Please note that you can always find the most up-to-date technical documentation on our Web site at http://www.vmware.com/support/.

The VMware Web site also provides the latest product updates.

Copyright © 1998-2005 VMware, Inc. All rights reserved. Protected by one or more of U.S. Patent Nos. 6,397,242, 6,496,847, 6,704,925, 6,711,672, 6,725,289, 6,735,601, 6,785,886, 6,789,156 and 6,795,966; patents pending.
VMware, the VMware "boxes" logo and design, Virtual SMP and VMotion are registered trademarks or trademarks of VMware, Inc. in the United States and/or other jurisdictions. Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation. Linux is a registered trademark of Linus Torvalds. All other marks and names mentioned herein may be trademarks of their respective companies. Revision: yyyyMMdd Version: XXX-ENG-QNNN-NNN
# Table of Contents

**Preface** ........................................................................................................... 7
  About This Guide .......................................................................................... 8
    Intended Audience ....................................................................................... 8
  Document History .......................................................................................... 8
  Related Documentation ................................................................................... 9
  Conventions ..................................................................................................... 10
    Abbreviations ............................................................................................... 10
  Technical Support Resources ......................................................................... 11
    Self-Service Support ..................................................................................... 11
    Online and Telephone Support .................................................................... 11
    Support Offerings ........................................................................................ 11

**Introduction** ................................................................................................. 13
  Networking ....................................................................................................... 14
  Storage ............................................................................................................. 14
  Security ............................................................................................................ 15
  Appendixes ..................................................................................................... 15

**Networking** ................................................................................................. 17
  Overview ......................................................................................................... 19
    Concepts ........................................................................................................ 19
    Network Services .......................................................................................... 20
      Viewing Networking Information on the VI Client .................................. 20
  Networking Tasks ............................................................................................ 23
  Virtual Switches ............................................................................................... 24
  Port Groups ...................................................................................................... 27
  Virtual Network Configuration for Virtual Machines .................................... 28
  VMkernel Configuration .................................................................................. 32
    TCP/IP Stack at the Hypervisor Level .......................................................... 32
      Implications and Guidelines ...................................................................... 32
  Service Console Configuration ......................................................................... 37
    Basic Service Console Configuration Tasks .............................................. 37
    Using DHCP for the Service Console ......................................................... 43
    Troubleshooting Service Console Networking ........................................... 43
Advanced Networking 45
Advanced Networking Tasks 46
Editing Virtual Switches 47
Virtual Switch Properties 47
Editing Virtual Switch Properties 47
Virtual Switch Policies 54
Layer 2 Security Policy 55
Traffic Shaping Policy 57
Load Balancing and Failover Policy 58
Editing Port Group Properties 63
DNS and Routing 66
Networking Tips and Best Practices 68
Networking Best Practices 68
Mounting NAS Volumes 68
Networking Tips 69
Setting Up MAC Addresses 70
MAC Addresses Generation 70
Setting MAC Addresses 71
Using MAC Addresses 72
Introduction to Storage 73
Storage Concepts 74
Storage Overview 76
Datastores and File Systems 76
File System Formats 77
Types of Storage 77
Supported Storage Adapters 78
How Virtual Machines Access Storage 78
Viewing Storage Information in the Virtual Infrastructure Client 80
Displaying Datastores 80
Viewing Storage Adapters 81
Configuring and Managing Storage 84
Configuring Storage on ESX Server Hosts 84
Configuring Storage on Virtual Machines 84
Storage Configuration and Management Tasks 84
Local SCSI Configuration Tasks 84
Fibre Channel Tasks 84
Hardware-Initiated iSCSI Tasks 84
Software-Initiated iSCSI Tasks 84
NFS Tasks 84
General Storage Tasks 85

Configuring Storage 87
Local SCSI Disk Storage 88
  Adding Local SCSI Storage 88
Fibre Channel Storage 93
  Adding Fibre Channel Storage 94
  Multipathing for Fibre Channel HBAs 97
    Viewing the Current Multipathing State 98
  Setting Your Multipathing Policy for a LUN 98
    In Case of Failover 102
iSCSI Storage 103
  About iSCSI Storage 103
    iSCSI Initiators 103
      Naming Requirements 104
      Discovery Methods 105
      iSCSI Security 105
    Configuring Hardware-Initiated iSCSI Storage 106
      Installing iSCSI Hardware Initiator 106
      Viewing iSCSI Hardware Initiator 106
      Configuring iSCSI Hardware Initiator 108
      Adding Hardware-Initiated iSCSI Storage 112
    Configuring Software-Initiated iSCSI Storage 117
      Viewing Software iSCSI Initiator 117
      Configuring iSCSI Software Initiator 119
      Adding Software-Initiated iSCSI Storage 123
  Performing a Rescan 128
Network Attached Storage 129
  Shared Storage Capabilities 129
  How Virtual Machines Use NFS 129
  Managing NFS Devices 130
  Configuring ESX Server to Access NFS Volumes 131
  Creating an NFS-Based Datastore 131

Managing Storage 135
Managing Datastores and File Systems 136
  Adding New Datastores 136
  Removing Existing Datastores 136
| Connecting ESX Server Hosts Through Firewalls | 185 |
| Opening Firewall Ports for Supported Services and Management Agents | 185 |
| Securing Virtual Machines with VLANs | 188 |
| Security Considerations for VLANs | 190 |
| Virtual Switch Protection and VLANs | 192 |
| Securing Virtual Switch Ports | 194 |
| Securing iSCSI Storage | 197 |
| Securing iSCSI Devices Through Authentication | 197 |
| Protecting an iSCSI SAN | 201 |
| Authentication and User Management | 203 |
| Securing ESX Server Through Authentication and Permissions | 204 |
| About Users, Groups, Permissions, and Roles | 206 |
| Understanding Users | 206 |
| Understanding Groups | 207 |
| Understanding Permissions | 208 |
| Understanding Roles | 210 |
| Working with Users and Groups on ESX Server Hosts | 211 |
| Viewing and Exporting Users and Group Information | 212 |
| Working with the Users Table | 213 |
| Working with the Groups Table | 216 |
| Encryption and Security Certificates for ESX Server | 219 |
| Configuring Virtual Machine Delegates | 226 |
| Service Console Security | 229 |
| General Security Recommendations | 231 |
| Logging on to the Service Console | 233 |
| Service Console Firewall Configuration | 234 |
| Changing the Service Console Security Level | 235 |
| Opening and Closing Ports in the Service Console Firewall | 236 |
| Password Restrictions | 238 |
| Password Aging | 238 |
| Password Complexity | 240 |
| Changing the Password Plugin | 244 |
| Cipher Strength | 246 |
| setuid and setgid Applications | 247 |
| Default setuid Applications | 247 |
| Default setgid Applications | 249 |
SSH Security .............................................................................................................. 250
Security Patches and Security Vulnerability Scanning Software .................... 252
Security Deployments and Recommendations ................................................... 255
Security Approaches for Common ESX Server Deployments ......................... 256
  Single Customer Deployment ........................................................................... 256
  Multiple Customer Restricted Deployment ...................................................... 257
  Multiple Customer Open Deployment .............................................................. 259
Virtual Machine Recommendations ..................................................................... 262
Installing Antivirus Software ................................................................................. 262
Disabling Copy and Paste Operations Between the Guest Operating System and Remote Console ............................................................................................. 262
Preventing the Guest Operating System Processes from Flooding the ESX Server Host .................................................................................................................. 265
Disabling Logging for the Guest Operating System ............................................ 266

Appendix A:
ESX Technical Support Commands .................................................................... 269

Appendix B:
Using vmkfstools .................................................................................................. 277
  vmkfstools Command Syntax ........................................................................... 278
    vmkfstools Syntax When Specifying a SCSI Device .................................. 278
    vmkfstools Syntax When Specifying a VMFS Volume or File ..................... 279
    -v Suboption .................................................................................................. 279
  vmkfstools Options ........................................................................................... 280
    File System Options ....................................................................................... 280
    Virtual Disk Options ....................................................................................... 282
    Device Options ............................................................................................... 285
Examples Using vmkfstools .................................................................................. 288
This preface describes the contents of this manual, lists related documentation, describes document conventions, and provides additional references for support. This preface contains the following topics:

- About This Guide on page 8
- Related Documentation on page 9
- Conventions on page 10
- Technical Support Resources on page 11
About This Guide

This manual, the Server Configuration Guide, provides information on how to configure networking for ESX Server, including how to create virtual switches and ports and how to set up networking for virtual machines, VMotion, IP storage, and the service console. It also covers configuring file system and various types of storage such as iSCSI, Fibre Channel, and so forth. To help you protect your ESX Server installation, the guide provides a discussion of security features built into ESX Server and the measures you can take to safeguard it from attack. In addition, it includes a list of ESX server commands along with their VI Client equivalents and a description of the vmkfstools utility.

Intended Audience

The information presented in this manual is written for system administrators who are experienced Windows or Linux system administrators and who are familiar with virtual machine technology and datacenter operations.

Document History

This is the Beta 2 version of the Server Configuration Guide.

This manual is revised with each release of the product or when deemed necessary. A revised version can contain minor or major changes.

<table>
<thead>
<tr>
<th>Release</th>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ESX Server 3 Beta 2 release</td>
<td>February 16, 2006</td>
<td>PDF on the Web</td>
</tr>
</tbody>
</table>
Related Documentation

ESX Server 3.0 and VirtualCenter 2.0 documentation consists of the following publications:

- Documentation Roadmap
- Introduction to Virtual Infrastructure
- Installation and Upgrade Guide
- Server Configuration Guide
- Virtual Machine Backup Guide
- Web Access Administrator’s Guide
- SAN Configuration Guide
- Resource Management Guide
- Setup for Microsoft Cluster Service
- Online help
- Hardware compatibility guides
  - I/O Compatibility Guide
  - SAN Compatibility Guide
  - Systems Compatibility Guide
  - Backup Software Compatibility Guide
- Release Notes
Conventions

This manual uses the following conventions.

<table>
<thead>
<tr>
<th>Style</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>blue (online only)</td>
<td>Cross references, links</td>
</tr>
<tr>
<td>Courier</td>
<td>Commands, filenames, directories, paths, user input</td>
</tr>
<tr>
<td>Semi-Bold</td>
<td>Interactive interface objects, keys, buttons</td>
</tr>
<tr>
<td>Bold</td>
<td>Items of highlighted interest, terms</td>
</tr>
<tr>
<td>Italic</td>
<td>Variables, parameters, emphasis in text</td>
</tr>
<tr>
<td>italic</td>
<td>Web addresses</td>
</tr>
</tbody>
</table>

Abbreviations

The graphics in this manual use the following abbreviations.

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VC</td>
<td>VirtualCenter</td>
</tr>
<tr>
<td>VI</td>
<td>Virtual Infrastructure</td>
</tr>
<tr>
<td>server</td>
<td>&lt;product name&gt; server</td>
</tr>
<tr>
<td>database</td>
<td>&lt;product name&gt; database</td>
</tr>
<tr>
<td>hostn</td>
<td>&lt;product name&gt; managed hosts</td>
</tr>
<tr>
<td>VM#</td>
<td>Virtual machines on a managed host</td>
</tr>
<tr>
<td>user#</td>
<td>Users with access permissions</td>
</tr>
<tr>
<td>vmdk#</td>
<td>Storage disk for the managed host</td>
</tr>
<tr>
<td>datastore</td>
<td>Storage for the managed host</td>
</tr>
<tr>
<td>SAN</td>
<td>Storage area network type datastore shared between managed hosts</td>
</tr>
<tr>
<td>tmplt</td>
<td>Template</td>
</tr>
</tbody>
</table>
Technical Support Resources

The following sections describe various technical support resources available to you.

- **Self-Service Support**
- **Online and Telephone Support**
- **Support Offerings**

**Self-Service Support**

Use the VMware Technology Network for self help tools and technical information:

- Product Information — [www.vmware.com/support/resources](http://www.vmware.com/support/resources)
- Technology Information — [www.vmware.com/vcommunity/technology](http://www.vmware.com/vcommunity/technology)
- Documentation — [www.vmware.com/support/pubs](http://www.vmware.com/support/pubs)
- Knowledge Base — [www.vmware.com/support/kb](http://www.vmware.com/support/kb)
- Discussion Forums — [www.vmware.com/community](http://www.vmware.com/community)

For more information about the VMware Technology Network, go to [www.vmtn.net](http://www.vmtn.net).

**Online and Telephone Support**

Use online support to submit technical support requests, view your product and contract information, and register your products. Go to [www.vmware.com/support](http://www.vmware.com/support).

Use phone support for the fastest response on priority 1 issues for customers with appropriate support contracts. Go to [www.vmware.com/support/phone_support.html](http://www.vmware.com/support/phone_support.html).

**Support Offerings**

Find out how VMware’s support offerings can help you meet your business needs. Go to [www.vmware.com/support/services](http://www.vmware.com/support/services).
Introduction

The Server Configuration Guide describes the tasks you need to complete to configure ESX Server host networking, storage, and security. In addition, it provides overviews, recommendations, and conceptual discussions to help you understand these tasks and how to deploy an ESX Server host to meet your needs. Before using the information in the Server Configuration Guide, read the Introduction to Virtual Infrastructure for an overview of system architecture and the physical and virtual devices that make up a Virtual Infrastructure system.

This introduction summarizes the contents of this guide so that you can find the information you need. This guide covers these subjects:

- ESX Server network configurations
- ESX Server storage configurations
- ESX Server security features
- ESX command reference
- The vmkfstools command
Networking
The ESX Server networking discussion spans two chapters designed to provide you with a conceptual understanding of physical and virtual network concepts, a description of the basic tasks you need to complete to configure your ESX Server host's network connections, and a discussion of advanced networking topics and tasks. The networking section contains the following chapters:

- Networking – The Networking chapter introduces you to network concepts and guides you through the most common tasks you need to complete when setting up the network for the ESX Server host.

- Advanced Networking – The Advanced Networking chapter covers advanced networking tasks such as setting up MAC addresses, editing virtual switches and ports, and DNS routing. In addition, it provides tips on making your network configuration more efficient.

Storage
The ESX Server storage discussion consists of four chapters designed to provide you with a basic understanding of storage, a description of the basic tasks you perform to configure and manage your ESX Server host’s storage, and a discussion of how to set up raw device mapping. The storage section contains the following chapters:

- Introduction to Storage – The Introduction to Storage chapter introduces you to the types of storage you can configure for the ESX Server host.

- Configuring Storage – The Configuring Storage chapter explains how to configure local SCSI storage, Fibre Channel storage, and iSCSI storage. It also addresses VMFS storage and network-attached storage.

- Managing Storage – The Managing Storage chapter explains how to manage existing datastores and the file systems that comprise datastores.

- Raw Device Mapping – The Raw Device Mapping chapter discusses raw device mapping, how to configure this type of storage, and how to manage raw device mappings by setting up multipathing, failover, and so forth.
Chapter 1: Introduction

Security

The ESX Server storage discussion consists of five chapters that discuss safeguards VMware has built into ESX Server and measures you can take to protect your ESX Server host from security threats. These measures include using firewalls, leveraging the security features of virtual switches, and setting up user authentication and permissions. The security section contains the following chapters:

- **Security for ESX Server Systems** – The Security for ESX Server Systems chapter introduces you to the ESX Server features that help you ensure a secure environment for your data and gives you an overview of system design as it relates to security.

- **Securing an ESX Server Host** – The Securing an ESX Server Configuration chapter explains how to configure firewall ports for ESX Server hosts and VMware VirtualCenter, how to use virtual switches and VLANs to ensure network isolation for virtual machines, and how to secure iSCSI storage.

- **Authentication and User Management** – The Authentication and User Management chapter discusses how to set up users, groups, permissions, and roles to control access to ESX Server hosts and VirtualCenter. It also discusses encryption and delegate users.

- **Service Console Security** – The Service Console Security chapter discusses the security features built into the service console and shows you how to configure these features.

- **Security Deployments and Recommendations** – The Security Deployments and Recommendations chapter provides some sample deployments to give you an idea of the issues you need to consider when setting up your own ESX Server deployment. This chapter also tells you about actions you can take to further secure virtual machines.

Appendixes

The Server Configuration Guide provides two appendixes that provide specialized information you may find useful when configuring an ESX Server host.

- **ESX Command Reference** – Appendix A: ESX Technical Support Commands covers the ESX Server configuration commands that can be issued through a command line shell such as SSH. While these commands are available for your use, you should not consider them to be an API upon which you can build scripts. These commands are subject to change and VMware does not support applications and scripts that rely on ESX Server configuration commands.
Appendix A provides you with VMware Virtual Infrastructure Client equivalents for these commands.

- **Using vmkfstools** – Appendix B: Using vmkfstools covers the vmkfstools utility, which you can use to perform management and migration tasks for iSCSI disks.
This chapter guides you through the basic concepts of networking in the ESX Server environment and how to set up and configure a network in a virtual infrastructure environment.

You use the Virtual Infrastructure (VI) Client to add networking based on three categories that reflect the three types of network services:

- Virtual machines
- VMkernel
- Service console

This chapter covers the following topics:

- Overview on page 19
- Networking Tasks on page 23
- Virtual Switches on page 24
- Port Groups on page 27
- Virtual Network Configuration for Virtual Machines on page 28
- VMkernel Configuration on page 32
- Service Console Configuration on page 37
Overview

Concepts
A few concepts are essential to a thorough understanding of virtual networking. If you are new to ESX Server 3, we highly recommend you read through this section.

A physical network is a network of physical machines that are connected so that they can send to and receive data from each other. VMware ESX Server runs on a physical machine.

A virtual network is a network of virtual machines running on a single physical machine that are connected logically to each other so that they can send to and receive data from each other. Virtual machines can be connected to the virtual networks that you create in the procedure to add a network. Each virtual network is serviced by a single virtual switch. A virtual network can be connected to a physical network by associating one or more physical ethernet adapters, also referred to as uplink adapters, with the virtual network’s virtual switch. If no uplink adapters are associated with the virtual switch, then all traffic on the virtual network is confined within the physical host machine. If one or more uplink adapters are associated with the virtual switch, then virtual machines connected to that virtual network are also able to access the physical networks connected to the uplink adapters.

A physical Ethernet switch intelligently manages network traffic between machines on the network. A switch has multiple ports, each of which can be connected to a single other machine or another switch on the network. Each port can be configured to behave in certain ways depending on the needs of the machine connected to it. The switch learns which hosts are connected to which of its ports and uses that information to forward traffic to the correct physical machines. Switches are the core of a physical network. Multiple switches can be connected together to form larger networks.

A virtual switch, vSwitch, works much like a physical Ethernet switch. It knows which virtual machines are logically connected to each of its virtual ports and uses that information to forward traffic to the correct virtual machines. A vSwitch can be connected to physical switches using physical Ethernet adapters, also referred to as uplink adapters, to join virtual networks with physical networks. This type of connection is similar to connecting physical switches together to create a larger network. Even though a vSwitch works much like a physical switch, it does not have some of the advanced functionality of a physical switch.
A port group specifies port configuration options such as bandwidth limitations and VLAN tagging policies for each member port. Network services connect to vSwitches through port groups. Port groups define how a connection is made through the vSwitch to the physical network. In typical use, one or more port groups is associated with a single vSwitch.

NIC teaming occurs when multiple uplink adapters are associated with a single vSwitch to form a team. A team can either share the load of traffic between physical and virtual networks among some or all of its members or provide passive failover in the event of a hardware failure or a network outage.

VLANs enable a single physical LAN segment to be further segmented so that groups of ports are isolated from one another as if they were on physically different segments. 802.1Q is the standard.

The VMkernel IP networking stack has been extended to handle iSCSI, NFS, and VMotion. Two new features in ESX Server 3, iSCSI and NFS, are referred as IP storage in this chapter. IP storage refers to any form of storage that uses IP network communication as its foundation. iSCSI can be used as a virtual machine datastore, and NFS can be used as a virtual machine datastore and for direct mounting of .ISO files, which are presented as CD-ROMs to virtual machines.

Note: The networking chapters cover only how to set up networking for iSCSI and NFS. To configure the storage portion of iSCSI and NFS, see the storage chapters.

Migration with VMotion enables a powered on virtual machine to be transferred from one ESX Server host to another without shutting down the virtual machine. The optional VMotion feature requires its own license key.

Network Services
There are two types of network services that you need to enable in ESX Server:

• Connecting virtual machines to the physical network, which is a network of physical machines

• Connecting VMkernel services (such as NFS, iSCSI, or VMotion) to the physical network

The service console, which runs the management services, is set up by default during the installation of ESX Server.

Viewing Networking Information on the VI Client
To view the networking information in the VI Client:

1. Log into the VMware VI Client and select the server from the inventory panel.
The hardware configuration page for this server appears.

2. Click the Configuration tab, and click Networking.

The following information can be viewed in the VI Client:

- Virtual switches
- Adapter information for each adapter
  - Link status
  - Apparent speed and duplex
- Service console and VMkernel TCP/IP services
  - IP address
- Service console
  - Virtual device name
- Virtual machines
  - Power status
  - Connection status
- Port group
  - Network label—common to all three port configuration types
  - Number of configured virtual machines
  - VLAN ID, if any—common to all three port configuration types
Networking Tasks

This chapter outlines how to perform the following networking tasks.

- To create or add a virtual network for a virtual machine: on page 28
  - Setting the connection type for a virtual machine
  - Adding the virtual network to a new or an existing virtual switch
  - Configuring the network label and VLAN ID connection settings
- To set up the VMkernel: on page 33
  - Setting the connection type for the VMkernel
  - Adding the virtual network to a new or an existing virtual switch
  - Configuring the network label, VLAN ID, IP, and gateway connection settings
- To configure a service console: on page 37
  - Setting the connection type for the service console
  - Adding the virtual network to a new or an existing virtual switch
  - Configuring the network label, VLAN ID, DHCP/Static IP, and gateway connection settings
- To set the default gateway: on page 41
- To display service console information: on page 42
Virtual Switches

Virtual Infrastructure (VI) Client allows you to create abstracted network devices called virtual switches (vSwitches). A vSwitch can route traffic internally between virtual machines or link to external networks.

Virtual switches can be used to combine the bandwidth of multiple network adapters and balance communications traffic among them. They can also be configured to handle physical NIC failover.

A vSwitch models a physical Ethernet switch. The default number of logical ports for a vSwitch is 24. However, a vSwitch can be created with up to 1024 ports in ESX Server 3.0. You can connect one network adapter of a virtual machine to each port. Each uplink adapter associated with a vSwitch uses one port. Each logical port on the vSwitch is a member of a single port group. Each vSwitch can also have one or more port groups assigned to it. See Port Groups on page 27.

Before virtual machines can be configured to access a network, you must create at least one vSwitch. When two or more virtual machines are connected to the same vSwitch, network traffic between them is routed locally. If an outbound adapter is attached to the switch, each virtual machine can access the external network that the adapter is connected to.
In the VI Client, the details for the selected vSwitch are presented as an interactive diagram. The most important information for each vSwitch is always visible.

Secondary and tertiary information can be selectively revealed by clicking the blue dialog icon.
A pop-up window displays detailed properties.

<table>
<thead>
<tr>
<th>VM Network</th>
</tr>
</thead>
<tbody>
<tr>
<td>Properties</td>
</tr>
</tbody>
</table>
| Network Label | VM Network  
| H.W.E.D. | None  
| Security |  
| Promiscuous Mode | Accept  
| Max Address Changes | Accept  
| Forged Transmis | Accept  
| Traffic Shaping |  
| Average bandwidth | N/A  
| Peak bandwidth | N/A  
| Burst size | N/A  
| Failover and Load Balancing |  
| Load Balancing | First  
| Network Failure Detection | Link Status only  
| Notify Switches | Yes  
| Fail | No  
| Active Adapters | vmnic2  
| Standby Adapters | None  
| Unused Adapters | None  

Key-value pairs are read-only in the main dialog box.
Port Groups

Port groups aggregate multiple ports under a common configuration and provide a stable anchor point for virtual machines connecting to labeled networks. Each port group is identified by a network label, which is unique to the current host. A VLAN ID, which restricts port group traffic to a logical Ethernet segment within the physical network, is optional.

Labeled networks are properly configured only when all port groups using the same network label are able to see the same broadcast traffic. Because a VLAN can restrict visibility on a physical network, it might be necessary to synchronize the network label and VLAN ID controls when one of them is changed. More than one port group can use the same VLAN ID.
Virtual Network Configuration for Virtual Machines

The VI Client’s Add Networking Wizard steps you through the tasks to create a virtual network for a virtual machine, which consists of:

- Setting the connection type for a virtual machine
- Adding the virtual network to a new or an existing vSwitch
- Configuring the connection settings for the network label and the VLAN ID

To create or add a virtual network for a virtual machine:

1. Log into the VMware VI Client and select the server from the inventory panel.
   The hardware configuration page for this server appears.
2. Click the Configuration tab, and click Networking.
3. On the right side of the screen, click Add Networking.
   Virtual switches are presented in an overview plus details layout. Important information is always visible.
4. Click Add Networking from the Configuration tab or select Edit for a vSwitch and click the Add button on the Properties dialog box.
   The Add Networking Wizard appears.
   The Add Networking Wizard is reused for new ports and port groups.
5. As a connection type, select Virtual Machines, which is the default.
   Selecting Virtual Machines allows you to add a labeled network to handle virtual machine network traffic.
6. Click Next.
Virtual machines reach physical networks through uplink adapters. A vSwitch is only able to transfer data to external networks when one or more network adapters are attached to it. When two or more adapters are attached to a single vSwitch, they are transparently teamed.

7. Select **Create a virtual switch**.
   You can create a new vSwitch with or without Ethernet adapters.
   If you create a vSwitch without physical network adapters, then all traffic on that vSwitch will be confined to that vSwitch. No other hosts on the physical network or virtual machines on other vSwitches will be able to send or receive traffic over this vSwitch. This may be desirable if you want a group of virtual machines to be able to communicate with each other, but not with other hosts or with virtual machines outside the group.
   Virtual machines can connect to a host-only network but usually do not.
   Changes are reflected in the Preview pane.
   Outbound adapters are listed.

8. Click **Next**.
   The Connection Settings screen appears.
9. Under Port Group Properties, enter a network label that identifies the port group that you are creating.

Use network labels to identify migration-compatible connections common to two or more hosts.

10. If you are using a VLAN, in the VLAN ID field, enter a number between 1 and 4095.
If you are unsure what to enter, leave this blank or ask your network administrator.

11. Click Next.
The Ready to Complete screen appears.

12. After you have determined that the vSwitch is configured correctly, click Finish.
Note: To enable failover (NIC teaming), bind two or more adapters to the same switch. If one outbound adapter is not operational, network traffic is routed to another adapter attached to the switch.
VMkernel Configuration

Moving a virtual machine from one host to another is called migration. Migrating a powered-on virtual machine is called VMotion. Migration with VMotion, designed to be used between highly compatible systems, allows you to migrate virtual machines with no downtime. Your VMkernel networking stack must be set up properly to accommodate VMotion.

IP Storage refers to any form of storage that uses IP network communication as its foundation, which includes iSCSI and NAS for ESX Server. Because both of these storage types are network-based, both types can use the same port group.

The network services provided by the VMkernel (iSCSI, NFS, and VMotion) use a TCP stack in the VMkernel. This TCP stack is completely separate from the TCP stack used in the service console. Each of these TCP stacks accesses various networks by attaching to one or more port groups on one or more vSwitches.

TCP/IP Stack at the Hypervisor Level

The VMware VMkernel IP networking stack has been extended to handle iSCSI, NFS and VMotion. iSCSI and NFS are new in ESX Server 3.

- iSCSI as a virtual machine datastore
- NFS as a virtual machine datastore
- NFS for the direct mounting of .ISO files, which are presented as CD-ROMs to virtual machines
- Migration with VMotion

Note: ESX supports only NFS version 3 over TCP/IP.

Implications and Guidelines

- The IP address that you assign to the service console during installation must be different from the IP address that you assign to VMkernel’s IP stack from the Configuration > Networking tab of the Virtual Infrastructure Client.
- Both NFS as a datastore and NFS for the mounting of .ISO files must be configured together. They always share the same IP address, gateway, netmask, and so on, and are connected to the same vSwitch and, therefore, the same physical network adapter.
- Before configuring software iSCSI for the ESX Server host, you need to open a firewall port. You do so by enabling the iSCSI software client service. For more on
opening firewall ports for supported services, see Opening Firewall Ports for Supported Services and Management Agents on page 185.

- Unlike other VMkernel services, iSCSI has a service console component, so networks that are used to reach iSCSI targets must be accessible to both service console and VMkernel TCP stacks.

To set up the VMkernel:

1. Log into the VMware VI Client and select the server from the inventory panel. The hardware configuration page for this server appears.
2. Click the Configuration tab, and click Networking.
3. Click the Add Networking link. The Add Networking Wizard appears.
4. Select VMkernel and click Next.
   Selecting VMotion and IP Storage allows you to connect the VMkernel, which runs services for VMotion and IP Storage (NFS or iSCSI), to the physical network. The Network Access screen appears.
5. Select the vSwitch you would like to use or the Create a virtual switch radio button.
6. Use the check boxes to select the network adapters your vSwitch will use.

Your choices appear in the Preview pane.

You should select adapters for each vSwitch so that virtual machines or other services that connect through the adapter can reach the correct Ethernet segment. If no adapters appear under Create a new virtual switch, this means that all the network adapters in the system are being used by existing vSwitches. You can either create a new vSwitch without a network adapter or select a network adapter used by an existing vSwitch. The selected adapter, currently used by another vSwitch, is removed from that vSwitch and added to the one you are creating.

7. Click Next.

The Connection Settings screen appears.

8. Under Port Group Properties, select or enter a network label and a VLAN ID.

- **Network Label**—a name that identifies the port group that you are creating. This is the label that you specify when configuring a virtual adapter to be attached to this port group, when configuring VMkernel services, such as VMotion and IP storage.
- **VLAN ID**—identifies the VLAN that the port group's network traffic will use.
9. Select the **Use this port group for VMotion** check box to enable this port group to advertise itself to another ESX Server as the network connection where VMotion traffic should be sent.

This property can be enabled for only one VMotion and IP Storage port group for each ESX Server host. If this property is not enabled for any port group, migration with VMotion to this host is not possible.

10. Under **IP Settings**, to set the **VMkernel Default Gateway** for VMkernel services, such as VMotion, NAS, and iSCSI, click the **Edit** button.

**Note:** Make sure that you set a default gateway for the port that you created. VirtualCenter 2 behaves differently here from VirtualCenter 1.x. Now you must use a valid IP address to configure the VMkernel IP stack, not a dummy address.

If you have not yet configured DNS, the DNS Configuration dialog box appears. Under the DNS Configuration tab, the name of the host is entered into the name field by default. The DNS server addresses that were specified during installation are also preselected as is the domain.

Under the Routing tab, the service console and the VMkernel each need their own gateway information. A gateway is needed if connectivity is desired to machines not on the same IP subnet as the service console or VMkernel.
Caution: There is a risk of misconfiguration, which can cause the UI to lose connectivity to the host, in which case the host will have to be reconfigured from the command line at the service console.

Static IP settings is the default.

11. Click OK to save your changes and close the DNS Configuration dialog box.

12. Click Next.

13. Use the Back button to make any changes.

14. Review your changes on the Ready to Complete page and click Finish.
Service Console Configuration

Both the service console and the VMkernel use virtual Ethernet adapters to connect to a vSwitch and to reach networks serviced by the vSwitch. Virtual adapters for the service console and the virtual machines can be enabled or disabled.

Basic Service Console Configuration Tasks
There are two common service console configuration changes: changing NICs and changing the settings for an existing NIC that is in use.

In the first case, when only one service console connection is present, changing the service console configuration is not allowed. Therefore, if you want a new connection, you must change the network settings to use an additional NIC. After verifying that the new connection is functioning properly, remove the old connection. Effectively, you are switching over to the new NIC.

To configure a service console:

1. Log into the VMware VI Client and select the server from the inventory panel.
   The hardware configuration page for this server appears.
2. Click the Configuration tab, and click Networking.
3. Click the Add Networking link.
   The Add Networking wizard appears.
4. Select Service Console on the Connection Types screen, and click Next.
The Service Console Network Access page appears

5. Select the vSwitch you want to use for network access or select Create a new vSwitch, and click Next.

If no adapters appear under Create a new virtual switch, this means that all the network adapters in the system are being used by existing vSwitches. You can either create a new vSwitch without a network adapter or select a network adapter used by an existing vSwitch. The selected adapter, currently used by another vSwitch, is removed from that vSwitch and added to the one you are creating.
6. Under *Port Properties*, select or enter the *Network Label* and *VLAN ID*.

Newer ports and port groups appear at the top of the vSwitch diagram.

7. Enter the *IP Address* and *Subnet Mask* or select the DHCP option *Obtain IP setting automatically* for the IP address and subnet mask.

8. Click the *Edit* button to set the *Service Console Default Gateway*.

   See To set the default gateway: on page 41.

9. Click *Next*.

   The Ready to Complete screen appears.

10. Check the information and click *Finish*.

**To configure service console ports**

1. Log into the VMware VI Client and select the server from the inventory panel.

   The hardware configuration page for this server appears.

2. Click the *Configuration* tab, and click *Networking*.

3. On the right side of the screen, find the vSwitch that you want to edit and click *Properties* for that vSwitch.
The vSwitch Properties dialog box appears.

4. In the vSwitch Properties dialog box, click the **Ports** tab.

5. Select **Service Console**, and click **Edit**.

   A warning dialog box appears to explain that modifying your service console connection may disconnect all management agents.

6. To continue with the service console configuration, click **Continue modifying this connection**.
7. Edit port properties, IP settings, and effective policies as necessary.

8. Click OK.

Only one default gateway can be configured per TCP/IP stack.

**To set the default gateway:**

1. Log into the VMware VI Client and select the server from the inventory panel. The hardware configuration page for this server appears.

2. Click the **Configuration** tab, and click **DNS and Routing**. The DNS and Routing panel appears.

3. Click the **Properties** link.
The DNS Configuration dialog box appears.

Under the DNS Configuration tab, the name of the host is entered into the name field by default. The DNS server addresses previously selected during installation are also preselected as is the domain.

Under the Routing tab, the service console and the VMkernel are often not connected to the same network, and as such each needs its own gateway information. A gateway is needed if connectivity is desired to machines not on the same IP subnet as the service console or VMkernel.

For the service console, the gateway device is needed only when two or more vswifs are using the same subnet. The gateway device is needed to decide which vswif will be used for the default route.

4. Click the Routing tab.
5. Set the VMkernel default gateway.
6. Click OK to save your changes and close the DNS Configuration dialog box.

To display service console information:

1. Click the blue dialog icon to reveal service console information.
2. Click the X to close the dialog.

**Using DHCP for the Service Console**

In most cases, you should use static IP addresses for the service console. You can also set up the service console to use dynamic addressing, DHCP, if your DNS server is capable of mapping the service console's host name to the dynamically-generated IP address.

If your DNS server cannot map the host's name to its DHCP-generated IP address, you must determine the service console's numeric IP address and use that numeric address when accessing the interface's web pages.

The numeric IP address might change as DHCP leases run out or when the system is rebooted. For this reason, we do not recommend using DHCP for the service console unless your DNS server can handle the host name translation.

**Caution:** Do not use DHCP when sharing the network adapter assigned to the service console with virtual machines. ESX Server requires a static IP address for the service console when sharing a network adapter.

**Troubleshooting Service Console Networking**

If certain parts of the service console's networking are misconfigured, you will lose your ability to access your ESX Server host with the VI Client. In the event that this happens, you can reconfigure networking by connecting directly to service console using SSH and using the following service console commands:

- **esxcfg-vswif -l**
  Provides a list of the service console's current network configurations.
  If you are unable to connect to the ESX Server host using the VI Client, check that vswif0 is present and that the current IP address and Netmask are correct.

- **esxcfg-vswitch -l**
  Provides a list of current virtual switch configurations.
  If you are unable to connect to the ESX Server host using the VI Client, check that the service console's uplink adapter is the same network adapter used to connect to the service console.

- **esxcfg-vswif -i <new ip address> vswifX**
  Changes the service console's IP address.

- **esxcfg-vswif -n <new netmask> vswifX**
  Changes the service console's netmask.
• esxcfg-vswitch -U <old vmnic> vswitch0
  esxcfg-vswitch -L <new vmnic> vswitch0
Changes the uplink for the service console.
This chapter describes those networking tasks that you perform infrequently.

This chapter covers the following topics:

- Advanced Networking Tasks on page 46
- Editing Virtual Switches on page 47
- Editing Port Group Properties on page 63
- DNS and Routing on page 66
- Networking Tips and Best Practices on page 68
- Setting Up MAC Addresses on page 70
Advanced Networking Tasks

This chapter contains step-by-step instructions to guide you through the following tasks:

- To edit the number of ports for a vSwitch on page 47
- To configure the uplink network adapter by changing its speed on page 50
- To add uplink adapters on page 51
- To edit the Layer2 Security policy on page 55
- To edit the Traffic Shaping policy on page 57
- To edit the failover and load balancing policy on page 59
- To edit port group properties on page 63
- To change the DNS and Routing configuration on page 66
Editing Virtual Switches

This section contains the following information:

- Virtual Switch Properties on page 47
- Virtual Switch Policies on page 54

Virtual Switch Properties

Virtual switch settings control vSwitch-wide defaults for ports, which can be overridden by port group settings for each vSwitch.

Editing Virtual Switch Properties

Editing vSwitch properties consists of:

- Configuring ports
- Configuring the uplink network adapters

To edit the number of ports for a vSwitch

1. Log into the VMware VI Client and select the server from the inventory panel. The hardware configuration page for this server appears.
2. Click the Configuration tab, and click Networking.
3. On the right side of the screen, find the vSwitch that you want to edit and click **Properties** for that vSwitch.
4. In the vSwitch Properties dialog box, click the **Ports** tab.
5. Click **Edit**.

The vSwitch Properties dialog box appears.

6. Click the **General** tab to set the number of ports.
7. Choose or enter the number of ports you want to use.
   
   Modifications will not take effect until the system is restarted.
8. Click **OK**.
To configure the uplink network adapter by changing its speed

1. Log into the VMware VI Client and select the server from the inventory panel.

   The hardware configuration page for this server appears.

2. Click the **Configuration** tab, and click **Networking**.

3. Select a vSwitch and click **Properties**.

4. In the vSwitch Properties dialog box, click the **Network Adapters** tab.

5. To change the configured speed, duplex value of a network adapter, select the network adapter and click **Edit**.
The Status dialog box appears. The default is Autonegotiate, which is usually the correct choice.

6. To select the connection speed manually, select the desired speed/duplex from the drop-down menu.

Choosing the connection speed manually is usually done if the NIC and a physical switch might fail to negotiate the proper connection speed. Symptoms of mismatched speed and duplex include very low bandwidth or no link connectivity at all.

The adapter and the physical switch port it’s connected to must be set to the same value, that is, auto/auto or ND/ND where ND is some speed and duplex, but not auto/ND.

7. Click OK.

To add uplink adapters

1. Log into the VMware VI Client and select the server from the inventory panel.

   The hardware configuration page for this server appears.

2. Click the Configuration tab, and click Networking.

3. Select a vSwitch and click Properties.
4. In the Properties dialog box for the vSwitch, click the **Network Adapters** tab.
5. Click **Add** to launch the Add Adapter Wizard.

You might want to associate multiple adapters to a single vSwitch to provide NIC teaming. Such a team can share traffic and provide passive failover. If there are adapters available for NIC teaming, you can select unclaimed adapters on this screen and connect them to an existing vSwitch.

**Caution**: Misconfiguration can result in the loss of the VI Client’s ability to connect to the host.

![Add Adapter Wizard](image)

6. Select one or more adapters from the list, and click **Next**.
7. To order the NICs, select a NIC and use the buttons to move it up or down into the category (Active or Standby) that you want.

8. Click **Next**.
   The Adapter Summary page appears.

9. Review the information on this page, use the **Back** button to change any entries, and click **Finish** to leave the Add Adapter Wizard.
   The list of network adapters re-appears, showing those adapters now claimed by the vSwitch.

10. Click **Close** to exit the vSwitch Properties dialog box.
    The Networking section in the Configuration tab shows the network adapters in their designated order and categories.

**Virtual Switch Policies**

You can apply a set of vSwitch-wide policies is applied by selecting the vSwitch at the top of the **Ports** tab and clicking **Edit**.
To override any of these settings for any particular port group, select that port group and click Edit. Any changes to the vSwitch-wide configuration are applied to any of the port groups on that vSwitch except for those configuration options that have been overridden by the port group.

The vSwitch policies consist of:

- Layer 2 Security policy
- Traffic Shaping policy
- Load Balancing and Failover policy

**Layer 2 Security Policy**

Layer 2 is the data link layer.

The three elements of the Layer 2 Security policy are promiscuous mode, MAC address changes, and forged transmits.

In non-promiscuous mode, the network adapter listens to traffic only on its own MAC address; in promiscuous mode, it listens to all the packets. By default, the network adapter is set to non-promiscuous mode.

For further information on security, see Securing Virtual Switch Ports on page 194.

**To edit the Layer 2 Security policy**

1. Log into the VMware VI Client and select the server from the inventory panel.
   The hardware configuration page for this server appears.
2. Click the Configuration tab, and click Networking.
3. Click Properties for the vSwitch whose Layer 2 Security policy you want to edit.
4. In the Properties dialog box for the vSwitch, click the Ports tab.
5. Select the vSwitch item and click Edit.
6. In the Properties dialog box for the vSwitch, click the **Security** tab.

By default, Promiscuous Mode is set to Reject, and Mac Address Changes and Forced Transmits are set to Accept.

The policy here is applied to each virtual adapter attached to the port group, not to the port group as a whole.

7. In the Policy Exceptions area, select whether to reject or accept the Layer2 Security policy exceptions:

   - **Promiscuous Mode**
     - Reject — Placing the adapter in Promiscuous Mode has no effect on which frames are received by the adapter.
     - Accept — Placing the adapter in Promiscuous Mode causes it to see all frames passed on the vSwitch that are allowed under the VLAN policy for the port group that the adapter is connected to.

   - **MAC Address Changes**
     - Reject — If you set the MAC Address Changes to Reject and the guest operating system changes the MAC address of the adapter to anything other than what is in the `.vmx config` file, then all inbound frames will be dropped. If the Guest OS changes the MAC address back to match the MAC address in the `.vmx config` file, then inbound frames will be passed again.
     - Accept — Changing the MAC address from the Guest OS has the intended effect: frames to the new MAC address are received.
Forged Transmits
- Reject — Any outbound frame with a source MAC address that is different from the one currently set on the adapter will be dropped.
- Accept — No such filtering is performed and all outbound frames are passed.

8. Click OK.

Traffic Shaping Policy
ESX Server shapes traffic by establishing parameters for three traffic characteristics: average bandwidth, burst size, and peak bandwidth. You can set values for these characteristics through the VI Client, establishing a traffic shaping policy.
- The average bandwidth parameter establishes the number of bits per second you want to allow across the vSwitch averaged over time — in other words, the allowed average load.
- The burst size parameter establishes the maximum number of bytes you want to allow in a burst. If a burst exceeds the burst size parameter, excess packets are queued for later transmission. If the queue is full, the packets are dropped. When you specify values for these two characteristics, you indicate what you expect the vSwitch to handle during normal operation.
- The peak bandwidth is the maximum bandwidth the vSwitch can absorb without dropping packets. If traffic exceeds the peak bandwidth you establish, excess packets are queued for later transmission after traffic on the connection has returned to the average and there are enough spare cycles to handle the queued packets. If the queue is full, the packets are dropped. Even if you have spare bandwidth because the connection has been idle, the peak bandwidth parameter limits transmission to no more than peak until traffic returns to the allowed average load.

To edit the Traffic Shaping policy
1. Start the VI Client.
2. Click the server icon in the inventory panel.
3. On the Configuration tab, click Networking.
4. Select a vSwitch and click Properties.
5. In the vSwitch Properties dialog box, click the Ports tab.
6. Select the vSwitch and click Edit.
   The Properties dialog box for the selected vSwitch appears.
7. Click the **Traffic Shaping** tab.

The Policy Exceptions area appears. When traffic shaping is disabled, the tunable features are dimmed. All traffic-shaping tunables can be overridden selectively at the port group level.

These are the policies to which the per port group exceptions are applied. The policy here is applied to each virtual adapter attached to the port group, not to the port group as a whole. That is, if you have five virtual machines attached to a vSwitch with a policy limiting bandwidth to 30Mb/s, the total bandwidth used would be limited to 30Mb/s per virtual machine or 150Mb/s total.

- **Status** — If you enable the policy exception in the Status field, you are setting limits on the amount of networking bandwidth allocation each virtual adapter associated with this particular port group. If you disable the policy, services will have a free, clear connection to the physical network by default.

The remaining fields define network traffic parameters discussed in detail in the Traffic Shaping Policy above:

- **Average Bandwidth** — A value measured over a particular period of time.
- **Peak Bandwidth** — A value that is the maximum bandwidth allowed and that can never be smaller than average bandwidth.
- **Burst Size** — A value specifying how large a burst can be in kilobytes (K). The burst parameter controls the amount of data that can be sent in one burst while exceeding the Average rate. The Peak Bandwidth parameter limits the maximum bandwidth during such bursts.

**Load Balancing and Failover Policy**

- Load Balancing policy
The Load Balancing policy determines how incoming and outgoing traffic is distributed among the network adapters assigned to a vSwitch.

- Failover Detection: Link Status/Beacon Probing
- Network Adapter Order (Active/Standby)

To edit the failover and load balancing policy

1. Log into the VMware VI Client and select the server from the inventory panel.
   The hardware configuration page for this server appears.
2. Click the Configuration tab, and click Networking.
3. Select a vSwitch and click Edit.
4. In the vSwitch Properties dialog box, click the Ports tab.
5. To edit the Failover and Load Balancing values for the vSwitch, select the vSwitch item and click Properties.
   The Properties dialog box for the vSwitch appears.
6. Click the Nic Teaming tab.
The Policy Exceptions area appears. Failover order can be overridden at the port group level. By default, new adapters are active for all policies. New adapters carry traffic for the vSwitch and its port group unless you specify otherwise.

7. In the Policy Exceptions area:
   - Load Balancing — Specify how to choose an uplink.
   - Route based on the source of the port ID — Choose an uplink based on the virtual port where the traffic entered the virtual switch.
   - Route based on ip hash — Choose an uplink based on a hash of the source and destination IP addresses of each packet. For non-IP packets, whatever is at those offsets is used to compute the hash.
   - Route based on source MAC hash — Choose an uplink based on a hash of the source ethernet.
• Use explicit failover order — Always use the highest order uplink from the list of Active adapters which passes failover detection criteria.

• Network Failover Detection — Link Status only or Beacon Probing
  Link Status Only: Relies solely on the link status provided by the network adapter. This detects failures, such as cable pulls and physical switch power failures, but not configuration errors, such as a physical switch port being blocked by spanning tree or misconfigured to the wrong VLAN or cable pulls on the other side of a physical switch.
  Beacon probing: Sends out and listens for beacon probes on all NICs in the team and uses this information, in addition to link status, to determine link failure. This detects many of the failures mentioned above that are not detected by link status alone.

• Notify Switches — Toggle yes or no to notify switches in the case of failover
  Notify Switches: If this is enabled, then whenever a virtual NIC is connected to the vSwitch or whenever that virtual NIC’s traffic would be routed over a different physical NIC in the team due to a failover event, a notification is sent out over the network to update the lookup tables on physical switches. In almost all cases, this is desirable for the lowest latency of failover occurrences and migrations with VMotion.
  
  **Note:** Do not use this option when the virtual machines using the port group are using Microsoft Network Load Balancing in unicast mode. No such issue exists with NLB running in multicast mode.

• Failover Order — Specify how to distribute the work load for adapters. If you want to use some adapters but reserve others for emergencies in case the ones in use fail, you can set this condition using the drop-down menu to place them into the two groups:
  • Active Adapter — Continue to use it when the network adapter connectivity is up and active.
  • Standby — Use this adapter if one of the active adapter’s connectivity is down.
  • Unused — Not for current use.

• Rolling — Toggle Yes or No to disable or enable rolling
  Rolling: This option determines how a physical adapter is returned to active duty after recovering from a failure. If rolling is set to **No**, then the adapter is returned to active duty immediately upon recovery, displacing the standby
adapter that took over its slot, if any. If rolling is set to Yes, then a failed adapter is left inactive even after recovery until another currently active adapter fails, requiring its replacement.
Editing Port Group Properties

To edit port group properties

1. Log into the VMware VI Client and select the server from the inventory panel. The hardware configuration page for this server appears.
2. Click the Configuration tab, and click Networking.
3. On the right side of the screen, click Properties for a network. The vSwitch Properties dialog box appears.
4. Click the Ports tab.
5. Select the port group and click Edit.
6. In the Properties dialog box for the port group, click the General tab to change
   - Network Label — a name that identifies the port group that you are creating. This is the label that you specify when configuring a virtual adapter to be attached to this port group, either when configuring virtual machines or VMkernel services, such as VMotion and IP storage.
   - VLAN ID — identifies the VLAN that the port group’s network traffic will use.
7. Click OK to exit the vSwitch Properties dialog box.

To override labeled network policies

1. To override any of these settings for any particular labeled network, select the network.
2. Click Edit.
3. Click the Security tab.
4. Select the check box for the labeled network policy that you want to override.
5. Click the Traffic Shaping tab.
6. Select the check box to override the enabled or disabled Status.

7. Click the **Nic Teaming** tab.
8. Select the check box to override the load balancing or failover order policies.

9. Click OK to exit the labeled VM Network Properties dialog box.
DNS and Routing

To change the DNS and Routing configuration

1. Log into the VMware VI Client and select the server from the inventory panel. The hardware configuration page for this server appears.

2. Click the Configuration tab, and click DNS and Routing.

3. On the right of the screen, click Properties.

4. In the DNS Configuration tab, enter values for the Name and Domain fields.

5. Choose to either obtain the DNS server address automatically or use a DNS server address.

   **Note:** DHCP is supported only if the DHCP server is accessible to the service console. In other words, the service console must have a virtual interface (vswif) configured and attached to the network where the DHCP server resides.

6. Specify the domains in which to look for hosts.
7. In the **Routing** tab, change Default Gateways information as needed. You need to select a gateway device only if you have configured the service console to connect to more than one subnet.

8. Click **OK** to exit the DNS Configuration dialog box.
Networking Tips and Best Practices

This section provides information about:

- Networking Best practices
- Network hints

Networking Best Practices

Consider these best practices for configuring your network:

- Separate network services from one another to achieve greater security or better performance.
  
  If you want a particular set of virtual machines to function at the highest performance levels, put them on a separate physical NIC. This separation allows for a portion of the total networking workload to be more evenly shared across multiple CPUs. The isolated virtual machines are then more able to serve traffic from a Web client, for instance.

- Either of the recommendations below can be satisfied either by using VLANs to segment a single physical network or by using separate physical networks (the latter is preferable).

- Keeping the service console on its own network is an important part of securing the ESX system. The service console network connectivity should be considered in the same light as any remote access device in a server because compromise of the service console gives an attacker full control of all virtual machines running on the system.

- Keeping the VMotion connection on a separate network devoted to this purpose is important because when migration with VMotion occurs, the contents of the guest operating system’s memory are transmitted over the network.

Mounting NAS Volumes

In ESX Server 3.0, the model of how ESX accesses NAS storage of ISO images that are used as virtual CD-ROMs for virtual machines is different from the model used in ESX Server 2.x.

In ESX Server 2.x, the best practice was to mount the NAS volume on the Service Console and access ISOs through the Service Console mount. You had the capability to browse the Service Console file system, including NFS mounts, in the virtual machine configuration editor and locate these ISOs.
ESX Server 3.0 has support for VMkernel-based NAS mounts. The new model is to mount your NAS volume with the ISO images through the VMkernel NAS functionality. All NAS volumes mounted in this way appear as datastores in the VI Client. The virtual machine configuration editor allows you to browse a datastore for ISO images to be used as virtual CD-ROM devices. VMware does not support for browsing the Service Console file system for ISO images.

Networking Tips
Consider the following network hints:

• The easiest way to physically separate network services and to dedicate a particular set of NICs to a specific network service is to create a vSwitch for each service. If this is not possible, they can be separated from each other on a single vSwitch by attaching them to port groups with different VLAN IDs. In either case, you should confirm with your network administrator that the networks or VLANs you choose are isolated in the rest of your environment, that is, no routers connect them.

• You can add and remove NICs from the vSwitch without affecting the virtual machines or the network service that is running behind that vSwitch. In fact, if you removed all of the running hardware, the virtual machines would still be able to communicate amongst themselves, as if they were going out to the network and back. Moreover, if you left one NIC intact, all of the virtual machines would still be able to connect with the physical network.

• Use port groups with different sets of active adapters in their teaming policy to separate virtual machines into groups, which can use separate adapters as long as all adapters are up but still fall back to sharing in the event of a network or hardware failure.

• Deploy firewalls in virtual machines that route between virtual networks with uplinks to physical networks and pure virtual networks with no uplinks to protect your most sensitive virtual machines.
Setting Up MAC Addresses

MAC addresses are generated for virtual network adapters used by the service console, the VMkernel and virtual machines. In most cases, these MAC addresses are appropriate. However, there might be times when you need to set a MAC address for a virtual network adapter as in the following cases:

- Virtual network adapters on different physical servers share the same subnet and are assigned the same MAC address, causing a conflict.
- You want to ensure that a virtual network adapter always has the same MAC address.

The following sections describe how MAC addresses are generated and how you can set the MAC address for a virtual network adapter.

MAC Addresses Generation

Each virtual network adapter in a virtual machine is assigned its own unique MAC address. A MAC address is a six-byte number. Each network adapter manufacturer is assigned a unique three-byte prefix called an OUI (Organizationally Unique Identifier) that it can use to generate unique MAC addresses.

VMware has three OUIs:
- One for generated MAC addresses
- One for manually set MAC addresses
- One which was previously used for legacy virtual machines, but is no longer used with ESX Server 3.

The first three bytes of the MAC address that is generated for each virtual network adapter have this value. This MAC address generation algorithm produces the other three bytes. The algorithm guarantees unique MAC addresses within a machine and attempts to provide unique MAC addresses across machines.

The network adapters for each virtual machine on the same subnet should have unique MAC addresses. Otherwise, they can behave unpredictably. The algorithm puts a limit on the number of running and suspended virtual machines at any one time on any given server. It also does not handle all cases when virtual machines on distinct physical machines share a subnet.

The VMware UUID (Universally Unique Identifier) generates MAC addresses that are then checked for any conflicts. The generated MAC addresses are created using three parts: the VMware OUI, the SMBIOS UUID for the physical ESX Server machine, and a hash based on the name of the entity that the MAC address is being generated for.
After the MAC address has been generated, it does not change unless the virtual machine is moved to a different location, for example, a different path on the same server. The MAC address in the configuration file of the virtual machine is saved. All MAC addresses that have been assigned to network adapters of running and suspended virtual machines on a given physical machine are tracked.

The MAC address of a powered-off virtual machine is not checked against those of running or suspended virtual machines. Therefore, it is possible but unlikely that when a virtual machine is powered on again, it can acquire a different MAC address. This acquisition is due to a conflict with a virtual machine that was powered on when this virtual machine was powered off.

**Setting MAC Addresses**

To circumvent the limit of 256 virtual network adapters per physical machine and possible MAC address conflicts between virtual machines, system administrators can manually assign MAC addresses. VMware uses this OUI for manually-generated addresses: 00:50:56.

The MAC address range is

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

You can set the addresses by adding the following line to a virtual machine's configuration file:

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

where `<number>` refers to the number of the Ethernet adapter, `XX` is a valid hexadecimal number between 00 and 3F, and `YY` and `ZZ` are valid hexadecimal numbers between 00 and FF. The value for `XX` must not be greater than 3F to avoid conflict with MAC addresses that are generated by the VMware Workstation and VMware GSX Server products. Therefore, the maximum value for a manually generated MAC address is

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

You must also set the option in a virtual machine's configuration file:

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

Since VMware ESX Server virtual machines do not support arbitrary MAC addresses, the above format must be used. So long as you choose a unique value for `XX:YY:ZZ` among your hard-coded addresses, conflicts between the automatically assigned MAC addresses and the manually assigned ones should never occur.
Using MAC Addresses
The easiest way to familiarize yourself with MAC addresses is to:
1. Set the MAC address statically.
2. Remove the virtual machine configuration file options:
   ```
   ethernet<number>.address, ethernet<number>.addressType
   and
   ethernet<number>.generatedAddressOffset.
   ```
3. Verify that the virtual machine receives a generated MAC address.
VMware cannot guarantee that a host stays within a specific MAC address range. However, VMware does guarantee that the MAC address will never conflict with any physical host by using the VMware OUIs (00:0C:29 and 00:50:56), which are unique to virtual machines.
This chapter contains overview information about the available storage options for ESX Server.

**Note:** For information about configuring SANs, see the *SAN Configuration Guide*.

**Note:** For information about configuring virtual machines, see the *Virtual Machine Management Guide*.

For more information, see the following:
- Storage Concepts on page 74
- Storage Overview on page 76
- Viewing Storage Information in the Virtual Infrastructure Client on page 80
- Configuring and Managing Storage on page 84
Storage Concepts

There are a few concepts that are essential for a thorough understanding of storage.

- **Datastore** — A formatted logical container analogous to a logical volume. The datastore is used to hold virtual machine files and can exist on different types of physical storage including SCSI, iSCSI, Fibre Channel SAN, or NAS. Datastores can be of the two types: VMFS-based or NFS-based.

- **Disk partition** — A reserved part of hard disk that is set aside for specific purposes. In the context of ESX Server storage, disk partitions on various physical storage devices can be reserved and formatted as datastores or their extents.

- **Extent** — In the ESX Server context, extent is a hard disk partition on a physical storage device that can be dynamically added to an existing datastore that has a VMFS format. The datastore can stretch over multiple extents, yet appear as a single volume analogous to a spanned volume.

- **Failover path** — A redundant physical path that the ESX Server system can use when communicating with its networked storage. The ESX Server system uses the failover path if any component responsible for transferring storage data fails. See Multipathing.

- **Fibre Channel (FC)** — A high-speed data transmitting technology that ESX Server systems use to transport SCSI traffic from virtual machines to storage devices on a SAN. The Fibre Channel Protocol (FCP) packages SCSI commands into Fibre Channel frames.

- **iSCSI (Internet SCSI)** — A standard that packages SCSI storage traffic into TCP so it can travel through IP networks instead of the specialized FC network. With iSCSI connection, your ESX Server system (initiator) communicates with a remote storage device (target) as it would do with a local hard disk.

- **LUN (logical unit number)** — An address uniquely identifying each SCSI disk that an ESX Server system uses for storage.

- **Multipathing** — A technique that allows you to use more than one physical path, or an element on this path, responsible for transferring data between the ESX Server system and its remote storage. This redundant use of physical paths or elements, such as adapters, helps ensure uninterrupted traffic between the ESX Server system and storage device.

- **NAS (network-attached storage)** — A specialized storage device that connects to a network and can provide file access services to ESX Server systems. ESX Server systems use the NFS protocol to communicate with NAS servers.
NFS (network file system) — A file sharing protocol ESX Server supports to communicate with a NAS device.

Raw device — A disk that doesn't have a file system deployed on it.

Raw device mapping (RDM) — A special file in a VMFS volume that acts as a proxy for a raw device. The mapping file contains metadata used to manage and redirect disk accesses to the physical device.

Spanned volume — A dynamic volume that uses disk space on more than one physical disk, yet appears as a single logical volume.

Storage device — A physical disk or storage array that can either be internal or located outside of your system and connected to the system either directly or through an adapter.

VMFS (VMware ESX Server file system) — A high-performance file system on physical SCSI disks and partitions used for storing large files such as virtual disks for ESX Server virtual machines. Each version of ESX Server uses a corresponding version of VMFS. For example, VMFS-3 is introduced with ESX Server 3.

Volume — A logical storage unit, which can use disk space on one physical device, or its part, or span several physical devices.
Storage Overview

In the most common configuration, an ESX Server virtual machine uses a virtual hard disk to store its operating system, program files, and other data associated with its activities. Normally, a virtual disk is a large physical file that resides on a specially formatted volume called datastore.

The datastore can be deployed on the host machine’s internal direct-attached storage devices or on networked storage devices. A networked storage device represents an external storage device or array that is located outside of your system and is typically accessed over a network through an adapter.

Storing virtual disks and other essential pieces of your virtual machine on the datastore located on the networked storage allows you to:

- Use such VMware features as Distributed Resource Scheduling and Distributed Availability Services.
- Use VMotion and be able to move running virtual machines from one ESX Server to another without service interruption.
- Use Consolidated Backup and be able to perform backups more efficiently.
- Have better protection from planned or unplanned server outages.
- Have more control over load balancing.

ESX Server allows you to access a variety of physical storage devices, both internal and external, configure and format them, and then use for your storage needs.

Most of the time, you will be using Virtual Infrastructure (VI) Client to work with your storage. The following sections teach you how to access and configure your storage devices, as well as how to deploy and manage datastores:

- Configuring Storage on page 87
- Managing Storage on page 135

Datastores and File Systems

Normally, ESX Server virtual machines store their virtual disk files on specially formatted logical containers, or datastores, that can exist on different types of physical storage devices. A datastore can use disk space on one physical device, a disk partition, or several physical devices.

Generally, your datastore management process starts with storage space that your storage administrator preallocates for your ESX Server system on different storage
CHAPTER 4 Introduction to Storage

devices. The storage space is presented to your ESX Server system as LUNs (logical unit numbers) or, in case of a network attached storage, as NFS volumes.

Using the VI Client, you can create datastores by accessing and formatting available LUNs, or by mounting the NFS volumes.

After you create the datastores, you can use them to store virtual machine files. When needed, you can modify the datastores. For example, you can add extents to your datastore, rename, or remove it.

For information on managing datastores, see Managing Datastores and File Systems on page 136.

File System Formats

Datastores you create can have the following file system formats:

- **VMFS** — ESX Server deploys this type of file system on local SCSI disks, iSCSI LUNs, or Fibre Channel LUNs, creating one directory for each virtual machine. VMFS is a clustered file system that can be accessed simultaneously by multiple ESX Server systems. VMFS uses automatic locking to ensure file system consistency.

  **Note:** ESX Server 3 supports VMFS version 3 (VMFS-3). VMFS-3 is not backward compatible with versions of ESX Server earlier than ESX Server 3. If you are using VMFS-2, you need to upgrade it to VMFS-3. For information on upgrading your VMFS-2, see Upgrading Datastores on page 139.

- **NFS** — ESX Server can use a designated NFS volume located on an NFS server. ESX Server mounts the NFS volume creating one directory for each virtual machine.

Types of Storage

Datastores can reside on a variety of storage devices. You can deploy a datastore on your system's direct-attached storage device or on a networked storage device.

ESX Server supports the following types of storage devices:

- **Local** — stores files locally on an internal or external SCSI device.
- **Fibre Channel** — stores files remotely on a Storage Area Network (SAN). Requires Fibre Channel adapters.
- **iSCSI (hardware initiated)** — stores files on remote iSCSI storage devices. Files are accessed over TCP/IP network using hardware-based iSCSI HBAs (host bus adapters).
• iSCSI (software initiated) — stores files on remote iSCSI storage devices. Files are accessed over TCP/IP network using a software-based iSCSI initiator. Requires a standard network adapter for network connectivity.

• Network attached storage (NAS) — stores files on remote file servers. Files are accessed over TCP/IP network using the NFS protocol. Requires a standard network adapter for network connectivity.

You use the VI Client to access storage devices mapped to your ESX Server system and deploy datastores on them. For more information, refer to Configuring Storage on page 87.

**Supported Storage Adapters**

To access different types of storage, your ESX Server system needs different adapters that provide connectivity to the storage device. ESX Server supports PCI-based SCSI, RAID, Fibre Channel, and Ethernet adapters and accesses them directly through device drivers in the VMkernel.

**How Virtual Machines Access Storage**

When a virtual machine communicates with its virtual disk stored on a datastore, it issues SCSI commands. Since datastores can exist on various types of physical storage, these commands are encapsulated into other forms depending on the protocol the ESX Server system uses to connect to a storage device. ESX Server supports Fibre Channel (FC), Internet SCSI (iSCSI), and NFS protocols.
The following diagram depicts five virtual machines using different types of storage to illustrate the differences between each type.

**Note:** This diagram is for conceptual purposes only; it is not a recommended configuration.

You can configure a virtual machine to access the virtual disks on the physical storage devices. To configure a virtual machine, refer to the *Virtual Machine Management Guide*. 
Viewing Storage Information in the Virtual Infrastructure Client

The VI Client displays detailed information on available datastores, storage devices the datastores use, and configured adapters. See these sections for more information:

- Displaying Datastores on page 80
- Viewing Storage Adapters on page 81

Displaying Datastores

Datastores are added to the VI Client in one of two ways:

- Discovered when a host is added to the inventory — When you add a host to the inventory, the VI Client displays any datastores known to the host.
- Created on an available storage device — You can use the Add Storage command to create and configure a new datastore. For more information, see Configuring Storage on page 87.

You can view a list of available datastores and analyze their properties. To display datastores, on the host Configuration tab, click the Storage link. For each datastore, the Storage section shows summary information, including:

- Target storage device where the datastore is located.
- Type of file system the datastore uses.
- Total capacity, including the used and available space.
- Recent tasks and triggered alarms.

To view additional details about the specific datastore, select the datastore from the list. The Details section shows the following information:

- The location of the datastore.
- Individual extents the datastore spans and their capacity.
- Paths used to access the storage device.
In the following example, the datastore “storage1(1)” is selected from the list of available datastores; the Details view provides information about the selected datastore.

You can edit or remove any of the existing datastores. When you edit a datastore, you can change its label, add extents, or modify paths for storage devices. You can also upgrade the datastore. For more information, see Managing Storage on page 135.

**Viewing Storage Adapters**

The VI Client displays any storage adapters available to your system. From the host Configuration tab, you can view details about the storage adapters, such as:

- Existing storage adapters.
- The type of storage adapter, such as Fibre Channel SCSI or iSCSI.
Details for each adapter, such as the storage device it connects to and target ID.

Configuration options and details about adapters are available through the VI Client. Select a storage device to view its properties.
In the following example, the Fibre Channel storage adapter “vmhba1” is selected; the Details view provides information about the number of LUNs the adapter connects to and the paths it uses.

<table>
<thead>
<tr>
<th>Path</th>
<th>Canonical Path</th>
<th>Capacity</th>
<th>LUN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmhba1:00</td>
<td>vmhba1:0:0</td>
<td>Tapedrive</td>
<td>vmhba1:0:0</td>
</tr>
<tr>
<td>vmhba1:01</td>
<td>vmhba1:0:1</td>
<td>Tapedrive</td>
<td>vmhba1:0:1</td>
</tr>
<tr>
<td>vmhba1:02</td>
<td>vmhba1:0:2</td>
<td>Tapedrive</td>
<td>vmhba1:0:2</td>
</tr>
<tr>
<td>vmhba1:03</td>
<td>vmhba1:0:3</td>
<td>Tapedrive</td>
<td>vmhba1:0:3</td>
</tr>
<tr>
<td>vmhba1:04</td>
<td>vmhba1:0:4</td>
<td>Tapedrive</td>
<td>vmhba1:0:4</td>
</tr>
<tr>
<td>vmhba1:05</td>
<td>vmhba1:0:5</td>
<td>Tapedrive</td>
<td>vmhba1:0:5</td>
</tr>
<tr>
<td>vmhba1:06</td>
<td>vmhba1:0:6</td>
<td>Tapedrive</td>
<td>vmhba1:0:6</td>
</tr>
<tr>
<td>vmhba1:07</td>
<td>vmhba1:0:7</td>
<td>Tapedrive</td>
<td>vmhba1:0:7</td>
</tr>
<tr>
<td>vmhba1:08</td>
<td>vmhba1:0:8</td>
<td>Tapedrive</td>
<td>vmhba1:0:8</td>
</tr>
<tr>
<td>vmhba1:09</td>
<td>vmhba1:0:9</td>
<td>Tapedrive</td>
<td>vmhba1:0:9</td>
</tr>
<tr>
<td>vmhba1:10</td>
<td>vmhba1:0:10</td>
<td>Tapedrive</td>
<td>vmhba1:0:10</td>
</tr>
<tr>
<td>vmhba1:11</td>
<td>vmhba1:0:11</td>
<td>Tapedrive</td>
<td>vmhba1:0:11</td>
</tr>
<tr>
<td>vmhba1:12</td>
<td>vmhba1:0:12</td>
<td>Tapedrive</td>
<td>vmhba1:0:12</td>
</tr>
<tr>
<td>vmhba1:13</td>
<td>vmhba1:0:13</td>
<td>Tapedrive</td>
<td>vmhba1:0:13</td>
</tr>
</tbody>
</table>
Configuring and Managing Storage

Configuring Storage on ESX Server Hosts
For detailed information on configuring and formatting storage, refer to Configuring Storage on page 87.
For detailed information on configuring SANs, refer to the SAN Configuration Guide.

Configuring Storage on Virtual Machines
For detailed information on configuring virtual machine storage, refer to the Virtual Machine Management Guide.

Storage Configuration and Management Tasks
The storage tasks you can perform in ESX Server are:

Local SCSI Configuration Tasks
- To create a datastore on a local SCSI disk on page 88

Fibre Channel Tasks
- To create a datastore on a Fibre Channel device on page 94
- To change failover policy on page 99

Hardware-Initiated iSCSI Tasks
- To view the iSCSI hardware initiator properties on page 106
- To enable the iSCSI hardware initiator on page 109
- To set up target addresses for the hardware initiator on page 109
- To set up CHAP parameters for the hardware initiator on page 111
- To create a datastore on a hardware-initiated iSCSI device on page 113

Software-Initiated iSCSI Tasks
- To view the iSCSI software initiator properties on page 117
- To enable the iSCSI software initiator on page 120
- To set up target addresses for the software initiator on page 120
- To set up CHAP parameters for the software initiator on page 122
- To create a datastore on a software-initiated iSCSI device on page 123

NFS Tasks
- To mount an NFS volume on page 131
General Storage Tasks

- To modify the NFS-based datastore on page 138
- To upgrade the VMFS-2 to VMFS-3 on page 139
- To edit the name of the datastore on page 139
- To add one or more extents to the datastore on page 140
- To remove a datastore on page 137
This chapter contains information about configuring local SCSI disks, Fibre Channel Storage Area Network (SAN) storage, iSCSI, and network attached storage (NAS).

**Note:** For additional information about configuring SANs, see the SAN Configuration Guide.

This chapter covers the following topics:
- Local SCSI Disk Storage on page 88
- Fibre Channel Storage on page 93
- iSCSI Storage on page 103
- Network Attached Storage on page 129
Local SCSI Disk Storage

This section contains information on configuring local storage on internal or external SCSI devices and provides the following information:

- Adding Local SCSI Storage on page 88

The simplest type of storage uses a SCSI device such as your system’s hard disk or any external SCSI storage device.

The following diagram depicts a virtual machine using local SCSI storage.

In this example of local storage configuration, the ESX Server SCSI card uses a cable to plug into a disk. On that disk, you can create a datastore, which you use to store virtual machine disk files. The datastore you create has the VMFS format.

Adding Local SCSI Storage

As soon as you load SCSI storage adapter drivers, ESX Server detects available SCSI storage devices. Before creating a new datastore on a SCSI device, you may need to perform a rescan. For more information, see Performing a Rescan on page 128.

When you create a datastore on a SCSI storage device, the Add Storage Wizard guides you through the configuration steps.

To create a datastore on a local SCSI disk

1. Log into the VMware VI Client and select the server from the inventory panel. The hardware configuration page for this server appears.
2. Click the Configuration tab, and then click Storage.
3. Click Add Storage. The Add Storage page appears.

4. Select storage type Disk/LUN.

5. Click Next.

   The Select Disk/LUN page appears.

6. Select the SCSI device you want to use for your datastore.
7. Click **Next**.
   The Current Disk Layout page appears.
8. Look over the current disk layout.
9. Click **Next**.
   The Properties page appears.

10. Enter a datastore name.
    The label name must be unique within the current Virtual Infrastructure instance.
11. Click **Next**.
The Disk/LUN–Formatting page appears.

12. If needed, adjust the file system values and capacity you use for the datastore. By default, the entire free space available on the storage device is offered to you.

13. Click Next.

The Ready to Complete page appears.

14. Click Finish.
This creates a datastore on the local SCSI disk on your ESX Server.
Fibre Channel Storage

ESX Server supports using Fibre Channel adapters, which allow an ESX Server system to be connected to a SAN and to see the disk arrays on the SAN.

For additional information about configuring SANs, see the VMware SAN Configuration Guide.

For a list of supported SAN storage devices for the beta version of ESX Server, see the SAN Compatibility Guide.

This section contains information on configuring Fibre Channel storage and adapters and provides the following information:

- Adding Fibre Channel Storage on page 94
- Multipathing for Fibre Channel HBAs on page 97
- Setting Your Multipathing Policy for a LUN on page 98
- In Case of Failover on page 102

The following diagram depicts virtual machines using Fibre Channel storage:

In this configuration, ESX Server connects to SAN storage using a Fibre Channel adapter. The adapter connects to SAN fabric consisting of Fibre Channel switches and storage arrays, which then present LUNs from physical disks to your ESX Server system.
You can format the LUNs and create a datastore that you use for your ESX Server storage needs. The datastore uses the VMFS format.

**Adding Fibre Channel Storage**

Before creating a new datastore on a Fibre Channel device, you need to rescan a Fibre Channel adapter to discover any newly added LUNs. For more information, see Performing a Rescan on page 128.

For more information on Fibre Channel adapters, see the SAN Configuration Guide.

When you create a datastore on a Fibre Channel storage device, the Add Storage Wizard guides you through the configuration.

**To create a datastore on a Fibre Channel device**

1. Log into the VMware VI Client and select a server from the inventory panel.
2. Click the Configuration tab, and then click Storage.
3. Click Add Storage. The Add Storage page appears.
4. Select the Disk/LUN storage type.
5. Click Next.
The Select Disk/LUN page appears.

6. Select the Fibre Channel device you want to use for your datastore.
7. Click Next.

The Current Disk Layout page appears.

8. Look over the current disk layout in the top panel and select a configuration from the bottom panel.

   **Note:** You should dedicate the entire disk/LUN to a single file system because additional file systems that are deployed to this device are only supported if they are used exclusively by the service console.

9. Click Next.
The Properties page appears.

10. Enter a datastore name.
   The datastore name appears in the VI Client and the label must be unique within the current Virtual Infrastructure instance.

11. Click Next.
   The Disk/LUN–Formatting page appears.
12. If needed, adjust the file system values and capacity you use for the datastore. By default, the entire free space available on the storage device is offered to you.

13. Click **Next**.

The Summary page appears.

14. Click **Finish**.

This creates the datastore on a Fibre Channel disk for the ESX Server host.

15. Perform a rescan. See **Performing a Rescan on page 128**.

For advanced configuration, such as using multipathing, masking, and zoning, refer to the **SAN Configuration Guide**.

**Multipathing for Fibre Channel HBAs**

Multipathing support maintains a constant connection between the server machine and the storage device in case of the failure of a host bus adapter (HBA), switch,
storage controller (or storage processor; abbreviated as SP in the following diagram), or a Fibre Channel cable.

This diagram illustrates multiple, redundant paths from each server to the storage device. For example, if HBA1 or the link between HBA1 and the Fibre Channel (FC) switch breaks, HBA2 takes over and provides the connection between the server and the switch. This process is called HBA failover.

Similarly, if SP1 or the link between SP1 and the switch breaks, SP2 takes over and provides the connection between the switch and the storage device. This process is called SP failover. VMware ESX Server provides both HBA and SP failover with its multipathing feature. (SP failover may not be supported by all disk arrays.)

For information on supported SAN hardware, refer to the *SAN Configuration Guide*.

**Viewing the Current Multipathing State**

You can view your current multipathing configuration, the current multipathing policy for a disk, and the connection state and mode for each path to the disk.

The report identifies disks by their canonical name. The canonical name for a disk is the first path ESX Server finds to the disk. Since ESX Server begins its scans at the first controller and the lowest device number, the first path (and thus the canonical name of the disk) is the path with the lowest number controller and device number. For example, if the paths to a disk are `vmhba0:0:2`, `vmhba1:0:2`, `vmhba0:1:2`, and `vmhba1:1:2`, then the canonical name of the disk is `vmhba0:0:2`.

**Setting Your Multipathing Policy for a LUN**

The Manage Paths option allows you to review the current state of paths between your system and SAN LUNs. Multipathing allows continued access to SAN LUNs in the event of hardware failure. Exactly one path is active and in use to any LUN at any time.
To change failover policy

1. Log into the VMware VI Client and select a server from the inventory panel. The hardware configuration page for this agent appears.
2. Click Properties.

3. From the Properties page, click Manage Paths. The Manage Paths page appears. It shows the list of paths to the disk, with the multipathing policy for a disk and the connection state and mode for each path to the disk.
There are two paths to the disk recognized by ESX Server. The list of paths indicates the different physical routes by which the disk can be accessed.

The status of each path to the disk is indicated in the third column. The report lists each path as active, standby, disabled, or dead:

- **Active** — indicates that the path is functional, and that data is being transferred successfully.
- **Standby** — indicates that the path is functional, but is not currently being used to transfer data.
- **Disabled** — indicates that this path has been deliberately turned off.
- **Dead** — indicates that the path should be active, but the software cannot connect to the disk through this path.

An asterisk (*) in the fourth column marks the preferred path. ESX Server always uses this path when it’s available.

The preferred mode is only used by ESX Server to access fixed policy disks. If a disk has a most-recently used (MRU) policy, then the preferred mode is displayed in the report above, but ESX Server will not necessarily use that path to access the disk.

4. Select a device and click **Change**.

You can change the Preference setting and the state of the path.

5. Choose the state of the path.
   - **Enabled** — Makes the path available for load balancing and failover.
   - **Disabled** — Makes the path unavailable for I/O traffic.

6. Click **OK**.
The Manage Paths page opens. From here, you can change the path policy.

7. Under Policy, click Change.

You can select a different policy for each disk. There are two policies:

- **Fixed** — ESX Server always uses the preferred path to the disk. If it cannot access the disk through the preferred path, then it tries the alternate paths. Fixed is the default policy for active/active storage devices.

- **Most Recently Used** — ESX Server uses the most recent path to the disk until this path becomes unavailable. That is, ESX Server does not automatically revert back to the preferred path. Most Recently Used path (MRU) is the default policy for active/passive storage devices.

**Note:** Use the MRU policy for disks on active/passive storage devices. Using the fixed policy may cause path thrashing and significantly reduced performance.

8. Click OK, and then click Close to save your settings and return to the Configuration page.
In Case of Failover

When a cable is pulled, I/O pauses for approximately 30-60 seconds, depending on the array—some interruptions are almost instantaneous, until the SAN driver determines that the link is down and failover occurs. While the I/O pauses, the virtual machines with their virtual disks installed on a SAN may appear unresponsive, and any operations on the /vmfs directory may appear to hang. After the failover occurs, I/O should resume normally.

Even though the ESX Server failover feature ensures high availability and prevents connection loss to SAN devices, all connections to SAN devices might be lost due to disastrous events that include multiple breakages.

If all connections to the storage device are not working, then the virtual machines begin to encounter I/O errors on their virtual SCSI disks. Also, operations in the /vmfs directory may eventually fail after reporting an I/O error.
iSCSI Storage

This section contains information on configuring iSCSI storage and provides the following information:

- About iSCSI Storage on page 103
- Configuring Hardware-Initiated iSCSI Storage on page 106
- Configuring Software-Initiated iSCSI Storage on page 117
- Performing a Rescan on page 128

About iSCSI Storage

This version of ESX Server supports iSCSI technology that allows your ESX Server system to use IP network while accessing remote storage. With iSCSI, SCSI storage commands that your virtual machine issues to its virtual disk are converted into TCP/IP protocol packets and transmitted to a remote device, or target, that stores the virtual disk. From the point of view of the virtual machine, the device appears as locally attached SCSI drive.

iSCSI Initiators

To access remote targets, your ESX Server host uses iSCSI initiators. Initiators transport SCSI requests and responses between the ESX Server system and the target storage device on the IP network.

ESX Server supports hardware-based and software-based iSCSI initiators:

- As a hardware iSCSI initiator, you can use a third-party host bus adapter (HBA) with the iSCSI over TCP/IP capability. This specialized iSCSI adapter is responsible for all iSCSI processing and management. The iSCSI adapter exposes itself as a SCSI HBA to the guest operating system.
- The ESX Server software iSCSI initiator, built into VMkernel, allows your ESX Server system to connect to the iSCSI storage device through the standard network adapter. The software initiator handles the iSCSI processing while communicating with the network adapter through the network stack. With the software initiator, you are able to use the iSCSI technology without purchasing specialized hardware.

Note: Guest operating systems in virtual machines cannot access iSCSI HBAs directly. Guest operating systems can access virtual SCSI drives, which ESX Server maps over iSCSI.
The following diagram depicts two virtual machines that use different types of iSCSI initiators:

- In the first example of iSCSI storage configuration, the ESX Server system uses the hardware iSCSI adapter. This specialized iSCSI adapter sends iSCSI packets to a disk over a LAN.
- In the second example, the ESX Server system is configured with the software iSCSI initiator. Using the software initiator, the ESX Server system connects to a LAN through an existing NIC card.

**Note:** This release does not support using both the hardware and software iSCSI initiators on the same ESX Server system. Use the software initiator only when iSCSI traffic goes over standard network adapters, not when the specialized iSCSI adapters are used.

**Naming Requirements**

Since storage area networks can become large and complex, all iSCSI initiators and targets that use the network have unique and permanent iSCSI names and are assigned addresses for access. The iSCSI name provides a correct identification of a particular iSCSI device, an initiator or a target, regardless of its physical location.
When configuring your iSCSI initiators, make sure they have properly formatted names. The initiators can use one of the following formats:

- IQN (iSCSI qualified name) — can be up to 255 characters long and has the following format:
  
  \[ \text{iqn.<year-mo>.<reversed_domain_name>:<unique_name>}, \]

  where \(<\text{year-mo}>\) represents the year and month your domain name was registered, \(<\text{reversed_domain_name}>\) is the official domain name, reversed, and \(<\text{unique_name}>\) is any name you want to use, for example, the name of your server.

  An example might be `iqn.1998-01.com.mycompany.myserver`.

- EUI (extended unique identifier) — represents the eui. prefix followed by the 16-character name. The name includes 24 bits for company name assigned by the IEEE and 40 bits for a unique ID such as a serial number.

**Discovery Methods**

To determine which storage resource on the network is available for access, the iSCSI initiators ESX Server system supports use these discovery methods:

- Dynamic Discovery — The initiator discovers iSCSI targets by sending a `Send Targets` request to a specified target address. To use this method, you need to enter the address of the target device so that the initiator can establish a discovery session with this target. The target device responds by forwarding a complete list of additional targets that the initiator is allowed to access.

- Static Discovery — After the target device used in the `Send Targets` session sends you the list of additional available targets, they appear on the Static Discovery list. To this list, you may manually add any targets you identify as accessible to your ESX Server host.

  The static discovery method is available only with the hardware-initiated storage.

**iSCSI Security**

Since iSCSI technology uses the Internet to connect to remote targets, it’s necessary to ensure security of the connection. The IP protocol itself does not protect the data it transports and it doesn’t have the capability to verify the legitimacy of initiators that access targets on the network. Therefore, you need to take specific measures to guarantee security across IP networks.

ESX Server supports the Challenge Handshake Authentication Protocol (CHAP) that your iSCSI initiators can use for authentication purposes. After your initiator
estimates the initial connection with the target, CHAP verifies the identity of the initiator and checks a CHAP secret that your initiator and the target share. This can be repeated periodically during the iSCSI session.

When configuring iSCSI initiators for your ESX Server system, make sure that CHAP is enabled. For more information, see Securing iSCSI Storage on page 197.

**Configuring Hardware-Initiated iSCSI Storage**

With the hardware-based iSCSI storage implementation, you use a specialized third-party adapter capable of accessing iSCSI storage over TCP/IP. This iSCSI adapter handles all iSCSI processing and management for your ESX Server system.

You need to install and configure the iSCSI hardware adapter before setting up the datastore that resides on an iSCSI storage device.

Use the following instructions when preparing and setting up datastores that you access through the iSCSI hardware connection:

- Installing iSCSI Hardware Initiator on page 106
- Viewing iSCSI Hardware Initiator on page 106
- Configuring iSCSI hardware initiator on page 108
- Adding Hardware-Initiated iSCSI Storage on page 112

**Installing iSCSI Hardware Initiator**

This release of ESX Server version 3 requires that your host system uses the QLogic QLA4010 iSCSI HBA to initiate iSCSI transactions.


For information on obtaining and installing the adapter, see the QLogic web site at www.qlogic.com.

**Viewing iSCSI Hardware Initiator**

Before you begin configuring the iSCSI hardware initiator, make sure that the iSCSI HBA is successfully installed and appears on the list of adapters available for configuration. If the initiator is installed, you can view its properties.

**To view the iSCSI hardware initiator properties**

1. Log into the VMware VI Client and select a server from the inventory panel.
2. Click the **Configuration** tab, and then click **Storage Adapters**.

The list of available storage adapters appears. The iSCSI HBA should be included in the list of storage adapters.
3. Under HBA, choose the initiator you want to configure.

The details for the initiator display, including the model, IP address, iSCSI name, discovery methods, iSCSI alias, and any discovered targets.
4. Click **Properties**. The iSCSI Initiator Properties dialog box opens. The **General** tab of the iSCSI Initiator Properties dialog box displays additional characteristics of the initiator.

You can now configure your hardware initiator or change its default characteristics.

**Configuring iSCSI hardware initiator**
While configuring the iSCSI hardware initiator, you need to enable your initiator and then set up the initiator’s target addresses and CHAP parameters. See the following sections for more information:

- To enable the iSCSI hardware initiator on page 109
- To set up target addresses for the hardware initiator on page 109
- To set up CHAP parameters for the hardware initiator on page 111

After you configure your iSCSI hardware initiator, perform a rescan, so that all LUNs that the initiator has access to can appear on the list of storage devices available to your ESX Server. For more information, see **Performing a Rescan on page 128.**
To enable the iSCSI hardware initiator

1. Open the iSCSI Initiator Properties dialog box by performing the steps listed in To view the iSCSI hardware initiator properties on page 106.

2. On the iSCSI Initiator Properties dialog box, click Configure. The General Properties dialog box opens, displaying the initiator’s status, default name, and alias.

3. To enable the initiator, select the Enabled check box.

4. To change the default iSCSI name for your initiator, enter the new name. Make sure the name you enter is properly formatted; otherwise, some storage devices may not recognize the iSCSI hardware initiator.

5. Enter the iSCSI alias. The alias is a friendly name that you use to identify the iSCSI hardware initiator.

6. Click OK to save your changes.

To set up target addresses for the hardware initiator

1. Open the iSCSI Initiator Properties dialog box by performing the steps listed in To view the iSCSI hardware initiator properties on page 106.
2. On the iSCSI Initiator Properties dialog box, click the Dynamic Discovery tab.

3. To add a new iSCSI target your ESX Server host can use for a Send Target session, click Add. The Add Send Targets Server dialog box appears.

4. Enter the target’s information and click OK.

   After your ESX Server host establishes the Send Target session with this target device, any newly discovered targets will appear in the Static Discovery list.

5. If you want to change or delete a specific target, select the target and click Edit or Remove.
6. Click the **Static Discovery** tab. The tab displays all dynamically discovered targets.

![Static Discovery Tab](image)

7. To add a target accessible to your ESX Server host, click **Add** and enter the target’s information.

8. If you want to change or delete a specific dynamically discovered target, select the target and click **Edit** or **Remove**.

   **Note:** If you remove a dynamically discovered static target, the target can be returned to the list the next time Send Targets session is run.

**To set up CHAP parameters for the hardware initiator**

1. Open the iSCSI Initiator Properties dialog box by performing the steps listed in To view the iSCSI hardware initiator properties on page 106.
2. On the iSCSI Initiator Properties dialog box, click the CHAP Authentication tab. The tab displays the default CHAP parameters.

3. To make any changes to the existing CHAP parameters, click Configure. The CHAP Authentication dialog box opens.

4. To keep CHAP enabled, make sure Use the following CHAP credentials is selected.

5. If you want to use a new CHAP name, deselect the Use initiator name check box and enter the name of your choice.

6. If needed, specify the CHAP secret. All new targets will use the CHAP secret to authenticate the initiator. Any established sessions are not affected.

7. Click OK to save changes.

   **Note:** If you decide to disable CHAP, all sessions that require CHAP authentication will end immediately.

**Adding Hardware-Initiated iSCSI Storage**

When you create a datastore on a hardware-initiated iSCSI storage device, the Add Storage Wizard guides you through the configuration.
To create a datastore on a hardware-initiated iSCSI device

1. Log into the VMware VI Client and select a server from the inventory panel. The hardware configuration page for this server appears.
2. Click the Configuration tab, and then click Storage.
3. Click Add Storage. The Add Storage page appears.
4. Select the Disk/LUN storage type.

5. Click Next. The Select Disk/LUN page appears.
6. Select the iSCSI device you want to use for your datastore.
7. Click **Next**.

   The Current Disk Layout page appears.

8. Look over the current disk layout in the top panel and select a configuration from the bottom panel.

   **Note:** You should dedicate the entire disk/LUN to a single file system because additional file systems that are deployed to this device are only supported if they are used exclusively by the Service Console.

9. Click **Next**.
The Properties page appears.

10. Enter a datastore name.
    The datastore name appears in the VI Client and the label must be unique within
    the current Virtual Infrastructure instance.
11. Click Next.
The Formatting page appears.

12. If needed, adjust the file system values and capacity you use for the datastore. By default, the entire free space available on the storage device is offered to you.

13. Click Next.

The Summary page appears.

14. Click Finish.

This creates the datastore on the hardware-initiated iSCSI device.
15. Perform a rescan. Performing a Rescan on page 128.

**Configuring Software-Initiated iSCSI Storage**

With the software-based iSCSI implementation, you don’t need to purchase specialized hardware, but can use a standard network adapter to connect your ESX Server system to a remote iSCSI target on the IP network. The ESX Server software iSCSI initiator built into VMkernel facilitates this connection communicating with the network adapter through the network stack.

Before configuring software-based iSCSI storage, you must first enable network connectivity and configure the iSCSI software initiator.

Use the following workflow when preparing and setting up datastores that use iSCSI software-initiated connection to access the iSCSI storage:

1. Configure the VMkernel TCP/IP networking stack. For more information, see VMkernel Configuration on page 32.
2. Open a firewall port. You do so by enabling the iSCSI software client service. For more information, see Opening Firewall Ports for Supported Services and Management Agents on page 185.
3. Configure the iSCSI software initiator. See Configuring iSCSI Software Initiator on page 119.
4. Rescan for new iSCSI LUNs. See Performing a Rescan on page 128.
5. Set up the datastore. See Adding Software-Initiated iSCSI Storage on page 123.

**Viewing Software iSCSI Initiator**

The software iSCSI adapter that your ESX Server system uses to access a software-initiated iSCSI storage device appears on the list of available adapters. You can use the VI Client to review its properties.

**To view the iSCSI software initiator properties**

1. Log into the VMware VI Client and select a server from the inventory panel.
2. Click the **Configuration** tab, and then click **Storage Adapter**.
   
   The list of available storage adapters appears.
3. Under iSCSI Software Adapter, choose the available software initiator.
The details for the initiator display, including the model, IP address, iSCSI name, discovery methods, iSCSI alias, and any discovered targets.

<table>
<thead>
<tr>
<th>Device</th>
<th>Type</th>
<th>Target ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>iSCSI Software Adapter</td>
<td>iSCSI</td>
<td>iqn.com...</td>
</tr>
<tr>
<td>Poweredge Expandable RAID Controller 4L/5L/8L</td>
<td>iSCSI</td>
<td>iqn.com...</td>
</tr>
<tr>
<td>vmhba0</td>
<td>Fibre Channel</td>
<td>iqn.com...</td>
</tr>
<tr>
<td>LP10000 2Gb Fibre Channel Host Adapter</td>
<td>Fibre Channel</td>
<td>iqn.com...</td>
</tr>
</tbody>
</table>

Table: Storage Adapters

Table: Details

- **Model**: iSCSI Software Adapter
- **iSCSI Name**: iqn vmware:vmhba0
- **iSCSI Alias**: vmhba0
- **IP Address**: iqn.com
- **Discovery Methods**: iqn.com
- **Targets**: 0
4. Click **Properties**. The iSCSI Initiator Properties dialog box opens. The **General** tab of the iSCSI Initiator Properties dialog box displays additional characteristics of the software initiator.

You can now configure your software initiator or change its default characteristics.

**Configuring iSCSI Software Initiator**

While configuring the iSCSI software initiator, you need to enable your initiator and then set up the initiator’s target addresses and CHAP parameters. See the following sections for more information:

- To enable the iSCSI software initiator on page 120
- To set up target addresses for the software initiator on page 120
- To set up CHAP parameters for the software initiator on page 122

After you configure your iSCSI hardware initiator, perform a rescan, so that all LUNs that the initiator has access to can appear on the list of storage devices available to your ESX Server. For more information, see **Performing a Rescan on page 128**.
To enable the iSCSI software initiator

1. Open the iSCSI Initiator Properties dialog box by performing the steps listed in To view the iSCSI software initiator properties on page 117.

2. On the iSCSI Initiator Properties dialog box, click **Configure**. The General Properties dialog box opens, displaying the initiator’s status, default name, and alias.

3. To enable the initiator, select the **Enabled** check box.

4. To change the default iSCSI name for your initiator, enter the new name. Make sure the name you enter is properly formatted; otherwise, some storage devices may not recognize the iSCSI hardware initiator.

5. Enter the iSCSI alias or change the existing one. The alias is a friendly name that you use to identify the iSCSI hardware initiator.

6. Click **OK** to save your changes.

To set up target addresses for the software initiator

1. Open the iSCSI Initiator Properties dialog box by performing the steps listed in To view the iSCSI software initiator properties on page 117.
2. On the iSCSI Initiator Properties dialog box, click the **Dynamic Discovery** tab.

![iSCSI Initiator Properties dialog box](image)

3. To add a new iSCSI target your ESX Server host can use for a Send Target session, click **Add**. The Add Send Targets Server dialog box appears.

![Add Send Targets Server](image)

4. Enter the Send Targets server information and click **OK**. After your ESX Server host contacts the Send Targets server, any newly discovered targets will appear in the Static Discovery list.

5. If you want to change or delete a specific Send Targets server, select the server and click **Edit** or **Remove**.
To set up CHAP parameters for the software initiator

1. Open the iSCSI Initiator Properties dialog box by performing the steps listed in To view the iSCSI software initiator properties on page 117.

2. On the iSCSI Initiator Properties dialog box, click the CHAP Authentication tab. The tab displays the default CHAP parameters.
3. To make any changes to the existing CHAP parameters, click Configure. The CHAP Authentication dialog box opens.

![CHAP Authentication dialog box]

4. To keep CHAP enabled, make sure Use the following CHAP credentials is selected.

5. If you want to use a new CHAP name, deselect the Use initiator name check box and enter the name of your choice.

6. If needed, specify the CHAP secret. All new targets will use the CHAP secret to authenticate the initiator. Any established sessions are not affected.

7. Click OK to save changes.

Note: If you decide to disable CHAP, all sessions that require CHAP authentication will end immediately.

Adding Software-Initiated iSCSI Storage

When you create a datastore on a software-initiated iSCSI storage device, the Add Storage Wizard guides you through the configuration.

To create a datastore on a software-initiated iSCSI device

1. Log into the VMware VI Client and select a server from the inventory panel. The hardware configuration page for this server appears.

2. Click the Configuration tab, and then click Storage.

3. Click Add Storage. The Add Storage page appears.
4. Select storage type **Disk/LUN**.

![Select Disk/LUN Page](image)

5. Click **Next**.

   The Select Disk/LUN page appears.

![Select Disk/LUN Page](image)
6. Select the iSCSI device that you want to use for your datastore.

7. Click **Next**.
   The Current Disk Layout page appears.

8. Look over the current disk layout.
   **Note:** You should dedicate the entire disk/LUN to a single file system because additional file systems that are deployed to this device are only supported if they are used exclusively by the Service Console.

9. Click **Next**.
   The Properties page appears.

10. Enter a datastore name.
    The datastore name appears in the VI Client and the label must be unique within the current Virtual Infrastructure instance.

11. Click **Next**.
12. If needed, adjust the file system values and capacity you use for the datastore. By default, the entire free space available on the storage device is offered to you.

13. Click Next.

The Ready to Complete page appears.

14. Click Finish.

This creates the datastore on the software-initiated iSCSI storage device.
15. Perform a rescan. See Performing a Rescan on page 128.
Performing a Rescan

If a new LUN becomes accessible through the adapter, then ESX Server registers this new virtual device for use by virtual machines. If an existing LUN is no longer used and appears to be gone, then it is removed from use by virtual machines.

Consider performing a rescan when:

- Any changes are made to storage disks or LUNs available to your ESX Server system
- Any changes are made to storage adapters
- New datastores are created
- Existing datastores are edited or removed

To perform a rescan

1. In the VI Client, select a host, and then click the Configuration tab.
2. Choose Storage Adapters in the Hardware panel, and then click Rescan above the Storage Adapters panel.
   
   **Note:** You can also select an individual adapter and click Rescan to rescan just that adapter.

3. To discover new disks or LUNs, select Scan for New Storage Devices. If new LUNs are discovered, they appear in the disk/LUN list.

4. To discover new datastores, select Scan for New VMFS Volumes. If new datastores or VMFS volumes are discovered, they appear in the datastore list.
Network Attached Storage

This section contains information about network attached storage (NAS) and provides the following information:

- Shared Storage Capabilities on page 129
- How Virtual Machines Use NFS on page 129
- Managing NFS Devices on page 130
- Configuring ESX Server to Access NFS Volumes on page 131
- Creating an NFS-Based Datastore on page 131

This version of ESX Server supports using network attached storage (NAS) through the NFS protocol. For some users, NFS may be a more cost-effective alternative to SAN storage.

**Shared Storage Capabilities**

ESX Server supports the following shared storage capabilities on NAS:

- Use VMotion — Move running virtual machines from one ESX Server to another without service interruption.
- Create virtual machines on NFS mounted volumes.
- Boot virtual machines stored on NFS mounted volumes.
- Create virtual machine snapshots on NFS mounted volumes. The snapshot feature allows you to preserve the state of the virtual machine so you can return to the same state repeatedly.

**How Virtual Machines Use NFS**

ESX Server allows you to access an NFS server and use NFS volumes to store virtual machine disks. ESX Server supports NFS Version 3 over TCP.

You use the VI Client to configure NFS volumes as datastores. Formatted NFS datastores appear in the VI Client and you can use them to store virtual machine disk files in the same way you use VMFS-based datastores.
The following diagram depicts a virtual machine using the NFS volume to store files.

![Diagram of virtual machine using NFS volume]

In this configuration, ESX Server connects to the NFS server, which stores the disk.

**Note:** If you are creating, configuring, and administering virtual machines on an NFS datastore, you may need to create a special user, known as a delegate user, at the ESX Server level in order for ESX Server users to perform operations on the virtual machine files. For more information, see Configuring Virtual Machine Delegates on page 226.

**Note:** When you use an NFS-based datastore to store a virtual machine disk file, a special .lck-XXX lock file is generated in the same directory where the disk file resides to prevent other ESX hosts from accessing this virtual disk file. You shouldn’t remove the .lck-XXX lock file, otherwise the running virtual machine will not be able to access its virtual disk file.

**Managing NFS Devices**

Using the VI Client, you can register and manage NFS volumes for your ESX Server. The management interface for storage lists registered NFS volumes.
Configuring ESX Server to Access NFS Volumes

NFS requires network connectivity in order to access data stored on remote servers. Before configuring NFS, you must first configure networking for VMotion and IP storage.

For information on configuring a network, see VMkernel Configuration on page 32.

Creating an NFS-Based Datastore

When you create a datastore on an NFS volume, the Add Storage Wizard guides you through the configuration steps.

To mount an NFS volume

1. Log into the VMware VI Client and select a server from the inventory panel.
2. Click the Configuration tab, and then click Storage.
   The Add Storage page appears.
3. Click the Add Storage link.
The Select Storage Type page appears.

4. Select **Network File System** as the storage type. Click **Next**.

   The Locate Network File System page appears.

5. Enter the server name, the mount point folder, and the datastore name.

   **Note:** Avoid using special characters.

6. Click **Next**.
The Network File System Summary page appears.

7. Click Finish.
Managing Storage

This chapter contains information about managing existing datastores and file systems that comprise datastores. The chapter includes the following sections:

- Managing Datastores and File Systems on page 136
- Editing Existing Datastores on page 138
- vmkfstools Commands on page 144
Managing Datastores and File Systems

An ESX Server system uses datastores to store all files associated with its virtual machines. The datastore is a logical storage unit, which can use disk space on one physical device, one disk partition, or span several physical devices. The datastore can exist on different types of physical devices including SCSI, iSCSI, Fibre Channel SAN, or NAS.

For more information on datastores, see Datastores and File Systems on page 76. Datastores are added to the VI Client in one of two ways:

- Discovered when a host is added to the inventory — When you add a host to the inventory, the VI Client displays any datastores known to the host.
- Created on an available storage device — You can use the Add Storage command to create and configure a new datastore.

After you create the datastores, you can use them to store virtual machine files. When needed, you can modify the datastores. For example, you can add extents to your datastore, rename, or remove it.

Adding New Datastores

You can create a datastore on a Fibre Channel, iSCSI, or local SCSI disk. You can also mount an NFS volume over a network connection and use it as a VMware datastore. To create a datastore, choose the type of datastore you want to create using the following options:

- Adding Local SCSI Storage on page 88
- Adding Fibre Channel Storage on page 94
- Adding Hardware-Initiated iSCSI Storage on page 112
- Adding Software-Initiated iSCSI Storage on page 123
- Creating an NFS-Based Datastore on page 131

Removing Existing Datastores

You can remove a datastore that you don’t use. Removing a datastore from the ESX Server system breaks the connection between the system and the storage device that holds the datastore and stops all functions of that storage device. You cannot remove the datastore if there is a currently running virtual machine with virtual disks stored on that datastore.
To remove a datastore

1. Log into the VMware VI Client and select a server from the inventory panel.
2. Click the Configuration tab, and then click Storage (SCSI, SAN, and NFS).
3. To remove a datastore, select the datastore and click Remove. You are asked to
   confirm that you want to remove the datastore.
Editing Existing Datastores

After you create a datastore you can modify it.

Modifying NFS-based Datastores

Your ESX Server can use an NFS volume as a datastore to store virtual machine files. After you have configured the NFS-based datastore, you can modify it if needed.

To modify the NFS-based datastore

1. Log into the VMware VI Client and select a server from the inventory panel.
2. Click the Configuration tab, and then click Storage (SCSI, SAN, and NFS).
3. Select the NFS-based datastore you want to modify and click Properties link. The NFS Datastore Properties dialog box appears.
4. Enter the desired ESX Server.
5. Enter the desired folder.
6. Enter the desired datastore label.
7. Click OK.

Modifying VMFS-based Datastores

Datastores that use the VMFS format are deployed on SCSI-based storage devices.

Note: ESX Server 3 supports VMFS version 3 (VMFS-3). VMFS-3 is not backward compatible with versions of ESX Server earlier than ESX Server 3. If you are using VMFS-2, you can upgrade it to VMFS-3.

You can make a number of changes to your datastore that uses VMFS format. See the following sections for more information:

- Upgrading Datastores on page 139
- Changing the Names of Datastores on page 139
- Adding Extents to Datastores on page 140
Upgrading Datastores

ESX Server 3 includes a new file system, VMFS version 3 (VMFS-3). If your datastore was formatted with VMFS-2, you can only read files stored on VMFS-2, but are not able to use them. To be able to use the files, upgrade VMFS-2 to VMFS-3.

Caution: The VMFS-2 to VMFS-3 conversion is a one-way process. Once the VMFS-based datastore is converted to VMFS-3, you cannot revert it back to VMFS-2.

To upgrade the VMFS-2 to VMFS-3

1. Log into the VMware VI Client and select a server from the inventory panel.
2. Click the Configuration tab, and then click Storage (SCSI, SAN, and NFS).
3. Click the datastore that uses the VMFS-2 format.
4. Click Upgrade to VMFS-3.

Changing the Names of Datastores

To edit the name of the datastore

1. Log into the VMware VI Client and select a server from the inventory panel.
2. Click the Configuration tab, and then click Storage (SCSI, SAN, and NFS).
3. Select the datastore whose name you want to edit and click the **Properties** link. The Properties dialog box appears.

![Properties dialog box](image)

4. Under Volume Properties, click **Change**. The Properties dialog box appears.

![Change button](image)

5. Change the name of the datastore and click **OK**.

**Adding Extents to Datastores**

You can expand a datastore that uses the VMFS format by attaching a hard disk partition as an extent.

**To add one or more extents to the datastore**

1. Log in to the VI Client as root or Administrator.
2. Click the **Configuration** tab, and then click **Storage (SCSI, SAN, and NFS)**.
3. Select the datastore you want to expand and click the **Properties** link. The Properties dialog box appears.
5. Select the disk you want to add as the new extent and click **Next**. The Current Disk Layout page appears.

6. Review the current layout of the disk you are using for the extent to make sure the disk doesn't contain any important information.

   **Note:** If a disk or partition you add was formatted previously, it will be reformatted and lose the file systems and any data it contained.
7. Click Next. The Extent Size page appears. From here, you can set the capacity of the extent.

8. To maximize the extent’s capacity, select Maximize capacity and set the amount in GB. Click Next. The Ready to Complete page appears.

9. Review the proposed extent layout and the new configuration of your datastore. Click Finish.
vmkfstools Commands

The vmkfstools commands provide additional functions that are useful when you need to create files of a particular size and when you need to import files from and export files to the service console’s file system. In addition, vmkfstools is designed to work with large files, overcoming the 2GB limit of some standard file utilities.

For a list of supported vmkfstools commands, see Appendix B: Using vmkfstools on page 277.
This chapter contains information about raw device mapping.

**Note:** For information about configuring SANs, see the *SAN Configuration Guide*.

This chapter covers the following topics:

- Overview on page 146
- Benefits of Raw Device Mapping on page 147
- More About Raw Device Mapping on page 151
- Managing Raw Device Mappings on page 156
Overview

Raw device mapping (RDM) allows a mapping file in a VMFS volume to act as a proxy for a raw device. The mapping file contains metadata used to manage and redirect disk accesses to the physical device. The file gives you some advantages of a virtual disk in the VMFS file system, while keeping some advantages of direct access to physical device. In effect, it merges VMFS manageability with raw device access.

![Diagram of Raw Device Mapping](image)

Raw Device Mapping Redirects Data Transfers

While VMFS is recommended for most virtual disk storage, there is sometimes a need for raw disks. The most common use is as data drives for Microsoft Cluster Service (MSCS) configurations using clusters between virtual machines or between physical and virtual machines.

VMware encourages the use of raw device mapping in the following situations:

- When SAN snapshot or other layered applications are run in the virtual machine. Raw device mapping better enables scalable backup offloading systems using features inherent to the SAN.
- In any MSCS clustering scenario that spans physical hosts — virtual to virtual clusters as well as physical to virtual clusters. VMware recommends that cluster data and quorum disks be configured as raw device mappings rather than as files on a “shared” VMFS.

A raw device mapping can be thought of as a symbolic link from a VMFS volume to a raw LUN. The mapping makes LUNs appear as files in a VMFS volume. The mapping file — not the raw LUN — is referenced in the virtual machine configuration. The mapping file contains a reference to the raw LUN. Using raw device mappings, you can:
• Use VMotion to migrate virtual machines using raw LUNs.
• Add raw LUNs to virtual machines using the Virtual Infrastructure Client.
• Use file system features such as distributed file locking, permissions, and naming.

There are two compatibility modes for raw device mappings: virtual and physical.
• Virtual compatibility mode allows a mapping to act exactly like a virtual disk file, including the use of snapshots.
• Physical compatibility mode allows direct access of the SCSI device, for those applications needing lower level control.

Terminology
In contexts other than this one, such as discussions of the Virtual Infrastructure Client, raw device mapping may be described in terms such as "Mapping a raw device into a datastore," "mapping a system LUN" or "mapping a disk file to a physical disk volume." These terms all refer to raw device mapping.
• Raw disk — A disk volume accessed by a virtual machine as an alternative to a virtual disk file; it may or may not be accessed via a mapping file.
• Raw device — Any SCSI device accessed via a mapping file.
• RDM — Acronym for raw device mapping.
• Raw LUN — A logical disk located in a SAN.
• Mapping file — A VMFS file containing metadata used to map and manage a raw device. A synonym for raw device mapping.
• Mapping — An abbreviated term for a raw device mapping.
• Mapped device — A raw device managed by a mapping file.
• Metadata file — A mapping file.
• Compatibility mode — The virtualization type used for SCSI device access (physical or virtual).

Benefits of Raw Device Mapping
Raw device mapping provides a number of benefits, but it shouldn’t be used in every situation. In general, virtual disk files are preferable to raw device mapping for manageability. When you need raw devices, however, the use of a mapping file is required. The following list highlights both the benefits and limitations of raw device mapping.
• User-Friendly Persistent Names — Raw device mapping provides a user-friendly name for a mapped device. When you use a mapping, you don’t need to
refer to the device by its device name. You refer to it by the name of the mapping file, for example:

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

- **Dynamic Name Resolution** — Raw device mapping stores unique identification information for each mapped device. The VMFS file system resolves each mapping to its current SCSI device, regardless of changes in the physical configuration of the server due to adapter hardware changes, path changes, device relocation, and so forth.

- **Distributed File Locking** — Raw device mapping makes it possible to use VMFS distributed locking for raw SCSI devices. Distributed locking on a raw device mapping makes it safe to use a shared raw LUN without losing data when two virtual machines on different servers try to access the same LUN.

- **File Permissions** — Raw device mapping makes file permissions possible. The permissions of the mapping file are enforced at file open time to protect the mapped volume.

- **File System Operations** — Raw device mapping makes it possible to use file system utilities to work with a mapped volume, using the mapping file as a proxy. Most operations that are valid for an ordinary file can be applied to the mapping file and are redirected to operate on the mapped device.

- **Snapshots** — Raw device mapping makes it possible to use virtual machine snapshots on a mapped volume. Note that snapshots are not available when raw device mapping is used in physical compatibility mode.

- **VMotion** — Raw device mapping allows you to migrate a virtual machine with VMotion. When you use raw device mapping, the mapping file acts as a proxy to
allow VirtualCenter to migrate the virtual machine using the same mechanism that exists for migrating virtual disk files.

- **SAN Management Agents** — Raw device mapping makes it possible to run some SAN management agents inside a virtual machine. Similarly, any software that needs to access a device using hardware-specific SCSI commands can be run inside a virtual machine. This kind of software may be referred to as “SCSI target based software.”

  **Note:** This use requires configuring physical compatibility mode for the mapping file.

  **Note:** VMware works with vendors of storage management software to ensure that their software functions correctly in environments that include ESX Server. Some applications of this kind are:

  - SAN management software.
  - Storage resource management (SRM) software.
  - Snapshot software.
  - Replication software.
Such software uses physical compatibility mode for raw device mappings, so that the software can access SCSI devices directly.

Various management products are best run centrally (not on the ESX Server machine), while others run well in the service console or in the virtual machines. VMware does not certify these applications or provide a compatibility matrix. To find out if a SAN management application is supported in an ESX Server environment, please contact the SAN management software provider.

Limitations of Raw Device Mapping

- **Not Available for Block Devices or Certain RAID Devices** — Raw device mapping (in the current implementation) uses a SCSI serial number to identify the mapped device. Since block devices and some direct-attach RAID devices do not export serial numbers, they can’t be used in raw device mappings.

- **Available with VMFS-2 and VMFS-3 Volumes Only** — Raw device mapping requires the VMFS-2 or VMFS-3 format. In ESX Server 3.0, the VMFS-2 file system is read-only, so you need to upgrade it to VMFS-3 to be able to use files it stores.

- **No Snapshots in Physical Compatibility Mode** — If you are using raw device mapping in physical compatibility mode, you can’t use a snapshot with the disk. Physical compatibility mode allows the virtual machine to manage its own snapshot or mirroring operations. This conflicts with the SCSI virtualization objectives of physical compatibility mode.

  Snapshots are available, however, in virtual mode. The compatibility mode is explained in more detail later in this document.

- **No Partition Mapping** — Note that raw device mapping requires the mapped device to be a whole LUN; mapping to a partition only is not supported.
More About Raw Device Mapping

A raw device mapping file is a special file in a VMFS volume that manages metadata for its mapped device. There is a one-to-one mapping between mapping files and mapped devices. The mapping file is presented to the management software as an ordinary disk file, available for the usual file system operations. To the virtual machine, the storage virtualization layer presents the mapped device as a virtual SCSI device.

Key contents of the metadata in the mapping file include the location of the mapped device (name resolution) and the locking state of the mapped device.

Virtual Compatibility Mode Versus Physical Compatibility Mode

Virtual mode for a mapping specifies full virtualization of the mapped device. It appears to the guest operating system exactly the same as a virtual disk file in a VMFS volume. The real hardware characteristics are hidden. Virtual mode allows customers using raw disks to realize the benefits of VMFS such as advanced file locking for data protection and snapshots for streamlining development processes. Virtual mode is also more portable across storage hardware than physical mode, presenting the same behavior as a virtual disk file.

Physical mode for a raw device mapping specifies minimal SCSI virtualization of the mapped device, allowing the greatest flexibility for SAN management software. In physical mode, the VMkernel passes all SCSI commands to the device, with one exception: The REPORT LUNs command is virtualized, so that the VMkernel can isolate the LUN for the owning virtual machine. Otherwise, all physical characteristics of the
underlying hardware are exposed. Physical mode is useful to run SAN management agents or other SCSI target based software in the virtual machine. Physical mode also allows virtual to physical clustering for cost-effective high availability.

Dynamic Name Resolution

Raw device mapping allows you to give a permanent name to a device by referring to the name of the mapping file in the /vmfs subtree.
The example in the following illustration shows three LUNs. LUN 1 is accessed by its device name, which is relative to the first visible LUN. LUN 2 is a mapped device, managed by a mapping file on LUN 3. The mapping file is accessed by its path name in the `/vmfs` subtree, which is fixed.

All mapped LUNs are uniquely identified by VMFS and the identification is stored in its internal data structures. Any change in the SCSI path, such as a Fibre Channel switch failure or the addition of a new host bus adapter, has the potential to change the `vmhba` device name, because the name includes the path designation (initiator, target, LUN). Dynamic name resolution compensates for all such changes by adjusting the data structures to re-target LUNs to their new device names.
Raw Device Mapping with Virtual Machine Clusters

VMware recommends the use of raw device mapping with virtual machine clusters that need to access the same raw LUN for failover scenarios. The setup is similar to that of a virtual machine cluster that accesses the same virtual disk file, but a raw device mapping file replaces the virtual disk file.

For more information on configuring clustering, refer to the *VMware VirtualCenter Virtual Machine Clustering Manual*.

Comparing Raw Device Mapping to Other Means of SCSI Device Access

To help you choose between several available access modes for SCSI devices, the following table provides a quick comparison of features available with the different modes.

<table>
<thead>
<tr>
<th></th>
<th>Virtual Disk File</th>
<th>Virtual Mode RDM</th>
<th>Physical Mode RDM</th>
</tr>
</thead>
<tbody>
<tr>
<td>SCSI Commands Passed Through</td>
<td>No</td>
<td>No</td>
<td>Yes^1</td>
</tr>
<tr>
<td>VirtualCenter Support</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Snapshots</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Distributed Locking</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Clustering</td>
<td>CIB^2 only</td>
<td>CIB, CAB^3,4</td>
<td>N+1^5 only</td>
</tr>
</tbody>
</table>

^1 Requires Pro Edition
^2 Requires Advanced Edition
^3 Requires Enterprise Edition
^4 Requires Datacenter Edition
^5 Requires vSphere Standard Edition

For more information on configuring clustering, refer to the *VMware VirtualCenter Virtual Machine Clustering Manual*.
1. REPORT LUNS is not passed through
2. CIB = Cluster-In-a-Box
3. CAB = Cluster-Across-Boxes
4. We recommend that you use virtual disk files for CIB. If you think your CIB clusters will be reconfigured as CAB clusters in the future, you can use virtual mode RDMs for CIB. For more information on clustering, see Resource Management Guide.
5. N+1 = Physical to Virtual Clustering

<table>
<thead>
<tr>
<th>SCSI Target-Based Software</th>
<th>Virtual Disk File</th>
<th>Virtual Mode RDM</th>
<th>Physical Mode RDM</th>
</tr>
</thead>
<tbody>
<tr>
<td>NO</td>
<td>NO</td>
<td>YES</td>
<td></td>
</tr>
</tbody>
</table>
Managing Raw Device Mappings

The tools available to manage raw device mappings include the VMware Virtual Infrastructure Client, the `vmkfstools` utility, and ordinary file system utilities used in the service console.

**VMware Virtual Infrastructure Client**

Using the VI Client, you can configure hardware, add disks, and create a raw device mapping. You can use the VI Client to import and export virtual disks, including mapped raw devices. You can also perform common file system operations, such as renaming and setting permissions.

**Creating a Raw Device Mapping**

Use the VI Client to create a raw device mapping.

To create a raw device mapping

1. Log on as administrator or as the owner of the virtual machine to which the mapped disk will belong.
2. Select the virtual machine from the inventory panel.
3. On the Summary tab, click the **Edit Settings** link.
   The Virtual Machine Properties dialog box opens.
4. Click **Add**.
Add Hardware Wizard opens.

5. Choose **Hard Disk** as the type of device you wish to add and click **Next**.
6. In the Select a Disk window, select **Mapped SAN LUN**.
7. Choose the LUN from the list of available LUNs.
8. Select **Store with Virtual Machine**.
9. Choose **Physical** for the Compatibility mode.
10. Specify the SCSI identifier in the Specify Advanced Options window. Normally, you don’t need to change the default settings.
11. In the Ready to Complete window, review your options and click **Finish** to add the disk.

**vmkfstools**

The `vmkfstools` command line utility can be used in the service console to do many of the same operations available through the VI Client. Typical operations applicable to raw device mappings are the commands to create a mapping, to query mapping information such as the name and identification of the mapped device, and to import or export a virtual disk.

For more information, see Appendix B: Using vmkfstools on page 277.
**File System Operations**

Most common file system operations done in the service console can be applied to raw device mappings.

`ls -l`

The `ls` command with the `-l` option shows the file name and permissions of the mapping file, while showing the length of the mapped device.

`du`

Similarly, the `du` command shows the space used by the mapped device, rather than the mapping file.

`mv`

The `mv` command renames the mapping file, but doesn’t affect the mapped device.

`cp`

You can use the `cp` command to copy the contents of a mapped device, but it does not work in reverse. You can’t use it to copy a virtual disk file to a mapped device. Instead, you can use the `vmkfstools` command.

`dd`

You can use the `dd` command to copy data into or out of a mapped device. However, we recommend that you use `vmkfstools` import and export commands to do this in an efficient manner.
Security for ESX Server Systems

ESX Server has been developed with a focus on strong security. This section provides you with an overview of how VMware ensures security in the ESX Server environment, addressing system architecture from a security standpoint and giving you a list of additional security resources you might find valuable.

This chapter contains the following sections:

- ESX Server Architecture and Security Features on page 160
- Other Security Resources and Information on page 171
ESX Server Architecture and Security

Features

From a security perspective, VMware ESX Server consists of four major components: the virtualization layer, the virtual machines, the service console, and the virtual networking layer. The following illustration provides an overview of these components:

Each of these components and this overall architecture have been carefully designed to ensure security of the ESX Server system as a whole.

Security and the Virtualization Layer

The virtualization layer, or VMkernel, is a lightweight kernel designed by VMware from the ground up to run virtual machines. It controls the hardware utilized by ESX Server hosts and schedules the allocation of hardware resources among the virtual machines. Because the VMkernel is fully dedicated to supporting virtual machines and is not used for other purposes, the interface to the VMkernel is strictly limited to the API required to manage virtual machines.
From a security viewpoint, the VMkernel’s tight focus distinguishes it from a general purpose operating system in it minimizes the risk of attackers executing their own code on the host. With a general purpose operating system, an attacker might be able to gain access to the kernel through security flaws in the applications executing on top of the operating system. In this case, the attacker drills into the kernel and starts malicious processes through the API exposed by the improperly secured application. By contrast, this type of attack is unlikely to occur in ESX Server because the VMkernel isn’t capable of doing anything other than running virtual machines and responding to commands from the management interface.

Security and Virtual Machines

Virtual machines are the containers in which applications and guest operating systems run. By design, all VMware virtual machines are isolated from one another. Virtual machine isolation is imperceptible to the guest operating system. Even a user with system administrator privileges on a virtual machine’s guest operating system cannot breach this layer of isolation to access another virtual machine without privileges explicitly granted by the ESX Server system administrator.

This isolation enables multiple virtual machines to run securely while sharing hardware and ensures both their ability to access hardware and their uninterrupted performance. For example, if a guest operating system running in a virtual machine crashes, other virtual machines on the same ESX Server host continue to run. The guest operating system crash has no effect on:

- The ability of users to access the other virtual machines
- The ability of the operational virtual machines to access the resources they need
- The performance of the other virtual machines
Each virtual machine is isolated from other virtual machines running on the same hardware. While virtual machines share physical resources such as CPU, memory, and I/O devices, a guest operating system in an individual virtual machine cannot see any device other than the virtual devices made available to it, as shown in the following illustration:

Because the VMkernel mediates the physical resources and all physical hardware access takes place through the VMkernel, virtual machines cannot circumvent this level of isolation.

Just as a physical machine can communicate with other machines in a network only through a network card, a virtual machine can communicate with other virtual machines running in the same ESX Server host only through a virtual switch. Further, a virtual machine communicates with the physical network, including virtual machines...
Virtual Networking Through Virtual Switches

In considering virtual machine isolation in a network context, you can apply these rules:

- If a virtual machine does not share a virtual switch with any other virtual machine, it is completely isolated from virtual networks within the host.
- If no physical network adapter is configured for a virtual machine, the virtual machine is completely isolated from any physical networks.
- If you use the same safeguards (firewalls, antivirus software, and so forth) to protect a virtual machine from the network as you would for a physical machine, the virtual machine is as secure as the physical machine would be.

You can further protect virtual machines by setting up resource reservations and limits on the ESX Server host. For example, through the fine-grained resource controls available in ESX Server, you can configure a virtual machine so that it always gets at least ten percent of the ESX Server host's CPU resources, but never more than twenty percent.

Resource reservations and limits protect virtual machines from performance degradation if another virtual machine tries to consume too many resources on shared hardware. For example, if one of the virtual machines on an ESX Server host is
incapacitated by a denial-of-service (DOS) or distributed denial-of-service (DDOS) attack, a resource limit on that machine prevents the attack taking up so many hardware resources that the other virtual machines are also affected. Similarly, a resource reservation on each of the virtual machines ensures that, in the event of high resource demands by the virtual machine targeted by the DOS attack, all the other virtual machines still have enough resources to operate. For a discussion of how to manage resource allocation for virtual machines, see the Resource Management Guide.

Security and the Service Console

The ESX Server 3.0 service console is a limited distribution of Linux based on Red Hat Enterprise Linux 3, Update 6 (RHEL 3 U6). The service console provides an execution environment to monitor and administer the entire ESX Server host.

If the service console is compromised in certain ways, the virtual machines it interacts with might also be compromised. To minimize the risk of an attack through the service console, VMware protects the service console with a firewall. For information on this firewall, see Service Console Firewall Configuration on page 234.

In addition to implementing the service console firewall, here are some of the other ways VMware mitigates risks to the service console:

- ESX Server runs only those services essential to managing its functions, and the distribution is limited to the features required to run ESX Server.
- By default, ESX Server is installed with a high security setting, which means that all outbound ports are closed and the only inbound ports that are open are those required for interactions with clients such as the VMware Virtual Infrastructure Client. VMware recommends that you keep this security setting unless the service console is connected to a trusted network.
- By default, all ports not specifically required for management access to the service console are closed. You must specifically open ports if you need additional services.
- All communications from clients are encrypted through SSL by default. The SSL connection uses 256-bit AES block encryption and 1024-bit RSA key encryption.
- The Tomcat Web service, used internally by ESX Server to support access to the service console by Web clients like VMware Virtual Infrastructure Web Access, has been modified to run only those functions required for administration and monitoring by a Web client. As a result, ESX Server is not vulnerable to the Tomcat security issues reported in broader usage.
- VMware carefully monitors all security alerts that could affect service console security and, if needed, issues a security patch, as it would for any other security
vulnerability that could affect ESX Server hosts. VMware provides security patches for RHEL 3 U6 and later as they become available

- Insecure services such as FTP and Telnet, are disabled by default. If you want to use these services, you need to explicitly open ports to support them. You should base this decision on how confident you are that your environment is secure and whether you have implemented sufficient protection for the service console.

- The number of applications that use a setuid or setgid flag has been minimized, and you can disable any setuid or setgid application that is optional to ESX Server operation. For information on required and options setuid and setgid applications, see setuid and setgid Applications on page 247.

For details on these security measures and other service console security recommendations, see Service Console Security on page 229.

While you can install and run certain types of programs designed for RHEL 3 U6 in the service console, this usage can have serious security consequences and is not supported unless VMware explicitly states that it is. If a security vulnerability is discovered in a supported configuration, VMware proactively notifies all customers with valid Support and Subscription contracts and provides all necessary patches.

**Note:** Some security advisories issued by Red Hat don't apply to the ESX Server environment. If this is the case, VMware does not provide notification or patches.

To learn more about VMware’s policies on security patches for supported programs as well as its policies on unsupported software, see Other Security Resources and Information on page 171.

**Security and the Virtual Networking Layer**

The virtual networking layer consists of the virtual network devices through which virtual machines and the service console interface with the rest of the network. ESX Server relies on the connectivity layer to support communications between virtual machines and their users. In addition, ESX Server hosts use the connectivity layer to communicate with iSCSI SANs, NAS storage, and so forth. The connectivity layer includes virtual network adapters and the virtual switches.

The methods you use to secure a virtual machine network depend on what guest operating system is installed, whether the virtual machines operate in a trusted environment, and a variety of other factors. Virtual switches provide a substantial degree of protection when used with other common security practices like installing firewalls. ESX Server also supports IEEE 802.1q VLANs, which you can use to further
protect the virtual machine network, service console, or storage configuration. VLANs let you segment a physical network so that two machines on the same physical network cannot send packets to or receive packets from each other unless they are on the same VLAN.

You can get a sense of how to use virtual switches to implement security tools like DMZs and configure virtual machines on different networks within the same ESX Server host by reviewing the following examples.

**Note:** For a specific discussion of how virtual switches and VLANs help safeguard the virtual machine network and a discussion of other security recommendations for virtual machine networks, see Securing Virtual Machines with VLANs on page 188.

**Example: Creating a Network DMZ Within a Single ESX Server Host**

One example of how to leverage ESX Server isolation and virtual networking features to configure a secure environment is the creation of a network demilitarized zone (DMZ) on a single ESX Server host, as shown in the following illustration:

![DMZ Configured Within a Single ESX Server Host](image)

This configuration includes four virtual machines configured to create a virtual DMZ on Virtual Switch 2. Virtual Machine 1 and Virtual Machine 4 run firewalls and are connected to virtual adapters through virtual switches, and both of these virtual machines are multihomed. Of the remaining two virtual machines, Virtual Machine 2...
runs a Web server and Virtual Machine 3 runs as an application server. Both these virtual machines are single homed.

The Web server and application server occupy the DMZ between the two firewalls. The conduit between these elements is Virtual Switch 2, which connects the firewalls with the servers. This switch has no direct connection with any elements outside the DMZ and is isolated from external traffic by the two firewalls.

From an operational viewpoint, external traffic from the Internet enters Virtual Machine 1 through Hardware Network Adapter 1 (routed by Virtual Switch 1) and is verified by the firewall installed on this machine. If the firewall authorizes the traffic, it is routed to the virtual switch in the DMZ, Virtual Switch 2. Because the Web server and application server are also connected to this switch, they can serve external requests. Virtual Switch 2 is also connected to Virtual Machine 4. This virtual machine provides a firewall between the DMZ and the internal corporate network. This firewall filters packets from the Web server and application server. If a packet is verified, it is routed to Hardware Network Adapter 2 through Virtual Switch 3. Hardware Network Adapter 2 is connected to the internal corporate network.

When creating a DMZ within a single ESX Server, you can use fairly lightweight firewalls. While a virtual machine in this configuration cannot exert direct control over another virtual machine or access its memory, all the virtual machines are still connected through a virtual network, and this network could be leveraged for virus propagation or targeted for other types of attacks. You can consider the virtual machines in the DMZ neither more nor less secure than separate physical machines connected to the same network.
**Example: Creating Multiple Networks Within a Single ESX Server Host**

The ESX Server system is designed so that you can connect some groups of virtual machines to the internal network, others to the external network, and still others to both—all within the same ESX Server host. This capability is an outgrowth of basic virtual machine isolation coupled with a well planned use of virtual networking features, as shown in the following illustration:

![Diagram of ESX Server network configuration](image)

*External Networks, Internal Networks, and a DMZ Configured Within a Single ESX Server Host*

Here, the system administrator configured an ESX Server host into three distinct virtual machine zones, each serving a unique function:

- **FTP server** – *Virtual Machine 1* is configured with FTP software and acts as a holding area for data sent to and from outside resources such as forms and collateral localized by a vendor.
This virtual machine is associated with an external network only. It has its own virtual switch and physical network adapter that connect it to External Network 1. This network is dedicated to servers that the company uses to receive data from outside sources. For example, the company uses External Network 1 to receive FTP traffic from vendors and allow vendors access to data stored on externally available servers through Telnet. In addition to servicing Virtual Machine 1, External Network 1 services FTP and Telnet servers configured on different ESX Server hosts throughout the site.

Because Virtual Machine 1 doesn’t share a virtual switch or physical network adapter with any virtual machines in the host, the other resident virtual machines cannot transmit packets to or receive packets from Virtual Machine 1’s network. This prevents sniffing attacks, which require sending network traffic to the victim. More importantly, an attacker cannot leverage the natural vulnerability of FTP to access any of the host’s other virtual machines.

- **Internal virtual machines** – Virtual Machines 2 – 5 are reserved for internal use. These virtual machines process and store company-private data such as medical records, legal settlements, and fraud investigations. As a result, the system administrators must ensure the highest level of protection for these virtual machines.

  These virtual machines connect to Internal Network 2 through their own virtual switch and network adapter. Internal Network 2 is reserved for internal use by personnel such as claims processors, in-house lawyers, or adjustors.

  Virtual Machines 2 – 5 can communicate with one another through the virtual switch and with internal virtual machines elsewhere on Internal Network 2 through the physical network adapter. They cannot communicate with externally-facing machines. As with the FTP server, these virtual machines cannot send packets to or receive packets from the other virtual machines’ networks. Similarly, the host’s other virtual machines cannot send packets to or receive packets from Virtual Machines 2 – 5.

- **DMZ** – Virtual Machines 6 – 8 are configured as a DMZ that the marketing group uses to publish the company’s external Web site.

  This group of virtual machines is associated with External Network 2 and Internal Network 2. The company uses External Network 2 to support the Web servers used by the marketing and financial department to host the corporate Web site and other Web facilities that it hosts to outside users. Internal Network 1 is the conduit that the marketing department uses to publish web pages to the corporate Web site, post downloads, and maintain services like user forums.
Because these networks are separate from *External Network 1* and *Internal Network 2* and the virtual machines have no shared points of contact (switches or adapters), there is no risk of attack to or from the FTP Server or the internal virtual machine group.

For an example of configuring a DMZ with virtual machines, see *Creating a Network DMZ Within a Single ESX Server Host* on page 166.

By capitalizing on virtual machine isolation, correctly configuring virtual switches, and maintaining network separation, the system administrator can house all three virtual machine zones in the same ESX Server host and be confident that there will be no data or resource breaches.

The company enforces isolation among the virtual machine groups by using multiple internal and external networks and making sure that the virtual switches and physical network adapters for each group are completely separate from those of other groups.

Because none of the virtual switches straddle virtual machine zones, the system administrator succeeds in eliminating the risk of packet leakage from one zone to another. A virtual switch, by design, cannot leak packets directly to another virtual switch. The only way for packets to travel from one virtual switch to another is if:

- The virtual switches are connected to the same physical LAN.
- The virtual switches connect to a common virtual machine, which could then be used to transmit packets.

Neither of these conditions occur in sample configuration. If the system administrator wants to verify that no common virtual switch paths exist, he or she can check for possible shared points of contact by reviewing the network switch layout in the VI Client or VI Web Access. For information on the virtual switch layout, see *Virtual Switches* on page 24.

To safeguard the virtual machines' resources, the system administrator lowers the risk of DOS and DDOS attacks by configuring a resource reservation and limit for each virtual machine. The system administrator further protects the ESX Server host and virtual machines by installing software firewalls at the front and back ends of the DMZ, ensuring that the ESX Server host is behind a physical firewall, and configuring the service console and networked storage resources so that each has its own virtual switch.
## Other Security Resources and Information

You can find additional information on security topics through the following resources:

<table>
<thead>
<tr>
<th>Topic</th>
<th>Resource</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware security policy, up-to-date security alerts, security downloads, and focus discussions of security topics</td>
<td><a href="http://www.vmware.com/vmtn/technology/security">http://www.vmware.com/vmtn/technology/security</a></td>
</tr>
</tbody>
</table>
VMware is deeply committed to helping you maintain a secure environment. To reassure you that any security issues will be corrected in a timely fashion, the VMware Security Response Policy states our commitment to resolve possible vulnerabilities in our products. |
Search for the term “VMware” on this site to find the certification status of specific VMware products. |
| Third-party software support policy               | [http://www.vmware.com/support/policies](http://www.vmware.com/support/policies)  
VMware supports a variety of storage systems, software agents such as backup agents, system management agents, and so forth. You can find lists of agents, tools, and other software supported by ESX Server by searching [http://www.vmware.com/vmtn/resources](http://www.vmware.com/vmtn/resources) for ESX Server compatibility guides.  
Be aware that the industry offers more products and configurations than VMware can test. If VMware does not list a product or configuration in a compatibility guide, Technical Support will attempt to help you with any problems you encounter, but cannot guarantee that the product or configuration can be used. Always evaluate any security risks for unsupported products or configurations carefully. |
Securing an ESX Server Configuration

This chapter describes measures you can take to promote a secure environment for your ESX Server hosts, virtual machines, and iSCSI SANs. The discussion focuses on network configuration planning from a security perspective and the steps you can take to protect the components in your configuration from attack.

This chapter covers the following topics:

- Securing the Network with Firewalls on page 174
- Securing Virtual Machines with VLANs on page 188
- Securing iSCSI Storage on page 197
Securing the Network with Firewalls

Security administrators use firewalls to safeguard the network or selected components within the network from intrusion. Firewalls control access to devices within their perimeter by closing all communication pathways except for those that the administrator explicitly or implicitly designates as authorized, thus preventing unauthorized use of the devices. The pathways, or ports, that administrators open in the firewall allow traffic between devices on different sides of the firewall.

In a virtual machine environment, you can plan your layout for firewalls between:

- Physical machines like VirtualCenter Management Server hosts and ESX Server hosts
- One virtual machine and another—for example, between a virtual machine acting as an external Web server and a virtual machine connected to your company's internal network
- A physical machine and a virtual machine as when you place a firewall between a physical network adapter card and a virtual machine

How you utilize firewalls in an ESX Server configuration is based on how you plan to use the network and how secure any given component needs to be. For example, if you create a virtual network where each virtual machine is dedicated to running a different benchmark test suite for the same department, the risk of unwanted access from one virtual machine to the next is minimal. Hence, you have little need to set up the configuration so that firewalls are present between the virtual machines. However, to prevent interruption of a test run from an outside host, you might set up the configuration so that a firewall is present at the entry point of the virtual network to protect the entire set of virtual machines.
This section shows firewall placement for configurations with and without VirtualCenter. It also provides information on the firewall ports required for ESX Server systems. The section covers the following topics:

- Firewalls for Configurations With a VirtualCenter Server on page 176
- Firewalls for Configurations Without a VirtualCenter Server on page 179
- TCP and UDP Ports for Management Access on page 180
- Connecting to VirtualCenter Server Through a Firewall on page 182
- Connecting to the Virtual Machine Console Through a Firewall on page 183
- Connecting ESX Server Hosts Through Firewalls on page 185
- Opening Firewall Ports for Supported Services and Management Agents on page 185

**Note:** For information on the service console firewall, see Service Console Firewall Configuration on page 234. To configure the firewall and port settings during installation, see the *Installation and Upgrade Guide.*
Firewalls for Configurations With a VirtualCenter Server

If you use a VirtualCenter Server, you can install firewalls at any of the locations shown in the following illustration.

**Note:** Depending on your configuration, you might not need all the firewalls in the illustration, or you might need firewalls in locations not shown.

Networks configured with a VirtualCenter Server can receive communications through several types of clients: the VI Client, VI Web Access, or third-party network management clients that use the SDK to interface with the host. During normal operation, VirtualCenter listens for data from its managed hosts and clients on...
designated ports. VirtualCenter also assumes that its managed hosts listen for data from VirtualCenter on designated ports. If a firewall is present between any of these elements, you must ensure that there are open ports in the firewall to support data transfer.

If you access ESX Server hosts through a VirtualCenter Server, you typically protect the VirtualCenter Server using a firewall. This firewall provides basic protection for your network. Whether this firewall lies between the clients and the VirtualCenter Server or both the VirtualCenter Server and the clients are behind the firewall depends on your deployment. The main thing is to ensure that a firewall is present at what you consider to be an entry point for the system as a whole.

You might also want to include firewalls at a variety of other access points in the network, depending on how you plan to use the network and how secure the various devices need to be. The following is a list of firewall locations common to ESX Server implementations. Many of the firewall locations in the list and illustration are optional. Select the locations for your firewalls based on the security risks that you've identified for your network configuration.

- Between your Web browser and VI Web Access HTTP and HTTPS proxy server.
- Between the VI Client, VI Web Access, or a third-party network management client and the VirtualCenter Server.
- If your users access virtual machines through the VI Client, between the VI Client and the ESX Server host. This connection is in addition to the connection between the VI Client and the VirtualCenter Server, and it requires a different port.
- If your users access virtual machines through a Web browser, between the Web browser and the ESX Server host. This connection is in addition to the connection between the VI Web Access Client and VirtualCenter Server, and it requires different ports.
- Between the license server and either the VirtualCenter Server or the ESX Server host. Typically, in configurations that include a VirtualCenter Server, the license server runs on the same physical machine as does the VirtualCenter Server. In this case, the license server connects to the ESX Server network through a firewall, running in parallel with the VirtualCenter Server but using different ports.

In some configurations, you might use an external license server—for example, if your company wants to control all licenses through a single, dedicated
appliance. Here, you would connect the license server to the VirtualCenter Server through a firewall between these two servers.

Regardless of how you set up the license server connection, the ports you use for license traffic are the same. For information on licensing, see the Installation and Upgrade Guide.

- Between the VirtualCenter Server and the ESX Server hosts.
- Between the ESX Server hosts in your network. Although traffic between ESX Server hosts is usually considered to be trusted, you can add firewalls between your ESX Server hosts if you are concerned about security breaches from machine to machine.

  If you add firewalls between ESX Server hosts and plan to migrate virtual machines between the servers, perform cloning, or use VMotion, you must also open ports in any firewall that divides the source host from the target hosts so that the source and targets can communicate.

- Between the ESX Server hosts and peripheral devices such as NFS storage. These ports are not specific to VMware, and you configure them according to the specifications for your network.

  For information on the ports to open for these communications paths, see TCP and UDP Ports for Management Access on page 180.
Firewalls for Configurations Without a VirtualCenter Server

If you connect clients directly to your ESX Server network instead of using a VirtualCenter Server, your firewall configuration is somewhat simpler. You might install firewalls at any of the locations shown in the following illustration.

**Note:** Depending on your configuration, you might not need all the firewalls in the illustration, or you might need firewalls in locations not shown.

Networks configured without a VirtualCenter Server receive communications through the same types of clients as they do if a VirtualCenter Server were present: VI Client, VI Web Access Clients, or third-party network management clients. For the most part, the firewall needs are the same, but there are several key differences:

- Just as you would for configurations that include a VirtualCenter Server, you should be sure a firewall is present to protect your ESX Server layer or, depending on your configuration, your clients and ESX Server layer. This firewall provides basic protection for your network. The firewall ports you use are the same as those you use if a VirtualCenter Server is in place.
Licensing in this type of configuration is part of the ESX Server package that you install on each of the ESX Server hosts. Because licensing is resident to the server, you do not need to install a separate license server. This eliminates the need for a firewall between the license server and the ESX Server network.

**Note:** In some situations, you might want to centralize your licenses. You can choose to maintain a separate license server or house the license server on one of the ESX Server hosts in your network. With either of these approaches, you connect the license server to the ESX Server network through a firewall using the ports normally reserved for virtual machine licensing, much as you do if a VirtualCenter Server is present. Configurations that use a license server other than the one automatically installed on the ESX Server host require additional setup. For information on licensing, see the *Installation and Upgrade Guide*.

**TCP and UDP Ports for Management Access**

This section lists predetermined TCP and UDP ports used for management access to your VirtualCenter Server, ESX Server hosts, and other network components. If you need to manage network components from outside a firewall, you might need to reconfigure the firewall to allow access on the appropriate ports.

**Note:** The ports listed in the table are connected through the service console interface unless otherwise indicated.

<table>
<thead>
<tr>
<th>Port</th>
<th>Purpose</th>
<th>Traffic Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>80</td>
<td>HTTP access. This is the default non-secure TCP Web port and is typically used in conjunction with port 443 as a front end for access to ESX Server networks from the Web. Port 80 redirects traffic to an HTTPS landing page (port 443) from which you launch your virtual machine console. Use port 80 for connection to VI Web Access from the Web.</td>
<td>Incoming TCP</td>
</tr>
<tr>
<td>443</td>
<td>HTTPS access. This is the default SSL Web port. Use Port 443 for the following: • Connection to VI Web Access from the Web. • VI Web Access and third-party network management client connections to the VirtualCenter Server. • Direct VI Web Access and third-party network management clients access to ESX Server hosts.</td>
<td>Incoming TCP</td>
</tr>
</tbody>
</table>
CHAPTER 9 Securing an ESX Server Configuration

<table>
<thead>
<tr>
<th>Port</th>
<th>Purpose</th>
<th>Traffic Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>902</td>
<td>Authentication traffic for the ESX Server host and virtual machine configuration. Use Port 902 for the following: • VI Client access to the VirtualCenter Server. • VirtualCenter Server access to ESX Server hosts. • Direct VI Client access to ESX Server hosts. • ESX Server host access to other ESX Server hosts for migration and provisioning.</td>
<td>Traffic Type: Incoming TCP, outgoing UDP</td>
</tr>
<tr>
<td>903</td>
<td>Remote console traffic generated by user access to virtual machines on a specific ESX Server host. Use Port 903 for the following: • VI Client access to virtual machine consoles. • VI Web Access Client access to virtual machine consoles.</td>
<td>Traffic Type: Incoming TCP</td>
</tr>
<tr>
<td>2049</td>
<td>Transactions from your NAS storage devices. This port is used on the VMkernel interface rather than the service console interface.</td>
<td>Traffic Type: Incoming and outgoing TCP</td>
</tr>
<tr>
<td>2050–5000</td>
<td>Traffic between ESX Server hosts for VMware High Availability (HA) and EMC Autostart Manager.</td>
<td>Traffic Type: Outgoing TCP, incoming and outgoing UDP</td>
</tr>
<tr>
<td>3260</td>
<td>Transactions from your iSCSI storage devices. This port is used on the VMkernel interface rather than the service console interface.</td>
<td>Traffic Type: Incoming and outgoing TCP</td>
</tr>
<tr>
<td>8000</td>
<td>Incoming requests from VMotion. This port is used on the VMkernel interface rather than the service console interface.</td>
<td>Traffic Type: Incoming and outgoing TCP</td>
</tr>
<tr>
<td>8042–8045</td>
<td>Traffic between ESX Server hosts for HA and EMC Autostart Manager.</td>
<td>Traffic Type: Outgoing TCP, incoming and outgoing UDP</td>
</tr>
<tr>
<td>27000</td>
<td>License transactions from ESX Server to the license server.</td>
<td>Traffic Type: Outgoing TCP</td>
</tr>
<tr>
<td>27010</td>
<td>License transactions from the license server.</td>
<td>Traffic Type: Incoming TCP</td>
</tr>
</tbody>
</table>

**Note:** ESX Server and VirtualCenter use port 8085 internally. For ESX Server, port 8085 is protected because it doesn’t accept remote connections. To ensure that VirtualCenter can operate correctly, you should reserve port 8085 for VirtualCenter use. You should also consider protecting port 8085 from outside traffic by keeping it closed.
In addition to the TCP and UDP ports just discussed, you can configure other ports depending on your needs:

- You can use VirtualCenter to open ports for installed management agents and supported services such as SSH, NFS, and so forth. For information on configuring additional ports for these services, see Opening Firewall Ports for Supported Services and Management Agents on page 185.

- You can open ports in the service console firewall for other services and agents required for your network by running command line scripts. For more information, see Service Console Firewall Configuration on page 234.

**Connecting to VirtualCenter Server Through a Firewall**

As shown in the table, the ports that VirtualCenter Server uses to listen for data transfer from its clients are 902 (VI Client) and 443 (other clients). If you have a firewall between your VirtualCenter Server and its clients, you must configure a means for the VirtualCenter Server to receive data from the clients.

To enable the VirtualCenter Server to receive data from a VI Client, open port 902 in the firewall to allow data transfer from the VI Client to the VirtualCenter Server. For connections between the VirtualCenter Server and VI Web Access Clients or third-party clients working through the SDK, open port 443. Contact the firewall system administrator for additional information on configuring ports in a firewall.

If you are using the VI Client and don’t want to use port 902 as the port for the VI Client-to-VirtualCenter Server communication, you can switch to another port by changing the VirtualCenter settings in the VI Client. To learn how to change these settings, see the Virtual Infrastructure User’s Guide.
Connecting to the Virtual Machine Console Through a Firewall

Whether you connect your client to ESX Server hosts through a VirtualCenter Server or use a direct connection to the ESX Server host, certain ports are required for user and administrator communication with virtual machine consoles. These ports support different client functions, interface with different layers within ESX Server, and use different authentication protocols:

- **Port 902** – The VirtualCenter Server uses this port to send data to the VirtualCenter managed hosts. Also, the VI Client, when connected directly to an ESX Server host, uses this port to support any management functions related to the server and its virtual machines. Port 902 is the port that the VirtualCenter Server and the VI Client assume is available when sending data to the ESX Server host. VMware doesn’t support configuring a different port for these connections. Port 902 connects the VirtualCenter Server or client to the ESX Server host through the VMware Authorization Daemon (vmware-authd) running in the service console. The authorization daemon multiplexes port 902 data to the VMware Host Agent (vmware-hostd) for processing.

- **Port 443** – The VI Web Access Client and SDK use this port to send data to the VirtualCenter managed hosts. Also, the VI Web Access Client and SDK, when connected directly to an ESX Server host, use this port to support any management functions related to the server and its virtual machines. Port 443 is the port that the VI Web Access Client and the SDK assume is available when sending data to the ESX Server host. VMware doesn’t support configuring a different port for these connections. Port 443 connects the VI Web Access Client or third-party network management client to the ESX Server host through the Tomcat Web service or the SDK, respectively. These processes multiplex port 443 data to vmware-hostd for processing.

- **Port 903** – The VI Client and VI Web Access use this port to provide a connection for guest operating system mouse/keyboard/screen (MKS) activities on virtual machines. It is through this port that users interact with the virtual machine guest operating systems and applications. Port 903 is the port that the VI Client and VI Web Access assume is available when interacting with virtual machines. VMware doesn’t support configuring a different port for this function. Port 903 connects the VI Client to a specified virtual machines configured on the ESX Server host.
The following illustration shows the relationships between VI Client functions, ports, and ESX Server processes. The VI Web Access Client uses the same basic mapping for its interactions with the ESX Server host.

**Port Usage for VI Client Communications with ESX Server**

If you have a firewall between your VirtualCenter Server and VirtualCenter managed host, open Ports 902 and 903 in the firewall to allow data transfer to:

- ESX Server hosts from the VirtualCenter Server.
- ESX Server hosts directly from the VI Client and VI Web Access.

Refer to the firewall system administrator for additional information on configuring the ports.
Connecting ESX Server Hosts Through Firewalls

If you have a firewall between two ESX Server hosts and you wish to allow transactions between the hosts or use VirtualCenter to perform any source/target activities, such as VMware High Availability (HA) traffic, migration, cloning, or VMotion, you must configure a means for the managed hosts to receive data. To do so, you open ports in the following ranges:

- 902 (server-to-server migration and provisioning traffic)
- 2050–5000 (for HA traffic)
- 8000 (for VMotion)
- 8042–8045 (for HA traffic)

Refer to the firewall system administrator for additional information on configuring the ports. For more detailed information on the directionality and protocol for these ports, see TCP and UDP Ports for Management Access on page 180.

Opening Firewall Ports for Supported Services and Management Agents

You use VI Client to configure the service console firewall to accept commonly supported services and installed management agents. When you configure the ESX Server host security profile in VirtualCenter, you add or remove these services or agents, automatically opening or closing predetermined ports in the firewall to allow communication with the service or agent. The following is a list of the services and agents you can add or remove:

- NIS client
- NFS client (insecure service)
- SMB client (insecure service)
- FTP client (insecure service)
- SSH client
- Telnet client (insecure service)
- NTP client
- iSCSI software client
- SSH server
- Telnet server (insecure service)
- FTP server (insecure service)
- NFS server (insecure service)
- CIM HTTP server (insecure service)
- CIM HTTPS server
- SNMP server
- Other supported management agents you install

**Note:** This list can change over time. As a result, you might find that the VI Client provides services and agents not mentioned in the list. Also, not all services on the list are installed by default. You may need to perform additional activities to configure and enable these services.

If you are installing a device, service, or agent not on this list, you need to open ports in the service console firewall from a command line. For more information, see Service Console Firewall Configuration on page 234.

**To allow access to ESX Server for a service or management agent**

1. Log on to the VI Client and select the server from the inventory panel. The hardware configuration page for this server appears.

2. Click the **Configuration** tab and then click **Security Profile**.

The VI Client displays a list of currently active incoming and outgoing connections with the corresponding firewall ports.

<table>
<thead>
<tr>
<th>Service</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>NFS Server</td>
<td>5600-5964 (TCP)</td>
</tr>
<tr>
<td>SSH Server</td>
<td>22 (TCP)</td>
</tr>
<tr>
<td>SNMP Server</td>
<td>161 (UDP)</td>
</tr>
<tr>
<td>CIM Server</td>
<td>9080 (TCP)</td>
</tr>
<tr>
<td>CIM API Client</td>
<td>2700-2709,3100-3149 (TCP, UDP)</td>
</tr>
<tr>
<td>CIM Secure Server</td>
<td>5989 (TCP)</td>
</tr>
<tr>
<td>CIM SLP</td>
<td>427 (UDP, TCP)</td>
</tr>
<tr>
<td>Other services/agents</td>
<td></td>
</tr>
</tbody>
</table>

**Incoming Connections**

<table>
<thead>
<tr>
<th>Service</th>
<th>Ports</th>
</tr>
</thead>
<tbody>
<tr>
<td>CIM API Client</td>
<td>2700-2709,3100-3149 (TCP, UDP)</td>
</tr>
<tr>
<td>CIM SLP</td>
<td>427 (UDP, TCP)</td>
</tr>
<tr>
<td>VMware License Client</td>
<td>2003,2004 (TCP)</td>
</tr>
<tr>
<td>NFS Client</td>
<td>111,1099 (UDP, TCP)</td>
</tr>
<tr>
<td>NIS Client</td>
<td>110,140 (UDP, TCP)</td>
</tr>
<tr>
<td>NTP Client</td>
<td>123 (UDP)</td>
</tr>
<tr>
<td>SNMP Client</td>
<td>161 (UDP)</td>
</tr>
<tr>
<td>SSH Client</td>
<td>22 (TCP)</td>
</tr>
<tr>
<td>Software Update Client</td>
<td>3999 (TCP)</td>
</tr>
<tr>
<td>Vmware VirtualCenter Agent</td>
<td>902 (UDP)</td>
</tr>
</tbody>
</table>
3. Click **Firewall > Properties** to open the **Firewall Properties** dialog box. This dialog box lists all the services and management agents you can configure for the host.

4. Select the check boxes for the services and agents you want to enable. The **Incoming Ports** and **Outgoing Ports** columns indicate the port or ports that the VI Client opens for the service, and the **Protocol** column indicates the protocol the service uses.

5. Click **OK**.
Securing Virtual Machines with VLANs

The network can be one of the most vulnerable parts of any system. Just as the physical network requires protection, so does your virtual machine network. If your virtual machine network is connected to a physical network, it can be subject to breaches to the same degree that a network made up of physical machines would be. Even if the virtual machine network is isolated from any physical network, virtual machines within the network can be subject to attacks from other virtual machines in the network. The requirements for securing virtual machines are often the same as those for physical machines.

Virtual machines are isolated from each other. One virtual machine can't read or write another virtual machine's memory, access its data, use its applications, and so forth. However, within the network, any virtual machine or group of virtual machines can still be the target of unauthorized access from other virtual machines and might require further protection by external means. You can add this level of security by:

- Adding firewall protection to your virtual network by installing and configuring software firewalls on some or all of its virtual machines.

  **Note:** For efficiency, you can set up private virtual machine Ethernet networks, or virtual networks, of up to 1024 virtual machines. With virtual networks, you install a software firewall on a virtual machine at the head of the virtual network. This serves as a protective buffer between the physical network adapter and the remaining virtual machines in the virtual network. While installing a software firewall on virtual machines at the head of virtual networks is a good security practice, your need to balance your security needs against performance factors if you are considering installing software firewalls on virtual machines elsewhere in the virtual network. For more information on virtual networks, see Concepts on page 19.

- Use separate physical network adapters for virtual machine zones to ensure that the zones are isolated. Maintaining separate physical network adapters for virtual machine zones within the host helps eliminate concerns that data can leak from one virtual machine zone to another.

- Setting up Virtual Local Area Networks (VLANs) to help safeguard your network against various security threats. These threats include Address Resolution Protocol (ARP) spoofing in which an attacker manipulates the ARP table to remap MAC and IP addresses, thereby gaining access to network traffic to and from a host. Attackers use ARP spoofing to generate denials of service, hijack the target system, and otherwise disrupt the virtual network.
Because VLANs provide the almost all of the security benefits inherent in implementing physically separate networks without the hardware overhead, they offer a viable solution that can save you the cost of deploying and maintaining additional devices, cabling, and so forth.

VLANs are an IEEE standard networking scheme with specific tagging methods that allow routing of packets to only those ports that are part of the VLAN. When properly configured, VLANs provide a dependable means for you to protect a set of virtual machines from accidental or malicious intrusions.

VLANs let you segment a physical network so that two machines in the network are unable to transmit packets back and forth unless they are part of the same VLAN. For example, accounting records and transactions are among a company’s most sensitive internal information. In a company whose sales, shipping, and accounting employees all use virtual machines in the same physical network, you might protect the virtual machines for the accounting department by setting up VLANs as shown in the following illustration:

![Sample VLAN Layout](image)

In this configuration, all employees in the accounting department use virtual machines in VLAN A and the employees in sales use virtual machines in VLAN B. The...
router forwards packets containing accounting data to the switches. These packets are tagged for distribution to VLAN A only. Therefore, the data is confined to Broadcast Domain A, and cannot be routed to Broadcast Domain B unless the router is configured to do so. This VLAN configuration prevents the sales force from intercepting packets destined for the accounting department. It also prevents the accounting department from receiving packets intended for the sales group. Note that the virtual machines serviced by a single virtual switch can be in different VLANs.

The following section provides suggestions for securing your network through virtual switches and VLANs. The section covers the following topics:

- Security Considerations for VLANs on page 190
- Virtual Switch Protection and VLANs on page 192
- Securing Virtual Switch Ports on page 194

Security Considerations for VLANs

ESX Server features a complete IEEE 802.1q-compliant VLAN implementation. The way you set up VLANs to secure parts of a network depends on a variety of factors such as the guest operating system you install, the way your network equipment is configured, and so forth. While VMware cannot make any specific recommendations on how to set up VLANs, here are some factors you should consider when using a VLAN deployment as part of your security enforcement policy:

- **Treat VLANs as part of a broader security implementation** – VLANs are an effective means of controlling where and how widely data is transmitted within the network. If an attacker gains access to the network, the attack is likely to be limited to the VLAN that served as the entry point, lessening the risk to the network as a whole.

VLANs provide protection only in that they control how data is routed and contained after it passes through the switches and enters the network. You can use VLANs to help secure Layer 2 of your network model—the data link layer. However, configuring VLANs doesn’t protect the physical layer of your network model or any of the other layers. Even if you create VLANs, you should provide additional protection by securing your hardware (routers, hubs, and so forth) and encrypting data transmissions.

Also, VLANs are not a substitute for software firewalls in your virtual machine configurations. Most network configurations that include VLANs also include software firewalls. If you include VLANs in your virtual network, be sure that any firewalls you install are VLAN-aware.
Be sure your VLANs are properly configured – Depending on your equipment vendor, a VLAN you set up can be vulnerable to VLAN hopping attacks. VLAN hopping occurs when an attacker with authorized access to one VLAN creates packets that trick physical switches into transmitting the packets to another VLAN that the attacker is not authorized to access. Vulnerability to this type of attack usually results from a switch being misconfigured for native VLAN operation, in which the switch can receive and transmit untagged packets. VMware virtual switches don’t support the concept of a native VLAN. All data passed on these switches is appropriately tagged. However, because there might be other switches in the network that are configured for native VLAN operation, VLANs configured with virtual switches can still be vulnerable to VLAN hopping. If you plan to use VLANs to enforce network security, VMware recommends that you disable the native VLAN feature for all switches unless you have a compelling need to operate some of your VLANs in native mode. If you do need to use native VLAN, pay particular attention to your switch vendor’s configuration guidelines for this feature.

Create a separate VLAN or virtual switch for the service console – Whether you use a management client or the command line, all configuration tasks for ESX Server are performed through the service console, including configuring storage, controlling aspects of virtual machine behavior, and setting up virtual switches or virtual networks. Because the service console is the point of control for ESX Server, safeguarding it from misuse is crucial.

While VMware ESX Server management clients use authentication and encryption to prevent unauthorized access to the service console, other services might not offer the same protection. If attackers gain access to the service console, they are free to reconfigure many attributes of the ESX Server host. For example, they could change the entire virtual switch configuration, change authorization methods, and so forth.

Network connectivity for the service console is established through virtual switches. To provide better protection for this critical ESX Server component, VMware recommends that you isolate the service console using one of these methods:

- Create a separate VLAN for the service console. This measure prevents anyone without access to that VLAN from seeing traffic to and from the service console. It also prevents attackers from sending any packets to the service console.
• Configure network access for the service console through a single virtual switch and one or more uplink ports. Because the virtual switch and ports are dedicated exclusively to the service console, the service console is protected from access by virtual machine users.

In addition to setting up a separate VLANs or virtual switch for the service console, you should set up separate a VLAN or virtual switch for VMotion and for network attached storage.

Virtual Switch Protection and VLANs
VMware virtual switches provide safeguards against certain threats to VLAN security. Because of the way that virtual switches are designed, they protect VLANs against a variety of attacks, many of which involve VLAN hopping.

The following discussion gives you an idea of some attacks virtual switches and VLANs can protect against. Having this protection does not guarantee that your virtual machine configuration is invulnerable to other types of attacks. For example, virtual switches do not protect the physical network against these attacks, just the virtual network.

• **MAC flooding** – These attacks flood a switch with packets containing MAC addresses tagged as having come from different sources. Many switches use a Content-Addressable Memory (CAM) table to learn and store the source address for each packet. When the table is full, the switch may enter a fully open state in which every incoming packet is broadcast on all ports, letting the attacker see all the switch's traffic. This state might result in packet leakage across VLANs.

  While VMware virtual switches do store a MAC address table, they don’t get the MAC addresses from observable traffic and are not vulnerable to this type of attack.

• **802.1q and ISL tagging attacks** – These attacks force a switch to redirect frames from one VLAN to another by tricking the switch into acting as a trunk and broadcasting the traffic to other VLANs.

  VMware virtual switches don’t perform the dynamic trunking required for this type of attack and, therefore, are not vulnerable.

• **Double-encapsulation attacks** – These attacks occur when an attacker creates a double-encapsulated packet in which the VLAN identifier in the inner tag is different from the VLAN identifier in the outer tag. For backward compatibility, native VLANs strip the outer tag from transmitted packets unless configured to do otherwise. When a native VLAN switch strips the outer tag, only the inner tag
is left, and that inner tag routes the packet to a different VLAN than the one identified in the now-missing outer tag.

VMware virtual switches drop any double-encapsulated frames that a virtual machine attempts to send on a port configured for a specific VLAN. Therefore, they are not vulnerable to this type of attack.

- **Multicast brute-force attacks** – These attacks involve sending large numbers of multicast frames to a known VLAN almost simultaneously in hopes of overloading the switch so that it mistakenly allows some of the frames to broadcast to other VLANs.

  VMware virtual switches do not allow frames to leave their correct broadcast domain (VLAN) and are not vulnerable to this type of attack.

- **Spanning-tree attacks** – These attacks target Spanning-Tree Protocol (STP), which is used to control bridging between parts of the LAN. The attacker sends Bridge Protocol Data Unit (BPDU) packets that attempt to change the network topology, establishing himself or herself as the root bridge. As the root bridge, the attacker can sniff the contents of transmitted frames.

  VMware virtual switches don’t support STP and are not vulnerable to this type of attack.

- **Random frame attacks** – These attacks involve sending large numbers of packets in which the source and destination addresses stay the same, but fields are randomly changed in length, type, or content. The goal of this attack is to force packets to be mistakenly rerouted to a different VLAN.

  VMware virtual switches are not vulnerable to this type of attack.

Because new security threats develop over time, you should not consider this an exhaustive list of attacks. Always regularly check VMware security resources on the Web (http://www.vmware.com/vmtn/technology/security) to learn about security, recent security alerts, and VMware security tactics.
Securing Virtual Switch Ports

As with physical network adapters, a virtual network adapter can send frames that appear to be from a different machine and impersonate another machine such that it is able to receive network frames intended for that machine. Also, like physical network adapters, a virtual network adapter can be configured such that it receives frames targeted for other machines.

When you create a virtual switch for your network, you add port groups to impose a policy configuration for the virtual machines, storage systems, and so forth attached to the switch. You create virtual switches through the VI Client.

As part of adding a port or port group to a virtual switch, the VI Client configures a security profile for the port. You can use this security profile to ensure that ESX Server prevents the guest operating systems for its virtual machines from impersonating other machines on the network. This security feature is implemented so that the guest operating system responsible for the impersonation is not aware that the impersonation has been prevented.

The security profile determines how strongly you enforce protection against impersonation and interception attacks on virtual machines. To correctly use the settings in the security profile, you need to understand the basics of how virtual network adapters control transmissions and how attacks are staged at this level.

Each virtual network adapter has its own MAC address assigned when the adapter is created. This address is called the initial MAC address. Although the MAC address can be reconfigured from outside the guest operating system, it cannot be changed by the guest operating system. In addition, each adapter has an effective MAC address that filters out incoming network traffic with a destination MAC address different from the effective MAC address. The guest operating system is responsible for settings the effective MAC address and typically matches the effective MAC address to the initial MAC address.

When sending packets, an operating system places its own network adapter’s initial MAC address in the source MAC address field of the Ethernet frame. It also places the MAC address for the receiving network adapter in the destination MAC address field. The receiving adapter accepts packets only when the destination MAC address in the packet matches its own effective MAC address.

At creation time, a network adapter’s effective MAC address and initial MAC address are the same. However, the operating system for a virtual machine can change the effective MAC address to another value at any time. If an operating system changes the effective MAC address, its network adapter then receives network traffic destined
for the new MAC address. The operating system can send frames with an impersonated source MAC address at any time. Thus, an operating system can stage malicious attacks on the devices in a network by impersonating a network adapter authorized by the receiving network.

You can use virtual switch security profiles on ESX Server hosts protect against this type of attack by setting three options:

- **MAC address changes** – By default, this option is set to **Accept**, meaning that the ESX Server host accepts requests to change the effective MAC address to other than the initial MAC address.

  To protect against MAC impersonation, you can set this option to **Reject**. If you do, the ESX Server host does not honor requests to change the effective MAC address to anything other than the initial MAC address. Instead, the port that the virtual adapter used to send the request is disabled. As a result, the virtual adapter does not receive any more frames until it changes the effective MAC address to match the initial MAC address.

  The guest operating system is unaware that the MAC address change has not been honored. Whenever it sends frames using the impersonated address, the ESX Server adapter intercepts these frames before they are delivered, and the guest operating system might assume that its frames have been dropped.

  **Note:** In some situations, you might have a legitimate need for more than one adapter to have the same MAC address on a network—for example, if you are using Microsoft Network Load Balancing in unicast mode. Note that when Microsoft Network Load Balancing is used in the standard multicast mode, adapters do not share MAC addresses.

- **Forged transmissions** – By default, this option is set to **Accept**, meaning the ESX Server host does not compare source and effective MAC addresses.

  To protect against MAC impersonation, you can set this option to **Reject**. If you do, the ESX Server host compares the source MAC address being transmitted by the operating system with the effective MAC address for its adapter to see if they match. If the addresses don’t match, ESX Server prevents the operating system from sending the packet.

  The guest operating system is unaware that its virtual network adapter cannot send packets using the impersonated MAC address. The ESX Server host intercepts any packets with impersonated addresses before they are delivered, and the guest operating system might assume that the packets have been dropped.
- **Promiscuous mode operation** – By default, this option is set to Reject, meaning that the virtual network adapter cannot operate in promiscuous mode. Promiscuous mode eliminates any transmission filtering that the virtual network adapter would perform so that every frame that the guest operating system receives all traffic observed on the wire.

  While promiscuous mode can be useful for tracking network activity, it is an insecure mode of operation because any adapter in promiscuous mode had access to the packets regardless of whether some of the packets should be received only by a particular network adapter. This means that an administrator or root user within a virtual machine can potentially view traffic destined for other guest or host operating systems.

  **Note**: In some situations, you might have a legitimate need to configure a virtual switch to operate in promiscuous mode—for example, if you are running network intrusion detection software or a packet sniffer.

  If you need to change any of these default settings for a port, you must modify the security profile by editing virtual switch settings in the VI Client. For information on editing these settings, see Virtual Switch Policies on page 54.
Securing iSCSI Storage

The storage you configure for an ESX Server host might include one or more storage area networks (SANs) that use iSCSI. Simply stated, iSCSI is a means of accessing SCSI devices and exchanging data records using TCP/IP protocol over a network port rather than through a direct connection to a SCSI device. In iSCSI transactions, blocks of raw SCSI data are encapsulated in iSCSI records and transmitted to the requesting device or user.

iSCSI SANs let you make efficient use of existing Ethernet infrastructures to provide ESX Server hosts access to storage resources that they can dynamically share. As such, iSCSI SANs provide an economical storage solution for environments that rely on a common storage pool to serve numerous users. As with any networked system, your iSCSI SANs can be subject to security breaches. When you configure iSCSI on an ESX Server host, you can take several measures to minimize security risks.

Note: The requirements and procedures for securing an iSCSI SAN are similar for the hardware iSCSI adapters you can use with ESX Server hosts and for iSCSI configured directly through the ESX Server host. For information on configuring iSCSI adapters and storage, see iSCSI Storage on page 103.

The following section tells you how to configure authentication for iSCSI SANs and provides suggestions for securing iSCSI SANs. The section covers the following topics:

- Securing iSCSI Devices Through Authentication on page 197
- Protecting an iSCSI SAN on page 201

Securing iSCSI Devices Through Authentication

One means of securing iSCSI devices from unwanted intrusion is to require that the ESX Server host, or initiator, be authenticated by the iSCSI device, or target, whenever the host attempts to access data on the target LUN. The goal of authentication is to prove that the initiator has the right to access a target, a right granted when you configure authentication.

You have two choices when setting up authentication for iSCSI SANs on the ESX Server host:

- **Challenge Handshake Authentication Protocol (CHAP)** – You can configure the iSCSI SAN to use CHAP authentication. In CHAP authentication, when the initiator contacts an iSCSI target, the target sends a predefined ID value and a random value, or key, to the initiator. The initiator then creates a one-way hash value that it sends to the target. The hash contains three elements: a predefined ID value, the random value sent by the target, and a private value, or CHAP secret,
shared by the initiator and target. When the target receives the hash from the
initiator, it creates its own hash value using the same elements and compares it
to the initiator’s hash. If the results match, the target authenticates the initiator.

ESX Server supports one-way CHAP authentication for iSCSI. In this form of
authentication, the target authenticates the initiator, but the initiator does not
authenticate the target. The initiator has only one set of credentials, and these
credentials are used by all the iSCSI targets.

ESX Server supports CHAP authentication at the HBA level only. It does not
support per-target CHAP authentication, which enables you to configure
different credentials for each target to achieve greater target refinement.

- **Disabled** – You can configure the iSCSI SAN to use no authentication. Be aware
  that communications between the initiator and target are still authenticated in a
  rudimentary way by virtue of the fact that the iSCSI target devices are typically
  set up to communicate with specific initiators only.

Choosing not to enforce more stringent authentication can make sense if your
iSCSI storage is all housed in one location and you create a dedicated network or
VLAN to service all your iSCSI devices. The premise here is that the iSCSI
configuration is secure because it is isolated from any unwanted access, much as
a Fibre Channel SAN would be.

As a basic rule, you should disable authentication only if you are willing to risk an
attack to the iSCSI SAN or cope with problems that result from human error.

ESX Server does not support Kerberos, Secure Remote Protocol (SRP), or public key
authentication methods for iSCSI. Additionally, it does not support IPsec
authentication and encryption.

You use the VI Client to determine whether authentication is currently being
performed and to configure the authentication method.

**To check the authentication method**

1. Log on to the VI Client and select the server from the inventory panel.
   The hardware configuration page for this server appears.

2. Click the **Configuration** tab and then click **Storage Adapter**.

3. Select the iSCSI adapter you want to check and then click **Properties** to open the
   iSCSI Initiator Properties dialog box.
4. Click **CHAP Authentication**. If **CHAP Name** shows a name—typically the CHAP initiator name, the iSCSI SAN is using CHAP authentication, as shown below.

![CHAP Authentication Dialog Box](image)

**Note:** If **CHAP Name** shows **Not Specified**, the iSCSI SAN is not using CHAP authentication.

5. Click **Close**.

**To configure iSCSI for CHAP authentication**

1. Log on to the VI Client and select the server from the inventory panel. The hardware configuration page for this server appears.
2. Click the **Configuration** tab and then click **Storage Adapter**.
3. Select the iSCSI adapter and then click **Properties** to open the iSCSI Initiator Properties dialog box.
4. Click **CHAP Authentication > Configure** to open the **CHAP Authentication** dialog box.
5. Click **Use the following CHAP credentials**.

![Image of CHAP Authentication dialog]

6. Perform one of the following actions:
   - If you want to set the CHAP name to the iSCSI adapter name, select **Use initiator name**.
     If you are using iqn names (iSCSI qualified names), the initiator name has the following format:
     
     \[ \text{iqn.<year-month>.com.<naming_authority>:<unique_name>} \]
     
     If you are using eui names (IEEE qualified names), the initiator name has the following format:
     
     \[ \text{eui:<16_place_value_assigned_by_ieee>} \]
   - If you want to set the CHAP name to anything other than the iSCSI adapter name, deselect **Use initiator name** and enter a name in the **CHAP Name** field.

7. Enter a CHAP secret to be used as part of authentication. The secret you enter is a text string.

   **Note:** The VI Client doesn’t impose a minimum or maximum length for the CHAP secret you enter. However, some iSCSI storage devices require that the secret exceed a minimum number of characters or have limitations on the character types you can use. Check the manufacturer’s documentation to determine the requirements.

8. Click **OK**.

**To disable iSCSI authentication**

1. Log on to the VI Client and select the server from the inventory panel.
   The hardware configuration page for this server appears.

2. Click the **Configuration** tab and then click **Storage Adapter**.
3. Select the iSCSI adapter and then click Properties to open the iSCSI Initiator Properties dialog box.

4. Click CHAP Authentication > Configure to open the CHAP Authentication dialog box. Then, select Disable CHAP authentication.

5. Click OK.

Protecting an iSCSI SAN

When planning your iSCSI configuration, you should take measures to improve the overall security of the iSCSI SAN. Be aware that your iSCSI configuration is only as secure as your IP network, so by enforcing good security standards when setting up your network, you help safeguard your iSCSI storage.

Here are some specific suggestions:

- Protecting transmitted data – A primary security risk in iSCSI SANs is that an attacker might sniff transmitted storage data.

  VMware recommends that you take additional measures to prevent attackers from easily seeing iSCSI data. Neither the hardware iSCSI adapter nor the ESX Server host iSCSI initiator encrypts the data they transmit to and from the targets, making the data more vulnerable to sniffing attacks.

  To help ensure that intruders can’t listen to iSCSI transmissions, you should make sure that none of your virtual machines can directly see the iSCSI storage array.
To do so, configure iSCSI storage through a different virtual switch than the one used by your virtual machines, as shown below:

If you place your virtual machines on the same virtual switch as your iSCSI configuration, your iSCSI traffic is potentially exposed to misuse by a virtual machine attacker.

In addition to protecting the iSCSI SAN by giving it a dedicated virtual switch, consider configuring your iSCSI SAN on its own VLAN. Placing your iSCSI configuration on a separate VLAN ensures that no devices other than the iSCSI adapter have visibility into transmissions within the iSCSI SAN. Using a separate VLAN for iSCSI can potentially improve performance because there is no interference or overhead from other types of network traffic.

- **Securing iSCSI ports** – When you run iSCSI devices, the ESX Server host opens only the ports it uses to communicate with the iSCSI SAN. This measure reduces the chances that an intruder can break into the ESX Server host through spare ports and gain control over the host. Therefore, running iSCSI doesn’t present any additional security risks at the ESX Server host end of the connection.

Be aware that any iSCSI target device that you run must have one or more open TCP ports used to listen for iSCSI connections. If any security vulnerabilities exist in the iSCSI device software, your data can be at risk through no fault of ESX Server. To lower this risk, you should install any security patches provided by your storage equipment manufacturer and limit the devices connected to the iSCSI network.
AUTHENTICATION AND USER MANAGEMENT

This chapter explains how ESX Server handles user authentication and shows you how to set up user and group permissions. In addition, it discusses encryption for connections to the VI Client, SDK, and VI Web Access as well as configuring a delegate user name for transactions with NFS storage.

This chapter covers the following topics:

- Securing ESX Server Through Authentication and Permissions on page 204
- Encryption and Security Certificates for ESX Server on page 219
- Configuring Virtual Machine Delegates on page 226
Securing ESX Server Through Authentication and Permissions

ESX Server uses the Pluggable Authentication Modules (PAM) structure for authentication when users access the ESX Server host using VirtualCenter, VI Web Access, or the service console. The PAM configuration for VMware services is located in /etc/pam.d/vmware-authd, which stores paths to authentication modules.

The default installation of ESX Server uses /etc/passwd authentication, just as Linux does, but you can configure ESX Server to use another distributed authentication mechanism. If you plan to use a third-party authentication tool instead of relying on the ESX Server default implementation, refer to the vendor documentation for instructions. As part of setting up third-party authentication, you might need to update the /etc/pam.d/vmware-authd file with new module information.

Every time a VI Client or VirtualCenter user connects to an ESX Server host, the xinetd process starts an instance of the VMware Authentication Daemon (vmware-authd), which is used as a proxy to pass the information to and from the VMware Host Agent (vmware-hostd) process. The vmware-authd process receives an incoming connection attempt and sends the user name and password returned by vmware-hostd, which forwards it to PAM to perform the authentication.
The following illustration gives you a basic idea of how ESX Server authenticates transactions from the VI Client.

The `vmware-authd` process exits as soon as a connection to a VMware process like `vmware-hostd` is established. Each virtual machine authentication process shuts down after the last user disconnects.

ESX Server transactions with VI Web Access and third-party network management clients interact directly with the `vmware-hostd` process during authentication. These management tools bypass the `vmware-authd` process.

To make sure that authentication works efficiently for your site, you might need to perform some basic tasks like setting up users, groups, permissions, and roles, configuring user attributes, adding your own certificates, determining whether you want to use SSL, and so forth. You can learn more about these issues and tasks in this section, which covers the following topics:

- About Users, Groups, Permissions, and Roles on page 206
- Working with Users and Groups on ESX Server Hosts on page 211
- Encryption and Security Certificates for ESX Server on page 219
- Configuring Virtual Machine Delegates on page 226
About Users, Groups, Permissions, and Roles

Access to an ESX Server host and its resources is granted when a known user with appropriate permissions logs on to the host with a password that matches the one stored for that user. VirtualCenter uses a similar approach when determining whether to grant access to a user. VirtualCenter and ESX Server hosts determine the level of access for the user based on the permissions assigned to the user. For example, one user might have permissions that enable him or her to create virtual machines on the host and another might have permissions that allow him or her to power on virtual machines but not create them.

The combination of user name, password, and permissions is the mechanism by which VirtualCenter and ESX Server hosts authenticate a user for access and authorize the user to perform activities. To support this mechanism, the VirtualCenter and ESX Server host maintain lists of authorized users, their passwords, and the permissions assigned to each user. VirtualCenter and ESX Server hosts deny access under the following circumstances:

- A user who is not in the user list attempts to log on.
- The user enters the wrong password.
- A user is in the list but has not been assigned permissions.
- A user who successfully logged on attempts operations that he or she does not have permission to perform.

As part of managing ESX Server hosts and VirtualCenter, you need to develop user and permission models, which are basic plans for how you want to handle particular types of users and how you want to design your permissions. In developing your user and permission models, be aware that:

- ESX Server and VirtualCenter use sets of privileges, or roles, to control which operations individual users or groups can perform. ESX Server and VirtualCenter provide you a set of pre-established roles, but you can also create new ones.
- You can manage users more easily by assigning them to groups. If you create groups, you can apply a role to the group, and this role is inherited by all the users in the group.

Understanding Users

A user is an individual authorized to log on to either an ESX Server host or to VirtualCenter. ESX Server users fall into two categories: those who can access the ESX Server host through VirtualCenter and those who can access the ESX Server host by
directly logging on to the host from the VI Client, VI Web Access, a third-party client, or a command shell. These two categories draw users from different sources.

- **VirtualCenter users** – Authorized users for VirtualCenter are those included in the Windows domain list referenced by VirtualCenter or are local Windows users on the VirtualCenter host.

  You cannot use VirtualCenter to manually create, remove, or otherwise change users. If you need to manipulate the user list or change user passwords, you must do so through the tools you normally use to manage your Windows domain. Any changes you make to the Windows domain are reflected in VirtualCenter. However, because you cannot directly manage users in VirtualCenter, the user interface doesn’t provide a user list for you to review. The only time you work with user and group lists is when you select users and groups during role assignment. You will notice these changes only when you select users in order to configure permissions.

- **Direct access users** – Users authorized to work directly on an ESX Server host are those added to the internal user list by default when ESX Server is installed or by a system administrator after installation.

  If you log on to the host as an administrator, you can perform a variety of management activities for these users, such as changing passwords, group memberships, permissions, and so forth. You can also add and remove users.

The user list maintained by VirtualCenter is completely separate from the user list maintained by the ESX Server host. Even if the lists maintained by a host and VirtualCenter appear to have common users (for instance, a user called devuser), these users should be treated as separate users who happen to have the same name. The attributes of devuser in VirtualCenter, including permissions, passwords, and so forth are separate from the attributes of devuser on the ESX Server host. Therefore, if you log on to VirtualCenter as devuser, you might have permission to view and delete files from a datastore, whereas if you log on to an ESX Server host as devuser, you might not.

Because of the confusion that duplicate naming can cause, VMware recommends that you check the VirtualCenter user list before you create ESX Server host users so that you can avoid creating host users that bear the same name as VirtualCenter users. You check for VirtualCenter users by reviewing the Windows domain list.

**Understanding Groups**

You can more efficiently manage some user attributes by creating groups. A group is a set of users that you want to manage through a common set of rules and permissions.
When you assign permissions to a group, they are inherited by all users in the group and you do not have to work with the user profiles one by one. Therefore, using groups can significantly reduce the time it takes to set up your permissions model and improve future scalability.

As an administrator, you need to decide how to structure groups to achieve your security and usage goals. For example, three part-time sales team members work different days, and you want them to share a single virtual machine but not use the virtual machines belonging to sales managers. In this case, you can create a group called SalesShare that includes the three sales people: Mary, John, and Tom. You can then give the SalesShare group permission to interact with only one object, Virtual Machine A. When you do so, Mary, John, and Tom inherit these permissions and are able to power up Virtual Machine A, start console sessions on Virtual Machine A, and so forth. They cannot perform these actions on the sales managers’ virtual machines: Virtual Machines B, C, and D.

The group lists in VirtualCenter and an ESX Server host are drawn from the same sources as their respective user lists are. If you are working through VirtualCenter, the group list is called from the Windows domain. If you are logged on to an ESX Server host directly, the group list is called from a table maintained by the host. All the recommendations for how you treat group lists are the same as those for user lists.

Understanding Permissions

For ESX Server and VirtualCenter, permissions are defined as access roles that consist of a user and the user’s assigned role for an object such as a virtual machine or ESX Server host. Permissions grant users the right to perform specific activities and manage specific objects on an ESX Server host or, if users are working from VirtualCenter, all VirtualCenter-managed objects. For example, to configure memory for an ESX Server host, you must have a permission that grants host configuration privileges.

Most VirtualCenter and ESX Server users have limited ability to manipulate the objects associated with the host. However, ESX Server provides full access rights and permissions on all virtual objects, such as datastores, hosts, virtual machines, and resource pools, to two users—root and, if the host is under VirtualCenter management, vpxuser.

- **root** – The root user can perform a complete range of control activities on the specific ESX Server host that he or she is logged on to, including manipulating permissions, creating groups and users, working with events, and so forth. A root user logged on to one ESX Server host cannot control the activities of any other host in the broader ESX Server deployment.
**Note:** By default, the root user has these abilities. After installation, you can change permissions such that the root user no longer has administrative privileges or you can delete the root user. However, if you do so, you must first create another user at the root level and then assign that user the Administrator role. Only then can you safely delete the root user or change its role to limit its privileges. If you delete the root user, you must use the new user you created as the host authentication point when you bring the host under VirtualCenter management. For more information on roles, see Understanding Roles on page 210.

Configuration commands that you run through the command line interface (e.g., `esxcfg` commands) do not perform an access check.

- **vpxuser** – This user is VirtualCenter acting as an entity with root rights on the ESX Server host, allowing it to manage activities for that host. vpxuser is created at the time that an ESX Server host is attached to VirtualCenter. It is not present on the ESX Server host unless the host is being managed through VirtualCenter.

  When an ESX Server host is managed through VirtualCenter, VirtualCenter has privileges on the host. For example, VirtualCenter can move virtual machines to and from hosts and perform configuration changes needed to support virtual machines.

  The VirtualCenter administrator, through vpxuser, can perform most of the same tasks on the host as the root user and also schedule tasks, work with templates, and so forth. However, there are certain activities you cannot perform as a VirtualCenter administrator. These activities, which include directly creating, deleting, or editing users and groups for ESX Server hosts, can be performed only by the root user directly on each ESX Server host.

  **Caution:** You should not change vpxuser in any way and you should not change its permissions. If you do so, you might experience problems in working with the ESX Server host through VirtualCenter.

  If you are acting as root, you can grant permissions on an ESX Server host to individual users or groups that have been added to the ESX Server user list and group list by default when ESX Server was installed or because they were manually added to the host after installation. If you are acting as vpxuser though VirtualCenter, you can grant permissions to any user or group included in the Windows domain list referenced by VirtualCenter.

  **Note:** VirtualCenter registers any selected Windows domain user or group through the process of assigning permissions. By default, all users who are members of the local Windows Administrators group on the VirtualCenter Server are granted the same
access rights as any user assigned to the Administrator role. Users who are members of the Administrators group can log on as individuals and have full access.

The method you use to configure permissions directly on an ESX Server host is identical to the method you use to configure permissions in VirtualCenter. Also, the list of privileges is the same for both ESX Server and VirtualCenter. For information on configuring permissions and to read about the privileges you can assign, see the Virtual Infrastructure User’s Guide.

Understanding Roles
VirtualCenter and ESX Server grant access to objects only to users who have been assigned permissions for the object. When you assign a user or group permissions for the object, you do so by pairing the user or group with a role. A role is a pre-defined set of privileges.

ESX Server hosts provide three default roles for you to use, and you cannot change the privileges associated with these roles. Each subsequent role includes the privileges of the previous role.

- **No Access User** – Users assigned this role for an object cannot view or change the object in any way. For example, a user who has a No Access role for a particular virtual machine cannot see the virtual machine in the VI Client inventory when he or she logs on to the ESX Server host. With a No Access role for a particular object, a user can select the VI Client tabs associated with the no-access object, but the tab displays no content. For example, if the user doesn’t have access to any virtual machines, he or she can select the Virtual Machines tab but won’t see a virtual machine listing on the tab or any status information—the table is blank.

  The No Access role is the default assigned to any user or group you create on an ESX Server host. You can elevate or lower a newly created user’s or group’s role on an object-by-object basis.

  **Note:** The root user and vpxuser are the only users not assigned the No Access role by default. Instead, they are assigned the Administrator role. Do not change the role for these users.

You can delete the root user provided that you first create a replacement permission at the root level with the Administrator role and assign this permission to another user. If you delete the root user, you must use the new user you created as the host authentication point when you bring the host under VirtualCenter management.
• **Read Only User** – Users assigned this role for an object are allowed to view the state of the object and details about the object.

  With this role, a user can view virtual machine, host, and resource pool attributes. The user cannot view the remote console for a host. All actions through the menus and toolbars are disallowed.

• **Administrator** – Users assigned this role for an object are allowed to view and perform all actions on the object. This role also includes all permissions inherent in the Read Only role.

You can create custom roles by using the role-editing facilities in the VI Client to create privilege sets that match your user needs. If you use the VI Client connected to VirtualCenter to manage your ESX Server hosts, you have additional roles to choose from in VirtualCenter. Also, the roles you create directly on an ESX Server host are not accessible within VirtualCenter. You can work with these roles only if you log on to the host directly from the VI Client.

If you manage ESX Server hosts through VirtualCenter, be aware that maintaining custom roles in both the host and VirtualCenter can result in confusion and misuse. In this type of configuration, VMware recommends that you maintain custom roles only in VirtualCenter. For information on creating, altering, and deleting roles as well as a discussion of additional roles available in VirtualCenter, see *Virtual Infrastructure User’s Guide*.

**Working with Users and Groups on ESX Server Hosts**

If you are directly connected to an ESX Server host through the VI Client, you can create, edit, and delete users and groups. These users and groups are visible in the VI Client whenever you log on to the ESX Server host but are not available if you log on to VirtualCenter.

The following section explains how to work with users and groups in the VI Client directly connected to an ESX Server host. The section covers basic tasks you can perform for users and groups, such as viewing and sorting information and exporting reports. It also shows you how to create, delete, and edit users and groups.

**Note:** You can also create roles and set permissions through a direct connection to the ESX Server host. But because these tasks are more widely performed in VirtualCenter, see the *Virtual Infrastructure User’s Guide* for information on working with permissions and roles.
Viewing and Exporting Users and Group Information

You work with users and groups through the Users & Groups tab in the VI Client. This tab displays a Users table or Groups table depending on whether you click the Users button or Group button.

The following illustration shows the Users table. The Groups table is similar.

You can sort the lists according to column, show and hide columns, and export the list in formats you can use when preparing reports or publishing user or group lists on the Web.

To view and sort ESX Server users or groups

1. Log on to the VI Client through the ESX Server host.
2. Select the server from the inventory panel.
   The hardware configuration page for this server appears.
3. Click the Users & Groups tab and then click Users or Groups.
4. Perform any of these actions as appropriate:
   - To sort the table by any of the columns, click the column heading.
   - To show or hide columns, right-click any of the column headings and deselect or select the name of the column you want to hide.

To export data in the ESX Server Users or Groups table

1. Log on to the VI Client through the ESX Server host.
2. Select the server from the inventory panel.
   The hardware configuration page for this server appears.
3. Click the Users & Groups tab and then click Users or Groups.
4. Determine how you want the table sorted, and hide or show columns according to the information you want to see in the exported file.
5. Right-click anywhere in the user table and then click Export to open the Save As dialog box.
6. Select a path and enter a filename.
7. Select the file type. You can export the user or group table in any of the following formats:
   • HTML (plain HTML or HTML formatted for use with a CSS style sheet)
   • XML
   • Microsoft Excel
   • CSV (Comma Separated Values)
8. Click OK.

Working with the Users Table
You can add users to the Users table for an ESX Server host, remove users, and change various user attributes such as password and group memberships. When you perform these activities, you are altering the internal user list maintained by the ESX Server host.

To add a user to the ESX Server Users table
1. Log on to the VI Client through the ESX Server host.
2. Select the server from the inventory panel.
   The hardware configuration page for this server appears.
3. Click the Users & Groups tab and then click Users.
4. Right-click anywhere in the **Users** table and then click **Add** to open the **Add New User** dialog box.

![Add New User dialog box](image)

5. Enter a login, a user name (optional), and a password. The password should meet the length and complexity requirements outlined in **Password Restrictions on page 238**.

6. If you want the user to be able to access the ESX Server host through a command shell, select **Grant shell access to this user**.

   **Note:** In general, you should not grant shell access to ESX Server host users unless you determine that they have a justifiable need to access the host through a shell rather than through the VI Client. Users that access the host only through the VI Client do not need shell access.

7. For each existing group you want the user to be part of, enter the group name and click **Add**.

   **Note:** If you type a nonexistent group name, the VI Client warns you and does not add the group to the **Group membership** list.
8. Click OK.

The login and user name you entered now appear in the Users table. The VI Client assigns the next available user ID to the user.

To modify the settings for a user
1. Log on to the VI Client through the ESX Server host.
2. Select the server from the inventory panel.
   The hardware configuration page for this server appears.
3. Click the Users & Groups tab and then click Users.
4. Right-click anywhere in the Users table and then click Edit to open the Edit User dialog box.

5. If you want to change the user ID, enter a numeric user ID in the UID field.

   Note: The VI Client assigns the next available user ID when you first create the user. In most cases, this assignment doesn't need to be changed. You typically
change the user ID only when you create a delegate user for NFS storage access. For more information, see Configuring Virtual Machine Delegates on page 226.

6. Enter a new user name.

7. To change the user's password, select Change Password and enter the new password.

8. To add the user to another group, enter the group name and click Add.  
   Note: If you type a nonexistent group name, the VI Client warns you and does not add the group to the Group membership list.

9. To remove the user from a group, select the group name from the list and click Remove.

10. Click OK.

To remove a user from the ESX Server Users table

1. Log on to the VI Client through the ESX Server host.

2. Select the server from the inventory panel.  
   The hardware configuration page for this server appears.

3. Click the Users & Groups tab and then click Users.

4. Right-click the user you want to remove and then click Remove.

Working with the Groups Table

You can add groups to the Groups table for an ESX Server host, remove groups, and add or remove group members. When you perform these activities, you are altering the internal group list maintained by the ESX Server host.

To add a group to the ESX Server Groups table

1. Log on to the VI Client through the ESX Server host.

2. Select the server from the inventory panel.  
   The hardware configuration page for this server appears.

3. Click the Users & Groups tab and then click Groups.
4. Right-click anywhere in the Groups table and then click Add to open the Create New Group dialog box.

![Create New Group dialog box]

5. Enter a group name and numeric group ID.
   
   **Note:** If don’t specify a group ID, the VI Client assigns the next available group ID.

6. For each user that you want as a group member, enter the user name and click Add.
   
   **Note:** If you type a nonexistent user name, the VI Client warns you and does not add the user to the Users in this group list.

7. Click OK.

The group ID and group name you entered now appear in the Groups table.

**To add or remove users from a group**

1. Log on to the VI Client through the ESX Server host.
2. Select the server from the inventory panel.
   
   The hardware configuration page for this server appears.
3. Click the Users & Groups tab and then click Groups.
4. Right-click anywhere in the **Groups** table and then click **Properties** to open the **Edit Group** dialog box.

5. To add a user to the group, enter the user name and click **Add**.
   
   **Note:** If you type an nonexistent group name, the VI Client warns you and does not add the user to the **Users in this group** list.

6. To remove a user from the group, select the user name from the list and click **Remove**.

7. Click **OK**.

**To remove a group from the ESX Server Groups table**

1. Log on to the VI Client through the ESX Server host.
2. Select the server from the inventory panel.
   
   The hardware configuration page for this server appears.
3. Click the **Users & Groups** tab and then click **Groups**.
4. Right-click the group you want to remove and then click **Remove**.
CHAPTER 10 Authentication and User Management

Encryption and Security Certificates for ESX Server

All network traffic including user names passwords sent to an ESX Server host over a network connection from VirtualCenter or VI Web Access pass through port 902 or 443, respectively, and are encrypted in ESX Server by default as long as the following conditions are true:

- SSL is enabled.
- You have not changed the Web proxy service to allow unencrypted traffic for the port.
- Your service console firewall is configured for medium or high security. For information on configuring the service console firewall, see Service Console Firewall Configuration on page 234.

Caution: If you disable your firewall by configuring it for low security, users can access the ESX Server host through port 8080, an insecure port. Anyone who connects to the ESX Server host through port 8080 using an authorized user name and password has free access to the services on the host.

Security certificates used for encryption are created by ESX Server and stored on the host. The certificates used to secure your VirtualCenter and VI Web Access sessions are not signed by a trusted certificate authority and, therefore, do not provide the authentication security you might need in a production environment. If you intend to use encrypted remote connections externally, consider purchasing a certificate from a trusted certificate authority or, if you prefer, use your own security certificate for your SSL connections.

The default location for your certificate is /etc/vmware/ssl/ on the ESX Server host. The certificate consists of two files: the certificate itself (rui.crt) and the private key file (rui.key). The private key file should be readable only by the root user (permission setting of 0400). The certificate file should be readable by the root user and group (permission setting of 0440).

In adding certificates for ESX Server and thinking about encryption and user security, be aware of the following:

- ESX Server doesn’t handle pass phrases, also known as encrypted keys. If you set up a pass phrase, ESX Server processes will be unable to start correctly, so avoid setting up certificates using pass phrases.
• You can configure the Web proxy so that it searches for certificates in a location other than the default location. This capability proves useful for companies that prefer to centralize their certificates on a single machine so the certificates can be used by multiple hosts.

  **Caution:** If you store certificates in a location other the ESX Server host, you will be unable to use the certificates if the host loses network connectivity with the machine storing the certificates.

• To support encryption for user names, passwords, and packets, SSL is enabled by default for VI Web Access and Web SDK connections. If you want to configure the these connections so that they don’t encrypt transmissions, disable SSL as described in To disable SSL for VI Web Access and Web SDK connections to ESX Server on page 221. You should consider disabling SSL only if you have created a fully trusted environment for the se clients, meaning that firewalls are in place and transmissions to and from the host are fully isolated. Disabling SSL can improve performance for VI Web Access because you avoid the overhead required to perform encryption.

• To protect against misuse of ESX Server services such as the internal Web server that hosts VI Web Access, most internal ESX Server services are accessible only through port 443, the port used for HTTPS transmission. Port 443 acts as a reverse proxy for ESX Server. You can see a list of services on ESX Server through an HTTP welcome page, but you can’t directly access these services without proper authorization. You can change this configuration such that individual services are directly accessible through HTTP connections. VMware recommends that you not make this change unless you are using ESX Server in a fully trusted environment.

• When you upgrade VirtualCenter and VI Web Access, the certificate remains in place. If you remove VirtualCenter and VI Web Access, the certificate directory is not removed from the service console.

**To configure the Web proxy to search for certificates in nondefault locations**

1. Log on to the service console as the root user.
2. Change directories to `/etc/vmware/hostd/`. 
3. Use nano or another text editor to open the config.xml file and find the following XML segment:

```xml
<ssl>
  <!-- The server private key file -->
  <privateKey>/etc/vmware/ssl/rui.key</privateKey>
  <!-- The server side certificate file -->
  <certificate>/etc/vmware/ssl/rui.crt</certificate>
</ssl>
```

4. Replace `/etc/vmware/ssl/rui.key` with the absolute path to the private key file that you received from your trusted certificate authority. This path can be on the ESX Server host or on a centralized machine on which you store certificates and keys for your company.

**Note:** Leave the `<privateKey>` and `</privateKey>` XML tags in place.

5. Replace `/etc/vmware/ssl/rui.crt` with the absolute path to the certificate file that you received from your trusted certificate authority.

**Caution:** Do not delete the original `rui.key` and `rui.crt` files. These files are used by the ESX Server host.

6. Save your changes and close the file.

7. Enter the following command to restart the `vmware-hostd` process:

```
    service mgmt-vmware restart
```

To disable SSL for VI Web Access and Web SDK connections to ESX Server

1. Log on to the service console as the root user.
2. Change directories to `/etc/vmware/hostd/`.
3. Use nano or another text editor to open the config.xml file and find the following XML segment:

```xml
<ssl>
  <!-- The server private key file -->
  <privateKey>/etc/vmware/ssl/rui.key</privateKey>
  <!-- The server side certificate file -->
  <certificate>/etc/vmware/ssl/rui.crt</certificate>
</ssl>
```

4. Delete the entire segment from the file.

5. Save your changes and close the file.

6. Enter the following command to restart the `vmware-hostd` process:

```
    service mgmt-vmware restart
```
To change security settings for a Web proxy service

1. Log on to the service console as the root user.
2. Change directories to `/etc/vmware/hostd/`.
3. Use nano or another text editor to open the `config.xml` file and find the following XML segment:

```xml
<proxysvc>
  <path>/usr/lib/vmware/hostd/libproxysvc.so</path>
  <http>
    <port>80</port>
    <proxyDatabase>
      <server id="0">
        <namespace> / </namespace>
        <host> localhost </host>
        <port> 9080 </port>
      </server>
      <redirect id="0"> /ui </redirect>
      <redirect id="1"> /mob </redirect>
      <redirect id="2"> /sdk </redirect>
    </proxyDatabase>
  </http>
  <https>
    <port>443</port>
    <proxyDatabase>
      <server id="0">
        <namespace> / </namespace>
        <host> localhost </host>
        <port> 9080 </port>
      </server>
      <server id="1">
        <namespace> /sdk </namespace>
        <host> localhost </host>
        <port> 8085 </port>
      </server>
      <server id="2">
        <namespace> /ui </namespace>
        <host> localhost </host>
        <port> 8080 </port>
      </server>
      <server id="3">
        <namespace>/mob</namespace>
      </server>
    </proxyDatabase>
  </https>
</proxysvc>
```
4. For every HTTPS service that you want to access using HTTP, move the following segment up to the HTTP area:

```xml
<server id="id_number">
  <namespace>service_domain</namespace>
  <host>localhost</host>
  <port>port_number</port>
</server>
```

Where:
- `id_number` is an ID number for the server ID XML tag. ID numbers should be unique within the HTTP area.
- `service_domain` is the name of the service you are moving, for example `/sdk` or `/mob`.
- `port_number` is the port number assigned to the service. You can assign a different port number to the service if you want.

5. In the HTTP section, remove the redirect statement for the service you are moving.

6. Save your changes and close the file.

7. Enter the following command to restart the `vmware-hostd` process:

   ```bash
   service mgmt-vmware restart
   ```

If you want to move an HTTP service to the HTTPS section, the procedure is similar, except that you need to add a redirect statement to the HTTP section after you move the service. You can place the new redirect statement after the other redirect statements and use a unique number as the ID number for the redirect tag.
**Example:** Setting up VI Web Access to communicate through an insecure port

VI Web Access normally communicates with an ESX Server host through a secure port (HTTPS, 443). If you are in a fully trusted environment, you might decide that you can use an insecure port (for example, HTTP, 80). To do so, you change the proxy services area of the `/etc/vmware/hostd/config.xml` file as described in the procedure. The result is as follows, with changed and moved areas shown in bold. Note that the server segment for `/ui` (the VI Web Access service) is moved to the HTTP section and the redirect statement for `/ui` has been removed.

```xml
<proxysvc>
  <path>/usr/lib/vmware/hostd/libproxysvc.so</path>
  <http>
    <port>80</port>
    <proxyDatabase>
      <server id="0">
        <namespace> / </namespace>
        <host> localhost </host>
        <port> 9080 </port>
      </server>
      <server id="1">
        <namespace> /ui </namespace>
        <host> localhost </host>
        <port> 8080 </port>
      </server>
      <redirect id="0"> /mob </redirect>
      <redirect id="1"> /sdk </redirect>
    </proxyDatabase>
  </http>
  <https>
    <port>443</port>
    <proxyDatabase>
      <server id="0">
        <namespace> / </namespace>
        <host> localhost </host>
        <port> 9080 </port>
      </server>
      <server id="1">
        <namespace> /sdk </namespace>
        <host> localhost </host>
        <port> 8085 </port>
      </server>
    </proxyDatabase>
  </https>
</proxysvc>
```
<namespace>/mob</namespace>
<host>localhost</host>
<port>8087</port>
</server>
</proxyDatabase>
</https>
</proxysvc>
Configuring Virtual Machine Delegates

To perform most activities on virtual machines, an ESX Server needs access to virtual machine files. For instance, to power on and off virtual machines the ESX Server must be able to create, manipulate, and delete files on the volume that is storing the virtual disk files.

If you are creating, configuring, or administering virtual machines on an NFS datastore you may need to modify a special user, known as the delegate user. The delegate user’s identity is used by the ESX Server for all IO issued to the underlying file system. By default, the delegate user for the ESX Server host is root. However, for the ESX Server host to perform file level operations, the directory configured as the NFS datastore must be owned by the delegate user, or the identity of the delegate user must be change to match the owner of the directory. In the latter case, you need to ask the NFS administrator for the delegate user name. You can then change the delegate user setting for the ESX Server host to match the owner of the directory, enabling NFS datastore to recognize the ESX Server host correctly. The delegate user is configured globally, and the same identity is used to access to every volume. Leaving the delegate user as root may not work for all NFS datastores. NFS administrators may export volumes with root squashing enabled. The root squash feature maps root to a user with no significant privileges on the NFS server, limiting the root user’s abilities. This feature is commonly used to prevent unauthorized access to files on an NFS volume. Therefore, if you keep root as the delegate user, the NFS system might refuse access to the ESX Server host because the NFS system invokes root squashing, therefore preventing access.

Setting up the delegate user on an ESX Server host requires that you complete these activities:

- From the Users & Groups tab for a VI Client running directly on the ESX Server host, add a user with the delegate user name and UID. For information on adding users, see Working with the Users Table on page 213.
- Configure a virtual machine delegate as part of the security profile for the host, as described in the procedure that follows.

To configure a virtual machine delegate

1. Log on to the VI Client through the ESX Server host.
2. Select the server from the inventory panel.
   The hardware configuration page for this server appears with the Summary tab displayed.
3. Click Enter Maintenance Mode.
4. Click the Configuration tab and then click Security Profile.
5. Click Virtual Machine Delegate > Edit to open the Virtual Machine Delegate dialog box.

![Virtual Machine Delegate Dialog Box]

6. Enter the user name for the delegate user.
7. Click OK.
8. Reboot the ESX Server host.

After you reboot the host, the delegate user setting is visible in both VirtualCenter and the VI Client running directly on the ESX Server host.
This chapter makes basic security recommendations for using the service console and explains some of the service console’s built-in security features. The service console is a management interface to ESX Server and, as such, its security is critical. To protect the service console against unauthorized intrusion and misuse, VMware imposes constraints on several service console parameters, settings, and activities.

These constraints are designed to raise the security level for ESX Server. You can loosen them to meet your particular configuration needs, but if you do so, make sure you are working in a trusted environment and have taken enough other security measures to protect the network as a whole and the devices connected to the ESX Server host.

This chapter covers the following topics:

- General Security Recommendations on page 231
- Service Console Firewall Configuration on page 234
- Password Restrictions on page 238
- Cipher Strength on page 246
- setuid and setgid Applications on page 247
- SSH Security on page 250
- Security Patches and Security Vulnerability Scanning Software on page 252
General Security Recommendations

Consider the following recommendations when evaluating service console security and administering the service console:

- **Install antivirus software.**
  
  Even though you can run an ESX Server host without connecting the service console to any network, most implementations allow network access to the service console. Because the service console is a full operating system, you should protect it from viruses, just as you would a standard operating system or virtual machine at your site. If you’re already using Linux antivirus software in your organization, you can install the same antivirus software on the service console. You can also install third-party intrusion and root kit detection software such as Tripwire.

  **Note:** Antivirus software can affect performance. If you are confident that the ESX Server host is operating in a fully trusted environment, you can balance the need for this security measure against performance costs.

- **Limit user access.**
  
  To improve security, restrict user access to the service console and enforce access security policies like setting up password restrictions—for example, character length, password aging limits, and use of a `grub` password for booting the host.

  The service console has privileged access to certain parts of ESX Server. Therefore, only trusted users should be provided logon access. By default, root access is limited by not allowing secure shell (SSH) logon as root, and you should strongly consider keeping this default. ESX Server system administrators should be required to log on as regular users and then use `sudo` to perform specific tasks that require root privileges.

  Also, try to run as few processes on the service console as possible. Ideally, you should strive to run only the processes, services, and agents that you absolutely need such as virus checkers, virtual machine backups, and so forth.
- **Use VI Client to administer your ESX Server hosts.**
  Whenever possible, use VI Client, VI Web Access, or a third-party network management tool to administer your ESX Server hosts instead of working though the command line interface as root. Using VI Client lets you limit the accounts with access to the service console, safely delegate responsibilities, and set up roles that prevent administrators and users from using capabilities they don’t need.

- **Use only VMware sources to upgrade ESX Server components you run on the service console.**
  The service console runs a variety of third-party packages such as the Tomcat Web service to support management interfaces or tasks that you need to perform. VMware does not support upgrading these packages from anything other than a VMware source. If you use a download or patch from another source, you might compromise service console security or functions. Also, regularly check third-party vendor sites and the VMware knowledge base for security alerts.
CHAPTER 11 Service Console Security

Logging on to the Service Console

Although you perform most ESX Server configuration activities through the VI Client, you use the service console command-line interface when configuring certain security features. Using the command line interface requires that you log on to the host. If you have direct access to the ESX Server host, you can log on to the physical console on that machine. To do so, press Alt-F2 to open the login screen. For remote connections, use SSH or another remote console connection to start a session on the host.

Whether you access the service console locally or through a remote connection such as SSH, you must log on using a user name and password recognized by the ESX Server host. For information on user names and passwords for ESX Server hosts, see Working with Users and Groups on ESX Server Hosts on page 211.

If you are logging onto the host to perform activities that require root privileges, you should log on to the service console as a recognized user and acquire root privileges through the `su` command or, preferably, the `sudo` command. The `sudo` command enhances security because it grants root privileges only for select activities in contrast to the `su` command, which grants root privileges for all activities. Using `sudo` also provides superior accountability because all `sudo` activities are logged, whereas if you use `su`, ESX Server only logs the fact that the user switched to `su`.

In addition to ESX-specific commands, you can use the service console command-line interface to execute many Linux and Unix commands. For detailed usage notes on service console commands, use the `man <command_name>` command to check for man pages.
Service Console Firewall Configuration

ESX Server includes a firewall between the service console and the network. To ensure the integrity of the service console, VMware has reduced the number of firewall ports that are open by default. At installation time, the service console firewall is configured to block all incoming and outgoing traffic except for that on ports 902, 80, 443, and 22, which are used for basic communication with ESX Server. This setting enforces a high level of security for your ESX Server host.

Note: The firewall also allows Internet Control Message Protocol (ICMP) pings and communication with DHCP and DNS (UDP only) clients.

In trusted environments, you might decide that a lower security level is acceptable. If so, you can set the firewall for either medium or low security:

- **Medium security** – All incoming traffic is blocked except on the default ports (902, 433, 80, and 22) and any ports you specifically open. Outgoing traffic is not blocked.

- **Low security** – There are no blocks on either incoming or outgoing traffic. This setting is equivalent to removing the firewall.

Because the ports open by default are strictly limited, you might need to open additional ports after installation. For a list of commonly used ports you might need to open, see TCP and UDP Ports for Management Access on page 180.

Be aware that as you add the supported services and management agents required to operate ESX Server effectively, you open other ports in the service console firewall. You add services and management agents through VirtualCenter as described in Opening Firewall Ports for Supported Services and Management Agents on page 185.

In addition to the ports you open for these services and agents, you might need to open other ports when you configure certain devices, services, or agents such as storage devices, backup agents, and management agents. For example, if you are using Veritas NetBackup™ 4.5 as a backup agent, you need to open ports 13720, 13724, 13782, and 13783, which NetBackup uses for client-media transactions, database backups, user backups or restores, and so forth. Refer to vendor specifications for the device, service, or agent to determine which ports to open.

The following discussion tells you how to change the service console security level and open ports for additional devices, services, and agents.

Note: Each time you lower your security setting or open additional ports, you increase the risk of intrusion in your network. You should balance your access needs against how tightly you want to control the security of the network.
Changing the Service Console Security Level

Altering the security level for the service console is a two-part process: determining the virtual firewall security level and resetting the virtual firewall setting. To prevent unnecessary steps, always check the firewall setting before changing it.

To determine the service console firewall security level

1. Log on to the service console and acquire root privileges.
2. Execute these two commands to determine whether incoming and outgoing traffic is blocked or allowed:
   ```
esxcfg-firewall -q incoming
esxcfg-firewall -q outgoing
   ```
3. Interpret the results as follows:

<table>
<thead>
<tr>
<th>Command Line Response</th>
<th>Security Level</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming ports blocked by default.</td>
<td>High</td>
</tr>
<tr>
<td>Outgoing ports blocked by default.</td>
<td>Medium</td>
</tr>
<tr>
<td>Incoming ports not blocked by default.</td>
<td>Low</td>
</tr>
<tr>
<td>Outgoing ports not blocked by default.</td>
<td></td>
</tr>
</tbody>
</table>

To set the service console firewall security level

1. Log on to the service console and acquire root privileges.
2. Execute one of the following commands as applicable:
   - To set the service console firewall to medium security:
     ```
esxcfg-firewall --allowOutgoing
     ```
   - To set the virtual firewall to low security:
     ```
esxcfg-firewall --allowIncoming --allowOutgoing
     ```
     **Caution:** Using the above command disables all firewall protection.
   - To return the service console firewall to high security:
     ```
esxcfg-firewall --blockIncoming --blockOutgoing
     ```
3. Execute the following command to restart the `vmware-hostd` process:
   ```
   service mgmt-vmware restart
   ```
Changing the service console firewall security level does not affect existing connections. For example, if the firewall is set to low security and a backup is running on a port you didn't explicitly open, raising the firewall setting to high does not terminate the backup. Rather, the backup completes, releases the connection, and the port closes.

**Opening and Closing Ports in the Service Console Firewall**

You can open service console firewall ports when you install third-party devices, services, and agents. Before you open ports to support the item you are installing, refer to vendor specifications to determine the necessary ports.

If you close a port, active sessions of the service associated with the port are not automatically disconnected when you close the port. For example, if a backup is executing and you close the port for the backup agent, the backup continues until it completes and the agent releases the connection.

Perform the following procedures only if you are opening or closing ports for services or agents not specifically configurable through the VI Client. For information on configuring additional ports in VirtualCenter, see Opening Firewall Ports for Supported Services and Management Agents on page 185.

To open a specific port in the service console firewall

1. Log on to the service console and acquire root privileges.
2. Execute this command:
   ```bash
   esxcfg-firewall --openPort <port_number>,tcp<udp,in|out,<port_name>
   ```
   Where:
   - `port_number` is the vendor-specified port number.
   - `tcp|udp` is the protocol. Select `tcp` for TCP traffic or `udp` for UDP traffic.
   - `in|out` is the traffic direction. Select `in` to open the port for inbound traffic or `out` to open it for outbound traffic.
   - `port_name` is a descriptive name. The name does not need to be unique, but it should be meaningful to help identify the service or agent using the port.
   
   For example:
   ```bash
   esxcfg-firewall --openPort 6380,tcp,in,Navisphere
   ```
3. Execute the following command to restart the `vmware-hostd` process:
   ```bash
   service mgmt-vmware restart
   ```
To close a specific port in the service console firewall

1. Log on to the service console and acquire root privileges.
2. Execute this command:
   ```
   esxcfg-firewall -closePort <port_number>,tcp|udp,in|out,<port_name>
   ```
   The `port_name` argument is optional for `-closePort`.
   For example:
   ```
   esxcfg-firewall --closePort 6380,tcp,in
   ```
3. Execute the following command to restart the `vmware-hostd` process:
   ```
   service mgmt-vmware restart
   ```
   You can only use the `-closePort` option to close ports that you opened with the `-openPort` option. If you used a different method to open the port, you need to use an equivalent method to close it. For example, you can close the SSH port (22) only by disabling the SSH Server incoming connection and SSH Client outgoing connection in the VI Client. For information on opening and closing ports through the VI Client, see Opening Firewall Ports for Supported Services and Management Agents on page 185.
Password Restrictions

The ease with which an attacker can log on to an ESX Server host depends on his or her ability to find a legitimate user name/password combination. A malicious user can obtain a password in a number of ways. For example, an attacker can sniff insecure network traffic, such as Telnet or FTP transmissions, for successful logon attempts.

Another common method is to crack the password by running a password generator. Password generators are useful for mounting various kinds of password attacks, including brute force attacks, in which the generator tries every character combination up to a certain password length, and dictionary attacks, in which the generator tries real words and simple mutations of real words.

Implementing restrictions that govern the length, character sets, and duration of passwords can make attacks initiated by a password generator far more difficult. The longer and more complex the password, the harder it is for an attacker to discover. The more often users have to change passwords, the more difficult it is to find a password that works repeatedly.

To help protect your password database from misuse, password shadowing is enabled for ESX Server so that password hashes are hidden from access. Also, ESX Server uses MD5 password hashes, which provide stronger password security and allow you to set minimum length requirements to more than 8 characters.

ESX Server provides password controls on two levels to help you enforce password policies for your users and limit the risk of password cracking:

- **Password aging** – These controls govern how long a user password can be active before the user is required to change it. They help ensure that passwords change often enough so that if an attacker obtains a password through sniffing or social engineering, he or she cannot keep accessing ESX Server indefinitely.

- **Password complexity** – These controls ensure that the users select passwords that are hard for password generators to determine.

Password Aging

To ensure that passwords don’t stay active for long periods, ESX Server imposes the following password aging restrictions for user logons by default:

- **Maximum days** – The number of days that a user can keep a password before it needs to be changed. The default setting for ESX Server is 90 days. By default, the
root account and other service accounts are exempt from the 90 day expiration.

- **Minimum days** – The minimum number of days between password changes. The default setting is 0, meaning that the users can change their passwords any time.
- **Warning time** – The number of days in advance of password expiration that ESX Server observes when issuing a password change reminder. The default setting is 7 days.

You can tighten or loosen any of these settings by executing `esxcfg-auth` command options. If you need to override the default password aging settings for an individual user, use the `chage` command.

**To change default password aging restrictions for ESX Server**

1. Log on to the service console and acquire root privileges.
2. Execute one or more of the following commands as applicable:
   - To change maximum number of days a user can keep a password:
     ```shell
     esxcfg-auth --passmaxdays=<number_of_days>
     ```
     Where `<number_of_days>` is the maximum number of days before password expiration.
   - To change minimum number of days between password changes:
     ```shell
     esxcfg-auth --passmindays=<number_of_days>
     ```
     Where `<number_of_days>` is the minimum number of days between password changes.
   - To change warning time before a password change:
     ```shell
     esxcfg-auth --passwarnage=<number_of_days>
     ```
     Where `<number_of_days>` is the number of days of advanced warning a user receives before a password change is due.

**To override default password aging restrictions for individual users or groups**

1. Log on to the service console and acquire root privileges.
2. Execute one or more of the following commands as applicable:
   - To specify a new maximum days value:
     ```shell
     chage -M <number_of_days> <username>
     ```
   - To specify a new minimum days value:
chage -m <number_of_days> <username>

- To specify a new warning time value:
  chage -W <number_of_days> <username>

You can use the man chage command to learn about other chage options.

**Password Complexity**

By default, ESX Server uses the `pam_cracklib.so` plugin to set the rules that users must observe when creating passwords and to check password strength during the creation process.

The `pam_cracklib.so` plugin lets you determine the basic standards that all passwords must meet. By default, ESX Server imposes no restrictions on the root password. However, when non-root users attempt to change their passwords, the passwords they choose must meet the basic standards set by `pam_cracklib.so`. In addition, non-root users can make only a certain number of password change attempts before `pam_cracklib.so` begins issuing messages and eventually closes the password change screen. The ESX Server defaults for `pam_cracklib.so` password standards and retry restrictions are as follows:

- **Minimum length** - The `pam_cracklib.so` minimum length parameter for ESX Server systems is set to 9. This means that the user must enter at least 8 characters if he or she uses only one character class (lower case, upper case, digit, or other).

  The password length algorithm allows shorter passwords if the user enters a mix of character classes. To calculate the actual character length a user needs to enter to form a valid password for a given minimum length setting, apply the password length algorithm as follows:

  \[ M - CC = E \]

  Where:

  - \( M \) is the minimum length parameter.
  - \( CC \) is the number of character classes the user includes in the password.
  - \( E \) is the number of characters the user must enter.
The following table shows how the algorithm works assuming the user enters at least one lower case character as part of the password:

<table>
<thead>
<tr>
<th># of Characters Required for a Valid Password</th>
<th>Character Types in the Password Attempt</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Lower Case Characters</td>
</tr>
<tr>
<td>8</td>
<td>yes</td>
</tr>
<tr>
<td>7</td>
<td>yes</td>
</tr>
<tr>
<td>6</td>
<td>yes</td>
</tr>
<tr>
<td>5 *</td>
<td>yes</td>
</tr>
</tbody>
</table>

*The pam_cracklib.so plugin does not allow passwords of fewer than six characters. Thus, while the mathematically accurate character requirement for a four character-class password is five characters, the effective requirement is six.

- **Retries** – The pam_cracklib.so retries parameter for ESX Server systems is set to 3, meaning that if the user doesn’t enter a strong enough password in three attempts, pam_cracklib.so closes the password change dialog. The user must then open a new password change session to try again.

The pam_cracklib.so plugin checks all password change attempts to ensure that passwords meet the following strength criteria:

- The new password must not be a palindrome—a password where the characters mirror each other around a central letter, as in radar or civic.
- The new password must not be the reverse of the old password.
- The new password must not be a rotation—a version of the old password in which one or more characters have been rotated to the front or back of the password string.
- The new password must differ from the old password by more than a change of case.
- The new password must differ from the old password by more than a few characters.
The new password must not have been used in the past. The `pam_cracklib.so` plugin applies this criterion only if you have configured a password reuse rule.

By default ESX Server does not enforce any password reuse rules, so ordinarily the `pam_cracklib.so` plugin never rejects a password change attempt on these grounds. However, you can configure a reuse rule if you want to ensure that your users don’t alternate between just a few passwords.

If you configure a reuse rule, old passwords are stored in a file that the `pam_cracklib.so` plugin references during each password change attempt. The number of old passwords that ESX Server retains is determined by the reuse rule. When a user has created enough passwords to reach the value specified in the reuse rule, old passwords are removed from the file in age order. To learn how to configure a reuse rule, see To configure a password reuse rule on page 242.

The new password must be long enough and complex enough. You configure these requirements by changing the `pam_cracklib.so` complexity parameters with the `esxcfg-auth` command, which lets you set the number of retries, the minimum password length, and a variety of character credits. Character credits let the user enter shorter passwords if they include more character types in the password. To learn how to configure password length and complexity, see To change default password complexity for the `pam_cracklib.so` plugin on page 243.

For more information on the `pam_cracklib.so` plugin, see your Linux documentation.

**Note:** The `pam_cracklib.so` plugin used in Linux provides more parameters than the ones supported for ESX Server. You cannot specify these additional parameters in `esxcfg-auth`.

**To configure a password reuse rule**

1. Log on to the service console and acquire root privileges.
2. Change directories by entering `cd /etc/pam.d/` at the command prompt.
3. Use nano or another text editor to open the `system-auth` file.
4. Locate the line that starts with:
   ```
   password sufficient /lib/security/$ISA/pam_unix.so
   ```
5. Add the following parameters to the end of the line:
   ```
   remember=X
   ```
CHAPTER 11 Service Console Security

Where X is the number of old passwords you want ESX Server to store for each user. Use a space as the delimiter between remember=X and the preceding parameter.

6. Save your changes and close the file.
7. Change directories to /etc/security/, and issue the following command to make a zero length file with opasswd as the filename:
   touch opasswd
8. Issue the following commands:
   chmod 0600 opasswd
   chown root:root /etc/security/opasswd

To change default password complexity for the pam_cracklib.so plugin
1. Log on to the service console and acquire root privileges.
2. Enter the following command:
   esxcfg-auth --usecrack=<retries> <minimum_length> <lc_credit> <uc_credit> <d_credit> <oc_credit>
Where:
   • retries is the number of retries the user is allowed before ESX Server locks him or her out of password change mode.
   • minimum_length is the minimum number of characters a user must enter the password acceptable. This number is the total length before any length credits are applied.
     Note: One length credit is always applied so, in effect, the password length is one character less than the minimum_length parameter you specify. Because the pam_cracklib.so plugin does not accept password of under 6 characters, you should calculate the minimum_length parameter so that users can't drop the password length below 6 as a result of subtracting the length credits.
   • lc_credit is the number by which the minimum_length parameter is reduced if the user includes at least one lower case character in the password.
   • uc_credit is the number by which the minimum_length parameter is reduced if the user includes at least one upper case character.
   • d_credit is the number by which the minimum_length parameter is reduced if the user includes at least one digit.
oc_credit is the number by which the minimum_length parameter is reduced if the user includes at least one special character, such as an underbar or dash.

Character credit parameters should be entered as a positive number or as 0 if you do not want the plugin to give the user credit for including this character class. Character credits are additive. The more different types of characters the user enters, the fewer characters are required to form a valid password. For example, you issue the following command:

```
esxcfg-auth --usecrack=3 11 1 1 1 2
```

With this setting in effect, a user creating a password that contains lower case characters and one underbar would need eight characters to create a valid password. If the user decided to include all types of characters (lower case alphabetical, upper case alphabetical, numeric, and special), he or she would need only six characters.

### Changing the Password Plugin

The pam_cracklib.so plugin provides sufficient password strength enforcement for most environments. However, if you decide that the pam_cracklib.so plugin is not stringent enough for your needs, you can use the pam_passwdqc.so plugin instead. You change the plugin through the `esxcfg-auth` command.

The pam_passwdqc.so plugin tests for the same password characteristics as the pam_cracklib.so plugin. However, it provides a greater number of options for fine-tuning password strength and performs password strength tests for all users, including the root user. The pam_passwdqc.so plugin is also somewhat more difficult to use than the pam_cracklib.so plugin. For more information on this plugin, see your Linux documentation.

**Note:** The pam_passwdqc.so plugin used in Linux provides more parameters than the ones supported for ESX Server. You cannot specify these additional parameters in `esxcfg-auth`.

**To switch to the pam_passwdqc.so plugin**

1. Log on to the service console and acquire root privileges.
2. Enter the following command:

```
esxcfg-auth --usepamqc=N0 <N1> <N2> <N3> <N4> <match>
```

Where:

- N0 is the number of characters required for a password that uses characters from only one character class.
• $N_1$ is the number of characters required for a password that uses characters from two character classes.
• $N_2$ is used for passphrases. ESX Server requires three words for a passphrase.
• $N_3$ is the number of characters required for a password that uses characters from three character classes.
• $N_4$ is the number of characters required for a password that uses characters from all four character classes.
• $match$ is the number of characters allowed in a string that is reused from the old password. If the `pam_passwdqc.so` plugin finds a reused string of this length or longer, it disqualifies the string from the strength test and uses only the remaining characters.

Setting any of these options to -1 directs the `pam_passwdqc.so` plugin to ignore the requirement. Setting any of these options to `disabled` directs the `pam_passwdqc.so` plugin to disqualify passwords with the associated characteristic. The values used must be in descending order except for -1 and `disabled`.

For example, you issue the following command:

```
esxcfg-auth --usepamdqc=disabled 18 -1 12 8
```

With this setting in effect, a user creating a password would never be able to set passwords that contain only one character class. He or she would be need to use at least 18 characters for a password with two-character class, 12 characters for a three-character class password, and eight characters for four-character class passwords. Attempts to create passphrases would be ignored.
Cipher Strength

Transmitting data over insecure connections presents a security risk because malicious users might be able to scan data as it travels through the network, particularly if the network is operating in promiscuous mode. As a safeguard, network components commonly encrypt the data so that it can’t be easily read. To encrypt data, the sending component, such as a gateway or redirector, applies algorithms, or ciphers, to alter the data before transmitting it. The receiving component uses a key to decrypt the data, returning it to its original form.

Several different ciphers are currently in use, and the level of security provided by each is different. One measure of a cipher’s ability to protect data is its cipher strength—the number of bits in the encryption key. The larger the number, the more secure the cipher.

To ensure the protection of the data transmitted to and from external network connections, ESX Server uses one of the strongest block ciphers available—256-bit AES block encryption. ESX Server also uses 1024-bit RSA for key exchange. These encryption algorithms are the default for the following connections:

- VI Client connections to the VirtualCenter Server and to the ESX Server host through the service console.
- VI Web Access connections to the ESX Server host through the service console.

  **Note:** Because VI Web Access cipher usage is determined by the Web browser you are using, this management tool might use other ciphers.
- SDK connections to the VirtualCenter Server and to the ESX Server.
- Service console connections to virtual machines through the VMkernel.
- SSH connections to the ESX Server host through the service console. For more information, see SSH Security on page 250.
setuid and setgid Applications

*setuid* is a flag that allows an application to temporarily change the permissions of the user running the application by setting the effective user ID to the program owner's user ID. *setgid* is a flag that allows an application to temporarily change the permissions of the group running the application by setting the effective group ID to the program owner's group ID.

During ESX Server installation, several applications that include the *setuid* and *setgid* flags are installed by default. These applications are initiated by or through the service console. Some of them provide facilities required for correct operation of the ESX Server host. Others are optional, but they can make maintaining and troubleshooting the ESX Server host and the network easier.

**Default setuid Applications**

The following table lists the default *setuid* applications and indicates whether the application is required or optional:

<table>
<thead>
<tr>
<th>Application</th>
<th>Purpose and Path</th>
<th>Required or Optional</th>
</tr>
</thead>
</table>
| crontab         | Lets individual users add cron jobs.  
Path: /usr/bin/crontab | Optional |
| pam_timestamp_check | Supports password authentication.  
Path: /sbin/pam_timestamp_check | Required |
| passwd          | Supports password authentication.  
Path: /usr/bin/passwd | Required |
| ping            | Sends and listens for control packets on the network interface. Useful for debugging networks.  
Path: /bin/ping | Optional |
| pwdb_chkpwd     | Supports password authentication.  
Path: /sbin/pwdb_chkpwd | Required |
| ssh-keysign     | Performs host-based authentication for SSH secure shells.  
Path: /usr/libexec/openssh/ssh-keysign | Required if you use host-based authentication. Otherwise optional. |
| su              | Lets a general user become the root user by changing users.  
Path: /bin/su | Required |
Disabling any of the required applications will result in problems with ESX Server authentication and virtual machine operation, but if you need to, you can disable any optional application.

<table>
<thead>
<tr>
<th>Application</th>
<th>Purpose and Path</th>
<th>Required or Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>sudo</td>
<td>Lets a general user act as the root user only for specific operations.</td>
<td>Optional</td>
</tr>
<tr>
<td>Path:</td>
<td>/usr/bin/sudo</td>
<td></td>
</tr>
<tr>
<td>unix_chkpwd</td>
<td>Supports password authentication.</td>
<td>Required</td>
</tr>
<tr>
<td>Path:</td>
<td>/sbin/unix_chkpwd</td>
<td></td>
</tr>
<tr>
<td>vmkload_app</td>
<td>Performs tasks required to run virtual machines. This application is installed in two locations: one for standard use and one for debugging.</td>
<td>Required in both paths</td>
</tr>
<tr>
<td>Path for standard use:</td>
<td>/usr/lib/vmware/bin/vmkload_app</td>
<td></td>
</tr>
<tr>
<td>Path for debugging:</td>
<td>/usr/lib/vmware/bin-debug/vmkload_app</td>
<td></td>
</tr>
<tr>
<td>vmkping</td>
<td>Sends and listens for control packets on the network interface. Useful for debugging networks.</td>
<td>Optional</td>
</tr>
<tr>
<td>Path:</td>
<td>/usr/lib/vmware/bin/vmkping</td>
<td></td>
</tr>
<tr>
<td>vmware-authd</td>
<td>Authenticates users for use of services specific to VMware.</td>
<td>Required</td>
</tr>
<tr>
<td>Path:</td>
<td>/usr/sbin/vmware-authd</td>
<td></td>
</tr>
<tr>
<td>vmware-vmx</td>
<td>Performs tasks required to run virtual machines. This application is installed in two locations: one for standard use and one for debugging.</td>
<td>Required in both paths</td>
</tr>
<tr>
<td>Path for standard use:</td>
<td>/usr/lib/vmware/bin/vmware-vmx</td>
<td></td>
</tr>
<tr>
<td>Path for debugging:</td>
<td>/usr/lib/vmware/bin-debug/vmware-vmk</td>
<td></td>
</tr>
</tbody>
</table>
To disable an optional setuid application
1. Log on to the service console and acquire root privileges.
2. Execute this command:
   ```
   chmod a-s <path_to_executable>
   ```

**Default setgid Applications**

Two applications that include the setgid flag are installed by default. The following table lists the default setgid applications and indicates whether the application is required or optional:

<table>
<thead>
<tr>
<th>Application</th>
<th>Purpose and Path</th>
<th>Required or Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>wall</td>
<td>Alerts all terminals that an action is about to occur. This application is called by shutdown and other commands. <strong>Path:</strong> /usr/bin/wall</td>
<td>Optional</td>
</tr>
<tr>
<td>lockfile</td>
<td>Performs locking for the Dell OM management agent. <strong>Path:</strong> /usr/bin/lockfile</td>
<td>Required for Dell OM but optional otherwise</td>
</tr>
</tbody>
</table>

Disabling a required application will result in problems with ESX Server authentication and virtual machine operation, but if you need to, you can disable any optional application.

To disable an optional setgid application
1. Log on to the service console and acquire root privileges.
2. Execute this command:
   ```
   chmod a-g <path_to_executable>
   ```
SSH Security

SSH is a commonly used UNIX and LINUX command shell that lets you remotely log on to the service console and perform certain management and configuration tasks for ESX Server. SSH is used for secure logons and data transfers because it offers stronger protection than other command shells. In this ESX Server release, the SSH configuration has been enhanced to provide a higher security level than in the past. Key features of this enhancement include:

- **Version 1 SSH protocol disabled** – VMware no longer supports Version 1 SSH protocol, and now uses Version 2 protocol exclusively. Version 2 eliminates certain security issues present in Version 1 and provides you with a safer communications interface to the service console.

- **Improved cipher strength** – SSH now supports only 256-bit and 128-bit AES ciphers for your connections.

- **Limits on remote logons as root** – You can no longer remotely log on as root. Instead, you log on as an identifiable user and either use the `sudo` command to execute specific operations that require root privileges or enter the `su` command to become the root user.

  **Note:** The `sudo` command provides security benefits in that it limits root activities and helps you check for possible misuse of root privileges by generating an audit trail of any root activities that the user performs.

These settings are designed to provide solid protection for the data you transmit to the service console through SSH. If this configuration is too rigid for your needs, you can lower security parameters.

**To change the default SSH configuration**

1. Log on to the service console and acquire root privileges.
2. Change directories by entering `cd /etc/ssh` at the command prompt.
3. Use nano or another text editor to perform any or all of following actions, as appropriate:
   - To allow remote root logon, change the setting to `yes` in the following line in the `sshd_config` file:

     ```
     PermitRootLogin no
     ```

   - To revert to the default SSH protocol (Version 1 and 2), comment out the following line in the `sshd_config` file:

     ```
     Protocol 2
     ```
• To revert to the 3DES cipher and other ciphers, comment out the following line in the `sshd_config` file:
  ```
  Ciphers aes256-cbc,aes128-cbc
  ```
• To disable Secure FTP (SFTP) on SSH, comment out the following line in the `sshd_config` file:
  ```
  Subsystem ftp /usr/libexec/openssh/sftp-server
  ```
4. Save your changes and close the file.
5. Execute the following command to restart the SSHD service:
   ```
   service sshd restart
   ```
Security Patches and Security Vulnerability Scanning Software

If a fix for a particular LINUX-supported software package provided by VMware as a service console component—for example, a service, facility, or protocol—becomes available, VMware provides an RPM Package Manager (RPM) package that you use to update the software package on ESX Server. Although these fixes might be available from other sources, you should always use RPMs generated by VMware instead of using third-party RPMs.

When providing patches for a software package, the VMware policy is to backport the fix to a version of the software known to be stable. This approach reduces the chance of introducing new problems and instability in the software. Because the patch is added to an existing version of the software, the version number of the software stays the same, but a patch number is added as a suffix.

Certain security scanners such as Nessus check the version number but not the patch suffix as they search for security holes. As a result, these scanners can falsely report that software is down-level and doesn’t include the most recent security patches even though it does. This problem is common to the industry and not specific to VMware.

Note: Some security scanners are able to handle this situation correctly, but they typically lag by a version or more. For example, the version of Nessus released after a Red Hat patch often doesn’t report these false positives.

Here is an example of how this problem occurs:

1. You initially install ESX Server with OpenSSL version 0.9.7a (where 0.9.7a is the original version with no patches).
2. OpenSSL releases a patch that fixes a security hole in version 0.9.7. This version is called 0.9.7x.
3. VMware backports the OpenSSL 0.9.7x fix to the original version, updates the patch number, and creates an RPM. The OpenSSL version in the RPM is 0.9.7a-1, indicating that the original version (0.9.7a) now contains patch 1.
4. You install the RPM.
5. The security scanner fails to note the -1 suffix and erroneously reports that security for OpenSSL isn’t up to date.
If your scanner reports that security for a package is down-level, perform the following checks:

- Look at the patch suffix to determine whether you actually need to get an update.
- Read the VMware RPM documentation for information on the patch contents.
- Use the following command to look for Common Vulnerabilities and Exposures (CVE) number from the security alert in the RPM change log:

  ```shell
  rpm-q --changelog openssl | grep <CVE_number>
  ```

If the CVE number is there, the package covers that vulnerability.
Security Deployments and Recommendations

The chapter focuses on giving you a better idea of how to secure your ESX Server in particular environments by presenting a series of ESX Server deployment scenarios that you can consider as you plan some of the security features of your own deployment. It also makes some basic security recommendations you can consider when creating and configuring virtual machines.

This chapter covers the following topics:

- Security Approaches for Common ESX Server Deployments on page 256
- Virtual Machine Recommendations on page 262
Security Approaches for Common ESX Server Deployments

The complexity of ESX Server deployments can vary significantly depending on the size of your company, the way that data and resources need to be shared with the outside world, whether there are multiple datacenters or just one, and so forth.

Inherent in the following deployments are policies for user access, resource sharing, and security level. By comparing the deployments, you can get a sense of the issues you face in planning security for your own ESX Server deployment.

Single Customer Deployment

In this deployment, the ESX Server hosts are owned and maintained within a single corporation and single datacenter. No ESX Server resources are shared with outside users. One site administrator maintains the ESX Server hosts, and these hosts run a number of virtual machines.

The deployment does not allow customer administrators, and the site administrator is solely responsible for maintaining the various virtual machines. The corporation staffs a set of system administrators who do not have accounts on the ESX Server host and cannot access any of the ESX Server tools such as VirtualCenter or command line shells for the host. These system administrators have access to virtual machines through the virtual machine console so that they can load software and perform other maintenance tasks inside the virtual machines.

The following table shows how you might handle sharing for the components you use and configure for the ESX Server host.

<table>
<thead>
<tr>
<th>Function</th>
<th>Configuration</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service console shares the same physical network as the virtual machines?</td>
<td>No</td>
<td>You should isolate the service console by configuring it on its own physical network.</td>
</tr>
<tr>
<td>Service console shares the same VLAN as the virtual machines?</td>
<td>No</td>
<td>You should isolate the service console by configuring it on its own VLAN. No virtual machine or other system facility such as VMotion should use this VLAN.</td>
</tr>
<tr>
<td>Virtual machines share the same physical network?</td>
<td>Yes</td>
<td>You can configure your virtual machines on the same physical network.</td>
</tr>
</tbody>
</table>
The following table shows how you might set up user accounts for the ESX Server host.

<table>
<thead>
<tr>
<th>User Category</th>
<th>Total Number of Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site administrators</td>
<td>1</td>
</tr>
<tr>
<td>Customer administrators</td>
<td>0</td>
</tr>
<tr>
<td>System administrators</td>
<td>0</td>
</tr>
<tr>
<td>Business users</td>
<td>0</td>
</tr>
</tbody>
</table>

The following table shows the level of access for each user.

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Site Administrator</th>
<th>System Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root access?</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Service console access through SSH?</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>VirtualCenter and VI Web Access?</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Virtual machine creation and modification?</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Virtual machine access through the console?</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Multiple Customer Restricted Deployment**

In this deployment, the ESX Server hosts are in the same datacenter and are used to serve applications for multiple customers. The site administrator maintains the ESX server and manages the ESX hosts. Here are the deployment details:

<table>
<thead>
<tr>
<th>Function</th>
<th>Configuration</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network adapter sharing?</td>
<td>Partial</td>
<td>You should isolate the service console by configuring it on its own virtual switch and virtual network adapter. No virtual machine or other system facility should use this switch or adapter. However, you can configure your virtual machines on the same virtual switch and network adapter.</td>
</tr>
<tr>
<td>VMFS sharing?</td>
<td>Yes</td>
<td>All .vmdk files should reside in the same VMFS partition.</td>
</tr>
<tr>
<td>Security level</td>
<td>High</td>
<td>You can open ports for needed services like FTP on an individual basis. See Service Console Firewall Configuration on page 234 for information on security levels.</td>
</tr>
<tr>
<td>Virtual machine memory overcommitment?</td>
<td>Yes</td>
<td>You can configure the total memory for the virtual machines as greater than the total physical memory.</td>
</tr>
</tbody>
</table>
Server hosts, and these hosts run a number of virtual machines dedicated to the customers. Virtual machines that belong to the various customers can be on the same ESX Server host, but the site administrator restricts resource sharing to prevent rogue interaction.

While there is only one site administrator, several customer administrators maintain the virtual machines assigned to their customers. This deployment also includes customer system administrators who do not have ESX Server accounts but have access to the virtual machines through the virtual machine console so that they can load software and perform other maintenance tasks inside the virtual machines.

The following table shows how you might handle sharing for the components you use and configure for the ESX Server host.

<table>
<thead>
<tr>
<th>Function</th>
<th>Configuration</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service console shares the same physical network as the virtual machines?</td>
<td>No</td>
<td>You should isolate the service console by configuring it on its own physical network.</td>
</tr>
<tr>
<td>Service console shares the same VLAN as the virtual machines?</td>
<td>No</td>
<td>You should isolate the service console by configuring it on its own VLAN. No virtual machine or other system facility such as VMotion should use this VLAN.</td>
</tr>
<tr>
<td>Virtual machines share the same physical network?</td>
<td>Partial</td>
<td>You should put the virtual machines for each customer on a different physical network. All physical networks are independent of each other.</td>
</tr>
<tr>
<td>Network adapter sharing?</td>
<td>Partial</td>
<td>You should isolate the service console by configuring it on its own virtual switch and virtual network adapter. No virtual machine or other system facility should use this switch or adapter. You configure virtual machines for one customer so that they all share the same virtual switch and network adapter. However, they do not share the switch and adapter with any other customers.</td>
</tr>
<tr>
<td>VMFS sharing?</td>
<td>No</td>
<td>Each customer has their own VMFS partition and their virtual machine .vmdk files reside exclusively on that partition. The partition can span multiple LUNs.</td>
</tr>
<tr>
<td>Security level</td>
<td>High</td>
<td>You can open ports for services like FTP.</td>
</tr>
</tbody>
</table>
The following table shows how you might set up user accounts for the ESX Server host.

<table>
<thead>
<tr>
<th>User Category</th>
<th>Total Number of Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site administrators</td>
<td>1</td>
</tr>
<tr>
<td>Customer administrators</td>
<td>10</td>
</tr>
<tr>
<td>System administrators</td>
<td>0</td>
</tr>
<tr>
<td>Business users</td>
<td>0</td>
</tr>
</tbody>
</table>

The following table shows the level of access for each user.

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Site Administrator</th>
<th>Customer Administrator</th>
<th>System Administrator</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root access?</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Service console access through SSH?</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>VirtualCenter and VI Web Access?</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Virtual machine creation and modification?</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Virtual machine access through the console?</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Multiple Customer Open Deployment**

In this deployment, the ESX Server hosts are in the same datacenter and are used to serve applications for multiple customers. The site administrator maintains the ESX Server hosts, and these hosts run a number of virtual machines dedicated to the customers. Virtual machines that belong to the various customers can be on the same ESX Server host, but there are fewer restrictions on resource sharing.

While there is only one site administrator, several customer administrators maintain the virtual machines assigned to their customers. The deployment also includes customer system administrators who do not have ESX Server accounts but have access to the virtual machines through the virtual machine console so that they can load software and perform other maintenance tasks inside the virtual machines.
Lastly, a group of business users who do not have accounts can use virtual machines to run their applications.

The following table shows how you might handle sharing for the components you use and configure for the ESX Server host.

<table>
<thead>
<tr>
<th>Function</th>
<th>Configuration</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service console shares the same physical network as the virtual machines?</td>
<td>No</td>
<td>You should isolate the service console by configuring it on its own physical network.</td>
</tr>
<tr>
<td>Service console shares the same VLAN as the virtual machines?</td>
<td>No</td>
<td>You should isolate the service console by configuring it on its own VLAN. No virtual machine or other system facility such as VMotion should use this VLAN.</td>
</tr>
<tr>
<td>Virtual machines share the same physical network?</td>
<td>Yes</td>
<td>You can configure your virtual machines on the same physical network.</td>
</tr>
<tr>
<td>Network adapter sharing?</td>
<td>Partial</td>
<td>You should isolate the service console by configuring it on its own virtual switch and virtual network adapter. No virtual machine or other system facility should use this switch or adapter. You configure all virtual machines on the same virtual switch and network adapter.</td>
</tr>
<tr>
<td>VMFS sharing?</td>
<td>Yes</td>
<td>Virtual machines can share VMFS partitions and their virtual machine .vmdk files can reside on shared partitions. Virtual machines do not share .vmdk files.</td>
</tr>
<tr>
<td>Security level</td>
<td>High</td>
<td>You can open ports for services like FTP.</td>
</tr>
<tr>
<td>Virtual machine memory overcommitment?</td>
<td>Yes</td>
<td>You can configure the total memory for the virtual machines as greater than the total physical memory.</td>
</tr>
</tbody>
</table>

The following table shows how you might set up user accounts for the ESX Server host.

<table>
<thead>
<tr>
<th>User Category</th>
<th>Total Number of Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Site administrators</td>
<td>1</td>
</tr>
<tr>
<td>Customer administrators</td>
<td>10</td>
</tr>
<tr>
<td>System administrators</td>
<td>0</td>
</tr>
</tbody>
</table>
The following table shows the level of access for each user.

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Site Administrator</th>
<th>Customer Administrator</th>
<th>System Administrator</th>
<th>Business User</th>
</tr>
</thead>
<tbody>
<tr>
<td>Root access?</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Service console access through SSH?</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>VirtualCenter and VI Web Access?</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Virtual machine creation and modification?</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Virtual machine access through the console?</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

The following table shows the level of access for each user.

<table>
<thead>
<tr>
<th>User Category</th>
<th>Total Number of Accounts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business users</td>
<td>0</td>
</tr>
</tbody>
</table>
Virtual Machine Recommendations

Consider the following recommendations when evaluating virtual machine security and administering virtual machines:

Installing Antivirus Software
Because each virtual machine hosts a standard operating system, you must protect it from viruses. You can do so by installing antivirus software. Depending on how you’re using the virtual machine, you might also want to install a software firewall.

Note: Software firewalls and antivirus software can be virtualization-intensive. If you are confident that your virtual machines are in a fully trusted environment, you can balance the need for these two security measures against virtual machine performance.

Disabling Copy and Paste Operations Between the Guest Operating System and Remote Console
When VMware Tools runs on a virtual machine, you can copy and paste between the guest operating system and remote console. As soon as the console window gains focus, non-privileged users and processes running in the virtual machine can access the clipboard for the virtual machine console. If a user copies sensitive information to the clipboard before using the console, the user—perhaps unknowingly—exposes sensitive data to the virtual machine.

To prevent this problem, you should consider disabling copy and paste operations for the guest operating system.

To disable copy and paste operations between the guest operating system and remote console
1. Log on to the VI Client and select the virtual machine from the inventory panel.
   The configuration page for this virtual machine appears with the Summary tab displayed.
2. Click Edit Settings.
3. Click Options > Advanced > Configuration Parameters to open the Configuration Parameters dialog box.
4. Click the Add button.
5. Type the following values in the Name field Value column:

<table>
<thead>
<tr>
<th>Name Field</th>
<th>Value Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>isolation.tools.copy.enable</td>
<td>FALSE</td>
</tr>
<tr>
<td>isolation.tools.paste.enable</td>
<td>FALSE</td>
</tr>
<tr>
<td>isolation.tools.setGUlOptions.enable</td>
<td>FALSE</td>
</tr>
</tbody>
</table>

The result appears as follows:

![Configuration Parameters dialog box]

**Note:** These options override any settings made in the guest operating system's VMware Tools control panel.

6. Click **OK** to close the Configuration Parameters dialog box and then click **OK** again to close the Virtual Machine Properties dialog box.

**Removing Unnecessary Hardware Devices**

Nonprivileged users and processes within virtual machines can connect or disconnect hardware devices, such as network adapters and CD-ROM drives. Attackers can use this capability to breach virtual machine security in several ways. For example, by default, an attacker with access to a virtual machine can:

- Connect a disconnected CD-ROM drive and access sensitive information on the media left in the drive.
- Disconnect a network adapter to isolate the virtual machine from its network, resulting in a denial of service.

As a general security precaution, you should use commands on the VI Client Configuration tab to remove any unneeded or unused hardware devices. While this
measure tightens virtual machine security, it isn't a good solution in situations where you might need to bring a currently unused device back into service at a later time.

If you don't want to permanently remove a device, you can prevent a virtual machine user or process from connecting or disconnecting the device from within the guest operating system.

To prevent a virtual machine user or process from disconnecting devices

1. Log on to the VI Client and select the virtual machine from the inventory panel.
   The configuration page for this virtual machine appears with the Summary tab displayed.

2. Click Edit Settings.

3. Click Options > Advanced > Configuration Parameters to open the Configuration Parameters dialog box.

4. Click the Add button and type the following:
   - Name field – <device_name>.allowGuestConnectionControl
   - Value field – FALSE

   Where <device_name> is the name of the device you want to protect, for example, ethernet0.

   The result appears as follows:

   ![Configuration Parameters dialog box](image)

5. Click OK to close the Configuration Parameters dialog box and then click OK again to close the Virtual Machine Properties dialog box.
Preventing the Guest Operating System Processes from Flooding the ESX Server Host

The guest operating system processes send informational messages to the ESX Server host through VMware Tools. These messages, known as setinfo messages, typically contain name-value pairs that define virtual machine characteristics or identifiers that the host stores—for example, ipaddress=10.17.87.224.

A setinfo message has no predefined format, and it can be any length. Therefore, the amount of data passed to the host by this means is unlimited. An unrestricted data flow provides an opportunity for an attacker to stage a DOS attack by writing software that mimics VMware Tools and flooding the host with packets, thus consuming resources needed by the virtual machines.

To prevent this problem, you should consider limiting the ability of VMware Tools to arbitrarily send setinfo messages to the ESX Server host.

**Note:** VMware Tools also sends other types of messages, but these have predefined formats and, therefore, are not good vehicles for DOS attacks.

**To prevent the guest operating system processes from sending arbitrary messages to the host**

1. Log on to the VI Client and select the virtual machine from the inventory panel. The configuration page for this virtual machine appears with the Summary tab displayed.
2. Click **Edit Settings**.
3. Click **Options > Advanced > Configuration Parameters** to open the Configuration Parameters dialog box.
4. Click the **Add** button and type the following:
   - **Name field** – isolation.tools.setinfo.disable
   - **Value field** – TRUE
5. Click OK to close the Configuration Parameters dialog box and then click OK again to close the Virtual Machine Properties dialog box.

Disabling Logging for the Guest Operating System

Virtual machines can write troubleshooting information into a virtual machine log file stored on the VMFS volume. Virtual machine users and processes can abuse logging either inadvertently or with intent such that large amounts of data flood the log file. Over time, the log file can consume enough of the service console’s file system space to cause a denial of service.

To prevent this problem, you can disable logging for virtual machine guest operating systems. In making this decision, be aware that you might not be able to gather adequate logs to allow troubleshooting. Further, VMware does not offer technical support for virtual machine problems if logging has been disabled.

To disable logging for the guest operating system

1. Log on to the VI Client and select the virtual machine from the inventory panel.

   The configuration page for this virtual machine appears with the Summary tab displayed.

2. Click Edit Settings.

3. Click Options > Advanced > Configuration Parameters to open the Configuration Parameters dialog box.
4. Click the Add button and type the following:
   - **Name field** – isolation.tools.log.disable
   - **Value field** – TRUE

   The result appears as follows:

5. Click OK to close the Configuration Parameters dialog box and then click OK again to close the Virtual Machine Properties dialog box.
Appendix A:
ESX Technical Support Commands

This appendix lists the various service console commands used to configure ESX Server. Most of these commands are reserved for Technical Support use and are included for your reference only. In a few cases, however, these commands provide the only means of performing a configuration task for the ESX Server host. Also, if you lose your connection to the host, executing certain of these commands through the command-line interface may be your only recourse—for example, if networking becomes nonfunctional and VI Client access is therefore unavailable. If you use the commands in this appendix, you must execute the service mgmt-vmware restart command to restart the vmware-hostd process and make the VI Client and other management tools aware of the changes.

The VI Client graphical user interface now provides the preferred means of performing the configuration tasks described in this appendix. You can use this appendix to learn which VI Client commands to use in place of the service console commands. This appendix provides a summary of the actions you take in VI Client but doesn’t give
complete instructions. For details on using commands and performing configuration tasks through VI Client, see the Virtual Infrastructure User’s Guide and the online help.

**Note:** You can perform most of the VI Client actions listed in the table only after you have selected an ESX Server host from the inventory panel and clicked the **Configuration** tab. These actions are preliminary to any procedure discussed below unless otherwise stated.

You can find additional information on a number of ESX commands by using the `man <esxcfg_command_name>` command to display man pages.

<table>
<thead>
<tr>
<th>Service Console Command</th>
<th>VI Client Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>esxcfg-advcfg</strong></td>
<td>Configures advanced options for ESX Server. To configure advanced options in VI Client, click <strong>Advanced Settings</strong>. When the <strong>Advanced Settings</strong> dialog box opens, use the list on the left to select the device type or activity you want to work with, then enter the appropriate settings.</td>
</tr>
<tr>
<td><strong>esxcfg-auth</strong></td>
<td>Configures authentication. This command is used to switch between the <code>pam_cracklib.so</code> and <code>pam_passwdqc.so</code> plugins for password change rule enforcement. You also use this command to reset options for these two plugins. For more information, see Password Complexity on page 240. There is no means of configuring these functions in VI Client.</td>
</tr>
<tr>
<td><strong>esxcfg-boot</strong></td>
<td>Configures bootstrap settings. This command is used for the bootstrap process and is intended for VMware Technical Support use only. You should not issue this command unless instructed to do so by a VMware Technical Support representative. There is no means of configuring these functions in VI Client.</td>
</tr>
</tbody>
</table>
## Service Console Command

<table>
<thead>
<tr>
<th>Command</th>
<th>VI Client Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>esxcfg-dumpart</td>
<td>Configures a diagnostic partition or searches for existing diagnostic partitions. When you install ESX Server, a diagnostic partition is created to store debugging information in the event of a system fault. You don't need to create this partition manually unless you can't find it in your volume list when you view the host's storage configuration. You can perform the following management activities for diagnostic partitions in VI Client:</td>
</tr>
<tr>
<td></td>
<td>• <strong>Determine whether there is a diagnostic partition</strong> — Click Storage &gt; Add and check the first page of the Add Storage Wizard to see whether it includes the Diagnostic option. If Diagnostic is not one of the options, ESX Server already has a diagnostic partition.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Configure a diagnostic partition</strong> — Click Storage &gt; Add &gt; Diagnostic and step through the wizard.</td>
</tr>
<tr>
<td>esxcfg-firewall</td>
<td>Configures the service console firewall ports. To configure firewall ports in VI Client, you select the Internet services that will be allowed to access the ESX Server host. Click Security Profile &gt; Firewall &gt; Properties and use the Firewall Properties dialog box to add services. For details on adding services and configuring firewalls, see Opening Firewall Ports for Supported Services and Management Agents on page 185.</td>
</tr>
<tr>
<td>esxcfg-info</td>
<td>Prints information about the state of the service console, VMKernel, various subsystems in the virtual network, and storage resource hardware. VI Client doesn't provide a method for printing this information, but you can obtain much of it through different tabs and functions in the user interface. For example, you can check the status of your virtual machines by reviewing the information on the Virtual Machines tab.</td>
</tr>
<tr>
<td>esxcfg-init</td>
<td>Performs internal initialization routines. This command is used for the bootstrap process and is intended for VMware Technical Support use only. You should not issue this command unless instructed to do so by a VMware Technical Support representative. There is no VI Client equivalent for this command.</td>
</tr>
<tr>
<td>Service Console Command</td>
<td>VI Client Procedure</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>esxcfg-linuxnet</td>
<td>Converts vswif to eth when booting ESX Server into service-console-only mode rather than into ESX mode. This command is used for the bootstrap process and is intended for VMware Technical Support use only. You should not issue this command unless instructed to do so by a VMware Technical Support representative. There is no VI Client equivalent for this command.</td>
</tr>
<tr>
<td>esxcfg-module</td>
<td>Sets driver parameters and modifies which drivers are loaded during startup. This command is used for the bootstrap process and is intended for VMware Technical Support use only. You should not issue this command unless instructed to do so by a VMware Technical Support representative. There is no VI Client equivalent for this command.</td>
</tr>
<tr>
<td>esxcfg-mpath</td>
<td>Configures multipath settings for your Fibre Channel or iSCSI disks. To configure multipath settings for your storage in VI Client, click Storage. Select a datastore or mapped LUN and click Properties. When the Properties dialog box opens, select the desired extent if necessary. Then, click Extent Device &gt; Manage Paths and use the Manage Path dialog box to configure the paths.</td>
</tr>
</tbody>
</table>
| esxcfg-nas             | Manages NAS mounts. You use this command to add, delete, list, and change the attributes of NAS devices. To view NAS devices in VI Client, click Storage and scroll through the storage list. You can also perform the following activities from the Storage view:  
  * Display the attributes of a NAS device — Click the device and review the information under Details.  
  * Add a NAS device — Click Add  
  * Delete a NAS device — Click Remove  
  * Change the attributes of a NAS device — Double-click the device and click Details > Properties.  
For complete instructions on how to create and configure NAS datastores, seeConfiguring ESX Server to Access NFS Volumes on page 131. |
## Appendix A: ESX Technical Support Commands

<table>
<thead>
<tr>
<th>Service Console Command</th>
<th>VI Client Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>esxcfg-nics</td>
<td>Prints a list of physical network adapters along with information on the driver, PCI device, and link state of each NIC. You can also use this command to control a physical network adapter’s speed and duplexing. To view information on the physical network adapters for the host in VI Client, click <strong>Network Adapters</strong>. To change the speed and duplexing for a physical network adapter in the VI Client, To set up connections for the service console in VI Client, click <strong>Networking &gt; Properties</strong> for any of the virtual switches associated with the physical network adapter. In the <strong>Properties</strong> dialog box, click <strong>Network Adapters &gt; Edit</strong> and select the speed and duplex combination. For complete instructions on how to change the speed and duplexing, see To configure the uplink network adapter by changing its speed on page 50.</td>
</tr>
<tr>
<td>esxcfg-resgrp</td>
<td>Restores resource group settings and lets you perform basic resource group management. Select a resource pool from the inventory panel and click <strong>Edit Resources</strong> on the <strong>Summary</strong> tab. Then, use the <strong>Edit Settings</strong> dialog box to change the resource group settings.</td>
</tr>
<tr>
<td>esxcfg-route</td>
<td>Sets or retrieves the default VMkernel gateway route. To view the default VMkernel gateway route in VI Client, click <strong>DNS and Routing</strong>. If you want to change the default routing, click <strong>Properties</strong> and update the information in both tabs of the <strong>DNS Configuration</strong> dialog box.</td>
</tr>
<tr>
<td>esxcfg-swiscsi</td>
<td>Configures your software iSCSI software adapter. To configure your software iSCSI system in VI Client, click <strong>Storage Adapters</strong>, select the iSCSI adapter you want to configure, and click <strong>Properties</strong>. Use the <strong>iSCSI Initiator Properties</strong> dialog box to configure the adapter. For complete instructions on how to create and configure iSCSI datastores, see <strong>iSCSI Storage on page 103</strong>.</td>
</tr>
</tbody>
</table>
## Service Console Command | VI Client Procedure
--- | ---
**esxcfg-upgrade** | Upgrades ESX Server from ESX Server 2.x to ESX Server 3.x. This command is not for general use.
You complete the following three tasks when upgrading from 2.x to 3.x. Some of these can be performed in VI Client:
- **Upgrade the host** — You upgrade the binaries, converting from ESX Server 2.x to ESX Server 3.x. You cannot perform this step from VI Client. For information on performing this upgrade, see the **Installation and Upgrade Guide**.
- **Upgrade the file system** — To upgrade VMFS-2 to VMFS-3, suspend or power off your virtual machines, then click **Inventory > Hosts > Enter Maintenance Mode**. Click **Storage**, select a storage device, and click **Upgrade to VMFS-3**. You must perform this step for each storage device you want to upgrade.
- **Migrate the virtual machines** — To migrate from VMS-2 to VMS-3, click **Inventory > Hosts > Relocate VM Files**.

**esxcfg-vmhbadevs** | Prints a map of VMkernel storage devices to service console devices. There is no VI Client equivalent for this command.

**esxcfg-vmknic** | Creates and updates VMkernel TCP/IP settings for VMotion, NAS, and iSCSI.
To set up VMotion, NFS, or iSCSI network connections in VI Client, click **Networking > Add Networking**. Select **VMotion and IP Storage** and step through the **Add Networking** Wizard.
You set up IP address subnet mask and VMkernel default gateway in the **Connection Settings** step.
To review your settings, click the icon to the left of the VMotion, iSCSI, or NFS port. If you want to edit any of these settings, click **Edit** for the switch. Select the port from the list on the switch **Properties** dialog box, then click **Edit** to open the port **Properties** dialog box and change the settings for the port.
For complete instructions on how to create and update VMotion, NFS, or iSCSI network connections, see **VMkernel Configuration on page 32**.
Appendix A: ESX Technical Support Commands

<table>
<thead>
<tr>
<th>Service Console Command</th>
<th>VI Client Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>esxcfg-vswif</td>
<td>Creates and updates service console network settings. This command is used if you cannot manage the ESX Server host through the VI Client because of network configuration issues. For more information, see Troubleshooting Service Console Networking on page 43. To set up connections for the service console in VI Client, click Networking &gt; Add Networking. Select Service Console and step through the Add Networking Wizard. You set up the IP address subnet mask and the VMkernel default gateway in the Connection Settings step. To review your settings, click the icon to the left of the desired Service Console Port Group. If you want to edit any of these settings, click Edit for the switch. Select the service console port from the list on the switch Properties dialog box, then click Edit to open the port Properties dialog box and change the settings for the port. For complete instructions on how to create and update the service console connection, see Service Console Configuration on page 37.</td>
</tr>
<tr>
<td>esxcfg-vswitch</td>
<td>Creates and updates virtual machine network settings. To set up connections for a virtual machine in VI Client, click Networking &gt; Add Networking. Select Virtual Machine and step through the Add Networking Wizard. To review your settings, click the icon to the left of the desired Virtual Machine Port Group. If you want to edit any of these settings, click Edit for the switch. Select the Virtual Machine port from the list on the switch Properties dialog box, then click Edit to open the port Properties dialog box and change the settings for the port. For complete instructions on how to create and update virtual machines, see Virtual Network Configuration for Virtual Machines on page 28.</td>
</tr>
</tbody>
</table>
Appendix B: Using vmkfstools

The `vmkfstools` command lets you create and manage Virtual Machine File Systems (VMFSs) on SCSI disks, or LUNs, that an ESX Server host uses for storage. You can also use this command to manage files stored in the VMFSs. In addition, you can use the `vmkfstools` command on SCSI disk partitions that you create using a SCSI partitioning tool such as `sfdisk(8)` or `fdisk(8)`. Most `vmkfstools` operations can also be performed through the VI Client. For information on using the VI Client to work with storage, see Configuring Storage on page 87.
vmkfstools Command Syntax

You must be logged in as the root user to run the vmkfstools command.

vmkfstools Syntax When Specifying a SCSI Device

The format for the vmkfstools command when specifying a SCSI device is:

   vmkfstools <options> <device_path>

Where:

- `<options>` are one or more command line options and associated arguments you use to specify the activity that you want vmkfstools to perform — for example, converting a VMFS-2 volume on a partition to VMFS-3 format.

- `<device_path>` specifies a SCSI device (a SCSI disk or a partition on a SCSI disk) being manipulated or a VMFS volume path.

If `<device_or_VMFS_volume>` path is a SCSI device, then it is specified as in the following example:

   /vmfs/devices/disks/vmhba1:2:0:0

Here, `/vmfs/devices/disks` is the mount point of the device file system. `vmhba1` specifies the second SCSI HBA created by the VMkernel, the second number (in this case, 2) specifies the target on the adapter, the third number (0) specifies the LUN, and the fourth number (3) specifies the partition. Partition 0 (zero) implies the whole disk; otherwise, the number specifies the indicated partition.
vmkfstools Syntax When Specifying a VMFS Volume or File

The format for the `vmkfstools` command when specifying a VMFS volume or file is:

```
vmkfstools <options> <path>
```

Where:

- `<options>` are one or more command line options you use to specify the activity that `vmkfstools` will perform.
- `<path>` is an absolute path that names a directory or a file under the `/vmfs` directory. For example, you can specify a VMFS file system using the following format:

```
/vmfs/volumes/<volume_name>
```

For example:

```
/vmfs/volumes/lun1
```

You can also specify a single VMFS file using the following format:

```
/vmfs/volumes/<volume_name>/<file>
```

For example:

```
/vmfs/volumes/lun1/rh9.vmdk
```

- **v Suboption**

The `-v` suboption indicates the verbosity level of the command output. The format for this suboption is as follows:

```
-v --verbose <number>
```

You specify the `<number>` value as an integer from 1 through 10.

You can specify the `-v` suboption with any `vmkfstools` option. If the output of the option isn't suitable for use with the `-v` suboption, `vmkfstools` ignores the `-v` part of the command line.

**Note:** Because you can include the `-v` suboption in any `vmkfstools` command line, the suboption is not specifically covered in any of the option descriptions.
vmkfstools Options

This section includes a list of all the options used with the `vmkfstools` command. Some of the tasks in this section include options suggested for advanced users only. The long and short (single letter) forms of options are equivalent. For example, the following commands are identical:

```
vmkfstools --createfs vmfs3 --blocksize 2m vmhba1:3:0:1
vmkfstools -C vmfs3 -b 2m vmhba1:3:0:1
```

File System Options

File system options are tasks that you may perform when setting up a VMFS file system. You can also perform some of these tasks through the VI Client.

Creating a VMFS file system on a specified SCSI device

```
-C --createfs vmfs3
  -b --blocksize <block_size>kK|mM
  -S --setfsname <fsName>
```

This option creates a VMFS-3 file system on the specified SCSI partition.

**Note:** VMFS-2 file systems are read-only on any ESX Server 3. Users cannot create or modify VMFS-2 file systems but are able to read files stored on VMFS-2 file systems.

**Caution:** Be aware that you can have only one VMFS volume for a LUN.

You can specify the following suboptions with the `-C` option:

- **--blocksize** — Define the block size for the VMFS-3 file system. The `<block_size>` value you specify must be a power of 2 and must lie between 1 KB and 8 MB. When entering a size, indicate the unit type by adding a suffix of `k` (kilobytes) or `m` (megabytes). The unit type is not case sensitive — in other words, `vmkfstools` interprets either `k` or `K` to mean kilobytes.

- **--setfsname** — Define the volume label of a VMFS volume for the VMFS-3 file system you are creating. The label you specify can be up to 31 characters long and cannot contain any leading or trailing blank spaces.

After you define a volume label, you can use it whenever specifying the VMFS volume for the `vmkfstools` command. You can also use the VMFS volume when referencing the volume in virtual machine configuration files. The volume name appears in listings generated for the Linux `ls -l` command and as a symbolic link to the VMFS volume under the `/vmfs/volumes` directory.
Appendix B: Using vmkfstools

If you need to change the VMFS volume label, use the Linux `ln -sf` command. Use the following as an example:

```
ln -sf /vmfs/volumes/<UUID> /vmfs/volumes/<fsName>
```

<fsName> is the new volume label you want to use for the <UUID> VMFS.

**Extending an existing logical VMFS-3 volume by spanning multiple partitions**

```
-Z --extendfs <extension-device> <existing-VMFS-volume>
```

This option adds another extent to a previously created VMFS volume <existing-VMFS-volume>. Each time you use this option, you extend a VMFS-3 volume with a new extent so that the volume spans multiple partitions. At most, a logical VMFS-3 volume can have 32 physical extents.

**Caution:** By running this option, you lose all data that previously existed on the SCSI device you specified in <extension-device>.

**Listing the attributes of a VMFS volume**

```
-P --queryfs
- h --human-readable
```

This option lists the attributes of the specified VMFS volume when used on any file in a directory that resides on the VMFS volume. The listed attributes include the VMFS version number (VMFS-2 or VMFS-3), the number of extents comprising the specified VMFS volume, the volume label if any, the UUID, and a listing of the SCSI device names where each extent comprising the VMFS volume resides.

You can specify the `-h` suboption with the `-P` option. If you do so, vmkfstools lists the capacity of the volume in a more readable form — for example, 5k, 12.1M, or 2.1G.

**Migrating a VMFS from VMFS-2 to VMFS-3**

```
-T --tovmfs3
```

This option converts the VMFS volume on the specified partition from VMFS-2 format to VMFS-3 format, while preserving all files in the volume. This option performs the conversion in place, and you must be sure the auxiliary file system driver module (fsaux) is loaded before issuing the vmkfstools command with this option. Here are some other guidelines you should consider before using the `-T` option:

- Back up the VMFS-2 volume that is being converted.
- Be sure there are no powered-on virtual machines using this VMFS-2 volume.
- (SAN only) Be sure no other ESX Server is accessing this VMFS-2 volume.
- (SAN only) Be sure this VMFS-2 volume is not mounted on any other ESX Server.
As a precaution, the ESX Server file-locking mechanism attempts to ensure that no remote ESX Server or local process is accessing the VMFS volume that is being converted. The conversion may take several minutes and signals completion by returning the command line prompt.

**Caution:** The VMFS-2 to VMFS-3 conversion is a one-way process. Once the VMFS volume is converted to VMFS-3, you cannot revert it back to a VMFS-2 volume.

**Virtual Disk Options**

Virtual disk options are tasks that you may perform when setting up, migrating, and managing virtual disks. You can also perform some of these tasks through the VI Client.

**Creating a virtual disk with the specified size on the file system**

```
-c --createvirtualdisk <size> [kK|mM|gG]
-a --adaptertype [buslogic|lsilogic]
```

This option creates a virtual disk at the specified path on a VMFS volume. You need to specify the size of the virtual disk. When entering the size for `<size>`, you can indicate the unit type by adding a suffix of `k` (kilobytes), `m` (megabytes), or `g` (gigabytes). The unit type is not case sensitive — in other words `vmkfstools` interprets either `k` or `K` to mean kilobytes. If you don’t specify a unit type, `vmkfstools` defaults to kilobytes.

You can specify the `-a` suboption with the `-c` option. This option specifies the device driver that will be used to communicate with the virtual disks. You can choose between BusLogic and LSI Logic SCSI drivers. By default, virtual machines use the BusLogic adapter. However, Windows Server 2003 virtual machines are configured to use the LSI Logic adapter by default.

**Deleting files associated with a virtual disk**

```
-U --deletevirtualdisk
```

This option deletes a file or files associated with the virtual disk listed at the specified path on the VMFS volume.

**Renaming files associated with a virtual disk**

```
-E --renamevirtualdisk <srcfile> <dstfile>
```

This option renames a file associated with the virtual disk listed in the path specification portion of the command line. For the `-E` option to work, you must indicate the original filename `<srcfile>` and define the new filename `<dstfile>`.
Appendix B: Using vmkfstools

Exporting the contents of a virtual disk file

```
-e --exportfile <dstfile> <srcfile>
```

This option exports the contents of the virtual disk file to a VMware Workstation format virtual disk on the service console. After the export, you can transfer the virtual disk to another server machine and import it to a VMFS volume or raw device mapping on the remote machine.

If your virtual disk has redo logs, you have the following options:

- If you use the `exportfile` option on the base virtual disk, only the base virtual disk is exported. Any uncommitted redo logs are not exported but can be copied out separately.
- If you use the `exportfile` option on an ESX Server redo log, the exported virtual disk contains the redo log, any previously created redo logs, and the base virtual disk. That is, the newly created exported virtual disk appears as if the redo log(s) was committed to its base virtual disk. However, your original source redo log(s) and base virtual disk remain unchanged.
- If you want to export your redo logs and base virtual disk separately, then use the `exportfile` option to export the base virtual disk and the `cp` command to export each redo log separately.

Use the combination of `exportfile` and `importfile` to copy VMFS files to remote machines. The virtual disk should take less space than the full size of the VMFS file, since the virtual disk does not include zeroed sectors of the VMFS file.

Importing the contents of a virtual, plain, or raw disk

```
-i --importfile <srcfile>
-d --diskformat
   [rdm:<device> | rdmp:<device> | raw:<device>]
```

This option imports the contents of a virtual, plain, or raw disk file (specified by `<srcfile>`) on the service console to a file at the specified path of the VMFS volume. This command is used to import the contents of a VMware Workstation virtual disk into a VMFS disk format. You can also run this command to import a virtual disk created by exporting the contents of a virtual disk from another VMFS volume.

The complete contents of the source disk are copied even if the source disk contained mostly free space, so ensure that the destination VMFS file system has enough space to accommodate the imported virtual disk file.

You can specify the `-d` suboption for the `-i` option. This suboption specifies the compatibility mode of the file that you are importing:
• Specify rdm if you are importing the file to a raw disk mapping that is set up for virtual compatibility mode.

• Specify rdmp if you are importing the file to a raw disk mapping that is set up for physical compatibility mode.

• Specify raw if you are importing the file to a raw device mapping that is set up for no particular compatibility.

When entering the <device> parameter, use the following format:

```
/vmfs/devices/disks/vmbaW:X:Y:Z
```
Where W:X:Y:Z is as described in vmkfstools Syntax When Specifying a SCSI Device on page 278.

**Note:** If you want to import your redo logs, use the cp command to import each redo log separately.

**Extending the specified VMFS to the specified length**

- `<X>` --extendvirtualdisk <size>[kK|mM|gG]

This option extends the size of a disk allocated to a virtual machine after the virtual machine has been created. The virtual machine that uses this disk file must be powered off when you enter this command. Also, the guest operating system must be able to recognize and use the new size of the disk, for example by updating the file system on the disk to take advantage of the extra space.

You specify the `<size>` parameter in kilobytes, megabytes, or gigabytes by adding a suffix of k (kilobytes), m (megabytes), or g (gigabytes), respectively. The unit type is not case sensitive — in other words, vmkfstools interprets either k or K to mean kilobytes. If you don't specify a unit type, vmkfstools defaults to kilobytes.

**Migrate VMFS-2 format virtual disk files to VMFS-3 format virtual disk files**

- `<M>` --migrate virtual disks

This option converts the specified virtual disk file from VMFS-2 format to VMFS-3 format.

**Mapping a raw disk to a file on a VMFS-3 volume**

- `<r>` --createrdm <device>

This option maps a raw disk to the specified virtual disk file on a VMFS-3 volume. Once this mapping is established, you can access the raw disk as you would a normal VMFS file. The file length of the mapping is the same as the size of the raw disk or partition. The mapping can be queried for the SCSI device name by using the --q option.

When entering the <device> parameter, specify the entire raw disk:
Appendix B: Using vmkfstools

`/vmfs/devices/disks/vmhbaW:X:Y:0`

Where W:X:Y:0 is as described in vmkfstools Syntax When Specifying a SCSI Device on page 278. The final zero indicates that the command will operate across the entire disk.

**Note:** All VMFS-3 file-locking mechanisms apply to raw disk mappings.

**List the attributes of a raw disk mapping**

```
-q --queryrdm <rdm_file>
```

This option lets you list the attributes of a raw disk mapping.

**Map a pass-through raw disk to avoid SCSI command filtering**

```
-z --createrdmpassthru <device>
```

This option lets you map a pass-through raw disk to a file on a VMFS volume. This mapping lets the virtual machine bypass VMkernel SCSI command filtering for VMFS files and can increase processing speed. Once you establish this type of mapping, you can use it to access the raw disk just as you would any other VMFS file. When entering the `<device>` parameter, specify the entire raw disk:

`/vmfs/devices/disks/vmhbaW:X:Y:0`

Where W:X:Y:0 is as described in vmkfstools Syntax When Specifying a SCSI Device on page 278. The final zero indicates that the command will operate across the entire disk.

**Create a raw disk descriptor file**

```
-Q --createrawdevice <device>
```

This option creates a raw disk device file on a VMFS volume. When entering the `<device>` parameter, use the following format:

`/vmfs/devices/disks/vmhbaW:X:Y:Z`

Where W:X:Y:Z is as described in vmkfstools Syntax When Specifying a SCSI Device on page 278.

**Device Options**

Device options let you perform administrative tasks for the virtual disks and SCSI disks you are working with. You can also perform some of these tasks through the VI Client.

**Scanning the specified vmhba adapter for devices and LUNs**

```
-s --scan <PC_SCSI_adapter>
```

This option scans a specified adapter for newly added or changed LUNs. The `-s` option is especially useful for adapters connected to storage area networks,
particularly if you are reconfiguring your SAN. If a new LUN becomes accessible through the adapter, then ESX Server registers this new device for use by virtual machines. If an existing LUN is no longer used and appears to be gone, then it is removed from use by virtual machines.

**Note:** If you want to scan all adapters, use the following command:

```
-s --scan
```

You can see the results of the scan by using `ls /vmfs/devices/disks`.

**Managing SCSI reservations of physical targets or LUNs**

```
-L --lock [reserve|release|lunreset|targetreset|busreset] <device>
```

This option lets you reserve a SCSI LUN for exclusive use by an ESX Server host, release a reservation so that other hosts can access the LUN, and reset a reservation, forcing all reservations from the target to be released.

**Caution:** Be careful when using the `-L` option because it can interrupt the operations of other servers on a storage area network (SAN). Use the `-L` option only in the context of clustering.

You can specify the `-L` option in several ways:

- `-L reserve` — Reserves the specified LUN. After the reservation, other servers will get a SCSI reservation error if they attempt to access that LUN, but the server that issued the reservation will be able to access the LUN normally.
- `-L release` — Releases the reservation on the specified LUN. Any other server can access the LUN again.
- `-L lunreset` — Performs a SCSI reset for the specified LUN. The reset clears any reservation on the LUN and makes the LUN available to all servers again. The reset does not affect any of the other LUNs on the device. If another LUN on the device is reserved, it remains reserved.
- `-L targetreset` — Performs a SCSI reset for a target. The reset clears any reservations on all the LUNs associated with that target and makes the LUNs available to all servers again.
- `-L busreset` — Performs a SCSI reset for all accessible targets on the bus. The reset clears any reservation on all the LUNs and makes them available to all servers again.

When entering the `<device>` parameter, use the following format:

```
/vmfs/devices/disks/vmhbaW:X:Y:0
```
Appendix B: Using vmkfstools

Where $W:X:Y:0$ is as described in `vmkfstools Syntax When Specifying a SCSI Device` on page 278.

**Displaying disk geometry for a VMware Workstation**

```
-g --geometry <srcfile>
```

The output is in the form: `Geometry information C/H/S is 1023/128/32`, where $C$ represents the number of cylinders, $H$ represents the number of heads, and $S$ represents the number of sectors.

When importing VMware Workstation virtual disks to ESX Server, you may see a disk geometry mismatch error message. A disk geometry mismatch may also be the cause of problems loading a guest operating system or running a newly created virtual machine.

You can compare the information listed by the `vmkfstools -g` option with information displayed in the VI Client by selecting the virtual machine on the VI Client inventory panel and looking at the events log on the Users and Events page. For information on using the VI Client, see the `Virtual Infrastructure User's Guide`.

If the disk geometry information is different, then specify the correct information by copying the results of the `vmkfstools -g` command to the configuration file of the newly created virtual machine.
Examples Using vmkfstools

This section includes examples using the vmkfstools command with the different options described previously.

Create a new VMFS-3 file system

```
vmkfstools -C vmfs3 -b 1m -S myvmfs vmhba1:3:0:1
```

This example illustrates creating a new VMFS-3 file system named myvmfs on the first partition of target 3, LUN 0 of SCSI adapter 1. The file block size is 1MB.

Add a partition to VMFS-3 file system

```
vmkfstools -Z vmhba0:1:2:4 vmhba1:3:0:1
```

This example illustrates extending the logical file system by allowing it to span to a new partition. The extended file system spans two partitions — vmhba1:3:0:1 and vmhba0:1:2:4.

Create a new file

```
vmkfstools -c 2000m /vmfs/volumes/mydisk/rh6.2.vmdk
```

This example illustrates creating a two-gigabyte virtual disk file named rh6.2.vmdk on the VMFS file system. This file represents an empty disk and can be accessed by a virtual machine.

Importing the contents of a virtual disk into a file

```
vmkfstools -i ~/vms/nt4.vmdk /vmfs/volumes/myvolume/nt4.vmdk
```

This example illustrates importing the contents of a virtual disk from the host file system to a file named nt4.vmdk on the volume with myvolume. You can configure a virtual machine to use this virtual disk by adding lines to the virtual machine configuration file, as in the following example:

```
scsi0.virtualDev = buslogic
scsi0:0.present = TRUE
scsi0:0.fileName = /vmfs/volumes/<volumelabel>/nt4.vmdk
```

To learn how to add lines to the virtual machine configuration file, see the Virtual Machine Management Guide.
Mapping a raw disk to a file

```
vmkfstools -r /vmfs/devices/disks/vmhba1:3:0:0 mymap_rdm.dsk
```

This example illustrates creating file named `mymap_rdm.dsk` and maps the `vmhba1:3:0:0` raw disk to that file. You can configure a virtual machine to use the `mymap_rdm.dsk` mapping file just as you would in the previous example.

Scan an adapter for changes

```
vmkfstools -s vmhba1
```

This example illustrates scanning the `vmhba1` adapter to determine whether any new targets or LUNs have been added. This command also determines if any targets or LUNs have been removed.
Index

A
accessing storage 78
active failover paths 100
adapters
  Fibre Channel 93
adding
  groups to ESX Server hosts 216
  users to ESX Server hosts 213
  users to groups 217
adding datastores 88
Administrator role 210
authenticating
  groups 207
  users 206
authentication daemon 204
C
certificates
  certificate file 219
  configuring ESX Server searches 220
  disabling SSL for VI Web Access and SDK 221
  key file 219
  location 219
certification 171
Challenge Handshake Authentication Protocol 112
changing
  password aging for ESX Server 239
  password aging for users and groups 239
  proxy services for ESX Server 222
  service console password plugin 244
  SSH configuration 250
CHAP authentication
  disabling 112
  enabling 112
CHAP parameters 109
checking authentication for iSCSI adapters 198
CIM and firewall ports 185
closing ports in the service console firewall 236
command reference for ESX Server 269
configuring
  delegate user 226
  ESX Server certificate searches 220
  password complexity 243
  password reuse rules 242
D
DAS firewall port for ESX Server 180
datastores 76
  adding 88
  naming 88
dead failover paths 100
deadend user 226
deployments for security 256
determining the firewall security level for the service console 235
disabled failover paths 100
disabling
  authentication for iSCSI adapters 200
  cut and paste for guest operating systems 262
  logging for guest operating systems 265, 266
  SSL for VI Web Access and SDK 221
dynamic discovery 109
E
enabling paths for failover 98
enabling paths for load balancing 98
encryption
  and enabling and disabling SSL 219
  for user name, passwords, and packets 219
ESX Server
  adding groups 216
  adding users 213
  architecture and security features 160
  authentication 204
  authentication for iSCSI storage 197
  changing proxy services 222
  cipher strength for connections 246
  command reference 269
delegate user 226
deployments and security 256
host to host firewall ports 185
password restrictions 238
security overview 160
users 204
virtual switch security 190
VLAN security 190
ESX Server host passwords
aging 238
changing the plugin 244
complexity 240
configuring password complexity 243
configuring password reuse rules 242
new password criteria 240
esxcfg commands 269
exporting ESX Server host users and groups 212
F
failover paths
mode 100
status 100
failovers 97
I/O interruption 102
Fibre Channel adapters 93
Fibre Channel storage 93
adding 94
firewall ports
and encryption 219
backup agents 234
CIM 185
configured with a VirtualCenter Server 176
configured without a VirtualCenter Server 179
determining the firewall security level for the service console 235
for connecting the virtual machine console 183
for management access 180
FTP 185
host to host 185
iSCSI software client 185
license server and VirtualCenter Server 176
management 185
NFS 185
NIS 185
opening and closing for the service console 236
opening with the VI Client 185
overview 174
SDK and the virtual machine console 183
security level 234
service console 234
setting the security level for the service console firewall 235
SMB 185
SNMP 185
SSH 185
supported services 185
VI Client and the virtual machine console 183
VI Client and VirtualCenter Server 176
VI Client direct connection 179
VI Web Access and the virtual machine console 183
VI Web Access and VirtualCenter Server 176
VI Web Access direct connection 179
fixed paths 101
FTP and firewall ports 185
G
groups
adding to ESX Server hosts 216
authentication 207
exporting a group list 212
Groups table for ESX Server hosts 212
modifying on ESX Server hosts 217
removing from ESX Server hosts 218
viewing group lists 212
guest operating systems
disabling cut and paste 262
disabling logging 265, 266
security recommendations 262
H
hardware-initiated iSCSI storage 103
configuring 106
HBA failover 97
HTTP and HTTPS firewall port 180

I

ISCSI
.authenticating 197
.CHAP 197
.checking authentication 198
.configuring CHAP authentication 199
.disabling authentication 200
.firewall port for ESX Server 180
.protecting transmitted data 201
.QLlogic iSCSI adapters 197
.security 197
.software client and firewall ports 185

iSCSI adapters
.rescanning 128
.iSCSI alias 109
.iSCSI hardware adapters
.configuring 109
.iSCSI hardware-initiated storage
.adding 112
.iSCSI initiator 109
.iSCSI securing ports 201
.iSCSI software-initiated storage
.configuring 117
.iSCSI storage
.hardware-initiated 103
.software-initiated 103

isolation
.virtual machine 161
.virtual networking layer 165
.virtual switches 165
.VLANs 165

L

license server
.firewall ports for 180
.firewall ports with VirtualCenter Server 176
.load balancing 98
.local SCSI storage 88
.adding 88

M

management access
.firewall ports 180
.modifying
.groups on ESX Server hosts 217
.users on ESX Server hosts 215
.MRU paths 101
.multipathing 97
.multiple paths 97
.managing 98
.viewing 98

N

NAS 129
.firewall port for ESX Server 180
.Nessus 252
.networks
.security 188
.NFS
.delegate users 226
.firewall ports 185
.NIS and firewall ports 185
.No Access role 210

O

.opening ports in the service console firewall 236

P

pam_cracklib.so plugin 240
.pam_passwdqc.so plugin 244
.password restrictions
.aging 238
.complexity 240
.for the ESX Server host 238
.minimum length 240

permissions
.and privileges 208
.overview 208
.root user 208
.VirtualCenter administrator 208
.vpxuser 208
.preventing malicious device disconnection 264
.privileges
.and permissions 208
proxy services and encryption 219
changing 222

R
Read Only role 210
removing
groups from ESX Server hosts 218
users from ESX Server hosts 216
users from groups 217
resource guarantees and security 161
resource limits and security 161
roles
Administrator 210
and permissions 210
default 210
No Access 210
Read Only 210
root login
delegate user 226
permissions 208
SSH 250
RPMs 252

S
SAN storage devices 93
SCSI
vmkfstools 277
SDK and firewall ports for connecting to the virtual machine console 183
security
CHAP authentication 197
cipher strength 246
delegate user 226
direct access users 206
encryption 219
ESX Server architecture 160
example, DMZ in a single ESX Server host 166, 168
forged transmissions 194
groups 207
iSCSI storage 197
MAC address changes 194
overview of users, groups, permissions, and roles 206
PAM authentication 204
password restrictions for the ESX Server host 238
patches 252
permissions 208
promiscuous mode 194
recommendations for virtual machines 262
roles 210
scanning software 252
security certificates 219
service console firewall security level 234
service console security measures 164
setgid applications 247
setuid applications 247
SSH connections 250
user authentication 204
user management 204
virtual machines 161
virtual network 188
virtual networking layer 165
VirtualCenter users 206
virtualization layer 160
VLAN hopping 190
VLANs 188
VMkernel 160
VMware policy 171
vmware-authd 204
service console
direct connections 233
logging on 233
password restrictions 238
recommendations for securing 231
remote connections 233
securing with VLANs and virtual switches 190
security 164
setgid applications 247
setuid applications 247
SSH connections 250
setgid applications 247
setting security level for the service console firewall 235
setting up CHAP authentication for iSCSI adapters 199
setuid applications 247
SMB and firewall ports 185
SNMP and firewall ports 185
software-initiated iSCSI storage 103
SP failover 97
SSH
changing configuration 250
firewall ports 185
security settings 250
standby failover paths 100
static discovery 109
storage
access for virtual machines 78
basic concepts 74
configuration tasks 84
devices 78
failover 97
Fibre Channel 93
fixed paths 101
iSCSI 103
local SCSI drive 88
MRU paths 101
multipathing 97
securing with VLANs and virtual switches 190
types 77
storage adapters 109
viewing in VI Client 81
storage devices 78
viewing in VI Client 80
storage type
selecting 88
T
TCP ports 180
third-party software support policy 171
Tomcat Web service 164
U
UDP ports 180
users
adding to ESX Server hosts 213
authentication 206
direct access users 206
exporting a user list 212
from Windows domain 206
modifying on ESX Server hosts 215
removing from ESX Server hosts 216
Users table for ESX Server hosts 212
viewing user list 212
VirtualCenter users 206

VI Client
firewall ports for connecting to the virtual machine console 183
firewall ports for direct connection 179
firewall ports with VirtualCenter Server 176

VI Web Access
and ESX Server services 219
disabling SSL 221
firewall ports for connecting to the virtual machine console 183
firewall ports for direct connection 179
firewall ports with VirtualCenter Server 176
viewing ESX Server host users and groups 212

virtual machines
configuring a delegate user 226
delegate user 226
disabling copy and paste 262
disabling logging 265, 266
isolation example 166, 168
preventing device disconnection 264
resource reservations and limits 161
security 161
security recommendations 262
virtual networking layer and security 165

virtual switches
802.1Q and ISL tagging attacks 192
and iSCSI 201
double-encapsulated attacks 192
forged transmissions 194
MAC address changes 194
MAC flooding 192
multicast brute-force attacks 192
promiscuous mode 194
random frame attacks 192
scenarios for deployment 256
security 192
spanning tree attacks 192

VirtualCenter Server
firewall ports 176
permissions 208
virtualization layer and security 160
VLANs
and iSCSI 201
Layer 2 security 190
scenarios for deployment 256
security 188
VLAN hopping 190
VMFS
sharing 256
vmkfstools 277
VMkernel
security 160
vmkfstools
device options 285
examples of usage 288
file system options 280
overview 277
syntax 278
virtual disk options 282
VMotion
firewall port 180
securing with VLANs and virtual switches 190