有的 Perl 安装，请取消 VI Perl Toolkit 安装过程。

如果覆写 VI Perl Toolkit 的现有安装，则脚本将无法使用。

4 在 [欢迎使用 (Welcome)] 页面单击 **[下一步 (Next)]** 继续。

此时会显示 [目标文件夹 (Destination Folder)] 页面。

5 如果不想将工具包安装在默认目录中，请单击 **[更改 (Change)]** 并选择不同的目录。默认位置为 `C:\Program Files\VMware\VMware VI Remote CLI\bin`。

6 单击 **[下一步 (Next)]** 继续。此时会显示 [准备安装 VMware VI Perl Toolkit 组件 (Ready to Install the VMware VI Perl Toolkit components)] 页面。

7 单击 **[安装 (Install)]** 以继续安装。

完成该过程可能需要几分钟时间。

安装向导结束时，可以通过运行示例脚本之一或实用程序之一来测试安装。

执行 Remote CLI

安装 Remote CLI 后，可以从 Windows 命令提示符执行命令。

从 Windows 命令提示符执行 Remote CLI 命令

1 打开命令提示符。

2 导航到 Remote CLI 的安装目录。

```
cd C:\Program Files\VMware\VMware VI Remote CLI\bin
```

3 传递连接参数和任何其他选项并执行命令。扩展名 .pl 是*必需的*。例如：

```
vicfg-ntp.pl --server <server_address> --username <user> --password
<user_password> --help
```

注意 如果未指定用户名和密码，系统会提示。

系统会显示信息或做出更改。

卸载 Remote CLI 软件包

可以像任何其他软件包那样卸载 Remote CLI。

在 Windows 系统上卸载 Remote CLI

1 选择 **[开始 (Start)] > [设置 (Settings)] > [控制面板 (Control Panel)] > [添加 / 删除程序 (Add or Remove Programs)]**。

2 在出现的面板中，选择 VMwareVIRemoteCLI，然后单击 **[删除 (Remove)]**。

3 在遇到提示时，请单击 **[是 (Yes)]**。

系统会卸载 VI Perl Toolkit 和 Remote CLI 软件包。

安装和使用 Remote CLI 虚拟设备

安装和使用 Remote CLI 虚拟设备包括以下步骤：

- “准备导入”（第 194 页）
- “导入虚拟设备”（第 195 页）
- “运行虚拟设备”（第 195 页）

准备导入

可通过以下两种方式之一导入虚拟设备：

- 下载虚拟设备，然后在导入虚拟设备向导中，选择 [从文件导入 (Import from File)]。可以从 http://www.vmware.com/go/remotecli 下载虚拟设备。
- 在导入虚拟设备向导中，选择 [从 URL 导入 (Import from URL)]，然后在位于 http://www.vmware.com/appliances/ 的虚拟设备市场中指向设备的位置。搜索 Remote CLI 设备并记下位置。

导入虚拟设备

下载虚拟设备或在虚拟设备市场上找到虚拟设备以后，可以开始导入虚拟设备。

导入虚拟设备

1 使用 VI Client，连接 VirtualCenter Server 或 ESX Server 主机。

2 在清单窗格中，选择设备的导入主机。

3 选择 **[文件 (File)] > [虚拟设备 (Virtual Appliance)] > [导入 (Import)]**。

此时将启动导入虚拟设备向导。您现在有两个选择：

- 单击 **[从文件导入 (Import from File)]**，浏览已经下载的 OVF 文件，然后单击 **[下一步 (Next)]**。
- 单击 **[从 URL 导入 (Import from URL)]**，浏览虚拟设备市场中的虚拟设备位置，然后单击 **[下一步 (Next)]**。

4 指定名称 （可选），然后选择虚拟机的位置。

此向导会提供所有适合的可用数据存储。

5 选择要存储虚拟机的数据存储，然后单击 **[下一步 (Next)]**。

6 检查信息，然后单击 **[完成 (Finish)]**。

此向导会在步骤 2 中选择的服务器上创建虚拟设备。此操作可能需要几分钟时间。

运行虚拟设备

导入虚拟机向导成功完成后， VI Client 清单窗格中会显示虚拟设备。

运行虚拟设备

1 选择并启动虚拟机。

2 接受最终用户许可协议并提供 root 帐户的密码以登录计算机。

现在可以登录设备并从 shell 提示符运行 Remote CLI 命令。

注意 每次运行命令时，必须提供连接信息。执行此操作的简便方法是使用配置文件。请参见 “指定 Remote CLI 的必要参数”（第 196 页）。

指定 Remote CLI 的必要参数

通过命令行或脚本执行 Remote CLI 时，至少需要指定执行服务器的名称，以及具有登录特权的用户的名称和相应密码。可以通过几种不同方式提供必要参数。

- "在命令行传递参数"（第 196 页）
- "设置环境变量"（第 196 页）
- "使用配置文件"（第 197 页）
- "使用会话文件"（第 197 页）

小心 请务必限制对配置文件的读取访问权限，尤其是当配置文件包含用户凭据时。

运行时，设备或 Remote CLI 软件包首先处理配置文件中设置的任何选项，然后处理任何环境变量，最后处理命令行的输入内容。

注意 系统始终会应用此优先顺序。例如，您无法使用配置文件覆盖环境变量设置。

在命令行传递参数

可以在命令行使用选项名称和选项值对 （某些选项没有值）传递参数。

```
--<optionname> <optionvalue>
```

例如，可以按如下所示运行 `vicfg-mpath --list`：

```
vicfg-mpath --server <server> --username <privileged_user> --password
                <password> --list
```

注意 使用引号括起密码和其他带有特殊字符的文本，或者使用反斜线 (\) 对每个特殊字符进行转义处理。特殊字符是对 shell 具有特殊含义的字符，例如 Linux 环境中的 "$"。

在 Linux 上，使用单引号 (' ')；在 Windows 上，使用双引号 (" ")。

设置环境变量

可以在 Linux 配置文件、 Microsoft Windows 系统控制面板的 [环境属性 (Environment properties)] 对话框，或者当前会话的命令行中，设置环境变量。例如：

```
set VI_SERVER=<your_server_name>
```

下面的示例显示 `/root/.visdkrc` 配置文件的内容：

```
VI_SERVER = 10.17.211.138
VI_USERNAME = root
```

```
VI_PASSWORD = <root_password>
VI_PROTOCOL = https
VI_PORTNUMBER = 443
```

注意 请勿在配置文件中对特殊字符进行转义处理。

请参见 "示例：将 NAS 数据存储添加到多台 ESX Server 3i 主机"（第 200 页）。

使用配置文件

可以使用包含变量名称和设置的文本文件作为配置文件。第 198 页上的表 A-2，"可用于所有 Remote CLI 命令的选项"中显示了对应于参数的变量。然后可以使用配置文件执行 RCLI 命令，如下面的示例所示：

```
vicfg-mpath --config <my_saved_config> --list
```

如果有多个 VirtualCenter Server 或 ESX Server 系统，并且单独管理每个系统，可以创建多个具有不同名称的配置文件。要在服务器上执行一条命令或一组命令时，可以在命令行使用适当的文件名传递 `--config` 选项。

注意 如果要将配置信息保存在非 `./visdkrc` 文件中，请使用 `--config`。如果指定 `--config`，系统会忽略 `./visdkrc` 设置。

使用会话文件

可以使用 VI Perl Toolkit `samples/session` 目录中包含的 `save_session.pl` 脚本，创建一个会话文件。该工具包是在安装 Remote CLI 软件包时自动安装的，并且包含在 Remote CLI 设备中。

创建会话文件

1 调用 `save_session.pl`。必须提供连接参数，以及脚本可以在其中保存身份验证 cookie 的会话文件的名称。 cookie 具有 30 分钟的生存期，并且不会泄露密码信息。

   如果指定服务器但没有指定用户名或密码，脚本会进行提示。

2 现在可以调用 Remote CLI 命令并使用 `--sessionfile` 参数传递会话文件。

   注意 如果使用会话文件，则任何其他连接参数都会被忽略。

可用来执行 Remote CLI 的选项

表 A-2 列出了可用于所有 Remote CLI 命令的选项。可以在命令行上使用参数，在配置文件中使用变量。

表 A-2. 可用于所有 Remote CLI 命令的选项

参数	变量	描述
`--config`	VI_CONFIG	使用指定位置的 VI Perl 配置文件。 **注意**：必须指定可以从当前目录读取的路径。
`--password`	VI_PASSWORD	使用指定密码 （与 `--username` 一起使用）登录服务器。 ■ 如果 --server 指定 VirtualCenter Server，则用户名和密码适用于该服务器。随后不需要密码即可在该服务器管理的 ESX Server 主机上执行。 ■ 如果 --server 指定 ESX Server 主机，则用户名和密码适用于该服务器。 **注意**：使用空字符串 （Linux 上为 ' '； Windows 上为 " "）指示无密码。 如果在命令行上未指定用户名和密码，系统会进行提示。
`--portnumber`	VI_PORTNUMBER	使用指定端口连接到 ESX Server 主机。默认为 443。
`--protocol`	VI_PROTOCOL	使用指定协议连接 ESX Server 主机。默认为 HTTPS。
`--server`	VI_SERVER	使用指定 VI 服务器。默认为 `localhost`。
`--servicepath`	VI_SERVICEPATH	使用指定服务路径连接 ESX Server 主机。默认为 `/sdk/webService`。
`--sessionfile`	VI_SESSIONFILE	使用指定会话 ID/cookie 文件。此选项可让您使用以前保存的会话的参数。请参见 “示例”（第 199 页）。
`--url`	VI_URL	连接指定 VI SDK URL。
`--username`	VI_USERNAME	使用指定用户名。 ■ 如果 `--server` 指定 VirtualCenter Server，则用户名和密码适用于该服务器。随后不需要密码即可在该服务器管理的 ESX Server 主机上执行。 ■ 如果 `--server` 指定 ESX Server 主机，则用户名和密码适用于该服务器。 如果在命令行上未指定用户名和密码，系统会进行提示。
`--verbose`	VI_VERBOSE	显示其他调试信息。
`--version`		显示版本信息。

示例

下面的示例说明如何传递选项。

```
cd /usr/local/viperltoolkit/samples/session
perl save_session.pl --sessionfile /tmp/vimsession
--server 10.17.211.130
--username root
--password ''
vicfg-mpath --sessionfile /tmp/vimsession --list
```

保存会话文件并使用它来连接服务器。

```
vicfg-mpath --server <server> --user snow\-white
--password dwarf\$
```

Linux：`vicfg-mpath --server <server> --user 'snow-white' --password 'dwarf$'`

Windows：`vicfg-mpath.pl --server <server> --user "snow-white" --password "dwarf$"`

以 snow-white 用户身份和密码 dwarf$ 连接到服务器。第一个示例对特殊字符进行了转义处理，另外两个使用了单引号 (Linux) 和双引号 (Windows)。

在脚本中使用 Remote CLI

如果需要管理多台 ESX Server 3i 主机，则使用脚本很可能是适当的方法。本节介绍一些常用方案和相应的脚本。您的方案和脚本会有所不同。

示例：在 ESX Server 3i 主机上编辑文件

如果要在 ESX Server 3i 主机上编辑文件，您无法直接进行编辑，因为您没有服务控制台访问权限。必须先从主机检索文件，随后进行更改，然后将文件放到 ESX Server 主机上。

例如，如果要更改主机代理日志级别，必须编辑 `hostAgentConfig.xml` 文件。下面是一个脚本，该脚本使用 `vifs` 来下载主机代理配置文件，使用 `sed` 将日志级别替换为用户提供的字符串，以及将 ESX Server 主机上的文件替换为已更改的配置文件。然后，该脚本将此过程中生成的临时文件清除。

```
HOST=your.hostname.com

vifs --server $HOST --username admin --password xxyyzz --get
              /host/hostAgentConfig.xml /tmp/ha.xml
sed -e "s#<level>.*</level>#<level>$1</level>#" < /tmp/ha.xml > /tmp/ha_new.xml
vifs --server $HOST --username admin --password xxyyzz --put /tmp/ha_new.xml
              /host/hostAgentConfig.xml
rm /tmp/ha.xml
rm /tmp/ha_new.xml
```

示例：将 NAS 数据存储添加到多台 ESX Server 3i 主机

如果要想在系统上使用新的数据存储，必须使该数据存储可用于每台 ESX Server 主机。下面的示例脚本说明如何使 NAS 数据存储可用于三台主机 （esxi_server_a、esxi_server_b 和 esxi_server_c）。

该示例假设每台主机都有一个预先配置的配置文件 /home/admin/.visdkrc.<hostname>。 esxi_server_a 的配置文件具有下面的内容：

```
VI_SERVER = esxi_server_a
VI_USERNAME = root
VI_PASSWORD = xysfdjkat
```

该脚本本身通过调用不同的配置文件来添加 NAS 数据存储。

```
#!bin/sh
for i in {"esxi_server_a","esxi_server_b","esxi_server_c"}
do
   echo "Adding NAS datastore for $i..."
   vicfg-nas --config /home/admin/.visdkrc.$i -a -o mainnas.x.com -s /shared nas_ds
   vicfg-nas --config /home/admin/.visdkrc.$i -l
done
```

远程命令行界面参考

B

本附录是在使用远程命令行界面配置 ESX Server 3i 主机时，或者为快速配置准备运行于多个主机的脚本时，可以使用的命令的参考。附录 A，“使用远程命令行界面”（第 187 页）说明如何安装和使用 RCLI。

本附录讨论以下主题：

注意 有关 `vmkfstools` 的论述，请参见附录 C，“使用 vmkfstools Remote CLI”（第 221 页）。

存储器管理命令

Remote CLI 包括本节中论述的以下存储器管理命令。

命令	请参见
vicfg-nas	"使用 vicfg-nas 管理 NAS 文件系统"（第 202 页）。
vicfg-vmhbadevs	"使用 vicfg-vmhbadevs 查找可用的 LUN"（第 203 页）。
vicfg-mpath	"使用 vicfg-mpath 配置多路径设置"（第 204 页）。
vicfg-rescan	"使用 vicfg-rescan 重新扫描"（第 206 页）。
vicfg-dumppart	"使用 vicfg-dumppart 管理诊断分区"（第 206 页）。

使用 vicfg-nas 管理 NAS 文件系统

可以使用 vicfg-nas 来操作与 ESX Server 3i 主机关联的 NAS 文件系统。有关使用 NAS 文件系统的详细信息，请参见 "网络附加存储"（第 90 页）。

vicfg-nas 的选项

可以使用以下特定于命令的选项来运行 vicfg-nas。有关其他选项，请参见 "可用于所有 Remote CLI 命令的选项"（第 198 页）。

表 B-1. vicfg-nas 的选项

选项	描述
--add -a	将新的 NAS 文件系统添加到 ESX Server 主机。 必须与 -o 和 -s 选项一起调用此选项，并且必须为新的文件系统指定标签名称。
--delete -d	删除 NAS 文件系统。 此命令卸载 NAS 文件系统并将其从已知文件系统列表中移除。
--help	显示帮助消息。
--list -l	列出所有已知的 NAS 文件系统及其装载名称、共享名称和主机名称，并指示每个文件系统是否已装载。
--nasserver <n_host> -o <n_host>	与 -a 选项一起使用，为新的 NAS 文件系统提供主机名称。
--share <share> -s <share>	与 -a 选项一起使用，为新的 NAS 文件系统提供共享名称。
--vihost <host> -h <host>	当使用指向 VirtualCenter Server 主机的 --server 选项执行 Remote CLI 时，可以使用 --vihost 来指定要在其上执行命令的 ESX Server 3i 主机。

vicfg-nas 的示例

下面的示例假设配置文件中指定了连接参数环境变量。

```
vicfg-nas -a -o fileserver.yourcompany.com -s /home FileServerHome
```

使用 vicfg-vmhbadevs 查找可用的 LUN

可以使用 vicfg-vmhbadevs 来获取有关 ESX Server 主机上可用的 LUN 的信息。默认情况下，该命令显示 vmhbaX:Y:Z 名称与控制台 /dev/ 名称的映射。

vicfg-vmhbadevs 的选项

可以使用以下选项来运行 vicfg-vmhbadevs。有关其他选项，请参见 “可用于所有 Remote CLI 命令的选项”（第 198 页）。

表 B-2. vicfg-vmhbadevs 的选项

选项	描述
--help	显示简要的用法消息。
--query -q	以 2.5 兼容模式显示输出。
--vihost <host> -h <host>	当使用指向 VirtualCenter Server 主机的 --server 选项执行 Remote CLI 时，可以使用 --vihost 来指定要用于执行命令的 ESX Server 3i 主机。
--vmfs -m	如果 LUN 是 VMFS 卷，则显示 VMFS UUID 以及 vmhba 和 /dev 名称。

vicfg-vmhbadevs 的示例

下面的示例假设配置文件中指定了连接参数环境变量。这些示例说明了执行 vicfg-vmhbadevs 以后所得到的输出。

```
#vicfg-vmhbadevs -q
vmhba1:0:0 /vmfs/devices/disks/vmhba1:0:0:0

#vicfg-vmhbadevs --vmfs
/vmfs/devices/disks/vmhba1:0:0:0 46f14706-2083a0f5-491f-001b7803ba96

# vicfg-vmhbadevs -m vmhba1:0:0:2
/vmfs/devices/disks/vmhba1:0:0:0 46f14706-2083a0f5-491f-001b7803ba96
```

使用 vicfg-mpath 配置多路径设置

可以使用 vicfg-mpath 来为光纤通道或 iSCSI LUN 配置多路径设置。有关多路径的详细信息，请参见 “管理多路径”（第 99 页）和 *《光纤通道 SAN 配置指南》*或 *《iSCSI SAN 配置指南》*。

注意 重新引导以后，不能保证虚拟机 HBA 的名称有效。可以使用 VML LUN 名称来确保一致性。

LUN 的 VML 名称是 VMware 赋予该 LUN 的唯一名称。此名称是 LUN 在全球范围内的唯一名称，并且在重新引导以后仍然与 LUN 相关联。

vicfg-mpath 的选项

可以使用以下选项来运行 vicfg-mpath。

注意 如果要更改首选路径，或者如果要更改路径的状况，请注意：

- 如果在更改路径设置时 I/O 处于活动状态，则更改操作会失败。在这种情况下，请重新发出命令。
- 要使更改生效，必须至少发布一项 I/O 操作。

有关其他选项，请参见 “可用于所有 Remote CLI 命令的选项”（第 198 页）。

表 B-3. vicfg-mpath 的选项

选项	描述
--bulk -b	以易于分析的脚本格式显示所有 LUN 和路径。
--detailed -d	显示有关 LUN 及其路径的所有信息，包括 LUN 的 VML 名称。 LUN 的 VML 名称是 VMware 分配给 LUN 的唯一名称。此名称是 LUN 在全球范围内的唯一名称，并且在重新引导以后仍然与 LUN 相关联。
--hbas -a	可通过唯一 ID 识别的 HBA 列表，其中包括光纤通道和 iSCSI 设备。并行设备和块设备不会显示在此列表中。
--help	显示帮助消息。
--list -l	列出系统上的所有 LUN 和通过适配器到达这些 LUN 的路径。针对每个 LUN，此命令显示类型、内部名称、控制台名称、大小、路径和路径选择策略。
--lun=<lun> -L=<lun>	指定用于操作的 LUN 的必要选项。此选项是其他选项的必要参数，不单独使用。

表 B-3. vicfg–mpath 的选项 （续）

选项	描述
--path=<path> –P=<path>	指定用于操作的路径的必要选项。此选项是其他选项的必要参数，不单独使用。
--policy [mru|fixed] –p [mru|fixed]	将特定 LUN 的策略设置为 mru 或 fixed。必须使用 --lun 选项指定 LUN。 ■ [最近使用 (Most Recently Used)] (mru) 选择最近使用的路径来将 I/O 发送到设备。 ■ [固定的 (Fixed)] (fixed) 仅使用活动路径。 **注意**：可以使用其他两个*实验性地* 策略：循环 (Round Robin, rr) 和自定义。请参见 *《循环负载平衡》* 技术说明。
--preferred –f	将指定路径设置为指定 LUN 的首选路径。设置此选项时，还必须设置 --lun 和 --path 选项。
--query –q	查询特定的 LUN 以获取其信息并显示信息。设置此选项时，还必须设置 --lun 选项。
--state [on|off] –s [on|off]	将特定 LUN 路径的状况设置为 on 或 off。 此选项还需要设置 --lun 和 --path 选项。
--vihost <host> –h <host>	当使用指向 VirtualCenter Server 主机的 --server 选项执行 Remote CLI 时，可以使用 --vihost 来指定执行命令的 ESX Server 3i 主机。

vicfg-mpath 的示例

下面的示例假设配置文件中指定了连接参数环境变量。

`vicfg–mpath –l`

显示所有可用路径。

```
vicfg–mpath –q
--lun=vml.123456
```

显示磁盘 vml.123456 的路径。

```
vicfg–mpath --policy=mru
--lun=vmhba0:0:1
```

将磁盘 vmhba0:0:1 的路径策略设置为 mru。

```
vicfg–mpath
--policy fixed
--path vmhba2:0:1
--lun vmhba2:0:1
--preferred
```

设置首选路径，产生以下输出：

```
Setting vmhba2:0:1 –– vmhba2:0:1 as preferred path
Setting vmhba2:0:1 policy to fixed
```

```
vicfg–mpath
--path=vmhba1:0:1
--lun=vmhba0:0:1 --state=on
```

启用磁盘 vmhba0:0:1 的路径。

`vicfg-mpath --path=vmhba0:1:1 --state=off --lun=vmhba0:0:1 -p fixed`	为磁盘 `vmhba0:0:1` 禁用路径并将策略设置为固定的。
`vicfg-mpath -l`	列出系统上的所有 LUN 和通过适配器到达这些 LUN 的路径。

`vicfg-mpath -a`	产生如下形式的输出。
	`vmhba2 2305843973628581845 42:2.0`
	`vmhba3 2305843973628747050 4c:00.0`
	`vmhba4 2306125448607554858 4c:00.1`
	`vmhba5 50:1.1`

使用 vicfg-rescan 重新扫描

执行特定的存储器管理操作以后，需要重新扫描。可以使用 `vicfg-rescan` 来执行重新扫描操作。请参见 “重新执行扫描”（第 89 页）。*《光纤通道 SAN 配置指南》*详细论述了重新扫描操作。

注意 在 ESX Server 3i 主机上执行重新扫描时，该命令只返回成功或失败的指示，不返回详细信息。

vicfg-rescan 的选项

可以使用以下选项来运行 `vicfg-rescan`。有关其他选项，请参见 “可用于所有 Remote CLI 命令的选项”（第 198 页）。

表 B-4. `vicfg-rescan` 的选项

选项	描述
`<vmkernel_SCSI_adapter_name>`	要扫描的适配器的名称，例如 `vmhba0`。
`--help`	显示此命令的帮助信息。
`--vihost <host>` `-h <host>`	当使用指向 VirtualCenter Server 主机的 `--server` 选项执行 Remote CLI 时，可以使用 `--vihost` 来指定执行命令的 ESX Server 3i 主机。

使用 vicfg-dumppart 管理诊断分区

可以使用 `vicfg-dumppart` 来查询、设置和扫描 ESX Server 3i 主机的诊断分区。有关诊断分区的详细信息，请参见 “创建诊断分区”（第 92 页）。

注意 运行 vicfg-dumppart Remote CLI 时，不显示分区的控制台名称。

因为选择的分区是自动激活的，所以活动和已配置状况是冗余的，不会显示。

vicfg-dumppart 的选项

可以使用以下选项来运行 vicfg-dumppart。有关其他选项，请参见 "可用于所有 Remote CLI 命令的选项"（第 198 页）。

表 B-5. vicfg-dumppart 的选项

选项	描述
--activate -a	激活已配置的诊断分区。 此选项是为实现向后兼容性而提供的，与 --set 的作用相同。
--deactivate -d	取消激活当前活动诊断分区。该选项也会取消设置转储分区。 **警告**：如果使用此选项运行 vicfg-dumppart，则直到激活另一个分区，系统才会将错误写入文件。如果出现错误，则会丢失任何错误记录。
--find -f	使用与 list 选项相同的方法，在此 ESX Server 3i 主机上查找所有诊断分区。按该类型的存储器用于诊断分区的要求顺序显示分区。顺序为：并行适配器、块适配器、光纤通道、硬件 iSCSI、软件 iSCSI。
--get-active -t	获取此系统的活动诊断分区。使用此选项运行 vicfg-dumppart 可以返回分区的内部名称 (vmbhaX:X:X:X) 或 none （如果未设置分区）。
--get-config -c	获取系统的已配置诊断分区。此分区可能是、也可能不是活动分区。如果诊断分区在 SAN 上，有可能已不再处于连接状态。
---help	显示帮助消息。
--list -l	列出系统上具有适合作为 ESX Server 诊断分区的分区类型的所有分区。 **小心**：执行此命令会扫描系统上的所有 LUN。执行过程可能需要几分钟时间，并且会使 ESX Server 3i 主机变慢。
--set vmbha<X:X:X:X> -s vmbha<X:X:X:X>	通过需使用的分区的 vmhba 名称，为此系统设置活动和已配置的诊断分区。 诊断分区在设置以后会自动激活。活动诊断分区和已配置诊断分区之间没有区别。将 --activate 选项包括在内只是为了实现向后兼容。
--vihost <host> -h <host	当使用指向 VirtualCenter Server 主机的 --server 选项执行 Remote CLI 时，可以使用 --vihost 来指定执行命令的 ESX Server 3i 主机。

vicfg-dumppart 的示例

下面的示例假设配置文件中指定了连接参数环境变量。

`vicfg-dumppart -t vmhba1:0:0:5 /dev/sda5`	显示 VMkernel 使用的当前诊断分区。
`vicfg-dumppart -c vmhba1:0:0:5 /dev/sda5`	显示 `esx.conf` 中配置为诊断分区的分区。
`vicfg-dumppart -s vmhba1:0:0:6`	更改 `-c` 和 `-t` 的输出，报告 `vmhba1:0:0:6`，而不是 `vmhba1:0:0:5`。
`vicfg-dumppart -f`	查找可以用作诊断分区的所有分区 （基本上是 `-l` 的不同格式）。输出可能显示如下。 `Partition number 5 on vml.010000000055505436503341303148443334d4150333336 -> vmhba1:0:0:5 -> /dev/sda5 Partition number 6 on vml.010000000055505436503341303148443334d4150333336 -> vmhba1:0:0:6 -> /dev/sda6 Partition number 7 on vml.010000000055505436503341303148443334d4150333336 -> vmhba1:0:0:7 -> /dev/sda7 Partition number 1 on vml.010000000033485a394757375a535433373333 -> vmhba1:3:0:1 -> /dev/sdb1`
`vicfg-dumppart -d`	取消激活诊断分区。执行此命令以后，将不设置诊断分区。

网络命令

Remote CLI 包括本节中论述的以下网络命令。

命令	请参见
`vicfg-nics`	“使用 vicfg-nics 管理物理网络适配器”（第 208 页）
`vicfg-vmknic`	“使用 vicfg-vmknic 管理 VMkernel 网卡”（第 209 页）
`vicfg-vswitch`	“使用 vicfg-vswitch 管理虚拟交换机”（第 210 页）
`vicfg-ntp`	“使用 vicfg-ntp 指定 NTP 服务器”（第 213 页）

使用 vicfg-nics 管理物理网络适配器

可以使用 `vicfg-nics` 来管理物理网络适配器，即 ESX Server 3i 主机使用的以太网交换机。 `--list` 选项显示网络适配器的 VMkernel 名称、 PCI ID、驱动程序、链路状况、速度、双工和网卡的简短 PCI 描述。

还可以使用 vicfg-nics 指定网络适配器的速度和双工设置。

有关网络的介绍，请参见第 21 页上的第 2 章，“网络”。

vicfg-nics 的选项

可以使用以下选项来运行 vicfg-nics。有关其他选项，请参见 “可用于所有 Remote CLI 命令的选项”（第 198 页）。

表 B-6. vicfg-nics 的选项

选项	描述
--auto -a	将特定网络适配器设置为自动协商其速度和双工设置。
--duplex [full|half] <nic> -d [full|half] <nic>	将特定网络适配器运行的双工值设置为 full （双向同时传输数据）或 half （某一时刻在一个方向上传输数据）。
--help	显示帮助消息。
--list -l	列出系统中的网络适配器，并显示它们当前的和配置的速度和双工信息。
--speed <speed> <nic> -s <speed> <nic>	设置特定网络适配器的运行速度。< 速度 > 的有效值为 10、 100、 1000 或 10000。
--vihost <host> -h <host>	当使用指向 VirtualCenter Server 主机的 --server 选项执行 Remote CLI 时，可以使用 --vihost 来指定执行命令的 ESX Server 3i 主机。

使用 vicfg-vmknic 管理 VMkernel 网卡

可以使用 vicfg-vmknic 来配置虚拟网络适配器。

与 --del 和 --enable 选项一起使用的 <port_group> 参数指定 VMkernel 网卡所关联的端口组。

vicfg-vmknic 的选项

可以使用以下选项来运行 vicfg-vmknic。有关其他选项，请参见 “可用于所有 Remote CLI 命令的选项”（第 198 页）。

表 B-7. vicfg-vmknic 的选项

选项	描述
--add -a	将虚拟网络适配器添加到系统。必须指定 IP 参数和端口组名称。该命令成功完成时，会启用新添加的虚拟网络适配器。
--del <port_group> -d <port_group>	删除指定端口组上的虚拟网络适配器。
--help	显示此命令的帮助消息。
--ip <ipaddress> | DHCP -i <ipaddress> | DHCP	设置要用于虚拟网络适配器的 IP 地址 (X.X.X.X)。设置 IP 地址时，必须在同一条命令中指定 --netmask 选项。 如果指定 DHCP，而不是 IP 地址， VMkernel 必须支持 DHCP。
--list -l	列出系统上的虚拟网络适配器。列表包含系统中每个虚拟网络适配器的网络信息、端口组、 MTU 和当前状况。
--netmask <netmask> -n	要用于虚拟网络适配器的 IP 子网掩码 (X.X.X.X)。设置子网掩码时，必须在同一条命令中指定 --ip 选项。
--vihost <host> -h <host>	当使用指向 VirtualCenter Server 主机的 --server 选项执行 Remote CLI 时，可以使用 --vihost 来指定执行该命令的 ESX Server 3i 主机。

使用 vicfg-vswitch 管理虚拟交换机

可以使用 vicfg-vswitch 来添加、移除和修改虚拟交换机及其设置。虚拟交换机是虚拟网络设备。它可在虚拟机之间进行内部流量路由或链接至外部网络。请参见 “虚拟交换机”（第 23 页）。

默认情况下，有一个名为 vSwitch0 的虚拟交换机。

vicfg-vswitch 的选项

可以使用以下选项运行 vicfg-vswitch。有关其他选项，请参见 “可用于所有 Remote CLI 命令的选项”（第 198 页）。

表 B-8. vicfg–vswitch 的选项

选项	描述
--add <vswitch_name> -a <vswitch_name>	将指定虚拟交换机添加到系统。
--add-pg <portgroup> <switch> -A <portgroup> <switch>	将端口组添加到指定虚拟交换机。
--check <virtual_switch> -c <virtual_switch>	检查是否有虚拟交换机存在。如果交换机存在，则该命令显示 1，否则显示 0。 使用虚拟交换机名称，例如 vSwitch0 或 vSwitch1，指定虚拟交换机。
--check-pg <port_group> -C <port_group>	检查是否有指定端口组存在。
--delete <vswitch_name> -d <vswitch_name>	删除虚拟交换机。如果虚拟交换机上的任何端口仍由 VMkernel 网络、vswifs 或虚拟机使用，则使用此选项执行该命令会失败。
--del-pg <portgroup> -D <portgroup>	删除端口组。如果正在使用端口组，则使用此选项执行该命令会失败。
--help	显示帮助消息。
--link <pnic> -L <pnic>	将上行链路适配器添加到虚拟交换机。使用此选项执行该命令会将未使用的新物理网络适配器连接到虚拟交换机。
--list -l	列出所有虚拟交换机及其端口组。
--mtu -m	设置虚拟交换机的最大传输单元 (Maximum Transmission Unit, MTU)。此选项会影响分配给虚拟交换机的所有上行链路。
--pg <port group> -p <port group>	为 --vlan 选项提供端口组的名称。指定 ALL 在虚拟交换机的所有端口组上设置 VLAN ID。
--unlink <pnic> -U <pnic>	将上行链路适配器从虚拟交换机中移除。上行链路适配器是虚拟交换机连接的物理以太网适配器。如果移除最后一个上行链路，则该交换机的物理网络连接会丢失。
--vihost <host> -h <host>	当使用指向 VirtualCenter Server 主机的 --server 选项执行 Remote CLI 时，可以使用 --vihost 来指定执行该命令的 ESX Server 3i 主机。
--vlan -v	为虚拟交换机的特定端口组设置 VLAN ID。将该选项设置为 0 会禁用此端口组的 VLAN。 如果指定此选项，还必须指定 --pg 选项。

vicfg-vswitch 的示例

下面的示例假设配置文件中指定了连接参数环境变量。

`vicfg-vswitch --add vSwitch1`	添加 vSwitch1 作为虚拟交换机。
`vicfg-vswitch --add-pg="<New_Portgroup>" vSwitch0`	将端口组添加到 vSwitch0。
`vicfg-vswitch -c vSwitch0`	检查是存在 vSwitch0。如果交换机存在，则显示 1；如果交换机不存在，则显示 0。
`vicfg-vswitch -m 9000 vswitch0`	将虚拟交换机 vswitch0 的 MTU 设置为 9000。
`vicfg-vswitch -l`	显示如下形式的信息。

```
Switch Name    Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch0       64          5           64                1500    vmnic2,vmnic0

  PortGroup Name      VLAN ID  Used Ports  Uplinks
  group1              0        0           vmnic0,vmnic2
  group2              0        0           vmnic0,vmnic2
  group3              0        1           vmnic0,vmnic2

Switch Name    Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch1       64          1           64                1500

          PortGroup Name      VLAN ID  Used Ports  Uplinks
  bldg1               0        0
  bldg2               0        0
  bldg3               0        0

Switch Name    Num Ports   Used Ports  Configured Ports  MTU     Uplinks
vSwitch2       64          1           64                1500

  PortGroup Name      VLAN ID  Used Ports  Uplinks
  Right               0        0
  Left                0        0
  Down                0        0
  Up                  0        0
```

使用 vicfg-ntp 指定 NTP 服务器

vicfg-ntp 命令可让您为 ESX Server 3i 主机指定 NTP 服务器。

vicfg-ntp 的选项

可以将 vicfg-ntp 与以下选项配合使用。有关其他选项，请参见 "可用于所有 Remote CLI 命令的选项"（第 198 页）。

表 B-9. vicfg-ntp 的选项

选项	描述
--add <server> -a <server>	添加主机名称或 IP 地址指定的 NTP 服务器。
--delete <server> -d <server>	删除主机名称或 IP 地址指定的 NTP 服务器。
--help	显示此命令的帮助信息。
--list -l	显示此主机使用的所有 NTP 服务器的列表。
--vihost <host> -h <host>	当使用指向 VirtualCenter Server 主机的 --server 选项执行 Remote CLI 时，可以使用 --vihost 来指定执行该命令的 ESX Server 3i 主机。

使用 vicfg-route 操作路由条目

可以使用 vicfg-route 显示或设置 VMkernel 默认 IP 路由表。 vicfg-route 命令支持 Linux route 命令选项的子集。

vicfg-route 的选项

可以使用以下选项运行 vicfg-route。有关其他选项，请参见 "可用于所有 Remote CLI 命令的选项"（第 198 页）。

表 B-10. vicfg-route 的选项

选项	描述
<gateway>	应设置为 VMkernel IP 堆栈网关的计算机的 IP 地址或主机名称。
--help	显示帮助消息。
--vihost <host> -h <host>	当使用指向 VirtualCenter Server 主机的 --server 选项执行 Remote CLI 时，可以使用 --vihost 来指定执行该命令的 ESX Server 3i 主机。

如果未指定选项，该命令显示默认网关。可以通过执行 vicfg-route <gateway> 来设置默认网关。

杂项管理命令

Remote CLI 包括本节中论述的以下杂项命令。

命令	请参见
vihostupdate	"使用 vihostupdate 进行性能维护"
vicfg-syslog	"使用 vicfg-syslog 指定 syslog 服务器"（第 216 页）
vicfg-advcfg	"在特殊情况下使用 vicfg-advcfg"（第 216 页）

使用 vihostupdate 进行性能维护

可以使用 vihostupdate 命令来维护 VMware ESX Server 3i 主机。该命令可以安装软件更新、强制执行软件更新策略，以及跟踪已安装的软件。

注意 与大多数其他 Remote CLI 命令相反，必须直接在 ESX Server 3i 主机上执行此命令。不支持从 VirtualCenter Server 更新和指定 --vihost 选项。

在更新 ESX Server 3i 主机的固件之前，必须能够在运行 vihostupdate 命令的计算机上本地访问更新包。更新进程首先将更新捆绑包推到主机，然后请求主机执行更新。

软件更新可能是用于解决重大安全问题的修补程序或紧急的缺陷修复，也可能是一般更新或维护版本。它们可能位于本地文件系统或 NFS、 FTP 或 HTTP 服务器上。每个更新都包含一个描述符文件和一组软件包。描述符控制安装过程并检查是否已满足各项要求。例如，可能必须关闭运行于要更新的服务器上的所有虚拟机，或者可能需要在更新以后重新启动服务器。

注意 有关 vihostupdate 的详细论述，请参见 *《ESX Server 3i 设置指南》*。

可以执行 vihostupdate --help 来显示简要的帮助屏幕。

vihostupdate 的选项

可以使用以下选项来运行 vihostupdate。有关其他选项，请参见 “可用于所有 Remote CLI 命令的选项”（第 198 页）。

表 B-11. vihostupdate 的选项

选项	描述
--bundle -b <bundle_file_name>	打开下载的捆绑包 ZIP 文件。如果指定此选项，则无法指定 --metadata。
--help	显示此命令的帮助信息。
--install -i	使用更新捆绑包中的可用软件包修补主机。此选项没有参数，但还必须包括 -b 以指定捆绑包，或者 -m 以指定元数据文件。
--metadata -m <metadata_xml_file>	包含更新捆绑包相关信息的 metadata.xml 文件的路径。如果指定此选项，则无法指定 --bundle。
--query -q	列出主机上安装的软件包。此选项返回 ESX Server 主机的版本信息，以及安装的所有软件包及其版本号。
--scan <dir> -s	在 <dir> 指定的目录中扫描是否有适用于主机的软件包。

vihostupdate 的示例

下面的示例假设配置文件中指定了连接参数环境变量。

假设捆绑包的路径为 EESX-142-test-release.zip。如果随后转到复制了该捆绑包的目录，可以执行下面的命令：

vihostupdate -i -b EESX-142-test-release.zip	打开软件包并修补主机
vihostupdate -b EESX-142-test-release.zip	解压文件，但*不*修补主机。
vihostupdate -i -m EESX-142-test-release.zip/metadata.xml	使用文件 EESX-142-test-release.zip 修补主机。

运行第一个示例相当于依次运行第二个和第三个示例。

使用 vicfg-syslog 指定 syslog 服务器

vicfg-syslog 命令可让您为主机指定远程 syslog 服务器。*《基本系统管理》*手册详细论述了系统日志并且说明了如何使用 VI Client 来设置系统日志。

vicfg-syslog 的选项

可以将 vicfg-syslog 与以下选项配合使用。有关其他选项，请参见 "可用于所有 Remote CLI 命令的选项"（第 198 页）。

表 B-12. vicfg-syslog 的选项

选项	描述
--help	显示此命令的帮助信息。
--setport -p	为 syslog 服务器设置端口。可以与 -s 一起使用。
--setserver <server> -s <server>	远程 syslog 服务器的主机名称或 IP 地址。可以与 -p 一起使用。
--show -i	如果已设置了 syslog 服务器，则显示远程 syslog 服务器。
--vihost <host> -h <host	当使用指向 VirtualCenter Server 主机的 --server 选项执行 Remote CLI 时，可以使用 --vihost 来指定执行该命令的 ESX Server 3i 主机。

在特殊情况下使用 vicfg-advcfg

vicfg-advcfg 命令执行许多低层高级选项，一般不希望客户使用。当 VMware 技术支持或 VMware 知识库文章指示您使用此命令时，您可能会用到它。

使用 vifs 执行文件系统操作

vifs 命令可让您对文件和目录执行一些常见操作，例如复制、移除、获取和存放。

注意 还可以使用 Web 浏览器浏览数据存储内容和主机文件。连接下面的位置：

```
http://ESX3ihost_IP_Address/host
http://ESX3ihost_IP_Address/folder
```

可以从此根 URL 查看数据中心和数据存储目录。

文件和目录组

可以将文件和目录分为三组。 vifs 命令支持这三个组，但每组可以使用不同的操作。

- 主机 - 主机配置文件。必须指定文件的唯一名称标识符。

可以使用 host/<path> 语法指定主机位置。

- 临时 - /tmp 目录和该目录中的文件。

  可以使用 tmp/dir/subdir 语法指定临时位置。

- 数据存储 - 数据存储文件和目录。指定数据存储有两个选择：

  - 数据存储前缀样式 '[ds_name] relative_path'

    例如 '[myStorage1] testvms/vm1/VM1.vmx'

  - URL 样式 /folder/dir/subdir/file&dsName=<name>

    例如 '/folder/testvms/VM1/VM1.vmx&dsName=myStorage1

  这两个示例的路径引用 myStorage1 数据存储 testvms/VM1 目录中虚拟机 VM1 的同一个虚拟机配置文件。

注意 因为目录名称通常使用特殊字符或空格，所以对于这两种样式，强烈建议为路径加上引号。

运行 vifs

运行 vifs 时，可以指定操作名称和参数，以及表 A-2 中论述的标准连接参数之一。可以使用别名、符号链接或包装脚本来简化调用语法。

通过将操作名称以及随后的适当参数传递给 vifs 命令，可以执行每个操作。例如：

```
vifs --dir '[myvmfs] dir_3'
```

注意 vifs 命令没有工作目录或者最后一次操作的目录或文件的概念。

vifs 的选项

表 B-13 按字母顺序列出了所有的 vifs 命令操作。所有 vifs 命令操作都可以处理数据存储文件或目录。某些操作还可以处理主机文件和 temp 目录中的文件，如表 B-13 中所示。有关其他选项，请参见 "可用于所有 Remote CLI 命令的选项"（第 198 页）。

表 B-13. 可用于 vifs 的操作

命令	描述	用于……	示例
--copy -c <source> <target>	将数据存储中的文件复制到数据存储中的另一个位置。<source> 必须是远程源路径，<target> 必须是远程目标路径或目录。 --force 选项替换现有目标文件。	数据存储（临时）	move src_file_path dst_directory_path [--force] move src_file_path dst_file_path [--force]
--dir -D <remote_dir>	列出数据存储目录的内容。	数据存储（临时）	dir datastore_directory_path
--get -g <remote_path> <local_path>	将文件从 ESX Server 3i 主机下载到运行 Remote CLI 的计算机上。此操作使用 HTTP GET。	数据存储（主机）	get src_dstore_file_path dst_local_file_path get src_d store_dir_path dst_local_file_path
--listdc -C	列出服务器上可用的数据中心路径。	数据存储（主机）	
--listds -S	列出服务器上的数据存储名称。当有多个数据中心可用时，可以使用 --dc (-Z) 参数来指定用于列出数据存储的数据中心的名称。	数据存储（主机）	vifs --listds
--mkdir -M <remote_dir>	在数据存储中创建目录。如果 dst_datastore_file_path 的父目录不存在，此操作会失败。	数据存储（临时）	mkdir dst_directory_path
--move -m <source> <target>	在数据存储中移动文件。<source> 必须是远程源路径，<target> 必须是远程目标路径或目录。 --force 选项替换现有目标文件。	数据存储（临时）	copy src_file_path dst_directory_path [--force] copy src_file_path dst_file_path [--force]
--put -p <local_path> <remote_path>	将文件从运行 Remote CLI 的计算机上传到 ESX Server 3i 主机。此操作使用 HTTP PUT。 **注意**：此命令可以替换现有主机文件，但无法创建新文件。	数据存储（主机，临时）	put src_local_file_path dst_file_path put src_local_file_path dst_directory_path
--rm -r <remote_path>	删除数据存储文件。	数据存储（临时）	rm dst_file_path
--rmdir -R <remote_dir>	删除数据存储目录。如果目录不是空的，此操作会失败。	数据存储（临时）	rmdir dst_directory_path

vifs 的示例

本节列举一些 vifs 的示例。只有在直接连接 ESX Server 3i 主机时，执行 vifs 才会起作用。如果连接 VirtualCenter Server 并尝试通过 VirtualCenter Server 连接 ESX Server 3i 主机，则该命令不起作用。

注意 可以在 Linux 系统上执行下列命令。对于 Windows 系统上的相应命令，请使用双引号 （而不是单引号）并且添加扩展名 .pl。

vifs --copy '[myvmfs] dir_1/my_text' '[myvmfs] dir_3/text'	将 my_text 文件从 dir_1 复制到 dir_3。
vifs --dir '[myvmfs] dir_3'	列出目录 dir_3 的内容。
vifs --copy '[myvmfs] dir_1/my_text' '[myvmfs] dir_3/my_text' --force	如果使用此命令，并且 dir_3 中已经有一个名为 my_text 的文件，则现有文件会由于 –force 选项的原因而被覆盖。
vifs --mkdir '[myvmfs] new_dir'	创建名为 new_dir 的目录。
vifs --put /root/test_put '[myvmfs] new_dir/test_put'	将本地 test_put 文件的副本放到指定服务器的 new_dir 目录中。
vifs --rm '[myvmfs] new_dir/test_put'	将 test_put 文件从 new_dir 文件夹中移除。
vifs --rmdir '[myvmfs] new_dir'	移除 new_dir 文件夹。
vifs --get '[myvmfs] dir_1/my_text' /root/my_text	从 ESX Server 3i 主机检索文件 my_text 并将其放到本机的 root 文件夹中。
vifs --move '[myvmfs] dir_1/my_text' '[myvmfs] dir_3/my_text'	将 my_text 文件从 dir_1 移至 dir_3。
vifs --listds	列出配置文件中指定服务器上所有数据存储的名称。可以使用返回的每个名称并使用方括号来引用数据存储路径，如下所示： ‘[my_datastore] dir/subdir/file’

带有 esxcfg 前缀的命令

对于本附录中列出的几个命令，有一些相应的服务控制台命令，这些命令以 `esxcfg` 前缀开头，您可能已在脚本中使用了这些命令来管理 ESX Server 3.0。为了便于从 ESX Server 3.0 迁移到 ESX Server 3i，带前缀为 `esxcfg` 的命令可以用作 Remote CLI 命令。

注意 VMware 建议使用前缀为 `vicfg` 的命令。之所以提供前缀为 `esxcfg` 的命令，主要是因为兼容性的原因，将来可能会弃用。

表 B-14 列出了带有 `esxcfg` 前缀的命令可用于的所有 Remote CLI 命令。

表 B-14. 带有 `esxcfg` 前缀的命令

带有 vicfg 前缀的命令	带有 esxcfg 前缀的命令	请参见
vicfg-advcfg	esxcfg-advcfg	“在特殊情况下使用 vicfg-advcfg”（第 216 页）。
vicfg-cfgbackup	esxcfg-cfgbackup	请参见 *《ESX Server 3i 设置指南》*。
vicfg-dumppart	esxcfg-dumppart	“使用 vicfg-dumppart 管理诊断分区”（第 206 页）。
vicfg-mpath	esxcfg-mpath	“使用 vicfg-mpath 配置多路径设置”（第 204 页）。
vicfg-nas	esxcfg-nas	“使用 vicfg-nas 管理 NAS 文件系统”（第 202 页）。
vicfg-nics	esxcfg-nics	“使用 vicfg-nics 管理物理网络适配器”（第 208 页）。
vicfg-rescan	esxcfg-rescan	“使用 vicfg-rescan 重新扫描”（第 206 页）。
vicfg-route	esxcfg-route	“使用 vicfg-route 操作路由条目”（第 213 页）。
vicfg-snmp	esxcfg-snmp	*《基本系统管理》*手册。
vicfg-vmhbadevs	esxcfg-vmhbadevs	“使用 vicfg-vmhbadevs 查找可用的 LUN”（第 203 页）。
vicfg-vmknic	esxcfg-vmknic	“使用 vicfg-vmknic 管理 VMkernel 网卡”（第 209 页）。
vicfg-vswitch	esxcfg-vswitch	“使用 vicfg-vswitch 管理虚拟交换机”（第 210 页）。

使用 vmkfstools Remote CLI

C

可以使用 vmkfstools Remote CLI 来创建和操作 VMware ESX Server 3i 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 可在磁盘的物理分区上创建和管理虚拟机文件系统 (Virtual Machine File System, VMFS)。还可以使用 vmkfstools 操作文件，例如存储在 VMFS-3 和 NFS 上的虚拟磁盘。

注意 ESX Server 3i 上的 vmkfstools 命令不支持 ESX Server 3 版本 3.5 支持的所有选项。

可使用 VI Client 执行大多数 vmkfstools 操作。有关 VI Client 和存储器配合使用的信息，请参见 “配置存储器”（第 69 页）。

本附录包括以下各节：

安装和执行 vmkfstools Remote CLI

安装 Remote CLI 虚拟设备时，或者在 Linux 或 Windows 管理服务器上安装 Remote CLI 软件包时，会安装 vmkfstools Remote CLI。请参见 “在 Linux 上安装和使用 Remote CLI”（第 191 页）、“在 Windows 上安装和使用 Remote CLI”（第 193 页）和 “安装和使用 Remote CLI 虚拟设备”（第 194 页）。

可以像任何其他 Remote CLI 那样执行 vmkfstools Remote CLI。指定要在其上执行该命令的 ESX Server 3i 主机，并指定其他选项，如 “指定 Remote CLI 的必要参数”（第 196 页）中所述。

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：

- < 选项 > 为一个或多个命令行选项及相关联的子选项，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。

- < 分区 > 指定磁盘分区。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。

- < 设备 > 指定设备或逻辑卷。此参数使用 ESX Server 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 逻辑卷。
  - /vmfs/devices/generic 适用于通用 SCSI 设备，例如磁带驱动器。

- < 路径 > 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/< 文件系统标签 | 文件系统 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。

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。某些选项仅供高级用户使用。有关每个 Remote CLI 支持的其他选项，请参见 "可用于所有 Remote CLI 命令的选项"（第 198 页）。

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
```

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 文件系统。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>
```

此选项将在指定的 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。

小心 一个 LUN 只有一个 VMFS 卷。

在任何 ESX Server 3i 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。

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。默认的文件块大小为 1 MB。指定的 <block_size> 值必须是 128 kb 的倍数，最小值为 128 kb。输入大小时，请加上后缀 （例如 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 的含义解释为兆字节，将 k 或 K 的含义解释为千字节。
- -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 vmkfstools 调用中指定 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> 是要用于 <UUID> VMFS 的新卷标。

创建 VMFS 文件系统的示例

下面的示例假设配置文件中指定了连接参数环境变量。

```
vmkfstools –C vmfs3 –b 1m –S my_vmfs/vmfs/devices/disks/vmhba1:3:0:1
```

在 SCSI 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。

```
vmkfstools –C vmfs3 –S my_vmfs vmhba1:0:0:4

vmkfstools ––createfs vmfs3 ––setfsname my_vmfs vmhba1:0:0:4

vmkfstools ––createfs vmfs3 ––blocksize 1m––setfsname my_vmfs vmhba1:0:0:4

vmkfstools ––createfs vmfs3 –b 4m ––setfsname my_vmfs vmhba1:0:0:4
```

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> 添加一个扩展。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，之前在 <extension–device> 中指定的 SCSI 设备上保存的所有数据均将丢失。

扩展现有卷的示例

下面的示例假设配置文件中指定了连接参数环境变量。

```
vmkfstools –Z /vmfs/devices/disks/vmhba0:1:2:1
    /vmfs/devices/disks/vmhba0:3:0:1
```

说明如何通过允许逻辑文件系统跨到新分区来对其进行扩展。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
```

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 卷中的扩展数、卷标 （如果有）、 UUID 以及各个扩展所驻留的设备名称列表。

列出属性的示例

下面的示例假设配置文件中指定了连接参数环境变量。

```
vmkfstools --queryfs /vmfs/volumes/my_vmfs
```

此命令可能返回下列内容：

```
VMFS-3.31 file system spanning 1 partitions.
Capacity :65229815808, 64641564672 avail
File system label :my_vmfs
UUID :46fd1460-6ec4e2b8-e048-000e0c7f4088
Path:/vmfs/volumes/46fd1460-6ec4e2b8-e048-000e0c7f4088
Partitions spanned:
       vmhba2:0:0:6
```

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。

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根据需要将其置零。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` 格式相反，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。只允许超级用户以此格式创建磁盘。
- `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 <大小>[kK|mM|gG]
      -a --adaptertype [buslogic|lsilogic] <srcfile>
      -d --diskformat [thin|zeroedthick|eagerzeroedthick]
```

此选项将在 VMFS 卷上按指定的位置创建虚拟磁盘。需要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 225 页）。

创建虚拟磁盘的示例

下面的示例假设配置文件中指定了连接参数环境变量。

```
vmkfstools -c 2048m /vmfs/volumes/my_vmfs/myOS.vmdk
```

在名称为 myVMFS 的 VMFS 文件系统中创建一个名为 myOS.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。

```
vmkfstools --createvirtualdisk 20m /vmfs/volumes/store1/test.vmdk
```

创建名为 test.vmdk 的 20 MB 虚拟磁盘。

```
vmkfstools --createvirtualdisk 20mb
    -d thin -a lsilogic /vmfs/volumes/M1/test.vmdk
```

创建一个与指定适配器关联的虚拟磁盘。

```
vmkfstools -c 200m /vmfs/volumes/my_vmfs/test01.vmdk
```

在名称为 my_vmfs 的 VMFS 文件系统中创建一个名为 test01.vmdk、大小为 200 MB 的虚拟磁盘。

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。

初始化虚拟磁盘的示例

下面的示例假设配置文件中指定了连接参数环境变量。

```
vmkfstools -w /vmfs/volumes/my_vmfs/test01.vmdk

vmkfstools --writezeros /vmfs/volumes/my_vmfs/text02.vmdk
```

填充精简虚拟磁盘

```
-j --inflatedisk
```

此选项将 thin 虚拟磁盘转换为 eagerzeroedthick 格式，并保留所有现有数据。

有关磁盘格式的详细信息，请参见 “受支持的磁盘格式”（第 225 页）。

填充虚拟磁盘的示例

下面的示例假设配置文件中指定了连接参数环境变量。

```
vmkfstools --inflatedisk '[myVMFS] testsep1.vmdk'

vmkfstools -j '[myVMFS] test02.vmdk'

vmkfstools --inflatedisk -a buslogic  /vmfs/volumes/myvmfs/thin.vmdk
```

删除虚拟磁盘

下面的示例假设配置文件中指定了连接参数环境变量。

```
-U --deletevirtualdisk
```

此选项将删除与虚拟磁盘 （它是在 VMFS 卷上指定路径中的虚拟磁盘）相关联的文件。

删除虚拟磁盘的示例

下面的示例删除虚拟磁盘 `test.vmdk`。该示例会提示您输入指定服务器的用户名和密码。

```
vmkfstools --server server1 -U /vmfs/volumes/store/test.vmdk
```

重命名虚拟磁盘

```
-E --renamevirtualdisk <oldName> <newName>
```

此选项重命名虚拟磁盘文件。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>。

重命名虚拟磁盘的示例

下面的示例会提示您输入指定服务器的用户名和密码。

```
vmkfstools --server server1 -E /vmfs/volumes/myvmfs/test.vmdk
    /vmfs/volumes/store/renamed.vmdk

vmkfstools --server server1 -E /vmfs/volumes/myvmfs/my_OS.vmdk
    /vmfs/volumes/myvmfs/my_new_OS.vmdk

vmkfstools --server 10.20.120.196 --renamevirtualdisk
    /vmfs/volumes/myvmfs/my_OS.vmdk /vmfs/volumes/myvmfs/my_new_OS.vmdk
```

克隆虚拟或裸磁盘

```
-i --importfile <srcfile> <destfile>
   -d --diskformat [rdm:<device>|rdmp:<device>|raw:<device>|thin|2gbsparse]
   -a --adaptertype <type>
```

此选项将创建指定虚拟磁盘或裸磁盘的副本。对于 ESX Server 3i，必须指定 `-i`、`--diskformat` 和 `--adaptertype` 选项。 `--diskformat` 选项为创建的副本指定磁盘格式。请参见 “受支持的磁盘格式”（第 225 页）。

注意 要克隆 ESX Server 3i 主机的重做日志，同时保留其层次结构，请使用 `vifs -C` 命令。

克隆虚拟磁盘或裸磁盘的示例

下面的示例假设配置文件中指定了连接参数环境变量。

```
vmkfstools –i /vmfs/volumes/templates/gold–master.vmdk
                /vmfs/volumes/myVMFS/myOS.vmdk –d thick –a lsilogic
```

此示例将主虚拟磁盘的内容从模板存储库克隆到 myVMFS 文件系统上名为 myOS.vmdk 的虚拟磁盘文件中。

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 系统中。但是，可使用 vmkfstools –i 命令将虚拟磁盘导入 ESX Server 系统，然后将此磁盘连接到在 ESX Server 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 使用 vmkfstools 将 VMware 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 VMware Workstation 或 GSX Server 磁盘。

扩展虚拟磁盘

```
–X ––extendvirtualdisk <新大小>[kK|mM|gG]
```

在创建虚拟机后，此选项可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。

注意 上述 newSize 参数将定义整个磁盘的大小，而不是只定义向磁盘添加的增量。

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。

扩展虚拟磁盘的示例

下面的示例会提示您输入指定服务器的用户名和密码。

```
vmkfstools ––server 10.20.120.132 –X 5g <disk name>.dsk
```

为 4 g 的虚拟磁盘扩展 1 g。

注意 请勿对有快照与其关联的虚拟机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。

```
vmkfstools --server 10.20.120.132 -X 50M
    /vmfs/volumes/my_newVMFS/my_disk.vmdk
```

创建虚拟兼容模式裸设备映射

`-r --createrdm <设备>`

此选项将在 VMFS-3 卷上创建虚拟兼容模式的裸设备映射 (Raw Device Mapping, 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 虚拟磁盘那样访问裸磁盘。映射的文件长度与其所指的裸磁盘的大小相同。

当指定 <设备> 参数时，为分区输入 0，这表示整个裸磁盘均已使用。具体格式如下：

`/vmfs/devices/disks/vmhbaA:T:L:0`

请参见 “vmkfstools 命令语法”（第 222 页）。

有关配置和使用 RDM 的详细信息，请参见 “裸设备映射”（第 107 页）。

注意 所有 VMFS-3 文件锁定机制均适用于 RDM。

创建虚拟兼容性模式 RDM 的示例

下面的示例会提示输入用户名和密码。

```
vmkfstools --server -r /vmfs/devices/disks/vmhba2:1:0:0
                /vmfs/volumes/storage1/rdm210.vmdk
```

创建虚拟兼容模式 RDM 文件 `/vmfs/volumes/storage1/rdm210.vmdk` 并将 `/vmfs/devices/disks/vmhba2:1:0:0` 裸磁盘映射到该文件。

```
vmkfstools -r --server server1 /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
```

创建物理兼容性模式裸设备映射

`-z --createrdmpassthru <设备>`

此选项允许将物理兼容模式裸设备映射到 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 SCSI 命令的筛选。当虚拟机需要发送专用的 SCSI 命令时，例如当虚拟机运行 SAN 感知软件时，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他 VMFS 虚拟磁盘一样访问裸磁盘了。

当指定 < 设备 > 参数时，为分区输入 0，这表示整个裸设备均已使用。具体格式如下：

```
/vmfs/devices/disks/vmhbaA:T:L:0
```

请参见 "vmkfstools 命令语法"（第 222 页）。

创建物理兼容模式 RDM 的示例

下面的示例假设配置文件中指定了连接参数环境变量。

```
vmkfstools –z /vmfs/devices/disks/vmhba2:1:0:0
    /vmfs/volumes/storage1/rdmpass.vmdk
```

创建名为 rdmpass.vmdk 的物理兼容模式 RDM 文件，并将 vmbha2:1:0:0 映射到该文件。不能使用已经存在的文件名。

列出 RDM 的属性

```
–q ––queryrdm
```

此选项可列出 RDM 的属性。

它将打印裸磁盘 RDM 的 vmhba 名称，还将打印裸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，而 S 代表扇区的数量。

注意 在将 VMware Workstation 虚拟磁盘导入 ESX Server 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。

索引

F

G

H

I

J

K

L

Y

Z