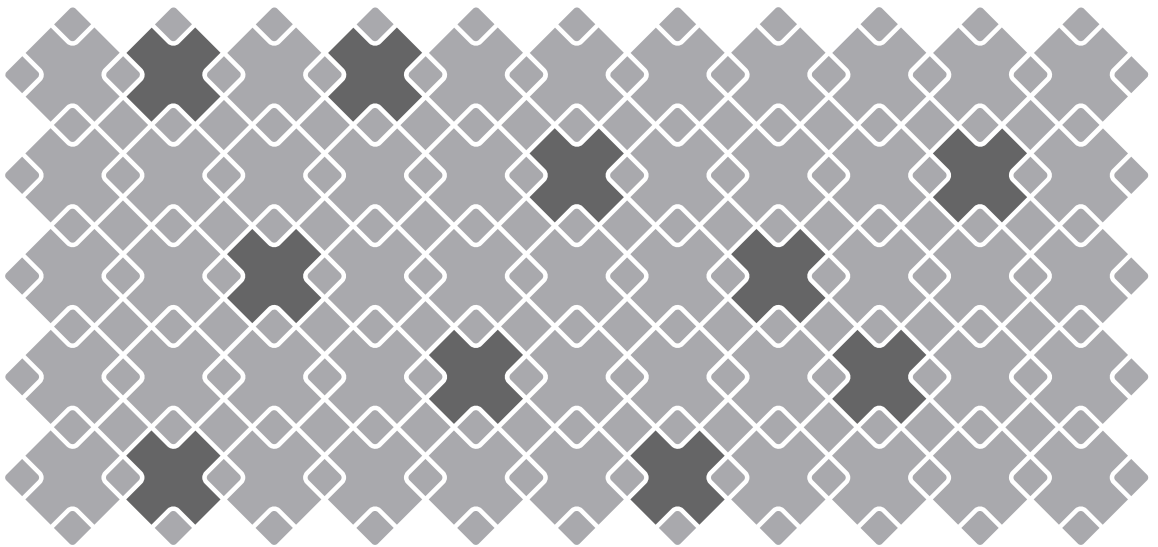


Administration Guide

VMware Server 1.0



VMware Server Administration Guide

Revision: 20060706

Item: SVR-ENG-Q206-226

You can find the most up-to-date technical documentation at:

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

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

© 2006 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, 6,795,966, 6,880,022, 6,961,941, 6,961,806 and 6,944,699; 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.

All other marks and names mentioned herein may be trademarks of their respective companies.

VMware, Inc.

3145 Porter Drive
Palo Alto, CA 94304
www.vmware.com

Contents

Chapter 1 Introduction and System Requirements	1
VMware Server Overview	1
Features of VMware Server	2
Support for 32-bit and 64-bit Guest Operating Systems	2
Two-Way Virtual SMP (Experimental Support)	2
Connect to VMware GSX Virtual Machines and Hosts	2
Upgrade and Use GSX Virtual Machines	3
Move Existing Virtual Machines	3
Compatible with VMware Workstation 5.x Virtual Machines	3
Configure Virtual Hardware Devices to be Automatically Detected	3
Take and Revert to Snapshots in the Background	3
Support for VMware Virtual Machine Importer	3
Support for VirtualCenter	4
APIs Included with VMware Server	4
Before You Install the Release	4
Host System Requirements	5
Server Host Hardware	5
Windows Host Operating System Requirements	7
Linux Host Operating System Requirements	7
Remote Client Requirements	10
Virtual Machine Specifications	12
Supported Guest Operating Systems	15
Hardware Requirements for 64-bit Guest Operating Systems	15
Hardware Requirements for 32-bit Guest Operating Systems	17
Technical Support Resources	20
Self-Service Support	20
Online and Telephone Support	20
Support Offerings	20
Reporting Problems	21
Log Files	22

Chapter 2 Installing VMware Server	25
Selecting Your Host System	25
About the VMware Server Console on the Server	26
Installing VMware Server on a Windows Host	26
Basic Installation	28
Default Directories	30
Installation Steps	30
Installing VMware Server on a Linux Host	36
Basic Installation	37
Default Directories	39
Installation Steps	40
Before Installing VMware Management Interface on a Linux Host	43
Installing the VMware Management Interface on a Linux Host	44
Installing an X Server	45
Before You Install on a SUSE Linux Enterprise Server 8 Host	45
Configuring Web Browsers for Use with VMware Server	46
Launching the VMware Server Console from the VMware Management Interface on an Encrypted Server	46
Connecting to the VMware Management Interface on a Proxy Server	47
Launching Help in Netscape on a Linux System	48
Installing the VMware Server Console	48
Installing the VMware Server Console on a Windows Host	49
Installing the VMware Server Console on a Linux Host	50
Installing the VMware APIs	51
Installing VmPerl and VmCOM APIs on a Windows Host	52
Installing VmPerl API on a Linux Host	54
Uninstalling VMware Server	55
Uninstalling VMware Server on a Windows Host	55
Uninstalling VMware Server on a Linux Host	57
 Chapter 3 Migrating from GSX Server to VMware Server	 59
Preparing for the Migration	59
Before You Install VMware Server	59
When You Remove a VMware Product and Install VMware Server	62
Migrating to VMware Server on a Windows Host	62
Migrating to VMware Server on a Linux Host	63
Using Virtual Machines Created with VMware GSX Server	64
Creating Everything New from the Start	65

Using a Legacy Virtual Machine Without Upgrading Virtual Hardware	65
Upgrading the Virtual Hardware on a Legacy Virtual Machine	65
Upgrading Virtual Hardware	66
Using Virtual Machines Created with Workstation 5.x	75

Chapter 4 Managing Virtual Machines and the VMware

Server Host	77
Remotely Managing Virtual Machines	77
Changing the Port Number for VMware Server Console Connections	78
Downloading the VMware Server Console	81
Securing Virtual Machines and the Host	82
Understanding Permissions and Virtual Machines	83
Authenticating Users and Running Virtual Machines for a Windows Host	85
Authenticating Users and Running Virtual Machines for a Linux Host	88
Checking Permissions in the VMware Management Interface	90
Securing Your Remote Sessions	90
Identifying a Virtual Machine by Its UUID	92
Specifying a UUID for a Virtual Machine	93
Logging VMware Server Events on Windows	94
Backing Up Virtual Machines and the VMware Server Host	95
Using a Backup Agent in the Virtual Machine	95
Using a Backup Agent Running on the Host Operating System	96
Backing Up the VMware Server Host	96
Considerations for Backing Up Virtual Machines	97
Using the VMware Management Interface	97
Setting the Session Length for the VMware Management Interface	99
Logging On to the VMware Management Interface	99
Using the Status Monitor	101
Configuring a Virtual Machine	105
The Apache Server and the VMware Management Interface	111
Logging Off the VMware Management Interface	111
Deleting Virtual Machines	111
Deleting a Virtual Machine Using the VMware Server Console	112
Configuring the VMware Server Host	112
Securing Remote Connections with SSL	112
Configuring Startup and Shutdown Options for Virtual Machines	113
Setting User Preferences for the VMware Server Host	117
Setting Global Preferences for VMware Server	123

Creating Network Labels	125
Setting MIME Type to Launch the VMware Server Console	128
Using VirtualCenter to Manage Virtual Machines	131
Creating Virtual Machines from a VirtualCenter Client	131
Connecting to a Virtual Machine from a VirtualCenter Client	131
Chapter 5 Moving and Sharing Virtual Machines	133
Moving a VMware Server Virtual Machine	133
Virtual Machines Use Relative Paths	134
Preparing Your Virtual Machine for the Move	134
Moving a Virtual Machine to a New Host	135
Moving VMware GSX Server 3 Virtual Machine to a New Host	136
Virtual Machines Use Relative Paths	137
Preparing Your Virtual Machine for the Move	137
Moving a Virtual Machine to a New Host	138
Moving Older Virtual Machines	138
Virtual Machines May Use Relative or Absolute Paths	139
Preparing Your Virtual Machine for the Move	139
Preparing the New Host Machine	140
Considerations for Moving Disks in Undoable Mode	141
Sharing Virtual Machines with Other Users	142
Chapter 6 Performance Tuning and the VMware Server Host 145	
Configuring and Maintaining the Host Computer	145
Location of the Working Directory	145
Defragmentation of Disk Drives	145
Adequate Free Disk Space	146
NIC Interrupts Coalescing	146
Configuring VMware Server	146
General VMware Server Options	147
VMware Server on a Windows Host	151
VMware Server on a Linux Host	154
Understanding Memory Usage	154
Memory Use on the Host	155
Specifying How Much RAM is Used by All Running Virtual Machines ...	155
Memory Usage on Older Linux Hosts	157

Chapter 7 Using High-Availability Configurations	161
Using SCSI Reservation to Share SCSI Disks with Virtual Machines	161
SCSI Reservation Support	162
Enabling SCSI Reservation	162
Issues to Consider When Sharing Disks	164
Overview of Clustering with VMware Server	165
Applications That Can Use Clustering	166
Clustering Software	166
Creating a Cluster in a Box	167
Configuring Virtual Machines for Cluster in a Box	168
Creating a Two-Node Cluster with Microsoft Clustering Services	169
Using Network Load Balancing with VMware Server	175
Overview of Network Load Balancing Clusters	175
Creating a Multinode Network Load Balancing Cluster	175
Creating Two-Node Clusters Using Novell Clustering Services	179
Creating the First Node's Base Virtual Machine	180
Creating the Second Node in the Cluster	181
Installing the Guest Operating System and VMware Tools	181
Adding the Shared Disks to Both Virtual Machines	181
Installing Novell Clustering Services on the Cluster Nodes	182
Clustering Using the iSCSI Protocol	183
Clustering Scenarios Using iSCSI	184
Creating and Configuring the iSCSI Initiator Virtual Machine	184
Configuring the iSCSI Target in the Cluster	185
Appendix: Mounting Virtual Disks	187
Considerations for Mounting Virtual Disks	187
Statement of Support	188
Installing the VMware DiskMount	188
Running the VMware DiskMount Utility	188
Examples Using the VMware DiskMount Utility	189
Glossary	191
Index	199

CHAPTER 1 Introduction and System Requirements

This chapter introduces you to VMware Server and covers the following topics:

- [“VMware Server Overview”](#) on page 1
- [“Features of VMware Server”](#) on page 2
- [“Host System Requirements”](#) on page 5
- [“Virtual Machine Specifications”](#) on page 12
- [“Supported Guest Operating Systems”](#) on page 15
- [“Technical Support Resources”](#) on page 20

VMware Server Overview

VMware Server is a free virtualization product for Microsoft Windows and Linux servers. It enables users to quickly provision new server capacity by partitioning a physical server into multiple virtual machines. You can use VMware Server to provision a wide variety of plug-and-play virtual appliances for commonly used infrastructure.

VMware Server supports:

- Any standard x86 hardware.
- A wide variety of Linux, NetWare, Solaris, and Windows operating systems, including 64-bit operating systems. For information about specific hardware requirements, see [VMware Knowledge Base article 1901](#) or [“Hardware Requirements for 64-bit Guest Operating Systems”](#) on page 15.
- Two-way Virtual SMP (experimental support).
- Intel Virtualization Technology (experimental support).

With VMware Server, you can:

- Provision a new server without investing in more hardware by locating multiple virtual machines on the same host.

- Run Windows and Linux operating systems and applications without software conflicts because virtual machines are completely isolated from one another and from the physical host.
- Move virtual machines from one physical host to another without having to reconfigure.
- Shorten the time for provisioning a new server by creating and deploying custom virtual machines with the VMware Server Virtual Machine Wizard.
- Move virtual machines to different physical hosts as conditions change.

For more information, see [“Features of VMware Server”](#) on page 2.

Features of VMware Server

This section provides information about key features of VMware Server.

Support for 32-bit and 64-bit Guest Operating Systems

VMware Server provides full and experimental support for virtual machines running 32-bit and 64-bit guest operating systems. For more information, see [“Supported Guest Operating Systems”](#) on page 15. The host machine—the server on which you install VMware Server—must have one of the processors that VMware Server supports. You can use a remote console running on a 32-bit machine to connect to a 64-bit host machine running 64-bit guest operating systems. For more information, see [“Hardware Requirements for 64-bit Guest Operating Systems”](#) on page 15.

Two-Way Virtual SMP (Experimental Support)

Experimental support for two-way Virtual Symmetric Multiprocessing (Virtual SMP) lets you assign two virtual processors to a virtual machine on any host machine that has at least two logical processors. VMware Server does not support guests with more than two virtual processors. You can, however, power on and run multiple dual-processor virtual machines. For more information, see [“Using Two-Way Virtual Symmetric Multiprocessing \(Experimental\)”](#) in the *VMware Server Virtual Machine Guide*.

Connect to VMware GSX Virtual Machines and Hosts

You can connect to hosts running VMware GSX Server 3 from the VMware Server Console and run virtual machines in VMware Server created under VMware GSX Server 3 as legacy machines. For information, see [“Connecting to VMware GSX Server and Older Virtual Machines”](#) in the VMware Server Virtual Machine Guide.

Upgrade and Use GSX Virtual Machines

You can upgrade the virtual hardware of virtual machines created under both VMware GSX Server 2 and 3. You must upgrade hardware of virtual machines created under GSX 2 to run them under VMware Server. For more information, see [“Upgrading the Virtual Hardware on a Legacy Virtual Machine”](#) on page 65..

Move Existing Virtual Machines

You can move virtual machines from one VMware Server host to another and from a VMware GSX Server or VMware Workstation host to a host running VMware Server. For more information, see [“Moving and Sharing Virtual Machines”](#) on page 133.

Compatible with VMware Workstation 5.x Virtual Machines

You can run virtual machines created using VMware Workstation 5.x. However, you cannot connect from a host running VMware Server to a host running VMware Workstation.

Configure Virtual Hardware Devices to be Automatically Detected

You can configure a number of virtual devices, including serial and parallel ports, DVD/CD-ROM drives, floppy drives, and sound drivers (Linux only) to be automatically detected. The benefit of auto-detect devices is that you can move them between virtual machines running different guest operating systems, such as Windows and Linux, without having to reconfigure the devices. For more information, see [“Using Devices in a Virtual Machine”](#) in the *VMware Server Virtual Machine Guide*.

Take and Revert to Snapshots in the Background

You can configure any virtual machine to take and revert to snapshots in the background. When you take a snapshot, you preserve the state of the virtual machine, including the state of the data on all the virtual machine disks and whether the virtual machine was powered on, powered off, or suspended. For more information, see [“Snapshot Actions as Background Activity”](#) in the *VMware Server Virtual Machine Guide*.

Support for VMware Virtual Machine Importer

VMware Server includes support for the VMware Virtual Machine Importer version 1.5, which lets you import virtual machines from Microsoft Virtual Server and Virtual PC as well as Symantec LiveState Recovery system images.

To access the VMware Virtual Machine Importer from the VMware Server Console, choose **File > Import** or **File > Open**. The Wizard to import a virtual machine or system image opens. You can access the VMware Virtual Machine Importer only from a Windows host machine.

For more detailed information about how to use the VMware Virtual Machine Importer, see the [VMware Virtual Machine Importer User's Manual](#).

Support for VirtualCenter

VMware Server includes support for using VirtualCenter version 1.4 to manage virtual machines running on VMware Server.

APIs Included with VMware Server

VMware Server supports the VMware scripting APIs, which include the VmPerl API and the VmCOM API, and the Programming API. All of the APIs are installed on a Windows host when you perform a complete installation using the VMware Server Windows Installer. The Programming API and VmPerl API are installed when you install the VMware Server software. You can also install any of the APIs on a client machine.

Before You Install the Release

Before you install this release, take the following steps to ensure the best possible experience with VMware Server.

If you plan to install VMware Server on a host machine that is already running any other VMware product, you must first uninstall that product. On a Microsoft Windows host, use the Add/Remove Programs control panel. On a Linux host, see your product manual for the commands needed to uninstall the product.

On a Windows host, the uninstaller asks whether you want to keep licenses in your registry. Do not remove the licenses. If you re-install the VMware product that you uninstalled, you do not need to enter the serial number again.

On a Linux host, the license remains in place. You do not need to take any special action.

VMware Server lets you connect to hosts running VMware GSX Server 3. You can either use virtual machines created using VMware GSX Server 3 in legacy mode or upgrade the virtual hardware of legacy virtual machines. To use virtual machines created using VMware GSX Server 2, you must upgrade the virtual hardware. For more information, see [“Migrating to VMware Server”](#) on page 55.

Installing VMware Tools

After you install VMware Server, it is recommended to install VMware Tools to ensure enhanced performance for your guest operating system. For more information, see [“Installing VMware Tools”](#) in the *VMware Server Virtual Machine Guide*.

Host System Requirements

You can install the VMware Server software on a Microsoft Windows or Linux server. You can store virtual machines on the server host or locate them on a network share.

Server Host Hardware

VMware Server supports up to 16-way multiprocessor servers. The number of virtual machines you can run concurrently depends on the resources they require, but VMware recommends you run no more than four virtual machines concurrently per processor. You can run a maximum of 64 virtual machines concurrently on one host.

The server host hardware includes:

- Standard x86-based server with up to 16 processors hosts with 32-bit IA-32 processors, and IA-32 processors with 64-bit extensions supported
- 733MHz or faster compatible x86 processor that supports the Pentium instruction set

Compatible processors include:

- Intel: Pentium II, Pentium III, Pentium 4, Pentium M Xeon, and EM64T.
- AMD: Athlon, Athlon MP, Athlon XP, AMD Opteron, AMD Athlon 64, Turion 64.
- Experimental support for AMD Sempron.
- Multiprocessor systems are supported.
- Dual-core processors are supported and counted as one processor for licensing.

Memory

You need enough memory to run the Microsoft Windows or Linux host operating system, plus memory required for each guest operating system and applications on the host and each guest. See your guest operating system and application documentation for their memory requirements.

Memory requirements include:

- Minimum: 512MB
- Maximum:
 - 64GB for Windows hosts and Linux hosts that support large memory or are PAE-enabled
 - 4GB for non-PAE-enabled Windows hosts or 2GB for Linux hosts with kernels in the 2.2.x series

Display

- 16-bit display adapter or higher

Host Hard Disk

- 250MB free disk space on Windows hosts required for VMware Server, VMware Management Interface, the VmPerl API, the VmCOM API, the Programming API, and VMware Server Console installation.
- 200MB free disk space on Linux hosts required for VMware Server, VMware Management Interface, VmPerl API, Programming API, and VMware Server Console installation.
 - Disk space in /tmp on Linux hosts should be equivalent to 1.5 times the amount of memory on the host. For information on the /tmp directory, read VMware knowledge base article 844 at http://www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=844.
- Sufficient free disk space for each guest operating system and the application software used with it. Using a default setup, the actual disk space needs are approximately the same as those for installing and running the guest operating system and applications on a physical computer.
- IDE or SCSI hard drives and DVD/CD-ROM drives supported.
- Guest operating systems can reside in virtual disk files or on physical (raw) disk partitions.

Local Area Networking

- Any Ethernet controller that the host operating system supports.
- Non-Ethernet networks are supported using built-in network address translation (NAT) or using a combination of host-only networking plus routing software on the host operating system.
- Static IP address for your host machine (recommended).

Windows Host Operating System Requirements

You must use a Microsoft Windows server operating system. To use the VMware Management Interface, Internet Information Server (IIS) 5.0 or 6.0 must be installed.

NOTE Operating systems and service packs that are not listed are not supported for use as a host operating system for VMware Server.

64-bit host computers can run the following operating systems for 64-bit extended systems:

- Microsoft Windows Server 2003 Enterprise, Standard, and Web Editions, R2
- Microsoft Windows Server 2003 Enterprise, Standard, and Web Editions, Service Pack 1

32-bit host computers can run the following operating systems:

- Microsoft Windows Server 2003 Enterprise, Standard, and Web Editions, R2
- Microsoft Windows Server 2003 Enterprise, Standard, Web, and Small Business Editions, including Service Pack 1
- Microsoft Windows 2000 Advanced Server, Service Pack 3 and Service Pack 4
- Microsoft Windows 2000 Server, Service Pack 3 and Service Pack 4

VmPerl API requires Perl 5.005x or higher.

VMware Management Interface requires one of these browsers:

- Internet Explorer 5.5 or 6.0 (6.0 highly recommended)
- Firefox 1.x
- Mozilla 1.x
- Netscape Navigator 7.0

NOTE VMware tests the VMware Management Interface for stability and reliability with new browser versions. VMware makes every effort to add support for new browser versions in a timely manner, but until a browser is added to the above list, its use with the product is not supported.

Linux Host Operating System Requirements

Supported distributions and kernels are listed in this section. VMware Server might not run on systems that do not meet these requirements. Platforms that are not listed are not supported.

64-bit host computers can run the following operating systems for 64-bit extended systems:

- Red Hat Enterprise Linux 3.0 AS, ES, and WS, stock 2.4.21, update 2.4.21-15, and updates 6 and 7
- Red Hat Enterprise Linux 3.0 AS, ES, and WS, update 8 (experimental support)
- Red Hat Enterprise Linux 4.0 AS, ES, and WS, including update 3
- Red Hat Enterprise Linux 4.0 update 4 (experimental support)
- SUSE Linux Enterprise Server 10 (experimental support)
- SUSE Linux Enterprise Server 9, including SP1, SP2, and SP3
- SUSE Linux 10
- SUSE Linux 10.1
- SUSE Linux 9.3
- SUSE Linux 9.2, including SP1
- SUSE Linux 9.1 stock 2.6.4-52
- Mandriva Linux 2006
- Ubuntu Linux 5.04 and 5.10
- Ubuntu Linux 6.06 (experimental support)

32-bit host computers can run the following operating systems:

- Mandriva Linux 2006
- Mandrake Linux 10.1
- Mandrake Linux 9.0 stock 2.4.19
- Red Hat Enterprise Linux 4.0 AS, ES, and WS, including updates 1,2, and 3
- Red Hat Enterprise Linux 4.0 update 4 (experimental support)
- Red Hat Enterprise Linux 3.0, updates 1, 2, 3, 4, 5, 6, and 7
- Red Hat Enterprise Linux 3.0 update 8 (experimental support)
- Red Hat Enterprise Linux 2.1 stock 2.4.9-e3
- Red Hat Linux 9.0, stock 2.4.20-8 and upgrade 2.4.20-20.9
- Red Hat Linux 8.0 stock 2.4.18
- Red Hat Linux 7.3 stock 2.4.18

- Red Hat Linux 7.2, stock 2.4.7-10 and upgrades 2.4.9-7, 2.4.9-13, 2.4.9-21, and 2.4.9-31
- SUSE Linux Enterprise Server 10 (experimental support)
- SUSE LINUX Enterprise Server 9, including SP1, SP2, and SP3
- SUSE Linux Enterprise Server 8 stock 2.4.19
- SUSE LINUX 9.3
- SUSE LINUX 9.2
- SUSE Linux 10
- SUSE Linux 10.1
- SUSE LINUX 9.1 stock 2.6.4-52
- SUSE LINUX 9.0 stock 2.4.21-99
- SUSE Linux 8.2 stock 2.4.20
- SUSE Linux 7.3
- Ubuntu Linux 5.04 and 5.10
- Ubuntu 6.06

NOTE As new Linux kernels and distributions are released, VMware modifies and tests its products for stability and reliability on those host platforms. VMware makes every effort to add support for new kernels and distributions in a timely manner, but until a kernel or distribution is added to the list, its use is not supported. Look for newer prebuilt modules in the Download section of VMware Web site. Go to <http://www.vmware.com/download>.

Other Linux host operating system requirements include:

- Linux kernel 2.2.14-5.0 is not supported.
- Standard Linux server installation is required with glibc version 2.1 or higher and libXpm.so.
- The inetd process must be configured and active for VMware Server Console and VMware Management Interface connections.
- Version 2.1.36 of the SCSI Generic (sg.0) driver is required to use generic SCSI devices in virtual machines.
- Perl 5.005x or higher is required to use VmPerl API.

- X server is required to run the VMware Server Console.

The VMware Management Interface requires one of these browsers:

- Firefox 1.x
- Mozilla 1.x
- Netscape Navigator 7.0

NOTE As new browser versions are released, VMware tests the VMware Management Interface for stability and reliability with these versions. VMware makes every effort to add support for new browser versions in a timely manner, but until a browser is added to the above list, its use with the product is not supported.

Running VMware Server on Some SUSE Linux Hosts

Keep in mind the following when you run VMware Server on these SUSE Linux hosts.

- **SLES 8** — Install gcc on your SLES 8 host before installing VMware Server.
- **SLES 7** — To upgrade the kernel, deselect any Samba components when you apply the update patch because the patch incorrectly updates Samba on your host. Running the update with the Samba packages selected can result in serious issues on your host such as system hangs or segmentation faults.

VmPerl and VmCOM APIs

The VmPerl API includes the `vmware-cmd` utility. The VmCOM API works only on Windows Server 2003, Windows XP, Windows 2000, and Windows NT clients. For more information, go to the VMware Web site at <http://www.vmware.com/support/developer>.

Programming API

VMware Server includes support for the Programming API (previously called C API). For more information, go to the VMware Web Site at http://www.vmware.com/support/pubs/server_pubs

Remote Client Requirements

The remote client is a Microsoft Windows or Linux system from which you launch the VMware Server Console or use VMware Scripting APIs to remotely manage virtual machines on the VMware Server host. You access the VMware Management Interface to manage virtual machines on the host using a Web browser.

Hardware Requirements

- Standard x86-based computer.
- 266MHz or faster processor.
- 64MB RAM minimum.
- 30MB (for Windows hosts) or 60MB (for Linux hosts) of free disk space is required for installation of the VMware Server Console.
- 17MB free disk space is required for VMware Scripting APIs (VmCOM and VmPerl APIs) installation on Windows remote clients. 14MB is required for VmPerl API on Linux remote clients.

Software Requirements – Windows Remote Client

- Windows Server 2003 x64 Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition, and Windows Server 2003 Web Edition
- Windows XP Professional and Windows XP Home Edition Service Pack 1 and Service Pack 2
- Windows 2000 Professional, Server and Advanced Server, Service Pack 1, Service Pack 2, Service Pack 3 and Service Pack 4
- Windows NT 4.0 Workstation and Server, Service Pack 6a, with Internet Explorer 6.0 installed
- The VMware Management Interface requires one of these browsers:
 - Internet Explorer 5.5 or 6.0 (6.0 highly recommended)
 - Firefox 1.x
 - Mozilla 1.x
 - Netscape Navigator 7.0

NOTE As new browser versions are released, VMware tests the VMware Management Interface for stability and reliability with these versions. VMware makes every effort to add support for new browser versions in a timely manner, but until a browser is added to the above list, its use with the product is not supported.

Software Requirements – Linux Remote Client

- Standard Linux installation is required with glibc version 2.1 or higher and one of the following kernels:

- For single-processor systems: kernel 2.0.32 or higher in the 2.0.x series, or kernel in the 2.2.x, 2.4.x or 2.6.x series.
- For SMP systems: kernel in the 2.2.x, 2.4.x or 2.6.x series

NOTE Linux kernel 2.2.14-5.0 is not supported.

- Perl 5.005x or higher is required to use VmPerl API.
- X server is required to run the VMware Server Console on the client.
- The VMware Management Interface requires one of these browsers:
 - Firefox 1.x
 - Mozilla 1.x
 - Netscape Navigator 7.0

NOTE As new browser versions are released, VMware tests the VMware Management Interface for stability and reliability with these versions. VMware makes every effort to add support for new browser versions in a timely manner, but until a browser is added to the above list, its use with the product is not supported.

VmPerl and VmCOM APIs

The VmPerl API includes the `vmware-cmd` utility. The VmCOM API works on Windows Server 2003, Windows XP, Windows 2000, and Windows NT clients only. For more information, go to the VMware Web site at <http://www.vmware.com/support/developer>.

Programming API

VMware Server includes support for the Programming API. For more information, go to the [VMware Web site at http://www.vmware.com/support/pubs/server_pubs](http://www.vmware.com/support/pubs/server_pubs).

Virtual Machine Specifications

Each virtual machine created with VMware Server provides a platform that includes the following devices that your guest operating system can see.

Virtual Processor

- Intel Pentium II or later, or AMD Athlon or later, depending on host processor; Intel EMT64VT (experimental support).

- Single and multiprocessor per virtual machine on symmetric multiprocessor (SMP) systems.

Virtual Chipset

- Intel 440BX-based motherboard with NS338 SIO chip and 82093AA IOAPIC

Virtual BIOS

- PhoenixBIOS 4.0 Release 6 with VESA BIOS
- DMI/SMBIOS-compliant for system management agent support

Virtual Memory

- Up to 3600MB of memory per virtual machine, depending upon the host system's configuration, the types of applications running on the host, and the amount of memory on the host.

Virtual Graphics

- VGA and SVGA support

Virtual IDE Drives

- Up to four devices: disks, CD-ROM or DVD (DVD drives can be used to read data DVD discs). DVD video is not supported.
- Hard disks can be virtual disks or physical disks.
- IDE virtual disks up to 950GB.
- CD-ROM can be a physical device or an ISO image file.

Virtual SCSI Devices

- Up to 60 devices on up to four virtual SCSI controllers.
- SCSI virtual disks up to 950GB.
- Hard disks can be virtual disks or physical disks.
- Generic SCSI support allows scanners, CD-ROM, DVD-ROM, tape drives, and other SCSI devices to be used without requiring drivers in the host operating system.
- Mylex (BusLogic) BT-958 compatible host bus adapter.
- LSI Logic Ultra160 LSI53C10xx SCSI controller.

Virtual PCI Slots

- Six virtual PCI slots, to be divided among the virtual SCSI controllers, virtual Ethernet cards, virtual display adapter, and virtual sound adapter.

Virtual Floppy Drives

- Up to two 1.44MB floppy devices.
- Physical drives or floppy image files.

Virtual Serial (COM) Ports

- Up to four serial (COM) ports.
- Output to serial ports, Windows files, Linux files, or named pipes.

Virtual Parallel (LPT) Ports

- Up to three bidirectional parallel (LPT) ports.
- Output to parallel ports or host operating system files.

Virtual USB ports

- Two-port USB 1.1 UHCI controller.
- Supported devices include USB printers, scanners, PDAs, hard disk drives, memory card readers, and still digital cameras.

Virtual Keyboard

- 104-key Windows 95/98 enhanced

Virtual Mouse and Drawing Tablets

- PS/2 mouse
- Serial tablet support

Virtual Ethernet Card

- Up to four virtual Ethernet cards
- AMD PCnet-PCI II compatible
- Wireless networking support with bridged and NAT networking
- PXE ROM version 2.0

Virtual Networking

- Nine virtual Ethernet switches (three configured by default for bridged, host-only and NAT networking).
- Virtual networking supports most Ethernet-based protocols, including TCP/IP, NetBEUI, Microsoft Networking, Samba, Novell NetWare, and Network File System.
- Built-in NAT supports client software using TCP/IP, FTP, DNS, HTTP, and Telnet.

Virtual Sound Adapter

- Sound output and input.
- Creative Labs Sound Blaster AudioPCI emulation. MIDI input, game controllers, and joysticks are not supported.

Supported Guest Operating Systems

The operating systems listed here have been tested in VMware Server virtual machines and are officially supported. For notes on installing guest operating systems, see the *VMware Guest Operating System Installation Guide* which is available from the VMware Web site.

VMware Server supports all guest operating systems supported by VMware Workstation 5.5. Operating systems that are not listed are not supported for use in a VMware Server virtual machine.

Hardware Requirements for 64-bit Guest Operating Systems

VMware Server supports virtual machines with 64-bit guest operating systems only on host machines that have one of the following 64-bit processors.

- AMD Athlon 64, revision D or later
- AMD Opteron, revision E or later
- AMD Turion 64, revision E or later
- AMD Sempron, 64-bit-capable revision D or later (experimental support)
- Intel EM64T VT-capable processors (experimental support)

VMware Server performs an internal check. If the host CPU is not a supported 64-bit processor, VMware Server displays an error message that indicates the hardware on your host machine is incompatible with 64-bit guest operating systems. You can, however, continue to power on the virtual machine.

VMware Server provides a standalone utility that performs the same check and determines whether your CPU is supported for VMware Server virtual machines with 64-bit guest operating systems. You can download the 64-bit processor check utility from the VMware Web site at <http://www.vmware.com/download>.

Microsoft Windows 64-bit Guest Operating Systems

- Microsoft Windows Vista (experimental support)
- Microsoft Windows Server 2003 Enterprise, Standard, and Web Editions, R2
- Microsoft Windows Server Enterprise 2003 Enterprise, Standard, and Web Editions, SP1
- Microsoft Windows XP Professional

Linux 64-bit Guest Operating Systems

- Mandriva Linux 2006
- Red Hat Enterprise Linux 3.0, including stock 2.4.21, update 2.4.21-15, and updates 6, and 7
- Red Hat Enterprise Linux 3.0, update 8 (experimental support)
- Red Hat Enterprise Linux 4.0, including update 3
- Red Hat Enterprise Linux 4.0, update 4 (experimental support)
- SUSE Linux 9.1 stock 2.6.4-52
- SUSE Linux 9.2, including SP1
- SUSE Linux 9.3
- SUSE Linux 10
- SUSE Linux 10.1
- SUSE Linux Enterprise Server 9, including SP1, SP2, and SP3
- SUSE Linux Enterprise Server 10 (experimental support)

FreeBSD

- FreeBSD 5.3 and 5.4
- FreeBSD 6.0

Sun Solaris

- Solaris 10, including update 1 and update 2 (experimental support)

Ubuntu

- Ubuntu Linux 5.04 and 5.10
- Ubuntu Linux 6.06 (experimental support)

Hardware Requirements for 32-bit Guest Operating Systems

VMware Server supports virtual machines with the following 32-bit guest operating systems.

Microsoft Windows 32-bit Guest Operating Systems

- Microsoft Windows Server 2003, including Small Business, Standard, and Web Editions
- Microsoft Windows Server 2003 Enterprise Edition, including R2
- Microsoft Windows XP Professional and Home Editions, including SP1 and SP2
- Microsoft Windows Vista (experimental support)
- Microsoft Windows 2000 Professional, including SP1, SP2, SP3, and SP4
- Microsoft Windows 2000 Server, including SP1, SP2, SP3, and SP4
- Microsoft Windows 2000 Advanced Server, SP3 and SP4 only
- Microsoft Windows NT 4.0 Server Service Pack 6a, Windows NT Workstation 4.0, including Service Pack 6a, and Windows NT 4.0 Terminal Server Edition Service Pack 6a
- Microsoft Windows Me
- Microsoft Windows 98, including all service packs
- Microsoft Windows 98 SE
- Microsoft Windows 95, including SP 1 and all OSR releases
- Microsoft Windows for Workgroups 3.11
- Microsoft Windows 3.1

Microsoft MS-DOS

- MS-DOS 6.x

Linux 32-bit Guest Operating Systems

- Mandriva Linux 2006

- Mandrake Linux 10.1
- Mandrake Linux 9.2
- Mandrake Linux 9 stock 2.4.19
- Mandrake Linux 3.2 stock 2.4.18-6mdk
- Red Hat Enterprise Linux 3.0 AS, ES, and WS, including updates 1, 2, 3, 4, 5, 6, and 7)
- Red Hat Enterprise Linux 3.0 update 8 (experimental support)
- Red Hat Enterprise Linux 4.0 AS, ES, and WS, including updates 1, 2, and 3
- Red Hat Enterprise Linux 4.0 update 4 (experimental support)
- Red Hat Enterprise Linux 2.1 AS, ES, and WS, including stock 2.4.9-e3
- Red Hat Linux 9.0, stock 2.4.20-8 and upgrade 2.4.20-20.9
- Red Hat Linux 8.0 stock 2.4.18
- Red Hat Linux 7.3 stock 2.4.18
- Red Hat Linux 7.2, stock 2.4.7-10 and upgrades 2.4.9-7, 2.4.9-13, 2.4.9-21, and 2.4.9-31
- Red Hat Linux 7.1 stock 2.4.2-2 and upgrade 2.2.3-12
- Red Hat Linux 7.0 stock 2.2.16-22 and upgrade 2.2.17-14
- SUSE Linux Enterprise Server 10 (experimental support)
- SUSE Linux Enterprise Server 9, including SP1, SP2, and SP3
- SUSE Linux Enterprise Server 8 stock 2.4.19
- SUSE Linux Enterprise Server 7 stock 2.4.7 and patch 2
- SUSE Linux 10
- SUSE Linux 10.1
- SUSE Linux 9.0 stock 2.4.21-99
- SUSE Linux 9.1 stock 2.6.4-52
- SUSE Linux 9.2, including SP1
- SUSE Linux 9.3
- SUSE Linux 8.2 stock 2.4.20
- SUSE Linux 8.1 stock 2.4.19

- SUSE Linux 8.0 stock 2.4.18
- SUSE Linux 7.3 stock 2.4.10
- Novell Linux Desktop 9, including SP2
- Novell Open Enterprise Server, including SP1
- Turbolinux Enterprise Server 8.0
- Turbolinux Server 7.0
- Turbolinux Workstation 8.0
- Turbolinux Desktop 10

Novell NetWare

- NetWare 4.2
- NetWare 5.1, SP8 only
- NetWare 6, SP 5 only
- Netware 6.5, SP3 only

FreeBSD

- FreeBSD 4.0–4.6.2
- FreeBSD 4.8
- FreeBSD 5
- Free BSD 5.1-5.3
- Free BSD 5.4
- FreeBSD 6.0

Sun Solaris

- Solaris 9 (experimental support)
- Solaris 10, including update 1 and update 2

Ubuntu

- Ubuntu Linux 5.04 and 5.10
- Ubuntu Linux 6.06

Technical Support Resources

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

- [“Self-Service Support”](#)
- [“Online and Telephone Support”](#)
- [“Support Offerings”](#)
- [“Reporting Problems”](#)
- [“Log Files”](#)

Self-Service Support

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

- Product Information — http://www.vmware.com/products/product_index.html
- Technology Information — <http://www.vmware.com/vcommunity/technology>
- Documentation — <http://www.vmware.com/support/pubs>
- Knowledge Base — <http://www.vmware.com/support/kb>
- Discussion Forums — <http://www.vmware.com/community>
- User Groups — <http://www.vmware.com/vcommunity/usergroups.html>

For more information about the VMware Technology Network, go to <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 <http://www.vmware.com/support>.

Use phone support for the fastest response on priority 1 issues for customers with appropriate support contracts. Go to 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 <http://www.vmware.com/support/services>.

Reporting Problems

If you have problems while running VMware Server, report them to the VMware support team. You must register your serial number and then you can report your problems by submitting a support request at <http://www.vmware.com/requestsupport>.

This section describes the information needed to diagnose and report problems. This information largely comes from log files. The required log files depend upon the problem you encounter.

You can simplify the process of collecting the needed information by running the support script to collect the appropriate log files and system information. Follow the steps that apply to your host computer.

NOTE The support script runs only on the VMware Server host. If you encounter problems on a remote client, you must supply the log files manually. The required log files depend on the problem encountered on the client. You should include the VMware Server Console log file and the installation log files.

To run the support script on a Windows host

- 1 Open a command prompt.
- 2 Change to the VMware Server program directory.

```
C:
cd \Program Files\VMware\VMware Server
```

If you did not install the program in the default directory, use the appropriate drive letter and substitute the appropriate path in the `cd` command above.

- 3 Run the support script.


```
cscript vm-support.vbs
```

After the script runs, it displays the name of the directory where it has stored its output.

- 4 Use a file compression utility such as WinZip or PKZIP to zip that directory, and include the zip file with your support request.

To run the support script on a Linux host

- 1 Open a terminal.
- 2 Run the support script as the user who is running the virtual machine or as root.


```
vm-support
```

If you do not run the script as root, the script displays messages indicating that it cannot collect some information. This is normal. If the VMware support team needs that information, a support representative may ask you to run the script again as root.

The script creates a compressed .tgz file in the current directory.

- 3 Include the output file with your support request.

Log Files

The following log files are generated by VMware Server and are collected by the support script as needed. Because the VMware Server Console does not include a support script, you need to submit a support request at <http://www.vmware.com/requestsupport> for any issues you encounter on a client and include the VMware Server Console's log file or its installation log files.

Virtual Machine Log File

If a virtual machine exits abnormally or crashes, run the support script or save the log file before you launch that virtual machine again.

On a Windows host, the `vmware.log` file is in the same directory as the configuration file (`.vmx`) of the virtual machine. The path to the log file of the active virtual machine is located under **Virtual Machine > Settings > Options > Advanced**.

On a Linux host, the `<vmname>.log` file is in the same directory as the configuration file (`.vmx`) of the virtual machine.

Also save any core files (`core` or `vmware-core`).

Virtual Machine Event Log File

The virtual machine's event log, some of which can be viewed in the VMware Management Interface, is stored as a file on the host. This file can also be useful in the event a virtual machine crashes.

Each virtual machine on the host includes an event log file called `event-<path_to_configuration_file>.vmx.log`.

On a Windows host, the log is stored in `C:\Program Files\VMware\VMware Server\vmserverdRoot\eventlog`.

On a Linux host, the log is stored in `/var/log/vmware`.

VMware Server Console Log File

The VMware Server Console keeps a log. If you encounter problems with the VMware Server Console on a remote client, submit a support request and this log file.

On a Windows host, the log is called `vmware-<username>-<PID>.log` and is stored in the user's TEMP directory; by default, this directory is `C:\Documents and Settings\<username>\Local Settings\Temp`. The path to this file appears in the About dialog box. In the VMware Server Console, choose **Help > About VMware Server**, and look under **Additional information**.

On a Linux host, the log is called `ui-<PID>.log` and is stored in the user's TEMP directory; by default, this directory is `/tmp/vmware-<username>`. The path to this file appears in the terminal when you start the VMware Server Console.

VMware Management Interface Log File

The VMware Management Interface keeps a log.

On a Windows host, the log is called `mui.log` and is stored by default in `C:\Program Files\VMware\VMware Management Interface`.

On a Linux host, the log is called `error_log` and is stored by default in `/var/log/vmware-mui`.

VMware Authorization Service Log File

You can manually enable logging for the VMware Authorization Service, known as `vmware-authd` on Linux hosts.

To enable logging for VMware Authorization Service

- 1 In a text editor, open the following file:
 - On a Windows host – edit `config.ini` located in `C:\Documents and Settings\All Users\Application Data\VMware\VMware Server`
 - On a Linux host – edit `/etc/vmware/config`
- 2 Add the following lines to the file:


```
vmauthd.logEnabled = TRUE
log.vmauthdFileName = "vmauthd.log"
```

A file is created called `vmauthd.log`. On a Windows host, this file appears by default in `C:\Windows\system32` or `C:\WINNT\system32`; on a Linux host, this file appears by default in `/var/log/vmware`.

- 3 Save and close the configuration file.

The log is enabled on a Linux host.

- 4 On a Windows host, choose **Start > Administrative Tools > Services**.
- 5 Right-click **VMware Authorization Service** and choose **Restart**.

The log is enabled on a Windows host.

VMware Registration Service Log File

The VMware Registration Service keeps a log.

On a Windows host, the log is called `vmware-serverd.log` and is stored in `C:\Windows\Temp`.

On a Linux host, the log is called `vmware-serverd.log` and is stored in `/var/log/vmware`.

VMware Server and VMware Server Console Installation Log Files

VMware Server keeps installation log files on the server host.

On a remote client, the VMware Server Console keeps two installation log files. If you encounter problems installing the VMware Server Console, submit a support request including the names of these log files.

On a Windows host, the files are `vminst.log` and `vmmsi.log` which are saved in your TEMP directory; the default location is `C:\Documents and Settings\\Local Settings\Temp`. The Local Settings folder is hidden by default. To see its contents, open **My Computer**, choose **Tools > Folder Options**, click the **View** tab and select **Show Hidden Files and Folders**.

On a Linux host, the log is called `locations` and is stored in `/etc/vmware`.

CHAPTER 2 **Installing VMware Server**

This chapter describes how to install VMware Server on your Linux or Windows host system and covers the following topics:

- [“Selecting Your Host System”](#) on page 25
- [“About the VMware Server Console on the Server”](#) on page 26
- [“Installing VMware Server on a Windows Host”](#) on page 26
- [“Installing VMware Server on a Linux Host”](#) on page 36
- [“Configuring Web Browsers for Use with VMware Server”](#) on page 46
- [“Installing the VMware Server Console”](#) on page 48
- [“Installing the VMware APIs”](#) on page 51
- [“Uninstalling VMware Server”](#) on page 55

Selecting Your Host System

VMware Server is available for both Windows and Linux host computers. Go to <http://www.vmware.com/download/server/> to download the software. You receive the serial numbers in an email message from VMware. The message includes one serial number for use on Windows hosts and another serial number for use on Linux hosts. Enter the serial number that is appropriate for your host operating system. To download the software again or request additional serial numbers, go to <http://www.vmware.com/download/server> and log on to receive another serial number.

To install on a supported Windows host computer, see [“Installing VMware Server on a Windows Host”](#) on page 26. To install on a Linux host computer, see [“Installing VMware Server on a Linux Host”](#) on page 36.

To review the list of supported host operating systems on which you can install VMware Server, see [“Host System Requirements”](#) on page 5.

Installing on a Computer with a Different VMware Product

You cannot install VMware Server on a computer with VMware Workstation, VMware Player, VMware ACE, or VMware GSX Server installed. If you have one of these products installed on the computer where you plan to install VMware Server, remove the existing product, and then install VMware Server. On a Windows host, use the

Add/Remove Programs control panel. On a Linux host, see your product manual for the commands needed to uninstall the product. You can connect to hosts running VMware GSX Server 3.

Upgrading to VMware Server

You can upgrade virtual machines created using VMware GSX Server 2 and 3. For more information about upgrading a host from VMware GSX Server to VMware Server, see [“Migrating from GSX Server to VMware Server”](#) on page 59.

About the VMware Server Console on the Server

VMware Server uses the VMware Server Console to manage virtual machines on any VMware Server host directly from the host or remotely from a client workstation or another host.

Multiple consoles can connect to a virtual machine at the same time, giving multiple authorized users concurrent access to the virtual machine. Similarly, multiple users can connect to the virtual machine with VMware Scripting APIs and the VMware Management Interface. You can run virtual machines in full screen mode from any console.

When you install the VMware Server software, the VMware Server Console is installed automatically. You should install the VMware Server Console on any client workstation from which you want to access virtual machines. This allows for remote management of virtual machines.

NOTE Do not mix components of VMware Server and VMware ESX Server. You cannot use the VMware Server Console from VMware ESX Server to connect to a VMware Server host, or vice versa. You can, however, use the VMware Server Console to connect to VMware GSX Server 3 hosts. To open virtual machines created on VMware GSX Server 2, you must first uninstall VMware GSX Server 2 and then install VMware Server.

To install the VMware Server Console on a client, see [“Installing the VMware Server Console”](#) on page 48. You can download the VMware Server Console from the VMware Management Interface for convenient installation on a remote client. For more information, see [“Downloading the VMware Server Console”](#) on page 81.

Installing VMware Server on a Windows Host

The following sections describe how to install VMware Server on your Windows host operating system:

- [“Basic Installation”](#) on page 28
- [“Default Directories”](#) on page 30
- [“Installation Steps”](#) on page 30

To get started with VMware Server on a Windows host

- 1 Install the VMware Server software (including VMware Management Interface, the VmCOM API, the VmPerl API, the Programming API, and the VMware Server Console) on the server.
- 2 Install the VMware Server Console and VMware Scripting APIs on Windows or Linux clients.
- 3 Start the VMware Server Console.

You are prompted to enter your serial number either during the installation process or the first time you start the VMware Server Console.

- 4 Enter the serial number only once.

NOTE You receive the serial numbers in an email message from VMware. The message includes one serial number to use on a Windows host and another serial number to use on a Linux host. Enter the serial number that is appropriate for your host operating system. To download the software again or request additional serial numbers, go to <http://www.vmware.com/download/server/>.

- 5 Create a virtual machine using the New Virtual Machine Wizard. See [“Creating a New Virtual Machine”](#).
- 6 Power on the virtual machine and install a guest operating system. You need the installation media (CD-ROM or floppy disks) for your guest operating system. See [“Installing a Guest Operating System”](#).
- 7 Install the VMware Tools package in your virtual machine for enhanced performance. See [“Installing VMware Tools”](#).
- 8 Install software in your virtual machine.
- 9 Start using your virtual machine. Use the VMware Server Console, VMware Management Interface, and VMware Scripting APIs to manage your server host and virtual machines.

Basic Installation

On a Windows host, install VMware Server from a master installer. The master installer is a convenient way to install all the components of VMware Server—the server software, the VMware Management Interface and the VMware Scripting APIs—or you can pick and choose which components to install. In addition, the VMware Server Console is always installed. All components are installed in their own directories under one master directory.

A basic installation of VMware Server uses two computers: a server hosting a number of virtual machines and a client workstation. The client communicates with the virtual machines on the server over a TCP/IP network link.

In more complex installations, one client can run multiple VMware Server Consoles, with each console managing multiple virtual machines on a separate server.

Before you begin, be sure you have:

- Server and host operating system that meet the system requirements for running VMware Server. See [“Host System Requirements”](#) on page 5.
- Remote management client and operating system that meet the system requirements for running the VMware Server remote management software. See [“Remote Client Requirements”](#) on page 10.
- VMware Server installation software that you downloaded.
- VMware Server serial number. The serial number is included in the email message you received from VMware or from the reseller from whom you purchased VMware Server.
- Installation CDs or disks for your guest operating systems.
- Internet Information Services (IIS) is installed and configured properly (necessary to use the VMware Management Interface).

Installation on the Server

A complete installation on the VMware Server host includes:

- VMware Server package for the server, which includes the tools needed to create and configure virtual machines and the VMware Server Console to view and control virtual machines.
- VMware Management Interface package, a Web server for managing virtual machines and the host from a browser. For more information, see [“Managing Virtual Machines and the VMware Server Host”](#) on page 77.

- VmCOM API package, a scripting tool that uses COM to manage virtual machines remotely. For more information, go to <http://www.vmware.com/support/developer>.
- VmPerl API package, a scripting tool that uses Perl to manage virtual machines remotely. For more information, go to <http://www.vmware.com/support/developer>.
- Programming API package. For more information, go to <http://www.vmware.com/support/developer>.

You can choose a custom installation path where you install only the packages you need. In most cases, you work directly at the server when you install the server software. You can manage and run virtual machines from the server or from any client.

Installation on a Client Workstation

In addition to a Web browser, you can install the following packages on a client:

- VMware Server Console.
- VmPerl and VmCOM APIs (the VmCOM API and the Programming API can be installed only on a Windows client).

The packages are available from the VMware Server installer (on Windows hosts only) and on the VMware Web site. The VMware Server Console is available in the VMware Management Interface. If you are installing the VMware Server Console on a Linux client, see “[Installing the VMware Server Console on a Linux Host](#)” on page 50.

The VMware Server Console can run on a remote client and on the server itself. The VMware Server Console is available in client packages for Windows (Windows 2000, Windows XP, and Windows Server 2003) and Linux.

Typically, you run the VMware Server Console and browser on a client. The browser allows access to the VMware Management Interface. The VMware Management Interface and VMware Server Console let you:

- Monitor the operation of virtual machines.
- Start, stop, reset, suspend, and resume virtual machines.

Essentially, the VMware Server Console allows you to manage virtual machines locally and remotely, while the VMware Management Interface allows you to remotely manage the server host and all the virtual machines on the host.

The VmPerl API, the VmCOM API, and the Programming API can connect to Linux and Windows hosts. However, the VmCOM API can run only on a Windows host or client. You can use the APIs to create scripts to automate management of virtual machines and the server host.

Default Directories

By default, the VMware Server components are installed into the following directories:

- The server components and the VMware Server Console are installed in
C:\Program Files\VMware\VMware Server.
- The VMware Management Interface components are installed in
C:\Program Files\VMware\VMware Management Interface.
- The VmCOM API components are installed in
C:\Program Files\VMware\VMware VmCOM Scripting API.
- The VmPerl API components are installed in
C:\Program Files\VMware\VMware VmPerl Scripting API.
- The Programming API components are installed in
C:\Program Files\VMware\VMware VIX.

You can change the directory that contains all the components, but make note of the new paths you intend to use. The instructions make use of the default paths.

Installation Steps

You cannot install VMware Server on a computer that already has any of the following VMware applications installed: VMware Workstation, VMware Player, VMware ACE, VMware GSX Server. You cannot have multiple versions of VMware Server installed on the same host. If you plan to install VMware Server on a host machine that is already running any of these VMware products, you must first uninstall that product. On a Microsoft Windows host, use the Add/Remove Programs control panel.

If you are migrating from VMware GSX Server, see [“Migrating from GSX Server to VMware Server”](#) on page 59.

CAUTION Do not use a Microsoft Windows Terminal Services session to install the server software on a host.

To automate the installation of VMware Server on a Windows host, see [“Automating the Installation of VMware Server”](#) on page 34.

To install VMware Server on a Windows host

- 1 Log on to your Microsoft Windows host as the Administrator user or as a user who is a member of the Administrators group.

NOTE On a Windows Server 2003 host, you must be logged on as a local administrator (that is, not logged on to the domain) to install VMware Server.

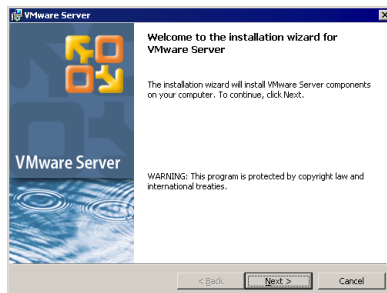
Although you must be logged on as an administrator to install VMware Server, you can run the program after it is installed as a user with normal user privileges.

NOTE A warning appears if you are installing VMware Server on a Windows host configured as an Active Directory server. You can safely ignore the message by clicking OK to continue the installation, or you can choose to cancel the installation.

- 2 Start the VMware Server installer.

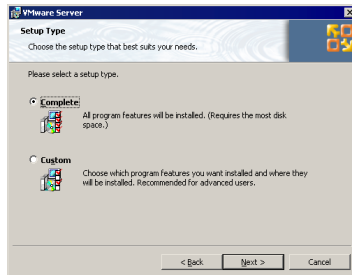
From the **Start** menu, choose **Run**, and browse to the directory where you saved the downloaded installer file (the name is similar to VMware-server-installer-**<xxxx>**.exe, where **<xxxx>** is a series of numbers representing the version and build numbers).

The installer starts.



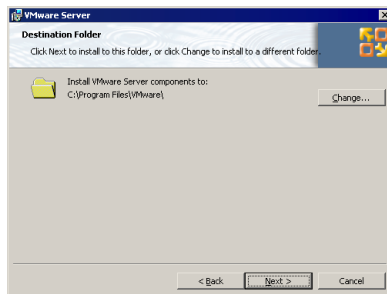
- 3 Click **Next**.
Accept the end user license agreement (EULA).
- 4 Select the **I accept the terms in the license agreement** option, and click **Next**.

5 Choose to perform a complete or a custom installation.



- A complete installation installs VMware Server, VMware Management Interface, VMware Server Console, VmCOM API, VmPerl API, Programming API, and VMware Disk Mount Utility on the host. To choose the complete installation, select **Complete**, and click **Next**.

If you want to install all the VMware Server components in a directory other than the default, click **Change** and browse to the directory of your choice. If the directory does not exist, the installer creates it for you.



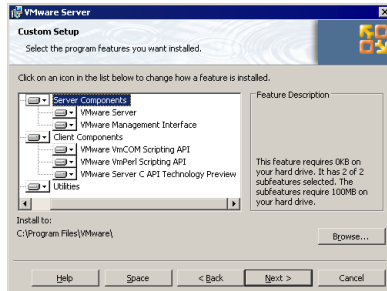
CAUTION VMware Server must be installed on a local drive, not a network drive.

Windows and the Microsoft Installer limit the length of a path to a folder to 255 characters for a path to a folder on a local drive and 240 characters for a path to a folder on a mapped or shared drive. If the path to the VMware Server program folder exceeds this limit, an error message appears. You must select or enter a shorter path.

When you are ready to continue, click **Next** and go to [Step 6](#).

- A custom installation lets you pick and choose which components to install. You can always run the installer again at a later date to install components you did not

install the first time. Select **Custom** and click **Next**. The Custom Setup screen appears.



In the Custom Setup screen, choose the components to install. Click the arrow to the left of the component you do not want to install and select the appropriate option from the menu.

If you need to determine how much free space is on your host, click **Space**. This is useful if you are choosing a custom installation due to limited disk space on your host.

If you want to install all the VMware Server components in a directory other than the default, click **Browse** and select the directory. If the directory does not exist, the installer creates it for you.

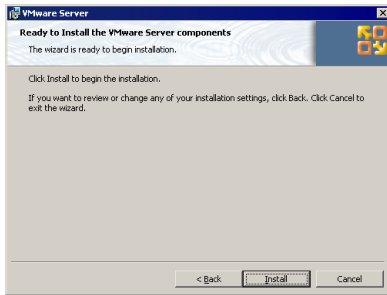
CAUTION VMware Server must be installed on a local drive, not a network drive.

Windows and the Microsoft Installer limit the length of a path to a folder to 255 characters for a path to a folder on a local drive, and 240 characters for a path to a folder on a mapped or shared drive. If the path to the VMware Server program folder exceeds this limit, an error message appears. You must select or enter a shorter path.

When you are ready to continue, click **Next**.

- 6 To change any settings or information you provided, click **Back** until you reach the screen containing the information you want to change.

Otherwise, click **Install**. The installer begins copying files to your host.



If the installer detects that the CD-ROM autorun feature is enabled, it displays a dialog box that gives you the option to disable this feature. Disabling it prevents undesirable interactions with the virtual machines you install on this system.

The installer creates one shortcut on your desktop. This shortcut gives you easy access to your virtual machines from the desktop of your host.

- 7 Click **Finish**. The VMware Server software is installed.
- 8 If you see a prompt that suggests you reboot your server, do so now to allow VMware Server to complete the installation process.

Automating the Installation of VMware Server

Use the Microsoft Windows Installer runtime engine to install the software silently (in quiet mode). If you are installing VMware Server on a number of Windows hosts, you might want to use the silent installation features.

The server on which you are installing VMware Server must have Microsoft Windows Installer runtime engine version 2.0 installed. This version is included with Windows Server 2003. If you are installing on a Windows 2000 host (or are installing the VMware Scripting APIs on a Windows NT 4.0 client), check the version of this file:

```
%WINDIR%\system32\msiexec.exe
```

If you need to upgrade the engine, run `instmsiw.exe`, which is located in the directory where you extract the installation packages; see below.

For more information on using the Microsoft Windows Installer, go to the Microsoft Web site at msdn.microsoft.com/library/default.asp?url=/library/en-us/msi/setup/about_windows_installer.asp.

To install VMware Server silently on a Windows host

- 1 Extract the individual installation packages. Open a command prompt and on one line type:

```
VMware-server-installer-1.0.0-<xxxx>.exe /a /s /v
      "TARGETDIR=C:\temp\server /qn"
```

where <xxxx> is a series of numbers representing version and build numbers.

- 2 Run the silent installation on the extracted installation packages. At the command prompt, on one line, type:

```
msiexec -i "C:\temp\server\VMware Server Standalone.msi" ADDLOCAL=ALL
      /qn
```

The installation command can be customized using standard Microsoft Windows Installer installation properties as well as any of the following:

Property Name	Description	Default
DESKTOP_SHORTCUT	Installs VMware Server shortcuts on the desktop. By default, shortcuts are installed on the desktop. To prevent shortcuts from being installed, add the following in Step 2: DESKTOP_SHORTCUT = 0	1
DISABLE_AUTORUN	Disables CD autorun on the host. By default, autorun is disabled during the installation. To enable autorun, add the following in Step 2: DISABLE_AUTORUN = 0	1
REMOVE_LICENSE	Uninstall only: Removes all stored licenses when you uninstall VMware Server. By default, VMware Server keeps the licenses on the server. To remove licenses, add the following in Step 2: REMOVE_LICENSE = 1 Caution: VMware strongly recommends you keep your licenses, in case you reinstall or upgrade your software.	0
SERIALNUMBER	Automatically enters the serial number. To enter the serial number, add the following in Step 2: SERIALNUMBER=<serialNumber>	none

The ADDLOCAL option defaults to install all VMware Server components. You can customize the installation using a combination of the ADDLOCAL and REMOVE options. You can add or remove the following components:

- ALL, which includes all the options in this list.
- Network, which includes the bridged networking adapter (vmnet0), the host-only networking adapter (vmnet1) and the NAT networking adapter (vmnet8). It also includes NAT and DHCP, but these can be removed from the installation.
- NAT, the VMware NAT Service.
- DHCP, the VMware DHCP Service.

To include a component, use it with the ADDLOCAL option.

To exclude a component, use it with the REMOVE option. You always install the bridged and host-only network adapters as part of the Network component.

For example, to install everything but the VMware NAT and DHCP services, specify on the command line:

```
ADDLOCAL=ALL REMOVE=DHCP,NAT
```

NOTE The DHCP and NAT components are children of the Network component. Thus, you also skip installation of the VMware NAT and DHCP services if you specify: ADDLOCAL=ALL REMOVE=Network

Installing VMware Server on a Linux Host

The following sections describe how to install VMware Server on your Linux host operating system:

- [“Basic Installation”](#) on page 37
- [“Default Directories”](#) on page 39
- [“Installation Steps”](#) on page 40
- [“Installing the VMware Management Interface on a Linux Host”](#) on page 44
- [“Before Installing VMware Management Interface on a Linux Host”](#) on page 43
- [“Installing an X Server”](#) on page 45
- [“Before You Install on a SUSE Linux Enterprise Server 8 Host”](#) on page 45
- [“Before You Install on a SUSE Linux Enterprise Server 8 Host”](#) on page 45

To get started with VMware Server on a Linux host

- 1 Install the VMware Server software (including VMware Management Interface, the VMware Server Console, the VmPerl API, and the Programming API on the server.
- 2 Install the VMware Server Console and VMware Scripting APIs on Windows or Linux clients.
- 3 Start the VMware Server Console and create a virtual machine using the New Virtual Machine Wizard, or create one from the VMware Management Interface. See [“Creating a New Virtual Machine”](#).
- 4 Power on the virtual machine and install a guest operating system in the new virtual machine. You need the installation media (CD-ROM or floppy disks) for your guest operating system. See [“Installing a Guest Operating System”](#).
- 5 Install the VMware Tools package in your virtual machine for enhanced performance. See [“Installing VMware Tools”](#).
- 6 Install software in your virtual machine.
- 7 Start using your virtual machine.

You can use the VMware Server Console, VMware Management Interface, and VMware Scripting APIs to manage your server host and virtual machines.

Basic Installation

A basic installation of VMware Server uses two computers: a server, hosting a number of virtual machines, and a client workstation. The client communicates with the virtual machines on the server over a TCP/IP network link.

In more complex installations, one client can run multiple instances of VMware Server Console, with each console managing multiple virtual machines on a separate server. And consoles on multiple clients can connect to virtual machines on any server.

Before you begin, be sure you have:

- A server and host operating system that meet the system requirements for running VMware Server. See [“Host System Requirements”](#) on page 5.
- A remote management client and operating system that meet the system requirements for running the VMware Server remote management software. See [“Remote Client Requirements”](#) on page 10.
- The installation CDs or disks for your guest operating systems.
- The VMware Server installation software, which is in the files you downloaded.

- Your VMware Server serial number. The serial number is included in the email message you received from VMware.

Also, before you install and run VMware Server, check the following information and make any necessary adjustments to the configuration of your host operating system:

- The real-time clock function must be compiled into your Linux kernel.
- VMware Server for Linux systems requires that the parallel port PC-style hardware option (CONFIG_PARPORT_PC) be built and loaded as a kernel module (that is, it must be set to `m` when the kernel is compiled).
- For SUSE Linux Enterprise Server 8 hosts, the `gcc` package must be installed on your host before you install VMware Server. See [“Before You Install on a SUSE Linux Enterprise Server 8 Host”](#) on page 45.

CAUTION Some operating systems, such as Red Hat Linux 7.2 and 7.3, include a firewall by default. This firewall prevents access from the VMware Server Console and the VMware Management Interface on client computers to the VMware Server host. For the VMware Server Console to connect to the host, you must open port 902. To connect to the host with the VMware Management Interface, you must open port 8333 and port 8222 if you plan to disable SSL for the VMware Management Interface.

Installation on the Server

You can install up to three software packages on the Linux server:

- The VMware Server package for the server (from an RPM or tar archive available on the VMware Server CD-ROM or the VMware Web site). The RPM file is called `VMware-server-<xxxx>.i386.rpm` and the tar archive is called `VMware-server-<xxxx>.tar.gz`, where `<xxxx>` is a series of numbers representing the version and build numbers.

NOTE The VmPerl API and the Programming API packages are installed when you install VMware Server. The VmPerl API is a scripting tool that uses Perl to manage virtual machines remotely.

- The VMware Management Interface package (from a tar archive available on the VMware Web site). This tar archive is called `VMware-mui-<xxxx>.tar.gz`.
- The VMware Server Console package (which you download from the VMware Management Interface.) The package is also available as an RPM file or as tar archive in a client GZip file that also contains the VmPerl API. The RPM and tar archives files are available on the VMware Web site. The RPM file is called

VMware-server-console-<xxxx>.i386.rpm, and the tar archive is called VMware-server-console-<xxxx>.tar.gz.

In most cases, you work directly at the server when you install the server software. You can manage and run virtual machines from the server or from any client.

Installation on a Client Workstation

In addition to a Web browser, you can install the following packages on a client:

- The VMware Server Console.
- The Programming API, the VmPerl API, and the VmCOM API (the VmCOM API can be installed only on a Windows client). For more information, go to <http://www.vmware.com/support/developer>.

The VMware Server Console is available in the VMware Management Interface. The VmPerl, VmCOM, and Programming API are available on the VMware Web site. If you are installing the VMware Server Console on a Windows client, see “Installing the VMware Server Console on a Windows Host” on page 49.

VMware Server Consoles can run on clients and on the server itself. The VMware Server Console packages are available for Windows (Windows NT 4.0, Windows 2000, Windows XP, and Windows Server 2003) and Linux.

Typically, you run the VMware Server Console and browser on a client. The browser allows access to the VMware Management Interface. The VMware Management Interface and VMware Server Console let you:

- Monitor the operation of virtual machines.
- Start, stop, reset, suspend, and resume virtual machines.
- Create and delete virtual machines.
- Configure host and virtual machine settings.

Essentially, the VMware Server Console allows you to manage virtual machines locally and remotely, while the VMware Management Interface allows you to remotely manage the server host and all the virtual machines on the host.

The VmPerl, VmCOM, and Programming API can connect to Linux and Windows hosts. However, the VmCOM API can run only on a Windows client. You can use the APIs to create scripts to automate management of virtual machines and the host.

Default Directories

By default, the VMware Server components are installed into the following directories:

- The server components are installed in

`/usr/bin`

- The VMware Management Interface components are installed in
`/usr/lib/vmware-mui`
- The VMware Server Console components are installed in
`/usr/bin`
- The Apache server components are installed in
`/usr/lib/vmware-mui/apache/bin`
(so they do not conflict with existing Apache software on your server)
- The VmPerl API executable files are installed in
`/usr/bin`
- The VmPerl API library files are installed in
`/usr/lib/vmware-api`
- The Programming API library files are installed in
`/usr/lib/vmware-vix`

If you installed the software from a tar installer, you can change these paths if you wish, but make note of the new paths you intend to use. The instructions make use of the default paths.

Installation Steps

The steps below describe an installation on a Red Hat Linux host. Start from the directory where you saved the downloaded installer file. If you are using a different Linux distribution, some of the commands might be different.

Before you install the VMware Server software, ensure your Linux distribution is for a server, not a workstation. If you are running a workstation distribution, you must install the `inetd` process to connect to the VMware Server Console and VMware Management Interface. If you need to, review the [“Host System Requirements”](#) on page 5.

If you currently have VMware GSX Server installed on your host machine, see [“Migrating from GSX Server to VMware Server”](#) on page 59. You should also read [“Before You Install the Release”](#) on page 4 before installing the software.

To install VMware Server on a Linux host

- 1 Log on to your Linux host with the user name you plan to use when running VMware Server.
- 2 In a terminal window, become root so you can perform the initial installation.
su -
- 3 Change to the directory where you saved the installer file.

Do one of the following:

- **Use the RPM installer**—Run RPM specifying the installation file.
rpm -Uvh VMware-server-<xxxx>.i386.rpm
VMware-server-<xxxx>.i386.rpm is the installation file on the CD; where <xxxx> is a series of numbers representing version and build numbers.
 - **Use the tar installer**—Complete the following steps:
 - a Copy the tar archive to a directory on your hard drive. For example, to /tmp.
cp VMware-server-<xxxx>.tar.gz /tmp where <xxxx> is a series of numbers representing the version and build numbers.
 - b Change to the directory to which you copied the file.
cd /tmp
 - c Unpack the archive.
tar xzf VMware-server-<xxxx>.tar.gz
 - d Change to the installation directory.
cd vmware-server-distrib
 - e Run the installation program.
./vmware-install.pl
 - f Accept the default directories for the binary files, daemon files, library files, manual files, documentation files, init directories and init scripts.
- 4 Run the configuration program.
vmware-config.pl
 - If you are installing VMware Server on a Mandrake Linux host, the configuration program asks for the location of lspci. When that prompt appears, enter the following path:
/usr/bin/lspcldrake
 - If you use the RPM installer, you must run the configuration program separately from the command line. If you install from the tar archive, the

installer offers to launch the configuration program for you. Answer Yes when you see the prompt.

Use this program to reconfigure VMware Server whenever you upgrade your kernel. It is not necessary to reinstall VMware Server after you upgrade your kernel.

You can also use `vmware-config.pl` to reconfigure the networking options for VMware Server—for example, to add or remove host-only networks.

- 5 Press Enter to read the end user license agreement (EULA). If the Do you accept prompt doesn't appear, press Q to get to the next prompt.
- 6 Configure networking for your virtual machines.
 - If you want to use any type of networking with virtual machines, answer Yes to this prompt: Do you want networking for your virtual machines?
 Bridged networking is always enabled if you enable networking. For more information, see [“Bridged Networking”](#).
 - To enable NAT, answer Yes to the following prompts:
 Do you want to be able to use NAT networking in your virtual machines?
 Do you want this script to probe for an unused private subnet?
 This allows you to connect your virtual machines to an external network when you have only one IP network address on the physical network, and that address is used by the host computer. For more information, see [“Network Address Translation \(NAT\)”](#).
 - To enable host-only networking, answer Yes to the following prompts:
 Do you want to be able to use host-only networking in your virtual machines?
 Do you want this script to probe for an unused private subnet?
 Host-only networking allows for networking between the virtual machine and the host operating system. For more information, see [“Host-Only Networking”](#).
- 7 Specify the port the VMware Server Console uses when connecting to the VMware Server host remotely. Port 902 is the default port. If your site uses this port for another application—for example, `ideafarm-chat` uses this port—then specify a different port for the VMware Server Console to use here. To change the port later, see [“Changing the Port Number for VMware Server Console Connections”](#) on page 78.
- 8 Specify the directory where you want to store your virtual machine files. By default, this directory is `/var/lib/vmware/Virtual Machines`. Make sure this

location is on a large enough file system to contain the files, as the virtual disk files for each virtual machine are usually gigabytes in size.

- 9 Enter your VMware Server serial number exactly as it appears (with hyphens) in the email message you received from VMware or from the reseller from whom you purchased VMware Server. When you enter the serial number, it is saved in your license file.

The configuration program displays a message saying the configuration completed successfully. If it does not display this message, run the configuration program again.

- 10 When you finish, do one of the following:
 - Log off the root account.
exit
 - Install the VMware Management Interface. Go to [Step 3](#) under “Installing the VMware Management Interface on a Linux Host” on page 44.
 - Install the VMware Server Console. Go to [Step 2](#) under “Installing the VMware Server Console on a Linux Host” on page 50.

Before Installing VMware Management Interface on a Linux Host

If you are running VMware Server on a 32-bit Linux host, you must install the `libdb.so.3` library from your Linux distribution’s CD-ROM before you install the VMware Management Interface. The version that comes with a default Linux installation is incompatible with the VMware Management Interface and returns the following error when you start the VMware Management Interface:

```
Couldn't find necessary components on your system. It appears that you are missing
the following library: libdb.so.3.
```

Some Linux distributions are known to ship without these libraries. From your Linux distribution CD, install this RPM package: `compat-db-<#>.<#>.<##>-<#>.i386.rpm` or `libdb#.deb`, where `<#>` is a version number particular to your version of the distribution.

If your distribution CD does not have this package, contact your vendor for a suitable library. If you install this package after you installed the VMware Management Interface software, start the Apache server with the following command:
`/etc/init.d/httpd.vmware start.`

Installing the VMware Management Interface on a Linux Host

The steps below describe an installation of the VMware Management Interface on a Red Hat Linux host. Start from the directory where you saved the installer file you downloaded. If you are using a different Linux distribution, some commands might be different.

NOTE You must install the `libdb.so.3` library from your Linux CD-ROM first. For more information, see [“Before Installing VMware Management Interface on a Linux Host”](#) on page 43.

To install VMware Management Interface on a Linux host

- 1 In a terminal window, become root so you can carry out the installation.
`su -`
- 2 Change to the directory where you saved the installer file.
- 3 Copy the tar archive to a directory on your hard drive (for example, to `/tmp`).
`cp VMware-mui-
<xxxx>.tar.gz /tmp`
 where `<xxxx>` is a series of numbers representing version and build numbers.

CAUTION Make sure the directory to which you plan to untar the archive does not contain any files from a previous tar installation.

Change to the directory to which you copied the file.

```
cd /tmp
```

Unpack the archive.

```
tar xzf VMware-mui-  
<xxxx>.tar.gz
```

where `<xxxx>` is a series of numbers representing version and build numbers.

- 4 Change to the installation directory.
`cd vmware-mui-distrib`
- 5 Run the installation program.
`./vmware-install.pl`
- 6 Press Enter to continue.
- 7 Accept the EULA.
- 8 Specify the directory where you want to install the management components, the binary files, VMware Management Interface files, `init` directories and `init` scripts. Or accept the default directories.
- 9 Allow the configuration program `vmware-config-mui.pl` to run.

- 10 Specify the number of minutes before a session times out. The default session length is 60 minutes.
- 11 When you finish, you can:
 - Log off the root account.
exit
 - Install the VMware Server Console. Go to [“Installing the VMware Server Console on a Linux Host”](#) on page 50.

Installing an X Server

You need an X server to run the VMware Server Console. If an X server is not installed, you must install `libxpm.so.4`, located on your Linux distribution disk.

Before You Install on a SUSE Linux Enterprise Server 8 Host

The `gcc` program is not installed on a SLES 8 host by default. This compiler is required by the VmPerl API.

Before you install VMware Server on a SLES 8 host system, you must install `gcc`.

To install gcc in the host operating system

- 1 Start your X server if it does not start by default. Log on as the root user.
- 2 Run YAST2, the default configuration utility for SLES 8.
- 3 Click **Software** in the left pane, click **Install or remove software** in the right pane.
- 4 Check **C++ Compiler and Tools** in the left pane, and click **Accept**.
- 5 When prompted, insert the SLES 8 CD.
- 6 Click **Close** to exit YAST2.

The `gcc` program is installed. Now install VMware Server.

To install the correct library, run the version of the Berkeley Database `compat-db-<#>.<#>.<##>-<#>.i386.rpm` RPM package included with your Linux distribution, as long as you install `compat-db-3.3.<##>-<#>.i386.rpm` or later.

If you installed this package after you installed the VMware Management Interface software, start the Apache server with this command:

```
/etc/init.d/httpd.vmware start
```

Configuring Web Browsers for Use with VMware Server

To run the VMware Management Interface in Internet Explorer 6.0 on a Windows system, you must take certain steps to configure Internet Explorer properly. These steps are needed whether the browser is running on a VMware Server Windows host or you are using a Windows client machine to connect to a VMware Server host.

To run the VMware Server in-product help from the VMware Server Console on a Linux system, you might need to link to the location of Netscape on the system if it is different from the location where VMware Server expects it to be.

The configuration steps allow you to perform the following activities:

- [“Launching the VMware Server Console from the VMware Management Interface on an Encrypted Server”](#) on page 46
- [“Connecting to the VMware Management Interface on a Proxy Server”](#) on page 47
- [“Launching Help in Netscape on a Linux System”](#) on page 48

Launching the VMware Server Console from the VMware Management Interface on an Encrypted Server

You can launch the VMware Server Console from the VMware Management Interface automatically. In order to do this in an Internet Explorer 6.0 browser on a Windows system where SSL is encrypting your VMware Server remote connections, you must ensure that the **Do not save encrypted pages to disk** option is disabled.

For information on encrypting remote connections, see [“Enabling and Disabling SSL for Remote Sessions”](#) on page 91.

When this option is enabled, Internet Explorer does not save any files to disk, including the files it needs to hand off to helper applications. This prevents the VMware Server Console from launching automatically. Some patches installed when you run Windows Update reset this setting, so you might need to repeat this process after you run Windows Update.

CAUTION This option might have been enabled deliberately at your site to prevent the saving of sensitive files to disk. Disabling it could permit other sensitive information to be saved to disk.

To enable the option to save encrypted pages to disk

- 1 In the Internet Explorer 6.0 window, open the Internet Options control panel. Choose **Tools > Internet Options**.
- 2 Click the **Advanced** tab.

- 3 Scroll down to the Security section, and deselect the **Do not save encrypted pages to disk** check box.
- 4 Click **OK**.

Connecting to the VMware Management Interface on a Proxy Server

If your network is protected behind a proxy server, you must take certain steps to use the VMware Management Interface in Internet Explorer 6.0 on a Windows system. Follow the steps for the appropriate Windows operating system.

To connect to the VMware Management Interface on Windows Server 2003

- 1 Launch Internet Explorer 6.0.
- 2 Choose **Tools > Internet Options**, and click the **Security** tab.
- 3 Select **Trusted sites**, and click **Sites**.
- 4 In the **Add this Web site to the zone** entry field, type
`https://*.<domain>`
where <domain> is your organization's domain name, such as vmware.com.
- 5 Click **Add**.
- 6 Click **OK** until you return to the browser window.

When you use Internet Explorer 6.0 to connect to the VMware Management Interface, be sure to use fully qualified domain names.

To connect to the VMware Management Interface on Windows 2000, Windows XP, and Windows NT operating systems

- 1 Launch Internet Explorer 6.0.
- 2 Choose **Tools > Internet Options**.
- 3 Click the **Connections** tab, and click **LAN Settings**.
- 4 Make sure that **Bypass proxy server for local addresses** is checked.
- 5 Click **OK** until you return to the browser window.

When you use Internet Explorer 6.0 to connect to the VMware Management Interface, do not use fully qualified domain names.

Connecting to the VMware Management Interface When There Is No Proxy Server

If you are on a Windows system and your network does not use a proxy server, you must use fully qualified domain names when connecting to the VMware Management Interface with Internet Explorer 6.0.

Launching Help in Netscape on a Linux System

To use VMware Server Help on a Linux system, you must have a Web browser installed on your physical computer. VMware Server expects to find the Netscape browser in `/usr/bin/netscape`. If this matches the configuration of your host computer, you do not need to take any special steps. If you are using a different browser or if your Netscape browser is in a different location, add a symbolic link to it from `/usr/bin`:

```
ln -s <path to browser> /usr/bin/netscape
```

Installing the VMware Server Console

The VMware Server Console enables you to view and control VMware Server virtual machines from a remote client or on the server host. Multiple users can use the VMware Server Console to connect to a virtual machine from the server host or from remote clients at the same time. Use the instructions below that correspond to the operating system running on your system.

The VMware Server Console can also be launched from the VMware Management Interface. If you use Netscape or Mozilla as your browser, you must configure the MIME type for the VMware Server Console. To set the MIME type, see [“Setting MIME Type to Launch the VMware Server Console”](#) on page 128. Internet Explorer is automatically configured when you install the VMware Server Console software.

CAUTION Do not install the VMware Server Console from a client installer package onto the VMware Server host. Do not download and install the VMware Server Console from an older version of VMware Server or VMware ESX Server onto any client.

The following sections describe how to install the VMware Server Console on Windows and Linux computers:

- [“Installing the VMware Server Console on a Windows Host”](#) on page 49
- [“Installing the VMware Server Console on a Linux Host”](#) on page 50

Installing the VMware Server Console on a Windows Host

On the VMware Server for Windows host, the VMware Server Console is installed automatically from the master installer when you install the VMware Server component. To upgrade the VMware Server Console on the VMware Server host, use the master installer.

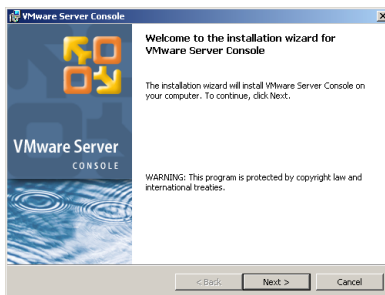
You can download the installer from the VMware Management Interface. You can run the VMware Server Console on any Windows client.

To install VMware Server Console on a Windows host

- 1 After you download the VMware Server Console installation package, go to the directory where you downloaded the installer and run `VMware-server-console-<xxxx>.exe`, where **<xxxx>** is a series of numbers representing the version and build numbers.

The InstallShield Wizard dialog box appears.

- 2 Click **Next**.



- 3 Accept the end user license agreement (EULA), and click **Next**.
- 4 Choose the directory in which to install the VMware Server Console. If you prefer to install it in a directory other than the default, click **Change** and change to your directory of choice. If the directory does not exist, it is created for you. Click **Next**.
- 5 If you want to change any settings or information you provided, click **Back** until you reach the dialog box containing the information you want to change.

Otherwise, click **Install**. The installer begins copying files to your host.

- 6 When the setup completes, click **Finish**. You do not need to reboot your host operating system after you install the VMware Server Console.

Installing the VMware Server Console on a Linux Host

This section describes an installation of the VMware Server Console on a Red Hat Linux host. Start from the directory where you saved the installer file you downloaded. If you are using a different Linux distribution, some commands might be different.

You can download the VMware Server Console installer from the VMware Management Interface. You can run the VMware Server Console on the VMware Server host or any Linux client.

To download the VMware Server Console from the VMware Management Interface, see [“Downloading the VMware Server Console”](#) on page 81.

To install VMware Server Console on a Linux host

- 1 In a terminal window, if you have not done so already, become root so you can carry out the installation steps:

```
su -
```
- 2 Change to the directory to where you saved the installer file.
 If you downloaded a .zip file from the VMware Web site, unzip the client installer archive to /tmp:

```
unzip VMware-server-linux-client-  
<xxxx>.zip -d /tmp
```

 where <xxxx> is a series of numbers representing the version and build numbers.

CAUTION To install the VMware Server Console from a tar package, make sure the directory to which you plan to untar the tar archive does not contain any files from a previous console tar installation.

- 3 Change to the /tmp directory.

```
cd /tmp
```
- 4 Do one of the following:
 - **Use the RPM installer.** Run RPM specifying the installation file.

```
rpm -Uhv VMware-server-console-  
<xxxx>.i386.rpm
```

 where <xxxx> is a series of numbers representing the version and build numbers.
 - **Use the tar installer.** Complete the following steps:
 - a Unpack the archive.

```
tar zxf VMware-server-console-  
<xxxx>.tar.gz
```

 where <xxxx> is a series of numbers representing the version and build numbers.

The archive unpacks to `vmware-server-console-distrib`.

- b Run the installer.

```
cd vmware-server-console-distrib
./vmware-install.pl
```
 - c Accept the EULA and answer the questions specifying default directories for the binary files, library files, manual files, and documentation files.
 - d If the `Do you accept` prompt doesn't appear, press `Q` to continue.
- 5 Run the configuration program `vmware-config-console.pl`.

NOTE If you use the RPM installer, you must run this program separately from the command line. If you install from the tar archive, the installer offers to launch the configuration program for you. Answer Yes when you see the prompt.

You see the following prompt: What port do you want the remote console to use to connect to server. [902]

- 6 If you specified a different port number when you installed the server software, enter that port number here. Otherwise, keep the default of 902.
- 7 When you finish, log off of the root account.

```
exit
```

Installing the VMware APIs

VMware Server supports VMware's scripting APIs which include the VmPerl API and the VmCOM API, and the Programming API. You can use these APIs to manage the VMware Server host and virtual machines locally and remotely.

The Programming API can be installed on a Windows or Linux host. For information on the Programming API and how to install it, see the API programming and reference documents.

For more information on the VMware APIs, go to <http://www.vmware.com/support/developer>.

The following sections describe how to install the scripting APIs on Windows and Linux hosts.

- ["Installing VmPerl and VmCOM APIs on a Windows Host"](#) on page 52
- ["Installing VmPerl API on a Linux Host"](#) on page 54

Installing VmPerl and VmCOM APIs on a Windows Host

On either a Windows server host or a Windows remote computer, you can use the VmPerl API or the VmCOM API. The APIs are installed automatically on the VMware Server for Windows host from the master installer if you chose a complete installation.

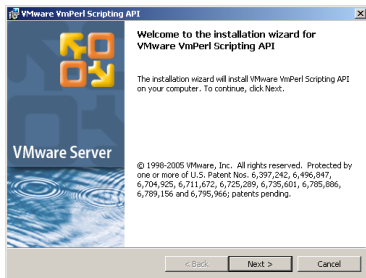
You can make the APIs available for download by customizing the download menu on the Login page of the VMware Management Interface. For more information, see [“Customizing the Download Menu”](#) on page 82.

To install the VMware Scripting APIs

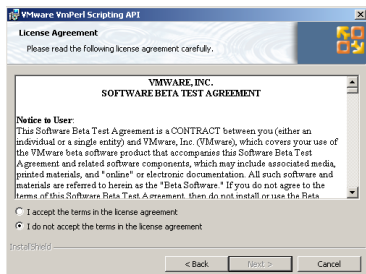
- 1 Choose **Start > Run** and browse to the directory where you saved the downloaded installer file (the name is similar to `VMware-VmPerlAPI-<xxxx>.exe` or `VMware-VmCOMAPI-<xxxx>.exe`, where `<xxxx>` is a series of numbers representing the version and build numbers).

The installer starts.

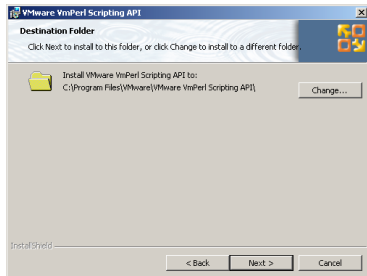
- 2 Click **Next**.



- 3 Accept the end user license agreement (EULA), and click **Next**.



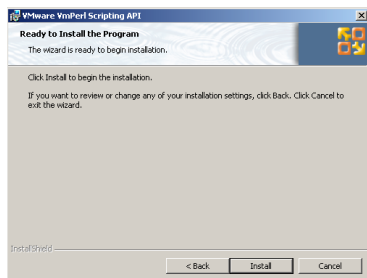
- 4 Choose the directory in which to install the scripting API. To install it in a directory other than the default, click **Change** and browse to your directory of choice. If the directory does not exist, the installer creates it for you. Click **Next**.



NOTE Windows and the Microsoft Installer limit the path length to 255 characters for a path to a folder on a local drive, and 240 characters for a path to a folder on a mapped or shared drive. If the path to the scripting API program folder exceeds this limit, an error message appears. You must select or enter a shorter path.

If you want to change any settings or information you provided, click **Back** until you reach the dialog box containing the information you want to change. Otherwise, click **Install**.

The installer begins copying files to your host.



- 5 Click **Finish**.

The VMware Scripting API is installed.

If you install the VmCOM API, two directories named MiniMUI and SampleScripts are created in the VmCOM API directory. The MiniMUI directory contains a sample

Microsoft Visual Basic 6 project that uses the VmCOM API. The `SampleScripts` directory contains VBScript and JScript samples using the VmCOM API.

If you install the VmPerl API, a `SampleScripts` directory is created in the VmPerl API directory. The `SampleScripts` directory contains sample scripts using the VmPerl API.

Installing VmPerl API on a Linux Host

On either a Linux server host or a Linux remote computer, you can use only the VmPerl API. The VmCOM API cannot be installed on a Linux host, although VmCOM API installed on a Windows remote client can communicate with a Linux host. You can make the VmPerl API tar archive available for download by customizing the download menu on the Login page of the VMware Management Interface. See [“Customizing the Download Menu”](#) on page 82.

NOTE There is no 64-bit version of the VmPerl API available for installation on a 64-bit Linux host. To use the VmPerl API with a 64-bit Linux host, install the 32-bit version of the VmPerl API on a 32-bit Linux host and use that API to control a 64-bit host.

To install the VmPerl API on a 32-bit host or client

- 1 Download the VmPerl API package from the VMware Management Interface Login page to the machine on which you want to run the VMware Scripting API.
- 2 In a terminal window, if you have not done so already, become root so you can carry out the installation steps.


```
su -
```
- 3 Untar the package.


```
tar zxf VMware-VmPerlAPI-<xxxx>.tar.gz
```

 where `<xxxx>` is a series of numbers representing the version and build numbers.
- 4 Change to the installation directory.


```
cd vmware-api-distrib
```
- 5 Run the installation program.


```
./vmware-install.pl
```
- 6 Press Enter to read the end user license agreement (EULA). You may page through it by pressing the spacebar. If the `Do you accept?` prompt doesn't appear, press `Q` to get to the next prompt. Accept the EULA.
- 7 Specify the directory where you want to install the VmPerl API executable files. The default is where Perl is installed on your host, typically `/usr/bin`.

- 8 Specify the directory where you want to install the VmPerl API library files. The default is `/usr/lib/vmware-api`.

This directory includes the sample scripts for the VmPerl API. The `SampleScripts` directory contains example scripts that demonstrate use of the VmPerl API. You can customize these scripts for your organization.
- 9 Specify the directory where you want to install the VmPerl API documentation files. These files consist of the README, end user license agreement and copyright information. The default is `/usr/share/doc/vmware-api`.
- 10 When you finish, log off of the root account.
`exit`

Uninstalling VMware Server

The following sections describe how to remove the VMware Server components from your system:

- [“Uninstalling VMware Server on a Windows Host”](#) on page 55
- [“Uninstalling VMware Server on a Linux Host”](#) on page 57

Uninstalling VMware Server on a Windows Host

To uninstall VMware Server, complete the following steps. These steps remove all the components you installed with the VMware Server master installer, including the VMware Management Interface and the VMware Scripting APIs.

To uninstall the VMware Server Console from a Windows client, see [“Uninstalling the VMware Server Console on a Windows Host”](#) on page 57.

To remove specific VMware Server components (for example, the scripting APIs or the VMware Management Interface), see [“Removing VMware Components on a Windows Host”](#) on page 56.

If you chose the custom installation path, any components you installed at that time are removed when you use the master installer to uninstall VMware Server.

To uninstall VMware Server on a Windows host

- 1 On a Windows Server 2003 host, choose **Start > Settings > Control Panel > Add or Remove Programs**. Select the **VMware Server**, and click **Remove**.

On a Windows 2000 host, choose **Start > Settings > Control Panel > Add/Remove Programs**. Select the **VMware Server**, and click **Remove**.
- 2 After the master installer launches, click **Next**.

- 3 Select **Remove**, and click **Next**.
- 4 When you are ready to begin removing VMware Server, click **Remove**.
During the uninstallation, you are asked whether you want to keep your VMware licenses in the Windows registry. VMware strongly recommends you keep your licenses, in case you reinstall or upgrade your software.
- 5 To keep the licenses in the registry, click **Yes**.
During the uninstallation, you are asked whether you want to keep any login information for any virtual machines configured to run as specific user accounts. If you choose to delete the login information, and reinstall VMware Server, any virtual machines configured to run as specific users will run as the user that powers on those virtual machines. After you decide whether to keep the login information, the uninstallation continues.
- 6 After all the components are removed, click **Finish**.
- 7 If you see a prompt that suggests you reboot your server, do so now to allow VMware Server to complete the uninstallation correctly.

Removing VMware Components on a Windows Host

With the master installer, you can choose to remove specific components from your VMware Server installation. For example, if you decide to not use the VmPerl API, you can remove only that component.

NOTE Do not use this method to remove VMware Server. Use it to remove only the VMware Scripting APIs or the VMware Management Interface.

To remove VMware components on a Windows host

- 1 On a Windows Server 2003 host, choose **Start > Settings > Control Panel > Add or Remove Programs**. Select the **VMware Server Installer** and click **Change**.
On a Windows 2000 host, choose **Start > Settings > Control Panel > Add/Remove Programs**. Select the **VMware Server Installer** and click **Change**.
- 2 After the master installer launches, click **Next**. The Program Maintenance screen appears.
- 3 Select **Modify**, and click **Next**. The Custom Setup screen appears.
- 4 Click the arrow to open the menu next to the component you want to remove, select **This feature will not be installed**, and click **Next**.
- 5 When you are ready to begin removing the component, click **Install**.

- 6 After the component is removed, click **Finish**.

Uninstalling the VMware Server Console on a Windows Host

Use the Add/Remove Programs in the Windows Control Panel to uninstall the VMware Server Console.

To uninstall the VMware Server Console on a Windows host

- 1 Choose **Start > Settings > Control Panel**.
- 2 Double-click **Add/Remove Programs** (**Add or Remove Programs** on a Windows Server 2003 host).
- 3 Select **VMware Server Console**, and click **Change**.

NOTE If the VMware Server Console was installed on Windows NT 4.0, click **Add/Remove**.

A wizard starts.

- 4 Click **Next**.
- 5 In the next screen, select **Remove**, and click **Next**.
- 6 To start removing the VMware Server Console, click **Remove**.
- 7 After the wizard finishes removing the VMware Server Console, click **Finish**.

You do not need to reboot the system after you remove the VMware Server Console.

Uninstalling VMware Server on a Linux Host

To uninstall VMware Server or any of its component, open a terminal and log on as the root user.

To uninstall VMware Server or any of its components on a Linux host

- If you used the RPM installer to install VMware Server, enter the following command to view the name of the package to uninstall:


```
rpm -qa | grep VM
```
- If you used the RPM installer to install VMware Server, remove the software from your system by running:


```
rpm -e <VMware-server package name>
```

- If you used the tar installer to install VMware Server, remove the software from your system by running:

```
vmware-uninstall.pl
```

NOTE Uninstalling the server software removes the VmPerl API and the Programming API that were installed with it.

- To uninstall the VMware Management Interface components, run the program:

```
/usr/bin/vmware-uninstall-mui.pl
```
- To uninstall a Linux console that was installed from an RPM package, type:

```
rpm -e VMware-server-console
```
- To uninstall a Linux console that was installed from a tar package, run the program:

```
/usr/bin/vmware-uninstall-server-console.pl
```
- To uninstall the VmPerl API that was installed on a remote client from a client package, type:

```
/usr/bin/vmware-uninstall-api.pl
```

CHAPTER 3 **Migrating from GSX Server to VMware Server**

This chapter describes how to migrate from VMware GSX Server to VMware Server on your Linux or Microsoft Windows host system. It also describes how to use virtual machines created with VMware GSX Server and Workstation 5.x. This chapter covers the following topics:

- [“Preparing for the Migration”](#) on page 59
- [“Migrating to VMware Server on a Windows Host”](#) on page 62
- [“Migrating to VMware Server on a Linux Host”](#) on page 63
- [“Using Virtual Machines Created with VMware GSX Server”](#) on page 64
- [“Using Virtual Machines Created with Workstation 5.x”](#) on page 75

Preparing for the Migration

The following sections describe how to prepare for the migration from VMware GSX Server to VMware Server:

- [“Before You Install VMware Server”](#) on page 59
- [“When You Remove a VMware Product and Install VMware Server”](#) on page 62

Before You Install VMware Server

Before you install or remove any VMware product from a host computer, review the information in the following sections to ensure the best possible migration experience.

Shut Down and Power Off All Virtual Machines

If you plan to use virtual machines created under VMware GSX Server, VMware Workstation 5.x, VMware Player, or VMware ACE, be sure they have been shut down completely before you uninstall the product you used to create them.

If a virtual machine is suspended, resume it in the current VMware product, shut down the guest operating system, and power off the virtual machine.

NOTE If you attempt to resume a virtual machine that was suspended under a different VMware product, a message appears, giving you the choice of discarding or keeping the file that stores the suspended state. To recover the suspended state, you must click **Preserve** and resume the virtual machine under the correct VMware product. If you click **Discard**, you can power on normally, but the suspended state is lost.

Make Sure All Disks Are in the Same Mode

If you have an existing virtual machine with one or more virtual disks, and all the disks use persistent mode, no special steps are required to upgrade.

If you have an existing virtual machine with one or more virtual disks, and all the disks use nonpersistent mode, you must take a few special steps when you upgrade VMware Tools. For details, see

http://www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=975.

Upgrading Virtual Machines with Disks in Undoable Mode

If you plan to use an existing virtual machine that has disks in undoable mode, commit or discard any changes to the virtual disks before you uninstall the product you used to create them.

NOTE VMware Server does not support undoable disks.

To upgrade a virtual machine with disks in undoable mode

- 1 Resume or power on the virtual machine in the earlier product.
- 2 Shut down the guest operating system.
- 3 Power off the virtual machine and either commit or discard changes to the disk in undoable mode when prompted.

If the disks are in persistent or nonpersistent mode, be sure the virtual machine is completely shut down. If it is suspended, resume it, shut down the guest operating system and power off the virtual machine.

Upgrading Virtual Machines with Multiple Virtual Disks

If you have an existing virtual machine that has multiple virtual disks and the disks are in multiple modes, the simplest approach to upgrading is to convert all the disks to persistent mode.

To upgrade a virtual machine with multiple virtual disks in multiple modes

- 1 Resume or power on the virtual machine in the earlier product.
- 2 Shut down the guest operating system.
- 3 Power off the virtual machine and either commit or discard changes to any undoable mode disks when prompted.
- 4 Open the Configuration Editor and change all disks to persistent mode.
- 5 After you upgrade to VMware Server, you can use the snapshot feature to preserve the state of a virtual machine and return to that state at a later time.

If you need to preserve special functionality that requires disks in multiple modes, review the information at http://vmware.com/support/kb/enduser/std_adp.php?p_faqid=976 before you upgrade.

Back Up Virtual Machines

As a precaution, back up all the files in your virtual machine directories—including the `.vmdk` or `.dsk`, `.vmx` or `.cfg` and `nvram` files—for any existing virtual machines you plan to migrate to the new version of VMware Server.

You have a choice with virtual machines that you created under VMware GSX Server 3 or updated to use the VMware GSX Server 3 virtual hardware:

- You can upgrade the virtual hardware of these virtual machines for full compatibility with VMware Server. In that case, the virtual machines can no longer be used under VMware GSX Server 3.x.
- You can choose not to upgrade the virtual hardware. In that case, you can run the virtual machines under both VMware GSX Server 3 and VMware Server, but you do not have the benefits of the new virtual hardware provided by VMware Server. Other new features are also not available.

To use virtual machines created under VMware GSX Server 2, you must upgrade the virtual hardware. After you upgrade the virtual hardware of machines created under VMware GSX Server 2, they are no longer compatible with VMware GSX Server 2.

Take Note of Custom Network Configurations

If you customized any virtual network settings or created a custom network, you must take note of these settings before you uninstall the previous version of VMware Server. Custom network settings cannot be preserved across product upgrades and must be configured again after you install the new version.

Remove Existing VMware Products

If you have VMware GSX Server, VMware Workstation, VMware Player, or VMware ACE installed on your host system, you must remove it before you install VMware Server. Also, see [“When You Remove a VMware Product and Install VMware Server”](#) on page 62.

NOTE You can run a virtual machine created with VMware Workstation 5.x on a VMware Server host, but you cannot connect remotely from a VMware Server host to a host running any version of VMware Workstation.

Make the Virtual Machine Accessible to Its Users

If the virtual machine is located on a different host or in a different directory on the VMware Server host, set permissions on the directory to make it accessible to all users of the virtual machine. For more information on permissions, see [“Securing Virtual Machines and the Host”](#) on page 82.

When You Remove a VMware Product and Install VMware Server

There is a key precaution you should take when you remove a VMware product and install VMware Server.

Leave the Existing License in Place

The installation steps for your host requires that you run an uninstaller to remove a previous version of the VMware product from your machine.

On a Windows host, the uninstaller asks whether you want to keep licenses on your system. Do not remove the licenses if you plan to use the old VMware product again. You can safely keep licenses for multiple versions of VMware products on your system at the same time.

On a Linux host, the license remains in place. You do not need to take any special action.

Migrating to VMware Server on a Windows Host

In most cases, migrating to VMware Server from VMware GSX Server is a four-step process.

To migrate to VMware Server on a Windows host

- 1 Uninstall VMware GSX Server on your system.

NOTE The uninstaller might offer to remove licenses from your registry. Do not remove the licenses.

- 2 If you are prompted, reboot your computer.
- 3 Install the latest version.
- 4 If you are prompted, reboot your computer.

Removing Versions 2 or 3

To uninstall versions 2 or 3, use the VMware GSX Server master installer. You must keep your existing license in the Windows registry.

After you reboot, follow the instructions in [“Installing VMware Server on a Windows Host”](#) on page 26.

Removing Version 1

To uninstall VMware GSX Server 1, use Add/Remove Programs in the Windows Control Panel. Be sure to uninstall VMware GSX Server, the VMware Management Interface, and the Remote Console.

After you remove the three packages, reboot your host and follow the instructions in [“Installing VMware Server on a Windows Host”](#) on page 26.

NOTE If you have VMware Workstation (or any other VMware product) installed on your host system, you must remove it before you install VMware Server. See the VMware Workstation product documentation for information on how to remove Workstation.

Migrating to VMware Server on a Linux Host

To migrate from VMware GSX Server to VMware Server, you must have the full VMware Server product. You must uninstall VMware GSX Server before installing VMware Server.

To uninstall VMware GSX Server on a Linux host

- 1 Open a terminal and log on as the root user.
- 2 If you used the RPM installer to install VMware GSX Server, remove the software from your system by running:

```
rpm -e VMware-gsx
```

If you used the tar installer to install VMware Server, remove the software from your system by running:

```
vmware-uninstall.pl
```

NOTE Uninstalling the server software removes the VmPerl API installed with it.

- To uninstall the VMware Management Interface components, run the program:
`/usr/bin/vmware-uninstall-mui.pl`
- To uninstall a Linux console that was installed from an RPM package, type:
`rpm -qa | grep -i vm` to query the package name, and then type:
`rpm -e VMware-server-console`
- To uninstall a Linux console that was installed from a tar package, run the program:
`/usr/bin/vmware-uninstall-console.pl`
- To uninstall the VmPerl API that was installed on a remote client from a client package, type:
`/usr/bin/vmware-uninstall-api.pl`

Using Virtual Machines Created with VMware GSX Server

The following sections describe how to set up older virtual machines to work with VMware Server.

- [“Creating Everything New from the Start”](#) on page 65
- [“Using a Legacy Virtual Machine Without Upgrading Virtual Hardware”](#) on page 65
- [“Upgrading the Virtual Hardware on a Legacy Virtual Machine”](#) on page 65
- [“Upgrading Virtual Hardware”](#) on page 66

Creating Everything New from the Start

Create a new virtual machine and install a guest operating system in the virtual machine as described in [“Creating a New Virtual Machine with the Virtual Machine Wizard”](#). Creating new virtual machines is the easiest way to ensure the best possible virtual machine performance.

Using a Legacy Virtual Machine Without Upgrading Virtual Hardware

A legacy virtual machine is a virtual machine created in VMware GSX Server 3 that can run on both VMware GSX Server 3 and VMware Server.

Upgrade VMware Tools to the new version, following the instructions in [“Installing VMware Tools”](#). You do not need to remove the older version of VMware Tools before installing the new version.

A legacy virtual machine set up in this way should run without problems. However, you do not have the benefits of certain new features, including better performance, improved networking, and Virtual SMP. Also, the VMware Server Console interface changes to accommodate older virtual machine features. For more information, see [“Connecting to VMware GSX Server and Older Virtual Machines”](#).

Upgrading the Virtual Hardware on a Legacy Virtual Machine

If you use an existing virtual machine and upgrade the virtual hardware, you gain access to new features, including:

- Two-way Virtual SMP (experimental)
- Support for 64-bit guest operating systems
- The ability to take and revert to snapshots in the background

NOTE You cannot reverse the process of upgrading the virtual hardware. Virtual Machines upgraded to VMware Server are incompatible with VMware GSX Server. You must upgrade all virtual machines created under VMware GSX Server 2 to use with VMware Server. It is recommended that you make backup copies of your virtual disks before beginning the upgrade.

Start by using an existing configuration file (.vmx) and virtual disk (.vmdk or .dsk).

Upgrade VMware Tools to the new version by following the instructions in [“Installing VMware Tools”](#). You do not need to remove the older version of VMware Tools before installing the new version.

NOTE When you update the virtual hardware for a Windows XP Professional or Windows Server 2003 virtual machine, the Microsoft product activation feature might require you to reactivate the guest operating system.

Upgrading Virtual Hardware

Upgrading a virtual machine's virtual hardware gives it access to new features in VMware Server. VMware Server supports upgrading virtual machines created with VMware GSX Server 2 and above and Workstation 3 and 4. VMware Server does not support upgrading the hardware of virtual machines created with VMware GSX Server 1.x. Before you upgrade the virtual hardware, however, consider the following:

- **The virtual hardware upgrade is irreversible** – The process of upgrading the virtual hardware is irreversible and makes the disks attached to this virtual machine incompatible with VMware GSX Server. You should make backup copies of your virtual disks before starting the upgrade.
- **VMware Server updates the CMOS** – If you are using a virtual machine created with VMware GSX Server 3, the first time you power on the virtual machine with VMware Server, the CMOS is updated. As a result, your guest operating system might detect hardware changes and install new drivers for the new hardware even if you do not choose to upgrade the virtual hardware.
- **An error might appear when upgrading from a physical disk** – If you are upgrading a virtual machine that runs from a physical disk, rather than a virtual disk, you might see the following error message while VMware Server is upgrading the virtual hardware: “Unable to upgrade <drivename>. One of the supplied parameters is invalid.” You can safely click **OK** to continue the upgrade process.

To upgrade the virtual machine's hardware

- 1 Shut down the guest operating system and power off the virtual machine.
- 2 Upgrade the host running GSX 2 or 3 to VMware Server.
- 3 Choose **VM > Upgrade Virtual Machine**.

A dialog box appears with a warning that the upgrade process cannot be reversed.

- 4 Click **Yes** to continue, and follow the on-screen directions.
- 5 Power on the virtual machine in VMware Server.
- 6 Upgrade VMware Tools to the new version.

Do not remove the older version of VMware Tools before installing the new version.

When you upgrade the virtual hardware on a virtual machine created using VMware GSX Server 2, you might then need to take several steps to be sure that the new virtual hardware is recognized properly by the guest operating system. If your guest operating system is listed below, the instructions for that guest operating system provide examples of the steps you might need to take to perform these updates.

These instructions do not apply to a virtual machine created using VMware GSX Server 3.

Windows 2000 Guest

The following steps provide examples of what you might see as your guest operating system recognizes the new virtual hardware. The specific steps may vary depending on the configuration of the virtual machine.

To ensure the virtual hardware is recognized by a Windows 2000 guest

- 1 Power on the virtual machine and let it update the CMOS.
Windows automatically installs the software for any devices it detects.
- 2 Install the new version of VMware Tools.
- 3 Shut down the Windows guest and power off the virtual machine.
- 4 Choose **VM > Upgrade Virtual Hardware**.
A message cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding.
- 5 To continue, click **Yes**.
A message describes what is about to happen.
- 6 Click **OK** to continue.
- 7 Power on the virtual machine.
Windows detects the PCI SVGA adapter, then it detects the VMware SVGA II adapter.
- 8 Click **Yes** to continue the installation.
A message asks you to insert a disk.
- 9 Navigate to: `C:\Program Files\VMware\drivers` to install the VMware SVGA II adapter.

- 10 If you have serial ports configured in the virtual machine, go to the Windows Device Manager and uninstall all the COM ports listed there.
- 11 Restart the virtual machine.
Windows detects the COM ports and installs them properly.

Windows NT 4.0 Guest

The following steps provide examples of what you might see as your guest operating system recognizes the new virtual hardware. The specific steps may vary depending on the configuration of the virtual machine.

To ensure the virtual hardware is recognized by a Windows NT 4.0 guest

- 1 Power on the virtual machine and let it update the CMOS.
Windows displays a message about the video driver in the guest operating system.
- 2 Click **OK**.
- 3 Install the new version of VMware Tools.
- 4 Restart the Windows guest and confirm that it is operating correctly.
- 5 Shut down the Windows guest and power off the virtual machine.
- 6 Choose **VM > Upgrade Virtual Hardware**.
A message cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding.
- 7 To continue, click **Yes**.
A message describes what is about to happen.
- 8 Click **OK** to continue.
You can now power on the virtual machine and use the new configuration.
Windows NT does not have a Plug and Play process, so no additional steps are required.

Windows XP Guest

The following steps provide examples of what you might see as your guest operating system recognizes the new virtual hardware. The specific steps may vary depending on the configuration of the virtual machine.

To ensure the virtual hardware is recognized by a Windows XP guest

- 1 Power on the virtual machine and let it update the CMOS.
- 2 Install the new version of VMware Tools.
- 3 Shut down the Windows guest and power off the virtual machine.
- 4 Choose **VM > Upgrade Virtual Hardware**.
A message cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding.
- 5 To continue, click **Yes**.
A message describes what is about to happen.
- 6 Click **OK** to continue.
- 7 Power on the virtual machine.
Windows detects the VMware SVGA adapter.
- 8 Select **Install the software automatically** and follow the on-screen instructions.
A message asks you to insert a disk.
- 9 Navigate to: C:\Program Files\VMware\drivers to install the VMware SVGA II adapter.
- 10 If you have serial ports configured in the virtual machine, go to the Windows Device Manager and uninstall all the COM ports listed there.
- 11 Restart the virtual machine.
Windows detects the COM ports and installs them properly.

Windows Me Guest

The following steps provide examples of what you might see as your guest operating system recognizes the new virtual hardware. The specific steps may vary depending on the configuration of the virtual machine.

To ensure the virtual hardware is recognized by a Windows Me guest

- 1 Power on the virtual machine and let it update the CMOS.
Plug and Play detects an Intel 82371 EB Power Management controller.
- 2 Select **Automatic search** and click **Next**.
Windows finds and installs the driver automatically.

Plug and Play detects an Intel 82443 BX Pentium II Processor to PCI bridge.

- 3 Select **Automatic search** and click **Next**.

Windows finds and installs the driver automatically.

- 4 Restart the guest operating system.

Plug and Play detects an Intel 82371 AB/EB PCI Bus Master IDE controller.

- 5 Select **Automatic search** and click **Next**.

Windows finds and install the driver automatically.

- 6 Install the new version of VMware Tools.

- 7 Shut down the Windows guest and power off the virtual machine.

- 8 Choose **VM > Upgrade Virtual Hardware**.

A message cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding.

- 9 To continue, click **Yes**.

A message describes what is about to happen.

- 10 Click **OK** to continue.

- 11 Power on the virtual machine.

Windows detects the PCI Multimedia Audio device and installs the driver for the Creative AudioPCI.

Windows detects an AMD PCNet adapter.

- 12 Select **Automatic search** and click **Next**.

Windows automatically installs the driver for the adapter.

- 13 Click **Finish** to restart the virtual machine.

Windows detects a Creative game port device and installs the driver automatically.

Windows detects a game port joystick and installs the driver.

Windows detects the PCI SVGA adapter, which it then identifies as the VMware SVGA II adapter and installs the driver automatically.

- 14 Click **Yes** to restart the virtual machine.

- 15 If you have serial ports configured in the virtual machine, go to the Windows Device Manager and uninstall all the COM ports listed there.

- 16 Restart the virtual machine.

Windows detects the COM ports and installs them properly.

Windows 98 Guest

The following steps provide examples of what you might see as your guest operating system recognizes the new virtual hardware. The specific steps may vary depending on the configuration of the virtual machine.

To ensure the virtual hardware is recognized by a Windows 98 guest

- 1 Power on the virtual machine and let it update the CMOS.
Windows detects a PCI to ISA bridge.
- 2 Go to C:\Windows\System and let Windows select the necessary driver.
Windows detects an Intel 82371EB Power Management Controller.
- 3 Go to C:\Windows\System and let Windows select the necessary file.
Windows detects lpt.vxd.
- 4 Go to C:\Windows\System and let Windows select the necessary file.
Windows detects an Intel 82443BX Pentium Processor to PCI bridge.
- 5 Go to C:\Windows\System and let Windows select the necessary file.
Windows detects an Intel 82371AB/EB PCI Bus Master IDE controller.
- 6 Go to C:\Windows\System and let Windows select the necessary file.
Windows asks for the file uhcd.sys.
- 7 Enter the location C:\Windows\System32\drivers, and click **OK**.
Windows detects an Intel 82371AB/EB PCI to USB Universal host controller.
- 8 Go to C:\Windows\System and let Windows select the necessary file.
Windows detects an AMD PCNET Family Ethernet Adapter.
- 9 Go to C:\Windows\System and let Windows select the necessary file.
Windows asks for the file inetmib1.dll.
- 10 Enter the location C:\Windows, then click **OK**.
Windows asks for the file locproxy.exe.
- 11 Enter the location C:\Windows\System, then click **OK**.

Windows asks for the file `ndishlp.sys`.

- 12 Enter the location `C:\Windows`, then click **OK**.

Windows asks for the file `wsock.vxd`.

- 13 Enter the location `C:\Windows\System`, then click **OK**.

- 14 When you finish installing the AMD Family Ethernet Adapter, restart Windows 98.

Plug and Play detects multiple devices and restarts Windows 98.

- 15 After the virtual machine restarts, install the new version of VMware Tools. For details, see [“Installing VMware Tools”](#).

- 16 Shut down the Windows guest and power off the virtual machine.

- 17 Choose **VM > Upgrade Virtual Hardware**.

A message cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding.

- 18 To continue, click **Yes**.

A message describes what is about to happen.

- 19 Click **OK** to continue.

- 20 Power on the virtual machine.

When Windows boots, it detects the PCI SVGA adapter. Later, it detects the VMware SVGA II adapter and installs the driver.

Windows detects PCI Multimedia Audio and offers to install a driver for it.

- 21 Click **Cancel**.

Windows detects an AMD PCNET Family Ethernet adapter.

- 22 Click **Next**.

- 23 Select **Search for the best driver** and click **Next**.

- 24 Select **Specify a location**, and enter `C:\Windows\System`. Click **Next**.

- 25 Select **The updated driver (Recommended) AMD PCNET Family Ethernet Adapter (PCI-ISA)**. Click **Next**.

Windows finds the `.inf` file for the adapter.

- 26 Click **Next**.

Windows asks for the file `dhcpcsvc.dll`.

- 27 Enter the location C:\Windows\System, and click **OK**.
Windows asks for the file inetmib1.dll.
- 28 Enter the location C:\Windows, and click **OK**.
Windows asks for the file locproxy.exe.
- 29 Enter the location C:\Windows\System, and click **OK**.
Windows asks for the file ndishlp.sys.
- 30 Enter the location C:\Windows, and click **OK**.
- 31 Windows asks for the file wshtcp.vxd. Enter the location C:\Windows\System, then click **OK**.
A dialog box indicates that Windows has finished installing the software.
- 32 Click **Finish**.
- 33 To install the sound adapter, follow the directions in [“Installing Sound Drivers in Windows 9x and NT Guest OS”](#).
- 34 If you have serial ports configured in the virtual machine, go to the Windows Device Manager and uninstall all the COM ports listed there.
- 35 Restart the virtual machine.
Windows detects the COM ports and installs them properly.

Windows 95 Guest

The following steps provide examples of what you might see as your guest operating system recognizes the new virtual hardware. The specific steps may vary depending on the configuration of the virtual machine.

To ensure the virtual hardware is recognized by a Windows 95 guest

- 1 Power on the virtual machine and let it update the CMOS.
Windows detects new devices and automatically installs the drivers.
- 2 Restart the guest operating system after this process is complete.
When Windows restarts, it detects more new devices.
Windows asks for the file lpt.vxd.
- 3 Enter the location C:\Windows\System, then click **OK**.
Windows detects a PCI standard host bridge and other devices.

- 4 Click **OK** to dismiss these messages. You do not need to install these drivers.
- 5 Click **Finish**.
- 6 Install the new version of VMware Tools. For details, see [“Installing VMware Tools”](#).
- 7 Shut down the Windows guest and power off the virtual machine.
- 8 Choose **VM > Upgrade Virtual Hardware**.
A message cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding.
- 9 To continue, click **Yes**.
A message describes what is about to happen.
- 10 Click **OK** to continue.
Windows detects a PCI Multimedia Audio device.
- 11 Click **Cancel**.
Windows detects a PCI Ethernet adapter, then the AMD Ethernet adapter.
Windows automatically installs the driver.
- 12 To install the sound adapter, follow the directions in [“Installing Sound Drivers in Windows 9x and NT Guest OS”](#).
- 13 If you have serial ports configured in the virtual machine, go to the Windows Device Manager and uninstall all the COM ports listed there.
- 14 Restart the virtual machine.
Windows detects the COM ports and installs them properly.

Mandrake Linux, Red Hat Linux, or SUSE Linux Guest

The following steps provide examples of what you might see as your guest operating system recognizes the new virtual hardware. The specific steps may vary depending on the configuration of the virtual machine.

To ensure the virtual hardware is recognized by a Mandrake Linux, Red Hat Linux, or SUSE Linux guest

- 1 Power on the virtual machine and let it update the CMOS.
- 2 When Kudzu appears, follow the instructions to detect new hardware and install the proper drivers.
- 3 Shut down the Linux guest and power off the virtual machine.

4 Choose **VM > Upgrade Virtual Hardware**.

A message cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding.

5 To continue, click **Yes**.

A message describes what is about to happen.

6 Click **OK** to continue.

7 Power on the virtual machine.

When Kudzu runs, it detects an Ensoniq:ES1371 [AudioPCI-97] sound device.

8 Click **Configure**.

NOTE When using Kudzu in a Mandrake Linux guest, do not migrate the existing network configuration. If you try to do so, you see a blank screen. Instead, click **No** when asked if you want to migrate the existing network configuration.

Using Virtual Machines Created with Workstation 5.x

You can run virtual machines created using Workstation 5.x on VMware Server. Virtual machines created using VMware Server are compatible with Workstation 5.x. However, virtual machines created using Workstation 5.x do not include support for multiple snapshots or teams when they are running on VMware Server.

You cannot open or configure teams when you are running a Workstation 5.x virtual machine on VMware Server. You cannot remotely connect from a VMware Server host to a host running Workstation.

CHAPTER 4 **Managing Virtual Machines and the VMware Server Host**

This chapter describes how to manage your virtual machines and the VMware Server host and covers the following topics:

- [“Remotely Managing Virtual Machines”](#) on page 77
- [“Securing Virtual Machines and the Host”](#) on page 82
- [“Identifying a Virtual Machine by Its UUID”](#) on page 92
- [“Logging VMware Server Events on Windows”](#) on page 94
- [“Backing Up Virtual Machines and the VMware Server Host”](#) on page 95
- [“Using the VMware Management Interface”](#) on page 97
- [“Deleting Virtual Machines”](#) on page 111
- [“Configuring the VMware Server Host”](#) on page 112
- [“Using VirtualCenter to Manage Virtual Machines”](#) on page 131

Remotely Managing Virtual Machines

VMware Server allows you to manage your virtual machines remotely. Any machine that can connect to your VMware Server host over an IP network can interact with virtual machines running on it.

Remote management has many components and levels. For a high-level view of your VMware Server host, use the VMware Management Interface, a Web-based tool for managing your virtual machines and the server host. For more information, see [“Using the VMware Management Interface”](#) on page 97.

To interact with a virtual machine directly from a remote location— for example, to maintain a database stored in a virtual machine—use the VMware Server Console. The VMware Server Console displays your virtual machine in a window where you interact with the virtual machine as you would interact with a physical computer.

For an automated way to remotely manage virtual machines and the VMware Server host, use the VMware Scripting APIs. If you are connecting to a VMware Server host

from a Windows remote machine, you can use the VmCOM, the VmPerl API, and the Programming API. If you are connecting to a VMware Server host from a Linux remote machine, you can use the VmPerl API and the Programming API.

Another automated way to manage virtual machines is to use the `vmware-cmd` utility. For more information, visit the VMware Web site at www.vmware.com/support/developer.

Finally, you can use third-party tools to remotely manage your virtual machines. You can use applications like VNC Viewer, Windows Terminal Services, or Windows XP Remote Desktop. To view a virtual machine with VNC Viewer, you must modify the virtual machine's configuration manually.

The following sections further explore remotely managing virtual machines:

- [“Changing the Port Number for VMware Server Console Connections”](#) on page 78
- [“Downloading the VMware Server Console”](#) on page 81

Changing the Port Number for VMware Server Console Connections

By default, the VMware Server Console connects to virtual machines via port 902. If this port assignment poses a conflict for your site—for example, if you use the `ideafarm-chat` program—you can change the port number that the console uses.

Changing the port number involves manually adding a variable to certain preference files. The steps you must take vary depending upon the server host operating system, the host on which the console is running, and whether you are making this change to VMware Server itself (by assigning the new port number to a variable called `authd.port`) or to the console (by assigning the new port number to a variable called `authd.client.port`).

The `authd.port` setting is different from the `authd.client.port` setting. The `authd.port` variable tells VMware Server (the server side) which port to listen on for console connections from remote hosts or clients. The `authd.client.port` variable tells the console (the client side) the port with which to connect. Thus, if you set only `authd.port` to a different port number, such as 9902, and you try to connect to a virtual machine on that host with a console on a remote host or client, the console still tries to connect to port 902.

You can substitute this new port number manually when you connect with a console. In the Connect to VMware Server dialog box, in the Host name field, enter the port number along with the name of the VMware Server host name and configuration file path, like this:

```
<server name>:<port> <config file>
```

Depending upon your site's needs or configuration, for example if you have multiple VMware Server hosts and they use different ports, then this might be acceptable. However, setting `authd.client.port` to the same port number you use for `authd.port` allows for seamless integration between the server and the client. It also lets you avoid manually entering the port number every time you connect to the server with a client.

To change the port number on a Windows host or client

Add the following line to `config.ini` in `C:\Documents and Settings\All Users\Application Data\VMware\VMware Server`:

```
authd.port = <portNumber>
```

where `<portNumber>` is the port number that all clients connecting to virtual machines on this host must use.

To change the port number that is used by the console installed on a Windows machine, you must create a file called `config.ini` and place it in `C:\Documents and Settings\All Users\Application Data\VMware\VMware Server Console`. In this file, add the following line:

```
authd.client.port = <portNumber>
```

where `<portNumber>` is the default port number that all clients on this machine connecting to virtual machines on the VMware Server host must use. The VMware Server host must have this port number set to the `authd.port` variable in its `config.ini` file (Windows host) or `vmware-authd` file (Linux host).

To change the port number for a specific user who is using the VMware Server Console installed on a Windows host, add the following line to the `preferences.ini` file located in `C:\Documents and Settings\<user>\Application Data\VMware`:

```
authd.client.port = <portNumber>
```

where `<portNumber>` is the port number to use only when this user is logged on and using a VMware Server Console to connect to a virtual machine on the VMware Server host.

The VMware Server host must have this port number set to the `authd.port` variable in its `config.ini` file (Windows host) or `vmware-authd` file (Linux host).

To change the port number on a Linux host or client

Determine whether your host is configured to use `xinetd` or `inetd`.

If your host is configured to use `xinetd`, look for the following line in `/etc/xinetd.d/vmware-authd`:

```
port = 902
```

Change the port number 902 in this case to the desired number.

If your host is configured to use `inetd`, look for the following line in `/etc/inetd.conf`:

```
902 ... vmware-authd
```

Change the port number 902 in this case to the desired number. All clients connecting to virtual machines on this host must use this port number.

To change the port number used by the VMware Server Console installed on a Linux host or client, add the following line to either `/etc/vmware-server-console/config` or `/usr/lib/vmware-server-console/config`:

```
authd.client.port = <portNumber>
```

where `<portNumber>` is the port number that all clients on this machine connecting to virtual machines on the VMware Server host must use. The VMware Server host must have this port number set to the `authd.port` variable in its `config.ini` file (Windows host) or `vmware-authd` file (Linux host).

NOTE If the port numbers specified in these files are different, the port number specified in `/etc/vmware-server-console/config` takes precedence.

To change the port number for a specific user who is using the VMware Server Console installed on a Linux host, add the following line to `~/.vmware/preferences`:

```
authd.client.port = <portNumber>
```

where `<portNumber>` is the port number to use only when this user is logged on and using a VMware Server Console to connect to a virtual machine on the VMware Server host.

The VMware Server host must have this port number set to the `authd.port` variable in its `config.ini` file (Windows host) or `vmware-authd` file (Linux host).

When this user is logged on, the port number specified in `~/.vmware/preferences` supersedes the port number specified in `/etc/vmware-server-console/config` or `/usr/lib/vmware-server-console/config`.

Substituting a Port Number with the VMware Scripting APIs

With the VMware Scripting APIs, you can supply a different port number when you create a new virtual machine object. This port number must match the port number set on the VMware Server host, which is set by the `authd.port` variable in the `config.ini` file (Windows host) or `vmware-authd` file (Linux host).

If you specify 0 as the port number, the console connects with the port number specified by `authd.client.port` instead. If `authd.client.port` is not specified, the console connects with the default port 902.

For more information about the VMware Scripting APIs, visit the VMware Web site at www.vmware.com/support/developer.

Downloading the VMware Server Console

You can download installation packages for the VMware Server Console from the VMware Management Interface. Packages are available for Linux and Windows hosts; download the package appropriate to the host machine on which the VMware Server Console is to be installed.

Downloading the VMware Server Console and installing it allows you to quickly manage virtual machines from the management interface.

Downloading the installer from the Status Monitor page allows you to access the console you need without logging off of the management interface.

CAUTION Do not install the VMware Server Console from the client installer package onto a host where VMware Server is installed. Do not download and install a console from VMware GSX Server or VMware ESX Server onto any client.

To download and install a VMware Server Console package from the Login or Status Monitor page

- 1 Connect to the VMware Server host with the VMware Management Interface.

For information on connecting to the management interface, see “[Logging On to the VMware Management Interface](#)” on page 99.

- 2 On the Status Monitor page, download the installer by clicking the link for the package appropriate to the operating system on which the VMware Server Console is to be installed.
- 3 On the Login page, select the installer appropriate to the operating system of the computer where you are installing the VMware Server Console, and click **Download**.

If you are installing the VMware Server Console on a Linux host, you can further choose between tar and RPM installation packages.

- 4 Run the installation package.

- To install the console on a Windows system, see [“Installing the VMware Server Console on a Windows Host”](#) on page 49.
- To install the console on a Linux system, see [“Installing the VMware Server Console on a Linux Host”](#) on page 50.

Customizing the Download Menu

You can customize the download menu on the Login page to suit your users’ needs. For example, if your site uses the VMware Scripting APIs, you can add the API installers to the download menu. Client packages containing the VMware Server Console and the VMware Scripting APIs are available in the packages you downloaded from the VMware Web site. The client packages are:

- `VMware-server-win32-client-<xxxx>.zip`
- `VMware-server-linux-client-<xxxx>.zip`

You can expand these archives and place the API installer files in a readily available area. Then modify the download menu on the Login page to point to them.

You can add more files to the download menu, hide items already listed and even hide the link or the menu itself. Click **Help** on the Login page and follow the instructions there.

On a Windows host with the VMware Management Interface installed, you can find the installers for the console and scripting APIs in `C:\Program Files\VMware\VMware Management Interface\htdocs\vmware\bin`. This folder contains:

- `VMware-server-console-<xxxx>.exe` – The installer for the VMware Server Console to run on Windows clients.
- `VMware-server-console-<xxxx>.i386.rpm` – The RPM installer for the VMware Server Console to run on Linux clients.
- `VMware-server-console-<xxxx>.tar.gz` – The tar installer for the VMware Server Console to run on Linux clients.
- `VMware-VmCOMAPI-<xxxx>.exe` – The installer for the VmCOM API for Windows hosts only.
- `VMware-VmPERLAPI-<xxxx>.exe` – The installer for the VmPerl API for Windows hosts.

Securing Virtual Machines and the Host

This section describes how you can set permissions and implement security features for your virtual machines and the server host. It includes the following topics:

- [“Understanding Permissions and Virtual Machines”](#) on page 83
- [“Authenticating Users and Running Virtual Machines for a Windows Host”](#) on page 85
- [“Authenticating Users and Running Virtual Machines for a Linux Host”](#) on page 88
- [“Checking Permissions in the VMware Management Interface”](#) on page 90
- [“Securing Your Remote Sessions”](#) on page 90

The VMware knowledge base has an article about best practices to improve security for the VMware Server host and virtual machines. For information, see http://www.vmware.com/support/kb/enduser/std_adp.php?&p_faqid=1042.

Understanding Permissions and Virtual Machines

Access to a virtual machine is based on the permissions you, as a user, are granted to the virtual machine's configuration file (.vmmx). Different permissions let you access virtual machines in different ways. These ways include:

- Browsing virtual machines.
- Interacting with virtual machines.
- Configuring virtual machines.
- Administering virtual machines and the host.

If the virtual machine is on a Windows host, permissions on more virtual machine files might be needed, depending upon the user account the virtual machine uses while running. For information, see [“Authenticating Users and Running Virtual Machines for a Windows Host”](#) on page 85.

Browsing a Virtual Machine

Browsing a virtual machine lets you connect to it with a console, but you can see only the virtual machine's power state. The virtual machine display is blank, even if the virtual machine is running. You cannot interact with the virtual machine at all.

To browse a virtual machine, you need **Read** permission for the virtual machine's configuration file on a Windows host, or read (r) permission on a Linux host.

Interacting with a Virtual Machine

Interacting with a virtual machine lets you change its power state (power on or off, suspend, or resume) and connect or disconnect removable devices. You cannot change the virtual machine's configuration. Among other restrictions, this means you cannot add or remove virtual hardware.

Your user name appears in the VMware Management Interface and in the Connected Users dialog box, which you access in the VMware Server Console by choosing **VM > Connected Users**.

To interact with a virtual machine, you must have **Read & Execute** permission for the virtual machine's configuration file on a Windows host, or read and execute (r and x) permissions on a Linux host.

Configuring a Virtual Machine

Configuring a virtual machine lets you add and remove virtual hardware to and from the virtual machine.

To configure a virtual machine, you must have **Read** and **Write** permissions for the virtual machine's configuration file and virtual machine resources (such as a physical disk or certain devices) on a Windows host, or read and write (r and w) permissions on a Linux host.

Administering Virtual Machines and the VMware Server Host

An administrator or root user can configure the VMware Server host and any virtual machines on the host. For example, you can enable SSL for client connections or change the amount of host memory allocated for all virtual machines.

To administer a virtual machine on a Windows host, your user account must be a member of the host's Administrators group. On a Linux host, you should have root access to the directories containing virtual machine files.

Alternatively, your user account can have **Read & Execute** and **Write** permissions on a Windows host, or read, write, and execute (r, w, and x) permissions on a Linux host to a particular virtual machine.

If You Have No Permissions

If you have no permissions for the virtual machine's configuration file, you cannot connect to the virtual machine at all. On a Windows host, if a permission is both allowed and denied, the denial takes precedence. If permissions are neither allowed nor denied, you are considered to have no permissions.

Only You Can See Virtual Machines You Create

When you create a new virtual machine, the virtual machine by default is private; other users cannot see or use the virtual machine. For all users to be able to use the virtual machine, follow the custom path when you create the virtual machine. You can also change the private setting in the virtual machine settings editor.

When a virtual machine is private, it appears in the inventory of the console of the user who created it. The virtual machine does not appear in the inventory of consoles for other users connected to the host. The virtual machine appears in the VMware Management Interface only when you are logged on with the account that created the virtual machine.

Other users cannot browse to the virtual machine and add it to the inventory.

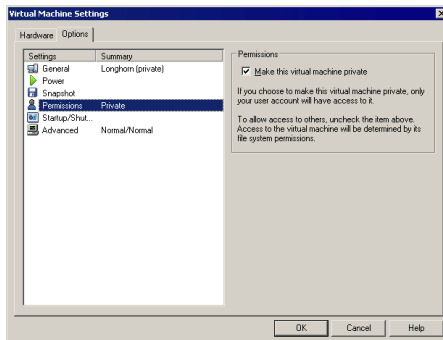
If the virtual machine is made private after it has been created, it disappears from other users' inventories.

To specify whether a virtual machine is private

- 1 Select the virtual machine in a console and choose **VM > Settings**.

The virtual machine settings editor appears.

- 2 Click the **Options** tab, and click **Permissions**.



- 3 To make the virtual machine private, select **Make this virtual machine private**.

To allow all users to see and use this virtual machine, deselect the check box.

- 4 Click **OK** to save your settings and close the virtual machine settings editor.

Authenticating Users and Running Virtual Machines for a Windows Host

Every time you connect to a VMware Server for Windows host with the VMware Server Console or VMware Management Interface, the VMware Authorization Service requests a user name and password and authenticates only valid users.

After you are authenticated, the console starts or the management interface's Status Monitor page appears. Access to a virtual machine is based on your permissions. See [“Understanding Permissions and Virtual Machines”](#) on page 83.

Each virtual machine runs as one of the following three user accounts:

- **The user who powers on the virtual machine** – The virtual machine runs as the account of the user who powered on the virtual machine until the virtual machine is powered off. Other users can connect to the virtual machine but it still runs as the user who powered on the virtual machine.
- **The local system account** – The virtual machine runs as the local system account. You can enable this option only if you are logged on to the host operating system as an Administrator.
- **A specific user account** – The virtual machine runs as the user account specified in the New Virtual Machine Wizard or the virtual machine settings editor. This account must be able to access the VMware Server host.

The user account is specified when you create the virtual machine and you can change it in the virtual machine settings editor.

Understanding Permissions and User Accounts

If the virtual machine is configured to run as the user who powers it on, the user must have **Read** and **Write** permissions to the virtual machine files, such as the configuration file, virtual disk files, and snapshot files. You must have an administrator account to access devices like physical disks, USB controllers, and generic SCSI devices.

An easy way to allow this user to access a virtual machine is to set the permissions for the directory containing the virtual machine files and let the user inherit the rights for that directory.

If another user connects to this virtual machine while it is running, that user only needs permissions for the configuration file.

For virtual machines configured to run as a specific user account or run as the local system user, any user connecting to the virtual machine needs permissions only for the configuration file.

An easy way to allow these users to access the virtual machine is to grant **Read** and **Write** permissions to all the files in the virtual machine's directory except for the configuration file. Grant **Read & Execute** permission to the configuration file and disallow the inheritance of permissions on the file.

Changing the User Account

You can change the user account for a virtual machine by choosing **VM > Settings > Options > Startup/Shutdown** and changing the user account information there.

If the virtual machine is configured to run as the user account who powers it on, you need to make sure the virtual machine is in a location that is accessible to that user. If you need to locate the virtual machines in a different area, or on another system on the network, make sure the user has access to the virtual machine resources (such as virtual disks, physical disks, devices and snapshot files).

To change the location where virtual machines are created, see [“Specifying Where Virtual Machines Are Created”](#) on page 123.

Permissions and Virtual Machine Devices

To configure a virtual machine to use a physical disk or generic SCSI device, the user must be a member of the Administrators group.

Configuring Permissions to Access a Virtual Machine

The system administrator (that is, the administrator responsible for setting up the host running VMware Server, not necessarily the Windows Administrator login) can set the access permissions on the configuration file using the following procedure. In general, VMware Server users should have **Read** permission to virtual machine configuration files; you can add any specific users that should have **Read & Execute** and **Write** permissions.

To configure permissions to access a virtual machine

- 1 Locate the configuration file on the host system. Right-click the configuration file and select **Properties**.

The Properties dialog box appears.

- 2 Click the **Security** tab.

NOTE If the virtual machine is stored on a Windows XP client system and is configured to use Workgroup mode, the Security tab is hidden by default. To show the tab, on the Windows XP system, choose **Start > Control Panel > Folder Options**, click **Advanced**, and clear the **Simple File Sharing** check box.

- 3 In the Properties dialog box, select each user or group and select the appropriate permission, typically **Read**.

If you want to limit access to the virtual machine, clear the **Allow inheritable permissions from parent to propagate to this object** check box.

- 4 To specify that a user or group that should not have access to the configuration file, either click **Remove** or check all permissions in the **Deny** column to deny all permissions to that user or group.
- 5 To add more users or groups, click **Add**.
The Select Users, Computers and Groups dialog box appears.
- 6 In the dialog box, select the groups or users that you want to access the virtual machine, then click **Add**.
- 7 After you finish adding the users or groups, click **OK**.
The users and groups are added with default **Read** and **Write** permissions.
- 8 In the Properties dialog box, change the type of access for the user or group to the configuration file. Choose either **Read** or **Read & Execute** and **Write**.
- 9 Click **OK** to set the permissions to the configuration file.

Authenticating Users and Running Virtual Machines for a Linux Host

VMware Server for Linux uses Pluggable Authentication Modules (PAM) for user authentication in the VMware Server Console and the VMware Management Interface. The default installation of VMware Server uses standard Linux `/etc/passwd` authentication, but can be configured to use LDAP, NIS, Kerberos or another distributed authentication mechanism.

Every time you connect to the VMware Server host with the VMware Server Console or VMware Management Interface, the `inetd` or `xinetd` process runs an instance of the VMware authentication daemon (`vmware-authd`). The `vmware-authd` process requests a username and password, and hands them off to PAM, which performs the authentication.

After you are authenticated, the console starts or the management interface's Status Monitor page appears. What you can now do with the virtual machines is based on your permissions. See [“Understanding Permissions and Virtual Machines”](#) on page 83.

The `vmware-authd` process starts a virtual machine process as the owner of the configuration file, not as the user connecting to the virtual machine. However, the user is still restricted by his or her permissions on the configuration file.

NOTE If you have full permissions on a configuration file but do not have execute permission to the directory in which the configuration file resides or any of its parent directories, then you cannot connect to the virtual machine with a VMware Server Console or a VMware Scripting API. Furthermore, you cannot see the virtual machine in the VMware Management Interface or in the VMware Server Console. Nor can you delete any files in the virtual machine's directory.

Virtual machines and their resources, such as virtual disks, physical disks, devices and snapshot files, should be located in areas accessible to their users.

If a `vmware` process is not running for this configuration file, `vmware-authd` checks to see if this virtual machine is in the inventory. If the virtual machine is in the inventory, `vmware-authd` becomes the owner of the configuration file (not necessarily the user that is currently authenticated) and starts the console with this configuration file as an argument (for example, `vmware /<path_to_config>/<configfile>.vmx`).

The `vmware-authd` process exits as soon as a connection is established to a `vmware` process and at least one user has connected. Each `vmware` process shuts down automatically after the last user disconnects.

Default Permissions

When you create a virtual machine with VMware Server on a Linux host, its configuration file is assigned the following default permissions, based on the user accessing it:

- Read, execute and write (7) – For the user who created the configuration file (the owner).
- Read and execute (5) – For the primary group to which the owner belongs.
- Read (4) – For users other than the owner or a member of the owner's group.

When you first install the VMware Server software and run the configuration program `vmware-config.pl`, you can set these permissions for any existing virtual machine configuration files.

If you plan to use a virtual machine and its configuration file you created in other VMware products with VMware Server, you must open the configuration file (choose **File > Open**) to connect to the virtual machine from the VMware Server Console or the VMware Management Interface. Then set the default permissions as above.

Creating Virtual Machines on NFS Shares

If the virtual machine is located on an NFS share, make sure the root user has access to the location of the virtual machine files. Otherwise, you may encounter problems configuring the virtual machine.

If you create a virtual machine on an NFS share to which the root user has no access, certain operations do not work when the virtual machine is not running. For example, you cannot revert to a snapshot, add or remove devices to or from the virtual machine, or otherwise change the virtual machine's configuration.

Checking Permissions in the VMware Management Interface

The VMware Management Interface lists the permissions you have for each configuration file on the host machine to which you are connected. The permissions appear on the Users and Events page for each virtual machine. For more information, see [“Viewing a List of Connected Users”](#) on page 109.

Only virtual machines for which you have read access are visible to you in the VMware Management Interface.

Securing Your Remote Sessions

The username, password, and network packets sent to the VMware Server host over a network connection when using the VMware Server Console or the VMware Management Interface are encrypted in VMware Server by default. As the Administrator user (Windows hosts) or root user (Linux hosts), you can disable Secure Sockets Layer (SSL) if you do not want to encrypt these sessions.

With SSL enabled, VMware Server creates security certificates and stores them on your host. However, the certificates used to secure your VMware Management Interface sessions are not signed by a trusted certificate authority. Therefore they do not provide authentication. To use encrypted remote connections externally, you should consider purchasing a certificate from a trusted certificate authority.

With SSL enabled, the console and management interface perform exactly as they do when SSL is disabled.

When SSL is enabled for the VMware Server Console, a lock icon appears in the lower right corner of the console window. Any consoles that are already open at the time SSL is enabled do not become encrypted, and the lock icon does not appear in these console windows. You must close these consoles and start new console sessions to ensure encryption.

When SSL is enabled for the VMware Management Interface, the URL to connect to the management interface is `https://<hostname>:8333`. The management interface

automatically redirects users to this URL if they use the insecure URL (`http://<hostname>:8222`) to connect. A lock icon appears in the status bar of the browser window.

If you disable SSL, users are automatically redirected to `http://<hostname>:8222` if they use `https://<hostname>:8333` to connect to the management interface.

NOTE If SSL is disabled and then enabled again, any new management interface connections to the non secure port (8222) are not redirected.

Using Your Own Security Certificates

You can use your own security certificate when you enable SSL.

On a Windows host, run the Microsoft Management Console (`mmc.exe`) and select your certificate. When you upgrade the VMware Management Interface on a VMware Server for Windows host, you must reassign your certificate to the VMware Management Interface.

On a Linux host, the VMware Management Interface certificate must be placed in `/etc/vmware-mui/ssl`. The certificate consists of two files: the certificate file (`mui.crt`) and the private key file (`mui.key`). The private key file should be readable only by the root user.

When you upgrade the VMware Management Interface on a Linux host, the certificate remains in place. In case you removed the VMware Management Interface, the directory is not removed from your host.

Enabling and Disabling SSL for Remote Sessions

You enable and disable SSL for VMware Server Console connections in the console or the management interface. You enable SSL for VMware Management Interface connections in the management interface. By default, SSL is enabled for all remote connections.

The certificates used in these secure sessions are not signed by a trusted certificate authority. Therefore they do not provide authentication. To use encrypted remote connections externally, consider purchasing a certificate from a trusted certificate authority.

To change SSL settings for console and management interface connections from the VMware Management Interface, see [“Securing Remote Connections with SSL”](#) on page 112.

To change the SSL setting for console connections from the VMware Server Console, see [“Enabling SSL for VMware Server Console Connections”](#) on page 125.

Identifying a Virtual Machine by Its UUID

Each virtual machine is automatically assigned a universally unique identifier (UUID), which is stored in the SMBIOS system information descriptor. The UUID can be accessed by standard SMBIOS scanning software, for example SiSoftware Sandra or the IBM utility `smbios2`, and used for system management in the same way you use the UUID of a physical computer.

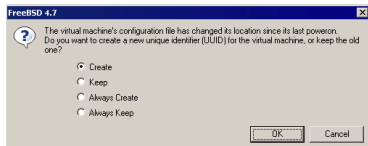
The UUID is a 128-bit integer. The 16 bytes of this value are separated by spaces, except for a dash between the eighth and ninth hexadecimal pairs. So a sample UUID looks like this:

```
00 11 22 33 44 55 66 77-88 99 aa bb cc dd ee ff
```

The UUID is based on the physical computer's identifier and the path to the virtual machine's configuration file. This UUID is generated when you power on or reset the virtual machine. As long as you do not move or copy the virtual machine to another location, the UUID remains constant.

If you move or copy the virtual machine, you have the choice of creating a new UUID the first time you power on the virtual machine. This new UUID is based on the physical computer's identifier and path to the virtual machine's configuration file in its new location.

When you power on a virtual machine that was moved or copied to a new location, a message appears.



If you moved this virtual machine, you can choose to keep the UUID. Select **Keep**, then click **OK** to continue powering on the virtual machine.

If you copied this virtual machine to a new location, you should create a new UUID, since the copy of the virtual machine is using the same UUID as the original virtual machine. Select **Create**, then click **OK** to continue powering on the virtual machine.

If the original virtual machine is being used as a template for more virtual machines, you can choose to create a new UUID the first time you power on each copy. After you configure the virtual machine and are ready to make it a template, move it to a new location and power it on. When the message appears after you power on, select **Always Create**, then click **OK** to continue powering on the virtual machine. The virtual machine is set up to create a new UUID every time it is moved. Power off the virtual

machine and begin using it as a template by copying the virtual machine files to other locations.

If you intend to move the virtual machine numerous times, and want to keep the same UUID each time the virtual machine moves, then select **Always Keep** and click **OK** to continue powering on the virtual machine.

NOTE If you want to change the Always Keep or Always Create setting, power off the virtual machine and edit its configuration file (.vmx). Delete the line that contains

```
uuid.action = "create"
```

or

```
uuid.action = "keep"
```

Suspending and resuming a virtual machine does not trigger the process that generates a UUID. Thus, the UUID in use at the time the virtual machine was suspended remains in use when the virtual machine is resumed, even if it has been copied or moved.

However, the next time the virtual machine is rebooted, the message appears, so you can choose to create a new UUID or keep the existing one.

Specifying a UUID for a Virtual Machine

In some circumstances you might want to assign a specific UUID to the virtual machine.

To specify a UUID for a virtual machine

- 1 Override the automatically generated UUID value.
- 2 Power off the virtual machine and edit its configuration file (.vmx) to set the value of the UUID parameter.
- 3 Use a text editor to edit the configuration file. The format for the line is:

```
uuid.bios = <uuidvalue>
```

The UUID value must be surrounded by quotation marks. A sample configuration line looks like:

```
uuid.bios = "00 11 22 33 44 55 66 77-88 99 aa bb cc dd ee ff"
```

- 4 After adding this line to the configuration file, power on the virtual machine.

The new UUID is used when the virtual machine boots.

Logging VMware Server Events on Windows

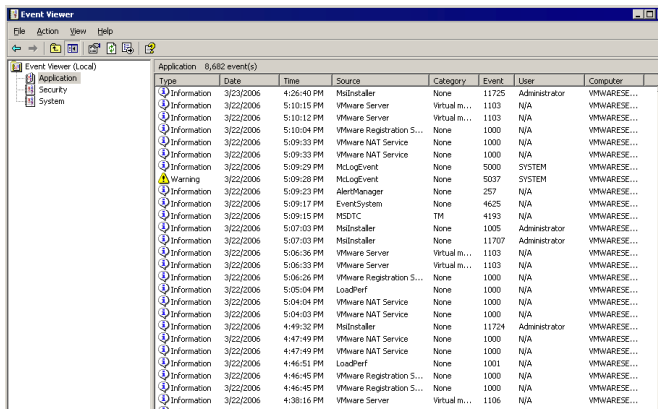
VMware Server sends information about events that occur in the application to the Event Viewer on Windows hosts. Each event has a unique identifier to assist you in tracking various events with automation tools.

The types of events that are sent to the Event Viewer include:

- Any changes to a virtual machine's power state. When a virtual machine is powered on or off, suspended or resumed, an entry is logged in the Event Viewer.
- The addition or removal of virtual machines from the inventory.
- The deletion of a virtual machine from the VMware Server system.
- Any messages and warnings generated by VMware Server and the responses to these messages and warnings. Whenever VMware Server generates a message or a warning prompt to which the user must respond, the message or warning and the user's response are logged in the Event Viewer. A message or a warning is any dialog box that VMware Server generates in the application that is not a hint.

To log VMware Server events on Windows

- 1 To access the Event Viewer, choose **Start > Administrative Tools > Event Viewer**.
- 2 Select the **Application** log to view VMware Server events.



- 3 Modify the information that gets logged for a particular machine or for all virtual machines.

The two options you can modify include:

- `eventlog.win.message=FALSE` — this setting prevents the logging of all dialog box and message events that appear in VMware Server.
- `eventlog.win.register=FALSE` — this setting prevents the logging of power state change events and logging of when a virtual machine is added to or removed from the inventory.

To modify what gets logged for a virtual machine, add either or both of the options to the virtual machine's configuration (`.vmx`) file.

To modify what gets logged for all virtual machines on a host, add either or both of the options to the VMware Server `config.ini` file, located by default in `C:\Documents and Settings\All Users\Application Data\VMware\VMware Server`.

Backing Up Virtual Machines and the VMware Server Host

This section discusses methods for backing up your virtual machines and the VMware Server host. It includes:

- [“Using a Backup Agent in the Virtual Machine”](#) on page 95
- [“Using a Backup Agent Running on the Host Operating System”](#) on page 96
- [“Backing Up the VMware Server Host”](#) on page 96
- [“Considerations for Backing Up Virtual Machines”](#) on page 97

Using a Backup Agent in the Virtual Machine

The best way to back up virtual machines that require constant uptime (24 hours a day, seven days a week) is to load a backup agent in each virtual machine. This agent should connect directly through your network to your backup servers. This method allows you to completely back up individual files on your virtual machines and recover files individually.

Supported Backup Configurations

VMware has tested the following backup software in virtual machines using the Dell PowerVault 120T tape drive/changer:

- BrightStor ARCserve Backup version 9.0 (build 1868)
- Veritas Backup Exec 9, Service Pack 1

The tape drive must be configured as a generic SCSI device. To add the drive to a virtual machine, see [“Adding a Generic SCSI Device to a Virtual Machine”](#).

NOTE If the virtual machine has a Windows guest operating system installed and is configured to use the BusLogic SCSI adapter, you must use the VMware BusLogic driver, available from the VMware Web site at <http://www.vmware.com/download>.

Using a Backup Agent Running on the Host Operating System

Another backup method uses a backup agent running on the VMware Server host. You back up a virtual machine by suspending and resuming it with batch files containing `vmware-cmd` commands. Suspending a virtual machine puts it in a state in which the host backup software can gain exclusive access to the virtual machine files to complete its task.

To backup a virtual machine directory using a backup agent

- 1 Add the following line to your suspend batch file:

```
vmware-cmd <path_to_config>\<config>.vmx suspend
```
- 2 Once the virtual machine is suspended, you can safely back up this virtual machine's directory using the backup agent installed on the VMware Server host.
- 3 After the backup job completes, run a resume batch job to restart the virtual machine.

The batch file should contain the following line:

```
vmware-cmd <path_to_config>\<config>.vmx start
```

This command resumes the virtual machine into an active, running state.

- If you want to restore a virtual machine to a server other than the VMware Server host where it was originally located, shut down the virtual machine. Instead of using the suspend batch file, use one that powers off the virtual machine.

```
vmware-cmd <path_to_config>\<config>.vmx stop
```

- The suspend, stop, and resume commands can be used in pre- and post-job scripts that are normally available via the backup software being used. Backup software such as Veritas Backup Exec has the capability to run pre- and post-batch jobs with scheduled backups.

Backing Up the VMware Server Host

To completely back up your entire VMware Server environment for a given point in time, back up your entire VMware Server host. Shut down all virtual machines on the

host, and back up the host and all virtual machine directories. However, restoring a virtual machine directory from such a backup returns you to that point in time; you cannot restore individual files in the virtual machine.

Considerations for Backing Up Virtual Machines

A virtual machine directory should not be backed up on the VMware Server host if the virtual machine is powered on. You should either suspend or shut down the virtual machine before backing up its directory.

If the virtual machine is running when you try to back it up, the virtual machine can hang and be unreachable.

Open file agents loaded on the VMware Server host do not always work reliably when you back up open virtual disks that are gigabytes in size.

Before implementing a backup method, test and document the method in advance to ensure a successful backup.

For more information on scripting and using the `vmware-cmd` file, read Appendix A of the *VMware Scripting API User's Manual*, available on the VMware Web site at <http://www.vmware.com/support/developer>.

Using the VMware Management Interface

VMware Server provides the VMware Management Interface, a Web-based management tool that allows you to:

- Monitor the state of virtual machines and the VMware Server host on which they are running.
- Control (power on, suspend, resume, reset and power off) the virtual machines on that host.
- Connect the VMware Server Console to a given virtual machine, for hands-on management.
- View details about each virtual machine, including system summary, hardware information, any connected users and a log of recent events.
- Secure console and management interface sessions with SSL (administrator and root users only).
- Answer questions and acknowledge messages posed by the virtual machine.

To manage a virtual machine from the VMware Management Interface, a user must have at least read permission for that virtual machine's configuration file. For more

information about permissions and VMware Server, see [“Understanding Permissions and Virtual Machines”](#) on page 83.

To properly view the VMware Management Interface, ensure that style sheets are enabled in your browser, regardless of which browser and version you are using.

NOTE To run the VMware Management Interface in Internet Explorer 6.0 on a Windows Server 2003 system, whether the VMware Server host is installed on Windows Server 2003 or a Windows Server 2003 client machine that connects to a VMware Server host, you need to follow some special configuration steps in order to use the management interface. For more information, see [“Configuring Web Browsers for Use with VMware Server”](#) on page 46.

The VMware Management Interface starts with a Login page, where you enter your user name and password to log on. The Login page contains links for downloading the VMware Server Console for Windows and Linux hosts. For more information, see [“Downloading the VMware Server Console”](#) on page 81.

After your user name and password are authorized by the management interface, the Status Monitor page appears. The Status Monitor page contains high-level details about all the virtual machines on the host server to which you are connected. The Status Monitor page links to a detailed set of pages specific to each virtual machine, where you find information about virtual devices, configuration options, and a summary of recent events. In addition, you can create and delete virtual machines from your browser.

These pages refresh or reload automatically every 90 seconds. You might want to refresh or reload these pages manually before you perform an operation like suspending, resuming, or powering on or off a virtual machine from the VMware Management Interface or after you perform a power operation in a console. Another user might have performed the same or a conflicting operation right before you. To refresh the page, click Refresh at the top of a page.

This section includes the following topics:

- [“Setting the Session Length for the VMware Management Interface”](#) on page 99
- [“Logging On to the VMware Management Interface”](#) on page 99
- [“Using the Status Monitor”](#) on page 101
- [“Configuring a Virtual Machine”](#) on page 105
- [“The Apache Server and the VMware Management Interface”](#) on page 111
- [“Logging Off the VMware Management Interface”](#) on page 111

Setting the Session Length for the VMware Management Interface

Your management interface sessions times out after 60 minutes of idle time.

On a Windows host, this setting is specified by the variable `vmware_SESSION_LENGTH`, stored in `C:\Program Files\VMware\VMware Management Interface\htdocs\init.pl`. You can change this setting to any number of minutes, or you can block access to the management interface for all users by setting `vmware_SESSION_LENGTH` to 0 minutes. You can have persistent sessions that never time out by setting `vmware_SESSION_LENGTH` to -1.

On a Linux host, you can change this setting by running the management interface configuration program `vmware-config-mui.pl`. You can block access to the management interface for all users by setting the timeout length to 0 minutes. You can have persistent sessions that never time out by setting the timeout length to -1.

Logging On to the VMware Management Interface

To use the VMware Management Interface, run a supported browser such as Internet Explorer 5.5 or 6.0. VMware highly recommends using 6.0, Netscape Navigator 7.0 or later, or Mozilla 1.x.

Before you log on to the VMware Management Interface

- You must know the host name or IP address of the server you want to manage.
- You must have a valid user name and password on that server.
- You can connect to the server with up to eight management interface sessions at a time. The URL to connect to the server is `https://<hostname>:8333`.
- If you are connecting to the VMware Management Interface from a browser on the host machine, you can use `localhost` as the `<hostname>`.
- If you disabled SSL for your management interface sessions, the URL to connect to the server is `http://<hostname>:8222`.

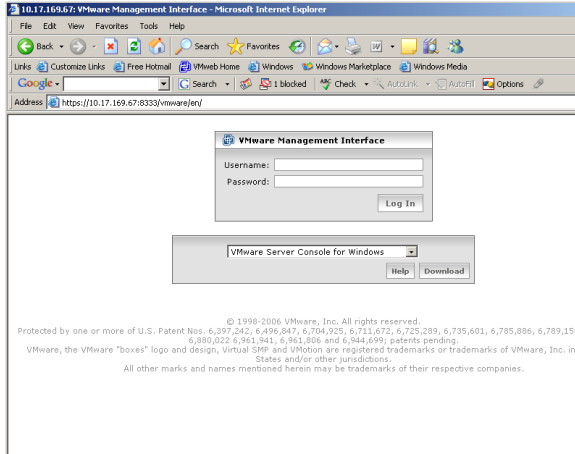
For more information, see [“Securing Your Remote Sessions”](#) on page 90. Users are automatically redirected to `http://<hostname>:8222` if they use `https://<hostname>:8333` to connect to the management interface.

NOTE If you are using Netscape Navigator or Mozilla, check the advanced preferences (**Edit > Preferences > Advanced**) to be sure JavaScript and style sheets are both enabled.

To log on to the VMware Management Interface

- 1 Enter the URL.

The Login page appears.



The Login page contains fields for your user name and password.

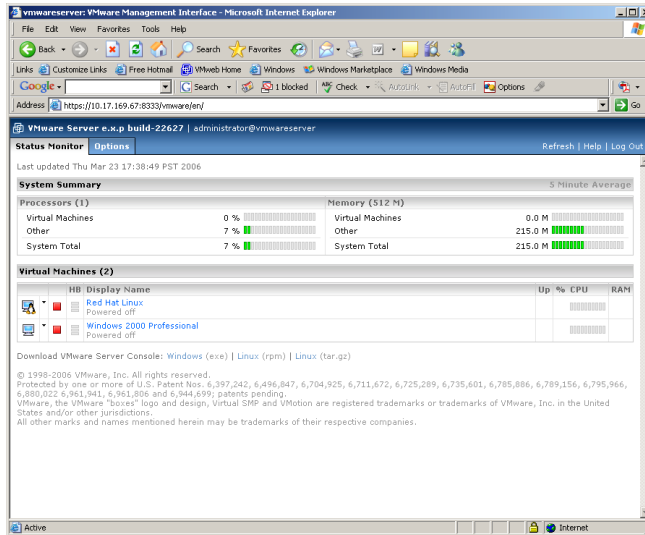
It also contains a menu so you can download installation packages for the VMware Server Console. To download a package, see [“Downloading the VMware Server Console”](#) on page 81.

- 2 On the Login page, enter your user name and password for the host machine, and click **Log In**.

The Status Monitor page appears. For information about the Status Monitor page, see [“Using the Status Monitor”](#) on page 101.

Using the Status Monitor

The Status Monitor page contains a high-level view of the VMware Server host including a host system summary and list of all virtual machines known to the host that you have sufficient permissions to see.



Viewing Summary Information About the VMware Server Host System

Under **System Summary**, you can view:

- The number of processors on the VMware Server host, including the average percentage of processor power used by virtual machines, other processes on the host, and the total being used by the whole system for the previous minute.
- The amount of memory on the VMware Server host, including the average amount of memory used by virtual machines, other processes on the host, and the total being used by the whole system for the previous minute.


Viewing Summary Information About Virtual Machines on the Host

Under **Virtual Machines**, you can view a list of all virtual machines known to the host that you have sufficient permissions to see. When a virtual machine is running, the Status Monitor page displays its ID number after the power status of the virtual machine.


Activities you can perform include:

- [“Connecting to a Virtual Machine with the VMware Server Console”](#) on page 103
- [“Monitoring the Virtual Machine’s Heartbeat”](#) on page 104
- [“Viewing Information about a Virtual Machine”](#) on page 104
- [“Downloading the VMware Server Console”](#) on page 81 (Login and Status Monitor pages)


Using the Virtual Machine Menu




Click the arrow to the right of the terminal icon () to display a menu of options for that virtual machine. The menu includes the following commands, most of which can be performed using the buttons and other visual elements of the management interface.

Depending on your permissions and the state of the virtual machine, some options might not be available.


- **Attach Console** – Launches the VMware Server Console, which connects to this virtual machine. Selecting this option is the same as clicking . You need to log on to the host. For more information, see [“Connecting to a Virtual Machine from a Windows Host or Client”](#) and [“Connecting to a Virtual Machine from a Linux Host or Client”](#).

NOTE Netscape and Mozilla users must define a MIME type before installing the VMware Server Console. Internet Explorer is automatically configured when the VMware Server Console is installed. For information, see [“Setting MIME Type to Launch the VMware Server Console”](#) on page 128.

- **Properties** – Opens the Virtual Machine Overview page for this virtual machine in a new browser window. Selecting this option is the same as clicking the virtual machine name link in the **Display Name** column.
- **Configure Options** – Opens the Options page, where you can edit a virtual machine’s configuration, such as the guest operating system type, display name, the location of the suspended state file and the startup and shutdown options. With the exception of the display name, you can edit these options only when the virtual machine is powered off.
- **Shut Down Guest** – Runs the script associated with this power state change, shuts down the guest operating system, and powers off the virtual machine. Selecting this option is the same as clicking  in the power state pop-up menu.


- **Suspend after Running Script** – Runs the associated script and suspends a running virtual machine. Selecting this option is the same as clicking  in the power state pop-up menu.
- **Power On/Resume and Run Script** – Powers on a stopped virtual machine or resumes a suspended virtual machine, and runs the script associated with this power state change. Selecting this option is the same as clicking  in the power state pop-up menu.
- **Restart Guest** – Gracefully restarts the guest operating system and the virtual machine. Selecting this option is the same as clicking  in the power state pop-up menu.
- **Power Off** – Powers off the virtual machine immediately without running a script or shutting down the guest operating system. Selecting this option is the same as turning off the power to a physical computer.
- **Suspend** – Suspends a powered on virtual machine without running a script.
- **Power On/Resume** – Powers on a stopped virtual machine or resumes a suspended virtual machine without running a script.
- **Reset** – Resets the virtual machine immediately without running a script or stopping the guest operating system. Selecting this option is the same as pressing the reset button on a physical computer.

Connecting to a Virtual Machine with the VMware Server Console


To view a particular virtual machine's desktop, attach the VMware Server Console and connect to the virtual machine. Click the terminal icon () in the row for the virtual machine to which you want to connect with the console. For information on connecting with the console, see [“Connecting to a Virtual Machine from a Windows Host or Client”](#) and [“Connecting to a Virtual Machine from a Linux Host or Client”](#).

The terminal icon appears slightly different, depending upon the guest operating system selected for the virtual machine when it was created. This visual cue helps to identify the virtual machine (for example, the display name might not indicate the guest operating system). The variations in the terminal icon are shown here.

 – indicates a Windows guest operating system.

 – indicates a Linux guest operating system.

 – indicates a FreeBSD guest operating system.

 – indicates a NetWare guest operating system.

 — indicates another guest operating system, such as MS-DOS.

 — indicates a Sun Solaris operating system.

Monitoring the Virtual Machine's Heartbeat

Under **HB** is a bar graph that represents the average percentage of heartbeats received by a virtual machine during the previous minute. The heartbeat represents the overall health of the guest operating system, based on whether applications running in the guest are consuming resources from other applications in the guest.

The heartbeats are sent by the VMware Tools service to the virtual machine from its guest operating system; the percentage is relative to the number of heartbeats the virtual machine expects to receive for the minute before the page was last updated. Heavily loaded guest operating systems might not send 100% of the expected heartbeats, even though the system is otherwise operating normally. In general, only when the heartbeat percentage drops to zero should the virtual machine or guest operating system be considered abnormal.

NOTE If VMware Tools is not installed or is not running, the guest operating system does not send any heartbeats to its virtual machine and this meter is disabled.

Viewing Information about a Virtual Machine

Important virtual machine information is readily available on the Status Monitor page.

- The link in the **Display Name** column indicates the display name for the virtual machine. If one is not specified, the path to the configuration file for the virtual machine appears here instead. This column also contains the virtual machine's power state, its process ID, and its virtual machine ID (if it is running) It also notes if VMware Tools is not installed.

If the virtual machine is waiting for a response to a system message, a **Waiting for input link** appears here. Click the link to view the message and respond to it.

Click the virtual machine link for more details about the virtual machine. The Virtual Machine Overview page appears in a new browser window. For more information, see [“Configuring a Virtual Machine”](#) on page 105.

- The value in the **Up** column indicates the length of time the virtual machine has been running.
- The value in the **% CPU** column indicates the average percentage of host operating system processor capacity the virtual machine used during the final minute before the page was last updated. More detailed processor information is available on the Virtual Machine Overview page.

- The value in the **RAM** column indicates the average amount of memory the virtual machine used during the final minute before the page was last updated. More memory information is available on the Virtual Machine Overview page.

Using Common Controls

The following links appear on most or all of the pages in the management interface.

Refresh — This link refreshes or reloads the current page. To avoid conflicts with other users, click this button before you perform an operation in the management interface like shutting down, suspending, resuming, or powering on a virtual machine — or **after** you perform such an operation in a console.

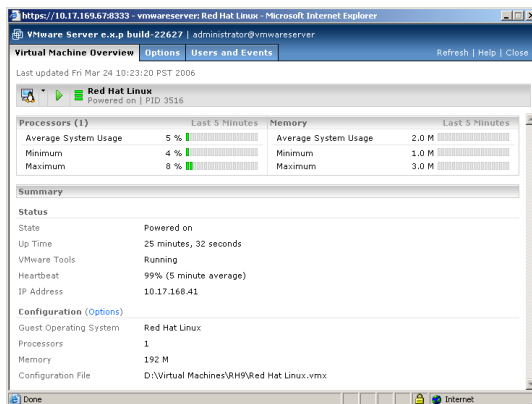
Help — This link connects you to the online documentation for the current page in the management interface.

Logout — This link logs you off of the management interface. You can log off from the Status Monitor and Options pages only. Click **Logout** to return to the Login page. See [“Logging Off the VMware Management Interface”](#) on page 111.

Close — This link closes the current management interface window.

Configuring a Virtual Machine

To see more information about a particular virtual machine and to modify its configuration, click the link to that virtual machine in the **Display Name** column on the Status Monitor page. The Virtual Machine Overview page appears in a new browser window.



The Virtual Machine Overview page contains these details about the virtual machine:

- The current power state of the virtual machine — whether it is powered on, powered off, or suspended.
- The process ID of the virtual machine.
- The VMID of the virtual machine, which is the VMware Server version of the PID for a running virtual machine.
- The minimum, maximum, and average percentage of VMware Server host processor capacity that the virtual machine used in the previous minute.
- The minimum, maximum, and average amount of VMware Server host memory that the virtual machine used in the previous minute.
- How long the virtual machine has been running.
- The status of VMware Tools — whether VMware Tools is installed and running.
- The average percentage of heartbeats received by a virtual machine during the previous minute. See [“Monitoring the Virtual Machine’s Heartbeat”](#) on page 104.
- The IP address of the virtual machine.
- Links to edit standard configuration options. Click **Options** to edit the virtual machine’s standard configuration options. The Options page appears. To change most options, you must power off the virtual machine.
- The guest operating system installed in the virtual machine.
- The number of virtual processors in the virtual machine.
- The amount of memory allocated to the virtual machine.
- The path to the virtual machine’s configuration file on the VMware Server host.

Activities you can perform when viewing a virtual machine’s details include:

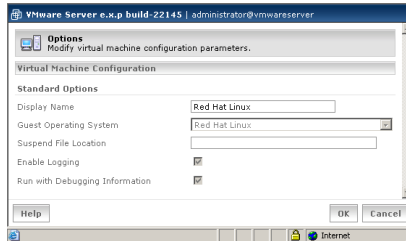
- [“Modifying the Configuration File Directly \(Advanced Users Only\)”](#) on page 107
- [“Viewing a List of Connected Users”](#) on page 109
- [“Viewing a Log of a Virtual Machine’s Events”](#) on page 110

Changing Configuration Options

To change any standard virtual machine configuration options, complete the following steps.

- 1 Power off the virtual machine and click **Edit**. The Options Configuration page appears.

NOTE You can change the display name when the virtual machine is running.



- 2 To change the display name, type the new name in the **Display Name** field.
- 3 To change the guest operating system (for example, if you are upgrading the guest operating system installed in the virtual machine), select the new guest operating system from the **Guest Operating System** list.
- 4 To change the location of the suspended state file, type the path to the directory on the host in the **Suspend File Location** field.
- 5 To change whether logging is enabled for the virtual machine, check (to enable) or clear (to disable) the **Enable Logging** check box.
- 6 To change whether the virtual machine is running with debugging information, check (to enable) or clear (to disable) the **Run with Debugging Information** check box.
- 7 Click **OK** to save your changes and close the window.

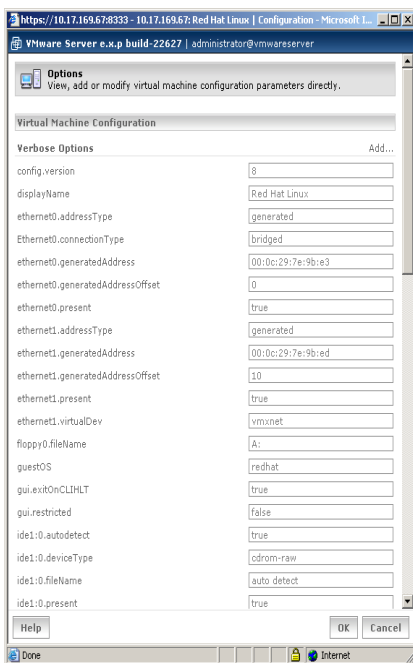
Modifying the Configuration File Directly (Advanced Users Only)

To add or change a virtual machine's configuration option that cannot be accessed from elsewhere in the management interface, edit the virtual machine's configuration file (.vmx) from the **Options** tab.

CAUTION You should not add or change any options in your configuration file unless you have been given specific instructions about an option in another part of the user documentation, or if you are working with VMware support to solve an issue with your virtual machine.

To add an option to the configuration file, make sure you are logged on to the management interface as the virtual machine user or as a user with the proper permissions to modify this virtual machine (such as the Administrator or root user), and complete the following steps. Make sure the virtual machine is powered off.

- 1 Under **Verbose Options**, click the **click here** link. The Options page appears.



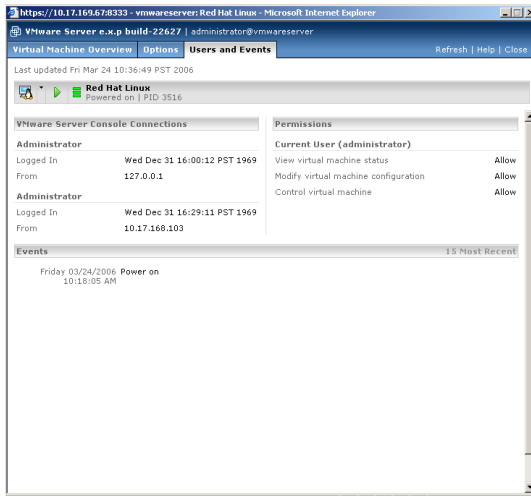
- 2 Click **Add**.
- 3 A prompt appears. Enter a name for the option, then click **OK**.
- 4 Another prompt appears. Enter a value for option you specified, then click **OK**.
- 5 Click **OK** in the Options page to save the change to the configuration file.

To change an option in the configuration file, complete the following steps.

- 1 Under **Verbose Options**, click the **click here** link. The Options page appears.
- 2 Locate the option you want to change, then change the value in the entry field to the right of the option.
- 3 Click **OK** to save your change and close the Options page.

Viewing a List of Connected Users

To see a list of users who are connected to a virtual machine with a console or VMware Scripting API, click the **Users and Events** tab.



The list under **Remote Console Connections** identifies any users connected to the virtual machine with a console or VMware Scripting API. The list includes the time and IP address from which the user connected to the virtual machine and the status of the user's activity.

NOTE You can determine which users are connected to a running virtual machine from the console; choose **VM > Connected Users**.

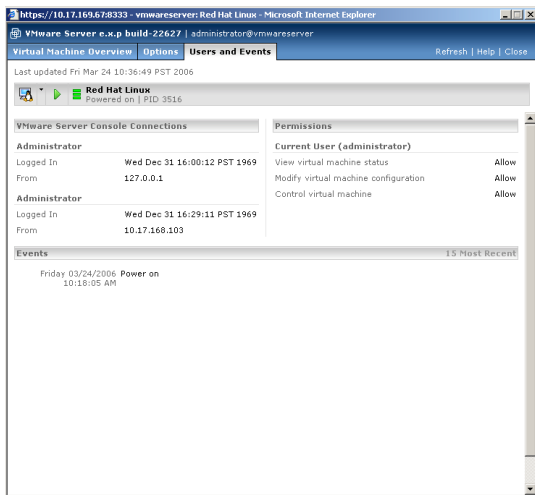
The list under **Permissions** indicates what you can do with the virtual machine. You are either allowed or denied the following abilities:

- Viewing virtual machine status.
- Modifying the virtual machine's configuration.

- Controlling the virtual machine — powering it on or off, suspending or resuming it.

Viewing a Log of a Virtual Machine’s Events

A log of the 15 most recent virtual machine events is available. Click the **Users and Events** tab. The Users and Events page appears.



The **Events** list displays a log of the most recent actions or events recorded in the virtual machine, such as the questions VMware Server asks, any errors and the powering on or off the virtual machine. Events appear in reverse chronological order; that is, the most recent events appear first in the list.

The event log draws its data from the log file for the virtual machine's configuration file. The log file is stored, by default, in the virtual machine's directory. On a Windows host, this directory is <installdrive>:\Virtual Machines\<guestOS>. On a Linux host, this directory is /var/lib/vmware/Virtual Machines/<guestOS>.

Sometimes you see a waiting for input message appears as a link in the **Display Name** column. This link appears when you perform an action in the management interface that prompts the virtual machine to generate a message; you must respond to the message before the virtual machine can proceed. When you click that link, a prompt appears, where you can enter a response. After you provide your answer, the prompt closes. Your response appears in the **Events** list.

The log shows the date and time the event occurred and an explanation of the event. Some events have a symbol associated with them that corresponds to the type of event that occurred.

- ▲ — This type of event indicates the virtual machine generated a question or warning.
- — This type of event indicates an error occurred in the virtual machine.

NOTE On Windows hosts, the host operating system's Event Viewer tracks virtual machine power state changes, VMware Server messages and answers to prompts that appear in the virtual machine. For more information, see [“Logging VMware Server Events on Windows”](#) on page 94.

The Apache Server and the VMware Management Interface

On VMware Server for Linux hosts, an Apache server is installed with the management interface. Listed here are the commands to start, stop and restart the Apache server.

In order to use these commands, you must first log on as root (su -), then open a terminal session.

To start the Apache server, type
`/etc/init.d/httpd.vmware start`

To stop the Apache server, type
`/etc/init.d/httpd.vmware stop`

To restart the Apache server, type
`/etc/init.d/httpd.vmware restart`

Logging Off the VMware Management Interface

When you are ready to log off of the VMware Management Interface, click **Logout** on the Status Monitor or Options page. You are prompted to confirm that you want to log off. Logging off of the management interface does not affect the virtual machines on the host or any consoles you opened from the management interface.

VMware Management Interface sessions expire automatically after 60 minutes of inactivity or idle time. To change the session length, see [“Setting the Session Length for the VMware Management Interface”](#) on page 99.

Deleting Virtual Machines

You can delete a virtual machine only if you are the Administrator or root user. You might delete a virtual machine if it is no longer needed or if you need to free up disk space on your host.

When you delete a virtual machine, the files associated with it — that is, all files located in the same directory — and the virtual machine's directory are deleted. The files

include the virtual machine's configuration file (.vmx), log file, nvram file, suspended state file and snapshot file.

Any virtual disks that are associated with another virtual machine on the host are not deleted. The directory containing these files is not deleted.

You delete virtual machines from the VMware Server Console only. The VMware Management Interface on VMware Server does not support deleting virtual machines. For more information, see [“Deleting a Virtual Machine Using the VMware Server Console”](#) on page 112.

Deleting a Virtual Machine Using the VMware Server Console

To use the console to delete a virtual machine, make sure the virtual machine is powered off. Select the virtual machine using either the tab at the top of the console or from the inventory list and choose **VM > Delete from Disk**. You are prompted to confirm your action. Click **Yes** to delete the virtual machine.

Configuring the VMware Server Host

Configuring the VMware Server host involves:

- [“Securing Remote Connections with SSL”](#) on page 112
- [“Configuring Startup and Shutdown Options for Virtual Machines”](#) on page 113
- [“Setting User Preferences for the VMware Server Host”](#) on page 117
- [“Setting Global Preferences for VMware Server”](#) on page 123
- [“Setting MIME Type to Launch the VMware Server Console”](#) on page 128

Securing Remote Connections with SSL

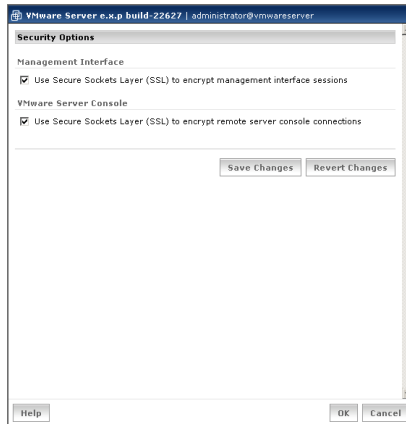
VMware Management Interface sessions and VMware Server Console connections are secured with SSL. For more information about SSL, see [“Securing Your Remote Sessions”](#) on page 90.

You can enable SSL for console connections from the console itself. For details, see [“Enabling SSL for VMware Server Console Connections”](#) on page 125.

To configure SSL from the management interface, complete the following steps.

- 1 Log on to the VMware Management Interface as the Administrator (VMware Server for Windows hosts) or root user (VMware Server for Linux hosts).
- 2 On the Status Monitor page, click the **Options** tab. The Options page appears.

- 3 Click **Security Settings**. The Security Settings page appears.



- 4 To secure your management interface sessions, check the **Use Secure Sockets Layer (SSL) to encrypt management interface sessions** check box.
- 5 To secure your console connections, check the **Use Secure Sockets Layer (SSL) to encrypt remote console connections** check box.

NOTE If you change the SSL setting for the management interface, the system automatically logs you off and must log on again.

- 6 To save your settings, click **OK**.

When SSL is enabled, a lock icon appears in the status bar of the browser running the VMware Management Interface, and in the status bar of the VMware Server Console window, unless the console is connected to a virtual machine on the local host.

After you change your SSL setting for the management interface, you are prompted to accept the security certificate in your browser the next time you log on to the management interface.

Configuring Startup and Shutdown Options for Virtual Machines

You can configure your host to determine if virtual machines start up or shut down when the host operating system starts or shuts down.

You can set a delay from the time one virtual machine starts or stops until the next one starts or stops. This delay helps to prevent overburdening the host, since significant

processor and memory are capacities required to simultaneously start or stop multiple guest operating systems.

You can determine the global order in which virtual machines start and stop.

The host is configured to start and stop virtual machines automatically by default. You can customize the global settings and virtual machine-specific settings. To customize these settings for a virtual machine, see [“Powering Virtual Machines On and Off”](#).

The system-wide virtual machine startup and shutdown options include:

- **Start Up and Shut Down Virtual Machines** — determines whether or not virtual machines are started and stopped with the system. If enabled, default startup and shutdown policies are applied to all virtual machines on your system (where no virtual machines are powered on when the host starts and all virtual machines are shut down when the host shuts down); you can customize each virtual machine’s startup and shutdown policies.

If this option is disabled, you cannot set startup and shutdown policies for any virtual machines on your system.

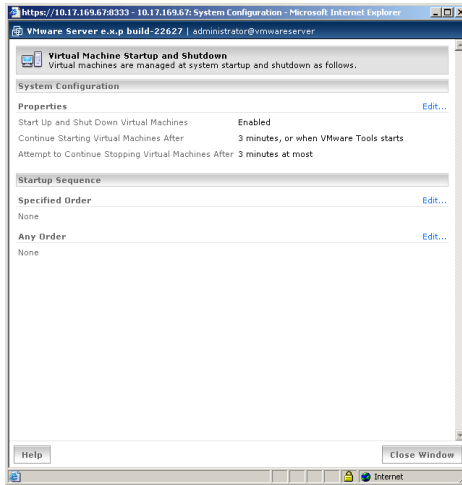
- **Continue Starting Virtual Machines After** — sets the amount of time VMware Server waits after starting one virtual machine before starting another virtual machine. You can set this so that VMware Server does not wait before starting the next virtual machine, waits a certain number of minutes before starting or starts when VMware Tools starts in the current virtual machine.
- **Attempt to Continue Stopping Virtual Machines After** — sets the amount of time VMware Server waits after stopping one virtual machine before stopping another virtual machine. You can set this so that VMware Server does not wait before stopping each virtual machine or waits a certain number of minutes before stopping each virtual machine.

Enabling the System’s Configuration Settings

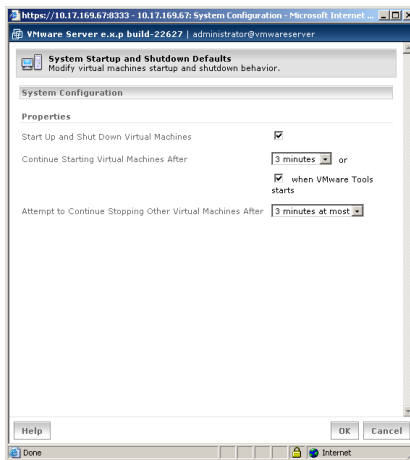
To enable the system-wide configuration settings for virtual machines, complete the following steps.

- 1 Log on to the VMware Management Interface as the Administrator (VMware Server for Windows hosts) or root user (VMware Server for Linux hosts).
- 2 On the Status Monitor page, click the **Options** tab. The Options page appears.

- 3 Click **Virtual Machine Startup and Shutdown**. The Virtual Machine Startup and Shutdown page appears.



- 4 Under **System Configuration**, click **Edit**. The System Startup and Shutdown Defaults page appears.



- 5 To enable system-wide startup and shutdown policies, check the **Start Up and Shut Down Virtual Machines** check box.

- 6 To configure when VMware Server should start the next virtual machine after a virtual machine starts, do one or both of the following:
 - To specify a period of time before the next virtual machine starts, in the **Continue Starting Virtual Machines After** list, either choose the number of minutes to wait or indicate that VMware Server should not wait before starting the next virtual machine. If you select **Other**, specify the number of minutes to wait in the prompt that appears. It is a good idea to set a delay between starting virtual machines, as a delay avoids placing an undue burden on the host processors and memory.
 - To specify that VMware Tools should start in a virtual machine before the next virtual machine starts, check **when VMware Tools starts**. If VMware Tools does not start in the virtual machine before the time specified in the **Continue Starting Virtual Machines After** list elapses, VMware Server starts the next virtual machine.
- 7 To configure when VMware Server should stop the next virtual machine after a virtual machine stops, in the **Attempt to Continue Stopping Other Virtual Machines After** list, either choose the number of minutes to wait or indicate that VMware Server should not wait before starting the next virtual machine. If you select **Other**, specify the number of minutes to wait in the prompt that appears. It is a good idea to set a delay between stopping virtual machines, as a delay avoids placing an undue burden on the host processors and memory.
- 8 Click **OK** to save your settings.
- 9 Click **Close Window** to return to the management interface's Options page.

Specifying the Order in Which Virtual Machines Start

Once you set whether or not virtual machines should start and stop with the system, you can set the order in which the virtual machines start and stop. Setting the sequence allows you to specify the position of a given virtual machine in the system-wide startup and shutdown sequence. If a sequence is set for a virtual machine, the virtual machine starts and stops in one of the following orders:

- **Specified Order** — lists the virtual machines in the order in which they are configured to start and stop.
- **Any Order** — lists the virtual machines specified to start and stop in any order.

You cannot specify the startup order for a virtual machine if it is configured to run as the user who powers it on. The virtual machine must be configured to run as the local system account or as a specific user.

Editing the Startup Sequence for Virtual Machines

To edit the startup sequence for virtual machines, click **Edit** under Startup Sequence. The Virtual Machine Startup Sequence configuration page appears and displays the virtual machines on your system.

To specify the startup order for the virtual machines on the host, select the check box next to one or more machines. Once you select a virtual machine, navigation arrows highlight, allowing you to move machines between the three lists. Virtual machines can be set to one of the following options:

- **Other** — lists the virtual machines that are configured to use the default start and stop policies when the system starts up and shuts down.
- **Specified Order** — lists the virtual machines in the order in which they are configured to start. The order in which the virtual machines stop is the reverse of the order in which they start, so the last virtual machine to start when the system starts up is the first to stop when the system shuts down. To specify the startup order, select machines and use the arrows to move them up or down within the list.
- **Any Order** — lists the virtual machines that are configured to start and stop in any order. Move virtual machines to this category if you want them to start and stop with the system, but you do not want to set the order for them. The virtual machines in this category do not start or stop until all the virtual machines listed in the **Specified Order** list have started or stopped.

Disabling the System's Configuration Settings

To disable the system-wide configuration settings, complete the following steps.

- 1 On the Virtual Machine Startup and Shutdown page, under **System Configuration**, click **Edit**. The System Startup and Shutdown Defaults page appears.
- 2 Clear the **Start Up and Shut Down Virtual Machines** check box, then click **OK**.
- 3 Click **Close Window** to return to the management interface's Options page.

Setting User Preferences for the VMware Server Host

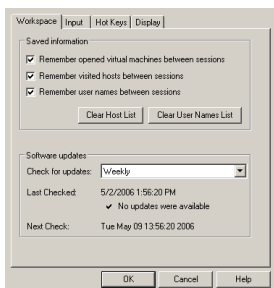
The Preferences dialog box allows you to change a number of settings that apply to all virtual machines running in a console. These settings apply to the user currently logged on to the host computer. The settings do not affect settings made by any other user when that user is logged on to the host. These settings can be changed by regular users, as well as root and Administrator users.

To change these settings, choose **Edit > Preferences**. The Preferences dialog box appears.

Setting Workspace Preferences

The **Workspace** tab lets you determine whether any virtual machines appear in the virtual machine display each time you open a console. On a Windows host, you can specify whether any host and user names appear in the console Login dialog box when you connect.

On both Windows and Linux hosts, you can specify how often VMware Server should check for software updates. The default is **Weekly**. From the Check for Updates drop-down list, you can select **Daily**, **Weekly**, or **Monthly**.



If you select the **Remember opened virtual machines between sessions** check box, you see a tab for each opened virtual machine in the virtual machine display the next time you open a console. A virtual machine is considered opened if both of the following conditions are true:

- The virtual machine was left open.
- The virtual machine was powered on and off, or powered on and suspended.

If you select the **Remember visited hosts between sessions** check box, the name of any VMware Server host to which you connected in a previous console session appears in the console's Login dialog box. To clear the list of remembered hosts, click **Clear Host List**.

If you select the **Remember user names between sessions** check box, any user names you used when you connected during previous console sessions appear in the console's Login dialog box. To clear the list of remembered user names, click **Clear User Names List**.

Configuring VMware Server to Check for Software Updates

You can configure VMware Server to check whether updates for the product are available. If you configure VMware Server to check for updates, and an update is available, the console displays a message when you launch it. You can check manually at any time by choosing **Help > Check for Updates on the Web**.

Choose **Edit > Preferences > Workspace**. Select the interval in the **Check for software updates** drop-down list.

You can set the interval to never, daily, weekly, or monthly.

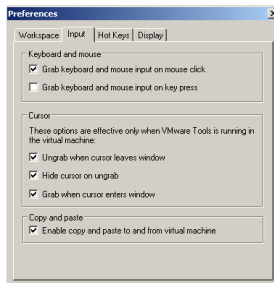
On a Linux host only, you can also check for software updates at anytime by clicking **Check Now**.

If you are running VMware Server on a Windows host behind a proxy server, make sure your browser is configured to connect to the Internet through your proxy server.

If you are running VMware Server on a Linux host behind a proxy server, make sure you configure `http_proxy` with the name of the proxy server and the port number the proxy server uses.

Changing Your Input Settings

The **Input** tab lets you adjust the way that the virtual machine captures control of the keyboard and mouse.



NOTE The **Grab when cursor enters window** option allows you to move the mouse pointer back into the virtual machine window easily if you have been working in the virtual machine and temporarily moved the mouse pointer outside the virtual machine window. The mouse pointer is grabbed only when VMware Server has focus (is the active application). If you release the mouse pointer by pressing a hot-key combination — the default is Ctrl-Alt — you must click inside the virtual machine window to make VMware Server grab the mouse pointer again.

The input settings you can specify include:

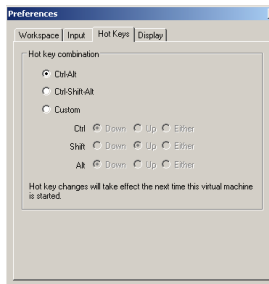
- **Grab keyboard and mouse input on mouse click** — VMware Server takes control of the keyboard and the mouse after the first primary mouse button click in the virtual machine console window.
- **Grab keyboard and mouse input on key press** — VMware Server takes control of the keyboard and the mouse after the first keystroke. The first keystroke is sent to the virtual machine. When the virtual machine console window is active and this option is selected, you cannot use the normal application and system accelerator key sequences.
- **Ungrab when cursor leaves window** — the mouse pointer becomes the mouse pointer of your host operating system when the mouse pointer exits the virtual machine console window. This option does not apply when the virtual machine is in full screen mode. Use this option to transition seamlessly between the virtual machine and your host operating system.
- **Hide cursor on ungrab** — the mouse pointer of the guest operating system is hidden when your mouse is controlling the pointer of the host operating system. This option is particularly useful when your guest operating system and your host operating system are identical: it eliminates the confusion of having to think about which of the two identical pointers moves when you move your mouse.
- **Grab when cursor enters window** — the mouse pointer becomes the mouse pointer of your guest operating system when the mouse pointer enters the virtual machine console window. This option does not apply when the virtual machine is in full screen mode.
- **Enable copy and paste to and from virtual machine** — use this option for copying and pasting text between the host and the virtual machine and among virtual machines. The clipboards of the two operating systems communicate with each other. When the mouse pointer of your guest operating system exits the console window, the contents of the guest operating system clipboard are copied into the host operating system clipboard. Similarly, each time the mouse pointer of your host operating system is grabbed by the console window, the contents of the host operating system clipboard are copied into the guest operating system clipboard.

NOTE At this time, you cannot copy and paste between Red Hat Linux 7.0 through 7.3 and Windows 2000. It does not matter which operating system is the guest and which is the host.

NOTE The best way to understand the cursor options is to play with them for a while. They describe how the mouse pointer should behave when you are in windowed mode; that is, the virtual machine is in a console window, not in full screen mode, and you can see your host operating system's desktop.

Setting Hot Key Preferences

Use the **Hot Key** tab to change which combination of keys (the Ctrl, Alt, and Shift keys in combination with other keys) are passed to the guest operating system or are intercepted by VMware Server.



You can construct your own custom hot-key combination if, for example, the default Ctrl+Alt combination conflicts with another application on the host that processes the same hot-key combination.

For example, you may want to change hot key combinations from Ctrl-Alt-<key> to Ctrl-Shift-Alt-<key> to prevent VMware Server from intercepting Ctrl-Alt-Delete instead of letting the key combination be sent to the guest operating system.

Or, you may be using PC Anywhere to connect to a machine running a console. The console is connected to a virtual machine running in full screen mode, and you want to run a different application. Normally, to return to window mode, you press Ctrl-Alt, but PC Anywhere processes Ctrl-Alt key combinations, so VMware Server cannot receive the key combination. Thus, you need to use an alternate hot-key combination to get out of full screen mode.

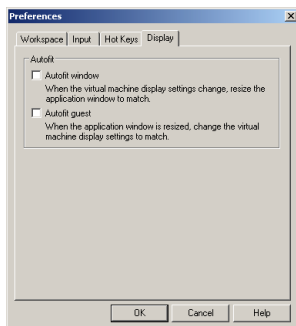
NOTE Because Ctrl-Alt is the key combination that tells VMware Server to release (ungrab) mouse and keyboard input, combinations that include Ctrl-Alt are not passed to the guest operating system. If you need to use such a combination — for example, Ctrl-Alt-<Fkey> to switch between Linux workspaces in a virtual machine — press Ctrl-Alt-Space, release Space without releasing Ctrl and Alt, then press the third key of the key combination you want to send to the guest.

You can also construct your own custom hot-key combination. Select **Custom**, then select the combination of Ctrl, Alt and Shift keys. You specify whether each key is:

- **Down** — where you must press the key down as part of the key combination.
- **Up** — where you must leave the key unpressed as part of the key combination.
- **Either** — where it does not matter if you press the key.

Setting Display Preferences

On both Linux and Windows hosts, the Display tab lets you adjust the way in which the console and the host display accommodate a different guest operating system resolution.



Use **Autofit** preferences to control how the console window behaves when Autofit is active. Check the **Autofit window** box to have VMware Server change the console window size to match the guest operating system resolution. This is the same as choosing **View > Autofit Window**. Check the **Autofit guest** box to have VMware Server change the guest operating system display resolution to match the console window size. This is the same as choosing **View > Autofit Guest**.

On Linux hosts only, the **Display** tab also lets you configure the display settings of the host and guest when you enter full-screen mode.

Setting Global Preferences for VMware Server

The Host Settings dialog box allows you to change a number of settings that apply to VMware Server.

To change these settings, choose **Host > Settings**. You must be either the root or Administrator user to change these settings.

Specifying Where Virtual Machines Are Created

Use the **General** tab to specify the default location where all virtual machines on this host are created.

The directory VMware Server uses by default is displayed under **Default location for virtual machines**. To set a different directory, type in the path or click **Browse** to navigate to the directory you want to use. VMware Server creates a directory for each new virtual machine under the directory you specify here.

On a Windows host, the default folder where new virtual machines are stored is <installdrive>\Virtual Machines.

On a Linux host, the default location where new virtual machines are stored is /var/lib/vmware/Virtual Machines.

Reserving Host Memory for Virtual Machines

Select the **Memory** tab to adjust the amount of memory reserved for all running virtual machines.

The settings on the Memory tab applies no matter what virtual machine is running or who is logged on to the host computer.

For more information about memory and virtual machines, see [“Understanding Memory Usage”](#) on page 154 and [“Allocating Memory to a Virtual Machine”](#).

Adjusting Priorities for Virtual Machine Processes (Windows Hosts Only)

VMware Server for Windows gives you the option to set the priority that the Windows process scheduler gives to your virtual machines when mouse and keyboard input are going to a particular virtual machine and when input is not going to that virtual machine.

You can adjust these settings to improve overall system performance based on the relative priority of work you are doing in various virtual machines and on the host computer.

The settings on the Priority tab apply to all virtual machines for the user currently logged on to the host computer. The priority settings do not affect priority settings made by any other user on the computer.

This setting is not available on a Linux host.

To set priority preferences, in the Host Settings dialog box, click the **Priority** tab.

The priority settings here are used by all virtual machines unless a virtual machine configuration overrides the global setting with a local setting. To change the local setting for a particular virtual machine, and override the global settings, open the virtual machine you want to adjust, choose **VM > Settings**, click the **Options** tab, select **Advanced**, then use the drop-down lists under **Process priorities** to make the setting you want for that virtual machine.

There are three possible process scheduling priorities: low, normal and high. The typical process on the host runs at normal priority. If you set the priority of the virtual machine to low, that virtual machine has lower priority than other processes on the host. If you set the priority of the virtual machine to normal, that virtual machine contends with all the processes on the host. If you set the virtual machine priority to high, that virtual machine gets priority over other processes on the host.

VMware Server gives you the option to automatically change the process scheduling priority that applies when the virtual machine grabs and ungrabs keyboard and mouse input. For more information on grabbing and ungrabbing input, see [“Changing Your Input Settings”](#) on page 119.

The four possible process priorities are

- **high - normal:** When input is grabbed, VMware Server gets priority over other processes on the host. When input is not grabbed, VMware Server contends with all the processes on the host.
- **high - low:** When input is grabbed, VMware Server gets priority over other processes on the host. When input is not grabbed, VMware Server has lower priority than other processes on the host.
- **normal - normal:** When input is grabbed, VMware Server contends with all the processes on the host. When input is not grabbed, VMware Server contends with all the processes on the host.
- **normal - low:** When input is grabbed, VMware Server contends with all the processes on the host. When input is not grabbed, VMware Server has lower priority than other processes on the host.

VMware Server defaults to process priority **normal - normal**.

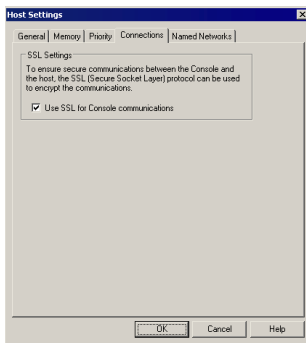
Configuring Virtual Machines to Take and Revert to Snapshots

You can configure your virtual machine to take and revert to snapshots in the background. In the VMware Server Console for Windows and Linux hosts, go to the Host > Settings > Priority tab to enable this option. For more information, go to [“Snapshot Actions as Background Activity”](#) in the *VMware Server Virtual Machine Guide*.

Enabling SSL for VMware Server Console Connections

Select the **Connections** tab to enable SSL for console connections over a network.

To enable SSL for console connections from the console, on the **Connections** tab, check the **Use SSL for Console communications** check box.



For more information about SSL, see [“Securing Your Remote Sessions”](#) on page 90.

Creating Network Labels

Beginning with the RC1 release, VMware Server supports using VMware Virtual Center to manage the virtual machines on your VMware Server hosts. To use VirtualCenter you must create labels for each virtual network adapter. VirtualCenter uses labels to identify which virtual network adapter is associated with which physical network.

Each virtual network adapter needs a label:

- To avoid confusion in a multiple-host, multiple-network environment. This is the typical VirtualCenter environment. VirtualCenter can manage virtual machines on multiple VMware Server hosts.
- To let you migrate virtual machines between VirtualCenter hosts. Virtual machines can be migrated from hosts on the same network only. The label ensures that VirtualCenter knows to which network the virtual machine is connected.
- To let you create virtual machines from the VirtualCenter client.

- To let you edit the virtual network configuration of an existing virtual machine from the VirtualCenter client.

NOTE If you configure virtual machines from the VirtualCenter client, you cannot take advantage of VMware Server features like snapshots.

If the adapter has no label, VirtualCenter cannot recognize the adapter. If a virtual machine is configured for a network name that does not exist, the virtual network adapter is disconnected when you power on the virtual machine.

You can create labels for the existing default virtual network adapters — like VMnet0, the default bridged network adapter, or VMnet8, the default NAT adapter. You configure the adapters in VMware Server. You can configure each adapter with bridged, host-only, NAT or custom networking. The type of networking configuration is irrelevant to VirtualCenter. VirtualCenter is concerned with the network label only.

NOTE To create and manage all your virtual machines from the VirtualCenter client, you should assign unique labels to each host-only adapter on a VMware Server host. This way, you can easily identify on which host each host-only network resides. However, if you have a VMware Server host where all the virtual machines use host-only networking, you could decide to not give the host-only adapter a network label.

For information on configuring new virtual network adapters, see [“Adding and Modifying Virtual Network Adapters”](#).

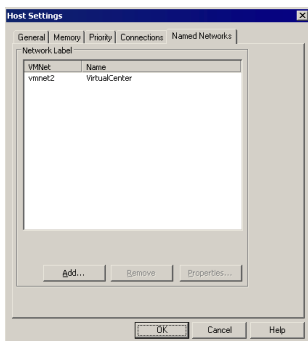
For more information on managing VMware Server virtual machines with VirtualCenter, see [“Using VirtualCenter to Manage Virtual Machines”](#) on page 131.

After your virtual network adapters are configured to your liking, create labels for each adapter so VirtualCenter can correctly manage the virtual machines on the host.

Creating Network Labels from the VMware Server Console

To create network labels for virtual machines managed by VirtualCenter, complete the following steps in a console.

- 1 Connect to the VMware Server host with a console, then choose **Host > Settings**. The Host Settings dialog box appears.
- 2 Click the **Named Networks** tab.



NOTE If the Named Networks tab does not appear in the Host Settings dialog box, then the VMware Server host has not been discovered by VirtualCenter. For information about adding a VMware Server host to VirtualCenter, see your VirtualCenter documentation.

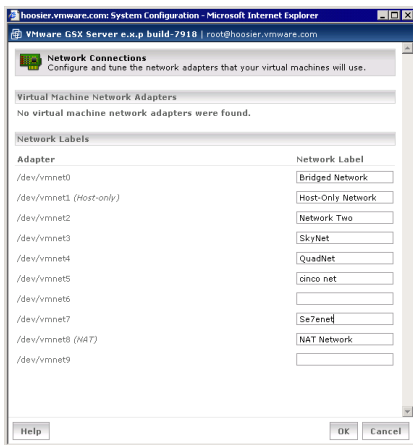
- 3 To add a label, click **Add**. The Add Named Network dialog box appears.
- 4 Select the virtual network adapter from the **Adapter** list. On a Windows host, if an adapter is configured for bridged, host-only or NAT networking, its networking type is indicated next to the adapter name.
- 5 Enter the name of the label in the **Label** entry field.
- 6 Click **OK** to add the label, then click **OK** to save your changes.

Creating Network Labels from the VMware Management Interface

To create network labels for virtual machines managed by VirtualCenter, complete the following steps in the management interface.

- 1 Log on to the VMware Management Interface as the Administrator (VMware Server for Windows hosts) or root user (VMware Server for Linux hosts). For information, see [“Logging On to the VMware Management Interface”](#) on page 99.
- 2 On the Status Monitor page, click the **Options** tab. The Options page appears.


- 3 Click **Network Connections**. The Network Connections page appears.



NOTE If the Network Connections link does not appear on the Options page, then the VMware Server host has not been discovered by VirtualCenter. For information on adding a VMware Server host to VirtualCenter, see your VirtualCenter documentation.

- 4 For each network adapter, add a label in the corresponding field under **Network Label**. On a Windows host, if an adapter is configured for host-only or NAT networking, its networking type is indicated next to the adapter name.
- 5 Click **OK** to save your changes.

Setting MIME Type to Launch the VMware Server Console

From the VMware Management Interface, you can connect to a virtual machine from a console by clicking the terminal icon () for that virtual machine. Before doing so, some browsers may require you to define a MIME type of `x-vmware-server console` and associate it with the console program file. Internet Explorer is automatically configured when you install the console.

The procedure for setting a MIME type for the console is similar for Windows and Linux hosts. Both involve writing a short script that provides the command to launch the console. You can choose to launch the console that was installed with VMware Server or you can launch the console that was installed from a file downloaded from the management interface.


NOTE You may not need to create a helper file manually if your browser prompts you to associate VMware Server with the file type.

Setting MIME Type for the VMware Server Console

- 1 Open a text editor and do one of the following.
 - On a Windows host, write a short batch file called `vmwareserver-helper.bat`. The batch file must contain the following line:
`"<path_to_vmwareserver>" -o "%1"`
 where the default `<path_to_vmwareserver>` is
`C:\Program Files\VMware\VMware Server\vmware.exe`
 - On a Linux host, write a short shell script called `vmware-vms-helper.sh`. The shell script must contain the following two lines:
`#!/bin/sh`
`"<path_to_vmware-vms>" -o $1 > /dev/null 2>&1;`
 where the default `<path_to_vmware-vms>` is `/usr/bin/vmware`.
- 2 Save the file in a location of your choice.

NOTE On a Linux host, change to the directory where you saved the file and give yourself permission to execute the file.

```
chmod +x vmware-server-helper.sh
```


- 3 Use the browser to connect to the server you want to manage.
- 4 Click the terminal icon () for the virtual machine you want to view in a console.
- 5 A dialog box asks what you want to do with the file. Click **Advanced**.
- 6 In the New Type dialog box, in the **Description of type** field, type `VMware Server`.
- 7 In the **File extension** field, type `xvm`.
- 8 In the **MIME type** field, type `application/x-vmware-server-console`.
- 9 In the **Application to use** field, type the path to `vmwareserver-helper.bat` or `vmware-server-helper.sh`.
- 10 Click **OK** twice. Your browser is now set to launch the console when you click the terminal icon in the future.

Setting MIME Type for VMware Server Console Installed from the Management Interface Download

- 1 Open a text editor and do one of the following.
 - On a Windows host, write a short batch file called `vmwareConsole-helper.bat`. The batch file must contain the following line:
`"<path_to_vmwareConsole>" -o "%1"`
 where the default `<path_to_vmwareConsole>` is
`C:\Program Files\VMware\VMware Server Console\vmware.exe`
 - On a Linux host, write a short shell script called `vmware-server-console-helper.sh`. The shell script must contain the following two lines:
`#!/bin/sh`
`"<path_to_vmware-server-console>" -o $1 > /dev/null 2>&1;`
 where the default `<path_to_vmware-server-console>` is
`/usr/bin/vmware-server-console`.
- 2 Save the file in a location of your choice.

NOTE On a Linux host, change to the directory where you saved the file and give yourself permission to execute the file.

```
chmod +x vmware-server-console-helper.sh
```

- 3 Use the browser to connect to the server you want to manage.
- 4 Click the terminal icon () for the virtual machine you want to view in a console.
- 5 A dialog box asks what you want to do with the file. Click **Advanced**.
- 6 In the New Type dialog box, in the **Description of type** field, type `VMware Server Console`.
- 7 In the **File extension** field, type `xvm`.
- 8 In the **MIME type** field, type `application/x-vmware-console`.
- 9 In the **Application to use** field, type the path to `vmwareConsole-helper.bat` or `vmware-server-console-helper.sh`.
- 10 Click **OK** twice. Your browser is now set to launch the console when you click the terminal icon in the future.

Using VirtualCenter to Manage Virtual Machines

If you are using VMware VirtualCenter to manage your VMware Server virtual machines, you must take certain steps before you can create virtual machines on a VMware Server host from a VirtualCenter client. In addition, you need to be aware of certain differences when you connect to a virtual machine from a VirtualCenter client.

For information about using VirtualCenter, see the VirtualCenter product documentation at http://www.vmware.com/support/pubs/vc_pubs.html.

Creating Virtual Machines from a VirtualCenter Client

Before you start creating virtual machines on a VMware Server host from a VirtualCenter client, complete the following tasks:

- 1 Confirm VirtualCenter and VMware Server are installed and operating correctly.
- 2 Locate the VMware Server host in VirtualCenter, and supply the credentials for a user account on the VMware Server host to use when running virtual machines.
- 3 Create network labels for your network adapters on the VMware Server host. VirtualCenter uses labels to identify which virtual network adapter is associated with which physical network. For information, see “[Creating Network Labels](#)” on page 125.
- 4 Create the virtual machines from a VirtualCenter client.

NOTE If you are creating a Red Hat Enterprise Linux 4 virtual machine, select **Other Linux 2.6.x Kernel**.

Connecting to a Virtual Machine from a VirtualCenter Client

In general, when a virtual machine on a VMware Server host is managed by VirtualCenter, it retains all the features and functionality that VMware Server provides. However, when you connect to a virtual machine from a VirtualCenter client, certain features accessible from the VMware Server Console are not available from the console in a VirtualCenter client.

Even though some features might be unavailable from the VirtualCenter client, these features still work with the virtual machine when connected with the VMware Server Console. The unavailable options include:

- **Snapshots are unavailable on a VirtualCenter client.** Snapshots are not available when you connect to a VMware Server virtual machine from a VirtualCenter client. If you take a snapshot of a VMware Server virtual machine when you connect to

the virtual machine with a VMware Server Console, and later connect to the virtual machine from a VirtualCenter client, the snapshot still exists.

You cannot update, remove, or revert to the current snapshot, or take a new snapshot when you connect to the virtual machine from a VirtualCenter client. When you connect to the virtual machine with a console, you can interact with the snapshot again.

- **Virtual machines created from a VirtualCenter client run as a specific user account.** A virtual machine created from a VirtualCenter client cannot be configured to run as the user that powers it on. You supply the user account information when you add the VMware Server host to VirtualCenter.
- **Virtual machines created from a VirtualCenter client are not private.** To make the virtual machine available only to the VirtualCenter user account, connect to the virtual machine with the VMware Server Console and change the setting there. For information, see [“Only You Can See Virtual Machines You Create”](#) on page 84.
- **You cannot specify a name for virtual disk files when you create a virtual machine from a VirtualCenter client.** The virtual disk files use the virtual machine name as the basis for the filenames. You can use the VMware Server Console to create more virtual disks with filenames that do not reflect the virtual machine name.
- **Virtual machines can use only the DVD/CD-ROM drive on the VMware Server host.** To use the client DVD/CD-ROM drive on a remote system, connect to the virtual machine with the VMware Server Console.
- **You cannot browse a remote file system when connected to the virtual machine from a VirtualCenter client.** You need to know the path to a file — such as an ISO image — and must enter it manually.

CHAPTER 5 **Moving and Sharing Virtual Machines**

This chapter provides information on how to move your virtual machines from one host to another, or elsewhere on the same host, plus recommendations on how to share virtual machines with other users.

This chapter also includes information on how to move a virtual machine running under VMware GSX Server 3 and VMware Workstation 5.x to a host running VMware Server and covers the following topics:

- [“Moving a VMware Server Virtual Machine”](#) on page 133
- [“Moving VMware GSX Server 3 Virtual Machine to a New Host”](#) on page 136
- [“Moving Older Virtual Machines”](#) on page 138
- [“Sharing Virtual Machines with Other Users”](#) on page 142

NOTE When you move a virtual machine to a new host computer or to a different directory on the same host computer — or when you rename a directory in the path to the virtual machine’s configuration file — VMware Server generates a different MAC address for each virtual Ethernet adapter (unless you specified the MAC address manually). For additional information, see [“Maintaining and Changing the MAC Address of a Virtual Machine”](#).

For information about moving virtual machines between VMware products, see the *VMware Virtual Machine Mobility Planning Guide* on the VMware Web site.

Moving a VMware Server Virtual Machine

This section describes how to move a virtual machine created under VMware Server to another host running VMware Server or to a different location on the same host. The process is not difficult, and in most cases you can even move your virtual machine from a Windows host to a Linux host — or vice versa.

NOTE These instructions assume that you are using a virtual disk — stored in one or more `.vmdk` files on your host computer.

It's always safest to make backup copies of all the files in your virtual machine's directory before you start a process like this.

CAUTION VMware recommends you not migrate a Red Hat Linux 7.3 or 7.2 virtual machine between hosts when one host is running on an AMD processor and the other is running on an Intel processor. For more information, read the Known Issues sections for these guest operating systems in the *VMware Guest Operating System Installation Guide*, available on the VMware Web site.

The following sections further describe moving a VMware Server virtual machine:

- [“Virtual Machines Use Relative Paths”](#) on page 134
- [“Preparing Your Virtual Machine for the Move”](#) on page 134
- [“Moving a Virtual Machine to a New Host”](#) on page 135

Virtual Machines Use Relative Paths

The path names for all files associated with a VMware Server virtual machine are relative, meaning the path to each file is relative to the currently active directory. For example, if you are in the virtual machine's directory, the relative path to the virtual disk file is `<machine name>.vmdk`.

Preparing Your Virtual Machine for the Move

- 1 Shut down the guest operating system and power off the virtual machine. If the virtual machine is suspended, resume it, then shut down the guest.
- 2 Do one of the following:
 - If you are moving the virtual machine to a new host and have a network connection between the original host machine and the new host, you are finished with the preparations on the original host. If you do not have a network connection, you need to have a way of moving the virtual disk (`.vmdk`) files from the virtual machine's directory to the new host. You could move them to a shared network directory, for example, or burn them to CD-ROMs or DVDs.

Once you know how you are going to move the virtual machine, go to [“Moving a Virtual Machine to a New Host”](#) on page 135.

- If you are moving this virtual machine to another directory on this host, then you are ready to make the move. Copy all the files in the virtual machine's original directory to the new location. If you stored any files in directories other than the virtual machine directory, be sure to move them into a directory of the same name and same position relative to the location of the virtual machine.

Start the VMware Server Console and open the new virtual machine you just moved. Choose **File > Open Virtual Machine**, then browse to the virtual machine's configuration (.vmtx) file.

Moving a Virtual Machine to a New Host

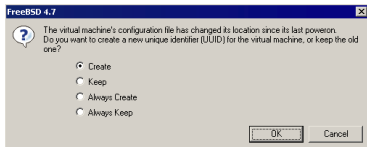
- 1 Make sure VMware Server is installed and working correctly on the new host.
- 2 Create a directory on the new host for the virtual machine you are moving. Locate the virtual disk files you are moving and copy them into the new directory. Be sure to copy all the files in the virtual machine's original directory. If you stored any files in directories other than the virtual machine directory, be sure to move them into a directory of the same name and same position relative to the location of the virtual machine. Set permissions on the directory so that it is accessible to all users of the virtual machine.

If, for some reason, you are **not** moving a file, make sure you do not have any paths pointing to that file. Use the virtual machine settings editor and check to see if your virtual machine is pointing to the correct location for files (choose **VM > Settings**) you do not move. In the virtual machine settings editor, select each device and be sure that any devices with associated files are pointed to the correct files. Also, check the Options tab to be sure the location for the redo-log file is correct.

NOTE If you have taken a snapshot of the virtual machine, you can simplify the move by removing the snapshot — or reverting to the snapshot, then removing it. If you want to keep the snapshot, be sure to move the redo-log (.REDO) files along with all the other files in the virtual machine's directory.

- 3 Launch the VMware Server Console and open the virtual machine you just moved. Choose **File > Open Virtual Machine**, then browse to the virtual machine's configuration (.vmtx) file.

- The first time you power on the virtual machine, you are asked to keep the existing UUID or create a new one.



If you are using the UUID for management purposes, you should select **Keep**, then click **OK** to continue powering on the virtual machine. For more information about the UUID, see [“Identifying a Virtual Machine by Its UUID”](#) on page 92.

Moving VMware GSX Server 3 Virtual Machine to a New Host

If you want to move the location of a virtual machine created with VMware GSX Server 3, it is recommended to upgrade it for full compatibility with VMware Server before moving it. To do so, run the virtual machine under VMware Server and use **VM > Upgrade Virtual Hardware**. If you upgrade the virtual hardware, you can then follow the instructions in [“Moving a VMware Server Virtual Machine”](#) on page 133.

If you upgrade the virtual machine, you can no longer run it under VMware GSX Server 3. If you need to run the virtual machine under both VMware GSX Server 3 and VMware Server, do not upgrade the virtual hardware. You can use a VMware Server Console to connect a VMware GSX 3 Server host, but you cannot use a VMware GSX Server Virtual Machine Console to connect to a host running VMware Server.

NOTE These instructions assume that you are using a virtual disk stored in one or more `.vmdk` files on your host computer. It’s always safest to make backup copies of all the files in your virtual machine’s directory before you start a process like this.

The following sections explain how to prepare and move the VMware GSX Server 2 or 3 to a new host, and cover the topics:

- [“Virtual Machines Use Relative Paths”](#) on page 137
- [“Preparing Your Virtual Machine for the Move”](#) on page 137
- [“Moving a Virtual Machine to a New Host”](#) on page 138

Virtual Machines Use Relative Paths

The path names for all files associated with a virtual machine created under VMware GSX Server 3 are relative, meaning the path to the each file is relative to the currently active directory. For example, if you are in the virtual machine's directory, the relative path to the virtual disk file is <machine name>.vmdk.

To move virtual machines created in a VMware product other than VMware GSX Server 3 higher, or VMware Workstation 5.x, see ["Moving Older Virtual Machines"](#) on page 138.

Preparing Your Virtual Machine for the Move

- 1 Use VMware Server to connect to the virtual machine. If the virtual machine has more than one virtual disk and if the virtual disks use different disk modes, you must use the Configuration Editor (choose **Settings** > **Configuration Editor**) to change one or more of the virtual disks so they all use the same mode.
- 2 Be sure the guest operating system is completely shut down. If the virtual machine is suspended and its virtual disks are in persistent or nonpersistent mode, resume it, then shut down the guest operating system.
- 3 If your virtual machine is using disks in undoable mode, it is best to commit or discard the changes when the guest operating system shuts down. If you cannot commit or discard the changes to your disk, read ["Considerations for Moving Disks in Undoable Mode"](#) on page 141.
- 4 Do one of the following:
 - If you are moving the virtual machine to a new host and have a network connection between the original host machine and the new host, you are finished with the preparations on the original host. If you do not have a network connection, you need to have a way of moving the virtual disk (.vmdk) files from the virtual machine's directory to the new host. You could move them to a shared network directory, for example, or burn them to CD-ROMs or DVD-ROMs.

Once you know how you are going to move the virtual machine, go to ["Moving a Virtual Machine to a New Host"](#).

- If you are moving this virtual machine to another directory on the same host, you are ready to make the move. Copy all the files in the virtual machine's original directory to the new location. If you stored any files in directories other than the virtual machine directory, be sure to move them into a directory of the same name and same position relative to the location of the virtual machine.

Launch the console and open the virtual machine you just moved. Choose **File** > **Open**, then browse to the virtual machine's configuration (.vmtx) file.

Moving a Virtual Machine to a New Host

- 1 Make sure VMware Server is installed and working correctly on the new host.
- 2 Locate the virtual disk files you are moving and copy them into the new virtual machine directory. Be sure to copy all the files in the virtual machine's original directory. If you stored any files in directories other than the virtual machine directory, be sure to move them into a directory of the same name and same position relative to the location of the virtual machine. Set permissions on the directory so that it is accessible to all users of the virtual machine.

If, for some reason, you are **not** moving a file, make sure you do not have any relative or absolute paths pointing to that file. Use the virtual machine settings editor and check to see if your virtual machine is pointing to the correct location for files you do not move. In the virtual machine settings editor, select each device and be sure that any devices with associated files are pointed to the correct files. Also, check the Options tab to be sure the location for the redo-log file is correct.

In addition, check to see you do not have any absolute paths pointing to any files you **are** moving.

NOTE If your virtual machine is using disks in undoable mode, it is best to commit or discard the changes when you shut down the guest operating system under VMware Server 2. If you cannot commit or discard the changes to your disk, read [“Considerations for Moving Disks in Undoable Mode”](#) on page 141.

- 3 Launch the VMware Server Console and open the virtual machine you just moved. Choose **File** > **Open Virtual Machine**, then browse to the virtual machine's configuration (.vmtx) file.

Moving Older Virtual Machines

If you have created a virtual machine using VMware GSX Server 2 or another VMware product, you must upgrade the virtual hardware the first time you run it under VMware Server. Once you have done this, you can follow the instructions in [“Moving a VMware Server Virtual Machine”](#) on page 133.

If you have created a virtual machine using VMware GSX Server 2 or another VMware product, and you want to move it to a different computer or to another directory on your host, you need to perform the following tasks.

NOTE These instructions assume that you are using a virtual disk — stored in a set of .vmdk or .dsk files on your host computer.

It is always safest to make backup copies of all the files in your virtual machine's directory before you start a process like this.

The following sections further describe moving older virtual machines:

- [“Virtual Machines May Use Relative or Absolute Paths”](#) on page 139
- [“Preparing Your Virtual Machine for the Move”](#) on page 139
- [“Preparing the New Host Machine”](#) on page 140
- [“Considerations for Moving Disks in Undoable Mode”](#) on page 141

Virtual Machines May Use Relative or Absolute Paths

In VMware Server 1, the path names for all files associated with a virtual machine were absolute, or fully qualified, meaning the complete route to the files on the host was stored. For example, the absolute path to a virtual disk file might be C:\Documents and Settings\\My Documents\My Virtual Machines\\

With VMware GSX Server 2 and higher, path names to files are relative, meaning the path to the each file is relative to the currently active directory. For example, if you are in the virtual machine's directory, the relative path to the virtual disk file is <machine name>.vmdk.

Preparing Your Virtual Machine for the Move

- 1 Open the virtual machine using the VMware product with which you created it. If the virtual machine has more than one virtual disk and if the virtual disks use different disk modes, you must use the Configuration Editor (choose **Settings > Configuration Editor**) to change one or more of the virtual disks so they all use the same mode.
- 2 Be sure you know whether the virtual disk is set up as an IDE disk or a SCSI disk. You can check this in the virtual machine settings editor.

Also, note the size of the virtual disk you are moving. You need this information when you prepare the new host machine, as described in the next section.

- 3 Be sure the guest operating system is completely shut down. If the virtual machine is suspended, resume it using the VMware product with which you created the virtual machine, then shut down the guest operating system.

NOTE Do not move a suspended virtual machine from one host to another.

- 4 If your virtual machine is using disks in undoable mode, it is best to commit or discard the changes when the guest operating system shuts down. If you cannot commit or discard the changes to your disk, read [“Considerations for Moving Disks in Undoable Mode”](#) on page 141.
- 5 If you have a network connection between the original host machine and the new host, you are finished with the preparations on the original host. If you do not have a network connection, you need to have a way of moving the virtual disk (.vmdk) files from the virtual machine’s directory to the new host. You could move them to a shared network directory, for example, or burn them to CD-ROMs or DVDs.

NOTE If your disks are using undoable mode and you have not committed or discarded your changes, you must also move the redo-log (.REDO) file to the new host computer.

Preparing the New Host Machine

- 1 Make sure VMware Server is installed and working correctly on the new host.
- 2 Start the VMware Server Console and run the New Virtual Machine Wizard. Select the appropriate guest operating system for the virtual machine you are moving.

Choose a virtual disk for your hard drive and use a drive type (IDE or SCSI) that matches the type of the virtual disk you plan to move.

Select all appropriate network, floppy and CD-ROM settings. Do not make any changes with the virtual machine settings editor at this point.

Save your settings and close the virtual machine settings editor.
- 3 In the directory just created for the new virtual machine, delete the brand new .vmdk files that were just created.
- 4 Locate the virtual disk files you are moving and copy them into the new virtual machine directory. Set permissions on the directory so that it is accessible to all users of the virtual machine.

NOTE If your virtual machine is using disks in undoable mode and you did not commit or discard your changes before the move, you must also move the redo-log (.REDO) file to the new host computer.

- 5 In the console's **Inventory** list, select the virtual machine you just created, then choose **VM > Settings**.
- 6 Be sure the virtual machine is configured to use the virtual disk files you moved from the original host. You need to confirm that the new disk's settings — IDE or SCSI and the filename for the first `.vmdk` file — match those that were used on the original host machine.

The device listing for the hard drive shows whether it is SCSI or IDE. If that setting does not match the virtual disk you are moving, select the hard disk and click **Remove**. Then click **Add** and use the Add Hardware Wizard to add an IDE or SCSI disk as appropriate. Be sure to specify IDE or SCSI when you reach the Select a Disk Type screen in the wizard.

Be sure the filename and path for the virtual disk match the actual filename and location for the first `.vmdk` file used by the virtual machine you are moving.

Considerations for Moving Disks in Undoable Mode

Once you commit or discard changes made to an older virtual disk in undoable mode, you can move your disk between Linux and Windows host operating systems. You can also move your disk to different locations on your computer and to other computers with the same host operating system.

However, if you cannot or do not want to commit or discard the changes made to your undoable disk, note the following:

- You can always move a disk in undoable mode between host operating systems of the same general type (for example, between two Microsoft Windows systems, or between two Linux systems). Depending upon how the disk was first set up, you may have to place the disk and its redo log in a directory that has a path name identical to that of the current directory.
- You might be able to move the disk in undoable mode between Windows and Linux host systems, or move the disk to a different directory on your current system, if there is no path name information in the virtual machine's configuration file.

Follow these steps to check the configuration and see whether or not you can move your undoable disk without committing or discarding changes:

- 1 Launch a VMware GSX Server 3 console.

If you are moving a disk in undoable mode from one computer to another computer, launch a VMware GSX Server 3 console on the computer that currently has the disk.

- 2 Open the configuration file for the virtual machine that uses the undoable mode disk you wish to move.

In the console window, select **File > Open** and choose the configuration file of the virtual machine with the disk you want to move.

- 3 Open the Configuration Editor. Choose **Settings > Configuration Editor**.
- 4 Examine the entry for your virtual disk to see whether it includes a full path to the first virtual disk file. For example, on a Windows host, you might see a disk file listing like this:

```
My Documents\My Virtual Machines\Windows 2000\Windows 2000.vmdk
```

Entries for SCSI disks are similar.

If your disk file information resembles the example above (with a full path to the first disk file) and you have not committed or discarded changes to the undoable disk, the following rules apply:

- You can move the disk to another computer of the same type only (Windows to Windows or Linux to Linux). You cannot move the disk to a computer of a different type (Windows to Linux or vice versa).
- You must place the virtual machine's other files (including `.vnx` and `.REDO` on Windows, and `.vnx` or `.cfg` and `.REDO` on Linux) in the same relative location on the new computer. In other words, if the virtual machine's files reside in `My Documents\My Virtual Machines\Windows 2000\` on the original host computer, you must place them in that same location on the new host computer.
- You cannot move the disk to another directory on the current system.

If your disk file information does not contain a path, it looks like this:

```
Windows 2000.vmdk
```

If your disk entry resembles the one above (just a filename with a `.vmdk` extension), you can move the disk and redo log anywhere you wish.

Sharing Virtual Machines with Other Users

If you intend to have other users access your virtual machines, you should consider the following points:

- On Windows hosts, the virtual machine files should be in a location on a system that is accessible to those users. When you configure the virtual machine in the

New Virtual Machine Wizard, you can specify a location for the virtual machine elsewhere on your system or on the network.

- On Linux hosts, permissions for the virtual machine files — especially the configuration file (.vmx) and virtual disks (.vmdk) — should be set for other users according to how you want them to use the virtual machine. For instance, if you want users to run a virtual machine but not be able to modify its configuration, do not make the configuration file writable.
- If your virtual machine was created under VMware GSX Server or another VMware product (such as VMware Workstation 5.x) and uses independent disks in nonpersistent mode, consider changing the location of the redo-log file, since by default it is placed in your TEMP directory, to which other users might not have access. To change the location of the redo-log file, take the following steps.
 - a With the virtual machine powered off, open the virtual machine settings editor. Choose **VM > Settings**.
 - b Click the **Options** tab.
 - c Click **Browse** and select a directory that is shared with other users.
 - d Click **OK** to save the change and close the virtual machine settings editor.
- The virtual machine must be located in a directory with permissions set so that it is accessible to all users of the virtual machine.
- The virtual machine must not be private. For more information, see [“Only You Can See Virtual Machines You Create”](#) on page 84.

CHAPTER 6 Performance Tuning and the VMware Server Host

This chapter provides suggestions for getting the best performance from VMware Server and your virtual machines, and covers the following topics:

- [“Configuring and Maintaining the Host Computer”](#) on page 145
- [“Configuring VMware Server”](#) on page 146
- [“Understanding Memory Usage”](#) on page 154

Configuring and Maintaining the Host Computer

The host computer is an obvious place to look to improve performance. This section discusses these key areas:

- [“Location of the Working Directory”](#) on page 145
- [“Defragmentation of Disk Drives”](#) on page 145
- [“Adequate Free Disk Space”](#) on page 146
- [“NIC Interrupts Coalescing”](#) on page 146

Location of the Working Directory

The installer locates the working directory—holding the virtual disk files—on the host computer. You can customize your configuration to place the working directory or the virtual disk files on a different physical computer. You might experience performance advantages to such customizing.

Defragmentation of Disk Drives

Host disks and virtual disks affect the performance of VMware Server.

Host Hard Drives

Performance is weakened by fragmentation of the physical disk holding the virtual machine’s working directory or virtual disk files. Fragmentation of the host disk can affect any or all of the following:

- The files that hold a virtual disk
- The files that store newly saved data when you take a snapshot
- The files that hold information used in suspending and resuming a virtual machine

If you are experiencing slow disk performance in the virtual machine, or if you want to improve the speed of suspend and resume operations, check to be sure the host disk that holds the virtual machine's working directory and virtual disk files is not badly fragmented. If it is fragmented, you can improve performance by running a defragmentation utility to reduce fragmentation on that host disk.

Virtual Drives

VMware strongly recommends that you defragment using a guest operating mechanism before taking the first snapshot.

VMware Server makes all its changes to the redo log, not to the original disk, when you run a defragmenting program on the guest after a snapshot. You permanently lose the ability to defragment inside the original disk.

Every sector that moves is copied to the redo log, making the virtual machine redo log extremely large when the disk is heavily fragmented and you run defragmentation after a snapshot.

Adequate Free Disk Space

For better performance, avoid having very low free disk space on the host disk. Performance can degrade considerably when VMware Server has to use a nearly full host hard disk to write guest sparse disk, snapshot, checkpoint, or redo files.

NIC Interrupts Coalescing

Increasing host NIC interrupt coalescing can improve performance for workloads involving heavy network traffic into the guest. Interrupt coalescing is a feature implemented in hardware under driver control on high-performance NICs, allowing the reception of a group of network frames to be notified to the operating system kernel through a single hardware interrupt.

Configuring VMware Server

The following sections offer advice and information about factors that can affect the performance of VMware Server itself. The sections do not address performance of the guest operating system or the host operating system.

- [“General VMware Server Options”](#) on page 147
- [“VMware Server on a Windows Host”](#) on page 151
- [“VMware Server on a Linux Host”](#) on page 154

NOTE In addition to the VMware Server configuration options discussed in this section, you should always install VMware Tools in any guest operating system for which a VMware Tools package exists. Installing VMware Tools provides better video and mouse performance and also greatly improves the usability of the virtual machine. For details, see [“Installing VMware Tools”](#).

General VMware Server Options

The following sections describe ways you can improve the performance of VMware Server on both Windows and Linux hosts.

Guest Operating System Selection

Make certain you select the correct guest operating system for each of your virtual machines. To check the guest operating system setting, choose **VM > Settings > Options > General**.

VMware Server optimizes certain internal configurations on the basis of this selection. For this reason, it is important to set the guest operating system correctly. The optimizations can greatly aid the operating system they target, but they might cause significant performance degradation if there is a mismatch between the selection and the operating system actually running in the virtual machine. (Selecting the wrong guest operating system is not likely to cause a virtual machine to run incorrectly, but it could degrade the virtual machine’s performance.)

Memory Settings

Make sure to choose a reasonable amount of memory for your virtual machine. Many modern operating systems have a growing need for memory, so assigning a generous amount is beneficial for the best virtual machine performance.

The same holds true for the host operating system, especially a Windows host.

The New Virtual Machine Wizard automatically selects a reasonable starting point for the virtual machine’s memory, but you might be able to improve performance by adjusting the settings in the virtual machine settings editor (choose **VM > Settings > Memory**).

If you plan to run one virtual machine at a time most of the time, a good starting point is to give the virtual machine half the memory available on the host.

Adjusting the reserved memory settings may also help. Choose **Host > Settings > Memory**.

For additional information, see [“Understanding Memory Usage”](#) on page 154.

Debugging Mode

You can configure each virtual machine to run in one of two modes — normal mode and a mode that provides extra debugging information. The debugging mode is slower than normal mode.

For normal use, make sure the virtual machine is not running in debugging mode. Choose **VM > Settings > Options** and select **Advanced**. Under **Settings**, make sure the **Run with debugging information** check box is cleared.

CD-ROM Drive Polling

Some operating systems — including Windows NT and Windows 98 — poll the CD-ROM drive every second or so to see whether a disc is present. (Doing this allows them to run autorun programs.) This polling can cause VMware Server to connect to the host CD-ROM drive, which can make the CD-ROM drive spin up while the virtual machine appears to pause.

If you have a CD-ROM drive that takes especially long to spin up, there are two ways you can eliminate these pauses.

- You can disable the polling inside your guest operating system. The method varies by operating system. For recent Microsoft Windows operating systems, the easiest way is to use TweakUI from the PowerToys utilities.

For information on finding TweakUI and installing it in your guest operating system, go to <http://www.microsoft.com> and search for TweakUI. Specific instructions depend on your operating system.

- Another approach is to configure your virtual CD-ROM drive to be disconnected when the virtual machine starts. The drive appears in the virtual machine, but it always appears to contain no disc (and VMware Server does not connect to your host CD-ROM drive).

To make this change, go to **VM > Settings**. Select the DVD/CD-ROM item in the **Device** list. Then clear the **Connect at Power On** check box.

When you want to use a CD-ROM in the virtual machine, go to the **VM > Removable Devices** menu and connect the CD-ROM drive.

Disk Options

The various disk options (SCSI versus IDE) and types (virtual or physical) affect performance in a number of ways.

Overall, SCSI disks are faster than IDE disks that uses direct memory access (DMA). However, in certain situations, such as single threaded disk access, an IDE disk that uses DMA is as fast as a SCSI disk. Inside a virtual machine, SCSI disks and IDE disks that use direct memory access (DMA) have approximately the same performance. If supported, VMware recommends that you enable DMA in SCSI disks. IDE disks can be very slow in a guest operating system that is not set to use DMA.

The easiest way to configure a Linux guest to use DMA for IDE drive access is to install VMware Tools (**VM > Install VMware Tools**). Among other things, the installation process automatically sets IDE virtual drives to use DMA.

In Windows Server 2003, Windows XP and Windows 2000, DMA access is enabled by default. The method for changing the setting varies with other Windows operating systems. See the following technical notes for details.

- [“Disk Performance in Windows NT Guests on Multiprocessor Hosts”](#)
- [“Windows 95 and Windows 98 Guest Operating System Performance Tips”](#)

When a snapshot exists, virtual disks often have very good performance for random or nonsequential access. But they can potentially become so fragmented that performance is affected. In order to defragment the disk, you must first remove the snapshot (**Snapshot > Remove Snapshot**).

When no snapshot exists, physical disks and preallocated virtual disks both use flat files that mimic the sequential and random access performance of the underlying disk. When a snapshot exists and you have made changes since powering on the virtual machine, any access to those changed files performs at a level similar to the performance of a virtual disk that does not have all space allocated in advance. If you remove the snapshot, performance is again similar to that of the underlying disk.

Overall, if no snapshot exists and you are using physical disks or preallocated virtual disks, you see somewhat better performance than that provided by other configurations.

Disk writes can be slower for virtual disks that do not have all space allocated in advance. You can improve performance for these disks by defragmenting them from the virtual machine settings editor. Choose **VM > Settings**, select the disk you want to defragment, then click **Defragment**.

Remote Disk Access

Whenever possible, do not use disks that are on remote machines and accessed over the network unless you have a very fast network. If you must run disks remotely, choose **VM > Settings > Options**, select **General** and set the **Working directory** to a directory on your local hard disk. Then take a snapshot. After you take the snapshot, changes you make are stored locally in the working directory.

Snapshots

If you do not need to use snapshots, run your virtual machine without a snapshot. This provides best performance. To be sure a virtual machine has no snapshot, choose **Snapshot > Remove Snapshot**.

Issues Installing or Running Applications in a Guest Operating System

You might notice that whenever you try to install or start a particular program in a virtual machine, the program seems to hang, crash, or complain that it is running under a debugger. VMware has seen this problem with a few programs, including the installer for the Japanese version of Trend Micro Virus Buster, the FoxPro database, the NetWare client in Windows 98, Mathcad, The Sims, and Civilization III.

You can work around this problem by disabling acceleration. Frequently, the problem occurs only during installation or early in the program's execution; in that case you should turn acceleration back on after getting past the problem. Follow these steps:

- 1 Power on the virtual machine.
- 2 Before running or installing the program that was encountering problems, disable acceleration.
Choose **VM > Settings > Advanced**, and check **Disable acceleration**.
- 3 Click **OK** to save the change and close the virtual machine settings editor.
- 4 Start the program or run the installer.
- 5 After you pass the point where the program was encountering problems, return to the virtual machine settings editor and remove the check beside **Disable acceleration**. You might be able to run the program with acceleration after it is started or installed.

NOTE Disabling acceleration can help you get past the execution problem, but it causes the virtual machine to run slowly. If the problem occurs only at startup or during installation, you can improve performance by resuming accelerated operation after the program that was encountering problems is running or is installed.

VMware Server on a Windows Host

The items in this section describe performance of VMware Server on a Windows host. For tips on configuring VMware Server on a Linux host, see [“VMware Server on a Linux Host”](#) on page 154.

Monitoring Virtual Machine Performance

VMware Server incorporates a set of counters that work with the Microsoft Performance console to allow for the collection of performance data from running virtual machines.

NOTE The Performance console is available only on Windows hosts. You cannot monitor performance for virtual machines on Linux hosts. However, you can monitor the performance of any guest operating system on the Windows host, including Linux guests.

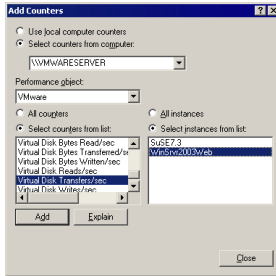
The VMware Server performance counters can monitor the following data from a running virtual machine:

- Reading and writing to **virtual disks**
- **Memory used by the virtual machine**
- **Virtual network traffic**

You can track virtual machine performance only when the VMware Server Console is open or when a virtual machine is running. The performance counters reflect the state of the virtual machine, not the guest operating system. For example, the counters can record how often the guest reads from a virtual disk, but they cannot know how many processes are running inside the guest. An explanation of each counter appears in the Performance console.

To add counters to track virtual machine performance, use the Windows Performance console. Complete the following steps.

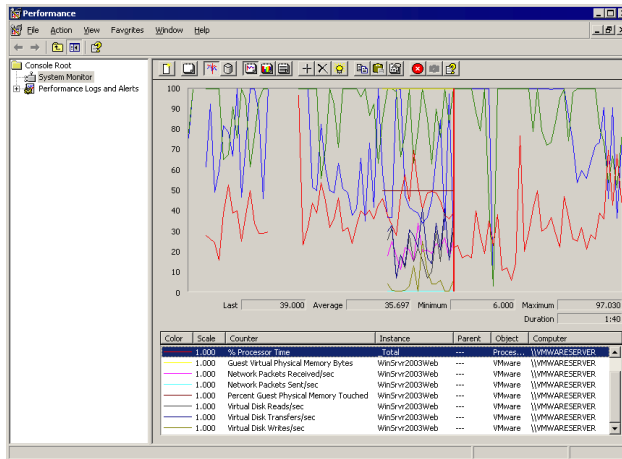
- 1 Choose **Start > Programs > Administrative Tools > Performance**. The Performance console opens.
- 2 Select **System Monitor**, then click the plus (+) sign on the toolbar, or press Ctrl+I. The Add Counters dialog box appears.



- 3 In the **Performance object** list, select **VMware**.
- 4 Decide whether you want to add all counters or select one or more counters from the list.
- 5 To use these counters for all running virtual machines, select **All instances**. To use the counters for specific virtual machines, click **Select instances from list**, then select the virtual machines you want.

NOTE For a brief description of each counter, click **Explain**. When you select a counter from the list, a description appears below the Add Counters dialog box.

6 Click **Add** to add the counters to the Performance console.



For more information about using the Performance console, use the console's in-product help or visit the Microsoft Web site.

Using Full Screen Mode

Full screen mode is faster than window mode. If you do not need to have your virtual machine and your host sharing the screen, try switching to full screen mode.

NOTE You see the most noticeable improvement using full screen mode when the guest is in VGA mode. VGA mode is any mode in which the screen is in text mode (DOS, for example, or Linux virtual terminals), or 16-color 640 x 480 graphics mode (for example, the Windows 95 or Windows 98 clouds boot screen, or any guest operating system that is running without the SVGA driver provided by VMware Tools).

Windows Host Disk Caching

On a Windows host, the Disk Properties Policies page associated with each hard drive provides a check box to enable write caching on the disk. In some cases, you can also enable advanced performance on the disk. Enabling one or both of these options can improve host disk performance in general. Enabling these options on the host disk that contains the VMware Server virtual disk files can improve VMware Server disk performance, especially when VMware Server is making heavy use of the disk.

VMware Server on a Linux Host

NOTE The items in this section describe performance of VMware Server on a Linux host. For tips on configuring VMware Server on a Windows host, see [“VMware Server on a Windows Host”](#) on page 151.

Using Full Screen Mode

Full screen mode is faster than window mode. If you do not need to have your virtual machine and your host sharing the screen, try switching to full screen mode.

NOTE You see the most noticeable improvement using full screen mode when the guest is in VGA mode. VGA mode is any mode in which the screen is in text mode (DOS, for example, or Linux virtual terminals), or 16-color 640 x 480 graphics mode (for example, the Windows 95 or Windows 98 clouds boot screen, or any guest operating system that is running without the SVGA driver provided by VMware Tools).

On a Linux host, full screen VGA mode uses the underlying video card directly, so graphics performance is quite close to that of the host. By contrast, window mode VGA requires more computer resources to emulate than window mode SVGA. As a result, if you need to run for an extended period of time in VGA mode (for example, when you are installing an operating system using a graphical installer) you should see a significant performance boost if you run in full screen mode.

Swap Space and /tmp

The amount of swap space on your host and the size of your /tmp directory affect performance. Your /tmp directory should be equivalent to 1.5 times the amount of memory on the host. For example, if your VMware Server host has 1GB of memory, make sure the host's /tmp directory is at least 1.5GB in size.

For more information on configuring swap space and the /tmp directory, read VMware knowledge base article 844 at http://www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=844.

Understanding Memory Usage

VMware Server allows you to set the memory size of each virtual machine and the amount of the host computer's memory that can be used for virtual machines. A third control governs the extent to which you want to allow the host operating system's memory manager to swap virtual machines out of physical RAM.

By adjusting these settings, you can affect both virtual machine and overall system performance.

The following sections describe how VMware Server uses the memory configuration parameters to manage virtual machines and system memory properly.

- [“Memory Use on the Host”](#) on page 155
- [“Specifying How Much RAM is Used by All Running Virtual Machines”](#) on page 155
- [“Memory Usage on Older Linux Hosts”](#) on page 157

For information on memory use for a specific virtual machine, see [“Allocating Memory to a Virtual Machine”](#).

Memory Use on the Host

Host operating systems do not behave well when they run low on free memory for their own use. When a Windows or Linux host operating system does not have enough RAM for its own use, it thrashes, that is, it constantly swaps parts of itself between RAM and its paging file on disk. To help guard against virtual machines causing the host to thrash, VMware Server enforces a limit on the total amount of RAM that can be consumed by virtual machines.

In general, the sum of the memories of all currently running virtual machines plus overhead for the VMware Server processes should not exceed the amount of physical memory on the host minus some memory that must be kept available for the host. For more information, see [“Using Additional Memory”](#) on page 156.

Some memory must be kept available on the host to ensure the host is able to operate properly while virtual machines are running. The amount of memory reserved for the host depends on the host operating system and the size of the host computer’s memory.

Specifying How Much RAM is Used by All Running Virtual Machines

You can set the amount of host RAM that VMware Server is allowed to reserve for all running virtual machines. To set this parameter, choose **Host > Settings > Memory**.

The reserved memory setting specifies a maximum amount of host RAM that VMware Server is allowed to use. But this memory is not allocated in advance. Even if multiple virtual machines are running at the same time, VMware Server might be using only a fraction of the RAM you specified here. Any unused RAM is available for use by other applications. If all the RAM you specify here is in use by one or more virtual machines,

the host operating system cannot use this memory itself or allow other applications to use it.

Virtual Machine Overhead

Virtual machines require relatively large amounts of memory to operate with reasonable performance. An individual virtual machine can use at most the amount of memory specified in its configuration file plus some overhead. The amount of overhead memory required depends upon the size of the guest's virtual disks, its behavior, and the amount of memory allocated to the virtual machine. Refer to the table below for the typical upper limit needed, based on the amount of memory allocated to the guest.

Table 6-1.

Amount of Memory Allocated to the Virtual Machine	Additional Amount of Overhead Needed
Up to 512MB	Up to 54MB
Up to 1000MB	Up to 62MB
Up to 2000MB	Up to 79MB
Up to 3600MB	Up to 105MB

The amount of RAM actually used for a particular virtual machine varies as a virtual machine runs. If multiple virtual machines run simultaneously, they work together to manage the memory.

The recommended amount of RAM to specify for all running virtual machines is calculated on the basis of the host computer's physical memory and is displayed in the memory settings slider control — **Host > Settings > Memory**. If you want VMware Server to use more or less physical memory, use this slider to change the amount.

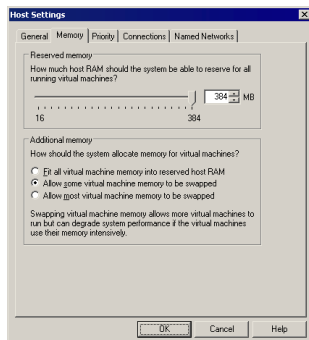
If you set this value too high, the host may thrash when other applications are run on the host. If you set this value too low, virtual machines may perform poorly and you cannot run as many virtual machines at once.

Using Additional Memory

By default, VMware Server limits the number of virtual machines that can run at once based on the amount of memory specified in the Host Settings dialog box. This limit prevents virtual machines from causing each other to perform poorly. If you try to power on a virtual machine and there is not enough memory available, a warning appears and the virtual machine fails to power on.

To increase the number or memory size of virtual machines that can run, adjust the amount of virtual machine memory that the host operating system may swap to disk.

To change this setting, choose **Host > Settings > Memory** and choose an option under **Additional memory**.



Select one of the following options:

- **Fit all virtual machine memory into reserved host RAM** — Strictly apply the reserved memory limit set in the top of the dialog box. This setting imposes the tightest restrictions on the number and memory size of virtual machines that may run at a given time. Because the virtual machines are running entirely in RAM, they have the best possible performance.
- **Allow some virtual machine memory to be swapped** — Allow the host operating system to swap a moderate amount of virtual machine memory to disk if necessary. This setting allows you to increase the number or memory size of virtual machines that can run on the host computer at a given time. It may also result in reduced performance if virtual machine memory must be shifted between RAM and disk.
- **Allow most virtual machine memory to be swapped** — Allow the host operating system to swap as much virtual machine memory to disk as it wants. This setting allows you to run even more virtual machines with even more memory than the intermediate setting does. In this case, too, performance may be lower if virtual machine memory must be shifted between RAM and disk.

If you try to power on a virtual machine and there is not enough memory available, VMware Server displays a warning message. The message shows how much memory the virtual machine is configured to use and how much memory is available. You can try to power on the virtual machine using the available memory by clicking **OK**. If you do not want to power on the virtual machine, click **Cancel**.

Memory Usage on Older Linux Hosts

By default, Linux kernels in the 2.2.x series support 1GB of physical memory. If you want to use more memory in Linux, you can take one of several approaches.

- Upgrade to a 2.4.x series kernel that allows for more physical memory.
- Recompile your kernel as a 2GB kernel using the CONFIG_2GB option.
- Enable the CONFIG_BIGMEM option to map more physical memory. (This approach requires special steps, described in detail in the Workarounds section below, to work with VMware products.)

Recompiling your kernel with CONFIG_2GB enabled allows Linux to support nearly 2GB of physical memory by dividing the address space into a 2GB user section and 2GB kernel section (as opposed to the normal division of 3GB for user and 1GB for kernel).

The third approach uses the CONFIG_BIGMEM option in Linux. With the CONFIG_BIGMEM option enabled, the kernel does not directly address all of physical memory and it can then map 1GB (or 2GB) of physical memory into the address space at a time. This allows the use of all of physical memory at the cost of changing the semantics the kernel uses to map virtual to physical addresses. However, VMware products expect physical memory to be mapped directly in the kernel's address space and thus do not work properly with the CONFIG_BIGMEM option enabled.

Workarounds

If you are using a 1GB kernel with CONFIG_BIGMEM enabled and have 960MB to 1983MB of memory, VMware Server does not run. To work around this issue, you can:

- Recompile the kernel as a 2GB kernel by enabling the CONFIG_2GB option. This allows for 100 percent use of physical memory.
- Pass the boot-time switch `mem=959M` at the LILO prompt, or add it to `lilo.conf`, to disable CONFIG_BIGMEM and thus allow you to run VMware Server. To do this:

To pass the switch at the LILO prompt, type
`linux-2.2.16xxx mem=959M`

To edit `lilo.conf`, open the file in a text editor. In the kernel section, add this line:
`append mem="959M"`

If you have a 1GB kernel with CONFIG_BIGMEM enabled and have more than 1983MB of memory, you can do one of the following:

- Recompile the kernel as a 2GB kernel by enabling the CONFIG_2GB option and either pass the boot-time switch `mem=1983M` at the LILO prompt or add it to `lilo.conf`. To use the switch:

To pass the switch at the LILO prompt, type
`linux-2.2.16xxx mem=1983M`

To edit `lilo.conf`, open the file in a text editor. In the kernel section, add this line:
`append mem="1983M"`

- Pass the boot-time switch `mem=959M` at the LILO prompt or add it to `lilo.conf` to disable `CONFIG_BIGMEM`. To use the switch:

To pass the switch at the LILO prompt, type
`linux-2.2.16xxx mem=959M`

To edit `lilo.conf`, open the file in a text editor. In the kernel section, add this line:
`append mem="959M"`

If you are using a 2GB kernel with `CONFIG_BIGMEM` enabled and have 1984MB or more memory, VMware Server does not run. You can either pass the boot-time switch `mem=1983M` at the LILO prompt, or add it to `lilo.conf` to disable `CONFIG_BIGMEM` and thus allow you to run VMware Server. To use the switch:

To pass the switch at the LILO prompt, type
`linux-2.2.16xxx mem=1983M`

To edit `lilo.conf`, open it in a text editor. In the kernel section, add this line:
`append mem="1983M"`

CHAPTER 7 **Using High-Availability Configurations**

This chapter describes using high-availability configurations with VMware Server and covers the following topics:

- [“Using SCSI Reservation to Share SCSI Disks with Virtual Machines”](#) on page 161
- [“Overview of Clustering with VMware Server”](#) on page 165
- [“Creating a Cluster in a Box”](#) on page 167
- [“Using Network Load Balancing with VMware Server”](#) on page 175
- [“Creating Two-Node Clusters Using Novell Clustering Services”](#) on page 179
- [“Clustering Using the iSCSI Protocol”](#) on page 183

Using SCSI Reservation to Share SCSI Disks with Virtual Machines

VMware Server permits the sharing of a preallocated virtual SCSI disk with multiple virtual machines running on the same host. When the disk is shared, all virtual machines connected to the disk use the SCSI reservation protocol to write to the disk concurrently.

You must install clustering software on each virtual machine that you plan to share a SCSI disk. Enabling SCSI reservation in and of itself does not automatically mean that a running virtual machine is a participant in the SCSI reservation protocol.

NOTE Although growable virtual disks and physical disks can be used with SCSI reservation, such use is considered experimental and should not be attempted in a production environment. Only the use of preallocated virtual disks is fully supported with SCSI reservation. When you create a new virtual machine, or add a new virtual disk to an existing virtual machine, VMware Server creates a preallocated virtual disk by default.

NOTE This feature is advanced. Use it only if you are familiar with SCSI in general and the SCSI reservation protocol in particular.

The following sections describe how to use SCSI reservation to share disks among multiple virtual machines.

- [“SCSI Reservation Support”](#) on page 162
- [“Enabling SCSI Reservation”](#) on page 162
- [“Issues to Consider When Sharing Disks”](#) on page 164

SCSI Reservation Support

SCSI reservation support is limited by the following:

- You can enable SCSI reservation for SCSI virtual and physical disks. No other type of SCSI devices can use SCSI reservation in a virtual machine. Specifically, you cannot enable SCSI reservation for a SCSI disk that is configured as a generic SCSI device. For more information about generic SCSI, see [“Connecting to a Generic SCSI Device”](#).

NOTE VMware Server supports SCSI reservation when used with preallocated virtual disks. Support for SCSI reservation with growable virtual disks and physical disks is considered experimental. For high-availability configurations, use SCSI reservation with preallocated virtual disks.

- SCSI disks can be shared using SCSI reservation among virtual machines running on the same host. This means that the configuration files for the virtual machines must all be located on the same VMware Server host. However, the disk or disks the virtual machines are sharing can be located remotely on a different host.
- A SCSI virtual disk can be located on a host with any type of hard disk (for example, IDE, SCSI or SATA). A shared physical disk must always be a SCSI disk.
- VMware Server virtual machines currently support only the SCSI-2 disk protocol, and not applications using SCSI-3 disk reservations. All popular clustering software (including MSCS and VCS) currently use SCSI-2 reservations.

Enabling SCSI Reservation

SCSI reservation must be enabled in a virtual machine before you can share its disks. VMware recommends you set up any shared disks on the same SCSI bus, which is a different bus from the one the guest operating system uses. For example, if your guest

operating system is on the `scsi0` bus, you should set up disks to share on the next available bus, typically the `scsi1` bus.

Sharing resources using two separate buses (for example, data on SCSI1:0 and quorum on SCSI2:0) causes the configuration file to become invalid, and you cannot boot the virtual machine.

To enable SCSI reservation, make sure the virtual machine is powered off. Open the configuration file (`.vmx`) in a text editor and add the line:

```
scsi<x>.sharedBus = "virtual"
```

anywhere in the file, where `<x>` is the SCSI bus being shared.

For example, to enable SCSI reservation for devices on the `scsi1` bus, add the following line to the virtual machine's configuration file:

```
scsi1.sharedBus = "virtual"
```

This allows the whole bus to be shared and is quicker than specifying each disk separately. However, if you do not want to share the whole bus, you can selectively enable SCSI reservation for a specific SCSI disk on the shared bus. For example, if you want to share a SCSI disk located at `scsi1:1`, add the following line to the configuration file:

```
scsi1:1.shared = "true"
```

You must specify the same SCSI target (that is, `scsi<x>:1`) in the configuration file for each virtual machine that is going to share the disk.

If SCSI reservation is enabled for the whole bus (that is, `scsi1.sharedBus` is set to "virtual"), this setting is ignored.

In addition to enabling SCSI reservation on the bus, you need to allow virtual machines to access the shared disk concurrently. Add the following line to the virtual machine's configuration file:

```
disk.locking = "false"
```

This prevents the locking of that disk, which permits multiple virtual machines to access a disk concurrently. Be careful though: if any virtual machine not configured for SCSI reservation tries to access this disk concurrently, the shared disk is vulnerable to corruption or data loss.

CAUTION This setting applies to all disks in the virtual machine.

When SCSI reservation is enabled, the system creates a reservation lock file that contains the shared state of the reservation for the given disk. The name of this file consists of the filename of the SCSI disk appended with `.RESLCK`.

For example, if the disk `scsi1:0.filename` is defined in the configuration file as

```
scsi1:0.fileName = "<path_to_config>/vmSCSI.vmdk"
```

the reservation lock file for this disk has the default name

```
<path_to_config>/vmSCSI.vmdk.RESLCK
```

You can provide your own lock filename. Add a definition for `scsi1:0.reslckname` to the configuration file. For example, if you add

```
scsi1:0.reslckname = "/tmp/scsi1-0.reslock"
```

to the configuration file, this name overrides the default lock filename.

CAUTION Use the same lock filename (for example, `/tmp/scsi1-0.reslock`) for each virtual machine in the cluster. You must also use the same SCSI target for each virtual machine when you define `scsi1:0.reslckname`. However, the SCSI bus (`scsi1` in this case) does not need to be the same.

After SCSI reservation is enabled for a disk — that is, the `scsi<x>.sharedBus = "virtual"` and `disk.locking = "false"` settings are added to the configuration file for each virtual machine wanting to share this disk — you need to point each virtual machine to this disk.

To add a virtual disk to a virtual machine, see [“Adding Virtual Disks to a Virtual Machine”](#).

Issues to Consider When Sharing Disks

- Do not try to share a disk among multiple running virtual machines that are not collocated on the same host. The disk file itself can be located remotely, but the virtual machines must be running together on the same VMware Server host. If you try to share a disk among virtual machines located on different hosts, data could be corrupted or lost.
- Do not share a disk on SCSI bus 0. This bus is usually used for the boot disk. If you share the boot disk, you run the risk of corrupting it, as the boot program is not aware that the disk is being shared and can write to the disk regardless of whether or not it is being shared. It is far more secure to use SCSI reservation on a data disk located on a different bus.
- If only one running virtual machine is using a given disk, and it is running applications that do not use SCSI reservation, the disk’s performance might be degraded slightly.

- At this time, if one virtual machine does not have SCSI reservation enabled for its virtual disk, but another virtual machine does have SCSI reservation enabled for the same virtual disk, VMware Server does allow the disk to be shared. However, any virtual machine not configured for SCSI reservation that tries to access this disk concurrently can cause corruption or data loss on the shared disk. VMware recommends you take care when sharing disks.
- If you need to shrink or defragment the virtual disk (which can be done only with a growable virtual disk), first disable SCSI reservation and make sure the virtual disk is not being used by any other virtual machine.

To disable SCSI reservation for all SCSI disks in a virtual machine, open the configuration file and comment out or remove the `scsi<x>.sharedBus = "virtual"` line and make sure the `disk.locking` line is set to `"true"`.

To disable SCSI reservation for only a specific SCSI disk on a shared bus, change the `scsi<x>:<y>.shared = "true"` line in the configuration file to `scsi<x>:<y>.shared = "false"`. You can also comment out the line.

- In a Windows virtual machine, some disk errors are recorded in the Windows event log in normal operation. These error messages have a format similar to "The driver detected a controller error on \Device\Scsi\BusLogic3"

The errors should appear in the log periodically only on the passive node of the cluster and should also appear when the passive node is taking over during a failover. The errors are logged because the active node of the cluster has reserved the shared virtual disk. The passive node periodically probes the shared disk and receives a SCSI reservation conflict error.

Overview of Clustering with VMware Server

VMware Server clustering capabilities are ideally suited for development, testing, and training applications.

NOTE Always rigorously test and review your cluster before deploying it in a production environment.

This section includes:

- [“Applications That Can Use Clustering”](#) on page 166
- [“Clustering Software”](#) on page 166

Clustering provides a service through a group of servers to get high availability, scalability, or both.

For example:

- In a Web server cluster where the Web site serves static content, a gateway distributes requests to all nodes according to load. The gateway also redirects requests to remaining nodes if one crashes.

This configuration increases availability and performance over a single-machine approach. Network Load Balancing in Windows 2000 and Windows Server 2003 provides such a service.

- In a more complex cluster, a single node might serve a database. If that node crashes, it must restart the database on another node. The database application knows how to recover from a crash. In normal operation, other nodes run other applications.

Microsoft Cluster Service and Veritas Cluster Service provide such a service.

In a typical virtual machine cluster:

- Each virtual machine is one node in the cluster.
- Disks are shared between nodes.

Shared disks are needed if the application uses dynamic data as mail servers or database servers do.

When using virtual disks, you must preallocate the disk space at the time you create the virtual disk.

- Extra network connections between nodes for monitoring heartbeat status are available.
- A method for redirecting incoming requests is available.

Applications That Can Use Clustering

To take advantage of clustering services, applications need to be clustering-aware. Such applications can be stateless, such as Web servers and VPN servers. Clustering-aware applications often include built-in recovery features, like those in database servers, mail servers, file servers, or print servers.

Clustering Software

Available clustering software includes:

- Microsoft Clustering Service (MSCS) — under Windows 2000, MSCS provides failover support for two- to four-node clusters for applications such as databases,

file servers, and mail servers. Under Windows Server 2003, MSCS provides failover support for eight-node clusters.

- Microsoft Network Load Balancing (NLB) — balances the load of incoming IP traffic across a cluster of up to 32 nodes for applications such as Web servers and terminal services.
- Veritas Clustering Service (VCS).
- Novell Clustering Services.

NOTE These clustering services are tested and supported by VMware only with Windows host operating systems.

Creating a Cluster in a Box

With VMware Server, you can create a simple cluster in a box to help mitigate the effects of software crashes or administrative problems.

CAUTION When you use VMware Server virtual machines in a cluster, you must turn off disk caching for each virtual machine that is a member of the cluster. If you do not turn off data on the shared drive might become corrupted. To turn off disk caching open the configuration .vmx file of each virtual machine in a text editor and add the following line:

```
diskLib.dataCacheMaxSize = "0"
```

NOTE When you configure a cluster, the ability to take snapshots is disabled in virtual machines in the cluster.

This type of cluster:

- Consists of multiple virtual machines (nodes) on a single physical machine.
- Supports shared disks without any shared SCSI hardware.
- Supports a heartbeat network without an extra physical network adapter.

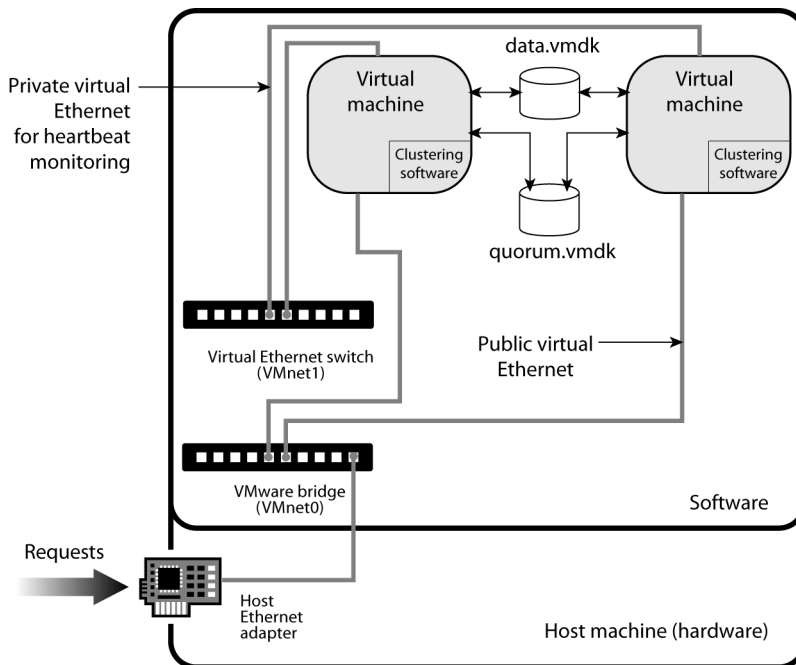


Figure 7-1. A two-node cluster on a single physical machine.

The following sections describe how to set up a cluster in a box:

- [“Configuring Virtual Machines for Cluster in a Box”](#) on page 168
- [“Creating a Two-Node Cluster with Microsoft Clustering Services”](#) on page 169

Configuring Virtual Machines for Cluster in a Box

To create a set of clustered virtual machines (a cluster in a box), configure each of them with the following:

- A primary virtual SCSI host adapter with one SCSI virtual disk.
- Two virtual network adapters:
 - A public network adapter bridged to a physical adapter either using VMnet0, or VMnet2-8 as configured in the virtual machine settings editor of the VMware Server machine.
 - A private network adapter connected to VMnet1 (host-only), or another physical adapter (VMnet2 through VMnet8). This is the network adapter that the clustering service uses to monitor the heartbeat between nodes. This device selection must match in all virtual machines in a cluster set.

- The remaining default virtual machine devices (such as the CD-ROM drive and the floppy disk drive).

In addition to the above devices, the following are required for shared storage:

- A secondary virtual SCSI host adapter.
- One or more preallocated virtual disks that are shared, attached to the secondary SCSI host adapter.

Note the following about virtual PCI slots in the virtual machines:

- Each virtual machine by default has six PCI slots available.
- This configuration (two network adapters and two SCSI host bus adapters) uses four of these slots.
- One more PCI slot is available for a third network adapter if needed. (The sixth slot is used by the virtual display adapter.)
- If the virtual machine's boot partition is on an IDE virtual disk, the partition occupies one of the PCI slots.

Creating a Two-Node Cluster with Microsoft Clustering Services

This procedure creates a two-node cluster using Microsoft Clustering Services on a single VMware Server computer using the following:

- SQL1 = host name of node 1 of the cluster
- SQL2 = host name of node 2 of the cluster
- SQLCLUSTER = public host name of the cluster

Creating the First Node's Base Virtual Machine

The following steps describe how to create the base virtual machine that serves as the first node in the cluster (and as a template for the additional node), and how to create the two preallocated virtual disks that are shared among the virtual machines in the cluster.

NOTE The virtual disks used to store the operating system and clustering software for each virtual machine (node) in the cluster do not have to be preallocated virtual disks.

- 1 Log on to your VMware Server host as the user who will own the virtual machine.
- 2 Launch a VMware Server Console and create a new virtual machine (for information on creating a new virtual machine, see [“Creating a New Virtual](#)

[Machine](#)”). Follow the Custom path. Choose the settings you want (for example, the size of the virtual disk or the amount of memory), but make sure you specify

- Windows 2000 Advanced Server or Windows Server 2003 Enterprise Edition as the guest operating system.
 - SQL1 as the virtual machine name.
 - The virtual machine directory as `d:\cluster\SQL1` (on a Windows host) or `/home/cluster/SQL1` (on a Linux host).
 - Bridged networking for the virtual machine.
 - SQL1 as the disk filename.
- 3 Open the virtual machine settings editor. Choose **VM > Settings**.
 - 4 Add a new network adapter that uses either another external adapter or the VMnet1 host-only adapter. (For complete isolation from the host, you can also use any unused virtual Ethernet switch, typically VMnet2 through VMnet7.) For information, see [“Adding and Modifying Virtual Network Adapters”](#).

This adapter is used as the virtual private Ethernet connection for heartbeat monitoring.

- 5 Add the two virtual disks that are to be shared:
 - A shared data disk (call it `data.vmdk`, for example)
 - A shared quorum disk (call it `quorum.vmdk`, for example) to store transactions before they are committed to the data disk

For information, see [“Adding Virtual Disks to a Virtual Machine”](#).

- 6 Click **OK** to save your changes and close the virtual machine settings editor.
- 7 Using a text editor, manually edit the configuration file `d:\cluster\SQL1\SQL1.vmx` (on a Windows host) or `/home/cluster/SQL1/SQL1.vmx` (on a Linux host).
- 8 Add the following lines to the configuration file:


```
scsi1.sharedBus = virtual
disk.locking = "false"
```

This enables SCSI reservation, which is described in more detail in the section [“Using SCSI Reservation to Share SCSI Disks with Virtual Machines”](#) on page 161.

You are finished creating the virtual machine for the first node in your cluster. The next step is to install a guest operating system in the virtual machine.

Installing the Guest Operating System in the First Virtual Machine (Node)

For information on installing Windows 2000 Advanced Server or Windows Server 2003 Enterprise Edition in the virtual machine, see the *VMware Guest Operating System Installation Guide*. It is available from the VMware Web site at <http://www.vmware.com/support/guestnotes/doc/index.html>.

NOTE During the installation of the guest operating system, do not install the clustering services.

When the installation is complete, install VMware Tools in the guest operating system. See “[Installing VMware Tools](#)”.

After you finish installing the guest operating system and VMware Tools, clone the virtual machine. (Later, you create the second cluster node using the clone.)

To clone the first virtual machine node

- 1 Run `sysprep.exe`, which is available on the Windows CD in the file `\support\tools\deploy.cab` (or from the Microsoft Web site).

The `sysprep.exe` utility removes the security ID assigned to the guest operating system, resets the machine information and resets the TCP/IP network configuration.

- 2 Shut down the guest operating system and power off the virtual machine.
- 3 Create a directory named `SQL2` under the `cluster` directory.
- 4 Copy the `SQL1*.vmdk` files into this directory.
- 5 Use the VMware Virtual Disk Manager to change the name of the virtual disk to `SQL2*.vmdk`. At a command prompt, type:

```
vmware-vdiskmanager -n SQL1.vmdk SQL2.vmdk
```

For more information about the virtual disk manager, see “[Using VMware Virtual Disk Manager](#)”.

You are finished cloning the first node. You are now ready to create the second node in the cluster using the clone.

To create the second node in the cluster from the clone of the first node

- 1 Log on to your VMware Server host as the user who will own the virtual machine.
- 2 Launch a VMware Server Console and create a new virtual machine (for information on creating a new virtual machine, see “[Creating a New Virtual Machine with the Virtual Machine Wizard](#)”). Choose the settings you want (for

example, the size of the virtual disk or the amount of memory), but make sure you specify:

- Windows 2000 Advanced Server or Windows Server 2003 Enterprise Edition as the guest operating system.
 - SQL2 as the virtual machine name.
 - The virtual machine directory as `d:\cluster\SQL2` (on a Windows host) or `/home/cluster/SQL2` (on a Linux host).
 - Bridged networking for the virtual machine.
 - To use an existing virtual disk, click **Browse** and select `SQL2.vmdk`.
- 3 Open the virtual machine settings editor. Choose **VM > Settings**.
 - 4 Add a new network adapter that uses either another external adapter or the VMnet1 host-only adapter. For information, see [“Adding and Modifying Virtual Network Adapters”](#).
 - 5 Add the two virtual disks (`quorum.vmdk` and `data.vmdk`) you previously created. For information, see [“Adding Virtual Disks to a Virtual Machine”](#). Make sure you select **Use an existing virtual disk** and browse to `quorum.vmdk` and `data.vmdk`.
 - 6 Click **OK** to save your settings and close the virtual machine settings editor.
 - 7 Using a text editor, manually edit the configuration file `d:\cluster\SQL2\SQL2.vmx` (on a Windows host) or `/home/cluster/SQL2/SQL2.vmx` (on a Linux host).
 - 8 Add the following lines to the bottom of the configuration file:


```
scsi1.sharedBus = virtual
disk.locking = "false"
```

This enables SCSI reservation, which is described in more detail in [“Using SCSI Reservation to Share SCSI Disks with Virtual Machines”](#) on page 161.
 - 9 In the console, verify that both virtual machines are powered off.

You are finished creating the second node.

Now that you have virtual machines for both nodes in your two-node cluster, you are ready to install the clustering services software.

To install Microsoft Clustering Services on the Cluster Nodes

- 1 Start the node 1 virtual machine.
- 2 Follow the Windows setup prompts to enter

- The Windows serial number.
- The host name (SQL1).
- The IP addresses of the public and private network adapters.

NOTE For the public network adapter, enter an IP address that belongs to the physical network. For the private IP address, you can use an address like 192.168.x.x with a class C subnet mask (255.255.255.0).

- 3 At the end of the process, Windows reboots.
- 4 Start the Disk Management tool and change both shared disks to **Basic** disks.
- 5 Format both shared virtual disks with NTFS if they are not already formatted.
- 6 Assign the first shared disk to Q: (quorum) and the second disk to R: (data).
If you have joined this virtual machine to an existing Active Directory domain, skip to [step 11](#).
- 7 Run `dcpromo.exe` from the command prompt. This starts the Active Directory Wizard.
- 8 Set up the current machine as a domain controller. For the domain name, use something similar to `<vmcluster>.<domain.com>` where `<domain.com>` is your DNS domain and `<vmcluster>` is your Active Directory domain.

You can set up this node as a new domain tree or a new domain forest, or join it to an existing domain tree or forest.
- 9 Make sure the DNS server is installed.
- 10 Set the domain permissions as mixed mode unless you plan otherwise.
- 11 To add a cluster services account in the domain, go to **Programs > Administrative Tools > Active Directory Users and Computers**.
- 12 Add a cluster service account named `cluster`:
 - Enter the user's password.
 - Check the **User cannot change password** check box.
 - Check the **Password never expires** check box.
- 13 Insert the Windows CD in the CD-ROM drive.
- 14 Choose **Control Panel > Add/Remove Programs**.
- 15 Select **Add/Remove Windows Components**.

- 16 Check the **Cluster Service** component.
- 17 Click **Next** and follow the prompts to install the service.
- 18 As you configure the cluster service, choose **Form a New Cluster**.
- 19 Specify SQLCLUSTER as the cluster name.
- 20 Specify the cluster service account created in [step 12](#).
- 21 Specify that both shared disks should be managed by the cluster service.
- 22 Indicate the shared disk (Q:) to be the quorum disk.
- 23 Specify which network adapter is public and which is private.
- 24 Specify the cluster IP address. This is the address that represents the cluster. It must be on the same network as the physical Ethernet device.
- 25 Stop the cluster service on the local node (node 1) so that the second virtual machine (node 2) can access the shared disks.

- From Cluster Manager, right-click the node name.
- Select **Stop Cluster Service**.

You are finished installing Microsoft Clustering Services on the first node. The steps to install the software on the second node are similar.

- 1 Start the node 2 virtual machine.
- 2 Repeat [step 2](#) and [step 3](#) in the procedure for the first node.
- 3 Start the Disk Management tool and assign the first shared disk to Q: (quorum) and the second disk to R: (data).
- 4 Start `dcpromo.exe` and add this virtual machine as a domain controller in the same domain created in [step 8](#) for the first node, or add it to an existing domain.

NOTE The setup in node 2 must match the setup in node 1, which you specified in [step 8](#) for node 1.

- 5 In the node 1 virtual machine, start the cluster service.
 - From Cluster Manager, right-click the node name.
 - Select **Start Cluster Service**.
- 6 In the node 2 virtual machine, repeat [step 14](#) through [step 24](#) in “To install Microsoft Clustering Services on the Cluster Nodes” on page 172, with one exception: in [step 18](#), select **Join a Cluster**.

You are now finished configuring the cluster.

Using Network Load Balancing with VMware Server

This section covers procedures for creating a multinode Network Load Balancing cluster using nodes running in virtual machines. These virtual machines can be located on one or more VMware Server computers.

The following sections describe how to create an example Network Load Balancing cluster:

- [“Overview of Network Load Balancing Clusters”](#) on page 175
- [“Creating a Multinode Network Load Balancing Cluster”](#) on page 175

Overview of Network Load Balancing Clusters

Network Load Balancing is a Windows 2000 Advanced Server and Windows Server 2003 feature. Using Network Load Balancing to build a server cluster:

- You can enhance the availability of Internet server programs, such as those used on these types of servers:
 - Web
 - Proxy
 - Domain name service (DNS)
 - FTP
 - Virtual private network (VPN)
 - Streaming media servers
 - Terminal services
- You can scale your server’s performance.
- You can create the cluster with virtual machines on the same physical server or with virtual machines on multiple physical servers (all running VMware Server).
- You can configure up to 32 nodes in the cluster.

Creating a Multinode Network Load Balancing Cluster

The following sections describe how to create a multinode Network Load Balancing cluster.

To create the first node's base virtual machine

- 1 Log on to your VMware Server host as the user who will own the virtual machine.
- 2 Launch a VMware Server Console and create a new virtual machine (for information on creating a new virtual machine, see [“Creating a New Virtual Machine”](#)). Choose the settings you want (for example, the size of the virtual disk or the amount of memory), but make sure you specify
 - Windows 2000 Advanced Server or Windows Server 2003 Enterprise Edition as the guest operating system.
 - NLB1 as the virtual machine name.
 - The virtual machine directory as `d:\cluster\nlb1` (on a Windows host) or `/home/cluster/nlb1` (on a Linux host).
 - Bridged networking for the virtual machine.
 - `nlb1` as the disk filename.
- 3 Connect to this virtual machine with the VMware Server Console and choose **VM > Settings**.
- 4 Add a second networking device, binding it to another physical NIC or to the host-only network.

You are finished creating the first virtual machine (node) in the cluster. The next step is to install a guest operating system in the virtual machine.

Installing the Guest Operating System in the First Virtual Machine (Node)

For information on installing Windows 2000 Advanced Server or Windows Server 2003 Enterprise Edition in the virtual machine, see the *VMware Guest Operating System Installation Guide*. It is available from the VMware Web site at <http://www.vmware.com/support/guestnotes/doc/index.html>.

NOTE During the installation of the guest operating system, do not install the clustering services.

When the installation is complete, install VMware Tools in the guest operating system. See [“Installing VMware Tools”](#).

After you finish installing the guest operating system and VMware Tools, clone the virtual machine. (Later, you create the second cluster node using the clone.)

You are finished creating the first cluster node. You can now clone that node for use in creating other nodes.

Cloning the First Cluster Node

Follow these steps to clone the first cluster node for use in creating the other nodes in the cluster, either on the same physical server or on other machines running VMware Server:

- 1 Run `sysprep.exe`, which is available on the Windows CD in the file `\support\tools\deploy.cab` or from the Microsoft Web site.

The `sysprep.exe` utility removes the security ID assigned to the guest operating system, resets the machine information, and resets the TCP/IP network configuration.
- 2 Shut down the guest operating system and power off the virtual machine.
- 3 Create a directory `n1b2` under the cluster directory, either on the local server or on different machines running VMware Server.
- 4 Copy the `n1b1*.vmdk` files into this directory.
- 5 Use the VMware Virtual Disk Manager to change the name of the virtual disk to `n1b<n>.vmdk` (where `<n>` is the Network Load Balancing node number). At a command prompt, type:

```
vmware-vdiskmanager -n n1b1.vmdk n1b<n>.vmdk
```

For more information about the virtual disk manager, see [“Using VMware Virtual Disk Manager”](#).

Repeat [step 3](#) through [step 5](#) for each additional node you want to create, either on the same physical server, or on additional machines running VMware Server. You can configure up to 32 nodes with Network Load Balancing.

When you are finished making clones of the first node, you are ready to create additional nodes from the clones.

Creating Additional Nodes in the Network Load Balancing Cluster

Follow these steps for each of the additional nodes you want to create (up to 32 nodes) in the Network Load Balancing cluster:

- 1 Log on to your VMware Server host as the user who will own the virtual machine.
- 2 Launch a VMware Server Console and create a new virtual machine (for information on creating a new virtual machine, see [“Creating a New Virtual Machine”](#)). Choose the settings you want (for example, the size of the virtual disk or the amount of memory), except you should specify
 - Windows 2000 Advanced Server or Windows Server 2003 Enterprise Edition as the guest operating system.

- nlb2 as the virtual machine name.

NOTE For each additional node, use the name of that node instead of nlb2.

- The virtual machine directory as d:\VMware\cluster\nlb2 (on a Windows host) or /home/cluster/nlb2 (on a Linux host).
 - To use an existing virtual disk. Click **Browse** and select nlb2.vmdk.
 - Bridged networking for the virtual machine.
- 3 Connect to this virtual machine with the VMware Server Console and choose **VM > Settings**.
 - 4 Add a second networking device, binding it to another physical NIC or to the host-only network. For information, see [“Adding and Modifying Virtual Network Adapters”](#).
 - 5 In the console, verify that both virtual machines are powered off.

After you have finished creating the additional nodes, you are ready to configure the cluster.

Configuring the Network Load Balancing Cluster

You can cluster up to 32 nodes using Network Load Balancing.

To configure the cluster for each node that joins the cluster

- 1 Connect to the first node virtual machine with the VMware Server Console.
- 2 Power on the virtual machine.
- 3 Follow the Windows mini-setup prompts to enter the following:
 - The Windows serial number
 - The host name
 - IP addresses for that host
- 4 At the end of the process, Windows reboots.
- 5 Log on to the virtual machine as the Administrator user.
- 6 Open **Network and Dial-up Connections**.
- 7 Right-click the local area connection on which you want to install Network Load Balancing and choose **Properties**.

The Local Area Connection Properties dialog box appears.

- 8 Under **Components checked are used by this connection**, select the **Network Load Balancing** check box.
- 9 Click **Properties**.
- 10 On the **Cluster Parameters** tab, configure cluster operations using these parameters:
 - **Primary IP Address:** This is the address for the cluster as a whole. Clients use this address to access the cluster.
 - **Subnet Mask:** This is the subnet mask of the network to which the above address belongs.
 - **Multicast:** Select this option, even if your virtual machine was configured with a single network adapter.

NOTE All members of the cluster must be configured for multicasting.

Refer to Network Load Balancing online Help for the remaining options.

- 11 When you finish with the cluster parameters, click **OK** to return to the Local Area Connection Properties dialog box.
- 12 Click **OK** to return to the Local Area Connection Status dialog box.
- 13 Right-click the local area connection on which Network Load Balancing is to be installed, and select **Properties**.
- 14 Click **Internet Protocol (TCP/IP)**, and click **Properties**.
- 15 Set up TCP/IP for Network Load Balancing.

For more information and links to procedures for setting up TCP/IP for Network Load Balancing on single and multiple network adapters, see Related Topics in the Network Load Balancing online Help.

NOTE You must add the cluster's primary IP address to the list of IP addresses bound to the adapter.

Repeat these steps on each host to be used in your Network Load Balancing cluster.

Creating Two-Node Clusters Using Novell Clustering Services

The following sections describe how to create a two-node cluster using Novell Clustering Services on a single VMware Server system:

- [“Creating the First Node's Base Virtual Machine”](#) on page 180
- [“Creating the Second Node in the Cluster”](#) on page 181
- [“Installing the Guest Operating System and VMware Tools”](#) on page 181
- [“Adding the Shared Disks to Both Virtual Machines”](#) on page 181
- [“Installing Novell Clustering Services on the Cluster Nodes”](#) on page 182

Creating the First Node's Base Virtual Machine

The following steps describe how to create the base virtual machine that serves as the first node in the cluster, as well as how to create the two preallocated virtual disks that are shared among the virtual machines in the cluster. You can install Novell NetWare 6.0 or 6.5 in a virtual machine using the standard NetWare 6.0 or 6.5 CD-ROM. VMware recommends you install NetWare 6.0 on a host with at least 384MB of memory; NetWare 6.5 must be installed on a host with at least 512MB of memory.

Creating and Configuring the NetWare Virtual Machine

NOTE The virtual disks used to store the operating system and clustering software for each virtual machine (node) in the cluster do not have to be preallocated virtual disks.

- 1 Log on to your VMware Server host as the user who will own the virtual machine.
- 2 Launch a VMware Server Console and create a new virtual machine (for information on creating a new virtual machine, see [“Creating a New Virtual Machine”](#)). Choose the settings you want (for example, the size of the virtual disk or the amount of memory), but make sure you specify:
 - Netware 6 as the guest operating system.
 - Cluster1 as the virtual machine name.
 - The virtual machine directory as D:\Netware6\Cluster1 (on a Windows host) or /home/Netware/Cluster1 (on a Linux host).
 - Bridged networking for the virtual machine.

You are finished creating the virtual machine for the first node in your cluster. The next step is to create the second node in your cluster. Then, for each node, install the guest operating system and VMware Tools.

Creating the Second Node in the Cluster

Next, create the second node of the cluster by following the same procedure for creating the first node listed above with the following changes:

- Use Cluster2 as the virtual machine name.
- Use D:\Netware6\Cluster2 as the virtual machine directory (on a Windows host) or /home/Netware/Cluster2 (on a Linux host).

Installing the Guest Operating System and VMware Tools

For information on installing NetWare 6.0 or 6.5 in a virtual machine, see the *VMware Guest Operating System Installation Guide*. It is available from the VMware Web site at <http://www.vmware.com/support/guestnotes/doc/index.html>. Make sure you follow the instructions for bridged networking.

When the installation is complete, install VMware Tools in the guest operating system. See “Installing VMware Tools”.

After you finish installing the guest operating system and VMware Tools, clone the virtual machine. (Later, you create the second cluster node using the clone.)

You are finished creating the first cluster node. You can now clone that node for use in creating other nodes.

Be sure to read the known issues for NetWare 6.0 or 6.5 in the installation guidelines.

Adding the Shared Disks to Both Virtual Machines

Follow the procedure outlined in “Adding Virtual Disks to a Virtual Machine” to create and add two shared preallocated virtual disks to the first node (called Cluster1). These disks are shared between both nodes and include:

- A shared data disk (call it data.vmdk, for example).
- A shared quorum disk (call it quorum.vmdk, for example).

NOTE Use the Advanced option when adding the preallocated virtual disks from the virtual machine settings editor to select SCSI virtual device nodes for the disks.

After you finish creating the virtual disks, add them to the second node by completing the following steps.

- 1 Open the virtual machine settings editor for the node 2 virtual machine (called Cluster2). Choose **VM > Settings**.
- 2 Add the two virtual disks that are to be shared. Instead of creating new virtual disks, use the existing virtual disks created for node 1 (called Cluster1).
- 3 Click **OK** to save your changes and close the virtual machine settings editor.
- 4 For the virtual machine named Cluster1, use a text editor to manually edit the configuration file. This file is D:\Netware6\Cluster1\Cluster1.vmx on a Windows host or /home/Netware/Cluster1/Cluster1.vmx on a Linux host.
- 5 For the virtual machine named Cluster2, use a text editor to manually edit the configuration file. This file is D:\Netware6\Cluster2\Cluster2.vmx on a Windows host or /home/Netware/Cluster2/Cluster2.vmx on a Linux host.
- 6 Add the following lines to each configuration file:

```
scsi0.sharedBus = "virtual"
disk.locking = "false"
```

NOTE The default virtual disk type is IDE for the base virtual machine's virtual disk created in ["Creating the First Node's Base Virtual Machine"](#) on page 180. If you are using SCSI virtual disks for the base virtual machine instead, the configuration file options for the shared bus are:

```
scsi1.present = "true" (If this line already exists, do not add it again.)
scsi1.sharedBus = "virtual"
disk.locking = "false"
```

These settings are necessary because your base virtual machine's virtual disk is attached to scsi0 and you **must** have a separate virtual SCSI card for attaching the shared disks. The settings enable SCSI reservation for scsi1, which is described in more detail in ["Using SCSI Reservation to Share SCSI Disks with Virtual Machines"](#) on page 161.

Installing Novell Clustering Services on the Cluster Nodes

Complete the following steps to install Novell Clustering Services in each virtual machine.

- 1 Power on the first node virtual machine (Cluster1).
- 2 Boot into DOS by pressing the F5 key to bypass running the startup files.

- 3 Insert the driver floppy disk in the host's floppy drive.
- 4 Copy the drivers to the c:\nwserver directory.
- 5 Remove the driver floppy disk from the host's floppy drive.
- 6 Reboot the virtual machine.
- 7 The server should be able to recognize the shared disks. You can verify that by running List Devices.

Repeat the above steps for the node 2 virtual machine (Cluster2).

Now you are ready to install the Novell Clustering Services (NCS) as you would normally on two physical machines. Refer to the NetWare 6.0 or 6.5 product documentation for details.

Clustering Using the iSCSI Protocol

You can use the iSCSI protocol with virtual machines and physical machines in a clustered environment to provide highly available network storage and failover.

Clustering with iSCSI is the only way you can use VMware Server to configure clustering across multiple hosts. Using the iSCSI protocol also means that you do not need to manually edit the virtual machine's configuration file as you do with the other clustering configuration methods. However, performance is limited by the slower speed of virtual networking.

Each virtual machine represents a cluster node. You configure each node of the cluster to act as an iSCSI initiator. The initiator communicates with the iSCSI target. The iSCSI target can be:

- A virtual machine on this host or another host.
- The VMware Server host itself or a different host on the network.

The iSCSI initiator must run the Microsoft iSCSI Software Initiator package, available for download from the Microsoft Web site at <http://www.microsoft.com/WindowsServer2003/technologies/storage/iscsi/default.mspx>. This software runs in a virtual machine with a Windows Server 2003, Windows 2000, or Windows XP guest operating system.

The iSCSI target software can run in a virtual machine or on a host with a Windows or Linux operating system. Examples of iSCSI target software include WinTarget (for Windows) and NetApp Filer (for Linux).

NOTE You can use any clustering software in these cluster nodes that is supported by other VMware Server clustering strategies. For more information, see [“Clustering Software”](#) on page 166.

The following sections describe how to set up clustering using the iSCSI protocol.

- [“Clustering Scenarios Using iSCSI”](#) on page 184
- [“Creating and Configuring the iSCSI Initiator Virtual Machine”](#) on page 184
- [“Configuring the iSCSI Target in the Cluster”](#) on page 185

Clustering Scenarios Using iSCSI

You can employ the following scenarios to cluster virtual machines with the iSCSI protocol:

- [“Using a Virtual Machine as the iSCSI Target”](#)
- [“Using a Host as the iSCSI Target”](#)

Using a Virtual Machine as the iSCSI Target

You can use a virtual machine as the iSCSI target. The setup involves at least three virtual machines. Two virtual machines are the cluster nodes that act as iSCSI initiators, so you must install the iSCSI initiator software in these virtual machines. The third virtual machine acts as the iSCSI target. The iSCSI target virtual machine must be running for clustering to work successfully.

Using a Host as the iSCSI Target

You can use a host on your network as the iSCSI target. Each cluster node (virtual machine) acts as an iSCSI initiator, so you must install the iSCSI initiator software in each virtual machine. Then you install the iSCSI target software on the target host.

Creating and Configuring the iSCSI Initiator Virtual Machine

The iSCSI initiator virtual machine is created in the same manner as a regular virtual machine. Unlike other clustering methods, you do not modify the virtual machine’s configuration file (.vmmx) manually in order to enable clustering.

The virtual disk used to store the guest operating system and clustering software for each virtual machine (node) in the cluster does not have to be a preallocated virtual disk or a SCSI virtual disk.

You should configure the virtual machine with at least two virtual network adapters — one to communicate with other iSCSI initiator nodes and the other to connect to the

iSCSI target and to the Internet. You could optionally configure the virtual machine with three virtual network adapters — the first to communicate with other iSCSI initiator nodes, the second to connect to the iSCSI target, and the third to the Internet.

For the virtual network adapter that communicates with the other cluster nodes, you should configure it to use bridged networking if the cluster nodes are located on different VMware Server hosts. If the nodes are on the same host, you can also use host-only networking.

To create an iSCSI initiator virtual machine

- 1 Log on to your VMware Server host as the user who will own the virtual machine.
- 2 Launch a VMware Server Console and create a new virtual machine (for information on creating a new virtual machine, see [“Creating a New Virtual Machine”](#)). Choose the settings you want (for example, the size of the virtual disk or the amount of memory), but make sure you specify bridged networking for the virtual machine.
- 3 Open the virtual machine settings editor. Choose **VM > Settings**.
- 4 Add a second virtual network adapter. For more information, see [“Adding and Modifying Virtual Network Adapters”](#). Again, make sure you specify bridged networking for the adapter.

If you choose, you can add a third virtual network adapter to the virtual machine.

- 5 Select the virtual network adapter you intend to use to communicate with the iSCSI target. Under **Adapter type**, select **vmxnet**.
- 6 Click **OK** to save your settings and close the virtual machine settings editor.
- 7 Power on the virtual machine and install the guest operating system and VMware Tools. See [“Installing VMware Tools”](#).
- 8 Install the iSCSI initiator software.

You are finished creating the iSCSI initiator virtual machine. Repeat these steps for each iSCSI initiator, or else use `sysprep.exe` to clone the first node. Then create the iSCSI target virtual machine.

Configuring the iSCSI Target in the Cluster

The configuration of the iSCSI target node of the cluster depends on whether you are using a virtual machine or a host for the target.

If you are using a host, you need to install the iSCSI target software on the host. After the iSCSI initiator virtual machines are configured and the iSCSI initiator software installed, the virtual machines can access the target.

If you are using a virtual machine as the iSCSI target, configure the virtual machine the same way you did for the initiator, except for the following:

- Make sure the virtual machine is configured with at least one SCSI virtual disk.
- You can configure the virtual machine with one virtual network adapter. If the virtual machine is located on the same host as the iSCSI initiators, you should configure it to use host-only networking. If the virtual machine is located on another VMware Server host, you should configure it to use bridged networking.
- You must install iSCSI target software instead of iSCSI initiator software on a SCSI virtual disk.

Appendix: Mounting Virtual Disks

VMware Server DiskMount Utility lets you mount an unused virtual disk in a Microsoft Windows host file system as a separate drive without needing to connect to the virtual disk from within a virtual machine. You can mount specific volumes of a virtual disk if the virtual disk is partitioned.

DiskMount Utility is a command line program called `vmware-mount` that works similarly to how you use the `subst` command on Windows. Once the disk is mounted, you can read from and write to the disk as if it were a separate file system with its own drive letter on your network. However, you cannot power on any virtual machine that uses this disk until the disk is unmounted.

You can perform activities such as scanning a virtual disk for viruses and transferring files between the host system and a powered off virtual machine.

When you are finished using the mounted virtual disk, delete the mapping so the virtual disk can be used by virtual machines again.

Considerations for Mounting Virtual Disks

- You can use DiskMount with virtual disks created with VMware Server as well VMware ESX Server 2, VMware GSX Server 3 and 2.5.1, VMware ACE, and VMware Workstation 5 and 4.

NOTE Virtual disks created with VMware ACE cannot be encrypted virtual disks. Encrypted virtual disks cannot be mounted with DiskMount.

- You can run DiskMount on any versions of Windows 2000, Windows XP, or Windows Server 2003.
- You must mount virtual disks as drive D: or greater. You cannot specify a letter already in use on the host.
- You can mount volumes formatted with FAT (12/16/32) or NTFS only. If the virtual disk has a mix of partitions (volumes) where, for example, a partition is unformatted or is formatted with a Linux operating system and another partition is formatted with a Windows operating system, you can mount the Windows partition with DiskMount.

- You can mount a virtual disk that has a snapshot. Any changes you make to the virtual disk while it is mounted are discarded when you revert to the snapshot.
- You cannot mount a virtual disk if any of its .vmdk files are compressed or have read-only permissions. Change these attributes before mounting the virtual disk.
- You cannot mount a virtual disk that is currently being used by a running or suspended virtual machine. Only disks that are in a powered off virtual machine can be mounted.

Statement of Support

The VMware DiskMount Utility is provided without support services from VMware under the terms in the VMware Server license agreement.

Installing the VMware DiskMount

The VMware Server installer includes the VMware DiskMount utility. After the utility is installed, run it on a Windows host machine. A VMware virtualization product such as VMware Server does not need to be installed on the host.

Running the VMware DiskMount Utility

To run the VMware DiskMount Utility, open a command prompt on a Windows 2000, Windows XP or Windows Server 2003 host, then change to the directory where you installed the software.

The command syntax is:

```
vmware-mount [options] [drive letter:] [\\path\to\virtual disk]
```

The options you can use include:

Table A-1.

Option	Definition
/v:N	Mounts volume N of a virtual disk. N defaults to 1.
/p	Displays the partitions (volumes) on the virtual disk.
/d	Deletes the mapping to a virtual disk drive volume.
/f	Forcibly deletes the mapping to a virtual disk drive volume. Use this option when a technical error or a correctable condition such as open file handles prevents VMware Server from unmounting the drive.
/?	Displays vmware-mount usage information.

Examples Using the VMware DiskMount Utility

Following are some examples that illustrate how to use the VMware DiskMount Utility.

Mounting a Virtual Disk

Use this command to mount a virtual disk:

```
vmware-mount h: "C:\My Virtual Machines\w2003std.vmdk"
```

List Virtual Disk Volumes Currently Mounted

Use this command to review which virtual disks are mounted under DiskMount.

```
vmware-mount  
Currently mounted volumes:  
f:\ => "C:\My Virtual Machines\w2003std\w2003std.vmdk"  
g:\ => "C:\My Virtual Machines\NT\NT.vmdk (volume 1)"
```

Mounting a Specific Volume in a Virtual Disk

Use this command to mount a specific volume in a virtual disk:

```
vmware-mount /v:2 h: "C:\My Virtual Machines\w2003std.vmdk"
```

Unmounting a Virtual Disk

Use this command to unmount a virtual disk so virtual machines can access it again:

```
vmware-mount h: /d
```


Glossary

Add Hardware Wizard

A point-and-click interface for adding virtual hardware to a virtual machine. To launch the Wizard, power off the virtual machine, open the virtual machine settings editor, then click **Add**. It prompts you for information for configuring the hardware, suggesting default values in most cases.
See also Virtual machine settings editor.

Bridged networking

A type of network connection between a virtual machine and the rest of the world. Under bridged networking, a virtual machine appears as an additional computer on the same physical Ethernet network as the host.
See also Host-only networking.

Configuration

See Virtual machine configuration file.

Console

See VMware Server Console.

Current virtual machine

A virtual machine created under the current VMware Server version and Workstation Server 5.x.
See also Legacy virtual machine.

Custom networking

Any type of network connection between virtual machines and the host that does not use the default bridged, host-only or network address translation (NAT) networking configurations. For instance, different virtual machines can be connected to the host by separate networks or connected to each other and not to the host. Any network topology is possible.

EULA

The end user license agreement.

Existing partition

A partition on a physical disk in the host machine.

See also Physical disk.

Full screen mode

A display mode in which the virtual machine's display fills the entire screen.

See also Quick switch mode.

Growable disk

A type of virtual disk where the disk space is not preallocated to its full size. Its files start out small in size and grow as data is written to it.

Guest operating system

An operating system that runs inside a virtual machine.

See also Host operating system.

Headless

A description for a program or application that runs in the background without any graphical user interface connected to it. A virtual machine running with no consoles connected to it is considered to be running headless.

Host-only networking

A type of network connection between a virtual machine and the host. Under host-only networking, a virtual machine is connected to the host on a private network, which normally is not visible outside the host. Multiple virtual machines configured with host-only networking on the same host are on the same network. See also Bridged networking, Custom networking and Network address translation.

Host computer

The physical computer on which the VMware Server software is installed. It hosts the VMware Server virtual machines.

Host operating system

An operating system that runs on the host machine.
See also Guest operating system.

Independent disk

An independent disk is a type of virtual disk that is not affected by snapshots. Independent disks can be configured in persistent and nonpersistent modes. See also Nonpersistent mode, Persistent mode.

Inventory

A list in the left panel of the console window that shows the names of virtual machines that a user has added to the list. The inventory makes it easy to launch a virtual machine or to connect to the virtual machine's configuration file in order to make changes in the virtual machine settings.

Legacy virtual machine

A virtual machine created under VMware GSX Server or VMware Workstation 3 or 4. See also Current virtual machine.

Network address translation (NAT)

A type of network connection that allows you to connect your virtual machines to an external network when you have only one IP network address, and that address is used by the host computer. If you use NAT, your virtual machine does not have its own IP address on the external network. Instead, a separate private network is set up on the host computer. Your virtual machine gets an address on that network from the VMware virtual DHCP server. The VMware NAT device passes network data between one or more virtual machines and the external network. It identifies incoming data packets intended for each virtual machine and sends them to the correct destination.

See also Bridged networking, Custom networking and Host-only networking.

New Virtual Machine Wizard

A point-and-click interface for convenient, easy creation of a virtual machine configuration. To launch the Wizard, choose **File > New Virtual Machine**. It prompts you for information, suggesting default values in most cases. It creates files that define the virtual machine, including a virtual machine configuration file and (optionally) a virtual disk or physical disk file.

See also Virtual machine settings editor.

Nonpersistent mode

A mode in which all disk writes issued by software running inside a virtual machine with a disk in nonpersistent mode appear to be written to disk but are in fact discarded after the virtual machine is powered off. If you configure a virtual disk or physical disk as an independent disk in nonpersistent mode, the disk is not modified by VMware Server.

See also Independent disk, Persistent mode

Persistent mode

A mode in which all disk writes issued by software running inside a virtual machine are immediately and permanently written to the virtual disk. If you configure a virtual disk or physical disk as an independent disk in persistent mode, the disk behaves like a conventional disk drive on a physical computer.

See also Independent disk, Nonpersistent mode

Physical disk

A hard disk in a virtual machine that is mapped to a physical disk drive or partition on the host machine. A virtual machine's disk can be stored as a file on the host file system or on a local hard disk. When a virtual machine is configured to use a physical disk, VMware Server directly accesses the local disk or partition as a raw device (not as a file on a file system).

See also Virtual disk.

Preallocated disk

A type of virtual disk where all disk space for the virtual machine is allocated at the time the disk is created. This is the default type of virtual disk created by VMware Server.

Quick switch mode

A display mode in which the virtual machine's display fills most of the screen. In this mode, tabs at the top of the screen allow you to switch quickly from one running virtual machine to another.

See also Full screen mode.

Raw disk

See physical disk.

Redo log

The file that stores the changes made to a disk in independent-nonpersistent mode. The redo-log file is deleted when you power off or reset the virtual machine without writing any changes to the disk.

Resume

Return a virtual machine to operation from its suspended state. When you resume a suspended virtual machine, all applications are in the same state they were when the virtual machine was suspended.
See also Suspend.

Shrink

Reduce the amount of file system space a virtual disk occupies in order to reclaim unused space in a virtual disk. If there is empty space in the disk, shrinking reduces the amount of space the virtual disk occupies on the host drive. You cannot shrink preallocated virtual disks or physical disks.

Snapshot

A way to preserve the state of a virtual machine — the state of the data on all the virtual machine's disks and the virtual machine's power state (whether the virtual machine was powered on, powered off or suspended). You can take a snapshot of a virtual machine at any time and revert to that snapshot at any time. The virtual machine can be powered on, powered off or suspended.

Supported partition

A virtual disk partition that VMware Tools can prepare for shrinking, such as one of the drives that comprise the virtual hard disk. You can choose to not prepare certain partitions for shrinking.
See also Shrink.

Suspend

Save the current state of a running virtual machine. To return a suspended virtual machine to operation, use the resume feature.
See also Resume.

Unsupported partition

A virtual disk partition that VMware Tools cannot prepare for shrinking. Unsupported partitions include read-only drive partitions, partitions on remote devices and partitions on removable devices such as floppy drives or CD-ROM

drives.

See also Shrink.

Virtual disk

A virtual disk is a file or set of files that appears as a physical disk drive to a guest operating system. These files can be on the host machine or on a remote file system. When you configure a virtual machine with a virtual disk, you can install a new operating system into the disk file without needing to repartition a physical disk or reboot the host. Virtual disks can be preallocated or growable. A preallocated virtual disk has all the disk space allocated at the time the virtual disk is created. A growable disk is not preallocated; its files start out small in size and grow as data is written to it.

See also Physical disk.

Virtual hardware

The devices that comprise a virtual machine. The virtual hardware includes the virtual disk, the removable devices such as the DVD-ROM/CD-ROM and floppy drives, and the virtual Ethernet adapter. You configure these devices with the virtual machine settings editor.

Virtual machine

A virtualized x86 PC environment in which a guest operating system and associated application software can run. Multiple virtual machines can operate on the same host machine concurrently.

Virtual machine configuration

The specification of what virtual devices (disks, memory size, and so forth) are present in a virtual machine and how they are mapped to host files and devices.

Virtual machine configuration file

A file containing a virtual machine configuration. It is created when you create the virtual machine. It is used by VMware Server to identify and run a specific virtual machine.

Virtual machine settings editor

A point-and-click control panel used to view and modify a virtual machine's settings. You launch it by choosing **VM > Settings**.

See also New Virtual Machine Wizard.

Virtual Network Editor

A point-and-click editor used to view and modify the networking settings for the virtual networks created by VMware Server. You launch by choosing **Host > Virtual Network Settings**.

Virtual SMP

Symmetric multiprocessing enables you to assign two virtual processors to a virtual machine on any host machine that has at least two logical processors.

VMware Authorization Service

The service VMware Server employs to authenticate users. For both Microsoft Windows and Linux hosts, this process is called `vmware-authd`.

VMware Management Interface

A browser-based tool that allows you to control (start, suspend, resume, reset and stop), configure and monitor virtual machines and the server on which they run.

VMware Registration Service

The service VMware Server employs for managing connections to virtual machines and the VMware Management Interface. This process is known as `vmware-serverd` on Linux hosts and `vmware-serverdwin32` on Microsoft Windows hosts.

VMware Tools

A suite of utilities and drivers that enhances the performance and functionality of your guest operating system. Key features of VMware Tools include some or all of the following, depending on your guest operating system: an SVGA driver, a mouse driver, the VMware Tools service, the VMware Tools control panel, and support for such features as the ability to shrink virtual disks, time synchronization with the host, VMware Tools scripts and the ability to connect and disconnect devices while the virtual machine is running.

VMware Tools service

One of the components installed with VMware Tools that performs various duties in the guest operating system, like executing commands in the virtual machine, gracefully shutting down and resetting a virtual machine, sending a heartbeat to VMware Server, synchronizing the time of the guest operating system with the host operating system and passing strings from the host operating system to the guest operating system.

VMware Server Console

An interface to a virtual machine that provides access to one or more virtual machines on the local host or a remote host running VMware Server. You can view the virtual machine's display to run programs within it or modify guest operating system settings. In addition, you can change the virtual machine's configuration, install the guest operating system or run the virtual machine in full screen mode.

Index

Symbols

.vmdk **134, 136, 139**

A

Add Hardware Wizard **191**

Apache, and management interface **111**

Authentication

 Linux hosts **88**

 Windows hosts **85**

Authentication daemon on Linux host **88**

B

Back up

 virtual machines **97**

 VMware Server host **96**

Backup agent

 in virtual machine **95**

 on host **96**

BIOS provided in virtual machine **13**

Bridged networking defined **191**

Browser

 configuring on Linux host **48**

 setting MIME type **128**

BSD

 supported guest operating
 systems **16, 19**

BSD, supported guest operating
systems **16, 19**

C

CD-ROM image file **13**

Chip set in a virtual machine **13**

Clustering **165**

 across multiple hosts **183**

 applications **166**

 cluster in a box **167**

 configuring virtual machines **168**

 iSCSI protocol **183**

 multinode Network Load Balancing
 cluster **175**

 Network Load Balancing **175**

 Novell Clustering Services **179**

 software **166**

 two-node cluster **169, 179**

Configuration, virtual machine **196**

Configure

 after Linux kernel upgrade **42**

 memory size **154**

 Web browser on Linux host **48**

Core files **22**

CPU

 host requirement **5**

 provided in virtual machine **12**

Creating virtual machines on NFS
shares **90**

Ctrl-Alt-Delete in virtual machines **121**

Current virtual machine

 defined **191**

D

Default directories **30, 39**

Devices

 provided in virtual machine **12**

Disks

- available in virtual machine **13**

- existing partition **192**

- physical **194**

- virtual **196**

- Display preferences **122**

- Drawing tablet in a virtual machine **14**

Drives

- See Disks

E

- Encrypting remote sessions **90**

Ethernet

- adapter in a virtual machine **14**

- See Network

- Event log **22**

- Event viewer **94**

F**Floppy**

- drives in virtual machine **14**

- image file **14**

FreeBSD

- supported guest operating systems **16, 19**

- FreeBSD, supported guest operating systems **16, 19**

- Full screen mode, defined **192**

G**Generic SCSI**

- and SCSI reservation **162**

- virtual machine backup **95**

Graphics

- Linux host and performance **154**

- Graphics support in virtual machine **13**

Guest operating system

- defined **192**

- supported **15**

H

- Headless **192**

Heartbeat

- and clustering virtual machines **168**

- virtual machine **104**

- Help, configuring Web browser on Linux host **48**

Host computer

- defined **192**

- system requirements **5**

- Host operating system, defined **193**

Host-only networking

- defined **192**

- enabling on Linux host **42**

- Hot key preferences **121**

I**IDE**

- drives in virtual machine **13**

- See Disks

Image file

- floppy **14**

- ISO **13**

- Input preferences **119**

Install

- default directories **30, 39**

- log **24**

- on Linux host **36**

- on Windows host **26**

- silent **34**

- VmCOM API **52**

- VmPerl API **54–55**

- VMware Management Interface software **44**

- VMware Server Console software **48, 50**

- VMware Workstation **25**
- Internet Explorer 6.0, and management interface **46**
- Inventory
 - and authentication on Linux hosts **89**
 - and private virtual machines **85**
 - defined **193**
- iSCSI protocol **183**
 - bridged networking **185**
 - configuration **184–185**
 - host as iSCSI target **184**
 - initiator virtual machine **184**
 - target node **185**
 - virtual machine as iSCSI target **184**
- ISO image file **13**

K

- Kernel, reconfiguring VMware Server after Linux kernel upgrade **42**
- Keyboard
 - grabbing input **119**
 - in a virtual machine **14**
- Knowledge base **20**

L

- Legacy virtual machine
 - defined **193**
- Linux
 - supported guest operating systems **16**
 - supported host operating systems **7**
- Linux host
 - authentication **88**
 - default permissions **89**
 - installing VMware Server **36**
 - performance **154**
 - permissions **89**

- real-time clock **38**
- uninstalling VMware Server **57**
- upgrading GSX Server **63**
- vmware-authd **88**
- Linux host authentication daemon **88**
- Log files
 - console installation **24**
 - virtual machine **22**
 - virtual machine event log **22**
 - VMware Authorization Service **23**
 - VMware Management Interface **23**
 - VMware Registration Service **24**
 - VMware Server Console **23**
 - VMware Server installation **24**

M

- Master installer, on Windows host **28**
- Memory
 - amount required on host **5**
 - available in virtual machine **13**
 - choosing for best performance **147**
 - for all virtual machines **123**
 - more than 1GB on a Linux host **157**
 - setting size **154**
- Migrate
 - disks in undoable mode **141**
 - virtual machine **64, 138**
- MIME type, configuring for virtual machine consoles **128**
- Mode
 - full screen **192**
 - quick switch **194**
- Mouse
 - grabbing input **119**
 - in a virtual machine **14**
- Moving virtual machines **133**
- UUID **93**

MS-DOS, supported guest operating systems **17**

N

NAT

defined **193**

enabling on Linux host **42**

Netscape, setting MIME type for console **128**

NetWare

See Novell NetWare

Network

bridged networking **191**

custom networking **191**

enabling host-only networking on Linux host **42**

enabling NAT on Linux host **42**

host-only **192**

NAT

Virtual Network Editor **197**

Network adapter in a virtual machine **14**

Network address translation

See NAT

Network Load Balancing

clustering **175**

multinode **175**

New Virtual Machine Wizard **193**

NFS shares, creating virtual machines **90**

Novell Clustering Services **179**

installing **182**

Novell NetWare

clustering **181**

Novell NetWare, supported guest operating systems **19**

O

Operating system

guest **192**

host **193**

supported guest **15**

supported Windows host **7**

P

Parallel port

and the Linux kernel **38**

in a virtual machine **14**

Partition, existing **192**

PCI slots

in virtual machine **14**

limits **14**

Performance

CD-ROM drive polling **148**

debugging mode **148**

disk options **149**

guest operating system selection **147**

installing applications in a guest **150**

memory settings **147**

memory usage **154**

remote disk access **150**

swap space on a Linux host **154**

temp directory on a Linux host **154**

using full screen mode on a Linux host **153-154**

Permissions

and user accounts **86**

Linux host **89**

physical disk **89**

snapshot **89**

virtual disks **89**

virtual machines **83**

Physical disk

defined **194**

permissions **89**

- Port numbers
 - console **78**
 - management interface **99**
- Preallocated disk, defined **194**
- Preferences
 - display **122**
 - hot keys **121**
 - input **119**
 - keyboard combinations **121**
 - shortcut keys **121**
 - user **117**
 - VMware Server **123**
 - workspace **118**
- Priority
 - preferences **123**
 - Windows host **123**
- Private virtual machines **84**
- Process scheduler on a Windows
 - host **123**
- Processor
 - host requirement **5**
 - provided in virtual machine **12**
- Q**
- Quick switch mode **194**
- Quiet mode, install VMware Server **34**
- R**
- RAM
 - amount required on host **5**
 - available in virtual machine **13**
- Real-time clock, requirement on Linux
 - host **38**
- Redo log, defined **195**
- Registration **21**
- Remote management **77**
 - encrypted communications **90**
 - SSL **90**
- VMware Management Interface **77**
- VMware Scripting APIs **77**
- VMware Server Console **77**
 - vmware-cmd **78**
- Resume, defined **195**
- S**
- SCSI
 - devices in virtual machine **13**
 - generic **95**
- SCSI reservation
 - and clustering **161**
 - enabling **162**
 - issues to consider **164**
 - preallocated virtual disks **161**
 - sharing SCSI disks **161**
 - support **162**
- Security certificates **91**
- Serial port, in a virtual machine **14**
- Set up
 - memory size **154**
 - Web browser on Linux host **48**
- Shortcut keys, configuring **121**
- Shrink, defined **195**
- Silent install **34**
- SMBIOS
 - in a virtual machine **13**
 - modifying UUID **92**
- Snapshot
 - defined **195**
 - permissions **89**
- Sound in a virtual machine **15**
- Specifications for virtual machine
 - platform **12**
- SSL
 - console connections **90**
 - custom security certificates **91**

- enabling **112**
- for consoles **91, 112, 125**
- for the management interface **91**
- management interface
 - connections **90**
- remote management **90**
- Support resources, technical **20**
- Supported guest operating system **15**
- Supported host operating system
 - Windows **7**
- Supported partition **195**
- Suspend, defined **195**
- System requirements **5**
 - remote workstation **10**

T

- Technical support resources **20**
- Tools
 - See VMware Tools

U

- Undoable mode, migrating **141**
- Uninstall
 - on Linux host **57**
 - on Windows host **55**
- Unsupported partition **195**
- Update VMware Server software **119**
- Upgrade
 - from GSX Server 1 and 2 **59**
 - Linux kernel, reconfiguring GSX Server after upgrade **42**
 - on Linux host **63**
 - on Windows host **62**
 - virtual machine **64**
 - VMware GSX Server **59**
- USB, virtual machine ports **14**
- User groups **20**
- User preferences **117**

UUID 92

- automatic generation **92**
- modifying **136**
- moving virtual machines **93**
- virtual machine configuration file **93**

V

- Virtual disk
 - defined **196**
 - permissions **89**
- Virtual hardware **196**
- Virtual machine
 - accessibility **86**
 - backing up **95**
 - changing user **87**
 - configuring in management interface **105**
 - connected users **109**
 - Ctrl+Alt+Delete **121**
 - default directory **123**
 - defined **196**
 - deleting from host **111**
 - event log **110**
 - grabbing input **119**
 - heartbeat **104**
 - log **22**
 - migrating **138**
 - moving **133**
 - moving between VMware products **133**
 - permissions **83**
 - platform specifications **12**
 - private **84**
 - resources and permissions **89**
 - running on Linux host **88**
 - running on Windows host **85**
 - upgrading **64**

- user **86**
- UUID **92**
- VMID **106**
- Virtual machine settings editor,
 - defined **196**
- Virtual Network Editor **197**
- VMware Authorization Service **85**
 - defined **197**
 - log **23**
- VMware community forums **20**
- VMware guest operating system service
 - defined **197**
 - virtual machine heartbeat **104**
- VMware Management Interface **97**
 - advanced configuration options **107**
 - Apache commands **111**
 - changing port number **99**
 - configuring to launch console **46**
 - configuring virtual machines **105**
 - connected users **109**
 - defined **197**
 - disabling SSL **91**
 - downloading console installer **81**
 - enable JavaScript **99**
 - enable style sheets **99**
 - enabling SSL **91**
 - enabling SSL for remote connections **112**
 - encrypted communications **90**
 - host summary information **101**
 - launching remote console **46**
 - launching remote consoles **48**
 - log **23**
 - logging in **99**
 - logging out **111**
 - permissions **90**
 - proxy servers **47**
 - refresh rate **98**
 - remote management **77**
 - setting session length **99**
 - SSL **90**
 - startup and shutdown options **114, 127**
 - Status Monitor **101**
 - supported browsers **99**
 - URL to log in **99**
 - virtual machine event log **110**
 - virtual machine heartbeat **104**
 - virtual machine menu **102**
 - virtual machine summary **101**
- VMware Registration Service
 - defined **197**
 - log **24**
- VMware Scripting APIs
 - downloading from management interface **82**
 - installing **51**
 - remote management **77**
- VMWare Server
 - global preferences **123**
- VMware Server
 - software updates **119**
 - user preferences **117**
- VMware Server Console **198**
 - changing port number **78**
 - connecting from management interface **103**
 - deleting virtual machines **112**
 - disabling SSL **91, 112, 125**
 - download from management interface **81, 100**
 - enabling SSL **91, 112, 125**
 - encrypted communications **90**
 - install **48**

- installation **50**
 - launching from management interface **46**
 - launching from Netscape **128**
 - log **23**
 - remote management **77**
 - securing connections **125**
 - setting MIME type **128**
 - SSL **90**
 - X server **45**
 - VMware Server host
 - backing up **95**
 - configuring **112**
 - default virtual machine directory **123**
 - securing connections with SSL **112**
 - VMware Tools
 - defined **197**
 - heartbeat **104**
 - VMware Virtual Machine Console
 - downloading installer **81**
 - vmware-authd **88**
 - See VMware Authorization Service
 - vmware-cmd **78**
 - vmware-config.pl **41**
 - vmware-serverd
 - See VMware Registration Service
 - VNC Viewer, using with virtual machines **78**
- W**
- Windows host
 - authentication **85**
 - configuring permissions **87**
 - Event Viewer **94**
 - installing GSX Server **26**
 - installing Scripting APIs on **52**
 - priority preferences **123**
 - process scheduler **123**
 - uninstalling VMware Server **55**
 - upgrading GSX Server **62**
 - Windows operating system
 - installing Scripting APIs on **52**
 - Windows Terminal Services, using with virtual machines **78**
 - Windows XP Remote Desktop, using with virtual machines **78**
 - Windows, supported guest operating systems **16**
 - Wizard
 - add hardware **191**
 - new virtual machine **193**
 - Workspace preferences **118**
- X**
- X server **45**
 - required on Linux client **12**
 - required on Linux host **10**
 - XFree86
 - required on Linux client **12**
 - required on Linux host **10**