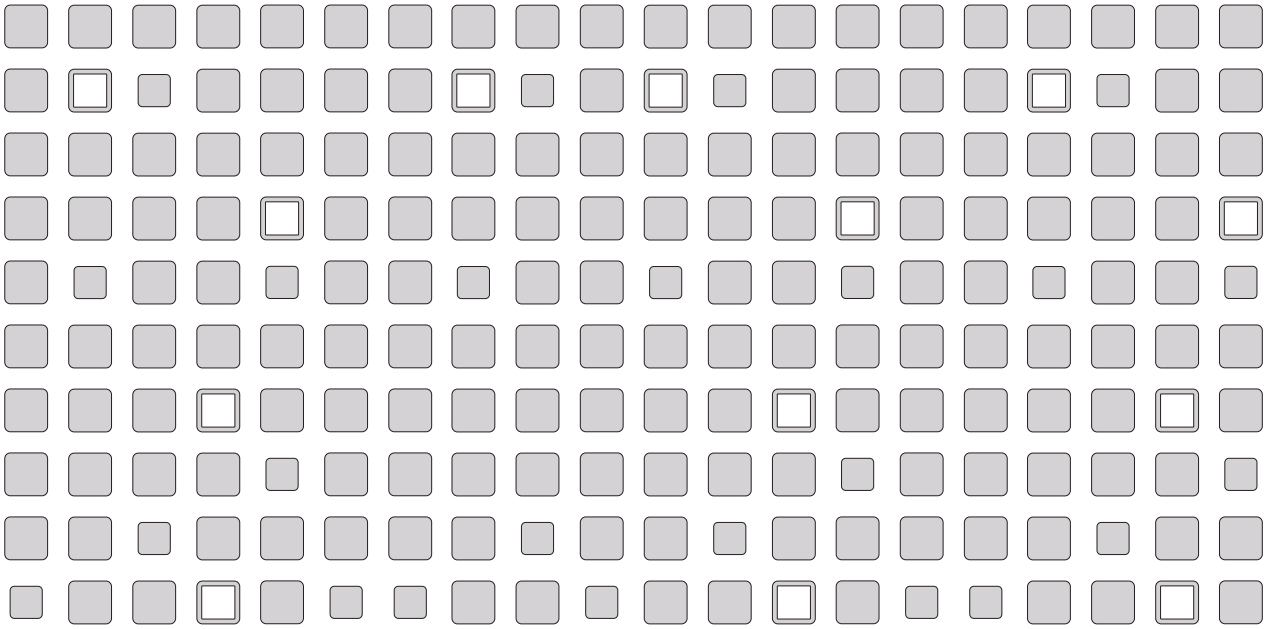
Workstation 4

Powerful Virtual Machine Software for the Technical Professional

User's Manual



vmware®

VMware, Inc.

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

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

 Revision: 20040611 Version: 4.5.2 Item: WS-ENG-Q204-018

Table of Contents

CHAPTER 1

Introduction and System Requirements

This section contains the following:

Thank you for choosing VMware® Workstation, the powerful virtual machine software for enterprise IT professionals that runs multiple operating systems and their applications simultaneously on a single PC.

If you're new to VMware Workstation, this is the place to start.

If you're a veteran user of VMware products, take a few minutes to see what's new in version 4 and check out the notes on upgrading your installation.

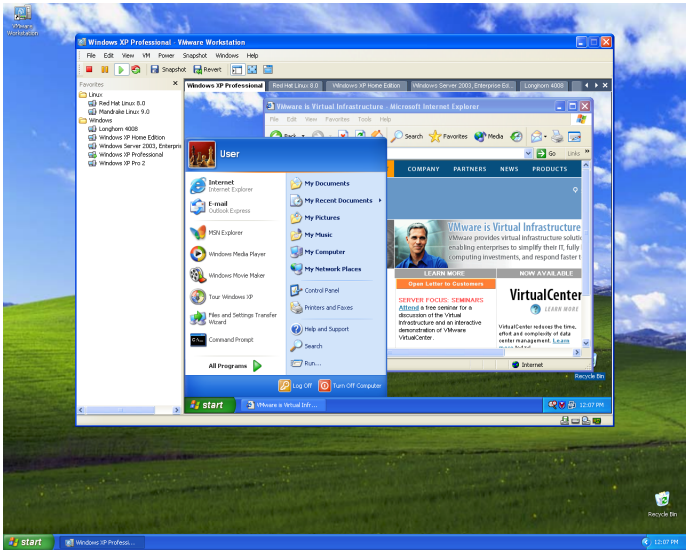
The first chapters of this manual — through Running VMware Workstation on page 95 — introduce you to some of the things you can do with VMware Workstation and guide you through the key steps for installing the software and putting it to work.

Later chapters provide in-depth reference material for getting the most out of the sophisticated features of VMware Workstation.

Powerful Virtual Machine Software for the Technical Professional

VMware Workstation is powerful virtual machine software for system administrators and developers who want to revolutionize software development, testing and deployment in their enterprise. Shipping for over five years and winner of over a dozen major product awards, VMware Workstation enables software developers to develop and test the most complex networked server-class applications running on Microsoft® Windows®, Linux® or Novell® NetWare® — all on a single desktop.

Essential features such as Windows, Linux and NetWare support, virtual networking, live snapshots, drag-and-drop, shared folders and PXE support make VMware Workstation a powerful, indispensable tool for enterprise IT developers and system administrators.



Run the operating systems and applications you need — all on a single desktop

With over five years of proven success and millions of users, VMware Workstation improves efficiency, reduces costs and increases flexibility and responsiveness. Installing VMware Workstation on the desktop is the first step to transforming your IT

infrastructure into virtual infrastructure. VMware Workstation is used in the enterprise to

- Streamline software development and testing operations
- Accelerate application deployments
- Ensure application compatibility and perform operating system migrations

VMware Workstation enables multiple operating systems and their applications to run concurrently on a single physical machine. These operating systems and applications are isolated in secure virtual machines that coexist on a single piece of hardware. The VMware virtualization layer maps the physical hardware resources to the virtual machine's resources, so each virtual machine has its own CPU, memory, disks and I/O devices. A virtual machines is the full equivalent of a standard x86 machine.

With VMware Workstation you can

- Build complex networks — and develop, test and deploy new applications — all on a single computer
- Leverage the portability of virtual machines so you can easily share development environments and prepackaged configurations — complete with operating system and applications — without risk
- Add or change operating systems without repartitioning disks or rebooting
- Run new operating systems and legacy applications on one computer

Since its launch in 1999, VMware Workstation has revolutionized the way software and IT infrastructure are developed and has become the de facto standard for IT professionals and developers worldwide. When you deploy VMware Workstation in your environment you will

- Shorten development cycles
- Reduce problem resolution time
- Increase productivity
- Accelerate time to market
- Improve project quality

If your business is looking to simplify and accelerate development, testing and deployment of software and IT infrastructure, VMware Workstation is essential.

.

Host and Guest

- The physical computer on which you install the VMware Workstation software is called the host computer, and its operating system is called the host operating system.
- The operating system running inside a virtual machine is called a guest operating system.
- For definitions of these and other special terms, see the glossary at the end of this manual.

What's New in Version 4

Whether you're a long-time power user of VMware Workstation or a beginning user who is just learning what you can do with virtual machines, the new features in VMware Workstation 4 extend its capabilities and make it easier to use.

New in Version 4.5.2

Here are highlights of some key features added in VMware Workstation 4.5.2:

Experimental Support for 64-bit Host Operating Systems
This means you can install this release of VMware Workstation on a 64-bit host computer that uses an AMD64 Opteron, Athlon 64 or Intel IA-32e CPU. Virtual machines you create on these hosts have 32-bit CPUs and can run 32-bit guest operating systems.

Experimental Support for Solaris Guest Operating Systems
This means you may install the x86 platform edition of Solaris 9 and of Solaris 10 beta as guest operating systems in this release of VMware Workstation. VMware Tools is not available for Solaris. If you want to run the guest operating system's X server, you may do so in 16 colors.

Support for SUSE LINUX 9.1 Guests
This means you may run SUSE LINUX 9.1 as a guest operating system in this release of VMware Workstation.

New in Version 4.5

Here are highlights of some key features added in VMware Workstation 4.5:

Increased Memory Size for Virtual Machines
This means you can create individual virtual machines with up to 3,600MB of memory and use up to 4GB of memory for all running virtual machines.

Experimental Support for Longhorn
This means you can install and run beta versions of the next version of Windows, code-named Longhorn. Because Longhorn is still in the beta stage of development, you should expect it to install and run more slowly than other guest operating systems.

Improved Support for Guests Using Linux Kernels in the 2.6 Series
This means better performance for virtual machines running manually installed 2.6 kernels and also for virtual machines using some of the later releases of Red Hat Linux 9, which incorporate some components from the 2.6 kernel.

Support for PXE
This means that if you use a preboot execution environment (commonly known as PXE) to boot and install operating systems into new virtual machines, you can do so without any add-on software.

Tip of the Day
A pop-up tip introduces you to a key feature of VMware Workstation each time you launch the program. You can turn the tips off if you prefer not to see them.

USB Device Installation for Nonadministrators
Any user on a Windows host can connect USB devices for use in a virtual machine. You no longer need administrative privileges on the host to connect a USB device to a virtual machine. See Installing USB Devices as a Non-Administrator on page 299 for details.

Automatic Check for Product Updates
VMware Workstation now checks automatically to see if updates for the product are available. You can adjust the interval between the automatic checks or turn off automatic checking. See Checking for Product Updates on page 124 for details.

New Operating System Support
Get the freedom to choose the operating systems and applications that work best for you. VMware Workstation 4.5 adds support for Novell NetWare 5.1, 6 and 6.5; and SUSE™ LINUX 9.0.

New in Version 4.0

Here are highlights of some key features added in VMware Workstation 4.0:

Snapshots
You can take a snapshot of your virtual machine's state, a point-in-time copy of the running system state, saved to disk. You can revert to that snapshot at any time — making it easier to do repetitive testing and debugging. You can also configure a virtual machine so it reverts to the snapshot each time you power it off. See Taking and Reverting to a Snapshot on page 118 for details.

Drag and Drop
You can drag and drop files and folders in both directions between Windows hosts and Windows guests. See Using Drag and Drop on page 116 for details.

Shared Folders
Shared folders give you an easy way to share files between the host and one or more guests. See Using Shared Folders on page 113 for details.

Full Debug Support
Programmers now have the full functionality of native program debugging within a virtual machine with support for both user- and kernel-level debuggers. For more information on configuring virtual machines for a debugging session, see Examples: Debugging over a Virtual Serial Port on page 286.

Improved Sound and Video
Listen to music in a virtual machine with the high fidelity provided by the new sound device, which emulates the popular Creative Labs Sound Blaster® AudioPCI. Get upgraded high performance graphics that let you display streaming video without skipping a beat.

New Operating System Support.
VMware Workstation 4.0 provides support for Microsoft Windows Server 2003; Red Hat™ Linux 8.0 and 9.0, Red Hat Linux Advanced Server 2.1, and Red Hat Enterprise Linux Workstation 2.1; SuSE Linux 8.0, 8.1, 8.2 and Enterprise Server 8; and Mandrake™ Linux 9.0.

New User Interface
The Linux user interface is updated throughout, and includes a completely revamped virtual machine settings editor. Windows hosts have an updated Favorites list. And on both hosts, you can run multiple virtual machines in the same window and tab from one to another using the new quick switch mode. See Running VMware Workstation on page 95 for details.

Network Settings (Windows Host)
The Virtual Network Editor for Windows hosts now provides a graphical interface you can use to change the configuration of the DHCP servers running on your virtual networks. It also lets you configure the NAT device and the host virtual adapters. See Changing the Networking Configuration on page 219 for details.

Host System Requirements

What do you need to get the most out of VMware Workstation 4? Take the following list of requirements as a starting point. Remember that the virtual machines running under VMware Workstation are like physical computers in many ways — and, like physical computers, they generally perform better if they have faster processors and more memory.

PC Hardware

- Standard PC
- 500MHz or faster compatible x86 processor (recommended; 400MHz minimum)

  Compatible processors include

  - Intel®: Celeron®, Pentium® II, Pentium III, Pentium 4, Pentium M (including computers with Centrino™ mobile technology), Xeon™ (including "Prestonia")
  - AMD™: Athlon™, Athlon MP, Athlon XP, Duron™, Opteron™

  For additional information, including notes on processors that are not compatible, see the VMware knowledge base at*www.vmware.com/support/kb/enduser/std_adp.php?p_faqid=967*.
- Multiprocessor systems supported
- Experimental support for AMD64 Opteron, Athlon 64 or Intel IA-32e CPU

Memory

- Enough memory to run the host operating system, plus memory required for each guest operating system and for applications on the host and guest; see your guest operating system and application documentation for their memory requirements
- 256MB recommended, 128MB minimum

Display

- 16-bit display adapter recommended; greater than 8-bit display adapter required
- Linux hosts must have an X server that meets the X11R6 specification (such as XFree86) and a video adapter supported by that server to run guest operating systems in full screen mode

Disk Drives

- 100MB (for Windows hosts), 20MB (for Linux hosts) free space required for basic installation

- At least 1GB free disk space recommended for each guest operating system and the application software used with it; if you use 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, CD-ROM and DVD-ROM drives supported
- Guest operating systems can reside on physical disk partitions or in virtual disk files

Local Area Networking (Optional)

- Any Ethernet controller supported by the host operating system
- Non-Ethernet networks supported using built-in network address translation (NAT) or using a combination of host-only networking plus routing software on the host operating system

Windows Host Operating Systems

- Windows Server 2003 Web Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition
- Windows XP Professional and Windows XP Home Edition with Service Pack 1 (listed versions also supported with no service pack)
- Windows 2000 Professional Service Pack 3 or 4, Windows 2000 Server Service Pack 3 or 4, Windows 2000 Advanced Server Service Pack 3 or 4 (listed versions also supported with no service pack)
- Windows NT® Workstation 4.0 Service Pack 6a, Windows NT Server 4.0 Service Pack 6a, Windows NT 4.0 Terminal Server Edition Service Pack 6

  Caution: Do not install VMware Workstation on a Windows NT 4.0 Server system that is configured as a primary or backup domain controller.

Internet Explorer 4.0 or higher required for Help system

Linux Host Operating Systems

Supported distributions and kernels are listed below. VMware Workstation may not run on systems that do not meet these requirements.

Note: As newer Linux kernels and distributions are released, VMware modifies and tests its products for stability and reliability on those host platforms. We make 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 below, its use with our products is not supported. Look for newer prebuilt modules in the download area of our Web site. Go to*www.vmware.com/download/*.

- Mandrake Linux 9.0 — stock 2.4.19
- Mandrake Linux 8.2 — stock 2.4.18-6mdk
- Red Hat Enterprise Linux 3.0 — stock 2.4.21, update 2.4.21-15.EL
- Red Hat Enterprise Linux 2.1 — stock 2.4.9-e3
- Red Hat Linux Advanced Server 2.1 — stock 2.4.9-e3
- Red Hat Linux 9.0 — stock 2.4.20-8, 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, upgrade 2.4.9-7, upgrade 2.4.9-13, upgrade 2.4.9-21, upgrade 2.4.9-31
- Red Hat Linux 7.1 — stock 2.4.2-2, upgrade 2.4.3-12
- Red Hat Linux 7.0 — stock 2.2.16-22, upgrade 2.2.17-14
- SUSE LINUX 9.1 — stock 2.6.4-52
- SUSE LINUX 9.0 — stock 2.4.21-99
- SuSE Linux Enterprise Server 8 — stock 2.4.19
- 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 Enterprise Server 7 — stock 2.4.7 and patch 2
- SuSE Linux 7.3 — stock 2.4.10

Platforms not listed above are not supported.

Web browser required for Help system

Virtual Machine Specifications

Each virtual machine created with VMware Workstation 4 provides a platform that includes the following devices that your guest operating system can see.

Processor

- Same processor as that on host computer

  Note: A 64-bit processor runs in 32-bit legacy mode inside the virtual machine.

- Single processor per virtual machine on symmetric multiprocessor systems

Chip Set

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

BIOS

- PhoenixBIOS™ 4.0 Release 6 with VESA BIOS

Memory

- Up to 3600MB, depending on host memory
- Maximum of 4GB total available for all virtual machines

Graphics

- VGA and SVGA support

IDE Drives

- Up to four devices — disks, CD-ROM or DVD-ROM (DVD drives can be used to read data DVD-ROM discs; DVD video is not supported)
- Hard disks can be virtual disks or physical disks
- IDE virtual disks up to 128GB
- CD-ROM can be a physical device or an ISO image file

SCSI Devices

- Up to seven devices
- SCSI virtual disks up to 256GB
- Hard disks can be virtual disks or physical disks
- Generic SCSI support allows devices to be used without need for drivers in the host operating system

  Works with scanners, CD-ROM, DVD-ROM, tape drives and other SCSI devices

- LSI Logic® LSI53C10xx Ultra160 SCSI I/O controller
- Mylex® (BusLogic) BT-958 compatible host bus adapter (requires add-on driver from VMware for Windows XP and Windows Server 2003)

Floppy Drives

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

Serial (COM) Ports

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

Parallel (LPT) Ports

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

USB ports

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

Keyboard

- 104-key Windows 95/98 enhanced

Mouse and Drawing Tablets

- PS/2 mouse
- Serial tablets supported

Ethernet Card

- Up to three virtual Ethernet cards
- AMD PCnet-PCI II compatible

Sound

- Sound output and input
- Emulates Creative Labs Sound Blaster AudioPCI (MIDI input, game controllers and joysticks not supported)

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

Supported Guest Operating Systems

The operating systems listed here have been tested in VMware Workstation 4 virtual machines and are officially supported. For notes on installing the most common guest operating systems, see the *VMware Guest Operating System Installation Guide*, available from the VMware Web site or from the Help menu.

Operating systems that are not listed are not supported for use in a VMware Workstation virtual machine. For the most recent list of supported guest operating systems, see the support section of the VMware Web site, *www.vmware.com/support/*.

Microsoft Windows

- Windows, code-named Longhorn, beta (experimental)
- Windows Server 2003 Web Edition, Windows Server 2003 Standard Edition, Windows Server 2003 Enterprise Edition
- Windows XP Professional and Windows XP Home Edition with Service Pack 1 or Service Pack 2 RC (listed versions also supported with no service pack)
- Windows 2000 Professional Service Pack 1, 2, 3 or 4; Windows 2000 Server Service Pack 1, 2, 3 or 4; Windows 2000 Advanced Server Service Pack 3 or 4 (listed versions also supported with no service pack)
- Windows NT® Workstation 4.0 Service Pack 6a, Windows NT Server 4.0 Service Pack 6a, Windows NT 4.0 Terminal Server Edition Service Pack 6
- Windows Me
- Windows 98 (including all Customer Service Packs) and Windows 98 SE
- Windows 95 (including Service Pack 1 and all OSR releases)
- Windows for Workgroups 3.11
- Windows 3.1

Microsoft MS-DOS

- MS-DOS 6.x

Linux

- Mandrake Linux 8.2, 9.0
- Red Hat Linux 7.0, 7.1, 7.2, 7.3, 8.0, 9.0
- Red Hat Enterprise Linux 2.1, 3.0
- Red Hat Linux Advanced Server 2.1
- SuSE Linux 7.3, 8.0, 8.1, 8.2, 9.0, 9.1

- SLES 7, 7 patch 2, 8
- Turbolinux Server 7.0, Enterprise Server 8, Workstation 8

Novell NetWare

- NetWare 5.1, 6, 6.5

FreeBSD

- FreeBSD 4.0–4.6.2, 4.8, 5.0

  Note: If you use SCSI virtual disks larger than 2GB with FreeBSD 4.0–4.3, there are known problems, and the guest operating system does not boot. To work around this issue, see the *VMware Guest Operating System Installation Guide*, available from the VMware Web site or from the Help menu.

Solaris

- Solaris x86 Platform Edition 9 (experimental), 10 beta (experimental)

Technical Support Resources

Documentation on the Web

Full documentation for VMware Workstation, including the latest updates to the manual, can be found on the VMware Web site at *www.vmware.com/support/*.

VMware Knowledge Base

You can find troubleshooting notes and tips for advanced users in the knowledge base on the VMware Web site at *www.vmware.com/kb*.

VMware User Community

Community Discussion Forums

The VMware Community is a set of moderated discussion forums hosted on the VMware Web site and is open to all VMware users. In the forums, you can share your experiences in using VMware products, raise technical questions or issues and benefit from the expertise and advice of other VMware users.

Newsgroups

The VMware newsgroups are primarily forums for users to help each other. You are encouraged to read and post issues, work-arounds and fixes. While VMware personnel may read and post to the newsgroups, they are not a channel for official support. The VMware NNTP news server is at *news.vmware.com*.

For more information on the forums and newsgroups, see *www.vmware.com/support/newsgroups.htm*.

Reporting Problems

If you have problems while running VMware Workstation, please report them to the VMware support team.

These guidelines describe the information we need from you to diagnose problems.

If a virtual machine exits abnormally or crashes, please run the support script to collect the appropriate log files and system information. Follow the steps below that apply to your host computer.

Windows Host

1. Open a command prompt.

2. Change to the VMware Workstation program directory.
   ```
   C:
   cd \Program Files\VMware\VMware Workstation
   ```
   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
   ```
4. After the script runs, it displays the name of the directory where it has stored its output. Use a file compression utility such as WinZip or PKZIP to zip that directory and include the zip file with your support request.

Linux Host

1. Open a terminal.
2. Run the support script as the user who is running the virtual machine.
   ```
   vm-support
   ```
   If you are not running 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 will ask you to run the script again as root.
3. The script creates a compressed `.tgz` file in the current directory. Include that output file with your support request.

If you are reporting a problem you encountered while installing VMware Workstation, it is also helpful to have your installation log file.

On a Windows host, the file is `VMInst.log`. It is saved in your temp folder. On a Windows NT host, the default location is `C:\temp`. On a Windows 2000, Windows XP or Windows Server 2003 host, the default location is `C:\Documents and Settings\<username>\Local Settings\Temp`. The `Local Settings` folder is hidden by default. To see its contents, open **My Computer**, go to **Tools** > **Folder Options**, click the **View** tab and select **Show Hidden Files and Folders**.

Be sure to register your serial number. You may then report your problems by submitting a support request at *www.vmware.com/requestsupport*.

CHAPTER 2

Installing VMware Workstation

The following sections describe how to install VMware Workstation on your Linux or Windows host system:

Selecting Your Host System

VMware Workstation is available for both Windows and Linux host computers. The installation files for both host platforms are included on the same CD-ROM.

Your serial number allows you to use VMware Workstation only on the host operating system for which you licensed the software. If you have a serial number for a Windows host, you cannot run the software on a Linux host, and vice versa.

To use VMware Workstation on a different host operating system — for example, to use it on a Linux host if you have licensed the software for a Windows host — purchase a license on the VMware Web site. You may also get an evaluation license at no charge for a 30-day evaluation of the software. For more information, see*www.vmware.com/download/*.

To install on a supported Windows host computer, see Installing VMware Workstation 4 on a Windows Host on page 29. To install on a Linux host computer, see Installing VMware Workstation 4 on a Linux Host on page 36.

Upgrading from Previous Versions

If you are upgrading from a previous version of VMware Workstation, read Upgrading VMware Workstation on page 41 before you begin.

Installing VMware Workstation 4 on a Windows Host

Getting started with VMware Workstation is simple. The key steps are

1. Install the VMware Workstation software as described in this section.
2. Start VMware Workstation and enter your serial number. You need to do this only once — the first time you start VMware Workstation after you install it.
3. Create a virtual machine using the New Virtual Machine Wizard. See Creating a New Virtual Machine on page 65.
4. 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 and VMware Tools on page 78.
5. Install the VMware Tools package in your virtual machine for enhanced performance. See Installing VMware Tools on page 81.
6. Start using your virtual machine.

Before you begin, be sure you have

- A computer and host operating system that meet the system requirements for running VMware Workstation. See Host System Requirements on page 17.
- The VMware Workstation installation software. If you bought the packaged distribution of VMware Workstation, the installation software is on the CD in your package. If you bought the electronic distribution, the installation software is in the file you downloaded.
- Your VMware Workstation serial number. The serial number is included in the VMware Workstation package or in the email message confirming your electronic distribution order.
- The installation CD or disks for your guest operating system.

Installing the VMware Workstation Software

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

   Caution: Do not install VMware Workstation on a Windows NT Server 4.0 system that is configured as a primary or backup domain controller.

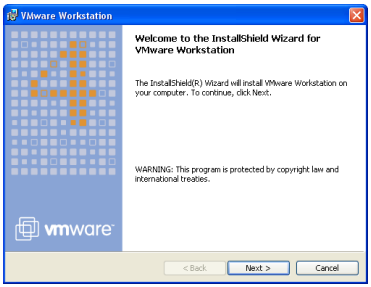
Note: On a Windows XP or Windows Server 2003 host computer, you must be logged in as a local administrator (that is, not logged in to the domain) in order to install VMware Workstation.

Note: Although you must be logged in as an administrator to install VMware Workstation, a user with normal user privileges can run the program after it is installed. Keep in mind that you need one license for each user.

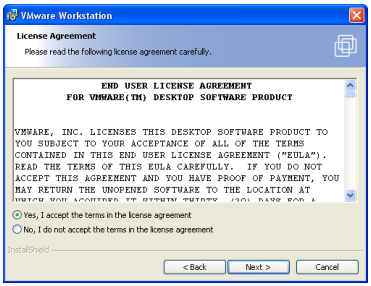
2. If you are installing from a CD, from the **Start** menu, choose **Run** and enter `D:\setup.exe`, where `D:` is the drive letter for your CD-ROM drive.

   If you are installing from a downloaded file, from the **Start** menu, choose **Run**, browse to the directory where you saved the downloaded installer file and run the installer. (The filename is similar to `VMwareWorkstation-<xxxx>.exe`, where `<xxxx>` is a series of numbers representing the version and build numbers.)

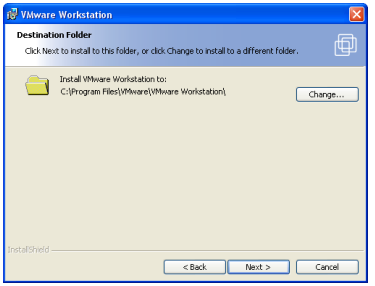
3. The Welcome dialog box appears.



Click **Next**.



4. Acknowledge the end user license agreement (EULA). Select the **Yes, I accept the terms in the license agreement** option, then click **Next**.

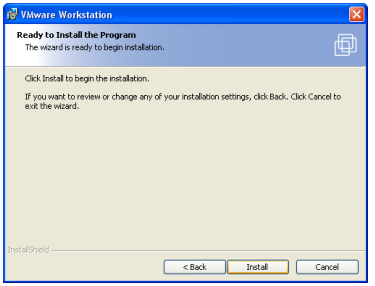


5. Choose the directory in which to install VMware Workstation. To install it in a directory other than the default, click **Change** and browse to your directory of choice. If the directory does not exist, the installer creates it for you. Click **Next**.

   Caution: Do not install VMware Workstation on a network drive.

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

6. The installer has gathered the necessary information and is ready to begin installing the software.



   If you want to change any settings or information you provided, now is the time to make those changes. Click **Back** until you reach the dialog box containing the information you want to change.

   If you do not need to make any changes, click **Install**. The installer begins copying files to your computer.

7. If the installer detects that the CD-ROM autorun feature is enabled, you see a message that gives you the option to disable this feature. Disabling it prevents undesirable interactions with the virtual machines you install on this system.
8. You may see one or more Digital Signature Not Found dialog boxes when the installer begins to install the VMware Virtual Ethernet Adapters. You can safely ignore these warnings and click **Yes** or **Continue** to approve installation of the drivers.
9. A dialog box appears, asking if you want to rename existing virtual disks using the `.vmdk` extension.

This naming convention was introduced in VMware Workstation 3. If your virtual disk files already use the `.vmdk` extension, click **No** to skip this process. Click **Yes** if you want to search all local drives on the host computer and make this change.

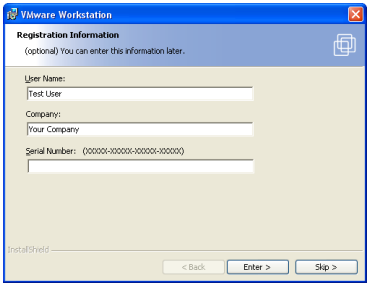
The converter also renames the files that store the state of a suspended virtual machine, if it finds them. It changes the old `.std` file extension to `.vmss`. However, it is best to resume and shut down all suspended virtual machines before you upgrade from VMware Workstation 3 to VMware Workstation 4.

Besides renaming files, the converter updates the corresponding virtual machine configuration files so they identify the virtual disks using the new filenames.

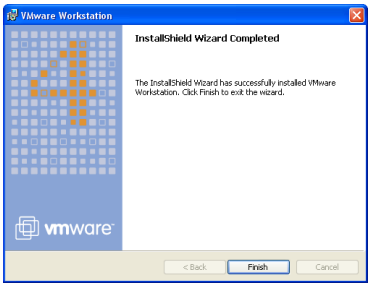
If you store your virtual disk files or suspended state files on a Windows XP or Windows Server 2003 host — or if you may do so in the future — it is important to convert the filenames to avoid conflicts with the System Restore feature of Windows XP and Windows Server 2003.

One Chance to Rename Disk Files

- The Rename Virtual Disks dialog box appears only once. If you click Cancel, you will not have another opportunity to update the filenames and configuration files automatically.



10. If you wish, enter your name, company name and serial number, then click **Next**. The serial number is on the registration card in your package. The user and company information you enter here is then made available in the About box (**Help** > **About VMware Workstation**). If you skip this step, you are prompted to enter your serial number the first time you run VMware Workstation.



11. Click **Finish**. The VMware Workstation software is installed.
12. A prompt suggests that you reboot your PC. Reboot now to allow VMware Workstation to complete the installation correctly.

Installing VMware Workstation Silently

If you are installing VMware Workstation on a number of Windows host computers — in a corporate environment, for example — you may want to use the silent install features of the Microsoft Windows Installer.

Before installing VMware Workstation silently, you must ensure that the host computer has version 2.0 or higher of the MSI runtime engine. This version of the installer is available in versions of Windows beginning with Windows XP and is available separately from Microsoft for versions of Windows beginning with Windows NT 4.0.

The following steps outline the procedures for a silent install. For additional details on using the Microsoft Windows Installer, see the Microsoft Web site.

1. Silently extract the administrative installation image from the VMware Workstation installer:

   ```
   setup.exe /a /s /v"/qn TARGETDIR=<InstallTempPath>"
   ```

   `setup.exe` is the name of the installer on the CD distribution. If you are using a downloaded installer, the filename is similar to `VMwareWorkstation-<xxxx>.exe`, where `<xxxx>` is a series of numbers representing the version and build numbers.

   `<InstallTempPath>` is the full path to the folder where you want to store the administrative installation image.

2. Run a silent installation using `msiexec` and the administrative installation image you extracted in the previous step:

   ```
   msiexec -i "<InstallTempPath>\VMware Workstation.msi"
   [INSTALLDIR="<PathToProgramDirectory>"] ADDLOCAL=ALL
   [REMOVE=<featurename,featurename>] /qn
   ```

   Enter the command on one line. If you want to install VMware Workstation in a location other than the default, change the path that follows `INSTALLDIR=` to specify the desired location.

   You may use the optional `REMOVE=` property to skip installation of certain features. The `REMOVE=` property can take one or more of the following values:

Value	Description
`Authd`	The VMware authorization service
`Network`	Networking components including the virtual bridge and the host adapters for host only networking and NAT networking; do not remove if you want to use NAT or DHCP
`DHCP`	The virtual DHCP server
`NAT`	The virtual NAT device

   If you specify more than one value, use a comma to separate the values. For example, `REMOVE=Authd,NAT`.

   Note: If you specify `REMOVE=Network`, the installer skips installation of certain networking components, including NAT and DHCP. There is no need to specify `DHCP` or `NAT` separately.

You may customize the installation further by adding any of the following installation properties to the command using the format `PROPERTY="value"`. A value of 1 means true; a value of 0 means false. If you use the serial number property, enter the serial number, complete with hyphens (`xxxxx-xxxxx-xxxxx-xxxxx`).

Property	Effect of the Property	Default
`DESKTOP_SHORTCUT`	Installs a shortcut on the desktop	1
`DISABLE_AUTORUN`	Disables CD autorun on the host	1
`REMOVE_LICENSE`	(Uninstall only) Removes all stored licenses at uninstall	0
`SERIALNUMBER`	Automatically enters the serial number	

Uninstalling VMware Workstation 4 on a Windows Host

To uninstall VMware Workstation 4, use the Add/Remove Programs control panel. Select the entry for VMware Workstation, then click **Remove**. Follow the on-screen instructions.

Installing VMware Workstation 4 on a Linux Host

Getting started with VMware Workstation is simple. The key steps are

1. Install the VMware Workstation software as described in this section.
2. Start VMware Workstation and enter your serial number. You need to do this only once — the first time you start VMware Workstation after you install it.
3. Create a virtual machine using the New Virtual Machine Wizard. See Creating a New Virtual Machine on page 65.
4. 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 and VMware Tools on page 78.
5. Install the VMware Tools package in your virtual machine for enhanced performance. See Installing VMware Tools on page 81.
6. Start using your virtual machine.

Before you begin, be sure you have

- A computer and host operating system that meet the system requirements for running VMware Workstation. See Host System Requirements on page 17.
- The VMware Workstation installation software. If you bought the packaged distribution of VMware Workstation, the installation software is on the CD in your package. If you bought the electronic distribution, the installation software is in the file you downloaded.
- Your VMware Workstation serial number. The serial number is included in the VMware Workstation package or in the email message confirming your electronic distribution order.
- The installation CD or disks for your guest operating system.

Before Installing on a Linux Host

Before you install and run VMware Workstation, check the following notes 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 Workstation for Linux 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).

Installing the VMware Workstation Software

Note: The steps below describe an installation from a CD-ROM disc. If you downloaded the software, the steps are the same except that you start from the directory where you saved the installer file you downloaded, not from the `Linux` directory on the CD.

1. Log on to your Linux host with the user name you plan to use when running VMware Workstation.
2. In a terminal window, become root so you can perform the initial installation steps.
   ```
   su -
   ```
3. Mount the VMware Workstation CD-ROM.
4. Change to the `Linux` directory on the CD.
5. Do one of the following:
   - **Use the RPM installer:** Run RPM specifying the installation file.
     ```
     rpm -Uhv VMware-<xxx>.rpm
     ```
     (`VMware-<xxx>.rpm` is the installation file on the CD; in place of `<xxx>` the filename contains numbers that correspond to the version and build.)

     Note: If you are upgrading from VMware Workstation 3.0, you must take a special step before you install the RPM package. You need to remove the prebuilt modules RPM package included in the 3.0 release. To remove the modules, type the following at a command prompt:
     ```
     rpm -e VMwareWorkstationKernelModules
     ```
   - **Use the tar installer:** You may copy a tar archive to your hard disk and install following the directions below. Or you may skip the steps for copying and unpacking the archive and install directly from the `vmware-distrib` directory on the CD.
     Copy the tar archive to a directory on your hard drive — for example, to `/tmp`.
     ```
     cp VMware-<xxx>.tar.gz /tmp
     ```
     Change to the directory to which you copied the file.
     ```
     cd /tmp
     ```
     Unpack the archive.
     ```
     tar zxf VMware-<xxxx>.tar.gz
     ```
     Change to the installation directory.
     ```
     cd vmware-distrib
     ```
     Run the installation program.
     ```
     ./vmware-install.pl
     ```

Accept the default directories for the binary files, library files, manual files, documentation files and init script.

6. Run the configuration program.
   `vmware-config.pl`

   Note: If you use the RPM installer, you need to 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.

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

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

   The installer places `vmware-config.pl` in `/usr/bin`. If `/usr/bin` is not in your default path, run the program with the following command:
   `/usr/bin/vmware-config.pl`

7. Press Enter to read the end user license agreement (EULA). You may page through it by pressing the space bar. If the `Do you accept` prompt doesn't appear, press Q to get to the next prompt.

8. The remaining prompts are worded in such a way that, in most cases, the default response is appropriate. Some exceptions are noted here:

   - The configuration program prompts you
     `Do you want this script to automatically configure your system to allow your virtual machines to access the host's file system?`
     If you already have Samba running on your host computer, answer No.
     If Samba is not already running on your host computer and you want to add it, answer Yes to this question; the VMware Workstation installer configures it for you. When prompted for a user name and password to use with the Samba configuration, enter the user name you used in step 1 above.
   - To enable host-only networking, respond Yes to the following prompts if they appear:
     `Do you want your virtual machines to be able to use the host's network resources?`
     `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?
```

This allows for the sharing of files between the virtual machine and the host operating system. For more information, see Host-Only Networking on page 214.

Note: If you do not enable host-only networking now, you cannot allow a virtual machine to use both bridged and host-only networking.

9. 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 done, exit from the root account.
    ```
    exit
    ```

Configuring Your Web Browser

To use the VMware Workstation Help system, you must have a Web browser installed on your host computer. VMware Workstation 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
```

Uninstalling VMware Workstation 4 on a Linux Host

If you used the RPM installer to install VMware Workstation, remove the software from your system by running

```
rpm -e VMwareWorkstation
```

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

```
vmware-uninstall.pl
```

CHAPTER 3

Upgrading VMware Workstation

The following sections describe how to upgrade VMware Workstation from version 2 and 3 to version 4 on your Linux or Windows host system and how to use existing virtual machines under VMware Workstation 4:

Preparing for the Upgrade

Before You Install VMware Workstation 4

There are a few steps you should take — while your previous version of VMware Workstation is still on your computer and before you install VMware Workstation 4 — to ensure the best possible upgrade experience.

Resume and Shut Down Suspended Virtual Machines

If you plan to use virtual machines created under VMware Workstation 2, 3 or a prerelease version of VMware Workstation 4, be sure they have been shut down completely before you remove the release you used to create them.

If the virtual machine is suspended, resume it in the earlier release, shut down the guest operating system, then power off the virtual machine.

Note: If you attempt to resume a virtual machine that was suspended under a different VMware product or a different version of VMware Workstation, a dialog box gives you the choice of discarding or keeping the file that stores the suspended state. To recover the suspended state, you must click **Keep**, then 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 or undoable mode, upgrading is straightforward.

If you have an existing virtual machine with one or more virtual disks and all the disks use nonpersistent mode, you need to take a few special steps when you upgrade VMware Tools. For details, see *www.vmware.com/info?id=44*.

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 remove the release you used to create them.

Resume or power on the virtual machine in the earlier release, shut down the guest operating system, 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.

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.

Resume or power on the virtual machine in the earlier release, shut down the guest operating system, power off the virtual machine and either commit or discard changes to any undoable mode disks when prompted. Then open the configuration editor and change all disks to persistent mode. After you upgrade to VMware Workstation 4, you can use the snapshot feature to preserve the state of a virtual machine and return to that state at a later time. For more information on the snapshot feature, see Using the Snapshot on page 200.

If you need to preserve special functionality that requires disks in multiple modes, review the information at *www.vmware.com/info?id=40* 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 VMware Workstation 4. Depending on your upgrade path, you may not be able to run your virtual machines under both VMware Workstation 4 and your previous version of VMware Workstation.

Virtual machines created under Workstation 2 must have their virtual hardware updated before they can run under Workstation 4. Once they are updated, they cannot be run under Workstation 2.

You have a choice with virtual machines that you created under Workstation 3 or updated to use the Workstation 3 virtual hardware.

- You may update these virtual machines for full compatibility with Workstation 4. In that case, the virtual machines can no longer be used under Workstation 3.
- You may choose not to update the virtual hardware. In that case, you can run the virtual machines under both Workstation 3 and Workstation 4, but you will not have the benefits of the new virtual hardware provided by Workstation 4. Other Workstation 4 features will not be available. For example, you cannot take a snapshot or revert to the snapshot while the virtual machine is running; you must power off before taking or reverting to the snapshot.

When You Remove Version 2 or 3 and Install Version 4

There is a key precaution you should take when you remove VMware Workstation 2 or 3 — or a prerelease version of VMware Workstation 4 — and install VMware Workstation 4.

Leave the Existing License in Place

The installation steps for your host may require that you run an uninstaller to remove a previous version of VMware Workstation from your machine.

On a Windows host, the uninstaller may offer to remove licenses from your registry. Do not remove the licenses. You can safely keep licenses for multiple VMware products on the computer at the same time.

On a Linux host, the license remains in place. You do not need to take any special action. You may safely leave the license where it is.

Upgrading on a Windows Host

Upgrading from an Earlier Release of Version 4

The Upgrade Process

Upgrading from an earlier release of version 4 is a four-step process.

1. Use the Add or Remove Programs control panel to uninstall the version now installed on your computer.

   Note: The uninstaller may offer to remove licenses from your registry. Do not remove the licenses.

2. Reboot your computer if you are prompted to do so.
3. Install version 4.5.
4. Reboot your computer if you are prompted to do so.

Upgrading from Version 2 or 3 to Version 4

The Upgrade Process

In most cases, upgrading from version 2 or 3 is a four-step process. If you are upgrading from Workstation 2 on a Windows 2000 host that has host-only networking, there is an additional step. See Upgrading on a Windows 2000 Host with Host-Only Networking below for details.

You may upgrade from version 3 to version 4 using the VMware Workstation 4 upgrade product. To upgrade from version 2 to version 4, you must have the full VMware Workstation 4 product.

1. Uninstall the version now installed on your computer. For details, see Removing Version 2 or Removing Version 3, below.

   Note: The uninstaller may offer to remove licenses from your registry. Do not remove the licenses.

2. Reboot your computer.
3. Install version 4.

   Note: When you are upgrading with an upgrade serial number, the installer checks for the presence of a version 3 license on the computer. If it finds no version 3 license, it prompts you to enter your version 3 serial number.

4. Reboot your computer.

Removing Version 2

To uninstall version 2, use the VMware Workstation uninstaller.

1. Launch the uninstaller.
   Start > **Programs** > **VMware** > **VMware for Windows NT Uninstallation**
2. Click **Yes**.
3. Follow the on-screen instructions. You may safely keep your existing license in the Windows registry.

After you reboot, follow the instructions in Installing VMware Workstation 4 on a Windows Host on page 29.

Removing Version 3

To uninstall version 3, use the VMware Workstation uninstaller.

1. Launch the uninstaller.
   Start > **Programs** > **VMware** > **VMware Workstation Uninstallation**
2. Click **Yes**.
3. Follow the on-screen instructions. You need to keep your existing license in the Windows registry.

After you reboot, follow the instructions in Installing VMware Workstation 4 on a Windows Host on page 29.

Upgrading on a Windows 2000 Host with Host-Only Networking

If you have set up host-only networking for VMware Workstation 2 on a Windows 2000 host, the upgrade process has five steps.

1. Uninstall your host-only adapter (or adapters).
   a. On the host computer, start the Add/Remove Hardware Wizard.
      Start > **Settings** > **Control Panel** > **Add/Remove Hardware**
      Click **Next**.
   b. Select **Uninstall/Unplug a Device**. Click **Next**.
   c. Select **Uninstall a Device**. Click **Next**.
   d. Select **VMware Virtual Ethernet Adapter**, then follow the wizard's instructions.

   If you have more than one host-only adapter, repeat these steps for each of them.
2. Uninstall version 2.

Note: The uninstaller may offer to remove licenses from your registry. Do not remove the licenses.

3. Reboot your computer.
4. Install version 4.

   Note: When you are upgrading with an upgrade serial number, the installer checks for the presence of a version 3 license on the computer. If it finds no version 3 license, it prompts you to enter your version 3 serial number.

5. Reboot your computer.

You may then reconfigure host-only networking under VMware Workstation 4.

Upgrading on a Linux Host

You may upgrade from version 3 to version 4 using the VMware Workstation 4 upgrade product. To upgrade from version 2 to version 4, you must have the full VMware Workstation 4 product.

The Tar Upgrade Process

If you used the tar installer to install version 2 or 3 or an earlier release of version 4 and you plan to use the tar installer for version 4.5, you do not need to take any special steps to uninstall the older version. Just follow the installation instructions Installing VMware Workstation 4 on a Linux Host on page 36.

Note: When you are upgrading with the upgrade product, the installer checks for the presence of a version 3 license on the computer. If it finds no version 3 license, it prompts you to enter your version 3 serial number.

The RPM Upgrade Process

If you used the RPM installer to install version 2 or 3 or an earlier release of version 4, take the following steps to upgrade to version 4.5. If you are currently using version 3.0, you need to uninstall the RPM package of prebuilt modules that was installed with 3.0 before you uninstall the 3.0 software. You do not need to take this step if you are currently using version 2.0 or 3.1.

1. If you are running version 2, uninstall it as root by running

   ```
   rpm -e VMware
   ```

   If you are running version 3.0, uninstall the prebuilt modules as root, then uninstall VMware Workstation by running

   ```
   rpm -e VMwareWorkstationKernelModules
   rpm -e VMwareWorkstation
   ```

   If you are running version 3.1 or 3.2 or an earlier release of version 4, uninstall it as root by running

   ```
   rpm -e VMwareWorkstation*
   ```

2. Install version 4.5 following the instructions in Installing VMware Workstation 4 on a Linux Host on page 36.

   Note: When you are upgrading with the upgrade product, the installer checks for the presence of a version 3 license on the computer. If it finds no version 3 license, it prompts you to enter your version 3 serial number.

Using Virtual Machines Created with Version 3 under Version 4

There are, broadly speaking, three approaches you can take to setting up virtual machines under VMware Workstation 4. Choose one of these approaches.

- Create Everything New from the Start on page 49
- Use an Existing Configuration File and Virtual Disk on page 49
- Use an Existing Virtual Machine and Upgrade the Virtual Hardware on page 50

Create Everything New from the Start

Use the New Virtual Machine Wizard to set up a new virtual machine and install a guest operating system in the virtual machine as described in Creating a New Virtual Machine on page 65. If you set up your virtual machines in this way, you will be using the latest technology and will enjoy the performance benefits of the new virtual hardware.

Use an Existing Configuration File and Virtual Disk

Upgrade VMware Tools to the new version following the instructions for your guest operating system in Installing VMware Tools on page 81. You should not remove the older version of VMware Tools before installing the new version.

A virtual machine set up in this way should run without problems. However, you will not have the benefits of certain new features, including improved sound quality, support for taking a snapshot while the virtual machine is running and improved virtual disk formats.

Note: The first time you power on the virtual machine under VMware Workstation 4, Workstation updates the CMOS. As a result, your guest operating system may detect hardware changes and install new drivers for the new hardware even if you do not choose **VM** > **Upgrade Virtual Hardware**. Similarly, if you switch back to VMware Workstation 3, your guest operating system may detect hardware changes and install the appropriate drivers. You should expect to see this behavior each time you switch from one version of VMware Workstation to the other.

Windows hosts: At the time you install VMware Workstation 4, the installer offers to convert virtual disk `.dsk` filenames to use the `.vmdk` extension introduced with version 3. If you still have virtual disks using the `.dsk` extension and if you are storing virtual disk files on a Windows XP or Windows Server 2003 host, it is especially important that you allow VMware Workstation to make this change in order to avoid

conflicts with the Windows XP or Windows Server 2003 System Restore feature. The `.vmdk` extension can be used for virtual disks under any VMware product. VMware Workstation 4 automatically updates references to the virtual disk files in configuration files on the host computer. If you are using the same virtual disk file from any other computer, you need to update the configuration files with the new filename. For details, see Updating Filenames for Virtual Disks Created with Earlier VMware Products on page 151.

Linux hosts: The first time you run a virtual machine after installing VMware Workstation 4, Workstation offers to convert virtual disk `.dsk` filenames to use the `.vmdk` extension introduced with version 3. If you still have virtual disks using the `.dsk` extension and if you are storing virtual disk files on a Windows XP or Windows Server 2003 host, it is especially important that you allow VMware Workstation to make this change in order to avoid conflicts with the Windows XP or Windows Server 2003 System Restore feature. The `.vmdk` extension can be used for virtual disks under any VMware product. VMware Workstation 4 automatically updates references to the virtual disk files in configuration files on the host computer. If you are using the same virtual disk file from any other computer, you need to update the configuration files with the new filename. For details, see Updating Filenames for Virtual Disks Created with Earlier VMware Products on page 151.

Use an Existing Virtual Machine and Upgrade the Virtual Hardware

If you use an existing virtual machine and upgrade the virtual hardware, you gain access to new features and enjoy the performance benefits of the new virtual hardware, but the process is one-way — you cannot reverse it.

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

Power on the virtual machine and upgrade VMware Tools to the new version, following the instructions for your guest operating system in Installing VMware Tools on page 81. You should not remove the older version of VMware Tools before installing the new version.

After shutting down the guest operating system and powering off the virtual machine, upgrade the virtual hardware. The upgraded virtual hardware gives you improved sound quality, support for taking a snapshot while the virtual machine is running and improved virtual disk formats.

Note: If you are upgrading a virtual machine that runs from a physical disk, rather than a virtual disk, you may see the following error message while VMware Workstation is upgrading the virtual hardware: "Unable to upgrade <drivename>. One

of the supplied parameters is invalid." You may safely click **OK** to continue the upgrade process.

Note: When you update the virtual hardware in a Windows XP or Windows Server 2003 virtual machine, the Microsoft product activation feature requires you to reactivate the guest operating system.

Windows hosts: At the time you install VMware Workstation 4, the installer offers to convert virtual disk `.dsk` filenames to use the `.vmdk` extension introduced with version 3. If you still have virtual disks using the `.dsk` extension and if you are storing virtual disk files on a Windows XP or Windows Server 2003 host, it is especially important that you allow VMware Workstation to make this change in order to avoid conflicts with the Windows XP or Windows Server 2003 System Restore feature. The `.vmdk` extension can be used for virtual disks under any VMware product. VMware Workstation 4 automatically updates references to the virtual disk files in configuration files on the host computer. If you are using the same virtual disk file from any other computer, you need to update the configuration files with the new filename. For details, see Updating Filenames for Virtual Disks Created with Earlier VMware Products on page 151.

Linux hosts: The first time you run a virtual machine after installing VMware Workstation 4, Workstation offers to convert virtual disk `.dsk` filenames to use the `.vmdk` extension introduced with version 3. If you still have virtual disks using the `.dsk` extension and if you are storing virtual disk files on a Windows XP or Windows Server 2003 host, it is especially important that you allow VMware Workstation to make this change in order to avoid conflicts with the Windows XP or Windows Server 2003 System Restore feature. The `.vmdk` extension can be used for virtual disks under any VMware product. VMware Workstation 4 automatically updates references to the virtual disk files in configuration files on the host computer. If you are using the same virtual disk file from any other computer, you need to update the configuration files with the new filename. For details, see Updating Filenames for Virtual Disks Created with Earlier VMware Products on page 151.

Upgrading Virtual Hardware in the Guest Operating System

If you are using a virtual machine created under VMware Workstation 3, the first time you power on the virtual machine under VMware Workstation 4, Workstation updates the CMOS. As a result, your guest operating system may detect hardware changes and install new drivers for the new hardware even if you do not choose **VM** > **Upgrade Virtual Hardware**.

Windows 95 and Windows 98 guests: The first time you run a VMware Workstation 3 virtual machine under VMware Workstation 4, the guest operating system discovers

new hardware and attempts to install drivers for it before it loads the CD-ROM driver. As a result, it is unable to load drivers from the operating system installation CD. In many cases, the drivers are already available in `C:\Windows`, `C:\Windows\System` or subdirectories under those two directories. However, a simpler approach is to skip any files that Windows does not find at this stage. Then, after the guest operating system has finished loading and is able to read from the CD-ROM, you can run the guest operating system's Add Hardware Wizard and allow it to detect new hardware and install the appropriate drivers.

You need to install the new version of VMware Tools. If you have decided to upgrade the virtual hardware, do that after you finish installing VMware Tools.

Note: If you are upgrading a virtual machine that runs from a physical disk, rather than a virtual disk, you may see the following error message while VMware Workstation is upgrading the virtual hardware: "Unable to upgrade <drivename>. One of the supplied parameters is invalid." You may safely click **OK** to continue the upgrade process.

If you upgrade the virtual hardware, you may then need to take several steps to be sure 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 may need to take to perform these updates.

Windows XP Guest

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

1. Power on the virtual machine and let it update the CMOS.
2. Install the new version of VMware Tools. For details, see Installing VMware Tools on page 81.
3. Shut down Windows and power off the virtual machine.
4. Choose **VM** > **Upgrade Virtual Hardware**.
5. A dialog box cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding. If you are ready to proceed, click **Yes**.
6. A dialog box displays a message describing what is about to happen. Click **OK** to continue.
7. Power on the virtual machine.

8. Windows detects the VMware SVGA adapter. Select **Install the software automatically** and follow the on-screen instructions.
9. A dialog box asks you to insert a disk. 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.
12. Windows detects the COM ports and installs them properly.

Windows Me Guest

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

1. Power on the virtual machine and let it update the CMOS.
2. Plug and Play detects an Intel 82371 EB Power Management controller. Select **Automatic search** and click **Next**. Windows finds and installs the driver automatically.
3. Plug and Play detects an Intel 82443 BX Pentium II Processor to PCI bridge. Select **Automatic search** and click **Next**. Windows finds and installs the driver automatically.
4. Restart the guest operating system.
5. Plug and Play detects an Intel 82371 AB/EB PCI Bus Master IDE controller. Select **Automatic search** and click **Next**. Windows finds and install the driver automatically.
6. Install the new version of VMware Tools. For details, see Installing VMware Tools on page 81.
7. Shut down Windows and power off the virtual machine.
8. Choose **VM** > **Upgrade Virtual Hardware**.
9. A dialog box cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding. If you are ready to proceed, click **Yes**.
10. A dialog box displays a message describing what is about to happen. Click **OK** to continue.
11. Power on the virtual machine.

12. Windows detects the PCI Multimedia Audio device and installs the driver for the Creative AudioPCI.
13. Windows detects an AMD PCNet adapter. Select **Automatic search** and click **Next**. Windows automatically installs the driver for the adapter.
14. Click **Finish** to restart the virtual machine.
15. Windows detects a Creative game port device and installs the driver automatically.
16. Windows detects a game port joystick and installs the driver automatically.
17. Windows detects the PCI SVGA adapter, then it detects the VMware SVGA II adapter and installs the driver automatically.
18. Click **Yes** to restart the virtual machine.
19. If you have serial ports configured in the virtual machine, go to the Windows Device Manager and uninstall all the COM ports listed there.
20. Restart the virtual machine.
21. Windows detects the COM ports and installs them properly.

Windows 2000 Guest

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

1. Power on the virtual machine and let it update the CMOS.
2. Windows automatically installs the software for any devices it detects.
3. Install the new version of VMware Tools. For details, see Installing VMware Tools on page 81.
4. Shut down Windows and power off the virtual machine.
5. Choose **VM** > **Upgrade Virtual Hardware**.
6. A dialog box cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding. If you are ready to proceed, click **Yes**.
7. A dialog box displays a message describing what is about to happen. Click **OK** to continue.
8. Power on the virtual machine.
9. Windows detects the PCI SVGA adapter, then it detects the VMware SVGA II adapter. Click **Yes** to continue installation.

10. A dialog box asks you to insert a disk. Navigate to `C:\Program Files\VMware\drivers` to install the VMware SVGA II adapter.
11. If you have serial ports configured in the virtual machine, go to the Windows Device Manager and uninstall all the COM ports listed there.
12. Restart the virtual machine.
13. Windows detects the COM ports and installs them properly.

Windows NT 4.0 Guest

1. Power on the virtual machine and let it update the CMOS.
2. Windows displays a message about the video driver in the guest operating system. Click **OK**.
3. Install the new version of VMware Tools. For details, see Installing VMware Tools on page 81.
4. Restart Windows and confirm that it is operating correctly.
5. Shut down Windows and power off the virtual machine.
6. Choose **VM** > **Upgrade Virtual Hardware**.
7. A dialog box cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding. If you are ready to proceed, click **Yes**.
8. A dialog box displays a message describing what is about to happen. Click **OK** to continue.
9. 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 98 Guest

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

1. Power on the virtual machine and let it update the CMOS.
2. Windows detects an Intel 82371EB Power Management Controller. Go to `C:\Windows\System` for the necessary file.
3. Windows detects `lpt.vxd`. Go to `C:\Windows\System` for the necessary file.

4. Windows detects an Intel 82443BX Pentium Processor to PCI bridge. Go to `C:\Windows\System` for the necessary file.
5. Windows detects an Intel 82371AB/EB PCI Bus Master IDE controller. Go to `C:\Windows\System` for the necessary file.
6. Windows detects an Intel 82371AB/EB PCI to USB Universal host controller. Go to `C:\Windows\System` for the necessary file.
7. Windows detects an AMD PCNET Family Ethernet Adapter. Go to `C:\Windows\System` for the necessary file.
8. Windows asks for the file `uhcd.sys`. Enter the location `C:\Windows\System32\drivers`, then click **OK**.
9. Windows asks for the file `inetmib1.dll`. Enter the location `C:\Windows`, then click **OK**.
10. Windows asks for the file `locproxy.exe`. Enter the location `C:\Windows\System`, then click **OK**.
11. Windows asks for the file `ndishlp.sys`. Enter the location `C:\Windows`, then click **OK**.
12. Windows asks for the file `wsock.vxd`. Enter the location `C:\Windows\System`, then click **OK**.
13. When you finish installing the AMD Family Ethernet Adapter, restart Windows 98.
14. 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 on page 81.
16. Shut down Windows and power off the virtual machine.
17. Choose **VM** > **Upgrade Virtual Hardware**.
18. A dialog box cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding. If you are ready to proceed, click **Yes**.
19. A dialog box displays a message describing what is about to happen. 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 for it automatically.
21. Windows detects PCI Multimedia Audio and offers to install a driver for it. Click **Cancel**.

22. Windows detects an AMD PCNET Family Ethernet adapter. Click **Next**.
23. Select **Search for the best driver** and click **Next**.
24. Select **Specify a location**, enter `C:\Windows\System` and click **Next**.
25. Select **The updated driver (Recommended) AMD PCNET Family Ethernet Adapter (PCI-ISA)**. Click **Next**.
26. Windows finds the `.inf` file for the adapter. Click **Next**.
27. Windows asks for the file `dhcpsvc.dll`. Enter the location `C:\Windows\System`, then click **OK**.
28. Windows asks for the file `inetmib1.dll`. Enter the location `C:\Windows`, then click **OK**.
29. Windows asks for the file `locproxy.exe`. Enter the location `C:\Windows\System`, then click **OK**.
30. Windows asks for the file `ndishlp.sys`. Enter the location `C:\Windows`, then click **OK**.
31. Windows asks for the file `wshtcp.vxd`. Enter the location `C:\Windows\System`, then click **OK**.
32. A dialog box indicates that Windows has finished installing the software. Click **Finish**.
33. To install the sound adapter, follow the directions in Installing Sound Drivers in Windows 9x and Windows NT Guest Operating Systems on page 269.
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.
36. Windows detects the COM ports and installs them properly.

Windows 95 Guest

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

1. Power on the virtual machine and let it update the CMOS.
2. Windows detects new devices and automatically installs the drivers. Restart the guest operating system after this process is complete.
3. When Windows restarts, it detects more new devices.

4. Windows asks for the file `lpt.vxd`. Enter the location `C:\Windows\System`, then click **OK**.
5. Windows detects a PCI standard host bridge and other devices. Click **OK** to dismiss these dialog boxes. You do not need to install these drivers.
6. Click **Finish**.
7. Install the new version of VMware Tools. For details, see Installing VMware Tools on page 81.
8. Shut down Windows and power off the virtual machine.
9. Choose **VM** > **Upgrade Virtual Hardware**.
10. A dialog box cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding. If you are ready to proceed, click **Yes**.
11. A dialog box displays a message describing what is about to happen. Click **OK** to continue.
12. Windows detects a PCI Multimedia Audio device. Click **Cancel**.
13. Windows detects a PCI Ethernet adapter, then the AMD Ethernet adapter. Windows automatically installs the driver.
14. To install the sound adapter, follow the directions in Installing Sound Drivers in Windows 9x and Windows NT Guest Operating Systems on page 269.
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.
17. Windows detects the COM ports and installs them properly.

Red Hat 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 Linux and power off the virtual machine.
4. Choose **VM** > **Upgrade Virtual Hardware**.
5. A dialog box cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding. If you are ready to proceed, click **Yes**.

6. A dialog box displays a message describing what is about to happen. Click **OK** to continue.
7. Power on the virtual machine.
8. When Kudzu runs, it detects an Ensoniq:ES1371 [AudioPCI-97] sound device.
9. Click **Configure**.

Mandrake 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 Linux and power off the virtual machine.
4. Choose **VM** > **Upgrade Virtual Hardware**.
5. A dialog box cautions you that the operation is irreversible and recommends that you back up the virtual disks before proceeding. If you are ready to proceed, click **Yes**.
6. A dialog box displays a message describing what is about to happen. Click **OK** to continue.
7. Power on the virtual machine.
8. When Kudzu runs, it detects an Ensoniq:ES1371 [AudioPCI-97] sound device.
9. Click **Configure**.

   Note: When using Kudzu, 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.

Upgrading the Virtual Hardware in an Existing Virtual Machine

On the **VM** menu, choose **Upgrade Virtual Hardware**. A dialog box appears, warning that the upgrade process cannot be reversed. Click **Yes** to continue, then follow the on-screen directions.

Note: If you are upgrading a virtual machine that runs from a physical disk, rather than a virtual disk, you may see the following error message while VMware Workstation is upgrading the virtual hardware: "Unable to upgrade <drivename>. One of the supplied parameters is invalid." You may safely click **OK** to continue the upgrade process.

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 Workstation 2 or 3. You should make backup copies of your virtual disks before starting the upgrade.

Using Virtual Machines Created with Version 2 under Version 4

If you use an existing VMware Workstation 2 virtual machine under VMware Workstation 4, the virtual hardware is upgraded automatically. The upgrade gives you access to new features, but the process is one-way — you cannot reverse it.

Start by using an existing configuration file (`.vmx`) and virtual disk (`.dsk` if you do not convert to new filenames when you install VMware Workstation or `.vmdk` if you do convert).

The first time you power on the virtual machine under Workstation 4, a dialog box appears, offering the choice of upgrading the virtual hardware or powering off. If you want to make a backup copy of the virtual machine before upgrading the virtual hardware, power off and make the backup. Otherwise, allow VMware Workstation to upgrade the virtual hardware.

Note: If you are upgrading a virtual machine that runs from a physical disk, rather than a virtual disk, you may see the following error message while VMware Workstation is upgrading the virtual hardware: "Unable to upgrade <drivename>. One of the supplied parameters is invalid." You may safely click **OK** to continue the upgrade process.

Upgrade VMware Tools to the new version following the instructions for your guest operating system in Installing VMware Tools on page 81. You should not remove the older version of VMware Tools before installing the new version.

Upgrading Virtual Hardware in the Guest Operating System

After upgrading the virtual hardware, you may need to take several steps to be sure the new virtual hardware is recognized properly by the guest operating system. If you are using a Windows 95, Windows 98 or Windows Me virtual machine created under VMware Workstation 2, take the steps listed under the name of your guest operating system.

With other guest operating systems, these special steps are not needed. Plug and Play should recognize the new virtual hardware and install any needed drivers smoothly.

Windows Me Guest

1. Power on the virtual machine.
2. Allow Workstation to upgrade the virtual hardware.
3. Click **OK** to dismiss the message "A legacy SVGA driver has been detected."

4. Several Plug and Play messages appear. You can safely ignore them.
5. Log on to Windows Me. More Plug and Play messages appear. One refers to the VMware SVGA driver.

   Click **Yes** to restart your computer.
6. Log on to Windows Me. The SVGA driver is not working properly.
7. From the Windows **Start** menu, choose **Settings** > **Control Panel** > **System** > **Device Manager** > **Display Adapters**.

   Manually remove the two SVGA drivers.
8. Restart Windows Me.

   A VMware SVGA II adapter is detected and Windows installs it.

   Windows notifies you to restart your computer.

   Click **Yes**.
9. The SVGA driver should be working correctly.
10. Install the new version of VMware Tools. See Installing VMware Tools on page 81 for details.

Windows 98 Guest

1. Power on the virtual machine.
2. Allow Workstation to upgrade the virtual hardware.
3. Click **OK** to dismiss the message "A legacy SVGA driver has been detected."
4. Log on to Windows 98. You see a number of Plug and Play messages. You may need to insert your Windows 98 installation CD.
5. A blue screen appears. Press any key to dismiss the blue screen.
6. Click **Reset** to restart the virtual machine (because it is not responding).
7. Click **OK** to dismiss the message "A legacy SVGA driver has been detected."

   Again, you see a number of Plug and Play messages.

   Windows notifies you to restart Windows.

   Click **Yes**.
8. Log on to Windows 98. The SVGA driver is not working properly.
9. From the Windows **Start** menu, choose **Settings** > **Control Panel** > **System** > **Device Manager** > **Display Adapters**.

   Manually remove the two conflicting SVGA drivers.

10. Restart Windows 98.

    A VMware SVGA II adapter is detected and Windows installs it.

11. Restart Windows 98.
12. The SVGA driver should be working correctly.
13. Install the new version of VMware Tools. See Installing VMware Tools on page 81 for details.

Windows 95 Guest

1. Power on the virtual machine.
2. Allow Workstation to upgrade the virtual hardware.
3. Click **OK** to dismiss the message "A legacy SVGA driver has been detected."
4. Log on to Windows 95.

   You see a number of Plug and Play messages. Click **Cancel** for those listing the following devices: Standard host CPU bridge, PCI bridge and PCI Universal bus.

5. The SVGA driver is not working properly.
6. From the Windows **Start** menu, choose **Settings** > **Control Panel** > **System** > **Device Manager** > **Display Adapters**.

   Manually remove the SVGA driver.

7. Restart Windows 95.
8. Again, you see a number of Plug and Play messages. Click **Cancel** for those listing the following devices: Standard host CPU bridge, PCI bridge and PCI Universal bus.
9. A VMware SVGA II adapter is detected and Windows installs it.
10. Restart Windows 95.
11. Once again, you see a number of Plug and Play messages. Again, click **Cancel** for those listing the following devices: Standard host CPU bridge, PCI bridge and PCI Universal bus.
12. The SVGA driver should be working correctly.
13. Install the new version of VMware Tools. See Installing VMware Tools on page 81 for details.

Check Windows 2000 Guest Operating System Selection

If your guest operating system is Windows 2000, update the setting in the virtual machine settings editor (**VM** > **Settings** > **Options**) to reflect the specific version of Windows 2000 you are running.

CHAPTER 4

Creating a New Virtual Machine

The following sections describe how to create a new virtual machine and install VMware Tools:

Setting Up a New Virtual Machine

The New Virtual Machine Wizard guides you through the key steps for setting up a new virtual machine, helping you set various options and parameters. You can then use the virtual machine settings editor (**VM** > **Settings**) if you need to make any changes to your virtual machine's setup.

What's in a Virtual Machine?

The virtual machine typically is stored on the host computer in a set of files, all of which are in a directory set aside for that particular virtual machine. In these examples, `<vmname>` is the name of your virtual machine. The key files are:

- `<vmname>.vmx` — the configuration file, which stores settings chosen in the New Virtual Machine Wizard or virtual machine settings editor. If you created the virtual machine under an earlier version of VMware Workstation on a Linux host, this file may have a `.cfg` extension.
- `nvram` — the file that stores the state of the virtual machine's BIOS.
- `<vmname>.vmdk` — the virtual disk file, which stores the contents of the virtual machine's hard disk drive.

  A virtual disk is made up of one or more `.vmdk` files. If you have specified that the virtual disk should be split into 2GB chunks, the number of `.vmdk` files depends on the size of the virtual disk. As data is added to a virtual disk, the `.vmdk` files grow in size, to a maximum of 2GB each. (If you specify that all space should be allocated when you create the disk, these files start at the maximum size and do not grow.) Almost all of a `.vmdk` file's content is the virtual machine's data, with a small portion allotted to virtual machine overhead.

  If the virtual machine is connected directly to a physical disk, rather than to a virtual disk, the `.vmdk` file stores information about the partitions the virtual machine is allowed to access.

  Note: Earlier VMware products used the extension `.dsk` for virtual disk files.
- `<vmname>.log` or `vmware.log` — the file that keeps a log of key VMware Workstation activity. This file can be useful in troubleshooting if you encounter problems. This file is stored in the directory that holds the configuration (`.vmx` or `.cfg`) file of the virtual machine.
- `<vmname>.vmdk.REDO_xxxxxx` — a redo-log file, created automatically when a virtual machine has a snapshot. This file stores changes made to a virtual disk while the virtual machine is running. There may be more than one such file.

The `xxxxxx` indicates a unique suffix added automatically by VMware Workstation to avoid duplicate file names.

- `<vmname>.vmss` — the suspended state file, which stores the state of a suspended virtual machine.

  Note: Some earlier VMware products used the extension `.std` for suspended state files.

- `<vmname>.vmsn` — the snapshot state file, which stores the running state of a virtual machine at the time you take a snapshot of it.
- `<vmname>.vmx.sav` or `<vmname>.cfg.sav` — the configuration snapshot file, which stores the configuration of a virtual machine at the time you take a snapshot of it.

There may be other files as well, some of which are present only while a virtual machine is running.

Simple Steps to a New Virtual Machine

By default, the new virtual machine uses an IDE disk for Windows 95, Windows 98, Windows Me, Windows XP, Windows Server 2003, NetWare and FreeBSD guests. The default for other guest operating systems is a SCSI disk.

Follow these steps to create a virtual machine using a virtual disk.

1. Start VMware Workstation.

   Windows hosts: Double-click the VMware Workstation icon on your desktop or use the **Start** menu (**Start** > **Programs** > **VMware** > **VMware Workstation**).

   Linux hosts: In a terminal window, enter the command

   ```
   vmware &
   ```

2. If this is the first time you have launched VMware Workstation and you did not enter the serial number when you installed the product (an option available on a Windows host), you are prompted to enter it. The serial number is on the registration card in your package or in the email message confirming your electronic distribution order. Enter your serial number and click **OK**.

   The serial number you enter is saved and VMware Workstation does not ask you for it again. For your convenience, VMware Workstation automatically sends the serial number to the VMware Web site when you use certain Web links built into the product (for example, **Help** > **VMware on the Web** > **Register Now!** and **Help** > **VMware on the Web** > **Request Support**). This allows us to direct you to the correct Web page to register and get support for your product.

3. **Linux hosts:** If this is the first time you have launched VMware Workstation, a dialog box asks if you want to rename existing virtual disks using the new `.vmdk` extension. Click **OK** to search all local drives on the host computer and make this change. (On Windows hosts, you have a chance to rename virtual disk files when you are installing VMware Workstation.)

   The converter also renames the files that store the state of a suspended virtual machine, if it finds them. It changes the old `.std` file extension to `.vmss`. However, you should resume and shut down all suspended virtual machines before you upgrade to Workstation 4.

   In addition to renaming files, the converter updates the corresponding virtual machine configuration files so they identify the virtual disks using the new filenames.

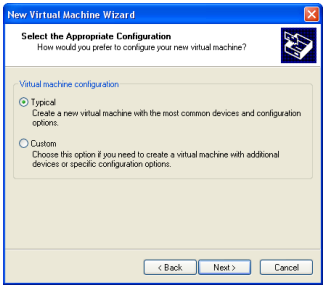
   If you store your virtual disk files or suspended state files on a Windows XP or Windows Server 2003 host — or if you may do so in the future — it is important to convert the filenames to avoid conflicts with the System Restore feature of Windows XP and Windows Server 2003.

4. Start the New Virtual Machine Wizard.

   When you start VMware Workstation, you can open an existing virtual machine or create a new one. Choose **File** > **New Virtual Machine** to begin creating your virtual machine.

5. The New Virtual Machine Wizard presents you with a series of screens that you navigate using the Next and Prev buttons at the bottom of each screen. At each screen, follow the instructions, then click **Next** to proceed to the next screen.

6. Select the method you want to use for configuring your virtual machine.



   If you select **Typical**, the wizard prompts you to specify or accept defaults for

   - The guest operating system
   - The virtual machine name and the location of the virtual machine's files

Linux Hosts: One Chance to Rename Disk Files

- The Rename Virtual Disks dialog box appears only once. If you click Cancel, you will not have another opportunity to update the filenames and configuration files automatically.

- The network connection type

If you select **Custom**, you also can specify how to set up your disk — create a new virtual disk, use an existing virtual disk or use a physical disk — and specify the settings needed for the type of disk you select.

Select **Custom** if you want to

- Make a virtual disk larger or smaller than 4GB
- Store your virtual disk's files in a particular location
- Use an IDE virtual disk for a guest operating system that would otherwise have a SCSI virtual disk created by default
- Allocate all the space for a virtual disk at the time you create it
- Choose whether to split a virtual disk into 2GB files
- Use a physical disk rather than a virtual disk (for expert users)
- Set memory options that are different from the defaults

7. Select a guest operating system.

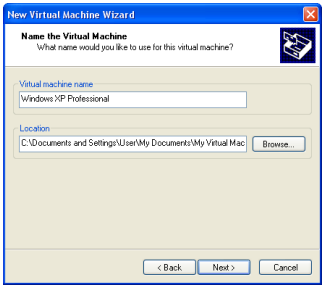
This screen asks which operating system you plan to install in the virtual machine. Select both an operating system and a version.

The New Virtual Machine Wizard uses this information to select appropriate default values, such as the amount of memory needed. The wizard also uses this information when naming associated virtual machine files.

If the operating system you plan to use is not listed, select **Other** for both guest operating system and version.

The remaining steps assume you plan to install a Windows XP Professional guest operating system. You can find detailed installation notes for this and other guest operating systems in the *VMware Guest Operating System Installation Guide*, available from the VMware Web site or from the Help menu.

8. Select a name and folder for the virtual machine.



The name specified here is used if you add this virtual machine to the VMware Workstation Favorites list. This name is also used as the name of the folder where the files associated with this virtual machine are stored.

Each virtual machine should have its own folder. All associated files, such as the configuration file and the disk file, are placed in this folder.

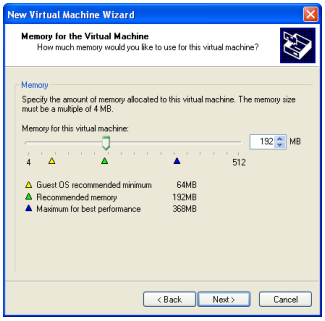
Windows hosts: On Windows 2000, Windows XP and Windows Server 2003, the default folder for this Windows XP Professional virtual machine is `C:\Documents and Settings\<username>\My Documents\My Virtual Machines\Windows XP Professional`. On Windows NT, the default folder is `C:\WINNT\Profiles\<username>\Personal\My Virtual Machines\Windows XP Professional`.

Linux hosts: The default location for this Windows XP Professional virtual machine is `<homedir>/vmware/winXPPro`, where `<homedir>` is the home directory of the user who is currently logged on.

Virtual machine performance may be slower if your virtual hard disk is on a network drive. For best performance, be sure the virtual machine's folder is on a local drive. However, if other users need to access this virtual machine, you should consider placing the virtual machine files in a location that is accessible to them. For more information, see Sharing Virtual Machines with Other Users on page 144.

9. If you selected **Typical** as your configuration path, skip to step 10.

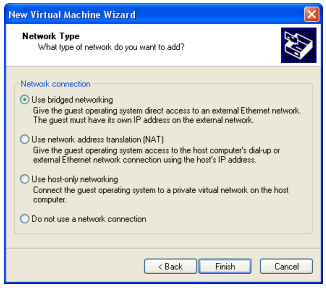
If you selected **Custom** as your configuration path, you may adjust the memory settings or accept the defaults, then click **Next** to continue.



In most cases, it is best to keep the default memory setting. If you plan to use the virtual machine to run many applications or applications that need high amounts of memory, you may want to use a higher memory setting. For more information, see Virtual Machine Memory Size on page 317.

Note: You cannot allocate more than 2GB of memory to a virtual machine if the virtual machine's files are stored on a file system such as FAT32 that does not support files greater than 2GB.

10. Configure the networking capabilities of the virtual machine.



If your host computer is on a network and you have a separate IP address for your virtual machine (or can get one automatically from a DHCP server), select **Use bridged networking**.

If you do not have a separate IP address for your virtual machine but you want to be able to connect to the Internet, select **Use network address translation (NAT)**. NAT is useful if you have a wireless network adapter on a Linux host (as bridged networking on wireless network adapters is supported only on

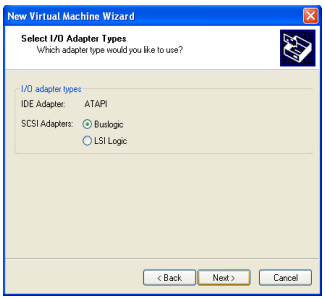
Windows hosts). NAT also allows you to share files between the virtual machine and the host operating system.

For more details about VMware Workstation networking options, see Configuring a Virtual Network on page 207.

11. If you selected **Typical** as your configuration path, click **Finish** and the wizard sets up the files needed for your virtual machine.

    If you selected **Custom** as your configuration path, continue with the steps below to configure a disk for your virtual machine.

12. Select the type of SCSI adapter you want to use with the virtual machine.

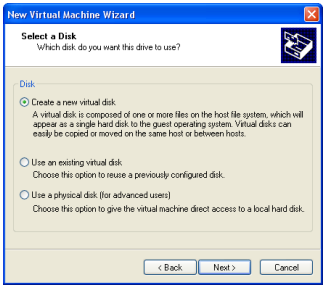


An IDE and a SCSI adapter are installed in the virtual machine. The IDE adapter is always ATAPI. You can choose a BusLogic or an LSI Logic SCSI adapter. The default for your guest operating system is already selected. All guests except for Windows Server 2003, Red Hat Enterprise Linux 3 and NetWare default to the BusLogic adapter.

The LSI Logic adapter has improved performance and works better with generic SCSI devices. The LSI Logic adapter is also supported by ESX Server 2 virtual machines, but not by virtual machines created with lower versions. Keep this in mind if you plan to migrate the virtual machine to another VMware product.

Your choice of SCSI adapter does not affect your decision to make your virtual disk an IDE or SCSI disk. However, most guest operating systems do not include a driver for the LSI Logic adapter; you must download the driver from the LSI Logic Web site. See the *VMware Guest Operating System Installation Guide* for details about the driver and the guest operating system you plan to install in this virtual machine.

13. Select the disk you want to use with the virtual machine.



Select **Create a new virtual disk**.

Virtual disks are the best choice for most virtual machines. They are quick and easy to set up and can be moved to new locations on the same host computer or to different host computers. By default, virtual disks start as small files on the host computer's hard drive, then expand as needed — up to the size you specify in the next step. The next step also allows you to allocate all the disk space when the virtual disk is created, if you wish.

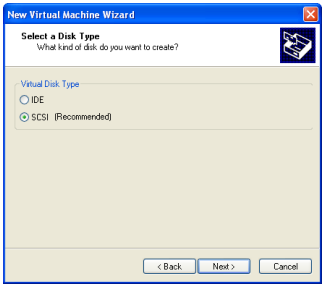
To use an existing operating system on a physical hard disk (a "raw" disk), read Configuring a Dual-Boot Computer for Use with a Virtual Machine on page 169. To install your guest operating system directly on an existing IDE disk partition, read the reference note Installing an Operating System onto a Raw Partition from a Virtual Machine on page 190.

Caution: Raw disk configurations are recommended only for expert users.

Caution: If you are using a Windows Server 2003, Windows XP or Windows 2000 host, see Do Not Use Windows 2000, Windows XP and Windows Server 2003 Dynamic Disks as Raw Disks on page 184.

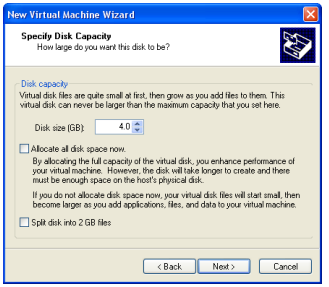
To install the guest operating system on a raw IDE disk, select **Existing IDE Disk Partition**. To use a raw SCSI disk, add it to the virtual machine later with the virtual machine settings editor. Booting from a raw SCSI disk is not supported. For a discussion of some of the issues involved in using a raw SCSI disk, see Configuring Dual- or Multiple-Boot SCSI Systems to Run with VMware Workstation on a Linux Host on page 184.

14. Select whether to create an IDE or SCSI disk.



The wizard recommends the best choice based on the guest operating system you selected. All Linux distributions you can select in the wizard use SCSI virtual disks by default, as do Windows NT, Windows 2000, Windows Server 2003 and Longhorn. All Windows operating systems except Windows NT, Windows 2000, Windows Server 2003 and Longhorn use IDE virtual disks by default; NetWare, FreeBSD, MS-DOS and other guests default to IDE virtual disks.

15. Specify the capacity of the virtual disk.



Enter the size of the virtual disk that you wish to create.

If you wish, select **Allocate all disk space now**.

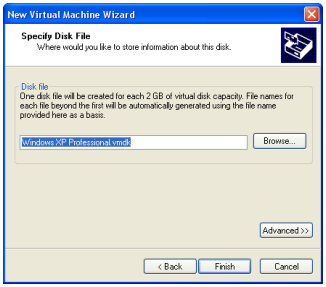
Allocating all the space at the time you create the virtual disk gives somewhat better performance, but it requires as much disk space as the size you specify for the virtual disk.

If you do not select this option, the virtual disk's files start small and grow as needed, but they can never grow larger than the size you set here.

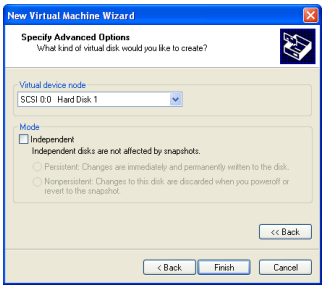
You can set a size between 0.1GB and 256GB for a SCSI virtual disk or 128GB for an IDE virtual disk. The default is 4GB.

You may also specify whether you want the virtual disk created as one large file or split into a set of 2GB files. You should split your virtual disk if it is stored on a FAT32 file system.

16. Specify the location of the virtual disk's files.



If you want to specify which device node should be used by your SCSI or IDE virtual disk, click **Advanced**.



On the advanced settings screen, you can also specify a disk mode. This is useful in certain special-purpose configurations in which you want to exclude disks from the snapshot. For more information on the snapshot feature, see Using the Snapshot on page 200.

Normal disks are included in the snapshot. In most cases, you should use normal disks, leaving **Independent** unchecked.

Independent disks are not included in the snapshot.

Caution: The independent disk option should be used only by advanced users who need it for special-purpose configurations.

You have the following options for an independent disk:

- **Persistent** — changes are immediately and permanently written to the disk.

- **Nonpersistent** — changes to the disk are discarded when you power off the virtual machine.

When you have set the filename and location you want to use and have made any selections you want to make on the advanced settings screen, click **Finish**.

17. Click **Finish**. The wizard sets up the files needed for your virtual machine.

Installing a Guest Operating System and VMware Tools

A new virtual machine is like a physical computer with a blank hard disk. Before you can use it, you need to partition and format the virtual disk and install an operating system. The operating system's installation program may handle the partitioning and formatting steps for you.

Installing a guest operating system inside your VMware Workstation virtual machine is essentially the same as installing it on a physical computer. The basic steps for a typical operating system are:

1. Start VMware Workstation.
2. Insert the installation CD-ROM or floppy disk for your guest operating system.

   Note: In some host configurations, the virtual machine is not able to boot from the installation CD-ROM. You can work around that problem by creating an ISO image file from the installation CD-ROM. Use the virtual machine settings editor to connect the virtual machine's CD drive to the ISO image file, then power on the virtual machine.
3. Power on your virtual machine by clicking the **Power On** button.
4. Follow the instructions provided by the operating system vendor.

The next section provides notes on installing a Windows XP guest operating system. The screen shots illustrate the process on a Windows host. The steps are the same on a Linux host.

For information on installing other guest operating systems, see the *VMware Guest Operating System Installation Guide*, available from the VMware Web site or from the Help menu.

Installing Windows XP as a Guest Operating System

You can install Windows XP Home Edition or Windows XP Professional in a virtual machine using the full installation CD.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the New Virtual Machine Wizard.

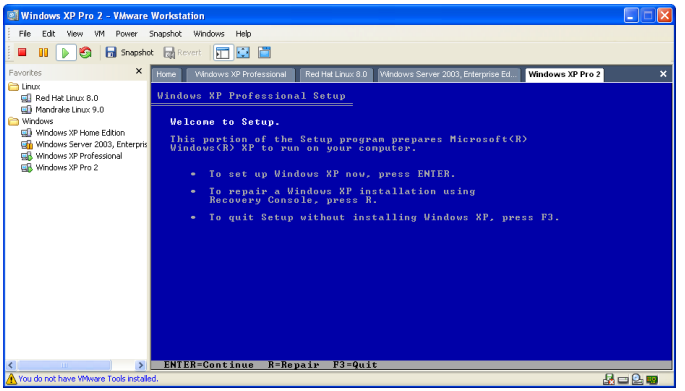
Note: To use SCSI disks in a Windows XP virtual machine, you need a special SCSI driver available from the download section of the VMware Web site at*www.vmware.com/download*. Follow the instructions on the Web site to use the driver with a fresh installation of Windows XP.

Installation Steps

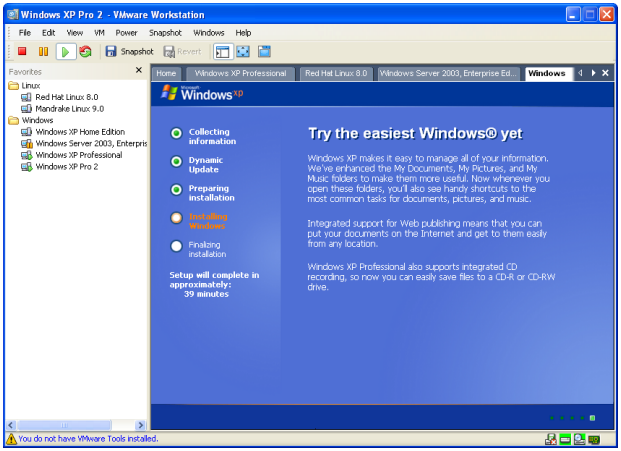
1. Insert the Windows XP CD in the CD-ROM drive.

   Note: If you plan to use a PXE server to install the guest operating system over a network connection, you do not need the operating system installation media. When you power on the virtual machine in the next step, the virtual machine detects the PXE server.

2. Power on the virtual machine to start installing Windows XP.



3. Follow the Windows XP installation steps as you would for a physical computer.



Installing VMware Tools

The installers for VMware Tools for Windows, Linux, FreeBSD and NetWare guest operating systems are built into VMware Workstation as ISO image files. (An ISO image file looks like a CD-ROM to your guest operating system and even appears as a CD-ROM in Windows Explorer. You do not use an actual CD-ROM to install VMware Tools, nor do you need to download the CD-ROM image or burn a physical CD-ROM of this image file.)

VMware Tools for Windows supports Windows 95, Windows 98, Windows Me, Windows NT 4.0, Windows 2000, Windows XP and Windows Server 2003 guest operating systems.

When you choose **VM** > **Install VMware Tools** from the VMware Workstation menu, VMware Workstation temporarily connects the virtual machine's first virtual CD-ROM drive to the ISO image file that contains the VMware Tools installer for your guest operating system and you are ready to begin the installation process.

Don't Forget VMware Tools

- It is very important that you install VMware Tools in the guest operating system.
- With the VMware Tools SVGA driver installed, Workstation supports significantly faster graphics performance.
- The VMware Tools package provides support required for shared folders and for drag and drop operations.
- Other tools in the package support synchronization of time in the guest operating system with time on the host, automatic grabbing and releasing of the mouse cursor, copying and pasting between guest and host, and improved mouse performance in some guest operating systems.

VMware Tools for Windows Guests

The detailed steps for installing VMware Tools depend on the version of Windows you are running. The steps that follow show how to install VMware Tools in a Windows XP guest. Some steps that are automated in newer versions of Windows must be performed manually in Windows 9x and Windows NT.

Note: If you are running VMware Workstation on a Windows host, and your virtual machine has only one CD-ROM drive, the CD-ROM drive must be configured as an IDE or SCSI CD-ROM drive. It cannot be configured as a generic SCSI device.

To add an IDE or SCSI CD-ROM drive, see Adding, Configuring and Removing Devices in a Virtual Machine on page 121. For information about generic SCSI, see Connecting to a Generic SCSI Device on page 302.

Installing VMware Tools in a Windows Guest Operating System

1. Power on the virtual machine.
2. When the guest operating system starts, prepare your virtual machine to install VMware Tools.

   Choose **VM** > **Install VMware Tools**.

The remaining steps take place inside the virtual machine.

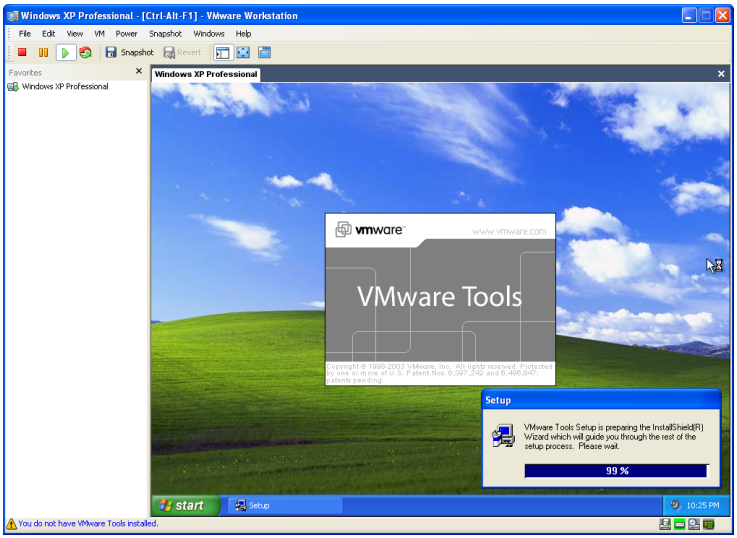
Note: You must log in to a Windows NT, Windows 2000, Windows XP, Windows Server 2003 or Longhorn guest operating system as an administrator in order to install

VMware Tools. Any user can install VMware Tools in a Windows 95, Windows 98 or Windows Me guest operating system.

3. If you have autorun enabled in your guest operating system (the default setting for Windows operating systems), a dialog box appears after a few seconds. It asks if you want to install VMware Tools. Click **Yes** to launch the InstallShield wizard.

   If autorun is not enabled, the dialog box does not appear automatically. If it doesn't appear, run the VMware Tools installer. Click **Start** > **Run** and enter `D:\setup\setup.exe` where `D:` is your first virtual CD-ROM drive.

   Note: You do not use an actual CD-ROM to install VMware Tools, nor do you need to download the CD-ROM image or burn a physical CD-ROM of this image file. The VMware Workstation software contains an ISO image that looks like a CD-ROM to your guest operating system and even appears as a CD-ROM in Windows Explorer. This image contains all the files needed to install VMware Tools in your guest operating system. When you finish installing VMware Tools, this image file no longer appears in your CD-ROM drive.



4. Follow the on-screen instructions.

5. On Windows Server 2003, Windows Me, Windows 98 SE and Windows 98 guests, the SVGA driver is installed automatically and the guest operating system uses it after it reboots. With Windows 2000 and Windows XP guests, you do not have to reboot to use the new driver.

Additional Steps for Some Versions of Windows When Migrating from Old Disk Versions

If you are migrating a VMware Workstation 2 disk to VMware Workstation 4 and your guest operating system is Windows NT, Windows Me, Windows 98 or Windows 95, you need to configure the video driver by hand. Instructions open automatically in Notepad at the end of the installation process. If the Notepad window is hidden, bring it to the front by clicking the **Notepad** button on the Windows taskbar.

For details, see the steps below that correspond to your guest operating system.

Windows NT

1. After installing VMware Tools, click **Finish**. The Display Properties dialog box appears.
2. Click the **Display Type** button. The Display Type dialog box appears.
3. Click the **Change** button. The Change Display dialog box appears.
4. Select **VMware, Inc.** from the **Manufacturer** list.
5. Select **VMware SVGA** as the display adapter and click **OK**.
6. Click **Yes** in response to the on-screen question about third-party drivers to install the driver, then click **OK** to confirm the drivers were installed.
7. Click **Close** from the Display Type dialog box, then click **Close** from the Display Properties dialog box.
8. Click **Yes** to restart Windows NT and start using the new video driver.
9. The VMware Tools background application is launched automatically when you reboot your virtual machine.

Windows Me

1. After installing VMware Tools, click **Finish**. The Display Settings dialog box appears.
2. Click the **Advanced** button.
3. Click the **Adapter** tab.
4. Click the **Change** button. This starts the Update Device Driver Wizard.
5. The wizard now presents two options. Choose the second option to **Specify the location of the driver**.

   Click **Next**.

6. Check the **Specify a location** checkbox. Enter the following path:

   `D:\video\win9x`

   `D:` is the drive letter for the first virtual CD-ROM drive in your virtual machine.

   Click **OK**.

7. Windows Me automatically locates your driver.
8. Select the **VMware SVGA II** display adapter and click **Next**.
9. Click **Next** to install the driver.

   If you are upgrading a virtual machine created under VMware Workstation 2, you may see a dialog box that warns, "The driver you are installing is not specifically designed for the hardware you have.… Do you wish to continue?" Click **Yes**.

   After the driver is installed, click **Finish**.

10. Click **Yes** to restart Windows Me and start using the new video driver.
11. The VMware Tools background application starts automatically when you reboot your virtual machine.

Windows 98

1. After installing VMware Tools, click **Finish**. The Display Settings dialog box appears.
2. Click the **Advanced** button. The Standard Display Adapter (VGA) Properties dialog box appears. If you are upgrading from a previous version of the VMware drivers, this dialog box is titled VMware SVGA Properties.
3. Click the **Adapter** tab.
4. Click the **Change** button. This starts the Update Device Driver Wizard. Click **Next**.
5. The wizard presents two options. Choose the option to **Display a list of all drivers in a specific location**. Click **Next**.
6. Select **Have Disk**. The Install From Disk dialog box appears.
7. Enter the following path:

   `D:\video\win9x`

   `D:` is the drive letter for the first virtual CD-ROM drive in your virtual machine.

   Click **OK**.

8. Select **VMware SVGA** display adapter and click **OK**.
9. Answer **Yes** to the on-screen question, then click **Next** to install the driver. After the driver is installed, click **Finish**.

10. Click **Close** in the SVGA Properties dialog box, then click **Close** in the Display Settings dialog box.
11. Click **Yes** to restart Windows 98 and start using the new video driver.
12. The VMware Tools background application starts automatically when you reboot your virtual machine.

Windows 95

1. After installing VMware Tools, click **Finish**. The Display Settings dialog box appears.
2. Click the **Advanced Properties** button. The Advanced Display Properties dialog box appears.
3. Click the **Change** button. The Select Device dialog box appears.
4. Select **Have Disk**.
5. Enter the following path:

   `D:\video\win9x`

   `D:` is the drive letter for the first virtual CD-ROM drive in your virtual machine.

   Click **OK**.
6. Click **OK** again to install the driver.
7. Click **Close** from the Advanced Display Properties dialog box, then click **Close** from the Display Setting dialog box.
8. Click **Yes** to restart Windows 95 and start using the new video driver.
9. The VMware Tools background application starts automatically when you reboot your virtual machine.

VMware Tools for Linux Guests

1. Power on the virtual machine.
2. After the guest operating system has started, prepare your virtual machine to install VMware Tools.

   Choose **VM** > **Install VMware Tools**.

The remaining steps take place inside the virtual machine.

3. Be sure the guest operating system is running in text mode. You cannot install VMware Tools from a terminal in an X window session.

   Some recent distributions of Linux are configured to run the X server when they boot and do not provide an easy way to stop the X server. However, you can

switch to a different workspace that is still in text mode and install VMware Tools from that workspace.

To switch between Linux workspaces in a virtual machine, press Ctrl-Alt-Space, release Space without releasing Ctrl and Alt, then press the function key for the workspace you want to use — for example, F2. If you change your hot key combination to something other than Ctrl-Alt, use that new combination with Space and the function key.

4. As root (`su -`), mount the VMware Tools virtual CD-ROM image, change to a working directory (for example, `/tmp`), uncompress the installer, then unmount the CD-ROM image.

   Note: You do not use an actual CD-ROM to install VMware Tools, nor do you need to download the CD-ROM image or burn a physical CD-ROM of this image file. The VMware Workstation software contains an ISO image that looks like a CD-ROM to your guest operating system. This image contains all the files needed to install VMware Tools in your guest operating system.

   Note: Some Linux distributions use different device names or organize the `/dev` directory differently. If your CD-ROM drive is not `/dev/cdrom`, modify the following commands to reflect the conventions used by your distribution.

   ```
   mount /dev/cdrom /mnt
   cd /tmp
   tar zxf /mnt/vmware-linux-tools.tar.gz
   umount /mnt
   ```

5. Run the VMware Tools installer.

   ```
   cd vmware-tools-distrib
   ./vmware-install.pl
   ```

   Respond to the questions the installer displays on the screen. Be sure to respond yes when the installer offers to run the configuration program.

6. Log out of the root account.

   ```
   exit
   ```

7. Start X and your graphical environment.

8. In an X terminal, launch the VMware Tools background application.

   ```
   vmware-toolbox &
   ```

   Note: You may run VMware Tools as root or as a normal user. To shrink virtual disks, you must run VMware Tools as root (`su -`).

Starting VMware Tools Automatically

You may find it helpful to configure your guest operating system so VMware Tools starts when you start your X server. The steps for doing so vary depending on your Linux distribution and your desktop environment. Check your operating system documentation for the appropriate steps to take.

For example, in a Red Hat Linux 7.1 guest using GNOME, follow these steps.

1. Open the Startup Programs panel in the GNOME Control Center.

   Main Menu (click the foot icon in the lower left corner of the screen) > Programs > Settings > Session > Startup Programs

2. Click Add.
3. In the Startup Command field, enter `vmware-toolbox`.
4. Click OK, click OK again, then close the GNOME Control Center.

The next time you start X, VMware Tools starts automatically.

Uninstalling VMware Tools

If you need to remove VMware Tools from your Linux guest operating system, log on as root (`su -`) and run the following command:

```
vmware-uninstall-tools.pl
```

VMware Tools for FreeBSD Guests

1. Power on the virtual machine.
2. Prepare your virtual machine to install VMware Tools.

   Choose VM > Install VMware Tools.

The remaining steps take place inside the virtual machine, not on the host computer.

3. Be sure the guest operating system is running in text mode. You cannot install VMware Tools while X is running.
4. As root (`su -`), mount the VMware Tools virtual CD-ROM image, change to a working directory (for example, `/tmp`), uncompress the installer, then unmount the CD-ROM image.

   Note: You do not use an actual CD-ROM to install VMware Tools, nor do you need to download the CD-ROM image or burn a physical CD-ROM of this image file. The VMware Workstation software contains an ISO image that looks like a CD-ROM to your guest operating system. This image contains all the files needed to install VMware Tools in your guest operating system.

```
mount /cdrom
cd /tmp
tar zxf /cdrom/vmware-freebsd-tools.tar.gz
umount /cdrom
```

5. Run the VMware Tools installer.

   ```
   cd vmware-tools-distrib
   ./vmware-install.pl
   ```

6. Log out of the root account.

   ```
   exit
   ```

7. Start X and your graphical environment
8. In an X terminal, launch the VMware Tools background application.

   ```
   vmware-toolbox &
   ```

   Note: You may run VMware Tools as root or as a normal user. To shrink virtual disks, you must run VMware Tools as root (`su -`).

Note: In a FreeBSD 4.5 guest operating system, sometimes VMware Tools does not start after you install VMware Tools, reboot the guest operating system or start VMware Tools on the command line in the guest. An error message appears:

```
Shared object 'libc.so.3' not found.
```

The required library was not installed. This does not happen with full installations of FreeBSD 4.5, but does occur for minimal installations. To fix the problem of the missing library, take the following steps:

1. Insert and mount the FreeBSD 4.5 installation CD or access the ISO image file.
2. Change directories and run the installation script.

   ```
   cd /cdrom/compat3x
   ./install.sh
   ```

Installing VMware Tools in a NetWare Virtual Machine

1. Power on the virtual machine.
2. Prepare your virtual machine to install VMware Tools.

   Choose VM > Install VMware Tools.

   The remaining steps take place inside the virtual machine.
3. Load the `CD9660.NSS` driver so the CD-ROM device mounts the ISO image as a volume. In the system console, type

   ```
   LOAD CD9660.NSS
   ```
4. When the driver finishes loading, you can begin installing VMware Tools. In the system console, type

   ```
   vmwtools:\setup.ncf
   ```
5. Restart the guest operating system. In the system console, type

   ```
   restart server
   ```

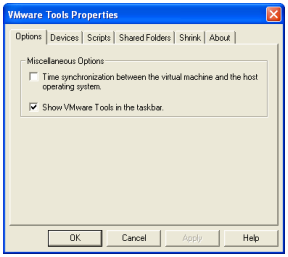
VMware Tools Configuration Options

This section shows the options available in a Windows XP guest operating system. Similar configuration options are available in VMware Tools for other guest operating systems.

When VMware Tools is running, an icon with the VMware boxes logo appears in the guest operating system's system tray.

To open the VMware Tools control panel, double-click the VMware Tools icon in the system tray.

If the VMware Tools icon does not appear in the system tray, go to **Start** > **Control Panel**. Locate the VMware Tools icon and double-click it.



The Options tab shows the Miscellaneous Options.

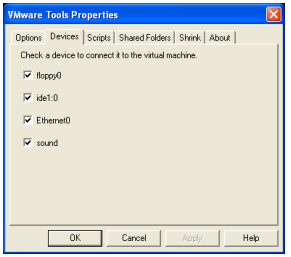
- Time synchronization between the virtual machine and the host operating system

  Note: You can synchronize the time in the guest operating system with the time on the host operating system only when you set the clock in the guest operating system to a time earlier than the time set on the host.

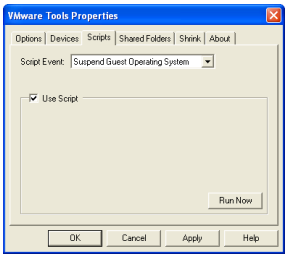
  Under some circumstances, the virtual machine may synchronize time with the host even though this item is not selected. If you want to disable time synchronization completely, open the virtual machine's configuration file (.vmx) in a text editor and set the following options to `FALSE`.

  ```
  tools.syncTime
  tools.synchronize.restore
  time.synchronize.resume.disk
  time.synchronize.continue
  time.synchronize.shrink
  ```

- Show VMware Tools in the taskbar



The Devices tab allows you to enable or disable removable devices. (You can also set these options from the Edit menu of the VMware Workstation application.)



The Scripts tab (available only in Windows guests) lets you enable, disable and run scripts that are associated with the Suspend, Resume, Power On and Power Off buttons.

Windows hosts: If the virtual machine is configured to use DHCP, the script executed when suspending a virtual machine releases the IP address of the virtual machine. The script executed when resuming a virtual machine renews the IP address of the virtual machine.

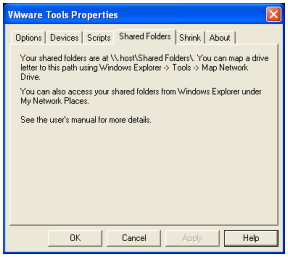
Linux hosts: The script executed when suspending a virtual machine stops networking for the virtual machine. The script executed when resuming a virtual machine starts networking for the virtual machine.

To run one of these scripts at some other time, select the script you want from the drop-down menu, then click **Run Now**.

To disable all scripts, deselect **Use Scripts**.

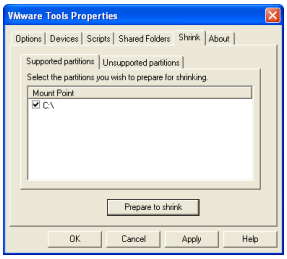
Note: Scripts cannot be run in Windows 95, NetWare and FreeBSD guest operating systems.

Note: Scripts in Windows NT and Windows Me guest operating systems do not release and renew the IP address.



The Shared Folders tab provides information on where to find your shared folders.

For more information on shared folders, see Using Shared Folders on page 113.



The Shrink tab gives you access to the controls you need if you wish to reclaim unused space in a virtual disk.

In some configurations, it is not possible to shrink virtual disks. If your virtual machine uses such a configuration, the Shrink tab displays information explaining why you cannot shrink your virtual disks.

Using the System Console to Configure VMware Tools in a NetWare Guest Operating System

You can configure certain virtual machine options such as time synchronization, CPU idling and device configuration with VMware Tools in a NetWare virtual machine using the system console. The VMware Tools command line program is called `vmwtool`. To see the options associated with this command, at the system console, type

```
vmwtool help
```

Summary of VMware Tools Commands for a NetWare Guest

Each command in the following table must be entered into the system console after the VMware Tools command `vmwtool`. Use the following format:
`vmwtool <command>`

`vmwtool` **Command**	**Definition**
`help`	Displays a summary of VMware Tools commands and options in a NetWare guest.
`partitonlist`	Displays a list of all disk partitions in the virtual disk and whether or not a partition can be shrunk.
`shrink <partition>`	Shrinks the listed partitions. If no partitions are specified, then all partitions in the virtual disk are shrunk. The status of the shrink process appears at the bottom of the system console.
`devicelist`	Lists each removable device in the virtual machine, its device ID and whether the device is enabled or disabled. Removable devices include the virtual network adapter, CD-ROM and floppy drives.
`disabledevice <device name>`	Disables the specified device or devices in the virtual machine. If no device is specified, then all removable devices in the virtual machine are disabled.
`enabledevice <device name>`	Enables the specified device or devices in the virtual machine. If no device is specified, then all removable devices in the virtual machine are enabled.
`synctime [on|off]`	Lets you turn on or off synchronization of time in the guest operating system with time on the host operating system. By default, time synchronization is turned off. Use this command without any options to view the current time synchronization status. You can synchronize the time in the guest operating system with time on the host operating system only when the time in the guest operating system is earlier than the time set in the host.
`idle [on|off]`	Lets you turn on or off the CPU idler. By default, the idler is turned on. The CPU idler program is included in VMware Tools for NetWare guests. The idler program is needed because NetWare servers do not idle the CPU when the operating system is idle. As a result, a virtual machine takes CPU time from the host regardless of whether the NetWare server software is idle or busy.

CHAPTER 5

Running VMware Workstation

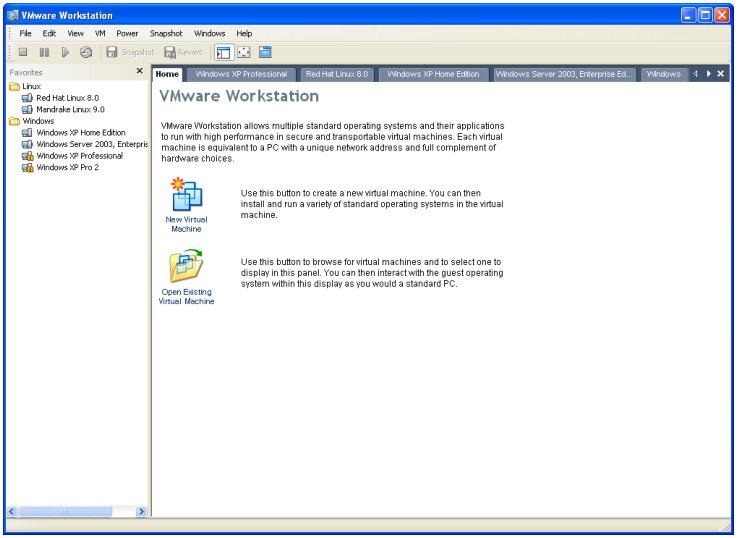
After you have installed VMware Workstation, a guest operating system and VMware Tools, how do you run your virtual machine? The following sections give you highlights of the most common tasks.

For purposes of illustration, the examples in these sections use a Windows XP guest operating system. Some commands used in the illustrations are different from those used in other guest operating systems.

Overview of the VMware Workstation Window

Think of your VMware Workstation virtual machine as a separate computer that runs in a window on your physical computer's desktop. The Workstation window lets you run multiple virtual machines and switch easily from one to another.

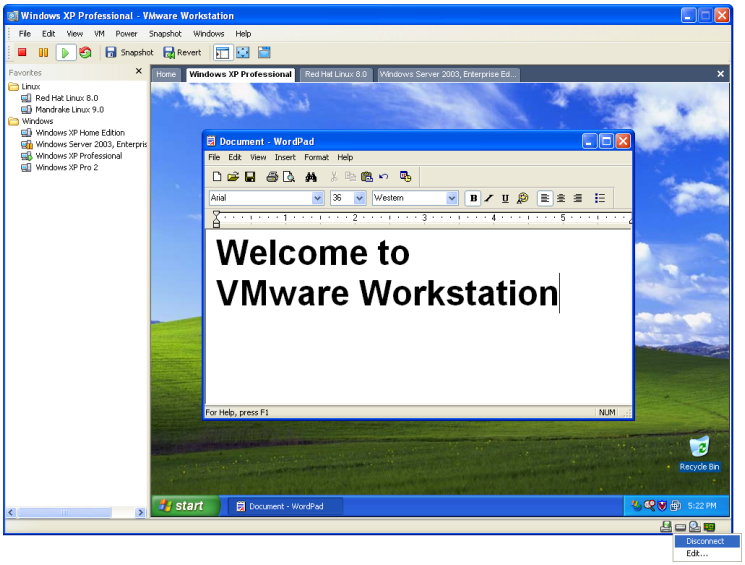
When no virtual machine is running, you see the VMware Workstation home page. Use the icons on the home page to start creating a new virtual machine or open an existing virtual machine.



One Window or Many — Your Choice

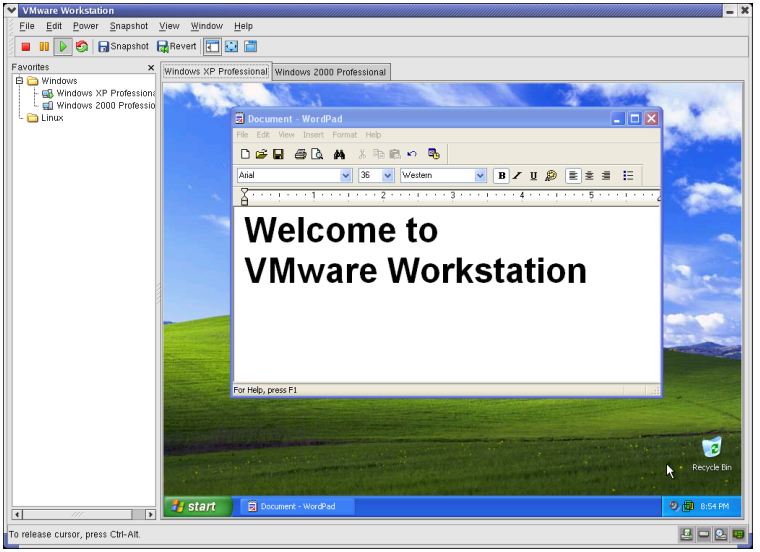
- In VMware Workstation 4, you can open multiple virtual machines in the same Workstation window. Or you can launch multiple instances of VMware Workstation. You can even run multiple instances of VMware Workstation and have more than one virtual machine in each window. Just be sure you have enough memory and processor power to handle the number of virtual machines you want to run.

To close the home page, click the X to the right of the tabs on a Windows host or the X on the tab on a Linux host. To display the home page again, choose **View** > **Go to Home Tab**.



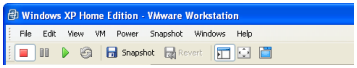
VMware Workstation main window on a Windows host

Windows host: Right-click the icon for a removable device on the status bar to disconnect it or edit its configuration.

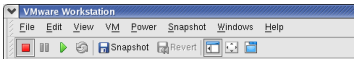


VMware Workstation main window on a Linux host

Instead of using physical buttons to turn this computer on and off, you use buttons on the toolbar at the top of the VMware Workstation window.

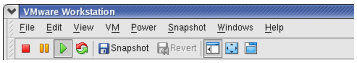


Toolbar when virtual machine is powered off (as seen on a Windows host)



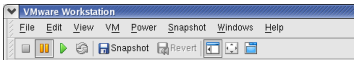
Toolbar when virtual machine is powered off (as seen on a Linux host)

Toolbar when virtual machine is powered on (as seen on a Windows host)



Toolbar when virtual machine is powered on (as seen on a Linux host)

Toolbar when virtual machine is suspended (as seen on a Windows host)



Toolbar when virtual machine is suspended (as seen on a Linux host)

There are separate Power Off and Power On buttons. When you suspend a virtual machine, the Power On button becomes a Resume button.

Menus in VMware Workstation 4.5 are organized somewhat differently from those in VMware Workstation 4.0. The following table lists the locations for the most commonly used menu items that have been moved:

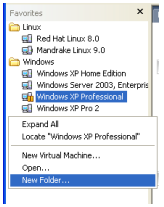
Old Location	New Location
File > New > New Virtual Machine	File > New Virtual Machine
File > New > New Window	File > New Window
File > Install VMware Tools	VM > Install VMware Tools
File > Upgrade Virtual Hardware	VM > Upgrade Virtual Hardware
File > Add <vmname> to Favorites	VM > Add to Favorites
File > Remove <vmname> from Favorites	VM > Remove from Favorites
Power > Send Ctrl+Alt+Del	VM > Send Ctrl+Alt+Del
Power > Grab Input	VM > Grab Input

Old Location	New Location
Edit > Removable Devices	VM > Removable Devices
Edit > Application Settings	Edit > Preferences
Edit > Virtual Machine Settings	VM > Settings

When a virtual machine is active, its virtual machine name is displayed in a tab at the top of the virtual machine window. To switch from one active virtual machine to another, click the tab of the virtual machine you want to see. It's like a soft KVM switch. You can use this feature in the windowed view and also in the quick switch view.

Tabs make it easy to switch among active virtual machines (as seen on a Windows host)

If you want to view more than one virtual machine at the same time, you can open multiple Workstation windows and launch one or more virtual machines in each.

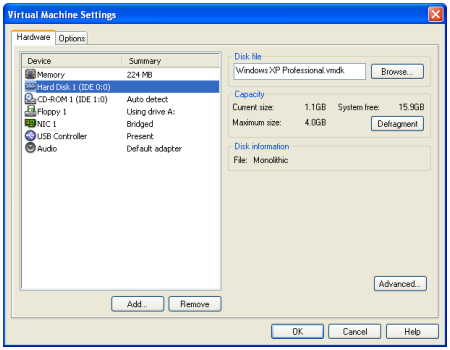


Add virtual machines you use often to the Favorites list (as seen on a Windows host). Right-click in the Favorites pane to create a folder. Drag and drop virtual machine names into folders to organize them.

The Favorites list gives you a convenient way to open frequently used virtual machines. To add a virtual machine to the Favorites list, open the virtual machine (**File** > **Open**), then choose **VM** > **Add to Favorites**. To remove an item from the list, click it to highlight it, then choose **VM** > **Remove from Favorites**.

Indicators on the icons for virtual machines in the Favorites list show whether a virtual machine is powered off, powered on or suspended.

To toggle the display of the Favorites list on or off, click the **Favorites** button on the toolbar.



Use the virtual machine settings editor to add, remove and modify virtual machine components

The virtual machine settings editor on Linux hosts now matches the virtual machine settings editor on Windows hosts. To change settings for a device, click its name in the list on the left, then make changes in the right-hand pane. Click **Add** and follow the directions in the Add Hardware Wizard to add a new device. To remove a device, click its name in the list on the left, then click **Remove**.

When you have finished making changes, click **OK** to save the changes and close the virtual machine settings editor.

An alert appears in the status bar — at the bottom left corner of the VMware Workstation window — when your virtual machine is not running the version of VMware Tools that matches your version of VMware Workstation. To launch the VMware Tools installer, choose **VM** > **Install VMware Tools**.

Note: Your guest operating system must be completely installed and running when you install VMware Tools.

For details, see Installing VMware Tools on page 81.

Starting a Virtual Machine

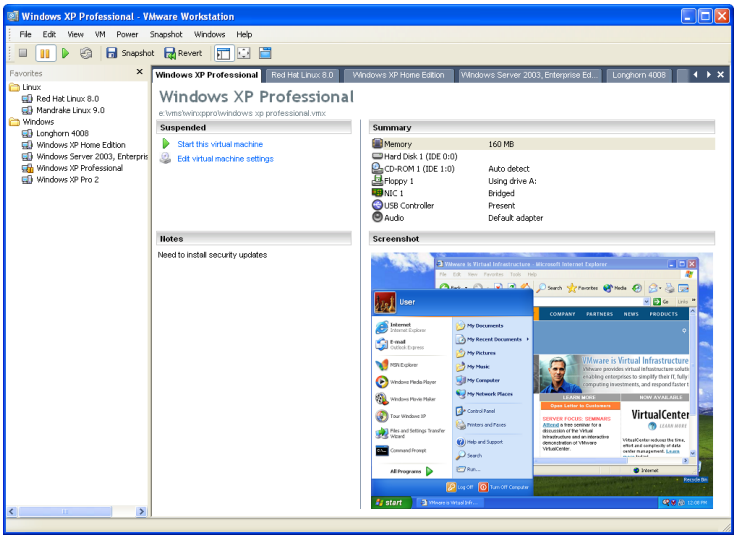
To start a virtual machine, take the steps described below for your host operating system.

Starting a Virtual Machine on a Windows Host

1. Start VMware Workstation by double-clicking the shortcut on your desktop or launch the program from the **Start** menu (**Start** > **Programs** > **VMware** > **VMware Workstation**).

   The VMware Workstation window opens.

2. Select the name of the virtual machine you want to use in the Favorites list at the left of the Workstation window.

   If the virtual machine you want to use is not shown there, choose **File** > **Open** and browse to the configuration (`.vmx`) file for the virtual machine you want to use. (On a Linux host, a virtual machine created with an earlier VMware product may have a configuration file with a `.cfg` extension.) To add that virtual machine to the Favorites list so you can open it easily the next time you want to use it, choose **VM** > **Add to Favorites**.

Note: By default, VMware Workstation 4 stores virtual machines in the `My Documents` folder of the user who is logged on when the virtual machine is created. On Windows Server 2003, Windows XP and Windows 2000, the default folder is `C:\Documents and Settings\<username>\My Documents\My Virtual Machines\<guestOSname>`. On Windows NT, the default folder is `C:\WINNT\Profiles\<username>\Personal\My Virtual Machines\<guestOSname>`.

3. Click the **Power On** button to start the virtual machine.
4. Click anywhere inside the virtual machine window to give the virtual machine control of your mouse and keyboard.
5. If you need to log on, type your name and password just as you would on a physical computer. If your guest operating system asks you to press Ctrl-Alt-Del before logging in, press Ctrl-Alt-Ins, instead.

Removing a Name from the Favorites List

You can remove the name of a virtual machine from the Favorites list at any time. Removing the name from the list does not affect the virtual machine's files. You can add the virtual machine to the list again at any time.

To remove a name from the Favorites list, take these steps.

1. Click a name in the list to select it.
2. Choose **VM** > **Remove from Favorites**.

Starting a Virtual Machine on a Linux Host

1. Open a terminal window, type `vmware &` and press Enter.
2. Select the name of the virtual machine you want to use in the Favorites list at the left of the Workstation window.

   If the virtual machine you want to use is not shown in the Favorites list, go to **File** > **Open** and browse to the configuration file (`.vmx` or `.cfg` file) for the virtual machine you want to use. To add that virtual machine to the Favorites list so you can open it easily the next time you want to use it, click **Add**, make any changes you wish to the display name and location in the Favorites list, then click **OK**.

   Note: By default, VMware Workstation 4 stores virtual machines in `<homedir>/vmware/<guestOSname>`, where `<homedir>` is the home directory of the user who is logged on when the virtual machine is created.
3. Click the **Power On** button to start the virtual machine.

4. Click anywhere inside the virtual machine window to give the virtual machine control of your mouse and keyboard.
5. If you need to log on, type in your name and password just as you would on a physical computer.

Checking the Status of VMware Tools

For best performance, it is important to have VMware Tools installed and running in your virtual machine.

After you install VMware Tools in a Windows virtual machine, the VMware Tools services start automatically when you start the guest operating system.

When VMware Tools is running in a Windows virtual machine, the VMware Tools icon appears in the system tray unless you disable the icon.

If the VMware Tools icon is not displayed in the system tray, you can use the VMware Tools control panel in the guest operating system. Go to **Start** > **Settings** > **Control Panel** or **Start** > **Control Panel**, depending on the version of Windows you are using, locate the VMware Tools icon and double-click it to change settings for VMware Tools. You can also reactivate the system tray icon. On the **Options** tab, check **Show VMware Tools in the taskbar**.

In a Linux or FreeBSD virtual machine, boot the guest operating system, start X and launch your graphical environment. Then you can launch the VMware Tools background application with this command:

```
vmware-toolbox &
```

You may run VMware Tools as root or as a normal user. To shrink virtual disks, you must run VMware Tools as root (`su -`).

With some window managers, you can place the command to start VMware Tools in a startup configuration so VMware Tools starts automatically when you start your graphical environment. Consult your window manager's documentation for details.

Controlling the Display

You can control the VMware Workstation display in a variety of ways to suit the way you prefer to work with your virtual machines.

Using Full Screen Mode

Virtual machines run faster in full screen mode.

If you want your VMware Workstation virtual machine's display to fill the screen — so you no longer see the borders of the VMware Workstation window — click the **Full Screen** button on the toolbar. You can also use a keyboard shortcut — press the Ctrl-Alt-Enter keys at the same time.

To get out of full screen mode — to show your virtual machine inside a VMware Workstation window again — press the Ctrl-Alt key combination.

Linux hosts: You can switch between virtual machines without leaving full screen mode by using a Ctrl-Alt-Fn key combination, where Fn is a function key corresponding to the virtual machine you want to see. To find out what function key to use for a particular virtual machine, check the title bar of the virtual machine while it is running in a window.

Windows hosts: For similar functionality, see Using Full Screen Switch Mode on page 334.

Note: VMware Workstation does not support running virtual machines in full screen mode on dual-monitor systems.

Using Quick Switch Mode

Quick switch mode is similar to full screen mode with the addition of tabs at the top of the screen for switching from one active virtual machine to another. The virtual machine's screen is resized to fill the screen completely, except for the space occupied by the tabs.

To enter quick switch mode, choose **View** > **Quick Switch**.

To view the VMware Workstation menu and toolbar while you are using quick switch mode, move the mouse pointer to the top of the screen.

To resize a Windows guest operating system's display so it fills as much of the screen as possible in quick switch mode, choose **View** > **Fit Guest to Window**. The Fit Guest to Window option works only if you have the current version of VMware Tools installed in the guest operating system.

Note: When you choose **Fit Guest to Window**, VMware Workstation adjusts the display settings of your Windows guest operating system as needed. If you subsequently run the virtual machine in normal mode, you may want to change the display settings back to their previous values.

To get out of quick switch mode, move the mouse pointer to the top of the screen to activate the menu, then choose **View** > **Quick Switch**.

Taking Advantage of Multiple Monitors

If your host has a standard multiple monitor display, you can run separate sets of virtual machines on each of the monitors. To use two monitors, launch two instances of VMware Workstation. Start one or more virtual machines in each VMware Workstation window, then drag each VMware Workstation window to the monitor on which you want to use it. For the largest possible screen display, switch each of the windows to quick switch mode (**View** > **Quick Switch**).

To switch mouse and keyboard input from the virtual machine on the first screen to the virtual machine on the second screen, move the mouse pointer from one to the other. You do not need to take any special steps if VMware Tools is running in both guest operating systems and if you are using the default settings for grabbing input. If you have changed the defaults, you may need to press Ctrl-Alt to release the mouse pointer from the first virtual machine, move it to the second virtual machine, then click in the second virtual machine so it will grab control of mouse and keyboard input.

Note: Multiple monitor support is experimental in this release of VMware Workstation. It does not work properly with some third-party desktop management software or display drivers.

Note: If you switch to full screen mode, VMware Workstation always uses the primary display. To use multiple monitors, you must use either the normal (windowed) mode or quick switch mode.

Fitting the VMware Workstation Window to the Virtual Machine

The **View** menu gives you two ways to adjust the size of the VMware Workstation window so it exactly fits the virtual machine's display.

Autofit is toggled on or off each time you click it. When **Autofit** is on, the window adjusts automatically to fit the virtual machine's display. When it is off, you can adjust the window to a size of your choice. If you make the window smaller than the virtual

machine's display, scroll bars appear so you can move to the part of the virtual machine's display that you want to see.

If **Autofit** is off, you can choose **View** > **Fit** to adjust the VMware Workstation window so it fits the virtual machine's display.

Fitting a Windows Guest Operating System's Display to the VMware Workstation Window

If your Windows guest operating system is set to a display resolution larger or smaller than the size of the virtual machine window, you can make it fit exactly by choosing **View** > **Fit Guest to Window**.

When you choose **Fit Guest to Window**, VMware Workstation adjusts the display settings of your Windows guest operating system as needed. If you want s to change the display settings back to their previous values, use the guest operating system's controls to make the change.

Note: When you use the Fit Guest to Window option and the window is small, your guest operating system's screen resolution may be set to something smaller than VGA (640 x 480). Some installers and other programs do not run at resolutions smaller than 640 x 480. If either width or height is smaller than the corresponding dimension required for VGA, the programs refuse to run. Error messages may include such phrases as "VGA Required To Install" or "You must have VGA to install."

There are two ways to work around this problem.

- If your host computer's screen resolution is high enough, you can enlarge the window, then choose **Fit Guest to Window**.
- If your host computer's screen resolution does not allow you to enlarge the window enough, manually set the guest operating system's screen resolution to 640 x 480 or larger.

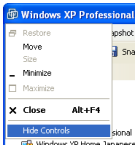
Simplifying the Screen Display

If you prefer, you can turn off display of many of the controls visible in the VMware Workstation window.

Use the **View** menu to toggle the following controls on or off:

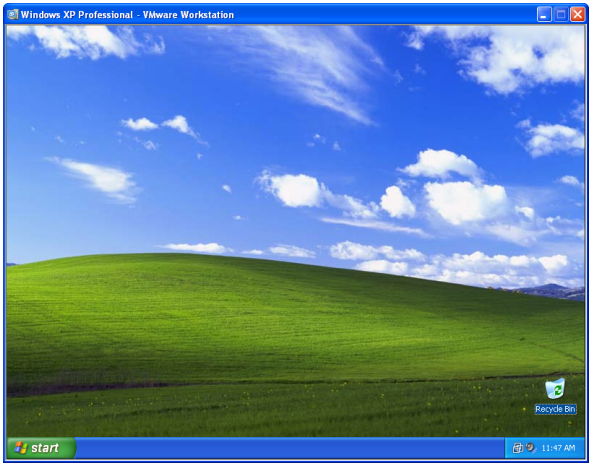
- Favorites
- Toolbar
- Status bar
- Virtual machine tabs

On a Windows host, you can also hide the menu bar. To do so, click the title bar icon, then choose **Hide Controls**.



Choosing **Hide Controls** hides the menu bar, the toolbar, the status bar and the Favorites panel.

For the simplest possible VMware Workstation window on a Windows host, first choose **View** > **Virtual Machine Tabs** to turn off the tabs. Then, from the title bar icon shortcut menu, choose **Hide Controls**.



Using the View menu and the title bar icon shortcut menu, you can remove all visible controls from the VMware Workstation window.

Installing New Software

Installing new software in a VMware Workstation virtual machine is just like installing it on a physical computer. For example, to install software in a Windows virtual machine, take the following steps:

1. Be sure you have started the virtual machine and, if necessary, logged on. On the Workstation menus, check **VM** > **Removable Devices** to be sure the virtual machine has access to the CD-ROM drive and, if needed, the floppy drive.
2. Insert the installation CD-ROM or floppy disk into the proper drive. If you are installing from a CD-ROM, the installation program may start automatically.
3. If the installation program does not start automatically, click the Windows **Start** button, go to **Settings** > **Control Panel**, then double-click **Add/Remove Programs** and click the **Install** button. Follow the instructions on screen and in the user manual for your new software.

Note: Some applications use a product activation feature that creates a key, based on the virtual hardware in the virtual machine where it is installed. Changes in the configuration of the virtual machine may require you to reactivate the software. To minimize the number of significant changes, set the final memory size for your virtual machine and install VMware Tools before you activate the software.

Note: When you try to run a few programs — including the installer for the Japanese-language version of Trend Micro Virus Buster — Workstation may appear to hang. For the workaround to this problem, see the troubleshooting note on the VMware Web site at *www.vmware.com/info?id=30*.

Cutting, Copying and Pasting Text

When VMware Tools is running, you can cut (or copy) and paste text between applications in the virtual machine and the host computer or between two virtual machines. Use the normal hot keys or menu choices to cut, copy and paste.

To turn off this feature — to prevent accidental copying and pasting from one environment to another — change your preferences.

Choose **Edit** > **Preferences**. On the Input tab, clear the check box beside **Enable copy and paste to and from virtual machine**.

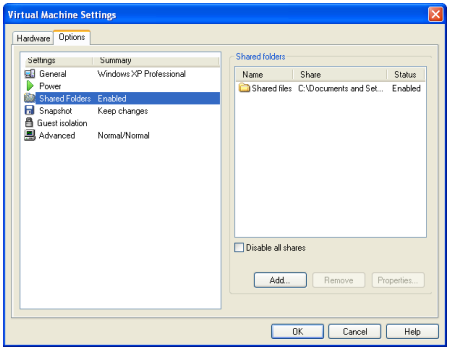
Using Shared Folders

With shared folders, you can easily share files among virtual machines and the host computer. To use shared folders, you must have the current version of VMware Tools installed in the guest operating system and you must use the virtual machine settings editor to specify which directories are to be shared.

You can use shared folders with virtual machines running the following guest operating systems:

- Windows Server 2003
- Windows XP
- Windows 2000
- Windows NT 4.0
- Linux with a kernel version of 2.4 or higher

To set up one or more shared folders for a virtual machine, be sure the virtual machine is open in Workstation and click its tab to make it the active virtual machine. Go to **VM** > **Settings** > **Options** and click **Shared folders**.



You can add one or more directories to the list. Those directories may be on the host computer or they may be network directories accessible from the host computer.

In a Windows virtual machine, shared folders appear in My Network Places (Network Neighborhood in a Windows NT virtual machine) under VMware Shared Folders. For example, if you specify the name `Test files` for one of your shared folders, you can navigate to it by opening **My Network Places** > **VMware Shared Folders** > **.host** > **Shared Folders** > **Test files**.

You can also go directly to the folder using the UNC path `\\.host\Shared Folders\Test files`.

You can map a shared folder to a drive letter just as you would with a network share.

Note: To see shared folders displayed in this way, you must update VMware Tools in the virtual machine to the current version. If your guest operating system has the version of VMware Tools that shipped with VMware Workstation 4.0, shared folders appear as folders on a designated drive letter.

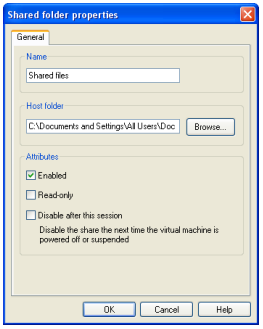
In a Linux virtual machine, shared folders appear under `/mnt/hgfs`. So the shared folder in this example would appear as `/mnt/hgfs/Test files`.

To add a new shared folder to the list, click **Add**. On a Windows host, a wizard guides you through the process. On a Linux host, a dialog box appears. Enter the required information, then click **OK**.

Provide the following information:

- The path on the host to the directory you want to share. Type in the full path or browse to the directory.
- The name for the directory. This is the name that appears inside the virtual machine.
- Whether the shared folder is enabled. You may want to add a folder to the list without enabling it immediately. You can then enable the folder at any time by clicking its name in this list, clicking **Properties** and enabling the folder in the Properties dialog box.
- Access options for the shared folder. You can give the current virtual machine read-only access, or read-write access. Access to files in the shared folder is also governed by permission settings on the host computer. For example, if you are running VMware Workstation as a user named User, the virtual machine can read and write files in the shared folder only if User has permission to read and write them.
- Expiration options for the shared folder. You can specify that the folder is always enabled or that it is enabled only during the current working session. If you select **Disable after this session**, the shared folder is disabled when you suspend or power off the virtual machine.

To change the settings for a shared folder on the list, click the folder's name to highlight it, then click **Properties**. The Properties dialog box appears.



Change any settings you wish, then click **OK**.

Note: You can use shared folders to share any type of file. However, Windows shortcuts and Linux symbolic links do not work correctly if you try to use them via shared folders.

Caution: Do not open a file in a shared folder from more than one application at a time. For example, you should not open the same file using an application on the host operating system and another application in the guest operating system. In some circumstances, doing so could cause data corruption in the file.

Using Drag and Drop

With the drag and drop features of VMware Workstation 4, you can move files easily between a Windows host and a Windows virtual machine. You can drag and drop individual files or entire directories.

You can drag and drop files or folders from a file manager, such as Windows Explorer, on the host to a file manager in the virtual machine or vice versa. You can also drag files from a file manager to an application that supports drag and drop — or from applications such as zip file managers that support drag-and-drop extraction of individual files.

When you drag a file or folder from host to virtual machine or from virtual machine to host, Workstation copies the file or folder to the location where you drop it. This means, for example, that if you drop a file on the desktop icon of a word processor, the word processor opens with a copy of the original file. The original file does not reflect any changes you make to the copy.

Initially, the application opens using a copy of the file that is stored in your temp directory (as specified in the `%TEMP%` environment variable). To protect any changes you make, choose **File** > **Save As** from the application's menu and save the file in a different directory. Otherwise it may be overwritten or deleted by mistake.

To disable or enable drag and drop for a virtual machine:

1. Open the virtual machine settings editor (**VM** > **Settings**), click the **Options** tab and select **Guest isolation**.
2. Select **Disable drag and drop to and from this virtual machine** to disable the feature. Deselect it to enable the feature.

Suspending and Resuming Virtual Machines

You can save the current state of your virtual machine by suspending it. Later, you can resume the virtual machine to pick up work quickly, right where you stopped — with all documents you were working on open and all applications in the same state as they were at the time you suspended the virtual machine.

To suspend a virtual machine:

1. If your virtual machine is running in full screen mode, return to window mode by pressing the Ctrl-Alt key combination.
2. Click **Suspend** on the VMware Workstation toolbar.
3. When VMware Workstation has completed the suspend operation, it is safe to exit VMware Workstation.

   File > **Exit**

To resume a virtual machine that you have suspended:

1. Start VMware Workstation and choose a virtual machine you have suspended. The process is the same as that described in Starting a Virtual Machine on page 103 or Starting a Virtual Machine on a Linux Host on page 104.
2. Click **Resume** on the VMware Workstation toolbar.

   Note that any applications you were running at the time you suspended the virtual machine are running and the content is the same as it was when you suspended the virtual machine.

For more information, see Using Suspend and Resume on page 199.

Taking and Reverting to a Snapshot

VMware Workstation lets you take a snapshot of a virtual machine at any time and revert to that snapshot at any time.

You can take a snapshot while a virtual machine is powered on, powered off or suspended. A snapshot preserves the virtual machine just as it was when you took the snapshot — the state of the data on all the virtual machine's disks and whether the virtual machine was powered on, powered off or suspended.

When you revert to a snapshot, you discard all changes made to the virtual machine since you took the snapshot.

Use the **Snapshot** and **Revert** buttons on the Workstation toolbar to take a snapshot and revert to it later.

You can take a new snapshot at any time. When you do so, you replace the previous snapshot. You can have only one active snapshot at a time.

For more information, including examples of ways you can use the snapshot, see Using the Snapshot on page 200.

Shutting Down a Virtual Machine

As with physical computers, you need to shut down your guest operating system before you power off your virtual machine. In a Windows guest operating system, take these steps.

1. Select **Shut Down** from the **Start** menu of the guest operating system (inside the virtual machine).
2. Select **Shut Down**, then click **OK**.
3. After the guest operating system shuts down, you can turn off the virtual machine. Click **Power Off**.
4. Now it is safe to exit VMware Workstation.

   File > **Exit**

If you are using a different guest operating system, the procedure is similar. Follow the usual steps to shut down the guest operating system inside your virtual machine, then turn off the virtual machine with the **Power Off** button and exit VMware Workstation.

Removing a Virtual Machine

To completely remove a virtual machine, remove the virtual machine's name from the Favorites list and delete its files from the host computer.

To remove the virtual machine name from the Favorites list, right-click the name and choose **Remove**. This choice affects only the listing in the Favorites list; it leaves all virtual machine files on the computer.

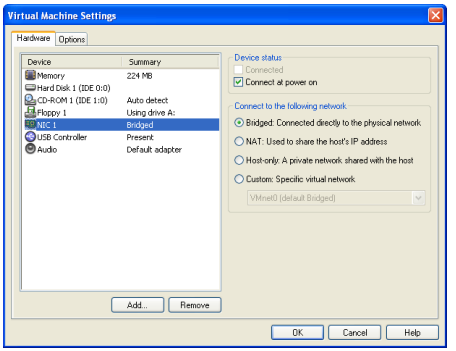
To delete the virtual machine's files from the host computer, navigate to the folder that holds the virtual machine's files, then delete the folder and all the files it contains. For more information on the files that are part of a virtual machine, see What's in a Virtual Machine? on page 67.

Using Devices in a Virtual Machine

Follow the guidelines in this section to add, remove, configure, connect and disconnect your virtual machine's devices.

Adding, Configuring and Removing Devices in a Virtual Machine

The virtual machine settings editor (**VM** > **Settings**) is the control center where you can add devices to a virtual machine, change the settings for those devices and remove them.



To add a new device, open the virtual machine settings editor, click **Add**, then follow the instructions in the Add New Hardware Wizard to add the new device to your virtual machine. Click **OK** to save your changes and close the virtual machine settings editor.

To change settings for a device, open the virtual machine settings editor, select the device you want to modify and make your changes. Click **OK** to save your changes and close the virtual machine settings editor.

To remove a device, open the virtual machine settings editor, click the name of the device you want to remove, then click **Remove**. Click **OK** to close the virtual machine settings editor.

Connecting and Disconnecting Removable Devices

Choose **VM** > **Removable Devices** to connect and disconnect removable devices that you have configured for your virtual machine — including floppy drives, DVD/CD-ROM drives, USB devices and Ethernet adapters — while the virtual machine is running.

When you choose **VM** > **Removable Devices**, a submenu appears. Choose a device from that menu to connect or disconnect it and to edit device settings. If you choose **Edit**, a dialog box appears. Make all the changes you want to make, then click **OK**.

Creating a Screen Shot of a Virtual Machine

You can capture a screen shot of a virtual machine using **File** > **Capture Screen**. You can save this image as a bitmap (`.bmp`) file on a Windows host or as a portable network graphics (`.png`) file on a Linux host.

Checking for Product Updates

VMware Workstation now checks automatically to see if updates for the product are available. By default, it checks once a week, at the time you launch Workstation. You can also change the interval for the automatic checks. You can have VMware Workstation check once a month, once a week, once each day or never.

Choose **Edit** > **Preferences** > **Workspace**. Use the **Check for updates automatically** drop-down list to set the interval.

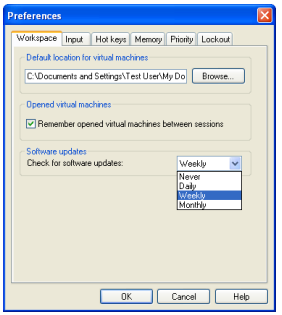
You can check manually at any time by choosing **Help** > **Check for Updates on the Web.**

This check works only if the host computer is connected to the Internet.

Setting Preferences for VMware Workstation

The Preferences dialog box allows you to change a number of settings that apply to VMware Workstation itself, no matter what virtual machine you are running. The settings on the **Workspace**, **Input** and **Hot Keys** tabs apply to the user currently logged on to the host computer. They do not affect settings made by any other user on the computer. The settings on the **Memory** and **Lockout** tabs apply no matter what virtual machine is running or who is logged on to the host computer. The settings on the **Priority** tab apply to all virtual machines for the user currently logged on to the host computer. They do not affect settings made by any other user on the computer.

To make changes to these settings, choose **Edit** > **Preferences**.

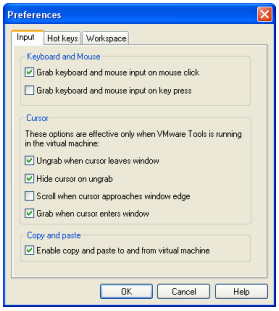


Workspace — The Workspace tab lets you change the directory in which newly created virtual machines are stored. The directory Workstation uses by default is displayed under **Default location for virtual machines**. To set a different directory, type in the path or click **Browse** to navigate to the directory you want to use. Workstation creates a directory for each new virtual machine under the directory you specify here.

If you select **Remember opened virtual machines between sessions** check box, you see a tab for each opened virtual machine in the virtual machine window the next time you start Workstation. A virtual machine is considered opened if both of the following conditions are true:

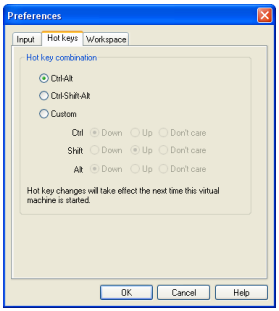
- The virtual machine was left open.
- The virtual machine was powered on and off or powered on and suspended.

Use the **Check for updates automatically** drop-down list to determine how often VMware Workstation checks to see if new versions of the product are available. You can choose daily, weekly or monthly automatic checks or choose **Never** to turn off automatic checking. You can check manually at any time by choosing **Help** > **Check for Updates on the Web.**



Input — The Input tab lets you adjust the way that the virtual machine captures control of keyboard and mouse.

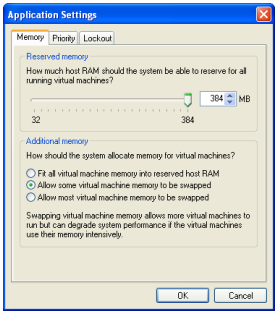
Note: The **Grab when cursor enters window** option allows you to move the mouse pointer back into the virtual machine window easily if you have been working in the virtual machine, then temporarily moved the mouse pointer outside the virtual machine window. The mouse pointer is grabbed only when VMware Workstation has focus (is the active application). Also, if you release the mouse pointer by pressing a hot-key combination — Ctrl-Alt by default — you must click inside the virtual machine window to make VMware Workstation grab the mouse pointer again.



Hot keys — The Hot Key tab lets you change the key combination that determines whether certain combinations of keys are passed to the guest operating system or intercepted by VMware Workstation.

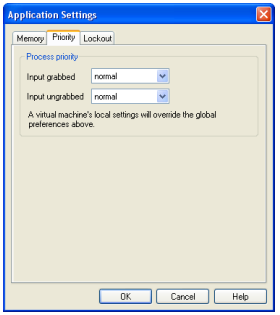
Note: Because Ctrl-Alt is the key combination used to tell VMware Workstation to release (ungrab) mouse and keyboard input, combinations that include Ctrl-Alt are not passed to the guest operating system. If you need to use such a combination — for example, use Ctrl-Alt-<Fkey> to switch between Linux 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.

Using this dialog box, you can also construct your own custom hot-key combination.



Memory usage— The Memory tab lets you adjust the amount of physical RAM that can be used by all running virtual machines. It also lets you adjust how much virtual machine memory may be swapped to disk, allowing you to run more or larger virtual machines if you are willing to accept slower performance.

For details on adjusting memory settings in VMware Workstation, see Memory Usage Notes on page 317.

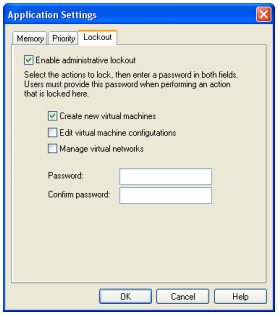


Process priorities — The Priority tab on a Windows host lets you determine the priority that the Windows process scheduler gives to your virtual machines when mouse and keyboard input are going to a particular virtual machine and when input is not going to that virtual machine.

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.

To change the settings 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 is no corresponding setting on a Linux host.



Administrative lockout for certain features — The Lockout tab on a Windows host lets you restrict who can create new virtual machines, edit virtual machine configurations and change networking settings. For details, see Locking Out Interface Features on page 329.

There are no corresponding settings on a Linux host.

Command Reference

The following sections describe command line options that are available when you launch VMware Workstation and keyboard shortcuts you can use while VMware Workstation is running.

Startup Options on a Linux Host

The following list describes various options available when you run VMware Workstation from the command line on a Linux host operating system.

```
vmware [-x] [-X] [-q] [-s <variablename>=<value>]
[-m] [-v] [/<path_to_config>/<config>.vmx ]
[X toolkit options ]
```

`-x` automatically powers on the virtual machine when VMware Workstation starts. This is equivalent to clicking the **Power On** button in the VMware Workstation toolbar.

`-X` automatically powers on the virtual machine, then switches the VMware Workstation window to full screen mode.

`-q` closes the virtual machine's tab when the virtual machine powers off. If no other virtual machine is open, it also exits VMware Workstation. This is particularly useful when the guest operating system is capable of powering off the virtual machine.

`-s` sets the specified variable to the specified value. Any variable names and values that are valid in the configuration file may be specified on the command line with the `-s` switch.

`-m` starts the program in quick switch mode on a Linux host.

`-v` displays the product name, version and build number.

`/<path_to_config>/<config>.vmx` (or `.cfg`) launches a virtual machine using the specified configuration file.

X toolkit options can be passed as arguments, although some of them (most notably the size and title of the VMware Workstation window) cannot be overridden.

Startup Options on a Windows Host

Most of the switches described above for Linux can also be used on a Windows host. The `-m` switch is for Linux hosts only. The most convenient way to use the switches is to incorporate them into the command generated by a Windows shortcut.

Create the shortcut, right-click the shortcut, then click **Properties**. In the **Target** field, add any switches you want to use after the `vmware.exe` filename. For example,

```
"C:\Program Files\VMware\VMware Workstation\Programs\vmware.exe -X
C:\Documents and Settings\<username>\My Documents\My Virtual
Machines\Windows Me\Windows Me.vmx"
```

launches the Windows Me virtual machine specified, powers it on automatically and switches to full screen mode.

Be sure to enclose the entire command string in quotation marks.

Note: On Windows, the configuration file has a `.vmx` extension by default. Path names on Windows use the backslash character (`\`). X toolkit options are not relevant on a Windows host.

Keyboard Shortcuts

If you prefer to work from the keyboard as much as possible, you may find the following keyboard shortcuts handy. If you have changed the Preferences setting for the hot-key combination, substitute your new setting for Ctrl-Alt as needed in the shortcuts listed here.

Shortcut	Action
Ctrl-B	Power on.
Ctrl-E	Power off.
Ctrl-R	Reset the power.
Ctrl-Z	Suspend.
Ctrl-N	Create a new virtual machine.
Ctrl-O	Open a virtual machine.
Ctrl-F4	Close the current virtual machine.
Ctrl-D	Edit the virtual machine's configuration.
Ctrl-G	Grab input from keyboard and mouse.
Ctrl-P	Edit preferences.
Ctrl-Alt-Enter	Go to full screen mode.
Ctrl-Alt	Return to normal (windowed) mode.
Ctrl-Alt-Tab	Switch among open virtual machines while mouse and keyboard input are grabbed.
Ctrl-Tab	Switch among open virtual machines while mouse and keyboard input are not grabbed. VMware Workstation must be the active application.
Ctrl-Shift-Tab	Switch among open virtual machines while mouse and keyboard input are not grabbed. VMware Workstation must be the active application.

Shortcut	Action
Ctrl-Alt-Fx	**Linux hosts:** Switch among open virtual machines while using full screen mode. Fx is a function key corresponding to the virtual machine you want to use. The key combination to use for a virtual machine is shown in the VMware Workstation title bar when that virtual machine is active and in normal (windowed) mode. **Windows hosts:** For similar functionality, see Using Full Screen Switch Mode on page 334.

CHAPTER 6

Moving and Sharing Virtual Machines

The following sections provide 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:

- Considerations for Moving Disks in Undoable Mode on page 142
- Sharing Virtual Machines with Other Users on page 144

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 Workstation generates a different MAC address for the virtual Ethernet adapter. For additional information, see Maintaining and Changing the MAC Address of a Virtual Machine on page 232.

Moving a VMware Workstation 4 Virtual Machine

What do you do if you have created a virtual machine using VMware Workstation and you want to move it to a different computer? Or even somewhere else on the same computer? 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. If the virtual machine was created under VMware Workstation 4, follow the directions in this section.

Note: These instructions assume that you are using a virtual disk — stored in a set of `.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.

Virtual Machines Use Relative Paths

The path names for all files associated with a VMware Workstation 4 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 operating system.
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. Otherwise, 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 if they are not too large.

     Once you know how you are going to move the virtual machine, go to Moving a Virtual Machine to a New Host Machine on page 136.
   - 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 VMware Workstation and open the new virtual machine you just created. Choose **File** > **Open**, then browse to the virtual machine's configuration (`.vmx`) file.

Moving a Virtual Machine to a New Host Machine

1. Make sure VMware Workstation is installed and working correctly on the new host computer.
2. Create a directory 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.

   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 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. Start VMware Workstation and open the virtual machine you just moved. Choose **File** > **Open**, then browse to the virtual machine's configuration (`.vmx`) file.

Moving a VMware Workstation 3.1 or 3.2 Virtual Machine

If you want to move a virtual machine created with VMware Workstation 3.1 or 3.2, you may prefer to upgrade it for full compatibility with VMware Workstation 4 before moving it. To do so, run the virtual machine under VMware Workstation 4 and use **VM** > **Upgrade Virtual Hardware**. If you upgrade the virtual hardware, you can then follow the instructions in Moving a VMware Workstation 4 Virtual Machine on page 135.

If you upgrade the virtual machine, you can no longer run it under VMware Workstation 3. If you need to run the virtual machine under both VMware Workstation 3 and VMware Workstation 4, do not upgrade the virtual hardware. Follow the instructions in this section.

Note: These instructions assume that you are using a virtual disk — stored in a set of `.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.

Virtual Machines May Have Relative or Absolute Paths

Before VMware Workstation 3.1, 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\<user name>\My Documents\My Virtual Machines\<machine name>\<machine name>.vmdk`.

With VMware Workstation 3.1 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`.

If you intend to move virtual machines created in a VMware product other than VMware Workstation 3.1 or higher (even VMware Workstation 3.0), see Moving an Older Virtual Machine on page 140.

Preparing Your Virtual Machine for the Move

1. Use VMware Workstation 3 to open 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 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 142.

   Note: If your disks are using nonpersistent mode, you must also move the redo-log (`.REDO`) file to the new host computer. By default, it is located in your host operating system's `temp` directory.
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. Otherwise, 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 if they are not too large.

     Once you know how you are going to move the virtual machine, go to Moving a Virtual Machine to a New Host Machine on page 138.
   - 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.

     Start VMware Workstation 4 and open the virtual machine you just moved. Choose **File** > **Open**, then browse to the virtual machine's configuration (`.vmx`) file.

Moving a Virtual Machine to a New Host Machine

1. Make sure VMware Workstation is installed and working correctly on the new host computer.
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.

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 Workstation 3. If you cannot commit or discard the changes to your disk, read Considerations for Moving Disks in Undoable Mode on page 142.

3. Start VMware Workstation 4 and open the virtual machine you just moved. Choose **File** > **Open**, then browse to the virtual machine's configuration (`.vmx`) file.

Moving an Older Virtual Machine

If you have created a virtual machine using VMware Workstation 2, you must upgrade the virtual hardware the first time you run it under VMware Workstation 4. Once you have done this, you can follow the instructions in Moving a VMware Workstation 4 Virtual Machine on page 135.

If you have created a virtual machine using VMware Workstation 3.0, 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` 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.

Preparing Your Virtual Machine for the Move

1. Use VMware Workstation 3 to open 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 virtual machine settings 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 142.
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. Otherwise, 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 if they are not too large.

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 Workstation 4 is installed and working correctly on the new host computer.
2. Run the New Virtual Machine Wizard and 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 size and type (IDE or SCSI) that matches the size and 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 VMware Workstation.
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.

   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. Start VMware Workstation 4 again and open the new virtual machine you just created. Go to **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 file name 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. To specify IDE or SCSI, when you reach the Disk File screen in the wizard, click the **Advanced** button.

   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 a 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 may 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. This is true for virtual machines created under VMware Workstation 3.1 or higher; however, virtual machines created with older versions of Workstation or any other VMware product contain full path names.

Follow these steps to check the configuration and see whether or not you can move your undoable disk without committing or discarding changes:

1. Start VMware Workstation 3.

   If you are moving a disk in undoable mode from one computer to another computer, start VMware Workstation 3 on the computer that currently has your disk.

2. Open the configuration file for the virtual machine that uses the undoable mode disk you wish to move.

   In the VMware Workstation window, select **File** > **Open** and choose the configuration file of the virtual machine with the disk you want to move.

3. Open the virtual machine settings 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 Me\Windows Me.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 (Windows to Windows or Linux to Linux).
- You must place the virtual machine's other files (including `.vmx` and `.REDO` on Windows, `.vmx` 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 Me\`
  on the original host computer, you must place them in that same location on the new host computer.
- You cannot move the disk to a computer of a different type (Windows to Linux or vice versa).
- 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 Me.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 create a virtual machine, by default all the files associated with it are placed in `C:\Documents and Settings\<user name>\My Documents\My Virtual Machines`. Other users typically do not have access to this folder. 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 Workstation 3 or another VMware product and uses disks in nonpersistent mode, you should consider changing the location of the redo-log file, since by default it is placed in your temp directory, to which other users may not have access (redo-log files for disks in undoable mode are placed in the same directory as the virtual machine's configuration file). 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.

  Note: VMware Workstation 3 virtual machines with disks in nonpersistent mode perform better when the redo-log files for those disks are located in the system's temp directory.

CHAPTER 7

Using Disks

The following sections provide information on configuring your virtual machine's hard disk storage so it best meets your needs:

Configuring Hard Disk Storage in a Virtual Machine

Like a physical computer, a VMware Workstation virtual machine stores its operating system, programs and data files on one or more hard disks. Unlike a physical computer, VMware Workstation gives you options for undoing changes to the virtual machine's hard disk.

The New Virtual Machine Wizard creates a virtual machine with one disk drive. You can use the virtual machine settings editor (**VM** > **Settings**) to add more disk drives to your virtual machine, to remove disk drives from your virtual machine or to change certain settings for the existing disk drives.

This section describes the choices you can make in setting up hard disk storage for your virtual machine.

Disk Types: Virtual and Physical

In the most common configurations, VMware Workstation creates virtual hard disks, which are made up of files that are typically stored on your host computer's hard disk. In some circumstances, you may need to give your virtual machine direct access to a physical hard drive on your host computer — using the disk type also referred to as a raw disk.

Virtual Disk

A virtual disk is a file or set of files that appears as a physical disk drive to a guest operating system. The files can be on the host machine or on a remote computer. When you configure a virtual machine with a virtual disk, you can install a new operating system onto the virtual disk without repartitioning a physical disk or rebooting the host.

IDE virtual disks can be as large as 128GB. SCSI virtual disks can be as large as 256GB. Depending on the size of the virtual disk and the host operating system, VMware Workstation creates one or more files to hold each virtual disk.

By default, the actual files used by the virtual disk start out small and grow to their maximum size as needed. The main advantage of this approach is the smaller file size. Smaller files require less storage space and are easier to move if you want to move the virtual machine to a new location. However, it takes longer to write data to disk configured in this way.

You may also configure virtual disks so all the disk space is allocated at the time the virtual disk is created. This approach provides enhanced performance and is useful if

you are running performance-sensitive applications in the virtual machine. Virtual disks created in this way are similar to the experimental plain disks that could be created under VMware Workstation 2.

Virtual disks can be set up as IDE disks for any guest operating system. They can be set up as SCSI disks for any guest operating system that has a driver for the LSI Logic or BusLogic SCSI adapter available in a VMware Workstation virtual machine. You determine which SCSI adapter to use at the time you create the virtual machine.

Note: To use SCSI disks in a Windows XP or Windows Server 2003 virtual machine, you need a special SCSI driver available from the download section of the VMware Web site at *www.vmware.com/download*. Follow the instructions on the Web site to use the driver with a fresh installation of Windows XP or Server 2003.

A virtual disk of either type can be stored on either type of physical hard disk. That is, the files that make up an IDE virtual disk can be stored on either an IDE hard disk or a SCSI hard disk. So can the files that make up a SCSI virtual disk. They can also be stored on other types of fast-access storage media, such as DVD-ROM or CD-ROM discs.

A key advantage of virtual disks is their portability. Because the virtual disks are stored as files on the host machine or a remote computer, you can move them easily to a new location on the same computer or to a different computer. You can also use VMware Workstation on a Windows host to create virtual disks, then move them to a Linux computer and use them under VMware Workstation for Linux — or vice versa. For information about moving virtual disks, see Moving and Sharing Virtual Machines on page 133.

Raw Disk

A raw disk directly accesses an existing local disk or partition. You can use raw disks if you want VMware Workstation to run one or more guest operating systems from existing disk partitions. Raw disks may be set up on both IDE and SCSI devices. At this time, however, booting from an operating system already set up on an existing SCSI disk or partition is not supported.

The most common use of a raw disk is for converting a dual-boot or multiple-boot machine so one or more of the existing operating systems can be run inside a virtual machine.

Caution: If you run an operating system natively on the host computer, then switch to running it inside a virtual machine, the change is like pulling the hard drive out of one computer and installing it in a second computer with a different motherboard and other hardware. You need to prepare carefully for such a switch. The specific steps you need to take depend on the operating system you want to use inside the virtual

machine. For details, see Configuring a Dual-Boot Computer for Use with a Virtual Machine on page 169.

You can also create a new virtual machine using a raw disk. For details, see Installing an Operating System onto a Raw Partition from a Virtual Machine on page 190. In most cases, however, it is better to use a virtual disk.

Only expert users should attempt raw disk configurations.

Note: You should not use a raw disk to share files between host and guest operating systems. It is not safe to make the same partition visible to both host and guest. You can cause data corruption if you do this. To share files between host and guest operating systems, use shared folders. For details, see Using Shared Folders on page 113.

File Locations

Disk Files

The virtual machine settings editor (**VM** > **Settings**) allows you to choose the disk files for a virtual machine.

You may want to choose a file other than the one created by the New Virtual Machine Wizard if you are using a virtual disk that you created in a different location or if you are moving the automatically created disk files to a new location.

The disk files for a virtual disk store the information that you write to a virtual machine's hard disk — the operating system, the program files and the data files. The virtual disk files have a `.vmdk` extension.

A virtual disk is made up of one or more `.vmdk` files.

On Windows hosts, each virtual disk is contained in one file by default. You may, as an option, configure the virtual disk to use a set of files limited to 2GB per file. Use this option if you plan to move the virtual disk to a file system that does not support files larger than 2GB.

You must set this option at the time the virtual disk is created.

If you are setting up a new virtual machine, in the New Virtual Machine Wizard follow the **Custom** path. In the screen that allows you to specify the virtual disk's capacity, select **Split disk into 2GB files**.

If you are adding a virtual disk to an existing virtual machine, follow the steps in the Add Hardware Wizard. In the screen that allows you to specify the virtual disk's capacity, select **Split disk into 2GB files**.

When a disk is split into multiple files, larger virtual disks have more `.vmdk` files.

The first `.vmdk` file for each disk is small and contains pointers to the other files that make up the virtual disk. The other `.vmdk` files contain data stored by your virtual machine and use a small amount of space for virtual machine overhead.

If you chose to allocate space for the virtual disk in advance, the file sizes are fixed, and most of the files are 2GB. As mentioned above, the first file is small. The last file in the series may also be smaller than 2GB.

If you did not allocate the space in advance, the `.vmdk` files grow as data is added, to a maximum of 2GB each — except for the first file in the set, which remains small.

The virtual machine settings editor shows the name of the first file in the set — the one that contains pointers to the other files in the set. The other files used for that disk are automatically given names based on the first file's name.

For example, a Windows XP Professional virtual machine using the default configuration, with files that grow as needed, stores the disk in files named `Windows XP Professional.vmdk`, `Windows XP Professional-s001.vmdk`, `Windows XP Professional-s002.vmdk` and so on.

If the disk space is allocated in advance, the names are similar, except that they include an `f` instead of an `s` — for example, `Windows XP Professional-f001.vmdk`.

If your virtual machine uses files created under earlier VMware products, with a `.dsk` extension, the filenames can be updated automatically on a Windows host. For details, see Updating Filenames for Virtual Disks Created with Earlier VMware Products on page 151.

If you are using a raw disk, the `.vmdk` file stores information about the physical disk or partition used by the virtual machine.

Lock Files

A running virtual machine creates lock files to prevent consistency problems on virtual disks. If the virtual machine did not use locks, multiple virtual machines might read and write to the disk, causing data corruption.

Lock files are always created in the same directory as the `.vmdk` file.

The locking methods used by VMware Workstation on Windows and Linux hosts are different, so files shared between them are not fully protected. If you use a common file repository that provides files to users on both Windows and Linux hosts, be sure that each virtual machine is run by only one user at a time.

When a virtual machine is powered off, it removes the lock files it created. If it cannot remove the lock, a stale lock file is left protecting the `.vmdk` file. For example, if the

host machine crashes before the virtual machine has a chance to remove its lock file, a stale lock remains.

If a stale lock file remains when the virtual machine is started again, the virtual machine tries to remove the stale lock. To make sure that no virtual machine could be using the lock file, the virtual machine checks the lock file to see if

1. The lock was created on the same host where the virtual machine is running.
2. The process that created the lock is not running.

If those two conditions are true, the virtual machine can safely remove the stale lock. If either of those conditions is not true, a dialog box appears, warning you that the virtual machine cannot be powered on. If you are sure it is safe to do so, you may delete the lock files manually. On Windows hosts, the filenames of the lock files end in `.lck`. On Linux hosts, the filenames of the lock files end in `.WRITELOCK`.

Raw disk partitions are also protected by locks. However, the host operating system is not aware of this locking convention and thus does not respect it. For this reason, VMware strongly recommends that the raw disk for a virtual machine not be installed on the same physical disk as the host operating system.

Updating Filenames for Virtual Disks Created with Earlier VMware Products

Except for VMware Workstation 3, previous VMware products, including VMware Workstation 2, named virtual disk files with a `.dsk` extension. To avoid conflicts with the System Restore feature on Windows XP and Windows Server 2003 hosts, VMware Workstation now uses a `.vmdk` extension for those files. VMware Workstation 4 updates existing virtual disk files automatically. It also automatically updates references to the virtual disk files in the configuration files for the virtual machine.

In addition, VMware Workstation converts the filename extensions for the files that store the state of a suspended virtual machine. The old extension was `.std`. The extension is now `.vmss`.

If your host computer is running Windows XP or Windows Server 2003, VMware Workstation must turn off System Restore on the host computer while it runs the updater. If this were not done and you restored the host to a restore point that was set sometime before you ran the updater, the System Restore feature would rename your virtual disk files to use the `.dsk` extension. You would again have the conflict the updater was designed to solve.

Note: Because the VMware Workstation updater turns off the System Restore feature while it runs, all existing restore points are deleted.

System Restore is turned back on after the updater completes its work.

Running the Updater at a Later Time

On a Windows host computer, you can run the filename updater at any time. To do so, follow these steps.

1. Open a command prompt.
2. Change to the folder in which the VMware Workstation program files are installed. If you installed the files in the default locations, use this command:

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

3. Run the updater.

   ```
   dskrename.exe
   ```

Defragmenting and Shrinking Virtual Disks

If you have a virtual disk that grows as data is added, you can defragment and shrink it as described in this section. If you allocated all the space for your virtual disk at the time you created it, you cannot defragment and shrink it.

To defragment the virtual disks attached to a virtual machine, power off the virtual machine, then go to the virtual machine settings editor (**VM** > **Settings**).

Select the virtual disk you want to defragment, then click **Defragment**.

Defragmenting disks may take considerable time.

Note: The defragmentation process requires free working space on the host computer's disk. If your virtual disk is contained in a single file, for example, you need free space equal to the size of the virtual disk file. Other virtual disk configurations require less free space.

When a virtual machine is powered on, you can shrink its virtual disks from the VMware Tools control panel. You cannot shrink virtual disks if a snapshot exists. To remove the snapshot if one exists, choose **Snapshot** > **Remove Snapshot**.

1. To launch the control panel in a Windows guest, double-click the VMware Tools icon in the system tray or choose **Start** > **Settings** > **Control Panel**, then double-click **VMware Tools**.

   To launch the control panel in a Linux or FreeBSD guest, become root (`su`), then run `vmware-toolbox`.

2. Click the **Shrink** tab.
3. Select the virtual disks you want to shrink, then click **Prepare to Shrink**.

The shrink tool reclaims unused space in the virtual disk. If there is empty space in the disk, this process reduces the amount of space the virtual disk occupies on the host drive.

Shrinking disks may take considerable time.

In some configurations, it is not possible to shrink virtual disks. If your virtual machine uses such a configuration, the Shrink tab displays information explaining why you cannot shrink your virtual disks.

For best disk performance, you can take the following three actions, in the order listed:

1. Run a disk defragmentation utility inside the virtual machine.
2. Use the VMware Workstation defragmentation tool. Go to **VM** > **Settings**, click the listing for the virtual disk you want to defragment, then click **Defragment**.
3. Run a disk defragmentation utility on the host computer.

Adding Drives to a Virtual Machine

VMware Workstation virtual machines can use up to four IDE devices and up to seven SCSI devices. Any of these devices can be a virtual hard disk or DVD or CD-ROM drive. A virtual machine can read data from a DVD-ROM disc. VMware Workstation does not support playing DVD movies in a virtual machine.

Many other SCSI devices can be connected to a virtual machine using the host operating system's generic SCSI driver. For details on connecting these devices, see Connecting to a Generic SCSI Device on page 302.

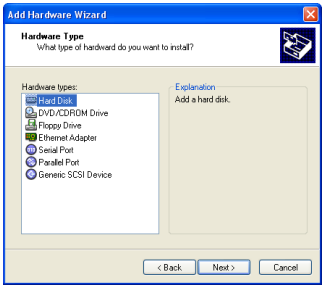
Adding Virtual Disks to a Virtual Machine

Virtual disks are stored as files on the host computer or on a network file server. It does not matter whether the physical disk that holds the files is IDE or SCSI. A virtual IDE drive can be stored on an IDE drive or on a SCSI drive. So can a virtual SCSI drive.

Use the virtual machine settings editor (**VM** > **Settings**) to add a new virtual disk to your virtual machine. The virtual machine should be powered off before you begin. If it is not, shut down the guest operating system normally, then click **Power Off** on the VMware Workstation toolbar.

Note: If you have a Windows NT 4.0 guest with a SCSI virtual disk, you cannot add both an additional SCSI disk and an IDE disk to the configuration.

1. Open the virtual machine settings editor (**VM** > **Settings**) and click **Add**. The Add Hardware Wizard guides you through the steps to create your virtual disk.



2. Click **Hard Disk**, then click **Next**.
3. Select **Create a New Virtual Disk**, then click **Next**.
4. Choose whether you want the virtual disk to be an IDE disk or a SCSI disk.
5. Set the capacity for the new virtual disk.

   If you wish, select **Allocate all disk space now**.

Allocating all the space at the time you create the virtual disk gives somewhat better performance, but it requires as much disk space as the size you specify for the virtual disk.

If you do not select this option, the virtual disk's files start small and grow as needed, but they can never grow larger than the size you set here.

You can set a size between 2GB and 256GB for a SCSI virtual disk or 128GB for an IDE virtual disk. The default is 4GB.

You may also specify whether you want the virtual disk created as one large file or split into a set of 2GB files. You should split your virtual disk if it is stored on a FAT32 file system.

6. Accept the default filename and location for the virtual disk file or change it, if you want to use a different name or location. To find a different folder, click **Browse**.

   If you want to specify a device node for your virtual disk, click **Advanced**.

   On the advanced settings screen, you can also specify a disk mode. This is useful in certain special-purpose configurations in which you want to exclude disks from the snapshot. For more information on the snapshot feature, see Using the Snapshot on page 200.

   Normal disks are included in the snapshot. In most cases, this is the setting you want — with **Independent** deselected.

   Independent disks are not included in the snapshot. If you select **Independent**, you have the following options:

   - **Persistent** — changes are immediately and permanently written to the disk.
   - **Nonpersistent** — changes to the disk are discarded when you power off or revert to the snapshot.

   When you have set the filename and location you want to use and have made any selections you want to make on the advanced settings screen, click **Finish**.

7. The wizard creates the new virtual disk. It appears to your guest operating system as a new, blank hard disk. Use the guest operating system's tools to partition and format the new drive for use.

Adding Raw Disks to a Virtual Machine

Use the virtual machine settings editor (**VM** > **Settings**) to add a new raw disk to your virtual machine. The virtual machine should be powered off before you begin. If it is

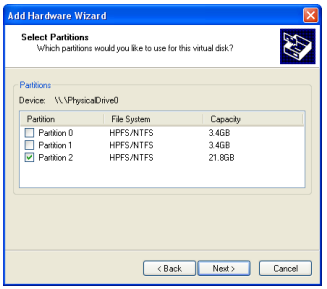
not, shut down the guest operating system normally, then click **Power Off** on the VMware Workstation toolbar.

Caution: Raw disks are an advanced feature and should be configured only by expert users.

1. Open the virtual machine settings editor (**VM** > **Settings**) and click **Add**. The Add Hardware Wizard guides you through the steps to create your virtual disk.
2. Click **Hard Disk**, then click **Next**.

3. Select **Use a physical disk**, then click **Next**.

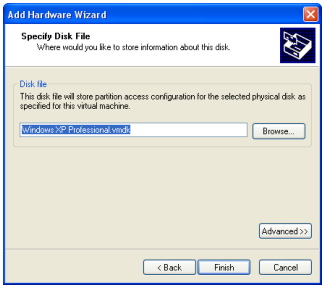
4. Choose the physical hard disk to use from the drop-down list. Select whether you want to use the entire disk or use only individual partitions on the disk. Click **Next**.



5. If you selected **Use individual partitions** in the previous step, select which partitions you want to use in the virtual machine. If you selected **Use entire disk**, this step does not appear.

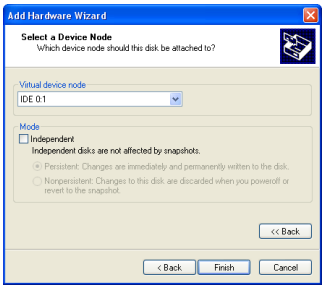
   Only the partitions you select in this step are visible to the virtual machine. All other partitions are hidden from it.

   Click **Next**.



6. Accept the default filename and location for the file that stores access information for this raw disk — or change it, if you want to use a different name or location. To find a different directory, click **Browse**.

   Click **Advanced** if you want to specify the virtual machine SCSI or IDE device node to which this disk is connected.



   On the advanced settings screen, you can also specify a disk mode. This is useful in certain special-purpose configurations in which you want to exclude disks from the snapshot. For more information on the snapshot feature, see Using the Snapshot on page 200.

   Normal disks are included in the snapshot. In most cases, this is the setting you want — with **Independent** deselected.

   Independent disks are not included in the snapshot. If you select **Independent**, you have the following options:

   - **Persistent** — changes are immediately and permanently written to the disk.
   - **Nonpersistent** — changes to the disk are discarded when you power off or revert to the snapshot.

   When you have set the filename and location you want to use and have made any selections you want to make on the advanced settings screen, click **Finish**.

7. The wizard configures the new raw disk. If the partitions used on the raw disk are not formatted for your guest operating system, use the guest operating system's tools to format them.

Note: After you create a raw disk using one or more partitions on a physical disk, you should never modify the partition tables by running `fdisk` or a similar utility in the guest operating system.

Note: If you use `fdisk` or a similar utility on the host operating system to modify the partition table of the physical disk, you must recreate the virtual machine's raw disk.

Adding DVD or CD Drives to a Virtual Machine

You can add one or more DVD or CD drives to your virtual machine. You can connect the virtual machine's drive to a physical drive on the host machine or to an ISO image file.

You can configure the virtual DVD or CD drive as either IDE or SCSI, no matter what kind of physical drive you connect it to. In other words, if your host computer has an IDE CD drive, you can set up the virtual machine's drive as either SCSI or IDE and connect it to the host's drive. The same is true if the host's physical drive is a SCSI drive.

Adding a DVD or CD Drive

1. Open the virtual machine settings editor (**VM** > **Settings**) and click **Add** to start the Add Hardware Wizard.
2. Click **DVD/CD-ROM Drive**, then click **Next**.
3. Select **Use physical drive** if you want to connect the virtual machine's drive to a physical drive on the host computer. Select **Use ISO Image** if you want to connect the virtual machine's drive to an ISO image file.
4. Do one of the following:
   - If you selected **Use physical drive**, choose the drive you want to use from the drop-down list or choose **Auto detect**.

     If you do not want the CD drive connected when the virtual machine starts, deselect **Connect at power on**.

     Click **Advanced** if you want to specify the device node the drive should use in the virtual machine.

     On the advanced settings screen you may also select **Legacy emulation**. This is necessary only if you have had problems using normal mode. The legacy emulation mode does not support all the capabilities of normal mode. For example, if you are using legacy emulation mode, you cannot record CDs, you cannot read multisession CDs, you cannot extract digital audio from a CD and you cannot read or write DVDs. For details, see Legacy Emulation for DVD and CD Drives on page 160.

     After you have made any desired changes in these settings, click **Finish**.
   - If you selected **Use ISO Image**, enter the path and filename for the image file or click **Browse** to navigate to the file.

     If you do not want the CD drive connected when the virtual machine starts, deselect **Connect at power on**.

Click **Advanced** if you want to specify the device node the drive should use in the virtual machine.

After you have made any desired changes in these settings, click **Finish**.

5. The drive is set up initially so it appears to the guest operating system as an IDE drive. If you want it to appear to the guest operating system as a SCSI drive, click the drive's entry in the virtual machine settings editor and make that change in the settings panel on the right.

Legacy Emulation for DVD and CD Drives

The virtual machine settings editor (**VM** > **Settings**) provides a **Legacy emulation** option for DVD and CD drives attached to the virtual machine.

On Windows hosts, this option is deselected by default.

On Linux hosts with IDE drives, the default setting for this option depends on whether the ide-scsi module is loaded in your kernel. The ide-scsi module must be loaded — or you must be using a physical SCSI drive — if you want to connect to the DVD or CD drive in raw mode.

If you encounter problems using your DVD or CD drive, try selecting **Legacy emulation**.

Note that in legacy emulation mode, you can read from data discs in the DVD or CD drive, but some other functions are not available.

When **Legacy emulation** is deselected, the guest operating system communicates directly with the drive. This direct communication enables capabilities that are not possible in legacy emulation mode, such as using CD and DVD writers to burn discs, reading multisession CDs, performing digital audio extraction and viewing video.

However, in some cases, the DVD or CD drive may not work correctly when the guest operating system is communicating directly with the drive. In addition, certain drives and their drivers do not work correctly in raw mode. Selecting **Legacy emulation** is a way to work around these problems.

If you run more than one virtual machine at a time, and if their CD drives are in legacy emulation mode, you may prefer to start the virtual machines with their CD drives disconnected. This ensures that you do not have multiple virtual machines connected to the CD drive at the same time.

Adding Floppy Drives to a Virtual Machine

You can add floppy drives to your virtual machine, to a total of two floppy drives. A virtual floppy drive can connect to a physical floppy drive on the host computer, to an existing floppy image file or to a blank floppy image file.

Adding a Floppy Drive

1. Open the virtual machine settings editor (**VM** > **Settings**) and click **Add** to start the Add Hardware Wizard.
2. Click **Floppy Drive**, then click **Next**.
3. Select what you want to connect to — a physical floppy drive on the host computer, an existing floppy image file or a new floppy image file. Click **Next**.
4. If you selected **Use a physical floppy drive**, choose the drive's letter (on a Windows host) or device name (on a Linux host) from the drop-down list, then click **Finish**.

   If you selected **Use a floppy image**, type the path and filename for the floppy image file you want to use or click **Browse** to navigate to the file. Click **Finish**.

   If you selected **Create a blank floppy image**, use the default path and filename or type in a new one. To navigate to a location, click **Browse**. When the field contains the path and filename you want to use for the new floppy image file, click **Finish**.

Note: By default, only one floppy drive is enabled in the virtual machine's BIOS. If you are adding a second floppy drive to the virtual machine, click inside the virtual machine window and press F2 as the virtual machine boots to enter the BIOS setup utility. On the main screen, choose **Legacy Diskette B:** and use the plus (+) and minus (-) keys on the numerical keypad to select the type of floppy drive you want to use. Then press F10 to save your changes and close the BIOS setup utility.

Connecting a CD-ROM or Floppy Drive to an Image File

You can use the virtual machine settings editor to connect an existing virtual CD-ROM or floppy drive to an image file.

You can connect a virtual CD-ROM drive to an ISO image file.

Connecting to an ISO Image File

1. Open the virtual machine settings editor (**VM** > **Settings**) and select the DVD/CD-ROM drive you want to connect to the image file.
2. Select **Use ISO Image** and enter the path and filename for the image file or click **Browse** to navigate to the file.
3. Click **OK** to save the configuration and close the virtual machine settings editor.

Connecting to a Floppy Image File

1. Open the virtual machine settings editor (**VM** > **Settings**) and select the floppy drive you want to connect to an image file.

2. Type the path and filename for the floppy image file you want to use or click **Browse** to navigate to the file.

   If you want to create a new image file, click **Create**. Use the default filename and folder or change them as you wish.

3. Click **Finish**.

Using VMware Virtual Disk Manager

VMware Virtual Disk Manager is a utility in VMware Workstation that allows you to create, manage and modify virtual disk files from the command line or within scripts.

One key feature is the ability to enlarge a virtual disk so its maximum capacity is larger than it was when you created it. This way, if you find you need more disk space in a given virtual machine, but you do not want to add another virtual disk or use ghosting software to transfer the data on a virtual disk to a larger virtual disk, you can instead change the maximum size of the virtual disk. This is something you cannot do with physical hard drives.

Another feature allows you to change disk types. When you create a virtual machine, you specify how disk space is allocated. You select one of the following:

- All space for the virtual disk is allocated in advance. This corresponds to what the virtual disk manager calls the preallocated disk type.
- Space allocated for the virtual disk begins small and grows as needed. This corresponds to what the virtual disk manager calls the growable disk type.

With virtual disk manager you can change whether the virtual disk type is preallocated or growable and whether the virtual disk is stored in a single file or split into 2GB files. For example, you may have allocated all the disk space for a virtual disk, then find that you need to reclaim some hard disk space on the host. You can convert the preallocated virtual disk into a growable disk, then remove the original virtual disk file. The new virtual disk is large enough to contain all the data in the original virtual disk. The virtual disk grows in size as you add data to it.

These features and the ability to use scripting to automate management of virtual disks were added to VMware Workstation in version 4.5.2.

You can use the virtual disk manager for the following tasks:

- Automate the management of virtual disks with scripts.
- Create virtual disks that are not associated with a particular virtual machine, to be used as templates, for example.
- Switch the virtual disk type from preallocated to growable, or vice versa. When you change the disk type to growable, you reclaim some space on the virtual disk. You can shrink the virtual disk to reclaim even more disk space.
- Expand the size of a virtual disk so it is larger than the size specified when you created it.
- Defragment virtual disks.

- Prepare and shrink virtual disks without powering on the virtual machine. (Windows hosts only.)

You can use the virtual disk manager with virtual disks created under VMware GSX Server, VMware Workstation and VMware VirtualCenter (provided the virtual disk was created on a GSX Server host managed by VirtualCenter).

You cannot use the virtual disk manager to create physical (raw) disks. Physical disks cannot be shrunk by the virtual disk manager or by Workstation.

Running the VMware Virtual Disk Manager Utility

To run the VMware Virtual Disk Manager utility, open a command prompt or terminal on the host operating system. On a Windows host, change to the directory where you installed your Workstation software. By default, this directory is `C:\Program Files\VMware\VMware Workstation`.

The command syntax is:

```
vmware-vdiskmanager [options]
```

The options you can or must use include the following:

Options/Parameters	Description
`<diskname>`	The name of the virtual disk file. The virtual disk file must have a `.vmdk` extension. You can specify a path to the folder where you want to store the disk files. If you mapped a network share on your host operating system, you can create the virtual disk on that share by providing the correct path information with the disk file name.
`-c`	Creates the virtual disk. You must use the `-a`, `-s` and `-t` options, and you must specify the name of the virtual disk (`<diskname>`).
`-r <sourcediskname>`	Converts the specified virtual disk, creating a new virtual disk as a result. You must use the `-t` option to specify the disk type to which the virtual disk is converted and you must specify the name of the target virtual disk (`<targetdiskname>`). Once the conversion is completed and you have tested the converted virtual disk to make sure it works as expected, you can delete the original virtual disk file. In order for the virtual machine to recognize the converted virtual disk, you should use the virtual machine settings editor to remove the existing virtual disk from the virtual machine, then add the converted disk to the virtual machine. For information on adding virtual disks to a virtual machine, see Adding Drives to a Virtual Machine on page 154.

Options/Parameters	Description
`-x <n>[GB|MB] <diskname>`	Expands the virtual disk to the specified capacity. You must specify the new, larger size of the virtual disk in gigabytes or megabytes. You cannot change the size of a physical (raw) disk. **Caution:** Before running the virtual disk manager utility, you should back up your virtual disk files.
`-d <diskname>`	Defragments the specified virtual disk. You can defragment only growable virtual disks. You cannot defragment preallocated virtual disks.
`-p <mountpoint>`	Prepares a virtual disk for shrinking. If the virtual disk is partitioned into volumes, each volume must be prepared separately. The volume (C: or D:, for example) must be mounted by VMware DiskMount at `<mountpoint>`. After you prepare the volume, unmount it with VMware DiskMount. Continue mounting each volume of the virtual disk and preparing it for shrinking until you complete this process for all the volumes of the virtual disk. You can mount only one volume of a virtual disk at a time with VMware DiskMount. You can prepare volumes of virtual disks for shrinking on Windows hosts only.
`-k <diskname>`	Shrinks the specified virtual disk. You can shrink only growable virtual disks. You can shrink virtual disks on Windows hosts only. You cannot shrink a virtual disk if the virtual machine has a snapshot. To keep the virtual disk in its current state, simply remove the snapshot. To discard changes made since you took the snapshot, revert to the snapshot.
`-a [ide|buslogic|lsilogic]`	Specifies the disk adapter type. You must specify an adapter type when creating a new virtual disk. Choose one of the following types: • `ide` — for an IDE adapter. • `buslogic` — for a BusLogic SCSI adapter. • `lsilogic` — for an LSI Logic SCSI adapter.
`-s <n>[GB|MB]`	Specifies the size of the virtual disk. Specify whether the size `<n>` is in `GB` (gigabytes) or `MB` (megabytes). You must specify the size of a virtual disk when you create it. Even though you must specify the size of a virtual disk when you expand it, you do not use the `-s` option.

Options/Parameters	Description
`-t [0|1|2|3]`	You must specify the type of virtual disk when you create a new one or reconfigure an existing one. Specify one of the following disk types: `0` — to create a growable virtual disk contained in a single virtual disk file `1` — to create a growable virtual disk split into 2GB files `2` — to create a preallocated virtual disk contained in a single virtual disk file `3` — to create a preallocated virtual disk split into 2GB files
`-q`	Disables virtual disk manager logging. If you keep logging enabled, messages generated by the virtual disk manager are stored in a log file. The name and location of the log file appear in the command prompt or terminal window after the virtual disk manager command is run.

Shrinking Virtual Disks with VMware Virtual Disk Manager

If the virtual disk is located on a Windows host, you can use the virtual disk manager to prepare and shrink virtual disks. You cannot use the virtual disk manager to prepare or shrink virtual disks located on a Linux host. You cannot use the virtual disk manager to shrink physical disks. Shrinking a virtual disk does not reduce the maximum capacity of the virtual disk itself. For more information about shrinking, see Defragmenting and Shrinking Virtual Disks on page 152.

Caution: You cannot shrink a virtual disk if the virtual machine has a snapshot. To keep the virtual disk in its current state, simply remove the snapshot. To discard changes made since you took the snapshot, revert to the snapshot.

You must prepare each volume of the virtual disk (drive C: or D:, for example) for shrinking before you can shrink the disk. To prepare a volume for shrinking, you must first mount it. To mount the volume, use the VMware DiskMount Utility, available as a free download from the VMware Web site. Go to *www.vmware.com/download/diskmount.html*.

The VMware DiskMount user's manual is available from the VMware Web site at *www.vmware.com/pdf/VMwareDiskMount.pdf*. It contains instructions on mounting and unmounting virtual disk volumes with DiskMount.

VMware DiskMount mounts individual volumes of a virtual disk. For the best results when you shrink of a virtual disk, you should mount all the volumes and prepare them for shrinking.

After you mount a virtual disk volume, use the virtual disk manager to prepare the volume for shrinking. Once you prepare a volume, unmount it, then repeat the

process for each volume of the virtual disk. After you prepare all the volumes of the virtual disk, you can shrink the virtual disk. For examples, see Preparing a Virtual Disk for Shrinking on page 167 and Shrinking a Virtual Disk on page 168.

Examples Using the VMware Virtual Disk Manager

The following examples illustrate how to use the virtual disk manager. You run the virtual disk manager from a command prompt.

Creating a Virtual Disk

To create a new virtual disk, use a command like the following:

```
vmware-vdiskmanager -c -t 0 -s 40GB -a ide myDisk.vmdk
```

This creates a 40GB IDE virtual disk named `myDisk.vmdk`. The virtual disk is contained in a single `.vmdk` file. The disk space is not preallocated.

Converting a Virtual Disk

To convert a virtual disk from preallocated to growable, use a command like the following:

```
vmware-vdiskmanager -r -t 0 sourceDisk.vmdk targetDisk.vmdk
```

This converts the disk from its original preallocated type to a growable virtual disk consisting of a single virtual disk file. The virtual disk space is no longer preallocated, and the virtual disk manager reclaims some disk space in the virtual disk so it is only as large as the data contained within it.

Expand the Size of an Existing Virtual Disk

To expand the size of a virtual disk, use a command like the following:

```
vmware-vdiskmanager -x 40GB myDisk.vmdk
```

This increases the maximum capacity of the virtual disk to 40GB.

Defragmenting a Virtual Disk

To defragment a virtual disk, use a command like the following:

```
vmware-vdiskmanager -d myDisk.vmdk
```

Remember, you cannot defragment a virtual disk if you allocated all the disk space when you created the virtual disk. You cannot defragment a physical disk.

Preparing a Virtual Disk for Shrinking

Before you can shrink a virtual disk, you must prepare each volume on the disk (C: or D:, for example) for shrinking. To prepare a volume, it must be located on a Windows host. First you must mount the volume. To mount the volume, use the VMware DiskMount Utility, available as a free download from the VMware Web site. For

information about downloading and using VMware DiskMount, see Shrinking Virtual Disks with VMware Virtual Disk Manager on page 166.

VMware DiskMount mounts individual volumes of a virtual disk. For the best results when you shrink a virtual disk, you should mount all the volumes and shrink them.

After you mount a virtual disk volume, use the virtual disk manager to prepare the disk for shrinking. To prepare the volume mounted as the M: drive for shrinking, use the following command:

```
vmware-vdiskmanager -p M:
```

Once the preparations are complete, unmount the volume. Repeat this process for each volume of the virtual disk. After you prepare all the volumes for shrinking, you can shrink the virtual disk.

Shrinking a Virtual Disk

To shrink a virtual disk, it must be located on a Windows host. Before you can shrink the virtual disk, make sure you prepare all the volumes of the virtual disk for shrinking. Then use a command like the following:

```
vmware-vdiskmanager -k myDisk.vmdk
```

Remember, you cannot shrink a virtual disk if you allocated all the disk space when you created the virtual disk. You cannot shrink a physical (raw) disk.

If the virtual disk has a snapshot, you cannot shrink the virtual disk. You must remove the snapshot before you shrink the virtual disk.

Configuring a Dual-Boot Computer for Use with a Virtual Machine

Many users install VMware Workstation on a dual-boot or multiple-boot computer so they can run one or more of the existing operating systems in a virtual machine. If you are doing this, you may want to use the existing installation of an operating system rather than reinstall it in a virtual machine.

To support such installations, VMware Workstation makes it possible for you to use a physical IDE disk or partition, also known as a raw disk, inside a virtual machine.

Note: VMware Workstation supports booting from raw disk partitions only on IDE drives. Booting guest operating systems from raw SCSI drives is not supported. For a discussion of the issues on a Linux host, see Configuring Dual- or Multiple-Boot SCSI Systems to Run with VMware Workstation on a Linux Host on page 184.

Setting up a raw disk configuration for a virtual machine is more complicated than using a virtual disk. Virtual disks are recommended unless you have a specific need to run directly from a physical disk or partition.

Caution: Raw disks are an advanced feature and should be configured only by expert users.

Using the Same Operating System in a Virtual Machine and on the Host Computer

You may sometimes want to run an operating system inside a virtual machine and at other times want to run that same installation of the operating system by booting the host computer directly into that operating system. If you want to use this approach, you must be aware of some special considerations

The issues arise because the virtual hardware that the operating system sees when it is running in a virtual machine is different from the physical hardware it sees when it is running directly on the host computer. It is as if you were removing the boot drive from one physical computer and running the operating system installed there in a second computer with a different motherboard, video card and other peripherals — then moving it back and forth between the two systems.

The general approach for resolving these issues is to set up profiles for each of the two operating environments — the virtual machine and the physical computer. You can then choose the appropriate profile when you start the operating system. On some hardware, however, booting a previously installed operating system within a virtual machine may not work.

Technical notes in this section document the issues most commonly encountered with various guest operating systems. Read the notes that apply to your guest operating system before you begin to set up your virtual machine.

Before You Begin

Before you begin, be sure to read all the sections listed under the name of the operating system you intend to run as a guest in a virtual machine.

Windows Server 2003

Caution: Running a Windows Server 2003 guest from a raw disk is not supported. You should not test a Windows Server 2003 raw disk configuration in a production environment.

- Configuring Dual- or Multiple-Boot Systems to Run with VMware Workstation on page 171
- Running a Windows 2000, Windows XP or Windows Server 2003 Virtual Machine from an Existing Multiple-Boot Installation on page 180
- Do Not Use Windows 2000, Windows XP and Windows Server 2003 Dynamic Disks as Raw Disks on page 184

Windows XP

Caution: Running a Windows XP guest from a raw disk is not supported. You should not test a Windows XP raw disk configuration in a production environment.

- Configuring Dual- or Multiple-Boot Systems to Run with VMware Workstation on page 171
- Running a Windows 2000, Windows XP or Windows Server 2003 Virtual Machine from an Existing Multiple-Boot Installation on page 180
- Do Not Use Windows 2000, Windows XP and Windows Server 2003 Dynamic Disks as Raw Disks on page 184

Windows 2000

- Configuring Dual- or Multiple-Boot Systems to Run with VMware Workstation on page 171
- Running a Windows 2000, Windows XP or Windows Server 2003 Virtual Machine from an Existing Multiple-Boot Installation on page 180
- Do Not Use Windows 2000, Windows XP and Windows Server 2003 Dynamic Disks as Raw Disks on page 184

Windows NT

- Configuring Dual- or Multiple-Boot Systems to Run with VMware Workstation on page 171

Windows 98

- Configuring Dual- or Multiple-Boot Systems to Run with VMware Workstation on page 171
- Setting Up the SVGA Video Driver for Use with a Windows 98 Guest Operating System Booted from a Raw Disk on page 182

Windows 95

- Configuring Dual- or Multiple-Boot Systems to Run with VMware Workstation on page 171
- Setting Up the SVGA Video Driver for a Windows 95 Guest Operating System Booted from a Raw Disk on page 181

SCSI Systems Using a Linux Host

- Configuring Dual- or Multiple-Boot SCSI Systems to Run with VMware Workstation on a Linux Host on page 184

Other Uses of Raw Disks

It is also possible to install a guest operating system on a raw disk when you plan to use that disk only within a virtual machine. For details on setting up a such a configuration, see Installing an Operating System onto a Raw Partition from a Virtual Machine on page 190.

Configuring Dual- or Multiple-Boot Systems to Run with VMware Workstation

VMware Workstation uses description files to control access to each raw IDE device on the system. These description files contain access privilege information that controls a virtual machine's access to certain partitions on the disks. This mechanism prevents users from accidentally running the host operating system again as a guest or running a guest operating system that the virtual machine was not configured to use. The description file also prevents accidental corruption of raw disk partitions by badly behaved operating systems or applications.

Use the New Virtual Machine Wizard to configure VMware Workstation to use existing raw disk partitions. The wizard guides you though creating a configuration for a new virtual machine including configuring the raw disk description files. Typically, you

rerun the wizard to create a separate configuration for each guest operating system installed on a raw partition.

If a boot manager is installed on the computer system, the boot manager runs inside the virtual machine and presents you with the choice of guest operating systems to run. You must manually choose the guest operating system that this configuration was intended to run.

Windows 2000, Windows XP and Windows Server 2003 Dynamic Disks
If your host is running Windows 2000, Windows XP or Windows Server 2003 and is using dynamic disks, see Do Not Use Windows 2000, Windows XP and Windows Server 2003 Dynamic Disks as Raw Disks on page 184.

Using the LILO Boot Loader
If you are using the LILO boot loader and try to boot a virtual machine from an existing raw partition, you may see `L 01 01 01 01 01 01 ...` instead of a `LILO:` prompt. This can happen regardless of the host operating system. As part of booting a physical PC or a virtual machine, the BIOS passes control to code located in the master boot record (MBR) of the boot device. LILO begins running from the MBR, and in order to finish running correctly, it needs access to the native Linux partition where the rest of LILO is located — usually the partition with the `/boot` directory. If LILO can't access the rest of itself, an error message like the one above appears.

To avoid the problem, follow the configuration steps below and be sure to select the native Linux partition where the rest of LILO is located. The next time the virtual machine tries to boot, the LILO code in the MBR should be able to access the rest of LILO and display the normal `LILO:` prompt.

Configuring a Windows Host
Use the following steps to run a guest operating system from a raw disk.

Note: If you use a Windows host's IDE disk in a raw disk configuration, you must not configure it as the slave on the secondary IDE channel if the master on that channel is a CD-ROM drive.

1. If you are running a Windows guest operating system, read Setting Up Hardware Profiles in Virtual Machines on page 177. You should boot the guest operating system natively on the computer and create a hardware profile for the virtual machine before proceeding.
2. Create a separate configuration for each guest operating system.

To configure a virtual machine to run from a raw disk or disk partition, start the New Virtual Machine Wizard (**File** > **New Virtual Machine**) and select **Custom**.

3. When you reach the Select a Disk step, select **Use a physical disk**.
4. Complete the wizard steps, specifying the appropriate disk or partition to use for this virtual machine.

   Note: The maximum size of an IDE disk in a virtual machine is 128GB.
5. To run multiple guest operating systems from different raw disk partitions, unmap these partitions on the host.

   On a Windows NT host, use the Disk Administrator (**Start** > **Programs** > **Administrative Tools**). First highlight the partition that contains the guest operating system, then select **Assign Drive Letter** from the **Tools** menu. In this form, choose **Do not assign a drive letter** for the partition and click **OK**. The unmapping happens immediately.

   On a Windows Server 2003, Windows XP or Windows 2000 host, use Disk Management (**Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Computer Management** > **Storage** > **Disk Management**). Select the partition you want to unmap, then from the **Action** menu select **All Tasks** > **Change Drive Letter and Path**. Click the **Remove** button.
6. Use the virtual machine settings editor (**VM** > **Settings**) if you want to change any configuration options from the wizard defaults — for example, to change the amount of memory allocated to the guest operating system.
7. If you have multiple IDE drives configured on a system, the VMware BIOS normally attempts to boot them in this sequence:

   a. Primary master

   b. Primary slave

   c. Secondary master

d. Secondary slave

If you have multiple SCSI drives configured on a system, the VMware BIOS normally attempts to boot them in the order of the SCSI device number.

If you have both SCSI and IDE drives configured, the VMware BIOS normally attempts to boot SCSI drives followed by IDE drives, in the order described above.

The boot sequence can be changed in the Boot menu of the virtual machine's Phoenix BIOS. After powering on the virtual machine, press F2 during the BIOS boot in the virtual machine to enter the BIOS setup menu.

8. Power on the virtual machine. Click the **Power On** button. The virtual machine starts, runs the Phoenix BIOS, then boots from the master boot record (MBR).

   Choose the target operating system from the list of options offered by the boot manager.

9. Remember that your virtual machine hardware environment, which the guest operating system is about to run in for the first time, probably differs significantly from the physical hardware of your host computer.

   For Windows guest operating systems, Plug and Play reconfigures Windows. Set up your virtual hardware profile with the devices found and configured by Plug and Play. See Setting Up Hardware Profiles in Virtual Machines on page 177 for more information.

10. Install VMware Tools in your guest operating system.

Warning: If you take a snapshot while using your raw disk, you must either revert to the snapshot or remove the snapshot before you reboot your guest operating system natively. This is necessary because any changes to sectors on the physical disk that have been modified on the disk invalidate the snapshot for the disk.

Configuring a Linux Host

1. If you are running a Windows guest operating system, read Setting Up Hardware Profiles in Virtual Machines on page 177. You should boot the guest operating system natively on the computer and create a hardware profile for the virtual machine before proceeding.
2. Create a separate configuration for each guest operating system.
3. Check operating system partition mounts. Be sure the existing disk partitions that you plan to configure the virtual machine to use are not mounted by Linux.
4. Set the device group membership or device ownership.

The master raw disk device or devices need to be readable and writable by the user who runs VMware Workstation. On most distributions, the raw devices, such as `/dev/hda` (IDE raw disk) and `/dev/sda` (SCSI raw disk) belong to group-id `disk`. If this is the case, you can add VMware Workstation users to the `disk` group. Another option is to change the owner of the device. Please think carefully about security issues when exploring different options here.

Often, the most convenient approach is to grant VMware Workstation users access to all `/dev/hd[abcd]` raw devices that contain operating systems or boot managers and then rely on VMware Workstation's raw disk configuration files to guard access. This provides boot managers access to configuration files and other files they may need to boot the operating systems. For example, LILO needs to read `/boot` on a Linux partition to boot a non-Linux operating system that may be on another drive. As noted above, you should consider the security implications of the configuration you choose.

5. If you plan to run a second Linux installation from an existing partition as a guest operating system and your physical computer's `/etc/lilo.conf` has a memory register statement such as `Append= "mem…"`, you may want to adjust the append memory parameter or create a new entry in LILO for running Linux in a virtual machine.

   If the amount of memory configured in `lilo.conf` exceeds the amount of memory assigned to the virtual machine, then when the virtual machine tries to boot the second Linux installation, the guest operating system will most likely panic.

   You can create another entry in `lilo.conf` for running Linux in a virtual machine by specifying a different amount of memory than what would normally be recognized when Linux boots directly on the physical machine.

6. To configure a virtual machine to run from a raw disk partition, start the New Virtual Machine Wizard (**File** > **New Virtual Machine**) and select **Custom**.

7. When you reach the Select a Disk step, select **Use a physical disk**.

8. Complete the wizard steps, specifying the appropriate disk or partition to use for this virtual machine.

   Caution: Corruption is possible if you allow the virtual machine to modify a partition that is simultaneously mounted under Linux. Since the virtual machine and guest operating system access an existing partition while the host continues to run Linux, it is critical that the virtual machine not be allowed to modify any partition mounted under Linux or in use by another virtual machine.

To safeguard against this problem, be sure the partition you use in the virtual machine is not mounted under the Linux host.

9. Complete the remaining steps in the wizard.
10. If you have multiple IDE drives configured on a system, the VMware BIOS normally attempts to boot them in this sequence:

    a. Primary master

    b. Primary slave

    c. Secondary master

    d. Secondary slave

    If you have multiple SCSI drives configured on a system, the VMware BIOS normally attempts to boot them in the order of the SCSI device number.

    If you have both SCSI and IDE drives configured, the VMware BIOS normally attempts to boot SCSI drives followed by IDE drives, in the order described above.

    You can change the boot sequence using the Boot menu of the virtual machine's Phoenix BIOS. To enter the BIOS setup utility, power on the virtual machine and press F2 as the virtual machine begins to boot.
11. Power on the virtual machine. Click the **Power On** button. The virtual machine starts, runs the Phoenix BIOS, then boots from the master boot record (MBR).

    Choose the target operating system from the list of options offered by the boot manager.
12. Remember that your virtual machine hardware environment, which the guest operating system is about to run in for the first time, probably differs significantly from the physical hardware of your machine.

    For Windows guest operating systems, Plug and Play reconfigures Windows. Set up your virtual hardware profile with the devices found and configured by Plug and Play. See Setting Up Hardware Profiles in Virtual Machines on page 177 for more information.
13. Install VMware Tools in your guest operating system.

Warning: If you take a snapshot while using your raw disk, you must either revert to the snapshot or remove the snapshot before you reboot your guest operating system natively. This is necessary because any changes to sectors on the physical disk that have been modified on the disk invalidate the snapshot for the disk.

Setting Up Hardware Profiles in Virtual Machines

Certain operating systems use hardware profiles to load the appropriate drivers for a given set of hardware devices. If you have a dual-boot system and want to use a virtual machine to boot a previously installed operating system from an existing partition, you must set up "physical" and "virtual" hardware profiles.

Only users who are familiar with VMware Workstation virtual machines and the Windows hardware profiles concept should attempt this.

If you haven't already done so, review Configuring Dual- or Multiple-Boot Systems to Run with VMware Workstation on page 171 before proceeding.

Each virtual machine provides a platform that consists of the following set of virtual devices:

- Virtual DVD/CD-ROM
- Virtual IDE and SCSI hard disk drives
- Standard PCI graphics adapter
- Standard floppy disk drive
- Intel 82371 PCI Bus Master IDE controller (includes primary and secondary IDE controllers)
- BusLogic BT-958 compatible SCSI host adapter
- Standard 101/102-key keyboard
- PS/2-compatible mouse
- AMD PCnet-PCI II compatible Ethernet adapter
- Serial ports (COM1-COM4)
- Parallel ports (LPT1-LPT2)
- Two-port USB hub
- Sound card compatible with the Sound Blaster AudioPCI
- 82093AA IOAPIC

This set of virtual devices is different from the set of physical hardware devices on the host computer and is independent of the underlying hardware with a few exceptions (the processor itself is such an exception). This feature provides a stable platform and allows operating system images installed within a virtual machine to be migrated to other physical machines, regardless of the configuration of the physical machine.

If an operating system is installed directly into a VMware Workstation virtual machine, the operating system properly detects all the virtual devices by scanning the

hardware. However, if an operating system is already installed on the physical computer (for example, in a dual-boot configuration), the operating system already is configured to use the physical hardware devices. In order to boot such a preinstalled operating system in a virtual machine, you need to create separate hardware profiles in order to simplify the boot process.

Microsoft Windows operating systems, beginning with Windows 95 and Windows NT 4.0, allow you to create hardware profiles. Each hardware profile is associated with a set of known devices. If more than one hardware profile exists, the system prompts the user to choose between different hardware profiles at boot time.

Windows 95, Windows 98, Windows Me, Windows 2000, Windows XP and Windows Server 2003 use Plug and Play at boot time to confirm that the actual devices match the chosen hardware profile. Mismatches lead to the automatic detection of new devices. Although this operation succeeds, it can be fairly slow.

Windows NT does not have Plug and Play support and uses the hardware profiles to initialize its devices. Mismatches lead to errors reported by the device drivers and the devices are disabled.

In order to set up hardware profiles for your physical and virtual machines, follow these steps:

1. Before running VMware Workstation to boot an operating system previously installed on a disk partition, boot the operating system natively and create two hardware profiles, which you can call Physical Machine and Virtual Machine. To do this, open **Control Panel** > **System**, then click the **Hardware Profiles** tab — or click the **Hardware** tab, then click **Hardware Profiles**, depending on the operating system. Click the **Copy** button and name the copies appropriately.
2. **Windows NT only:** While still running the operating system natively, use the Device Manager to disable some devices from the Virtual Machine hardware profile. To do this, open **Control Panel** > **Devices**, then select the individual devices to disable. Devices to disable in the Virtual Machine hardware profile include audio, MIDI and joystick devices, Ethernet and other network devices and USB devices. Remember to disable them in the Virtual Machine hardware profile only.

   Skip this step if you are running Windows 95, Windows 98, Windows Me, Windows 2000, Windows XP or Windows Server 2003. The initial Plug and Play phase detects device mismatches.
3. Reboot the computer into your intended host operating system — for example, into Linux if you are running VMware Workstation on a Linux host.

4. Use the New Virtual Machine Wizard to configure your virtual machine as described in Configuring Dual- or Multiple-Boot Systems to Run with VMware Workstation on page 171.
5. Boot the virtual machine and use your existing boot manager to select the guest operating system. Choose Virtual Machine at the hardware profile menu prompt. You encounter device failure messages and delays during this initial boot.
6. **Windows Server 2003, Windows XP and Windows 2000 guests:** After you log on to Windows Server 2003, Windows XP or Windows 2000 (now running as a guest operating system) you should see a Found New Hardware dialog box for the video controller as Plug and Play runs and discovers the virtual hardware. Do not install drivers at this time. Click **Cancel** to close the Found New Hardware dialog box.

   Do not reboot the virtual machine. Click **No** in the System Settings Change/ Reboot dialog box.

   Windows Server 2003, Windows XP or Windows 2000 automatically detects and loads the driver for the AMD PCnet PCI Ethernet card. At this point, you should install VMware Tools inside the virtual machine. Allow the virtual machine to reboot after VMware Tools has been installed. Once Windows Server 2003, Windows XP or Windows 2000 reboots inside the virtual machine, select a new SVGA resolution from the **Settings** tab of the **Display Properties** dialog box to increase the size of the virtual machine's display window.

   Windows 95 and Windows 98 guests: You should see New Hardware Detected dialog boxes as Plug and Play runs and discovers the virtual hardware. Windows prompts you for locations to search for device drivers. Most of the device drivers are available in the existing operating system installation, but you may need the installation CD-ROM for some networking device drivers. Windows also asks you to reboot your system several times as it installs the device drivers.

   In some instances, Windows may not recognize the CD-ROM drive when it prompts you to insert the CD-ROM to look for device drivers during the initial hardware detection. In such cases, you can cancel the installation of the particular device or try pointing to `C:\windows\system\` to search for device drivers on the hard disk. Any failed device installations may be performed at a later time after the CD-ROM drive is recognized.

   After Windows has installed the virtual hardware and its drivers, you can remove the failed devices corresponding to the physical hardware using the Device Manager (**Control Panel** > **System** > **Device Manager**).

Select the device, then click the **Remove** button. If a device appears in multiple hardware profiles, you can select the hardware profile or profiles from which to remove the device.

If you want to enable the virtual machine's sound adapter to work inside the Windows 9x guest operating system, finish the remaining steps in this section, then refer to Configuring Sound on page 269.

Windows NT guests only: After the operating system has finished booting in the virtual machine, view the event log to see which physical devices have failed to start properly. You can disable them from the Virtual Hardware profile using the Device Manager (**Control Panel** > **Devices**).

If you want to enable the virtual machine's sound adapter to work inside the Windows NT guest operating system, finish the remaining steps in this section, then refer to Configuring Sound on page 269.

7. Confirm that your virtual devices — specifically, the network adapter — are working properly.

   Windows 95 and Windows 98 guests: If any virtual device is missing, you can detect it by running **Control Panel** > **Add New Hardware**.

8. Install VMware Tools. VMware Tools appears and runs in both hardware configurations but affects only the virtual machine.

   Note: The next time you reboot Windows natively using the Physical Machine hardware profile, some virtual devices may appear in the device list. You can disable or remove these virtual devices from the Physical Machine hardware profile in the same way that you removed physical devices from the virtual machine hardware profile in step 6, above.

Running a Windows 2000, Windows XP or Windows Server 2003 Virtual Machine from an Existing Multiple-Boot Installation

If you have installed Windows 2000, Windows XP or Windows Server 2003 on a computer, then try to run that same installation of the operating system as a VMware Workstation virtual machine running from a raw disk, the virtual machine may fail with an error message reporting an inaccessible boot device.

The problem occurs because the physical computer and the virtual machine require different IDE drivers. The Windows plug and play feature, which handles drivers for many hardware devices, does not install new IDE drivers.

If you encounter this problem, VMware recommends that you install your Windows 2000, Windows XP or Windows Server 2003 guest operating system in a virtual disk, rather than running it from a raw disk.

If you encounter this problem but it is important for you to run the virtual machine from the existing raw disk configuration, you can set up separate hardware profiles (described in Setting Up Hardware Profiles in Virtual Machines on page 177) and manually update the IDE driver in the profile for the virtual machine. For a detailed description of the workaround, see the VMware knowledge base (*www.vmware.com/info?id=41*).

Setting Up the SVGA Video Driver for a Windows 95 Guest Operating System Booted from a Raw Disk

This section explains how to configure the video driver in a Windows 95 raw disk installation using VMware Workstation. The steps below assume you are using Windows 95 as one of the operating systems in a dual-boot or multiple-boot configuration. Following these steps, you create separate hardware profiles for your virtual machine and your physical machine. For more details on hardware profiles, see Setting Up Hardware Profiles in Virtual Machines on page 177.

1. Boot Windows 95 natively (not in a virtual machine).
2. Right-click the **My Computer** icon on the desktop, then select **Properties**.
3. Click the **Hardware Profiles** tab.
4. Highlight the **Original Configuration** profile, then click **Copy**.
5. Name the profile Virtual Machine, then click **OK**.

   You may also want to rename the Original Configuration profile to Physical Machine.
6. Click **OK** to close the System Properties dialog box.
7. Shut down Windows 95 and reboot the system.
8. Boot into your host operating system (Linux, Windows NT, Windows 2000, Windows XP or Windows Server 2003).
9. Start the Windows 95 virtual machine.
10. Select **Virtual Machine** from the list of profiles when prompted.
11. If you are prompted to select the CPU Bridge, accept the default, then click **OK**.
12. Restart Windows 95 when prompted.
13. Again, select **Virtual Machine** from the list of profiles when prompted.

14. When the video card is detected, you are prompted to select which driver you want to install for your new hardware. Click the **Select from a list of alternate drivers** radio button, then click **OK**.
15. Select **Display Adapters** from the Select Hardware Type dialog box.
16. Select **Standard Display Adapter (VGA)** from the device list, then click **OK**.
17. Restart Windows 95 when prompted.
18. Install VMware Tools as outlined in Installing a Guest Operating System and VMware Tools on page 78, then restart the virtual machine.
19. Start the Device Manager and expand the **Display adapters** tree.
20. Highlight **VMware SVGA**. Click **Properties**.
21. Uncheck **Physical Machine**, then click **OK**. Click **Close**.
22. Shut down Windows 95 and power off the virtual machine.
23. Shut down your host operating system (Linux, Windows NT, Windows 2000, Windows XP or Windows Server 2003) and reboot into Windows 95.
24. Select the **Physical Machine** profile when prompted.
25. Repeat steps 19 through 21 and uncheck **Virtual Machine**, leaving **Physical Machine** checked.

Setting Up the SVGA Video Driver for Use with a Windows 98 Guest Operating System Booted from a Raw Disk

This section explains how to configure the video driver in a Windows 98 raw disk installation using VMware Workstation. The steps below assume you are using Windows 98 as one of the operating systems in a dual-boot or multiple-boot configuration. Following these steps, you create separate hardware profiles for your virtual machine and your physical machine. For more details on hardware profiles, see Setting Up Hardware Profiles in Virtual Machines on page 177.

1. Boot Windows 98 natively (not in a virtual machine).
2. Right-click the **My Computer** icon on the desktop, then select **Properties**.
3. Click the **Hardware Profiles** tab.
4. Highlight the **Original Configuration** profile, then click **Copy**.
5. Name the profile Virtual Machine, then click **OK**.

   You may also want to rename the Original Configuration profile to Physical Machine.

6. Click **OK** to close the System Properties dialog box.
7. Shut down Windows 98 and reboot the system.
8. Boot into your host operating system (Linux, Windows NT, Windows 2000, Windows XP or Windows Server 2003).
9. Select **Virtual Machine** from the list of profiles when prompted.
10. Windows 98 auto-detects the virtual machine's devices and installs the device drivers.
11. When Windows detects the video card driver, select **Search for the best driver**.
12. When prompted to reboot, click **No**. The AMD PCNET driver is installed, followed by the IDE controller drivers.
13. When prompted to reboot, click **Yes**.
14. Select the **Virtual Machine** hardware profile.
15. After Windows 98 has completed booting, start the Add New Hardware wizard from the Control Panel.
16. Click **Next**, then **Next** again.
17. Select **No, the device isn't in the list**.
18. Click **Yes**, then click **Next**.
19. After all devices have been detected, click the **Details** button to list the detected non-Plug and Play devices.
20. Click **Finish**, then reboot the virtual machine when prompted.
21. Select the **VMware Workstation** configuration profile. Notice that an unknown monitor is detected and installed.
22. Install VMware Tools as outlined in Installing a Guest Operating System and VMware Tools on page 78.
23. Open the Device Manager. It should show that you have
    - Standard PCI Graphics Adapter
    - VMware SVGA Display Adapter
24. Shut down the Windows 98 virtual machine and your host operating system.
25. Boot natively into Windows 98, then start the Device Manager.
26. Select the **VMware SVGA** device if listed, then click **Remove**.
27. Select the **Remove from Specific Configuration** radio button, then select **Physical Machine** from the configuration list.

28. Click **OK**, then reboot Windows 98 when prompted.
29. Boot into Windows 98 natively and verify the display settings. You should be able to use the display driver that you installed natively before starting this procedure.

Do Not Use Windows 2000, Windows XP and Windows Server 2003 Dynamic Disks as Raw Disks

Windows 2000, Windows XP and Windows Server 2003 support a disk type called a dynamic disk. Dynamic disks use a proprietary Microsoft format for recording partition information. This format is not publicly documented and thus is not supported for use in raw disk configurations under VMware Workstation.

Windows 2000, Windows XP and Windows Server 2003 also support the older type of partition table. Disks that use this type of partition table are called basic disks.

You can use the disk management tool to check the type of disk used on your Windows 2000, Windows XP or Windows Server 2003 host and, if it is a dynamic disk, change it to basic.

Caution: If you change a dynamic disk to a basic disk, you lose all data on the disk.

Use this procedure to convert a dynamic disk to a basic disk.

1. Open the disk management tool.

   Start > Settings > Control Panel > Administrative Tools > Computer Management > Disk Management
2. Delete all logical volumes on the disk. This destroys all data on the disk.
3. Right-click the disk icon and select Revert to Basic Disk.
4. Create the partitions you want on the disk.

Configuring Dual- or Multiple-Boot SCSI Systems to Run with VMware Workstation on a Linux Host

It may be possible to configure VMware Workstation so that you can use an operating system already installed and configured on a SCSI disk as a guest operating system inside a VMware Workstation virtual machine.

Using an existing SCSI disk — or SCSI raw disk — inside a virtual machine is supported only if the host has an LSI Logic or BusLogic SCSI adapter. LSI Logic is the preferred choice because it is easier to find drivers for LSI Logic adapters. It may be possible to configure a host with a different SCSI adapter so the same operating system can be booted both natively and inside a virtual machine, but this approach is not supported

by VMware. For details on some of the key issues involved, see Known Issues and Background Information on Using SCSI Raw Disks on page 188.

Before You Create the Virtual Machine Configuration

You must create a separate configuration for each guest operating system. Allow read and write access to the partitions used by that operating system only.

1. Before starting, if you are running a Windows guest operating system you should read Setting Up Hardware Profiles in Virtual Machines on page 177. You should boot the guest operating system natively on the computer and create a hardware profile for the virtual machine before proceeding.
2. Check to see what SCSI ID is set for the drive you plan to use in the virtual machine.
3. Make certain that in addition to any SCSI drivers you have configured for the host, you have also installed the driver for the LSI Logic or BusLogic virtual adapter you plan to use in the virtual machine.

   Drivers for LSI Logic controllers are available from the LSI Logic Web site — *www.lsilogic.com*.In the download area of the site, find a driver for any of the adapters in the LSI53C10xx Ultra160 SCSI I/O controller series — for example, the LSI53C1000.

   The LSI Logic Web site no longer provides drivers for the Mylex (BusLogic) BT/KT-958 compatible host bus adapter.

   The LSI Logic or BusLogic driver needs to be installed in the profile for the guest operating system.

   Note: To use the virtual BusLogic SCSI adapter in a Windows XP or Windows Server 2003 virtual machine, you need a special SCSI driver available from the download section of the VMware Web site at *www.vmware.com/download*.
4. Check operating system partition mounts. Be sure the existing raw disk partitions that you plan to configure the virtual machine to use are not mounted by the Linux host.

   Caution: A raw disk partition should not be used (mounted) simultaneously by the host and the guest operating system. Because each operating system is unaware of the other, data corruption may occur if both operating systems read or write to the same partition. It is critical that the virtual machine not be allowed to modify any partition mounted under the Linux host or in use by another virtual machine. To safeguard against this problem, be sure the partition you use for the virtual machine is not mounted under the Linux host.

5. Set the device group membership or device ownership. The master raw disk devices must be readable and writable by the user who runs VMware Workstation. On most distributions, the raw devices (such as `/dev/hda` and `/dev/hdb`) belong to group-id `disk`. If this is the case, you can add VMware Workstation users to the `disk` group. Another option is to change the owner of the device. Please think carefully about security issues when you explore different options here.

   It is typically a good idea to grant VMware Workstation users access to all `/dev/hd[abcd]` raw devices that contain operating systems or boot managers and then rely on VMware Workstation's raw disk configuration files to guard access. This provides boot managers access to configuration and other files they may need to boot the operating systems. For example, LILO needs to read `/boot` on a Linux partition to boot a non-Linux operating system that may be on another drive.

6. If you plan to run a second Linux installation from an existing partition as a guest operating system, and your physical machine's `/etc/lilo.conf` has a memory register statement such as `Append= "mem…"`, you may want to adjust the append memory parameter or create a new entry in LILO for running Linux in a virtual machine.

   Many newer Linux distributions recognize all physical memory in the physical machine, whereas many older Linux distributions see only the first 64MB of memory by default. Machines with more than 64MB of memory that run the older distributions may have the `Append= "mem=…"` parameter added under the `Image=…` section of `lilo.conf` to tell Linux to look for more memory than seen by default.

   If the amount of memory configured in `lilo.conf` exceeds the amount of memory assigned to the virtual machine, the guest operating system is likely to panic when the virtual machine tries to boot the second Linux installation.

   You can create another entry in `lilo.conf` for running Linux in a virtual machine by specifying a different amount of memory than what should normally be recognized when Linux boots directly on the physical machine.

Setting Up the Virtual Machine Configuration

1. Start VMware Workstation.
2. Start the New Virtual Machine Wizard (**File** > **New Virtual Machine**) and select **Custom**.

3. When you reach the Select I/O Adapter Types step, select the SCSI adapter type that matches the driver you installed in the virtual machine profile.
4. When you reach the Select a Disk step, select **Use a physical disk**.
5. In the **Device** list, select the physical drive.

   Under **Usage**, select whether to use the entire disk or individual partitions.

   If you selected **Use entire disk**, click **Next** then go to step 6.

   If you selected **Use individual partitions**, the Select Physical Disk Partitions panel appears.

   Select the partitions you want the virtual machine to use, then click **Next**.
6. In the entry field, enter a name of your choice for the physical disk.

   Caution: If you browse to place the disk file in another directory, do not select an existing virtual disk file.

   To specify a device ID for the physical disk, click **Advanced**. In the **Virtual device node** list, select the SCSI ID that corresponds to the one used by your SCSI drive. For example, if your SCSI drive has SCSI ID 2, select **SCSI 0:2**. If you do not know the SCSI ID set on your physical SCSI drive, try using **SCSI 0:0**.

   On the advanced settings screen, you can also specify a disk mode. This is useful in certain special-purpose configurations in which you want to exclude disks from the snapshot. For more information on the snapshot feature, see Using the Snapshot on page 200.

   Normal disks are included in the snapshot. In most cases, this is the setting you want.

   Independent disks are not included in the snapshot. You have the following options for an independent disk:

   - **Persistent** — changes are immediately and permanently written to the disk.
   - **Nonpersistent** — changes to the disk are discarded when you power off or revert to the snapshot.

   When you have set the filename and location you want to use and have made any selections you want to make on the advanced settings screen, click **Finish**.
7. Begin using your virtual machine.

Known Issues and Background Information on Using SCSI Raw Disks

Geometry

In some cases, it is not possible to boot a raw SCSI drive inside a virtual machine because the SCSI adapter in the physical computer and the BusLogic adapter in the virtual machine describe the drive in different ways. The virtual machine might hang during the boot, VMware Workstation might crash or VMware Workstation might fail with an ASSERT or other error message.

This problem is most likely to affect smaller drives — less than 2GB.

In order to share the same BIOS interface used by IDE disks (which is required in order to boot), all SCSI disks need to have a geometry, which is a fabricated value for the number of cylinders, sectors and heads on the disk.

In fact, a SCSI disk appears to a computer as a single flat entity from sector 1 up to the highest sector on the disk. As a result, every SCSI vendor has its own approach to taking the capacity of a SCSI disk and generating a geometry to use for booting.

The conversion from a given geometry to an absolute sector number depends on the geometry. If you have a disk with a boot sector written by a program running on the host and you try to boot that disk inside a virtual machine, the boot program can fail if the host geometry does not match the geometry used by the BusLogic virtual SCSI adapter. The symptoms are that you see the first part of the boot loader — possibly an `LI` from LILO, for example — but then the boot either stops or crashes.

BusLogic uses the following rules for generating disk geometries:

Disk size	Heads	Sectors
<= 1GB	64	32
> 1GB and <= 2GB	128	32
> 2GB	255	63

In each case the number of cylinders is calculated by taking the total capacity of the disk and dividing by (heads*sectors). Fortunately, for sufficiently big disks, practically all vendors use 255 heads and 63 sectors.

Drivers

In contrast to IDE adapters, SCSI adapters are not interchangeable and cannot all use the same drivers. That is, if you have an Adaptec SCSI host adapter in your machine and you remove it and replace it with a BusLogic SCSI host adapter, your operating system will most likely fail to boot unless you install a BusLogic driver.

Dual booting from a disk that is also used as a virtual disk is no different. To your operating system, it appears that the SCSI card in the machine suddenly changed from whatever you own to an LSI Logic or BusLogic card, and your operating system needs to have a corresponding driver installed. If that driver is not installed, you get a panic, a blue screen or some similar fatal error as soon as the boot process tries to switch from the BIOS bootstrap to the disk driver installed in the operating system.

Operating System Configuration

Many operating systems have configuration information that is different for SCSI and IDE drives. For example, Linux uses `/dev/hd[x]` as the device name for IDE disks and `/dev/sd[x]` for SCSI disks. References to these names appear in `/etc/fstab` and other configuration files.

This is one reason that booting a raw IDE disk as a SCSI disk or vice versa does not work well (if at all).

However, even when you are dealing only with SCSI devices, it is possible for an operating system to encode information in a way that causes problems when you are dual booting. For example, Solaris names its SCSI disks `/dev/c[x]t[y]d[z]s0`, where the `y` represents the SCSI ID. So if you had a raw disk configured as SCSI ID 3 on the host and as SCSI ID 0 in your VMware Workstation configuration file, it would move if you were running Solaris, and most likely Solaris would not boot.

The precise dependencies in various operating systems can be complex. That is why it is safest to configure SCSI raw disks in a virtual machine using the same SCSI ID as they use on the host.

Installing an Operating System onto a Raw Partition from a Virtual Machine

In some situations, you may want to install a guest operating system directly on a physical disk or partition — known as a raw disk — even if you do not need to boot that disk on the host, outside of the virtual machine.

It is possible to use either an unused partition or a completely unused disk on the host as a disk in the virtual machine. However, it is important to be aware that an operating system installed in this setting probably cannot boot outside of the virtual machine, even though the data is available to the host.

If you have a dual-boot system and want to configure a virtual machine to boot from an existing partition, see Configuring a Dual-Boot Computer for Use with a Virtual Machine on page 169. The instructions in this section do not apply to a disk with a previously installed operating system.

Caution: Raw disks are an advanced feature and should be configured only by expert users.

VMware Workstation uses description files to control access to each raw disk on the system. These description files contain access privilege information that controls a virtual machine's access to certain partitions on the disks. This mechanism prevents users from accidentally running the host operating system again as a guest or running a guest operating system that the virtual machine is not configured to use. The description file also prevents accidental writes to raw disk partitions from badly behaved operating systems or applications.

Use the New Virtual Machine Wizard to configure VMware Workstation to use existing raw disk partitions. The wizard guides you though creating a new virtual machine including configuring the raw disk description files. Rerun the wizard to create a separate configuration for each guest operating system installed on a raw partition.

Configuring a Windows Host

Windows 2000, Windows XP and Windows Server 2003 Dynamic Disks

If your host is running Windows 2000, Windows XP or Windows Server 2003 and is using dynamic disks, see Do Not Use Windows 2000, Windows XP and Windows Server 2003 Dynamic Disks as Raw Disks on page 184.

Configuring the Virtual Machine to Use a Raw Disk

Use the following steps to run a guest operating system from a raw disk.

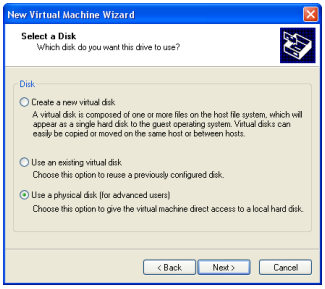
Note: If you use a Windows host's IDE disk in a raw disk configuration, it cannot be configured as the slave on the secondary IDE channel if the master on that channel is a CD-ROM drive.

1. Identify the raw partition on which you plan to install the guest operating system.

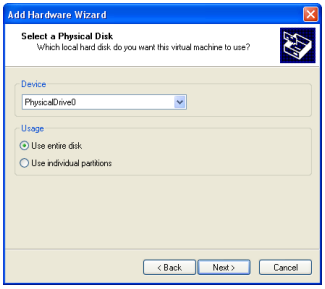
   Check the guest operating system documentation regarding the type of partition on which the operating system can be installed. For example, operating systems like DOS, Windows 95 and Windows 98 must be installed on the first primary partition while others, like Linux, can be installed on a primary or extended partition on any part of the drive.

   Identify an appropriate raw partition or disk for the guest operating system to use. Be sure that the raw partition is not mounted by the Windows host and not in use by others. Also, be sure the raw partition or disk does not have data you will need in the future; if it does, back up that data now.

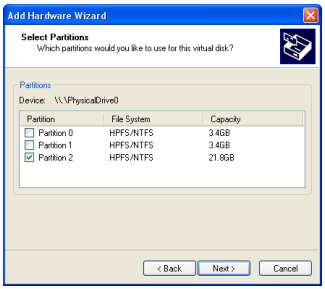
2. Start the New Virtual Machine Wizard (**File** > **New Virtual Machine**) and select **Custom**.



3. When you reach the Select a Disk step, select **Use a physical disk**.



4. Choose the physical hard disk to use from the drop-down list. Select whether you want to use the entire disk or use only individual partitions on the disk. Click **Next**.



5. If you selected **Use individual partitions** in the previous step, select which partitions you want to use in the virtual machine. If you selected **Use entire disk**, this step does not appear.

   Click **Next**.

6. The partition on which you are installing the guest operating system should be unmapped in the host.

   Caution: Corruption is possible if you allow the virtual machine to modify a partition that is simultaneously mounted under Windows. Since the virtual machine and guest operating system access a raw disk partition while the host continues to run Windows, it is critical that you not allow the virtual machine to modify any partition mounted by the host or in use by another virtual machine. To safeguard against this problem, be sure the raw disk partition you use for the virtual machine is not in use by the host.

Windows NT host: Use the Disk Administrator (**Start** > **Programs** > **Administrative Tools**). First highlight the partition that contains the guest operating system, then choose **Tools** > **Assign Drive Letter**. In the dialog box, choose **Do not assign a drive letter** for the partition and click **OK**. The unmapping happens immediately.

Windows Server 2003, Windows XP or Windows 2000 host: Use Disk Management (**Start** > **Settings** > **Control Panel** > **Administrative Tools** > **Computer Management** > **Storage** > **Disk Management**). Select the partition you want to unmap, then choose **Action** > **All Tasks** > **Change Drive Letter and Path**. Click the **Remove** button.

7. Use the virtual machine settings editor (**VM** > **Settings**) if you want to change any configuration options from the wizard defaults — for example, to change the amount of memory allocated to the guest operating system.
8. At this point you are ready to begin installing the guest operating system onto the raw disk you configured for the virtual machine. For more details, read the installation notes for various guest operating systems in the *VMware Guest Operating System Installation Guide*, available from the VMware Web site or from the Help menu.

Configuring a Linux Host

1. Identify the raw partition on which the guest operating system will be installed.

   Check the guest operating system documentation regarding the type of partition on which the operating system can be installed. For example, operating systems like DOS, Windows 95 and Windows 98 must be installed on the first primary partition while others, like Linux, can be installed on a primary or extended partition on any part of the drive.

   Identify an appropriate raw partition or disk for the guest operating system to use. Check that the raw partition is not mounted by the Linux host and not in use by others. Also, be sure the raw partition or disk does not have data you will need in the future; if it does, back up that data now.
2. Check the operating system partition mounts. Be sure the existing disk partitions that you plan to use in the virtual machine are not mounted by Linux.
3. Set the device group membership or device ownership.

   The master raw disk device or devices need to be readable and writable by the user who runs VMware Workstation. On most distributions, the raw devices, such as `/dev/hda` (IDE raw disk) and `/dev/sdb` (SCSI raw disk) belong to group-id `disk`. If this is the case, you can add VMware Workstation users to the `disk`

group. Another option is to change the owner of the device. Please think carefully about security issues when you explore different options here.

It is a good idea to grant VMware Workstation users access to all `/dev/hd[abcd]` raw devices that contain operating systems or boot managers, then rely on VMware Workstation's raw disk configuration files to guard access. This provides boot managers access to configuration and other files they may need to boot the operating systems. For example, LILO needs to read `/boot` on a Linux partition to boot a non-Linux operating system that may be on another drive.

4. Start the New Virtual Machine Wizard (**File** > **New Virtual Machine**) and select **Custom**.
5. When you reach the Select a Disk step, select **Use a physical disk**.
6. If the raw disk you plan to use has multiple partitions on it already, be aware that certain operating systems (DOS, Windows 95, Windows 98) must be installed on the first primary partition.

   Caution: Corruption is possible if you allow the virtual machine to modify a partition that is simultaneously mounted under the Linux host operating system. Since the virtual machine and guest operating system access an existing partition while the host continues to run Linux, it is critical that the virtual machine not be allowed to modify any partition mounted by the host or in use by another virtual machine.

   To safeguard against this problem, be sure the partition you use for the virtual machine is not mounted under the Linux host.
7. At this point you are ready to begin installing the guest operating system on the raw disk you configured for the virtual machine. For more details, read the installation notes for various guest operating systems in the *VMware Guest Operating System Installation Guide*, available from the VMware Web site or from the Help menu.

Disk Performance in Windows NT Guests on Multiprocessor Hosts

Some users have seen slower than expected disk input and output performance when running Windows NT guest operating systems. They see the problem in a VMware Workstation virtual machine using IDE virtual disks on a multiprocessor host computer. The I/O issue is especially noticeable when the virtual machine is booting.

Note: Performance in Windows NT guest operating systems may also be affected by disk fragmentation on the host computer. For details, see Configuring and Maintaining the Host Computer on page 309.

Improving Performance

You may increase performance by enabling DMA (direct memory access) on the virtual hard disk's IDE channel in the virtual machine.

If you have a virtual disk and a DVD/CD-ROM attached as master and slave to the primary IDE controller (channel 0) and you want to enable DMA, power off the virtual machine and use the virtual machine settings editor (**VM** > **Settings**) to move the DVD/CD-ROM drive to the secondary IDE controller (channel 1) at IDE 1:0.

You can enable the DMA feature after you finish installing Windows NT. You must install Service Pack 6a. Download `DMACHECK.EXE` from the Microsoft Web site (*support.microsoft.com/support/kb/articles/Q191/7/74.ASP*) and run it.

Click the **Enabled** option for the IDE controller and channel configured for the virtual disk. Typically, this is channel 0 only, unless you have the virtual machine configured with multiple virtual disks and no virtual DVD/CD-ROM drive.

As noted above, you should not enable DMA on an IDE channel with a virtual DVD/CD-ROM drive attached.

CHAPTER 8

Preserving the State of a Virtual Machine

VMware Workstation 4 offers two ways to preserve the state of a virtual machine. The following sections describe these features and help you understand which is appropriate in particular situations:

- The Snapshot and the Virtual Machine's Hard Disks on page 204
- The Snapshot and Other Activity in the Virtual Machine on page 205

Using Suspend and Resume

The suspend and resume feature is most useful when you want to save the current state of your virtual machine, then pick up work later with the virtual machine in the same state it was when you stopped.

Once you resume and do additional work in the virtual machine, there is no way to return to the state the virtual machine was in at the time you suspended.

To preserve the state of the virtual machine so you can return to the same state repeatedly, take a snapshot. For details, see Using the Snapshot on page 200.

The speed of the suspend and resume operations depends on how much data has changed while the virtual machine has been running. In general, the first suspend operation takes a bit longer than later suspend operations do.

When you suspend a virtual machine, a file with a `.vmss` extension is created. This file contains the entire state of the virtual machine. When you resume the virtual machine, its state is restored from the `.vmss` file.

To suspend a virtual machine:

1. If your virtual machine is running in full screen mode, return to window mode by pressing the Ctrl-Alt key combination.
2. Click **Suspend** on the VMware Workstation toolbar.
3. When VMware Workstation has completed the suspend operation, it is safe to exit VMware Workstation.

   File > **Exit**

To resume a virtual machine that you have suspended:

1. Start VMware Workstation and choose a virtual machine you have suspended.
2. Click **Resume** on the VMware Workstation toolbar.

   Note that any applications you were running at the time you suspended the virtual machine are running and the content is the same as it was when you suspended the virtual machine.

Using the Snapshot

The snapshot feature is most useful when you want to preserve the state of the virtual machine so you can return to the same state repeatedly.

To simply save the current state of your virtual machine, then pick up work later with the virtual machine in the same state it was when you stopped, suspend the virtual machine. For details, see Using Suspend and Resume on page 199.

You can take a snapshot while a virtual machine is powered on, powered off or suspended. (If you are suspending a virtual machine, wait until the suspend operation has finished before taking the snapshot.) A snapshot preserves the virtual machine just as it was when you took the snapshot — the state of the data on all the virtual machine's disks and whether the virtual machine was powered on, powered off or suspended. You can then revert to that snapshot at any time.

Note: If you are using a legacy virtual machine — a virtual machine created under VMware Workstation 3 and not upgraded to use the new VMware Workstation 4 virtual hardware — you must power off the virtual machine before taking a snapshot. For information on upgrading the virtual hardware, see Upgrading VMware Workstation on page 41. You also must power off the virtual machine before taking a snapshot if the virtual machine has multiple disks in different disk modes — for example, if you have a special purpose configuration that requires you to use an independent disk.

When you revert to a snapshot, you discard all changes made to the virtual machine since you took the snapshot.

Use the **Snapshot** and **Revert** buttons on the Workstation toolbar to take a snapshot and revert to it later.

You can take a new snapshot at almost any time. When you take a new snapshot, you replace the previous snapshot. You can have only one active snapshot at a time.

What Is Captured by the Snapshot?

The snapshot captures the entire state of the virtual machine at the time you take the snapshot. This includes:

- The state of all the virtual machine's disks.
- The contents of the virtual machine's memory.
- The virtual machine settings.

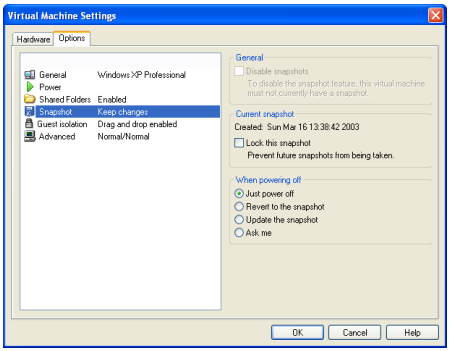
When you revert to the snapshot, you return all these items to the state they were in at the time you took the snapshot.

Note: In certain special purpose configurations, you may want to exclude one or more of the virtual machine's disks from the snapshot. To exclude a disk from the snapshot, choose **VM** > **Settings**, select the drive you want to exclude, then click **Advanced**. On the advanced settings screen, select **Independent**. You have the following options for an independent disk:

- **Persistent** — changes are immediately and permanently written to the disk. All changes to an independent disk in persistent mode remain, even when you revert to the snapshot.
- **Nonpersistent** — changes to the disk are discarded when you power off or revert to the snapshot.

Settings for the Snapshot

You can also specify what you want VMware Workstation to do with the snapshot any time the virtual machine is powered off. To do so, go to **VM** > **Settings** > **Options** > **Snapshot** and select one of the choices under **When powering off**.



Options when powering off include

- **Just power off** — leaves the snapshot as it is. This is the default setting.
- **Revert to the snapshot** — reverts to the snapshot so the virtual machine always starts in the same state; reverting to the snapshot discards changes.
- **Update the snapshot**— takes a new snapshot of the virtual machine state as it was just before you powered off; this replaces the previous snapshot.
- **Ask me** — always asks what you want to do with the snapshot when you power off.

If the virtual machine has no snapshot, you can disable the snapshot feature by selecting **Disable snapshots**. If you have a snapshot and want to disable the snapshot

feature, first go to the VMware Workstation menu and choose **Snapshot** > **Remove Snapshot**. Then return to the virtual machine settings editor and select **Disable snapshots**.

To lock the snapshot so no new snapshot can be taken, select **Lock this snapshot**.

Updating the Snapshot When You Change Virtual Machine Settings

When you change settings in the virtual machine settings editor, you may want to update the snapshot so these new settings are in effect when you revert to the snapshot. The most convenient way to do so is to select **Update the snapshot after changing settings** at the bottom of the virtual machine settings editor.

If this option is selected, when you click **OK** in the virtual machine settings editor, VMware Workstation updates the snapshot of the virtual machine. To avoid updating the snapshot, click **Cancel** or deselect **Update the snapshot after changing settings** before you click **OK**.

Removing the Snapshot

You can remove the snapshot any time the virtual machine is powered off. Removing the snapshot does not destroy any data in the virtual machine. You keep all changes made since you took the snapshot. For example, changes made to data stored on the virtual hard disk are written to the virtual disk files. You then permanently accumulate additional changes as you run the virtual machine. You cannot revert to a previous state because the snapshot no longer exists.

To remove the snapshot, shut down and power off the virtual machine. Then, on the VMware Workstation menu, choose **Snapshot** > **Remove Snapshot**.

Ways of Using the Snapshot

The following examples illustrate the most common ways you can use the snapshot.

No Snapshot

If you do not take a snapshot, your virtual machine runs the same way a physical computer does. All changes you make while you are working with a virtual machine are saved and you cannot return to an earlier state.

If you do not need to use the snapshot feature, it is best to run your virtual machine with no snapshot. This provides best performance. To be sure a virtual machine has no snapshot, choose **Snapshot** > **Remove Snapshot**. You can then disable the snapshot functionality for the virtual machine. Go to **VM** > **Settings** > **Options** > **Snapshot** and select **Disable snapshots**.

Making Risky Changes

If you plan to make risky changes in a virtual machine (for example, testing new software or examining a virus), take a snapshot before you begin to make those risky changes. If you encounter a problem, click **Revert** to return the virtual machine to its state at the time you took the snapshot.

If the first action you take causes no problems and you want to protect the virtual machine in its new state, you can take a new snapshot. You can have only one snapshot at a given time. When you take the new snapshot, you replace your previous snapshot. You do not lose any data. For example, changes made to data stored on the virtual hard disk are written to the virtual disk files.

Starting a Virtual Machine Repeatedly in the Same State

You can configure the virtual machine to revert to the snapshot any time it is powered off. To do so, go to **VM** > **Settings** > **Options** > **Snapshot**. Under **When powering off**, select **Revert to the snapshot**. If you want the virtual machine to be suspended when you launch it, suspend the virtual machine before saving the snapshot. Similarly, if you want the virtual machine to be powered on or powered off when you launch it, be sure it is powered on or powered off when you take the snapshot.

The Snapshot and Legacy Disk Modes

If you are familiar with the disk modes used in earlier versions of VMware Workstation, you can use the snapshot to achieve equivalent results.

- Persistent mode — Do not take a snapshot.
- Undoable mode — Take a snapshot when you begin your working session. To discard all work done during the session, revert to the snapshot. To commit the work done during the session, take a new snapshot at the end of the working session. To keep the work done during a session without committing it, leave the original snapshot unchanged.
- Nonpersistent mode — Be sure the virtual machine is in the state you want it. Power off the virtual machine. Take a snapshot. Go to **VM** > **Settings** > **Options** > **Snapshot**. Under **When powering off** select **Revert to snapshot**.

Note: In earlier versions of VMware Workstation, disk modes had to be set individually for each disk. The snapshot introduced in VMware Workstation 4 applies by default to the entire virtual machine, including all disks attached to the virtual machine.

The Snapshot and Repeatable Resume

The repeatable resume feature in earlier versions of Workstation allowed you to resume a suspended virtual machine repeatedly in the same state. You can use the snapshot to accomplish the same thing. Run the virtual machine, be sure it is in the state you want it, then suspend it. Take a snapshot. Go to VM > Settings > Options > Snapshot. Under When powering off, select Revert to the snapshot.

The Snapshot and Legacy Virtual Machines

If you are using a legacy virtual machine — a virtual machine created under VMware Workstation 3 and not upgraded to use the new VMware Workstation 4 virtual hardware — and you have disks in undoable or nonpersistent mode, you have a snapshot. If you have persistent disks, you have no snapshot. You have the following options:

- Persistent mode — You have no snapshot. You may take a snapshot any time the virtual machine is powered off.
- Undoable mode — You have a snapshot. You may update or remove the snapshot any time the virtual machine is powered off.
- Nonpersistent mode — You have a snapshot. In addition, in the virtual machine settings editor, the virtual machine is set to revert to the snapshot every time it is powered off. You may update or remove the snapshot any time the virtual machine is powered off. You may also change the settings in the virtual machine settings editor any time the virtual machine is powered off.

The Snapshot and the Virtual Machine's Hard Disks

When a snapshot exists and the virtual machine saves data to disk, that data is written to a set of redo-log files. These files have `.REDO` as part of the filename and are stored in the virtual machine's working directory.

Newly saved data continues to accumulate in the redo-log files until you take an action that affects the snapshot.

- Remove the snapshot — When you remove the snapshot, the changes accumulated in the redo-log files are written permanently to the base disks., either the virtual disk files or the physical disks, depending on your virtual machine's hard disk configuration. This is similar to committing changes to a disk in VMware Workstation 3.
- Revert to the snapshot — When you revert to the snapshot, the contents of the redo-log files are discarded. Any additional changes are, once again,

accumulated in the redo-log files. This is similar to discarding changes to a disk in VMware Workstation 3.

- Take a snapshot — If you take a snapshot when the virtual machine already has a snapshot, changes stored in the redo-log files are written permanently to the base disk. Then any subsequent changes are, once again, accumulated in the redo-log files.

The Snapshot and Other Activity in the Virtual Machine

When you take a snapshot, be aware of other activity going on in the virtual machine and the likely impact of reverting to the snapshot. In general, it is best to take the snapshot when no applications in the virtual machine are communicating with other computers.

The potential for problems is greatest if the virtual machine is communicating with another computer, especially in a production environment.

Consider a case in which you take a snapshot while the virtual machine is downloading a file from a server on the network. After you take the snapshot, the virtual machine continues downloading the file, communicating its progress to the server. If you revert to the snapshot, communications between the virtual machine and the server are confused and the file transfer fails.

Or consider a case in which you take a snapshot while an application in the virtual machine is sending a transaction to a database on a separate machine. If you revert to the snapshot — especially if you revert after the transaction starts but before it has been committed — the database is likely to be confused.

CHAPTER 9

Configuring a Virtual Network

VMware Workstation provides virtual networking components that let you create a wide range of configurations.

If you select the **Typical** setup path in the New Virtual Machine Wizard when you create a virtual machine, the wizard sets up bridged networking for the virtual machine. You can choose any of the common configurations — bridged networking, network address translation (NAT) and host-only networking — by selecting the **Custom** setup path. The wizard then connects the virtual machine to the appropriate virtual network.

You can set up more specialized configurations by choosing the appropriate settings in the virtual machine settings editor, in the Virtual Network Editor (on Windows hosts) and on your host computer.

On a Windows host, the software needed for all networking configurations is installed when you install VMware Workstation. On a Linux host, all components are available if you choose to have both bridged and host-only networking available to your virtual machines at the time you install VMware Workstation.

The first topics in this section give you a quick look at the virtual networking components that VMware Workstation provides and show how you can use them

with your virtual machine. The rest of the section provides more detail on some networking capabilities and specialized configurations.

Components of the Virtual Network

Virtual switch — Like a physical switch, a virtual switch lets you connect other networking components together. Virtual switches are created as needed by the VMware Workstation software, up to a total of nine switches. You can connect one or more virtual machines to a switch.

A few of the switches and the networks associated with them are, by default, used for special named configurations. The bridged network normally uses VMnet0. The host-only network uses VMnet1 by default. And the NAT network uses VMnet8 by default. The others available networks are simply named VMnet2, VMnet3, VMnet4, and so on.

You connect a virtual machine to a switch by selecting the virtual network adapter you want to connect in the virtual machine settings editor, then configuring it to use the desired virtual network.

Bridge — The bridge lets you connect your virtual machine to the LAN used by your host computer. It connects the virtual network adapter in your virtual machine to the physical Ethernet adapter in your host computer.

The bridge is installed during VMware Workstation installation (on a Linux host, you must choose to make bridged networking available to your virtual machines). It is set up automatically when you create a new virtual machine using bridged networking.

Additional virtual bridges can be set up for use in custom configurations that require connections to more than one physical Ethernet adapter on the host computer.

Host virtual adapter — The host virtual adapter is a virtual Ethernet adapter that appears to your host operating system as a VMware Virtual Ethernet Adapter on a Windows host and as a Host-Only Interface on a Linux host. It allows you to communicate between your host computer and the virtual machines on that host computer. The host virtual adapter is used in host-only and NAT configurations.

The host virtual adapter is not connected to any external network unless you set up special software on the host computer — a proxy server, for example — to connect the host-only adapter to the physical network adapter.

The software that creates the host virtual adapter is installed when you install VMware Workstation (on a Linux host, you must choose to make host-only networking available to your virtual machines). A host virtual adapter is then created automatically when you boot the host computer.

You can set up additional host virtual adapters as needed.

NAT device — The NAT (network address translation) device 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. You can, for example, use NAT to connect your virtual machines to the Internet through a dial-up connection on the host computer or through the host computer's Ethernet adapter or wireless Ethernet adapter. NAT is also useful when you need to connect to a non-Ethernet network, such as Token Ring or ATM.

The NAT device is set up automatically when you install VMware Workstation. (On a Linux host, you must choose to make NAT available to your virtual machines.)

DHCP server — The DHCP (dynamic host configuration protocol) server provides IP network addresses to virtual machines in configurations that are not bridged to an external network — for example, host-only and NAT configurations.

Network adapter — One virtual network adapter is set up for your virtual machine when you create it with the New Virtual Machine Wizard using any type of networking. It appears to the guest operating system as an AMD PCNET PCI adapter.

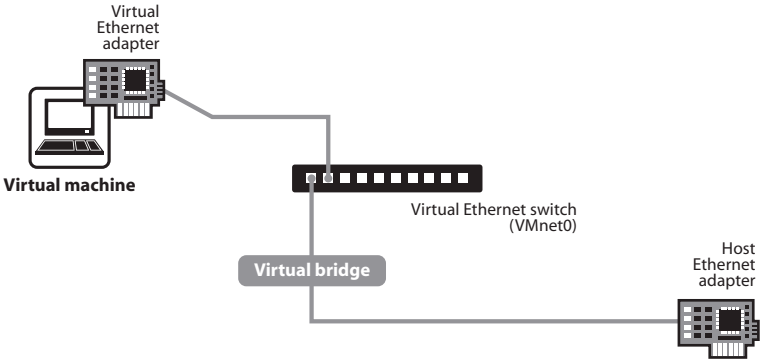
You can create and configure up to three virtual network adapters in each virtual machine using the virtual machine settings editor.

Common Networking Configurations

The following sections illustrate the networking configurations that are set up for you automatically when you choose the standard networking options in the New Virtual Machine Wizard or virtual machine settings editor.

Only one virtual machine is shown in each example, but multiple virtual machines can be connected to the same virtual Ethernet switch. On a Windows host, you can connect an unlimited number of virtual network devices to a virtual switch. On a Linux host, you can connect up to 32 devices.

Bridged Networking



Bridged networking connects a virtual machine to a network using the host computer's Ethernet adapter.

Bridged networking is set up automatically if you select **Use bridged networking** in the New Virtual Machine Wizard or if you select the **Typical** setup path. This selection is available on a Linux host only if you enable the bridged networking option when you install VMware Workstation.

If your host computer is on an Ethernet network, this is often the easiest way to give your virtual machine access to that network. On a Windows host, you can use bridged networking to connect to either a wired or a wireless network. On a Linux host, you can use bridged networking to connect to a wired network.

If you use bridged networking, your virtual machine needs to have its own identity on the network. For example, on a TCP/IP network, the virtual machine needs its own IP address. Your network administrator can tell you whether IP addresses are available for your virtual machine and what networking settings you should use in the guest operating system. Generally, your guest operating system may acquire an IP address

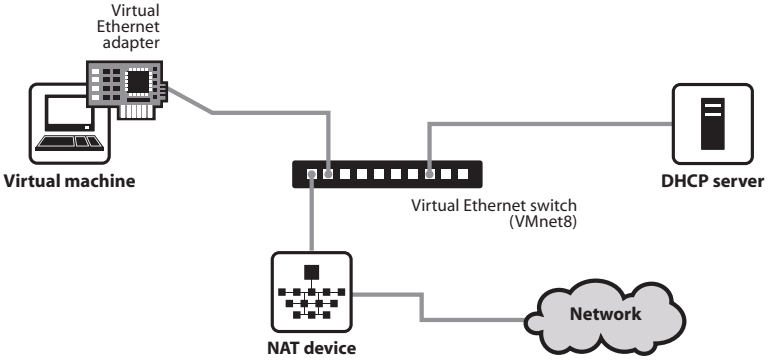
and other network details automatically from a DHCP server, or you may need to set the IP address and other details manually in the guest operating system.

If you use bridged networking, the virtual machine is a full participant in the network. It has access to other machines on the network and can be contacted by other machines on the network as if it were a physical computer on the network.

Be aware that if the host computer is set up to boot multiple operating systems and you run one or more of them in virtual machines, you need to configure each operating system with a unique network address. People who boot multiple operating systems often assign all systems the same address, since they assume only one operating system will be running at a time. If you use one or more of the operating systems in a virtual machine, this assumption is no longer true.

If you make some other selection in the New Virtual Machine Wizard and later decide you want to use bridged networking, you can make that change in the virtual machine settings editor (**VM** > **Settings**). For details, see Changing the Networking Configuration on page 219.

Network Address Translation (NAT)



NAT gives a virtual machine access to network resources using the host computer's IP address.

A network address translation connection is set up automatically if you follow the **Custom** path in the New Virtual Machine Wizard and select **Use network address translation**.

If you want to connect to the Internet or other TCP/IP network using the host computer's dial-up networking or broadband connection and you are not able to give your virtual machine an IP address on the external network, NAT is often the easiest way to give your virtual machine access to that network.

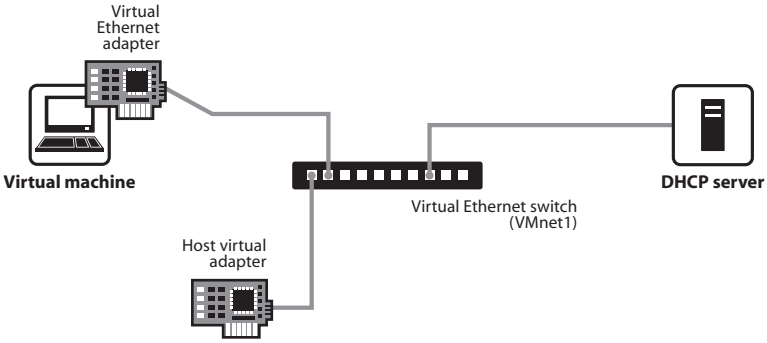
NAT also allows you to connect to a TCP/IP network using a Token Ring adapter on the host computer.

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.

If you select NAT, the virtual machine can use many standard TCP/IP protocols to connect to other machines on the external network. For example, you can use HTTP to browse Web sites, FTP to transfer files and Telnet to log on to other computers. In the default configuration, computers on the external network cannot initiate connections to the virtual machine. That means, for example, that the default configuration does not let you use the virtual machine as a Web server to send Web pages to computers on the external network.

If you make some other selection in the New Virtual Machine Wizard and later decide you want to use NAT, you can make that change in the virtual machine settings editor (**VM** > **Settings**). For details, see Changing the Networking Configuration on page 219.

Host-Only Networking



Host-only networking creates a network that is completely contained within the host computer.

A host-only network is set up automatically if you select **Use Host-Only Networking** in the New Virtual Machine Wizard. On Linux hosts, this selection is available only if you enabled the host-only networking option when you installed VMware Workstation.

Host-only networking provides a network connection between the virtual machine and the host computer, using a virtual Ethernet adapter that is visible to the host operating system. This approach can be useful if you need to set up an isolated virtual network.

If you use host-only networking, your virtual machine and the host virtual adapter are connected to a private TCP/IP network. Addresses on this network are provided by the VMware DHCP server.

If you make some other selection in the New Virtual Machine Wizard and later decide you want to use host-only networking, you can make that change in the virtual machine settings editor (**VM** > **Settings**). For details, see Changing the Networking Configuration on page 219.

Routing and Connection Sharing

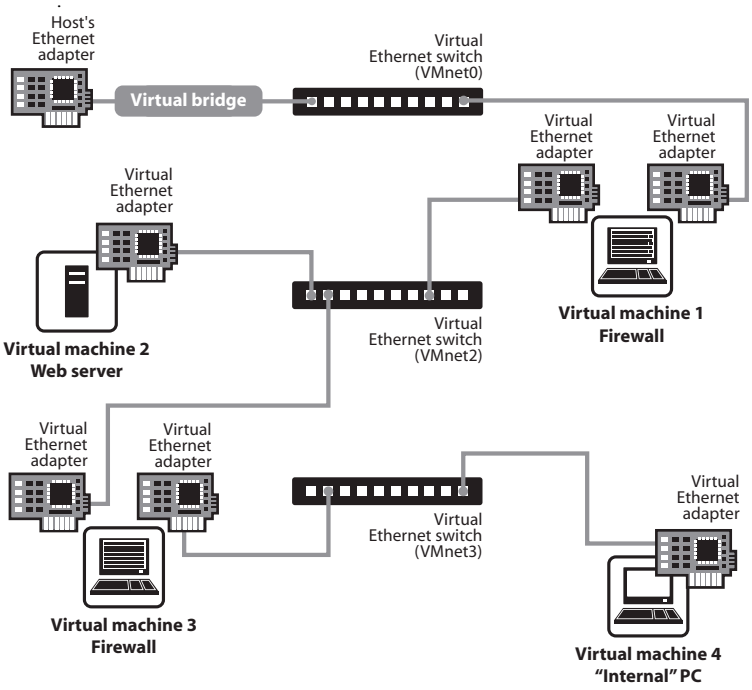
- If you install the proper routing or proxy software on your host computer, you can establish a connection between the host virtual Ethernet adapter and a physical network adapter on the host computer. This allows you, for example, to connect the virtual machine to a Token Ring or other non-Ethernet network.
- On a Windows 2000, Windows XP or Windows Server 2003 host computer, you can use host-only networking in combination with the Internet connection sharing feature in Windows to allow a virtual machine to use the host's dial-up networking adapter or other connection to the Internet. See your Windows documentation for details on configuring Internet connection sharing.

Custom Networking Configurations

The virtual networking components provided by VMware Workstation make it possible for you to create sophisticated virtual networks. The virtual networks can be connected to one or more external networks, or they may run entirely on the host computer.

Setting up networking components for your custom virtual network is a straightforward process. Before attempting to set up complex virtual networks, you should have a good understanding of how to configure network devices in your host and guest operating systems.

The sample configuration described in this section illustrates many of the ways you can combine devices on a virtual network. Other custom configurations are described in Advanced Networking Topics on page 228 and Understanding NAT on page 244.



In this custom configuration, a Web server connects through a firewall to an external network. An administrator's computer can connect to the Web server through a second firewall.

To set up this configuration, you must create four virtual machines and use the virtual machine settings editor to adjust the settings for their virtual Ethernet adapters. You also need to install the appropriate guest operating systems and application software in each virtual machine and make the appropriate networking settings in each virtual machine.

1. Set up four virtual machines using the New Virtual Machine Wizard.

   Create the first virtual machine with bridged networking so it can connect to an external network using the host computer's Ethernet adapter.

   Create the other three virtual machines without networking. You will set up their virtual Ethernet adapters in later steps.

2. Start VMware Workstation and open virtual machine 1. Do not power on the virtual machine.

   Use the virtual machine settings editor (**VM** > **Settings**) to add a second virtual network adapter, as described in Changing the Networking Configuration on page 219. Connect the second adapter to **Custom (VMnet2)**.

   Click **OK** to save the configuration and close the virtual machine settings editor.

3. If VMware Workstation is not running, start it. Open virtual machine 2. Do not power on the virtual machine.

   Use the virtual machine settings editor (**VM** > **Settings**) to add a virtual network adapter. Connect the adapter to **Custom (VMnet2)**.

   Click **OK** to save the configuration and close the virtual machine settings editor.

4. If VMware Workstation is not running, start it. Open virtual machine 3. Do not power on the virtual machine.

   Use the virtual machine settings editor (**VM** > **Settings**) to add a virtual network adapter. Connect the adapter to **Custom (VMnet2)**.

   Use the virtual machine settings editor to add a second virtual network adapter. Connect the adapter to **Custom (VMnet3)**.

   Click **OK** to save the configuration and close the virtual machine settings editor.

5. If VMware Workstation is not running, start it. Open virtual machine 4. Do not power on the virtual machine.

   Use the virtual machine settings editor (**VM** > **Settings**) to add a virtual network adapter. Connect the adapter to **Custom (VMnet3)**.

   Click **OK** to save the configuration and close the virtual machine settings editor.

6. Determine the network addresses used for VMnet2 and VMnet3.

   Note: On a Windows host, you may skip the steps for configuring network addresses manually and, instead, use Workstation's DHCP server. Go to **Edit** > **Virtual Network Settings** > **DHCP** and add VMnet2 and VMnet3 to the list of virtual networks served by the virtual DHCP server. Then skip to step 9.

   On a Windows host, open a command prompt on the host computer and run `ipconfig /all`. Note the network addresses used by each virtual adapter.

   On a Linux host, run `ifconfig` at the console or in a terminal window on the host computer. Note the network addresses used by each virtual switch.

7. Start VMware Workstation, open each virtual machine in turn and install the appropriate guest operating system.

8. Configure the networking in each guest operating system.

   For the bridged Ethernet adapter in virtual machine 1, use the networking settings needed for a connection to the external network. If the virtual machine gets its IP address from a DHCP server on the external network, the default settings should work.

   For the second Ethernet adapter in virtual machine 1, manually assign an IP address in the range you are using with VMnet2.

   In virtual machine 2, assign an IP address in the range you are using with VMnet2.

   In virtual machine 3, network adapters are connected to VMnet2 and VMnet3. Assign each adapter an IP address in the range you are using with the virtual network to which it is connected.

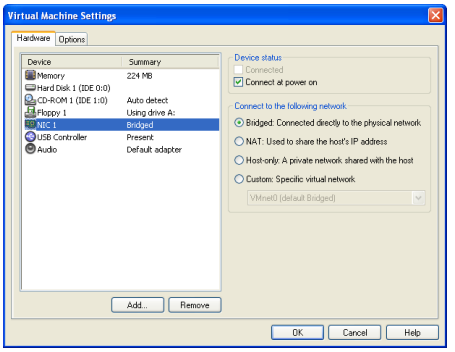
   In virtual machine 4, assign an IP address in the range you are using with VMnet3.

9. Install the necessary application software in each virtual machine.

Changing the Networking Configuration

Using the virtual machine settings editor (**VM** > **Settings**), you can add virtual Ethernet adapters to your virtual machine and change the configuration of existing adapters.

Adding and Modifying Virtual Network Adapters



To add a new virtual Ethernet adapter, follow these steps.

1. Be sure the virtual machine to which you want to add the adapter is powered off.
2. Open the virtual machine settings editor (**VM** > **Settings**).
3. Click **Add**.
4. The Add Hardware Wizard starts. Select **Network Adapter**. Click **Next**.
5. Select the network type you want to use — **Bridged**, **NAT**, **Host-only** or **Custom**.
6. If you select **Custom**, choose the VMnet network you want to use from the drop-down list.

   Note: Although VMnet0, VMnet1 and VMnet8 are available in this list, they are normally used for bridged, host-only and NAT configurations, respectively. Special steps are required to make them available for use in custom configurations. You should choose one of the other switches.
7. Click **Finish**. The new adapter is added.
8. Click **OK** to save your configuration and close the virtual machine settings editor.

To change the configuration of an existing virtual network adapter, follow these steps.

1. Open the virtual machine settings editor (**VM** > **Settings**).
2. Select the adapter you want to modify.

3. Select the network type you want to use — **Bridged**, **NAT**, **Host-only** or **Custom**.
4. If you select **Custom**, choose the VMnet virtual network you want to use for the network from the drop-down list.
5. Click **OK** to save your changes and close the virtual machine settings editor.
6. Be sure the guest operating system is configured to use an appropriate IP address on the new network. If the guest is using DHCP, release and renew the lease. If the IP address is set statically, be sure the guest has an address on the correct virtual network.

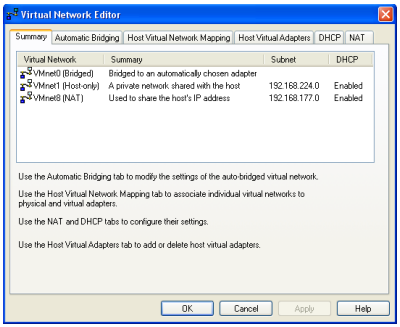
Configuring Bridged Networking Options on a Windows Host

You can view and change the settings for bridged networking on your host. These changes affect all virtual machines using bridged networking on the host.

You can decide which network adapters on your host to use for bridged networking. You can map specific network adapters to specific virtual networks (VMnets).

1. Open a VMware Workstation window.
2. Choose **Edit** > **Virtual Network Settings**.

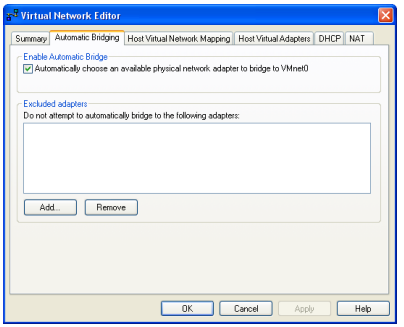
   The Virtual Network Editor appears, with the Summary tab active.



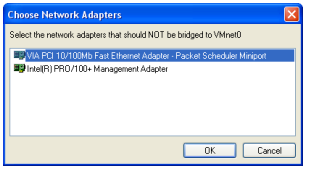
3. By default, the VMnet0 virtual network is set up in bridged mode and bridges to one of the active Ethernet adapters on the host computer.

   The choice of which adapter it uses is arbitrary. You can restrict the range of choices using options on the Automatic Bridging tab.

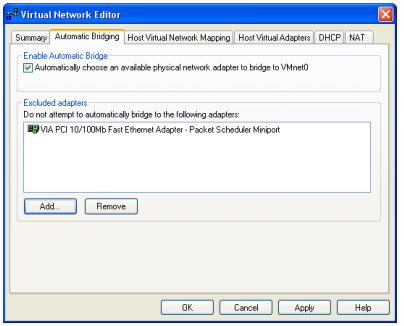
(Also shown are VMnet1, the default virtual network for host-only networking, and VMnet8, the default virtual network for NAT, if they are enabled in VMware Workstation.)



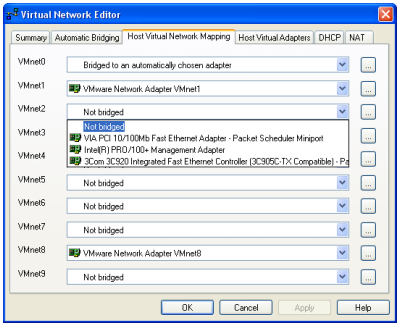
4. To exclude one or more physical Ethernet adapters from the list to which VMnet0 may be bridged, click the **Automatic Bridging** tab. To exclude an Ethernet adapter, click **Add** to add it to the list of excluded devices.



In the Choose Network Adapters dialog box, select the listing for the adapter you want to exclude, then click **OK**.

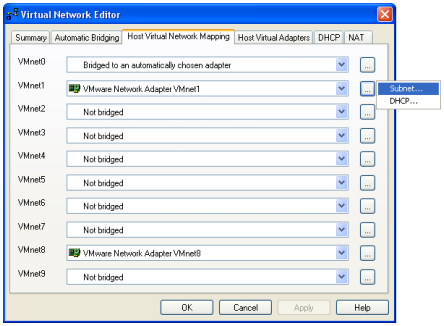


To remove an adapter from the list of excluded adapters, select its name in the list, then click **Remove**.

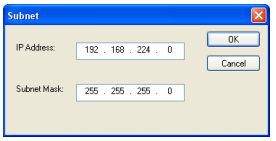


5. To designate a physical Ethernet adapter to be used for bridged networking on virtual switches named VMnet2–VMnet7, click the **Host Virtual Network Mapping** tab. Choose an adapter from the drop-down list beside the name of the virtual switch you want to use.

   Caution: Be careful when you change the bridged adapter mappings. If you re-assign a physical Ethernet adapter to a different virtual network, any virtual machine using the original network loses its network connectivity via that network. You must then change the setting for each affected virtual machine's network adapter individually. This can be especially troublesome if your host has only one physical Ethernet adapter and you reassign it to a VMnet other than VMnet0; even though the VMnet still appears to be bridged to an automatically chosen adapter, the only adapter it can use has been assigned to another VMnet.



6. To make changes to the subnet or the DHCP settings for a virtual network, click the button on the right that corresponds to the virtual network you want to configure, then choose **Subnet** or **DHCP**.

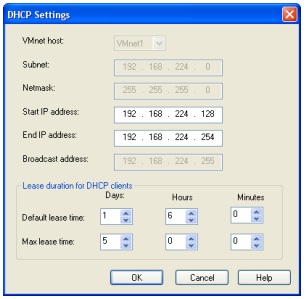


7. In the Subnet dialog box, you can change the subnet's IP address and the subnet mask.

   The address should specify a valid network address that is suitable for use with the subnet mask.

   The default subnet mask is 255.255.255.0 (a class-C network). Typically, this means you should modify only the third number in the IP address — for example, x in 192.168.x.0 or 172.16.x.0. In general, you should not change the subnet mask. Certain virtual network services may not work as well with a customized subnet mask.

   When you modify the network address or subnet mask, VMware Workstation automatically updates the IP address settings for other components — such as DHCP, NAT and host virtual adapter — on that virtual network to reflect the new settings. The specific settings that are automatically updated include DHCP lease range, DHCP server address, NAT gateway address and host virtual adapter IP address. However, if you have changed any of these settings from its default value — even if you have later changed the setting back to the default — VMware Workstation does not update that setting automatically. It presumes that custom settings are not to be modified.



8. In the DHCP settings dialog box, you can change the range of IP addresses provided by the DHCP server on a particular virtual network. You can also set the duration of leases provided to clients on the virtual network.
9. When you have made all the changes you want to make on all panels of the VMware Network Configuration dialog box, click **OK**.

Enabling, Disabling, Adding and Removing Host Virtual Adapters

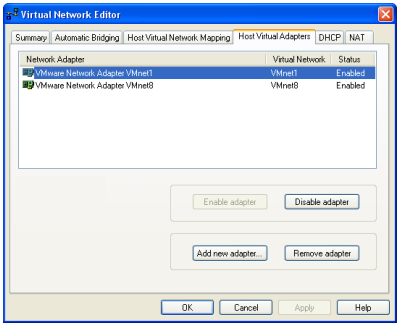
When you install VMware Workstation, two network adapters are added to the configuration of your host operating system — one that allows the host to connect to the host-only network and one that allows the host to connect to the NAT network.

If you are not using these adapters, you may wish to remove them (users on Windows hosts can choose to disable the adapters instead of removing them). The presence of these adapters has a slight performance cost, because broadcast packets must go to the extra adapters. On Windows networks, browsing your network may be slower than usual. And in some cases, these adapters interact with the host computer's networking configuration in undesirable ways.

Disabling a Host Virtual Adapter on a Windows 2000, Windows XP or Windows Server 2003 Host

Use the Virtual Network Editor to disable any unwanted adapters.

1. Choose **Edit** > **Virtual Network Settings** > **Host Virtual Adapters**.



2. Select the adapter you want to disable.
3. Click **Disable adapter**.
4. Click **OK**.

Disabling a Host Virtual Adapter on a Windows NT Host

Use the host operating system's networking control panel to disable any unwanted adapters.

1. Choose **Start** > **Settings** > **Control Panel**.
2. Double-click **Network**.
3. Click the **Bindings** tab.
4. Choose **All adapters**.
5. Select the VMware Virtual Ethernet Adapter you want to disable. The host-only network is VMnet1; the NAT network is VMnet8. Click **Disable**.

Enabling a Disabled Host Virtual Adapter on a Windows Host

Follow these steps to enable a host virtual adapter on a Windows host.

1. Go to **Edit** > **Virtual Network Settings** > **Host Virtual Adapters**.
2. Select the disabled adapter you want to enable.
3. Click **Enable adapter**.
4. Click **OK**.

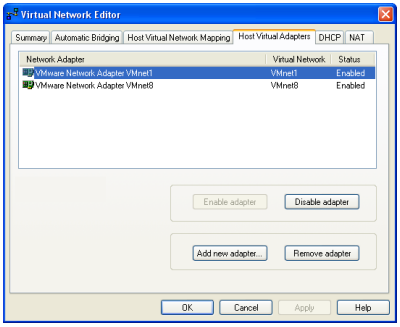
Adding a Host Virtual Adapter on a Windows Host

Follow these steps to add a host virtual adapter on a Windows host.

1. Go to **Edit** > **Virtual Network Settings** > **Host Virtual Adapters**.
2. Click **Add new adapter**.
3. Choose the virtual network on which you want to use the adapter and click **OK**.
4. Click **Apply**.
5. Click **OK** to close the Virtual Network Editor.
6. **Windows NT only:** Reboot the host computer.

Removing a Host Virtual Adapter on a Windows Host

1. Go to **Edit** > **Virtual Network Settings** > **Host Virtual Adapters**.



2. Select the adapter you want to remove, then click **Remove adapter**.
3. Click **OK**.

Removing a Host Virtual Adapter on a Linux Host

1. Become root and run the VMware Workstation configuration program.

```
su
vmware-config.pl
```

2. Watch for the following question

```
Do you want networking for your Virtual Machines? (yes/
no/help) [yes]
```

   Answer Yes if you still want to use any networking in your virtual machines, then continue to the next question.

   Otherwise, answer No to remove all networking.

3. If you answer Yes, the program prompts you to select the wizard or editor to edit your network configuration. Select editor. This is the only way to delete virtual network adapters without removing all of them.

```
Would you prefer to modify your existing networking
configuration using the wizard or the editor? (wizard/
editor/help) [wizard] editor
```

4. You see a list of virtual networks that have been configured. Select the network corresponding to the adapter you wish to disable.

```
The following virtual networks have been defined:
```

```
. vmnet0 is bridged to eth0
. vmnet1 is a host-only network on subnet 172.16.155.0.
. vmnet8 is NAT network on a private subnet 172.16.107.0.

Which virtual network do you wish to configure? (0-99) 1
```

5. You may be prompted to keep this virtual network. If you are sure you want to remove it, answer Yes to the question.

```
The network vmnet1 has been reserved for a host-only
network. You may change it, but it is highly recommended
that you use it as a host-only network. Are you sure you
want to modify it? (yes/no) [no] yes
```

6. When prompted about the type of virtual network, select None and the virtual network will be removed.

```
What type of virtual network do you wish to set vmnet1?
(bridged,hostonly,nat,none) [hostonly] none
```

Advanced Networking Topics

Selecting IP Addresses on a Host-Only Network or NAT Configuration

A host-only network uses a private virtual network. The host and all virtual machines configured for host-only networking are connected to the network through a virtual switch. Typically all the parties on this private network use the TCP/IP protocol suite, although other communication protocols may be used.

A network address translation (NAT) configuration also sets up a private network, which must be a TCP/IP network. The virtual machines configured for NAT are connected to that network through a virtual switch. The host computer is also connected to the private network used for NAT via a host virtual adapter.

Each virtual machine and the host must be assigned addresses on the private network. This is typically done using the DHCP server that comes with VMware Workstation. Note that this server does not service virtual (or physical) machines residing on bridged networks.

Addresses can also be assigned statically from a pool of addresses that are not assigned by the DHCP server.

When host-only networking is enabled at the time VMware Workstation is installed, the network number to use for the virtual network is automatically selected as an unused private IP network number. To find out what network is used on a Windows host, choose **Edit** > **Virtual Network Settings** and check the subnet number associated with the virtual network. On a Linux host, run `ifconfig` in a terminal.

A NAT configuration also uses an unused private network automatically selected when you install VMware Workstation. To find out what network is used on a Windows host, choose **Edit** > **Virtual Network Settings** and check the subnet number associated with the virtual network. On a Linux host, run `ifconfig` in a terminal.

Using DHCP to assign IP addresses is simpler and more automatic than statically assigning them. Most Windows operating systems, for example, come preconfigured to use DHCP at boot time, so Windows virtual machines can connect to the network the first time they are booted, without additional configuration. If you want your virtual machines to communicate with each other using names instead of IP addresses, however, you must set up a naming convention, a name server on the private network, or both. In that case it may be simpler to use static IP addresses.

In general, if you have virtual machines you intend to use frequently or for extended periods of time, it is probably most convenient to assign them static IP addresses or configure the VMware DHCP server to always assign the same IP address to each of these virtual machines.

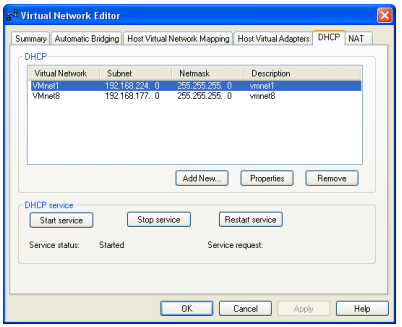
Configuring the DHCP Server on a Linux Host

On a Linux host, you configure the host-only DHCP server by editing the DHCP configuration file for VMnet1 (`/etc/vmware/vmnet1/dhcp/dhcp.conf`). To configure the DHCP server for the NAT network, edit the configuration file for VMnet8 (`/etc/vmware/vmnet8/dhcp/dhcp.conf`).

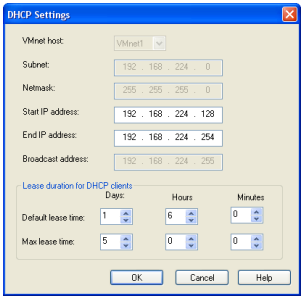
Editing the DHCP server configuration file requires information that is best obtained directly from the DHCP server documentation. Consult the manual pages `dhcpd(8)` and `dhcpd.conf(8)`.

Configuring the DHCP Server on a Windows Host

On a Windows host, you configure the DHCP server using the Virtual Network Editor (**Edit** > **Virtual Network Settings** > **DHCP**).



Select the virtual network for which you want to change settings and click **Properties**.



Make the desired changes, then click **OK**.

Choosing the Method for Assigning IP Addresses

For virtual machines that you do not expect to keep for long, use DHCP and let it allocate an IP address.

For each host-only or NAT network, the available IP addresses are split up using the conventions shown in the tables below, where <net> is the network number assigned to your host-only or NAT network. VMware Workstation always uses a Class C address for host-only and NAT networks.

Address Use on a Host-Only Network

Range	Address use	Example
<net>.1	Host machine	192.168.0.1
<net>.2–<net>.127	Static addresses	192.168.0.2–192.168.0.127
<net>.128–<net>.253	DHCP-assigned	192.168.0.128–192.168.0.253
<net>.254	DHCP server	192.168.0.254
<net>.255	Broadcasting	192.168.0.255

Address Use on a NAT Network

Range	Address use	Example
<net>.1	Host machine	192.168.0.1
<net>.2	NAT device	192.168.0.2
<net>.3–<net>.127	Static addresses	192.168.0.3–192.168.0.127
<net>.128–<net>.253	DHCP-assigned	192.168.0.128–192.168.0.253
<net>.254	DHCP server	192.168.0.254
<net>.255	Broadcasting	192.168.0.255

Avoiding IP Packet Leakage in a Host-Only Network

By design, each host-only network should be confined to the host machine on which it is set up. That is, no packets sent by virtual machines on this network should leak out to a physical network attached to the host. Packet leakage can occur only if a machine actively forwards packets. It is possible for the host machine or any virtual machine running on the host-only network to be configured in a way that permits packet leakage.

Windows Hosts

Windows NT systems and systems using server versions of Windows 2000 are capable of forwarding IP packets that are not addressed to them. By default, however, these systems come with IP packet forwarding disabled. IP forwarding is not an issue on Windows 2000 Professional, Windows XP Professional or Windows XP Home Edition hosts.

If you find packets leaking out of a host-only network on a Windows NT or Windows 2000 host computer, check to see if forwarding has been enabled on the host machine. If it is enabled, disable it.

On a Windows NT host, go to **Start** > **Settings** > **Control Panel** > **Networking**. Choose **TCP/IP**, click **Properties**, then click the **Routing** tab. Clear the check box to disable IP forwarding.

On a Windows 2000 or Windows Server 2003 host, go to **Start** > **Programs** > **Administrative Tools** > **Routing and Remote Access**. An icon on the left is labeled with the host name. If a green dot appears over the icon, IP forwarding is turned on. To turn it off, right-click the icon and disable **Routing and Remote Access**. A red dot appears, indicating that IP forwarding is disabled.

Windows 2000 Professional Users: The Windows 2000 Administration Tools are not installed on a Windows 2000 Professional system. However, you can install these tools from a Windows 2000 Server or Windows 2000 Advanced Server CD-ROM.

To install Windows 2000 Administration Tools on a local computer:

1. Open the i386 folder on the applicable Windows 2000 Server disc.
2. Double-click the `adminpak.msi` file. Follow the instructions that appear in the Windows 2000 Administration Tools Setup wizard.
3. After Windows 2000 Administration Tools are installed, you can access most of the server administrative tools by choosing **Start** > **Programs** > **Administrative Tools**.

Linux Hosts

If you find packets leaking out of a host-only network on a Linux host computer, check to see if forwarding has mistakenly been enabled on the host machine. If it is enabled, disable it.

For many Linux systems, disable forwarding by writing a 0 (zero) to the special file `/proc/sys/net/ipv4/ip_forward`. As root, enter this command:

```
echo 0 > /proc/sys/net/ipv4/ip_forward
```

Other Linux systems have a system configuration option that you can set. The method depends on your Linux distribution. You may use a control panel, specify a setting at the time you compile your kernel or possibly enter a specification when you boot your system. Consult your operating system documentation for details on the method to use with your particular distribution.

Using Filtering

If the host computer has multiple network adapters, it may be intentionally configured to do IP forwarding. If that is the case, you do not want to disable forwarding. In that case, to avoid packet leakage you must enable a packet filtering facility and specify that packets from the host-only network should not be sent outside the host computer. Consult your operating system documentation for details on how to configure packet filtering.

Leaks from a Virtual Machine

Virtual machines may leak packets, as well. For example, if you use Dial-Up Networking support in a virtual machine and packet forwarding is enabled, host-only network traffic may leak out through the dial-up connection.

To prevent the leakage, be sure packet forwarding is disabled in your guest operating system.

Maintaining and Changing the MAC Address of a Virtual Machine

When a virtual machine is powered on, VMware Workstation automatically assigns each of its virtual network adapters an Ethernet MAC address. MAC stands for media access control. A MAC address is the unique address assigned to each Ethernet network device.

The software guarantees that virtual machines are assigned unique MAC addresses within a given host system. In most cases, the virtual machine is assigned the same MAC address every time it is powered on, so long as the virtual machine is not moved (the path and filename for the virtual machine's configuration file must remain the same) and no changes are made to certain settings in that file.

In addition, VMware Workstation does its best, but cannot guarantee, to automatically assign unique MAC addresses for virtual machines running on multiple host systems.

Avoiding MAC Changes

To avoid changes in the MAC address automatically assigned to a virtual machine, you must not move the virtual machine's configuration file. Moving it to a different host

computer or even moving it to a different location on the same host computer changes the MAC address.

You also need to be sure not to change certain settings in the virtual machine's configuration files. If you never edit the configuration file by hand and do not remove the virtual Ethernet adapter, these settings remain untouched. If you do edit the configuration file by hand, be sure not to remove or change the following options:

```
ethernet[n].generatedAddress
ethernet[n].addressType
ethernet[n].generatedAddressOffset
uuid.location
uuid.bios
ethernet[n].present
```

In these options, `[n]` is the number of the virtual Ethernet adapter, for example `ethernet0`.

Note: To preserve a virtual Ethernet adapter's MAC address, you also must be careful not to remove it. If you remove the adapter, then recreate it, it may receive a different MAC address.

Manually Assigning a MAC Address

If you want to guarantee that the same MAC address is assigned to a given virtual machine every time, even if the virtual machine is moved, or if you want to guarantee a unique MAC address for each virtual machine within a networked environment, you can assign the address manually instead of allowing VMware Workstation to assign it automatically.

To assign the same, unique MAC address to any virtual machine manually, use a text editor to remove three lines from the configuration file and add one line. The configuration file has a `.vmx` extension at the end of the filename. On a Linux host, a virtual machine created with an earlier VMware product may have a configuration file with a `.cfg` extension.

Remove the three lines that begin with the following from the configuration file:

```
ethernet[n].generatedAddress
ethernet[n].addressType
ethernet[n].generatedAddressOffset
```

In these options, `[n]` is the number of the virtual Ethernet adapter — for example `ethernet0`.

Add the following line to the configuration file:

```
ethernet[n].address = 00:50:56:XX:YY:ZZ
```

In this line, XX must be a valid hexadecimal number between 00h and 3Fh, and YY and ZZ must be valid hexadecimal numbers between 00h and FFh. Because VMware Workstation virtual machines do not support arbitrary MAC addresses, you must use the above format.

So long as you choose a value for XX:YY:ZZ that is unique among your hard-coded addresses (where XX is a valid hexadecimal number between 00h and 3Fh, and YY and ZZ are valid hexadecimal numbers between 00h and FFh), conflicts between the automatically assigned MAC addresses and the manually assigned ones should never occur.

Controlling Routing Information for a Host-Only Network on a Linux Host

A host-only network is a full-fledged network. It has a network interface associated with it (VMnet1) that is marked "up" at the time the host operating system is booted. Consequently, routing server processes that operate on the host operating system, such as routed and gated, automatically discover it and propagate information on how to reach it unless you explicitly configure them not to do so.

If either of these programs is being run only to receive routing information, the easiest solution is to run it with a -q option so that it does not supply routing information, only receives it.

If, however, they are running because they are to supply routing information, then you need to configure them so they do not advertise routes to the host-only network.

Unfortunately, the version of routed that comes with many distributions of Linux has no support for specifying that an interface should not be advertised. Consult the routed(8) manual page for your system in case you have a more contemporary version of the software.

For gated, configuration is involved. You need to explicitly exclude the VMnet1 interface from any protocol activity. If you need to run virtual machines on a host-only network on a multihomed system where gated is used and have problems doing so, please contact VMware technical support by submitting a support request at *www.vmware.com/requestsupport*.

Other Potential Issues with Host-Only Networking on a Linux Host

The following are common issues you may encounter when you are configuring a host-only network.

DHCPD on the Linux Host Does Not Work after VMware Workstation Installation

If you were running the DHCP server program `dhcpd` on your machine before installing VMware Workstation, it probably was configured to respond to DHCP requests from clients on any network interface present on the machine. When host-only networking is configured, an additional network interface, VMnet1, is marked "up" and available for use, and `dhcpd` may notice this.

In such cases, some `dhcpd` implementations abort if their configuration files do not include a subnet specification for the interface — even if `dhcpd` is not supposed to respond to messages that arrive through the interface.

The best solution to this problem is to add a line in the following format to the `dhcpd` configuration file:

```
subnet <net>.0 netmask 255.255.255.0 {}
```

`<net>` is the network number assigned to your host-only network — for example, 192.168.0. This line in the configuration file informs `dhcpd` about the host-only network and tells it explicitly not to respond to any DHCP requests it sees coming from it.

An alternative solution is to explicitly state the set of network interfaces that you want `dhcpd` to listen to each time you start the program. For example, if your machine has one Ethernet interface, `eth0`, then each time you start `dhcpd`, list it on the command line:

```
dhcpd eth0
```

This keeps `dhcpd` from probing for all available network interfaces.

If the above solutions do not work for your DHCP server program, then it likely is old. You can try upgrading to a more current version such as the DHCP software available from the ISC(*www.isc.org*).

DHCP and Dynamic Domain Name Service (DDNS)

DHCP can be used to hand out IP addresses as well as other information, such as the identity of a host running a name server and the nearest router or gateway. The DHCP server in VMware Workstation 4 does not provide a means to dynamically establish a relationship between the IP address it assigns and a client's name (that is, to update a DNS server using DDNS).

If you want to use names to communicate with other virtual machines you must either edit the DHCP configuration file for VMnet1 (`/etc/vmware/vmnet1.conf`) or use IP addresses that are statically bound to a host name. Editing the DHCP server configuration file requires information that is best

obtained directly from the DHCP server documentation. Consult the manual pages `dhcpd(8)` and `dhcpd.conf(8)`.

Setting Up a Second Bridged Network Interface on a Linux Host

If you have two Ethernet adapters installed on your host computer, connected to two different networks, you may want your virtual machines on that host computer to bridge to both Ethernet adapters so the virtual machines can access either or both physical networks.

When you install VMware Workstation on a host computer with multiple Ethernet adapters, you have the option of configuring more than one bridged network. You can also configure additional bridged networks at any time by rerunning `vmware-config.pl`.

1. On the host computer, become root (`su`) and run the VMware Workstation configuration program.

   ```
   vmware-config.pl
   ```

2. If you have more than one physical Ethernet adapter, one of the prompts you see is similar to this:

   ```
   The following bridged networks have been defined:
   . vmnet0 is bridged to eth0
   Do you wish to configure another bridged network? (yes/no)
   [no]
   ```

   Enter `yes`.

3. If you have additional physical Ethernet adapters not yet connected to a bridged network, the prompt is repeated, showing information about all currently configured bridged networks.

4. When you have set up all the bridged networks you want, enter `no`.

Setting Up Two Separate Host-Only Networks

For some configurations, you may need to set up more than one host-only network on the same host computer.

You may, for example, want to have two virtual machines connected to one host-only network, and at the same time have other virtual machines connected to another host-only network so the network traffic on each network is isolated.

Or you may want to test routing between two virtual networks. Or test a virtual machine with multiple network interface cards — without using any physical Ethernet adapters.

On Windows hosts, the first host-only network is set up automatically when you install VMware Workstation.

On Linux hosts, the first host-only network is set up when you run the `vmware-config.pl` program after you install VMware Workstation, provided you agree to install host-only networking. If you did not agree to use host-only networking, you need to run the program again to set up host-only networking.

To set up the second host-only network, follow the steps outlined below for your host operating system.

Setting Up the Second Host-Only Interface on a Windows Host

Follow these steps to set up the second host-only interface on a Windows host.

1. Go to **Edit** > **Virtual Network Settings** > **Host Virtual Adapters**.
2. Click **Add new adapter**.
3. Choose the virtual network on which you want to use the adapter and click **OK**.
4. Click **Apply**.
5. Click **OK** to close the Virtual Network Editor.

Setting Up the Second Host-Only Interface on a Linux Host

1. As root (`su`), run the VMware Workstation configuration program.

   ```
   /usr/bin/vmware-config.pl
   ```

2. Use the wizard to modify your configuration. After asking about a NAT network, the program asks:

   ```
   Do you want to be able to use host-only networking in your
   virtual machines?
   ```

   Answer Yes.

   The wizard reports on host-only networks that you have already set up on the host or, if none is present, configures the first host-only network.

3. The wizard asks:

   ```
   Do you wish to configure another host-only network?
   ```

   Answer Yes.

   Repeat this step until you have as many host-only networks as you want. Then answer No.

4. Complete the remaining steps in the wizard. When it is finished, it restarts all services used by VMware Workstation.

5. Run `ifconfig`. You should see at least four network interfaces — `eth0`, `lo`, `vmnet1` and `vmnet2`. If the VMnet interfaces do not show up immediately, wait for a minute, then run the command again. These four interfaces should have different IP address on separate subnets.

Configuring the Virtual Machines

Now you have two host-only interfaces (VMnet1 and VMnet2). You are ready to set up your virtual machines for one of the following configurations:

1. The virtual machine is configured with one virtual Ethernet adapter, and that virtual adapter is connected to the default host-only interface (VMnet 1).
2. The virtual machine is configured with one virtual Ethernet adapter, and that virtual adapter is connected to the newly created host-only interface (VMnet2).
3. The virtual machine is configured with two virtual Ethernet adapters. One virtual adapter is connected to the default host-only interface (VMnet1) and the other virtual adapter is connected to the newly created host-only interface (VMnet2).

Configuration 1 – Connect to the Default Host-Only Interface

1. Create the virtual machine using the New Virtual Machine Wizard or use an existing virtual machine.
2. Launch VMware Workstation and open the virtual machine.
3. Edit the configuration using the virtual machine settings editor (**VM** > **Settings**).

   Select **Network Adapter**, then select **Host-only (VMnet1)** from the drop-down list on the right.

   If no network adapter is shown in the list of devices, click **Add**, then use the Add Hardware Wizard to add an adapter.

Configuration 2 – Connect to the Newly Created Host-Only Interface

1. Create the virtual machine using the New Virtual Machine Wizard or use an existing virtual machine.
2. Launch VMware Workstation and open the virtual machine.
3. Edit the configuration using the virtual machine settings editor (**VM** > **Settings**).

   Select **Network Adapter**, then select **Custom (VMnet2)** from the drop-down list on the right.

   If no network adapter is shown in the list of devices, click **Add**, then use the Add Hardware Wizard to add an adapter.

Configuration 3 – Connect to Two Host-Only Interfaces

1. Create the virtual machine using the New Virtual Machine Wizard or use an existing virtual machine.
2. Launch VMware Workstation and open the virtual machine.
3. Edit the configuration using the virtual machine settings editor (**VM** > **Settings**).

   Select the first network adapter in the list of devices, then select **Host-only (VMnet1)** from the drop-down list on the right. Select the second network adapter in the list of devices, then select **Custom (VMnet2)** from the drop-down list on the right.

   If you need to add one or more network adapters, click **Add**, then use the Add Hardware Wizard to add an adapter.

At this point you can power on the virtual machine and install your guest operating system. In configurations 1 and 2 you see one AMD PCNet Family Adapter. In configuration 3 you see two AMD PCNet Family Adapters within the guest. Configure the Ethernet adapters as you would physical adapters on a physical computer, giving each an IP address on the appropriate VMnet subnet.

On Windows hosts, you can open a command prompt and run `ipconfig /all` to see what IP addresses each host-only network is using.

On Linux hosts, you can open a terminal and run `ifconfig` to see what IP addresses each host-only network is using.

Routing between Two Host-Only Networks

If you are setting up a complex test network using virtual machines, you may want to have two independent host-only networks with a router between them.

There are two basic approaches. In one, the router software runs on the host computer. In the other, the router software runs in its own virtual machine. In both cases, you need two host-only interfaces.

The examples described here outline the simplest case, with one virtual machine on each of the host-only networks. For more complex configurations, you can add more virtual machines and host-only networks as appropriate.

Setting Up the First Host-Only Interface

On Windows hosts, the first host-only network is set up automatically when you install VMware Workstation.

On Linux hosts, the first host-only network was set up when you ran the `vmware-config.pl` program after you installed VMware Workstation, provided you agreed

to install host-only networking. If you did not agree to use host-only networking, you need to run the program again to set up host-only networking.

Setting Up the Second Host-Only Interface – Windows Host

Follow these steps to set up the second host-only interface on a Windows host.

1. Go to **Edit** > **Virtual Network Settings** > **Host Virtual Adapters**.
2. Click **Add new adapter**.
3. Choose the virtual network on which you want to use the adapter and click **OK**.
4. Click **Apply**.
5. Click **OK** to close the Virtual Network Editor.

Setting Up the Second Host-Only Interface – Linux Host

1. As root (`su`), run the VMware Workstation configuration program.

   ```
   /usr/bin/vmware-config.pl
   ```

2. Use the wizard to modify your configuration. After asking about a NAT network, the program asks:

   ```
   Do you want to be able to use host-only networking in your
   virtual machines?
   ```

   Answer Yes.

   The wizard reports on host-only networks that you have already set up on the host or, if none is present, configures the first host-only network.

3. The wizard asks:

   ```
   Do you wish to configure another host-only network?
   ```

   Answer Yes.

   Repeat this step until you have as many host-only networks as you want. Then answer No.

4. Complete the wizard. When it is finished, it restarts all services used by VMware Workstation.
5. Run `ifconfig`. You should see at least four network interfaces — `eth0`, `lo`, `vmnet1` and `vmnet2`. If the VMnet interfaces do not show up immediately, wait for a minute, then run the command again. These four interfaces should have different IP address on separate subnets.

Setting Up the Virtual Machines

Now you have two host-only network adapters on the host computer. Each is connected to its own virtual switch (VMnet1 and VMnet2). You are ready to create and configure your virtual machines and connect them to the appropriate virtual switches.

Virtual Machine 1 – Connected to the Default Host-Only Interface

1. Create the virtual machine using the New Virtual Machine Wizard or use an existing virtual machine.
2. Launch VMware Workstation and open the virtual machine.
3. Edit the configuration using the virtual machine settings editor (**VM** > **Settings**).

   Select **Network Adapter** and select **Host-only (VMnet1)** from the drop-down list on the right.

   If no network adapter is shown in the list of devices, click **Add**, then use the Add Hardware Wizard to add an adapter.

Virtual Machine 2 – Connected to the Newly Created Host-Only Interface

1. Create the virtual machine using the New Virtual Machine Wizard or use an existing virtual machine.
2. Launch VMware Workstation and open the virtual machine.
3. Edit the configuration using the virtual machine settings editor (**VM** > **Settings**).

   Select **Network Adapter** and select **Custom (VMnet2)** from the drop-down list on the right.

   If no network adapter is shown in the list of devices, click **Add**, then use the Add Hardware Wizard to add an adapter.

If you plan to run the router software on your host computer, you can skip the next section.

Virtual Machine 3 – Connected to Both Host-Only Interfaces

If you plan to run the router software on a virtual machine, set up a third virtual machine for that purpose.

1. Create the virtual machine using the New Virtual Machine Wizard or use an existing virtual machine.
2. Launch VMware Workstation and open the virtual machine.
3. Edit the configuration using the virtual machine settings editor (**VM** > **Settings**).

Select the first network adapter in the list of devices and select **Host-only (VMnet1)** from the drop-down list on the right. Select the second network adapter in the list of devices, then select **Custom (VMnet2)** from the drop-down list on the right.

If you need to add one or more network adapters, click **Add**, then use the Add Hardware Wizard to add an adapter.

Now you need to configure the networking components on the host and in the virtual machines. The recommended approach uses static IP addresses for all the virtual machines.

1. Stop the VMnet DHCP server service.

   Windows host: Choose **Edit** > **Virtual Network Settings** > **DHCP** and click **Stop service**.

   Linux host: Stop the `vmnet-dhcpd` service.

   ```
   killall -TERM vmnet-dhcpd
   ```

2. Install guest operating systems in each of the virtual machines.
3. Install the router software — on the host computer or in the third virtual machine, depending on the approach you are using.
4. Configure networking in the first two virtual machines to use addresses on the appropriate host-only network.

   On Windows hosts, you can open a command prompt and run `ipconfig /all` to see what IP addresses each host-only network is using.

   On Linux hosts, you can open a terminal and run `ifconfig` to see what IP addresses each host-only network is using.

5. If you are running the router on the host computer, assign default router addresses based on the addresses of the host-only adapters on the host computer. In the first virtual machine's networking configuration, the default router address should be the IP address for the host-only adapter connected to VMnet1. In the second virtual machine's networking configuration, the default router address should be the IP address for the host-only adapter connected to VMnet2.

   If you are running the router software on the third virtual machine, set the default router addresses in the first two virtual machines based on those used by the third virtual machine. In the first virtual machine's networking configuration, the default router address should be the IP address for the third virtual machine's Ethernet adapter connected to VMnet1. In the second virtual machine's

networking configuration, the default router address should be the IP address for the third virtual machine's Ethernet adapter connected to VMnet2.

At this point you should be able to ping the router machine from virtual machines one and two. And if the router software is set up correctly, you should be able to communicate between the first and second virtual machines.

Using Virtual Ethernet Adapters in Promiscuous Mode on a Linux Host

VMware Workstation does not allow the virtual Ethernet adapter to go into promiscuous mode unless the user running VMware Workstation has permission to make that setting. This follows the standard Linux practice that only root can put a network interface into promiscuous mode.

When you install and configure VMware Workstation, you must run the installation as root. VMware Workstation creates the VMnet devices with root ownership and root group ownership, which means that only root has read and write permissions to the devices.

To set the virtual machine's Ethernet adapter to promiscuous mode, you must launch VMware Workstation as root because you must have read and write access to the VMnet device. For example, if you are using bridged networking, you must have access to `/dev/vmnet0`.

To grant selected other users read and write access to the VMnet device, you can create a new group, add the appropriate users to the group and grant that group read and write access to the appropriate device. You must make these changes on the host operating system as root (`su`). For example, you can enter the following commands:

```
chgrp <newgroup> /dev/vmnet0
chmod g+rw /dev/vmnet0
```

`<newgroup>` is the group that should have the ability to set `vmnet0` to promiscuous mode.

If you want all users to be able to set the virtual Ethernet Adapter (`/dev/vmnet0` in our example) to promiscuous mode, you can simply run the following command on the host operating system as root:

```
chmod a+rw /dev/vmnet0
```

Understanding NAT

Network address translation — or NAT — is a networking option that first appeared in VMware Workstation 3.0.

NAT provides a simple way for virtual machines to use most client applications over almost any type of network connection available to the host. The only requirement is that the network connection must support TCP/IP.

NAT is useful when you have a limited supply of IP addresses or are connected to the network through a non-Ethernet network adapter. NAT works by translating addresses of virtual machines in a private VMnet network to that of the host machine. When a virtual machine sends a request to access a network resource, it appears to the network resource as if the request came from the host machine.

NAT uses the host's own network resources to connect to the external network. Thus, any TCP/IP network resource to which the host has access should be available through the NAT connection.

The chief advantage of NAT is that it provides a transparent, easy to configure way for virtual machines to gain access to network resources.

Using NAT

The NAT device is connected to the VMnet8 virtual switch. Virtual machines connected to the NAT network also use the VMnet8 virtual switch.

The NAT device waits for packets coming from virtual machines on the VMnet8 virtual network. When a packet arrives, the NAT device translates the address of the virtual machine to that of the host before forwarding the packet to the external network. When data arrives from the external network for the virtual machine on the private network, the NAT device receives the data, replaces the network address with that of the virtual machine and forwards the data to the virtual machine on the virtual network. This translation occurs automatically and requires minimal configuration on the guest and the host.

The Host Computer and the NAT Network

The host computer has a host virtual adapter on the NAT network (identical to the host virtual adapter on the host-only network). This adapter allows the host and the virtual machines to communicate with each other for such purposes as file sharing. The NAT never forwards traffic from the host virtual adapter.

DHCP on the NAT Network

In order to make networking configuration easy, a DHCP server is automatically installed when you install VMware Workstation. Virtual machines running on the network with the NAT device can dynamically obtain their IP addresses by sending out DHCP requests. The DHCP server on the NAT network, which is also used in host-only networking configurations, dynamically allocates IP addresses in the range of <net>.128 through <net>.254, where <net> is the network number assigned to your NAT network. VMware Workstation always uses a Class C address for NAT networks. IP addresses <net>.3 through <net>.127 can be used for static IP addresses. IP address <net>.1 is reserved for the host adapter; <net>.2 is reserved for the NAT device.

In addition to the IP address, the DHCP server on the NAT network also sends out additional configuration information that enables the virtual machine to operate automatically. This information includes the default gateway and the DNS server. In the DHCP response, the NAT device instructs the virtual machine to use the IP address <net>.2 as the default gateway and DNS server. This causes all IP packets destined for the external network and DNS requests to be forwarded to the NAT device.

DNS on the NAT Network

The NAT device acts as a DNS server for the virtual machines on the NAT network. Actually, the NAT device is a DNS proxy and merely forwards DNS requests from the virtual machines to a DNS server that is known by the host. Responses come back to the NAT device, which then forwards them to the virtual machines.

If they get their configuration information from DHCP, the virtual machines on the NAT network automatically use the NAT device as the DNS server. However, the virtual machines can be statically configured to use another DNS server.

The virtual machines in the private NAT network are not, themselves, accessible via DNS. If you want the virtual machines running on the NAT network to access each other by DNS names, you must set up a private DNS server connected to the NAT network.

External Access from the NAT Network

In general, any protocol using TCP or UDP can be used automatically by a virtual machine on the NAT network so long as the virtual machine initiates the network connection. This is true for most client applications such as Web browsing, Telnet, passive-mode FTP and downloading streaming video. Additional protocol support has been built into the NAT device to allow FTP and ICMP echo (ping) to work completely transparently through the NAT.

On the external network to which the host is connected, any virtual machine on the NAT network appears to be the host itself, because its network traffic uses the host's IP address. It is able to send and receive data using TCP/IP to any machine that is accessible from the host.

Before any such communication can occur, the NAT device must set up a mapping between the virtual machine's address on the private NAT network and the host's network address on the external network.

When a virtual machine initiates a network connection with another network resource, this mapping is created automatically. The operation is perfectly transparent to the user of the virtual machine on the NAT network. No additional work needs to be done to let the virtual machine access the external network.

The same cannot be said for network connections that are initiated from the external network to a virtual machine on the NAT network.

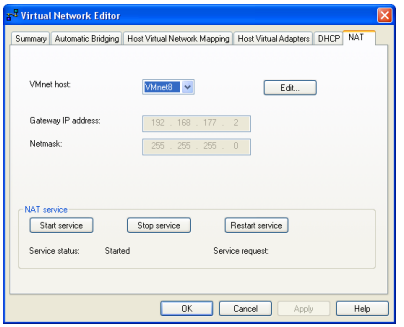
When a machine on the external network attempts to initiate a connection with a virtual machine on the NAT network, it cannot reach the virtual machine because the NAT device does not forward the request. Network connections that are initiated from outside the NAT network are not transparent.

However, it is possible to configure port forwarding manually on the NAT device so network traffic destined for a certain port can still be forwarded automatically to a virtual machine on the NAT network. For details, see Advanced NAT Configuration below.

File sharing of the type used by Windows operating systems and Samba is possible among computers on the NAT network — including virtual machines and the host computer. If you are using WINS servers on your network, a virtual machine using NAT networking can access shared files and folders on the host that are known by the WINS server so long as those shared files and folders are in the same workgroup or domain.

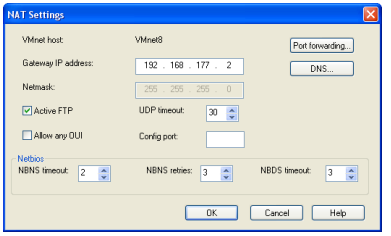
Advanced NAT Configuration

Windows host: Configure the NAT device using the Virtual Network Editor (**Edit** > **Virtual Network Settings** > **NAT**).



You can stop and start the virtual NAT device by clicking the appropriate buttons.

To edit NAT settings for a virtual network, choose it from the drop-down menu, then click **Edit**.



Change any NAT settings you wish. Click the appropriate button to set up or change port forwarding or to specify DNS servers the virtual NAT device should use.

Linux host: Use the NAT configuration file on the host to configure the NAT device. This file is `/etc/vmware/vmnet8/nat/nat.conf`.

The configuration file is divided into sections. Each section configures a part of the NAT device. Text surrounded by square brackets — such as `[host]` — marks the beginning of a section. In each section is a configuration parameter that can be set. The configuration parameters take the form `ip = 192.168.27.1/24`.

For an example of a NAT configuration file, see Sample Linux vmnetnat.conf File on page 253. The configuration file variables are described below.

The [host] Section

`ip`
The IP address that the NAT device should use. It can optionally be followed by a slash and the number of bits in the subnet.

`netmask`
The subnet mask to use for the NAT. DHCP addresses are allocated from this range of addresses.

`configport`
A port that can be used to access status information about the NAT.

`device`
The VMnet device to use. Windows devices are of the form `VMnet<x>` where `<x>` is the number of the VMnet. Linux devices are of the form `/dev/vmnet<x>`.

`activeFTP`
Flag to indicate if active FTP is to be allowed. Active FTP allows incoming connections to be opened by the remote FTP server. Turning this off means that only passive mode FTP works. Set to `0` to turn it off.

The [udp] Section

`timeout`
Number of minutes to keep the UDP mapping for the NAT.

The [dns] Section

This section is for Windows hosts only. Linux does not use this section.

`policy`
Policy to use for DNS forwarding. Accepted values include `order`, `rotate`, and `burst`.

- `order` — send one DNS request at a time in order of the name servers
- `rotate` — send one DNS request at a time and rotate through the DNS servers
- `burst` — send to three servers and wait for the first one to respond

`timeout`
Time in seconds before retrying a DNS request.

`retries`
Number of retries before the NAT device gives up on a DNS request.

`autodetect`
Flag to indicate if the NAT should automatically detect the DNS servers available to the host.

`nameserver1`
IP address of a DNS server to use.

`nameserver2`
IP address of a DNS server to use.

`nameserver3`
IP address of a DNS server to use.

If autodetect is on and some name servers are specified, the DNS servers specified in `nameserver1`, `nameserver2` and `nameserver3` are added before the list of detected DNS servers.

The [netbios] Section
This section applies to Windows hosts only. Linux does not use this section.

`nbnsTimeout = 2`
Timeout for NBNS queries.

`nbnsRetries = 3`
Number of retries for each NBNS query.

`nbdsTimeout = 3`
Timeout for NBDS queries.

The [incomingtcp] Section
This section is used to configure TCP port forwarding for NAT. In this section, you can assign a port number to an IP address and port number on a virtual machine.

The following line shows the format used in this section.

```
8887 = 192.168.27.128:21
```

This example creates a mapping from port 8887 on the host to the IP address 192.168.27.128 and port 21. When this mapping is set and an external machine connects to the host at port 8887, the network packets are automatically forwarded to port 21 (the standard port for FTP) on the virtual machine with IP address 192.168.27.128.

The [incomingudp] Section
This section is used to configure UDP port forwarding for NAT. In this section, you can assign a port number to an IP address and port number on a virtual machine.

The following line shows the format used in this section. It illustrates a way to forward X server traffic from the host port 6000 to the virtual machine's port 6001.

```
6000 = 192.168.27.128:6001
```

This example creates a mapping from port 6000 on the host to the IP address 192.168.27.128 and port 6001. When this mapping is set and an external machine connects to the host at port 6000, the network packets are automatically forwarded to port 6001 on the virtual machine with IP address 192.168.27.128.

Custom NAT and DHCP Configuration on a Windows Host

If you are an advanced user on a Windows host computer, you may wish to make custom configuration settings by editing the NAT and DHCP configuration files. If your host operating system is installed on the C drive, the configuration files for NAT and DHCP are in the following locations:

- **NAT:** `C:\Documents and Settings\All Users\Application Data\VMware\vmnetnat.conf`
- **DHCP:** `C:\Documents and Settings\All Users\Application Data\VMware\vmnetdhcp.conf`

Note: In VMware Workstation 4, you can change many key NAT and DCHP settings using the Virtual Network Editor (**Edit** > **Virtual Network Settings**). However, if you have made manual changes to the configuration files, some or all of those changes may be lost when you use the Virtual Network Editor. If you have made manual changes, you should make backup copies of the files before changing any settings in the Virtual Network Editor. After making changes in the Virtual Network Editor, you can copy your manual changes back into the appropriate configuration files.

Specifying Connections from Ports Below 1024

When a client machine makes a TCP or UDP connection to a server, the connection comes from a particular port on the client (the source port) and connects to a particular port on the server (the destination port). For security reasons, some servers accept connections only from source ports below 1024. You may see this configuration on machines used as NFS file servers, for example.

If a virtual machine using NAT attempts to connect to a server that requires the client to use a source port below 1024, it is important that the NAT device forward the request from a port below 1024. Beginning in VMware Workstation 4.5, you can specify this behavior in the `vmnetnat.conf` file.

This behavior is controlled by entries in sections headed `[privilegedUDP]` and `{privilegedTCP]`. You may need to add settings to or modify settings in either or both of these sections, depending on the kind of connection you need to make.

You can set two parameters, each of which appears on a separate line.

`autodetect = <n>`
The autodetect setting determines whether the VMware NAT device automatically attempts to map virtual machine source ports below 1024 to NAT source ports below 1024. A setting of `1` means true. A setting of `0` means false. On a Windows host, the default is `1` (true). On a Linux host, the default is `0` (false).

`port = <n>`
The port setting specifies a destination port (where `<n>` is the port on the server that accepts the connection from the client). Whenever a virtual machine connects to the specified port on any server, the NAT device attempts to make the connection from a source port below 1024. You may include one or more port settings in the `[privilegedUDP]` or `[privilegedTCP]` section or in both sections, as required for the connections you need to make. Enter each port setting on a separate line.

Considerations for Using NAT

Because NAT requires that every packet sent and received from virtual machines is in the NAT network, there is an unavoidable performance penalty. Our experiments show that the penalty is minor for dial-up and DSL connections and performance is adequate for most VMware Workstation uses.

NAT is not perfectly transparent. It does not normally allow connections to be initiated from outside the network, although you can set up server connections by manually configuring the NAT device. The practical result is that some TCP and UDP protocols that require a connection be initiated from the server machine — some peer to peer applications, for example — do not work automatically, and some may not work at all.

A standard NAT configuration provides basic-level firewall protection because the NAT device can initiate connections from the private NAT network, but devices on the external network cannot normally initiate connections to the private NAT network.

Using NAT with NetLogon

When using NAT networking in a virtual machine with a Windows guest operating system running on a Windows host, you can use NetLogon to log on to a Windows domain from the virtual machine. You can then access file shares known by the WINS server in the domain.

To use NetLogon, you need to know how WINS servers and Windows domain controllers work. This section explains how to set up the virtual machine to use NetLogon. The setup process is similar to the way you set up a physical computer on one LAN that is using a domain controller on another LAN.

In order to log on to a Windows domain outside the virtual NAT network, the virtual machine needs access to a WINS server for that domain. There are two ways you can connect the virtual machine to a WINS server. You can connect to the WINS server provided by the DHCP server used on the NAT network, provided that the WINS server is already set up on the host. If you want to connect from the virtual machine to a WINS server not set up on the host, you can manually enter the IP address of the WINS server.

Using NAT to Connect to an Existing WINS Server Already Set Up on the Host
In order to use this method, a WINS server in the same workgroup or domain must be set up on the host. These steps use Windows 2000, Windows XP or Windows Server 2003 as a guide. The process is similar for Windows NT, Windows Me and Windows 9x guests.

1. In the virtual machine, right-click on **My Network Places** and select **Properties**.
2. In the Network Connections window, right-click the virtual network adapter and select **Properties**.
3. In the Properties dialog box, select **Internet Protocol (TCP/IP)**, then click **Properties**.
4. In the TCP/IP Properties dialog box, click **Advanced**.
5. Click the **WINS** tab, then under **NetBIOS setting**, select **Use NetBIOS setting from DHCP Server**.
6. Click **OK** twice, then click **Close**.

Manually Entering the IP Address of a WINS Server
Use this method to connect to a WINS server in the same workgroup or domain that is not already set up on the host.

1. In the virtual machine, right-click on **My Network Places** and select **Properties**.
2. In the Network Connections window, right-click the virtual network adapter and select **Properties**.
3. In the Properties dialog box, select **Internet Protocol (TCP/IP)**, then click **Properties**.
4. In the TCP/IP Properties dialog box, click **Advanced**.
5. Click the **WINS** tab, then click **Add**.
6. In the TCP/IP WINS Server dialog box, enter the IP address for the WINS server in the **WINS server** field, then click **OK**. The IP address of the WINS server appears in the **WINS addresses** list on the **WINS** tab.

Repeat steps 5 and 6 for each WINS server to which you want to connect from this virtual machine.

7. Click **OK** twice, then click **Close**.

Now that the virtual machine has an IP address for a WINS server, you use NetLogon in the virtual machine to log on to a domain and access shares in that domain.

For example, if the WINS server covers a domain with a domain controller it is possible to access that domain controller from the virtual machine and add the virtual machine to the domain. You need to know the user ID and password of the Administrator on the domain controller.

Note: Your access is limited to shares of virtual machines that are on the same NAT network or are bridged on the same domain.

Sample Linux vmnetnat.conf File

```
# Linux NAT configuration file

[host]

# NAT gateway address
ip = 192.168.237.2/24
hostMAC = 00:50:56:C0:00:08

# enable configuration; disabled by default for security reasons
#configport = 33445

# VMnet device if not specified on command line
device = VMnet8

# Allow PORT/EPRT FTP commands (they need incoming TCP stream...)
activeFTP = 1

# Allows the source to have any OUI. Turn this one if you change the OUI
# in the MAC address of your virtual machines.
#allowAnyOUI = 1

[udp]
# Timeout in seconds, 0 = no timeout, default = 60; real value might
# be up to 100% longer
timeout = 30

[dns]
# This section applies only to Windows.
#
# Policy to use for DNS forwarding. Accepted values include order,
```

```
# rotate, burst.
#
# order: send one DNS request at a time in order of the name servers
# rotate: send one DNS request at a time, rotate through the DNS servers
# burst: send to three servers and wait for the first one to respond
policy = order;

# Timeout in seconds before retrying DNS request.
timeout = 2

# Retries before giving up on DNS request
retries = 3

# Automatically detect the DNS servers (not supported in Windows NT)
autodetect = 1

# List of DNS servers to use. Up to three may be specified
#nameserver1 = 208.23.14.2
#nameserver2 = 63.93.12.3
#nameserver3 = 208.23.14.4

[netbios]
# This section applies only to Windows.

# Timeout for NBNS queries.
nbnsTimeout = 2

# Number of retries for each NBNS query.
nbnsRetries = 3

# Timeout for NBDS queries.
nbdsTimeout = 3

[incomingtcp]
# Use these with care - anyone can enter into your virtual machine through
# these...

# FTP (both active and passive FTP is always enabled)
#   ftp localhost 8887
#8887 = 192.168.27.128:21

# WEB (make sure that if you are using named webhosting, names point to
#   your host, not to guest... And if you are forwarding port other
#   than 80 make sure that your server copes with mismatched port
#   number in Host: header)
#   lynx http://localhost:8888
#8888 = 192.168.27.128:80
```

```
# SSH
#   ssh -p 8889 root@localhost
#8889 = 192.168.27.128:22

[incomingudp]
# UDP port forwarding example
#6000 = 192.168.27.128:6001
```

Using Samba on a Linux Host

Using Samba for File Sharing on a Linux Host

On a Linux host computer, VMware Workstation can automatically install and configure a Samba server to act as a file server for Microsoft Windows guest operating systems.

You can then use Windows Explorer in the virtual machine to move and copy files between virtual machine and host — or between virtual machines on the same network — just as you would with files on physical computers that share a network connection.

The lightly modified Samba server installed by VMware Workstation runs over the VMware Workstation virtual Ethernet, and the Samba traffic between different operating systems is isolated from actual local area networks.

The source code differences for the changes (in `diff` format and based on Samba 2.0.6) are available from VMware.

If you already have Samba configured on your Linux host, the recommended approach is to modify that configuration so it includes the IP subnet used by the VMware Workstation virtual Ethernet adapter, VMnet1.

You can configure your existing Samba server to work with a host-only network. Note, however, that all the shares you set up in Samba and in the guest operating system normally appear on the bridged network, as well.

If you need to be sure the shares set up in the guest operating system are seen only on the host-only network, you may find it easiest to install and use the Samba server provided with VMware Workstation.

If you do not need any shares to appear on your bridged network, you can use your existing Samba server and set up the configuration file so it works only on the host-only network.

Samba configurations can be quite complex. This section provides several sample configuration files. If you need to go beyond the issues covered here, see the man page for the `smb.conf` file. To view this man page, type one of the following commands in a terminal window:

```
man smb.conf
```

or

```
man 5 smb.conf
```

Pay particular attention to the section on encrypted passwords. If you have enabled clear-text passwords in the guest operating system, be sure that `smb.conf` is set up to use clear-text passwords. Similarly, if you are using encrypted passwords, you must have the same setting in the guest operating system and in `smb.conf`.

Note: Using Samba printer sharing with virtual machines is not supported. Consult the man pages for guidance on configuring Samba for printing.

Sample smb.conf for Host-Only Networking

The following sample Samba configuration file is for use with host-only networking. This configuration is for the 2.0.6 version of Samba installed by VMware Workstation. The configuration files are placed in `/etc/vmware/vmnet1/smb` by default.

```
# This is the VMware(TM) Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options
# most of which are not shown in this example
#
# Any line that starts with a ; (semicolon) or a # (hash)
# is a comment and is ignored. In this example we will use a #
# for commentary and a ; for parts of the config file that you
# may wish to enable
#
#
# Configuration file for Samba 2.0.6 vmware-[sn]mbd operating on
# vmnet1.
#
# This file was generated by the VMware configuration
# program and modified for this document.
#
# If you modify it, it will be backed up the next time you run the
# configuration program.

# Global settings
[global]

# This should be polled at install time from the private subnet created by
# vmware-config.pl
socket address = 192.168.183.1
interfaces = vmnet1
bind interfaces only = yes

workgroup = WORKGROUP
netbios name = HOSTNAME
server string = VMware host-only

security = user
encrypt passwords = yes

# Note: Printers not loaded in this example. Resource definitions commented
# below.
; load printers = yes

socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
```

```
# VMware extension to use a different shared memory access key on each
# Samba server running on this host
sysv shm key = /dev/vmnet1

; log file = /etc/vmware/vmnet1/smb/var/log.smb
; log level = 1
; max log size in KB
; max log size = 50

lock directory = /etc/vmware/vmnet1/smb/var/locks

smb passwd file = /etc/vmware/vmnet1/smb/private/smbpasswd

codepage dir = /usr/lib/vmware/smb/codepages

dns proxy = no

# Shared resources

# Home directories
[homes]
comment = Home directories
browseable = no
writable = yes

# Printers
;[printers]
; comment = All printers
; path = /var/lpd
; browseable = no
; guest ok = no
; writable = no
; printable = yes

;[HostFS]
; comment = VMware host filesystem
; path = /
; public = no
; writeable = yes
; printable = no
```

Sample smb.conf for Bridged Networking

The following sample Samba configuration file is for use with bridged networking. This configuration file is based on the 2.0.7 version of Samba and assumes that you are using your existing Samba server, as provided with your host computer's Linux distribution. The configuration file is placed in `/etc` by default.

```
# This is the main Samba configuration file. You should read the
# smb.conf(5) manual page in order to understand the options listed
# here. Samba has a huge number of configurable options
# most of which are not shown in this example
#
# Any line that starts with a ; (semicolon) or a # (hash)
# is a comment and is ignored. In this example we will use a #
# for commentary and a ; for parts of the config file that you
```

```
# may wish to enable
#
# NOTE: Whenever you modify this file you should run the command
# "testparm" to check that you have not many any basic syntactic
# errors.

# Global Settings

[global]

interfaces = eth0

workgroup = WORKGROUP
netbios name = HOSTNAME
server string = Samba Host Box

# Note: Printers not loaded in this example. Resource definitions commented
# below.
; printcap name = lpstat
; load printers = yes
; printing = cups

socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192

log file = /var/log/samba/log.%m
max log size = 50

security = user
encrypt passwords = yes
smb passwd file = /etc/smbpasswd

dns proxy = no

preserve case = yes
short preserve case = yes
default case = lower
; case sensitive = no

# Shared Resources

[homes]
comment = Home Directories
browseable = yes
writable = yes

;[printers]
; comment = All Printers
; path = /var/spool/samba
; browseable = yes
; guest ok = yes
; writable = no
; printable = yes
; create mode = 0700
; print command = lpr-cups -P %p -o raw %s -r # using client side
; printer drivers.
; print command = lpr-cups -P %p %s # using cups own drivers (use
; generic PostScript on clients).
; lpq command = lpstat -o %p
```

```
; lprm command = cancel %p-%j

;[system]
; comment = System share
; path = /
; valid users = username
; public = no
; browsable = yes
; writable = yes
; printable = no
```

Adding User Names and Passwords to the VMware Workstation Samba Password File

You must be sure the Samba password file includes entries for all users of the virtual machine who will access the host's file system. The user names and passwords in the Samba password file must be the same as those used for logging on to the guest operating system.

You may add user names and passwords to the VMware Workstation Samba password file at any time from a terminal window on your Linux host computer.

1. Log on to the root account.
   `su`
2. Run the VMware Workstation Samba password command.
   `vmware-smbpasswd vmnet1 -a <username>`
   `<username>` is the user name you want to add. Follow the instructions on the screen.

   Note: `vmware-smbpasswd` is based on the standard Samba password program. If you are familiar with the options used in `smbpasswd`, you may use any of them in `vmware-smbpasswd`.
3. Log out of the root account.
   `exit`

You may receive an error message that says
`Unknown virtual interface "vmnet1"`
This indicates your machine is not using the VMware Workstation Samba server.

If your installation of VMware Workstation does not include the VMware Workstation Samba server and you want to set it up, log on to the root account on your host computer (`su`), then run `vmware-config.pl` from a terminal on the host. The configuration program asks
`Do you want this script to automatically configure your system to allow your virtual machines to access the host`

`file system?`
Answer Yes.

If You Are Already Running Samba
If you already have Samba running on your Linux host, you should not install the VMware Workstation Samba server when you are installing VMware Workstation on your host.

The configuration program prompts you
`Do you want this script to automatically configure your system to allow your virtual machines to access the host file system?`
Answer No.

Be sure to modify your Samba configuration so it includes the IP subnet used by the VMware Workstation virtual Ethernet adapter, VMnet1.

To determine what subnet is being used by VMnet1, run

```
/sbin/ifconfig vmnet1
```

You must be sure the Samba password file includes entries for all users of the virtual machine who will access the host's file system. The user names and passwords in the Samba password file must be the same as those used for logging on to the guest operating system.

You may add user names and passwords to the Samba password file at any time from a terminal window on your Linux host computer.

1. Log on to the root account.
   `su`
2. Run the Samba password command.
   `smbpasswd -a <username>`
   `<username>` is the user name you want to add. Follow the instructions on the screen.
3. Log out of the root account.
   `exit`

Using a Samba Server for Both Bridged and Host-Only Networks
You may use the Samba server of your choice — either the existing Samba server from your host operating system's distribution or the one provided with VMware Workstation — for both host-only and bridged networking. To do so, you must modify

one parameter in the `smb.conf` file. You can define the `interface` parameter so your Samba server serves multiple interfaces. An example of this is:

```
interface = eth0 vmnet1
```

This example tells the Samba server that it is to listen to and use both the `eth0` and `vmnet1` interfaces — the interfaces used by bridged and host-only networking, respectively.

Using VMware Workstation's Samba with an Existing Installation

It may also be possible to run both your existing Samba server and the VMware Workstation Samba server at the same time. In order to do this, your current Samba server must be version 2.0.6 or higher and must be configured correctly. However, this approach is not recommended.

To determine the version of your Samba server, run

```
smbd -V
```

If you want to try running both Samba servers at the same time, use this sample `smb.conf` file as a basis for configuring the regular Samba server on your host computer.

Sample smb.conf for Running Two Samba Servers at the Same Time

```
; This file is the recommended smb.conf file for your
; normal Samba server if you want to run it concurrently
; (which we don't advise) with the VMware Samba server.
;
; Your normal samba server should be at least v 2.0.6
;
; Note that you will need to insert specific information
; for your system at several points indicated in the file
; by <text in angle brackets>.
;
; --------------
;
; Larmor samba server configuration
;
; Global settings
[global]
;
; Identity
;
; Allow several Samba servers on the same machine
interfaces = <your real subnet>/<your real netmask>
bind interfaces only = yes
; Workgroup the host belongs to
workgroup = VMware
; SMB name of the host (the hostname by default)
netbios name = <your Windows name>
; Description of the host
server string = Linux running Samba 2.0.6
;
```

```
; Access
;
; Allow connections from
; hosts allow = <your real subnet>/<your real netmask>
; Authentication scheme
security = user
encrypt passwords = yes
;
; Options
;
; Automatically load the printer list (from /etc/printcap
; by default)
load printers = yes
; Gives better performance
socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192
;
; Files and directories
;
; Max log size in KB
max log size = 1024
; Locks
lock directory = /var/samba
; SMB passwords
smb passwd file = /etc/samba/smbpasswd
;
; Name browsing
;
; Allow the host to participate in master browser
; elections
local master = yes
; Force a local browser election upon startup
; We need that otherwise it takes a long time before the
; windows network is browsable
preferred master = yes
; Do not try to resolve SMB names via DNS
dns proxy = no

; Shared resources
;
; Home directories
[homes]
comment = Home directories
browseable = no
writable = yes
; Printers
;[printers]
; comment = All printers
; path = /var/lpd
; browseable = no
; guest ok = no
; writable = no
; printable = yes
[Slash]
comment = Whole filesystem
path = /
public = no
writeable = yes
printable = no
```

CHAPTER 10

Configuring Video and Sound

The following sections provide information on configuring the video display and sound for VMware Workstation.

Setting Screen Color Depth in a Virtual Machine

The number of screen colors available in the guest operating system depends on the screen color setting of the host operating system.

Virtual machines support

- 16-color (VGA) mode
- 8-bit pseudocolor
- 16 bits per pixel (16 significant bits per pixel)
- 32 bits per pixel (24 significant bits per pixel)

If the host is in 15-bit color mode, the guest operating system's color setting controls offer 15-bit mode in place of 16-bit mode.

If the host is in 24-bit color mode, the guest operating system's color setting controls offer 24-bit mode in place of 32-bit mode.

If you run a guest operating system set for a greater number of colors than your host operating system is using, you can encounter various problems. In some cases, for example, the colors in the guest are not correct. In others, the guest operating system is not able to use a graphical interface.

In such a case, you can either increase the number of colors available on the host or decrease the number of colors used in the guest.

For best performance, use the same number of colors in the guest and on the host.

Changing Screen Color Depth on the Host

If you choose to change the color settings on your host operating system, you should first shut down all guest operating systems, power off the virtual machines and close VMware Workstation.

Follow standard procedures for changing the color settings on your host operating system, then restart VMware Workstation and the virtual machines.

Changing Screen Color Depth in the Virtual Machine

If you choose to change the color settings in the guest operating system, the approach depends on the combination of host and guest you are using.

Follow the normal process for changing screen colors in your guest operating system. In a Windows guest, the Display Properties control panel offers only those settings that are supported.

In a Linux or FreeBSD guest, you must change the color depth before you start the X server or restart the X server after making the changes.

Using Full Screen Mode on a Linux Host

When you switch to full screen mode, VMware Workstation changes the full screen display resolution to better match the resolution set in the guest operating system. On a Linux host, VMware Workstation uses the VidMode or DGA2 extension from the XFree86 Project or XiG's Xfs to match the host resolution to the one requested by the guest running in the virtual machine.

In a few cases, VMware Workstation may not find the best resolution.

When VMware Workstation switches to full screen mode, it can choose only those resolutions that are already configured for the host's X server. If a virtual machine runs at a resolution that does not match a mode listed in host's X server configuration, then VMware Workstation chooses the closest larger mode (and uses black borders) for full screen mode or else simply does not offer full screen mode at all.

It is possible to have bad modes configured for the X server on your host. If your host's X configuration was automatically generated, or if you never tested all modes with your current monitor and video card, it is possible that some enabled modes do not work with your monitor. However, the mode-switching code in VMware Workstation has no way of knowing this and a virtual machine that tries to use a resolution with a bad mode line can cause your display to fail to display correctly.

If this happens, immediately leave full screen mode by pressing Ctrl-Alt, then fix your X server configuration and restart X. However, if the only problem is that the image is off center or is not quite the right size on the monitor, you can usually correct it using the controls on your monitor. Note that most modern monitors are capable of storing separate settings for each resolution, so changing the settings for a new mode should not impair the settings for the host resolution.

Configuring Sound

VMware Workstation provides a sound device compatible with the Sound Blaster AudioPCI and supports sound in Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, Windows XP, Windows Server 2003 and Linux guest operating systems. The VMware Workstation sound device is enabled by default.

Sound support includes PCM (pulse code modulation) output and input. For example, you can play `.wav` files, MP3 audio and Real Media audio. MIDI output from Windows guests is supported through the Windows software synthesizer. MIDI input is not supported, and no MIDI support is available for Linux guests.

Windows 2000, Windows XP and most recent Linux distributions automatically detect the sound device and install appropriate drivers for it.

Installing Sound Drivers in Windows 9x and Windows NT Guest Operating Systems

Windows 95, Windows 98, Windows 98SE and Windows NT 4.0 do not have drivers for the Sound Blaster AudioPCI adapter. To use sound in these guest operating systems, you must download the driver from the Creative Labs Web site (*www.creative.com*) and install it in the guest operating system.

Creative Labs has a number of Web sites serving various regions of the world. The adapter name varies, depending on the region, but usually includes AudioPCI.

CHAPTER 11

Connecting Devices

The following sections describe how to use various devices with a virtual machine:

Using Parallel Ports

VMware Workstation supports a partial emulation of bidirectional PS/2-style ports.

On Linux hosts, VMware Workstation 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"). VMware Workstation is unable to use parallel port devices if CONFIG_PARPORT_PC is built directly (compiled) into the kernel. This limitation exists because CONFIG_PARPORT_PC does not correctly export its symbols.

Parallel Ports

Parallel ports are used by a variety of devices, including printers, scanners, dongles and disk drives.

Currently, VMware Workstation provides only partial emulation of PS/2 hardware. Specifically, interrupts requested by a device connected to the physical port are not passed to the virtual machine. Also, the guest operating system cannot use DMA (direct memory access) to move data to or from the port. For this reason, not all devices that attach to the parallel port are guaranteed to work correctly.

Installation in Guest Operating Systems

If the virtual machine is configured with a parallel port, most guest operating systems automatically detect it at installation time and install the required drivers. Some operating systems, including Linux, Windows NT and Windows 2000, automatically detect the ports at boot time. Others, like Windows 95 and Windows 98, do not.

To add a parallel port to the virtual machine's configuration, take these steps with the virtual machine powered off.

1. Open the virtual machine settings editor.

   VM > Settings

2. Click **Add** to start the New Hardware Wizard.
3. Select **Parallel Port**, then click **Next**.
4. Make the appropriate selection to use a physical parallel port or connect the virtual parallel port to a file.
5. If you selected **Use physical port**, choose the port from the drop-down list.

   If you selected **Use output file**, enter the path and filename or browse to the location of the file.

Under **Device status**, the default setting is **Connect at power on**. Clear the check box if you want to deselect this setting.

Click **Finish**.

In a Windows 95 or Windows 98 guest, after you add the port, run the guest operating system's Add New Hardware Wizard (**Start** > **Settings** > **Control Panel** > **Add New Hardware**) and let Windows detect the new device.

Configuring a Parallel Port on a Linux Host

For the parallel port to work properly in a guest, it must first be configured properly on the host. Most issues involving parallel port functionality are a result of the host configuration. Check these areas of concern: the version of your Linux kernel, your device access permissions and the required modules.

Parallel Ports and Linux 2.2.x Kernels

The 2.2.x kernels that support parallel ports use the `parport`, `parport_pc` and `vmppuser` modules. Be sure that PC Style Hardware (CONFIG_PARPORT_PC) is loaded as a module, as mentioned at the beginning of Using Parallel Ports on page 273. The `vmppuser` module is supplied by VMware Workstation to give virtual machines user-level access to the parallel port.

To see if these modules are installed and running on your system, run the `lsmod` command as the root user. These three modules should be included in the listing of running modules. You can also look at the `/proc/modules` file for the same list.

To load the proper modules, run this command:

```
insmod -k <modulename>
```

If none of the listed parallel port modules is running, use this command:

```
insmod -k parport_pc
```

This command inserts the three modules needed for a parallel port.

If you continue to see problems, it is possible that the `lp` module is running. If it is, the virtual machine cannot use the parallel port correctly. To remove the `lp` module, run this command as the root user:

```
rmmod lp
```

You should also ensure that the line referring to the `lp` module in the `/etc/modules.conf` or `/etc/conf.modules` file is removed or commented out by inserting a hash character (#) at the beginning of the line. The name of the configuration file depends on the Linux distribution you are using. When you reboot

the host after removing this line, the configuration file no longer starts the `lp` module.

To ensure that the proper modules for the parallel port are loaded at boot time, add this line to the `/etc/modules.conf` or `/etc/conf.modules` file:

```
alias parport_lowlevel parport_pc
```

Parallel Ports and Linux 2.4.x Kernels

Be sure that PC Style Hardware (CONFIG_PARPORT_PC) is loaded as a module as mentioned at the beginning of Using Parallel Ports on page 273. If you are using a 2.4.x kernel, the modules that provide parallel port functionality are `parport`, `parport_pc` and `ppdev`.

To see if these modules are installed and running on your system, run the `lsmod` command as the root user. These three modules should be included in the listing of running modules. You can also look at the `/proc/modules` file for the same list.

To load the proper modules, run this command:

```
insmod -k <modulename>
```

If none of the listed parallel port modules is running, use this command:

```
insmod -k parport_pc
```

This command inserts the three modules needed for a parallel port.

If you continue to see problems, it is possible that the `lp` module is running. If it is, the virtual machine cannot use the parallel port correctly. To remove the `lp` module, run this command as the root user:

```
rmmod lp
```

You should also ensure that the line referring to the `lp` module in the `/etc/modules.conf` or `/etc/conf.modules` file is removed or commented out by inserting a hash character (#) at the beginning of the line. The name of the configuration file depends on the Linux distribution you are using. When you reboot the host after removing this line, the configuration file no longer starts the `lp` module.

To ensure that the proper modules for the parallel port are loaded at boot time, add this line to the `/etc/modules.conf` or `/etc/conf.modules` file:

```
alias parport_lowlevel parport_pc
```

Linux kernels in the 2.4.x series also use a special arbitrator that allows access to the parallel port hardware. If the parallel port is in use by the host, the guest cannot use it. If a virtual machine is using the parallel port, the host and any users accessing the host

are not given access to the device. VMware Workstation puts a lock on the device, and this lock restricts access so only the virtual machine can use the port.

You can choose **VM** > **Removable Devices** to disconnect the parallel port from the virtual machine and reconnect it.

Device Permissions

Some Linux distributions by default do not grant the virtual machine access to the `lp` and `parport` devices. In most of these cases, the owner of the device is `root` and the associated group is `lp`. To allow the VMware user to access the device, add the user to the associated group. To view the owner and group of the device, run this command:

```
ls –la /dev/parport0
```

The third and fourth columns of the output show the owner and group, respectively.

To add the user to the device group, edit the `/etc/group` file. On the line starting with `lp`, which defines the `lp` group, add the VMware Workstation user's user name. You must make this change as the root user. The following line provides an example for a user whose user name is `userj`.

```
lp::7:daemon,lp,userj
```

The next time the user logs on to the host, the changes take effect.

Special Notes for the Iomega Zip Drive

On Windows 95 or Windows 98, use of older drivers for the Iomega Zip drive may cause the guest operating system to lock up intermittently at boot time or during installation of the guest operating system. The newest Iomega drivers work reliably in our tests. They are available at*www.iomega.com/software/index.html*.

Using Serial Ports

A VMware Workstation virtual machine can use up to four virtual serial ports. The virtual serial ports can be configured in several ways.

- You can connect a virtual serial port to a physical serial port on the host computer.
- You can connect a virtual serial port to a file on the host computer.
- You can make a direct connection between two virtual machines or between a virtual machine and an application running on the host computer.

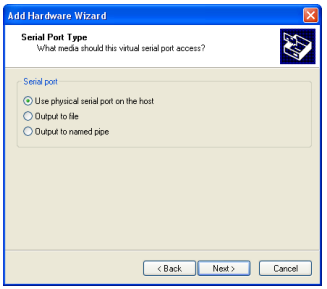
You can also select whether to connect the virtual serial port when you power on the virtual machine.

Using a Serial Port on the Host Computer

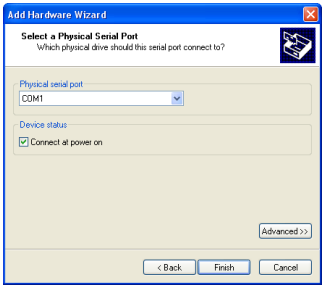
You can set up the virtual serial port in a virtual machine to use a physical serial port on the host computer. This is useful, for example, if you want to use an external modem or a hand-held device in your virtual machine.

To install a virtual serial port that connects to a physical serial port on the host computer, take the following steps:

1. Open the virtual machine settings editor (**VM** > **Settings**).
2. Click **Add** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.



4. Select **Use physical serial port on the host**, then click **Next**.



5. Choose the port on the host computer that you want to use for this serial connection. By default, the device status setting is **Connect at power on**. You may deselect this setting if you wish.

   Click **Advanced** if you want to configure this serial port to use polled mode. This option is of interest primarily to developers who are using debugging tools that communicate over a serial connection. For more information, see Special Configuration Options for Advanced Users on page 285.

6. Click **Finish**, then click **OK** to close the virtual machine settings editor.
7. Power on the virtual machine.

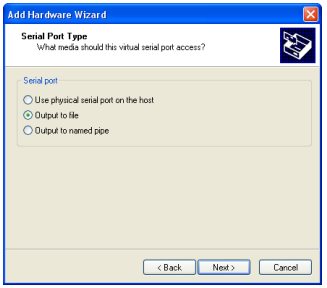
Using a File on the Host Computer

You can set up the virtual serial port in a virtual machine to send its output to a file on the host computer. This is useful, for example, if you want to capture the data a program running in the virtual machine sends to the virtual serial port or if you need a quick way to transfer a file from the guest to the host.

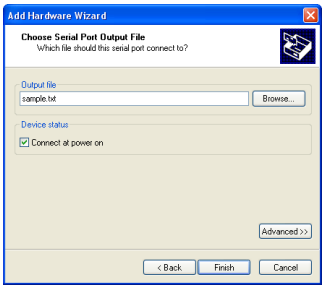
To install a virtual serial port that connects to a file on the host computer, take the following steps:

1. Open the virtual machine settings editor (**VM** > **Settings**).
2. Click **Add** to start the Add Hardware Wizard.

3. Select **Serial Port**, then click **Next**.



4. Select **Output to file**, then click **Next**.



5. Browse to the file on the host computer that you want to use to store the output of the virtual serial port. By default, the device status setting is **Connect at power on**. You may deselect this setting if you wish.

   Click **Advanced** if you want to configure this serial port to use polled mode. This option is of interest primarily to developers who are using debugging tools that communicate over a serial connection. For more information, see Special Configuration Options for Advanced Users on page 285.

6. Click **Finish**, then click **OK** to close the virtual machine settings editor.

7. Power on the virtual machine.

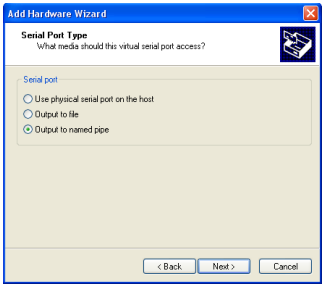
Connecting an Application on the Host to a Virtual Machine

You can set up the virtual serial port in a virtual machine to connect to an application on the host computer. This is useful, for example, if you want to use an application on the host to capture debugging information sent from the virtual machine's serial port.

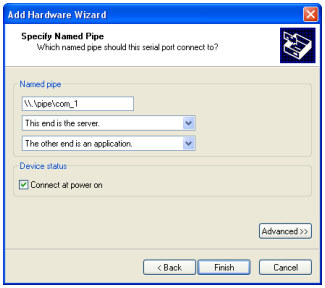
To install a direct serial connection between an application on the host and a virtual machine, take the following steps:

Windows Host

1. Open the virtual machine settings editor (**VM** > **Settings**).
2. Click **Add** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.



4. Select **Output to named pipe**, then click **Next**.



5. Use the default pipe name, or enter another pipe name of your choice. The pipe name must follow the form `\\.\pipe\<namedpipe>` — that is, it must begin with `\\.\pipe\`.
6. Select **This end is the server** or **This end is the client**. In general, select **This end is the server** if you plan to start this end of the connection first.
7. Select **The other end is an application**.
8. By default, the device status setting is **Connect at power on**. You may deselect this setting if you wish.

   Click **Advanced** if you want to configure this serial port to use polled mode. This option is of interest primarily to developers who are using debugging tools that

communicate over a serial connection. For more information, see Special Configuration Options for Advanced Users on page 285.

9. Click **Finish**, then click **OK** to close the virtual machine settings editor.
10. On your host computer, configure the application that communicates with the virtual machine to use the same pipe name.
11. Power on the virtual machine.

Linux Host

1. Open the virtual machine settings editor (**VM** > **Settings**).
2. Click **Add** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.
4. Select **Output to named pipe**, then click **Next**.
5. In the **Path** field, enter `/tmp/<socket>` or another Unix socket name of your choice.
6. Select **This end is the server** or **This end is the client**. In general, select **This end is the server** if you plan to start this end of the connection first.
7. Select **The other end is an application**.
8. By default, the device status setting is **Connect at power on**. You may deselect this setting if you wish.

   Click **Advanced** if you want to configure this serial port to use polled mode. This option is of interest primarily to developers who are using debugging tools that communicate over a serial connection. For more information, see Special Configuration Options for Advanced Users on page 285.
9. Click **Finish**.
10. Click **OK** to save your configuration and close the virtual machine settings editor.
11. On your host computer, configure the application that communicates with the virtual machine to use the same Unix socket name.
12. Power on the virtual machine.

Connecting Two Virtual Machines

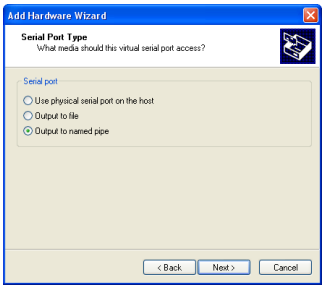
You can set up the virtual serial ports in two virtual machines to connect to each other. This is useful, for example, if you want to use an application in one virtual machine to capture debugging information sent from the other virtual machine's serial port.

To install a direct serial connection between two virtual machines (a server and a client), take the following steps:

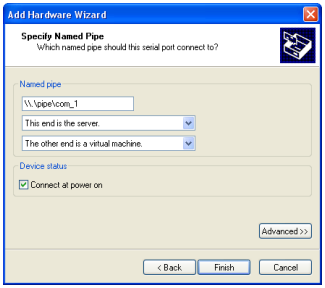
Windows Host

In the server virtual machine

1. Open the virtual machine settings editor (**VM** > **Settings**).
2. Click **Add** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.



4. Select **Output to named pipe**, then click **Next**.



5. Use the default pipe name, or enter another pipe name of your choice. The pipe name must follow the form `\\.\pipe\<namedpipe>` — that is, it must begin with `\\.\pipe\`.
6. Select **This end is the server**.
7. Select **The other end is a virtual machine**.
8. By default, the device status setting is **Connect at power on**. You may deselect this setting if you wish.

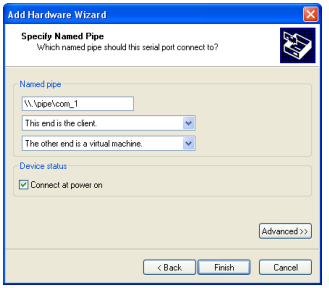
   Click **Advanced** if you want to configure this serial port to use polled mode. This option is of interest primarily to developers who are using debugging tools that

communicate over a serial connection. For more information, see Special Configuration Options for Advanced Users on page 285.

9. Click **Finish**, then click **OK** to close the virtual machine settings editor.

In the client virtual machine

1. Open the virtual machine settings editor (**VM** > **Settings**).
2. Click **Add** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.



4. Select **Use named pipe**.
5. Use the default name, or enter another pipe name of your choice. The pipe name must follow the form `\\.\pipe\<namedpipe>` — that is, it must begin with `\\.\pipe\`. The pipe name must be the same on both server and client.
6. Select **This end is the client**.
7. Select **The other end is a virtual machine**.
8. By default, the device status setting is **Connect at power on**. You may deselect this setting if you wish.

   Click **Advanced** if you want to configure this serial port to use polled mode. This option is of interest primarily to developers who are using debugging tools that communicate over a serial connection. For more information, see Special Configuration Options for Advanced Users on page 285.
9. Click **Finish**, then click **OK** to close the virtual machine settings editor.

Linux Host

In the server virtual machine

1. Open the virtual machine settings editor (**VM** > **Settings**).

2. Click **Add** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.
4. Select **Output to named pipe**, then click **Next**.
5. In the **Path** field, enter `/tmp/<socket>` or another Unix socket name of your choice.
6. Select **This end is the server**.
7. Select **The other end is a virtual machine**.
8. By default, the device status setting is **Connect at power on**. You may deselect this setting if you wish.

   Click **Advanced** if you want to configure this serial port to use polled mode. This option is of interest primarily to developers who are using debugging tools that communicate over a serial connection. For more information, see Special Configuration Options for Advanced Users on page 285.
9. Click **Finish**, then click **OK** to save your configuration and close the virtual machine settings editor.

In the client virtual machine

1. Open the virtual machine settings editor (**VM** > **Settings**).
2. Click **Add** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.
4. Select **Output to named pipe**, then click **Next**.
5. In the **Path** field, enter `/tmp/<socket>` or another Unix socket name of your choice. The pipe name must be the same on both server and client.
6. Select **This end is the client**.
7. Select **The other end is a virtual machine**.
8. By default, the device status setting is **Connect at power on**. You may deselect this setting if you wish.

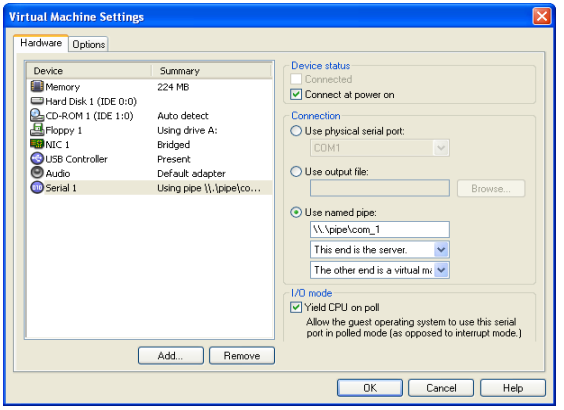
   Click **Advanced** if you want to configure this serial port to use polled mode. This option is of interest primarily to developers who are using debugging tools that communicate over a serial connection. For more information, see Special Configuration Options for Advanced Users on page 285.
9. Click **Finish**, then click **OK** to save your configuration and close the virtual machine settings editor.

Special Configuration Options for Advanced Users

Two special configuration options are available for serial connections between a virtual machine and the host or between two virtual machines. These options are of interest primarily to developers who are using debugging tools that communicate over a serial connection.

Improving CPU Performance when Debugging

The first option must be set in the virtual machine settings editor. This option is useful when the serial port is being used by the guest operating system in polled mode as opposed to interrupt mode. Polled mode causes the virtual machine to consume a disproportionate share of CPU time. This makes the host and other guests run sluggishly.



To restore performance for applications on the host, in the virtual machine settings editor, select the virtual serial port, and check the **Yield CPU on poll** check box. This configuration option forces the affected virtual machine to yield processor time if the only task it is trying to do is poll the virtual serial port.

Changing the Input Speed of the Serial Connection

To use the second option, power off the virtual machine and close the VMware Workstation window, then use a text editor to add the following line to your virtual machine's configuration file:

```
serial<n>.pipe.charTimePercent = <x>
```

This option is useful if you want to squeeze every possible bit of speed from your serial connection over a pipe to the virtual machine. In principle, there is no limit on the output speed — the speed at which the virtual machine sends data through the

virtual serial port. In practice, the output speed depends on how fast the application at the other end of the pipe reads data inbound to it.

<n> is the number of the serial port, starting from 0. So the first serial port is serial0.

<x> is any positive integer. It specifies the time taken to transmit a character, expressed as a percentage of the default speed set for the serial port in the guest operating system. For example, a setting of 200 forces the port to take twice as long per character, or send data at half the default speed. A setting of 50 forces the port to take only half as long per character, or send data at twice the default speed.

You should first use the guest operating system to configure the serial port for the highest setting supported by the application you are running in the virtual machine.

Once the serial port speed is set appropriately in the guest operating system, experiment with this setting. Start with a value of 100 and gradually decrease it until you find the highest speed at which your connection works reliably.

Examples: Debugging over a Virtual Serial Port

You can use Debugging Tools for Windows (WinDbg) or Kernel Debugger (KD) to debug kernel code in a virtual machine over a virtual serial port. You can download Debugging Tools for Windows from the Windows DDK Web site at*www.microsoft.com/whdc/devtools/debugging/default.mspx*.

The following two examples illustrate how to use a virtual serial port to debug kernel code in a virtual machine:

- With the debugging application on the VMware Workstation host (Windows hosts only)
- With the debugging application in another virtual machine on the same VMware Workstation host (useful on a Linux host and can also be done on a Windows host)

Using either of these methods lets you debug kernel code on one system, without the need for two physical computers, a modem or serial cable.

Debugging an Application in a Virtual Machine from the Windows Host

In this example, you have kernel code to debug in a virtual machine (called the target virtual machine) and are running WinDbg or KD on your Windows host.

To prepare the target virtual machine, follow the steps for a Windows host in Connecting an Application on the Host to a Virtual Machine on page 279. Make sure you configure the virtual machine's virtual serial port as follows:

- Select **This end is the server**
- Under **I/O Mode**, select the **Yield CPU on poll** check box, as the kernel in the target virtual machine uses the virtual serial port in polled mode, not interrupt mode

To prepare the host, make sure you have a recent version of Debugging Tools for Windows — one that supports debugging over a pipe. You need version 4.0.18.0 or higher.

When you are ready to begin, complete the following steps:

1. Power on the virtual machine.
2. Check to make sure the serial port is connected. Choose choose **VM** > **Removable Devices**. On that menu, **serial<n>** should be reported as **\\.\pipe\<namedpipe>** (on Windows hosts) or **/tmp/<socket>** (on Linux hosts). If the serial port is not connected, choose the virtual serial port, then **Connect**.
3. On the host, open a Command Prompt window and do one of the following:
   - If you are using `WinDbg`, type the following:

     ```
     windbg -k com:port=\\.\pipe\<namedpipe>,pipe
     ```

   - If you are using `KD`, type the following:

     ```
     kd -k com:port=\\.\pipe\<namedpipe>,pipe
     ```

   Then press Enter to start debugging.

Debugging an Application in a Virtual Machine from another Virtual Machine

In this situation, you have kernel code to debug in a virtual machine (called the target virtual machine) and are running Debugging Tools for Windows (`WinDbg`) or Kernel Debugger (`KD`) in another virtual machine (called the debugger virtual machine) on the same host.

This is useful if you are running VMware Workstation on a Linux host. The debugger virtual machine must be running Debugging Tools for Windows (`WinDbg`) or Kernel Debugger (`KD`) in a Windows guest operating system.

To prepare the target virtual machine, follow the steps for the server virtual machine for the appropriate host in Connecting Two Virtual Machines on page 281. Make sure when you configure the target virtual machine's virtual serial port that you select the

Yield CPU on poll check box, as the kernel in the target virtual machine uses the virtual serial port in polled mode, not interrupt mode.

To prepare the debugger virtual machine, make sure you have downloaded Debugging Tools for Windows. Then follow the steps for the client virtual machine in Connecting Two Virtual Machines on page 281.

When you are ready to begin, complete the following steps:

1. Power on both virtual machines.
2. Check to make sure the serial port is connected. Choose choose **VM** > **Removable Devices**. If the serial port is not connected, choose the virtual serial port, then **Connect**.
3. In the debugger virtual machine, start debugging with `WinDbg` or `KD` normally.

Keyboard Mapping on a Linux Host

This section addresses the following issues and provides additional details on keyboard mapping in Linux:

- My (language-specific) keyboard is not supported by VMware Workstation.
- Some of the keys on my keyboard don't work right in the virtual machine.
- My keyboard works fine when I run a virtual machine locally, but not when I run the same virtual machine with a remote X server.

Quick Answers

If your keyboard works correctly with a local X server, and you just want the same behavior with a remote X server (which is also an XFree86 server running on a PC), just power off the virtual machine and close the VMware Workstation window, then add the line

```
xkeymap.usekeycodeMapIfXFree86 = true
```

to the virtual machine configuration file or to `~/.vmware/config`. Make this change on the host machine, where you run the virtual machine, not on the machine with the remote X server.

If you are using an XFree86-based server that VMware Workstation does not recognize as an XFree86 server, use this instead:

```
xkeymap.usekeycodeMap = true
```

If you are using an XFree86 server running locally, and the keyboard does not work correctly, please report the problem to the VMware technical support department.

The Longer Story

Unfortunately, keyboard support for the PC (virtual or otherwise) is a complex affair. To do it justice, we have to start with some background information — greatly simplified.

Pressing a key on the PC keyboard generates a scan code based roughly on the position of the key. For example, the Z key on a German keyboard generates the same code as the Y key on an English keyboard, because they are in the same position on the keyboard. Most keys have one-byte scan codes, but some keys have two-byte scan codes with prefix 0xe0.

Internally, VMware Workstation uses a simplified version of the PC scan code that is a single nine-bit numeric value, called a v-scan code. A v-scan code is written as a three-digit hexadecimal number. The first digit is 0 or 1. For example, the left-hand Ctrl key

has a one-byte scan code (0x1d); its v-scan code is 0x01d. The right-hand Ctrl key scan code is two bytes (0xe0, 0x1d); its v-scan code is 0x11d.

An X server uses a two-level encoding of keys. An X key code is a one-byte value. The assignment of key codes to keys depends on the X server implementation and the physical keyboard. As a result, an X application normally cannot use key codes directly. Instead, the key codes are mapped into keysyms that have names like space, escape, x and 2. The mapping can be controlled by an X application via the function `XChangeKeyboardMapping()` or by the program `xmodmap`. To explore keyboard mappings, you can use `xev`, which shows the key codes and keysyms for keys typed into its window.

To recap, a key code corresponds roughly to a physical key, while a keysym corresponds to the symbol on the key top. For example, with an XFree86 server running on a PC, the Z key on the German keyboard has the same key code as the Y key on an English keyboard. The German Z keysym, however, is the same as the English Z keysym, and different from the English Y keysym.

For an XFree86 server on a PC, there is a one-to-one mapping from X key codes to PC scan codes (or v-scan codes, which is what VMware Workstation really uses). VMware Workstation takes advantage of this fact. When it is using an XFree86 server on the local host, it uses the built-in mapping from X key codes to v-scan codes. This mapping is keyboard independent and should be correct for most, if not all, languages. In other cases (not an XFree86 server or not a local server), VMware Workstation must map keysyms to v-scan codes, using a set of keyboard-specific tables.

Key code mapping is simple, automatic and foolproof. (Keysym mapping is more complex and described later.) However, because the program cannot tell whether a remote server is running on a PC or on some other kind of computer, it errs on the safe side and uses key code mapping only with local X servers. This is often too conservative and has undesirable effects. Luckily, this and other behavior related to key code-mapping can be controlled by powering off the virtual machine and closing the VMware Workstation window, then using a text editor to add configuration settings to the virtual machine's configuration file.

- `xkeymap.usekeycodeMapIfXFree86 = true`
  Use key code mapping if you are using an XFree86 server, even if it is remote.
- `xkeymap.usekeycodeMap = true`
  Always use key code mapping regardless of server type.
- `xkeymap.nokeycodeMap = true`
  Never use key code mapping.

- `xkeymap.keycode.<code> = <v-scan code>`
  If using key code mapping, map key code `<code>` to `<v-scan code>`. In this example, `<code>` must be a decimal number and `<v-scan code>` should be a C-syntax hexadecimal number (for example, `0x001`).

The easiest way to find the X key code for a key is to run `xev` or `xmodmap -pk`. Most of the v-scan codes are covered in V-Scan Code Table on page 292. The keysym mapping tables described in this section are also helpful.

Use this feature to make small modifications to the mapping. For example, to swap left Ctrl and Caps Lock, use the following lines:

```
xkeymap.keycode.64 = 0x01d # X Caps_Lock -> VM left ctrl
xkeymap.keycode.37 = 0x03a # X Control_L -> VM caps lock
```

These configuration lines can be added to the individual virtual machine configuration, to your personal VMware Workstation configuration (`~/.vmware/config`), or even to the host-wide (`/etc/vmware/config`) or installation-wide (usually `/usr/local/lib/vmware/config`) configuration.

When key code mapping cannot be used (or is disabled), VMware Workstation maps keysyms to v-scan codes. It does this using one of the tables in the `xkeymap` directory in the VMware Workstation installation (usually `/usr/local/lib/vmware`).

Which table you should use depends on the keyboard layout. The normal distribution includes tables for PC keyboards for the United States and a number of European countries and languages. And for most of these, there are both the 101-key (or 102-key) and the 104-key (or 105-key) variants.

VMware Workstation automatically determines which table to use by examining the current X keymap. However, its decision-making process may sometimes fail. In addition, each mapping is fixed and may not be completely right for any given keyboard and X key code-to-keysym mapping. For example, a user may have swapped Ctrl and Caps Lock using `xmodmap`. This means the keys are swapped in the virtual machine when using a remote server (keysym mapping) but unswapped when using a local server (key code mapping).

Therefore, keysym mapping is necessarily imperfect. To make up for this defect, you can change most of the behavior using configuration settings:

- `xkeymap.language = <keyboard-type>`
  Use this if VMware Workstation has a table in `xkeymap` for your keyboard but can't detect it. `<keyboard-type>` must be one of the tables in the `xkeymap`

directory. (See above for location.) However, the failure to detect the keyboard probably means the table isn't completely correct for you.

- `xkeymap.keysym.<sym> = <v-scan code>`
  If you use keysym mapping, map keysym `<sym>` to `<v-scan code>`. When you do, `<sym>` must be an X keysym name and `<v-scan code>` should be a C-syntax hexadecimal number (for example, `0x001`).

  The easiest way to find the keysym name for a key is to run `xev` or `xmodmap -pk`.

  The X header file `/usr/X11R6/include/X11/keysymdef.h` has a complete list of keysyms. (The name of a keysym is the same as its C constant without the XK_ prefix.) Most v-scan codes are in V-Scan Code Table on page 292.

  The `xkeymap` tables themselves are also helpful. Use them to fix small errors in an existing mapping.

- `xkeymap.fileName = <file-path>`
  Use the keysym mapping table in `<file-path>`. A table is a sequence of configuration lines of the form
  `<sym> = <v-scan code>`
  where `<sym>` is an X keysym name, and `<v-scan code>` is a C-syntax hexadecimal number (for example, `0x001`). (See the explanation of `xkeymap.keysym` above for tips on finding the keysyms and v-scan codes for your keyboard.)

  Compiling a complete keysym mapping is difficult. It is best to start with an existing table and make small changes.

V-Scan Code Table

These are the v-scan codes for the 104-key U.S. keyboard:

Symbol	Shifted symbol	Location	V-scan code
Esc			0x001
1	!		0x002
2	@		0x003
3	#		0x004
4	$		0x005
5	%		0x006
6	^		0x007

Symbol	Shifted symbol	Location	V-scan code
7	&		0x008
8	*		0x009
9	(		0x00a
0	)		0x00b
-	_		0x00c
=	+		0x00d
Backspace			0x00e
Tab			0x00f
Q			0x010
W			0x011
E			0x012
R			0x013
T			0x014
Y			0x015
U			0x016
I			0x017
O			0x018
P			0x019
[	{		0x01a
]	}		0x01b
Enter			0x01c
Ctrl		left	0x01d
A			0x01e
S			0x01f
D			0x020
F			0x021
G			0x022
H			0x023
J			0x024
K			0x025
L			0x026

Symbol	Shifted symbol	Location	V-scan code
;			0x027
'			0x028
`			0x029
Shift		left	0x02a
\	|		0x02b
Z			0x02c
X			0x02d
C			0x02e
V			0x02f
B			0x030
N			0x031
M			0x032
,	<		0x033
.	>		0x034
/	?		0x035
Shift		right	0x036
*		numeric pad	0x037
Alt		left	0x038
Space bar			0x039
Caps Lock			0x03a
F1			0x03b
F2			0x03c
F3			0x03d
F4			0x03e
F5			0x03f
F6			0x040
F7			0x041
F8			0x042
F9			0x043
F10			0x044
Num Lock		numeric pad	0x045

Symbol	Shifted symbol	Location	V-scan code
Scroll Lock			0x046
Home	7	numeric pad	0x047
Up arrow	8	numeric pad	0x048
PgUp	9	numeric pad	0x049
-		numeric pad	0x04a
Left arrow	4	numeric pad	0x04b
5		numeric pad	0x04c
Right arrow	6	numeric pad	0x04d
+		numeric pad	0x04e
End	1	numeric pad	0x04f
Down arrow	2	numeric pad	0x050
PgDn	3	numeric pad	0x051
Ins	0	numeric pad	0x052
Del		numeric pad	0x053
F11			0x057
F12			0x058
Break	Pause		0x100
Enter		numeric pad	0x11c
Ctrl		right	0x11d
/		numeric pad	0x135
SysRq	Print Scrn		0x137
Alt		right	0x138
Home		function pad	0x147
Up arrow		function pad	0x148
Page Up		function pad	0x149
Left arrow		function pad	0x14b
Right arrow		function pad	0x14d
End		function pad	0x14f
Down arrow		function pad	0x150
Page Down		function pad	0x151
Insert		function pad	0x152

Symbol	Shifted symbol	Location	V-scan code
Delete		function pad	0x153
Windows		left	0x15b
Windows		right	0x15c
Menu			0x15d

The 84-key keyboard has a Sys Req key on the numeric pad:

Symbol	Shifted symbol	Location	V-scan code
Sys Req		numeric pad	0x054

Keyboards outside the U.S. usually have an extra key (often < > or < > |) next to the left shift key:

Symbol	Shifted symbol	Location	V-scan code
<	>		0x056

Using USB Devices in a Virtual Machine

VMware Workstation 4 provides a two-port USB 1.1 controller. You can use up to two USB devices in your virtual machine if both your host operating system and your guest operating system support USB. If your host computer supports USB 2.0 devices, you can use those devices in the virtual machine.

Note: Windows NT and Linux kernels older than 2.2.17 do not support USB.

Although your host operating system must support USB, you do not need to install device-specific drivers for your USB devices in the host operating system if you want to use those devices only in the virtual machine.

On a Windows 2000 host computer with USB 2.0 support, be sure you are using the Microsoft USB 2.0 driver for the USB controller. Third-party USB 2.0 drivers, such as those provided by some motherboard manufacturers, are not supported. For notes on replacing the third-party drivers, see Replacing USB 2.0 Drivers on a Windows 2000 Host on page 298.

Notes on USB Support in Version 4

We have tested a variety of USB devices with this release. In general, if the guest operating system has appropriate drivers, you should be able to use PDAs, printers, storage (disk) devices, scanners, MP3 players, digital cameras and memory card readers.

Modems and certain streaming data devices, such as speakers and Web cams, do not work properly.

Enabling and Disabling the USB Controller

The virtual machine's USB ports are enabled by default. If you will not be using USB devices in a virtual machine, you can disable its USB controller using the virtual machine settings editor.

Connecting USB Devices

When a virtual machine is running, its window is the active window and a USB device is plugged into the host computer, the device automatically connects to the guest instead of the host. This autoconnect feature can be disabled in the USB Controller panel of the virtual machine settings editor (**VM** > **Settings**). If all of the virtual machine's USB ports are already occupied when it is trying to connect automatically to a new device, a dialog box gives you a choice: you can either disconnect one of the existing USB devices to free its port or ignore the new device, allowing the device to connect to the host.

Choose **VM** > **Removable Devices** to connect specific USB devices to your virtual machine. You can connect up to two USB devices at a time. If the physical USB devices are connected to the host computer through a hub, the virtual machine sees only the USB devices, not the hub.

There is a menu item for each of the USB ports. Move the mouse over one of these items to see a cascading menu of devices that are plugged into your host computer and available for use. To connect a device to the virtual machine, click its name.

If a device is already connected to that port, click the name of a new device to release the first device and connect the new one.

To release a connected device, click **None** on the cascading menu for the port to which it is connected.

If you physically plug a new device into the host computer and the autoconnect feature does not connect it to a virtual machine, the device is initially connected to the host. Its name is also added to the **VM** > **Removable Devices** menu so you can connect it to the virtual machine manually.

Using USB with a Windows Host

Windows 2000, Windows XP and Windows Server 2003 hosts: When a particular USB device is connected to a virtual machine for the first time, the host detects it as a new device named VMware USB Device and installs the appropriate VMware driver.

Windows XP and Windows Server 2003 hosts: User confirmation is required in the Found New Hardware Wizard. Select the default action — **Install the software automatically**. Once the software is installed, the guest operating system detects the USB device and searches for a suitable driver.

When you are synchronizing a PDA, such as a Palm handheld or Handspring Visor, to a virtual machine for the first time, the total time required to load the VMware USB device driver in the host and the PDA driver in the guest may exceed the device's connection timeout value. This causes the device to disconnect itself from the computer before the guest can synchronize with it. If this occurs, let the guest finish installing the PDA driver, dismiss any connection error warnings, then try synchronizing the PDA again. The second attempt should succeed.

Replacing USB 2.0 Drivers on a Windows 2000 Host

To use VMware Workstation 4 on a Windows 2000 host that has USB 2.0 ports, you must use the Microsoft USB 2.0 drivers for the USB controller in the host operating system. If your host operating system is using a third-party driver — a driver supplied by your motherboard vendor, for example — you must replace it.

Take the following steps to check the provider of your driver:

1. Go to the Device Manager. Right-click **My Computer**, choose **Properties**, click the **Hardware** tab, then click **Device Manager**.
2. Expand the listing for Universal Serial Bus controllers.
3. Right-click the listing for the controller and choose **Properties**.
4. Click the **Driver** tab. If the driver provider shown on that page is Microsoft, you have the correct driver already.

If the driver provider is not Microsoft, download the latest USB driver for your host operating system from the Microsoft Web site and follow the Microsoft instructions to install it. Details are available in Microsoft knowledge base article 319973.

Installing USB Devices as a Non-Administrator

Any user on a Windows host can connect USB devices for use in a virtual machine. You no longer need administrative privileges on the host to connect a USB device to a virtual machine.

This functionality is not enabled by default. To enable it, you must use a text editor such as Notepad to add one line to the global configuration file. This file is `C:\Documents and Settings\<username>\Application Data\VMware\config.ini`

Add the following line anywhere in the file:

```
usb.EnablePnpMgr = TRUE
```

Note: A user with administrative privileges on the host operating system must install a USB device on the host before it can be connected by users who do not have administrative privileges.

Using USB with a Linux Host

On Linux hosts, VMware Workstation uses the USB device file system to connect to USB devices. In most Linux systems that support USB, the USB device file system is at `/proc/bus/usb`. If your host operating system uses a different path to the USB device file system, you can change it in the virtual machine settings editor (**VM** > **Settings** > **USB**). Enter the correct path in the **Path to usbdevfs** field.

Who Has Control over a USB Device?

Only one computer — host or guest — can have control of a USB device at any one time.

Device Control on a Windows Host

When you connect a device to a virtual machine, it is "unplugged" from the host or from the virtual machine that previously had control of the device. When you disconnect a device from a virtual machine, it is "plugged in" to the host.

Caution: On Windows 2000, Windows XP and Windows Server 2003 hosts, you need to take a special step to disconnect USB network and storage devices from the host. There is a system tray icon called Eject Hardware on Windows 2000 and Safely Remove Hardware on Windows XP and Windows Server 2003. Use this icon to disconnect the device from the host before connecting it to a virtual machine.

Note: On Windows 2000, Windows XP and Windows Server 2003 hosts, when you connect a USB network or storage device in a virtual machine, you may see a message on your host that says the device can be removed safely. This is normal behavior, and you can simply dismiss the dialog box. However, do **not** remove the device from your physical computer. VMware Workstation automatically transfers control of the device to the virtual machine.

Under some circumstances, if a USB storage device is in use on the host (for example, one or more files stored on the device are open on the host), an error appears in the virtual machine when you try to connect to the device. You must let the host complete its operation or close any application connected to the device on the host, then connect to the device in the virtual machine again.

Device Control on a Linux Host

On Linux hosts, guest operating systems can use devices that are not already in use by the host — that is, devices that are not claimed by a host operating system driver.

If your device is in use by the host and you try to connect it to the guest using the **VM** > **Removable Devices** menu, a dialog box appears, informing you that there is a problem connecting to the device.

To disconnect the device from the host, you must unload the device driver. You can unload the driver manually as root (`su`) using the `rmmod` command. Or, if the driver was automatically loaded by `hotplug`, you can disable it in the `hotplug` configuration files in the `/etc/hotplug` directory. See your Linux distribution's documentation for details on editing these configuration files.

A related issue sometimes affects devices that rely on automatic connection (as PDAs often do).

If you have successfully used autoconnection to connect the device to your virtual machine, then experience problems with the connection to the device, take the following steps:

1. Disconnect and reconnect the device. You can either unplug it physically, then plug it back in or use the **VM** > **Removable Devices** menu to disconnect it and reconnect it.
2. If you see a dialog box warning that the device is in use, disable it in the `hotplug` configuration files in the `/etc/hotplug` directory.

Disconnecting USB Devices from a Virtual Machine

Before unplugging a USB device or using the **VM** > **Removable Devices** menu to disconnect it from a virtual machine, be sure it is in a safe state.

You should follow the procedures the device manufacturer specifies for unplugging the device from a physical computer. This is true whether you are physically unplugging it, moving it from host to virtual machine, moving it between virtual machines or moving it from virtual machine to host.

This is particularly important with data storage devices (a Zip drive, for example). If you move a data storage device too soon after saving a file and the operating system has not actually written the data to the disk, you can lose data.

Human Interface Devices

USB human interface devices, such as the keyboard and mouse, are not handled though the virtual machine's USB controller. Instead, they appear in the virtual machine as a standard PS/2 keyboard and mouse, even though they are plugged into USB ports on the host.

Connecting to a Generic SCSI Device

Generic SCSI lets a virtual machine run any SCSI device that is supported by the guest operating system in the virtual machine. Generic SCSI gives the guest operating system direct access to SCSI devices connected to the host, such as scanners and tape drives.

Generic SCSI on a Windows Host Operating System

Using the SCSI Generic driver in Windows, VMware Workstation allows your guest operating system to operate generic SCSI devices — including scanners, tape drives and other data storage devices — in a virtual machine.

Note: In order to access host SCSI devices as Generic SCSI devices from within a virtual machine, you must run VMware Workstation as a user with administrator access.

Device Support

In theory, generic SCSI is completely device independent, but VMware has discovered it is sensitive to the guest operating system, device class and specific SCSI hardware. We encourage you to try any SCSI hardware you want to use and report problems to VMware technical support.

Note: If you are using generic SCSI devices in a Windows 95, Windows 98 or Windows Me guest operating system and are experiencing problems with the devices, download the latest Mylex® (BusLogic) BT/KT-958 compatible host bus adapter from *www.lsilogic.com*. This driver overrides what Windows chooses as the best driver, but it corrects known problems.

Preparing a Windows XP or Windows Server 2003 Guest Operating System to Use SCSI Devices

To use SCSI devices in a Windows XP or Windows Server 2003 virtual machine, you need a special SCSI driver available from the download section of the VMware Web site at *www.vmware.com/download*. Follow the instructions on the Web site to install the driver.

Preparing a Windows NT 4.0 Guest Operating System to Use SCSI Devices

Generic SCSI devices use the virtual Mylex (BusLogic) BT/KT-958 compatible host bus adapter provided by the virtual machine. Some guest operating systems guide you through installing the drivers after you install the first SCSI device in the virtual machine. On Windows NT 4.0, however, you may need to install the driver manually, if

it is not already installed for a virtual SCSI disk. You should do so before you add a generic SCSI device.

To install the BusLogic driver in a Windows NT 4.0 guest, have your Windows NT installation CD available and follow these steps.

1. Open the SCSI Adapters control panel.

   Start > **Settings** > **Control Panel** > **SCSI Adapters**
2. Click the **Drivers** tab.
3. Click **Add**.
4. In the list of vendors on the left, select **BusLogic**.
5. In the list of drivers on the right, select **BusLogic MultiMaster PCI SCSI Host Adapters**.
6. Click **OK**.
7. Insert the Windows NT CD when you are prompted. Click **OK**.
8. Reboot when you are prompted.

Adding a Generic SCSI Device to a Virtual Machine

You can add generic SCSI devices to your virtual machine in the virtual machine settings editor. When you set up a generic SCSI device, the virtual machine must be powered off.

1. If it is not already running, launch VMware Workstation.

   Start > **Programs** > **VMware** > **VMware Workstation**
2. Open the virtual machine in which you want to use the generic SCSI device. Make sure the virtual machine is powered off.
3. From the VMware Workstation window, choose **VM** > **Settings**. The virtual machine settings editor opens.
4. Click **Add** to start the Add Hardware Wizard. Click **Next**.
5. Select **Generic SCSI Device**, then click **Next**.
6. Choose the name of the physical device you want to use.

   Then choose the virtual device node where you want this device to appear in the virtual machine.

   A check box under Device status allows you to specify whether the device should be connected each time the virtual machine is powered on.
7. Click **Finish** to install the new device.

8. Click **OK** to save the configuration and close the virtual machine settings editor.

To remove this device, launch the virtual machine settings editor, select the generic SCSI device, then click **Remove**.

Generic SCSI on a Linux Host Operating System

Using the SCSI Generic driver in Linux, VMware Workstation allows your guest operating system to operate generic SCSI devices within a virtual machine. The SCSI Generic driver sets up a mapping for each SCSI device in `/dev`. Each entry starts with `sg` (for the SCSI Generic driver) followed by a letter. For example, `/dev/sga` is the first generic SCSI device.

Each entry corresponds to a SCSI device, in the order specified in `/proc/scsi/scsi`, from the lowest device ID on the lowest adapter to the highest device ID on the lowest adapter, and so on to the highest device ID on the highest adapter. Do not enter `/dev/st0` or `/dev/scd0`.

Note: When setting up a generic SCSI device in the virtual machine settings editor, as described later in this section, you specify the device you wish to install in the virtual machine by typing its `/dev/sg` entry in the **Connection** field. You must be logged on as a user who has permissions to use the device.

Requirements

Generic SCSI requires version 2.1.36 of the SCSI Generic (`sg.o`) driver, which comes with kernel 2.2.14 and higher.

Avoiding Concurrent Access to a Generic SCSI Device

Under Linux some devices — specifically tape drives, disk drives and CD-ROM drives — already have a designated `/dev` entry (traditionally, `st`, `sd` and `scd`, respectively). When the SCSI Generic driver is installed, Linux also identifies these devices with corresponding `sg` entries in `/dev` — in addition to their traditional entries. VMware Workstation ensures that multiple programs are not using the same `/dev/sg` entry at the same time but cannot always ensure that multiple programs are not using the `/dev/sg` and the traditional `/dev` entry at the same time. It is important that you do not attempt to use the same device in both host and guest. This can cause unexpected behavior and may cause loss or corruption of data.

Permissions on a Generic SCSI Device

You must have read and write permissions on a given generic SCSI device in order to use the device within a virtual machine, even if the device is a read-only device such as a CD-ROM drive. These devices typically default to root-only permissions. Your

administrator should create a group with access to read and write to these devices, then add the appropriate users to that group.

Device Support

In theory, generic SCSI is completely device independent, but VMware has discovered it is sensitive to the guest operating system, device class and specific SCSI hardware. We encourage you to try any SCSI hardware you want to use and report problems to VMware technical support.

Note: If you are using generic SCSI devices in a Windows 95, Windows 98 or Windows Me guest operating system and are experiencing problems with the devices, download the latest Mylex (BusLogic) BT/KT-958 compatible host bus adapter from *www.lsilogic.com*. This driver overrides what Windows chooses as the best driver, but it corrects known problems. To use SCSI devices in a Windows XP or Windows Server 2003 virtual machine, you need a special SCSI driver available from the download section of the VMware Web site at *www.vmware.com/download*.

Adding a Generic SCSI Device to a Virtual Machine

You can add generic SCSI devices to your virtual machine in the virtual machine settings editor. The virtual machine settings editor lets you map virtual SCSI devices to physical generic SCSI devices on the host.

When you set up a generic SCSI device, the virtual machine must be powered off.

1. Launch VMware Workstation and select the virtual machine. Make sure the virtual machine is powered off.
2. Choose **VM** > **Settings**. The virtual machine settings editor opens.
3. Click **Add** to start the Add Hardware Wizard. Select **Generic SCSI Device**, then click **Next**.
4. Choose the name of the physical device you want to use.

   Then choose the virtual device node where you want this device to appear in the virtual machine.

   A check box under Device status allows you to specify whether the device should be connected each time the virtual machine is powered on.
5. Click **Finish** to install the new device.
6. Click **OK** to save the configuration and close the virtual machine settings editor.

To remove this device, launch the virtual machine settings editor, select the generic SCSI device, then click **Remove**.

CHAPTER 12

Performance Tuning

The following sections offer suggestions for getting the best performance from VMware Workstation and your virtual machines:

Configuring and Maintaining the Host Computer

You may see slower virtual machine performance if the physical disk that holds the virtual machine's working directory or the physical disk that holds the virtual disk files is badly fragmented. By default, the working directory holds the virtual disk files and is on the host computer. If you have customized the virtual machine configuration, you may have placed the working directory or the virtual disk files on a different physical computer.

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 have 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.

Configuring VMware Workstation

This section offers advice and information about factors that can affect the performance of VMware Workstation itself. This section does not address performance of the guest operating system or the host operating system.

Note: In addition to the VMware Workstation configuration options discussed below, 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 on page 81.

General VMware Workstation Options

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 Workstation 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 may 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 should not cause a virtual machine to run incorrectly, but it may 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 a good thing.

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 may be able to improve performance by adjusting the settings in the virtual machine settings editor (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 application memory settings may also help. Go to **Edit** > **Preferences** > **Memory**.

For additional information, see Memory Usage Notes on page 317.

Debugging Mode

VMware Workstation can run in two modes — normal mode and a mode that provides extra debugging information. The debugging mode is slower than normal mode.

For normal use, check to be sure you are not running in debugging mode. Go to **VM** > **Settings** > **Options** and select **Advanced**. In the Advanced Options section, be sure there is no check in the **Run with debugging information** check box.

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. (This allows them to run autorun programs.) This polling can cause VMware Workstation to connect to the host CD-ROM drive, which can make it 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*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 start disconnected. The drive appears in the virtual machine, but it always appears to contain no disc (and VMware Workstation does not connect to your host CD-ROM drive).

  To make this change, go to **VM** > **Settings**. Click 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 raw) affect performance in a number of ways.

Inside a virtual machine, SCSI disks and IDE disks that use direct memory access (DMA) have approximately the same performance. However, IDE disks can be very slow in a guest operating system that either cannot use or 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 2000, DMA access is enabled by default. In other Windows guest operating systems, the method for changing the setting varies with the operating system. See the following technical notes for details.

- Disk Performance in Windows NT Guests on Multiprocessor Hosts on page 195
- Windows 95 and Windows 98 Guest Operating System Performance Tips on page 322

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, raw disks and virtual disks with all the space allocated in advance 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 raw disks or virtual disks with all the space allocated in advance, you see somewhat better performance than that provided by other configurations.

Disk writes may be slower for virtual disks that do not have all space allocated in advance. However, 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.

Snapshot

If you do not need to use the snapshot feature, it is best to run your virtual machine with no snapshot. This provides best performance. To be sure a virtual machine has no snapshot, choose **Snapshot** > **Remove Snapshot**.

VMware Workstation on a Windows Host

Note: The items in this section describe performance of VMware Workstation on a Windows host. For tips on configuring VMware Workstation on a Linux host, see VMware Workstation on a Linux Host on page 314.

Process Scheduling

Note: The information in this hint was created to address scheduling problems with Windows NT. The issues are likely to be different in Windows 2000, Windows XP and Windows Server 2003; however, we do not currently have corresponding information for Windows 2000, Windows XP or Windows Server 2003 hosts.

The process scheduler on Windows NT does not necessarily schedule processes in a way that allows you to get the best performance from your particular combination of virtual machines and applications running on the host. VMware Workstation on a Windows host provides configuration options that let you adjust scheduling priorities to meet your needs.

These configuration options are available from the **Edit** > **Preferences** > **Priority** and **VM** > **Settings** > **Options** > **Advanced** menu options. These menu items allow you to specify either high or normal priority when the mouse and keyboard are grabbed by the virtual machine and either normal or low priority when they are not grabbed.

Global priority is taken as the default across all virtual machines. Local priority overrides the global settings for just the specific virtual machine where you make the changes.

Pay particular attention to the **grabbed: HIGH – ungrabbed: NORMAL** and **grabbed: NORMAL – ungrabbed: LOW** settings.

The **grabbed: HIGH – ungrabbed: NORMAL** setting is useful if you have many background processes or applications and you do not care if they run with fairly low relative priority while VMware Workstation is in the foreground. In return, you get a very noticeable performance boost using a VMware Workstation virtual machine while another virtual machine is running or while some other processor-intensive task (a compile, for example) is running in the background.

The reverse is true of the **grabbed: NORMAL – ungrabbed: LOW** setting. If your host machine feels too sluggish when a virtual machine is running in the background, you can direct the virtual machine to drop its priority when it does not have control of the

mouse and keyboard. As with the high setting, this is a heavy-handed change of priority, so the virtual machine and any background applications run much more slowly.

VMware Workstation on a Linux Host

Note: The items in this section describe performance of VMware Workstation on a Linux host. For tips on configuring VMware Workstation on a Windows host, see VMware Workstation on a Windows Host on page 313.

Using Full Screen Mode

Full screen mode is faster than window mode. As a result, if you do not need to have your virtual machine and your host sharing the screen, try switching to full screen mode.

Note: The extreme case of this is 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.

Monitoring Virtual Machine Performance

VMware Workstation incorporates a set of performance counters that work with Microsoft's Performance console so you can collect 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 virtual machines running on the Windows host, including those running Linux guest operating systems.

The VMware Workstation performance counters can monitor the following data from a running virtual machine:

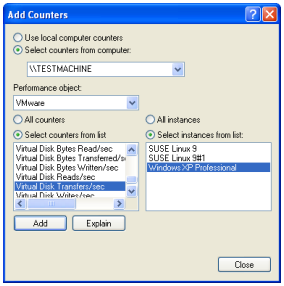
- Reading and writing to virtual disks
- Memory used by the virtual machine
- Virtual network traffic

You can track virtual machine performance only when 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 a virtual machine reads from a virtual disk, but they cannot track how many processes are running inside the guest operating system. An explanation of each counter appears in the Performance console.

To add counters to track virtual machine performance, use the Windows Performance console. Take the following steps.

1. Open the Administrative Tools control panel and double-click **Performance**. The Performance console opens.

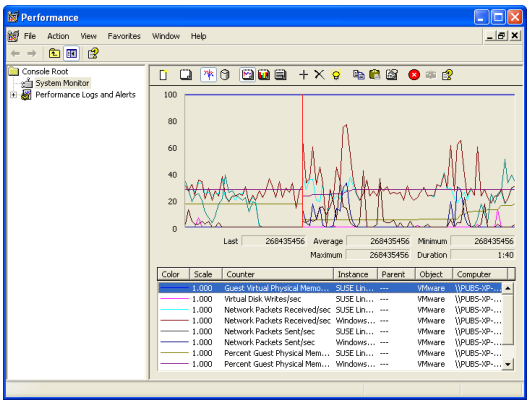
2. Click the plus (+) sign on the toolbar. The Add Counters dialog box appears.



3. In the **Performance object** list, select **VMware**.
4. Decide whether you want to add all counters or select specific 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, select **Select instances from list**, then choose the virtual machines you want. The names shown in the list correspond to the display names of running virtual machines.

   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, choose **Action** > **Help** in the Performance console or go to the Microsoft Web site.

Memory Usage Notes

VMware Workstation allows you to make the following memory-related settings:

- The memory size of a particular virtual machine
- The amount of the host computer's RAM that can be used for virtual machines.
- 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 three settings, you can affect both virtual machine and overall system performance.

This section describes how VMware Workstation uses the memory configuration parameters to manage virtual machines and system memory properly.

Virtual Machine Memory Size

The first configuration parameter you can set is the size of an individual virtual machine's memory. Set this configuration parameter for the virtual machine in the virtual machine settings editor (**VM** > **Settings** > **Memory**). The guest memory size should not be set lower than the minimum recommendations of the operating system provider.

The New Virtual Machine Wizard sets reasonable defaults for the memory size of a virtual machine, based on the type of the guest operating system and the amount of memory in the host computer. This value also appears in the virtual machine settings editor as the recommended memory value.

The virtual machine settings editor also shows a value for the maximum amount of memory for best performance. If you have only one virtual machine running on the host and you set virtual machine memory to this value, the virtual machine can run entirely in RAM. A virtual machine running completely in RAM performs better than a virtual machine that must swap some of its memory to disk.

The actual memory size you should give to a virtual machine depends on a few practical considerations:

- What kinds of applications will run in the virtual machine
- What other virtual machines will contend with this virtual machine for memory resources
- What applications will run on the host at the same time as the virtual machine

Note: You cannot allocate more than 2GB of memory to a virtual machine if the virtual machine's files are stored on a file system such as FAT32 that does not support files greater than 2GB.

The total amount of memory you assign to all virtual machines running on a single host may not exceed 4GB.

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 — 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 Workstation enforces a limit on the total amount of RAM that may be consumed by virtual machines.

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 Virtual Machines

The second configuration parameter you can set is the amount of RAM that VMware Workstation is allowed to reserve for all running virtual machines combined. To set this parameter, go to Edit > Preferences > Memory.

The reserved memory setting specifies a maximum amount of RAM that VMware Workstation is allowed to use. But this memory is not allocated in advance. Even if multiple virtual machines are running at the same time, VMware Workstation may be using only a fraction of the RAM you specify here. Any unused RAM is available to be used 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 RAM itself or allow other applications to use it.

The RAM used by VMware Workstation includes the RAM made available to the guest operating systems plus a small amount of overhead memory associated with running a virtual machine.

The amount of RAM actually used for a particular virtual machine varies dynamically 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 appears in the

reserved memory control — **Edit** > **Preferences** > **Memory**. If you want VMware Workstation to use more or less RAM, move 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 very poorly and you cannot run as many virtual machines at once.

Using Additional Memory

By default, VMware Workstation limits the number of virtual machines that can run at once based on the amount of memory specified in the application settings. This prevents virtual machines from causing each other to perform poorly.

To allow more or larger virtual machines to run, you can adjust a third setting — the amount of virtual machine memory that the host operating system may swap to disk. To change this setting, go to **Edit** > **Preferences** > **Memory** and change the additional memory setting. Select one of the following radio buttons:

- **Fit all virtual machine memory into reserved host RAM** — Strictly apply the reserved memory limit set in the top of the panel. 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 Workstation displays a warning message. The message shows how much memory the virtual machine is configured to use and how much memory is available. To try to power on the virtual machine using the available memory, click **OK**. If you do not want to power on the virtual machine, click **Cancel**.

Using More Than 1GB of Memory on a Linux Host

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.)

The CONFIG_2GB option calls for recompiling your kernel as a 2GB kernel. You do this by recompiling your kernel with CONFIG_2GB enabled. This allows Linux to support nearly 2GB of physical memory by dividing the address space into a 2GB user section and a 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 Workstation does not run. To work around this issue, you can either:

- 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 Workstation. To do this:
  - At the LILO prompt, type `linux-2.2.16xxx mem=959M`.
  - Or, edit `lilo.conf`. 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:
  - At the LILO prompt, type `linux-2.2.16xxx mem=1983M`.
  - Or, edit `lilo.conf`. 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:
  - At the LILO prompt, type `linux-2.2.16xxx mem=959M`.
  - Or, edit lilo.conf. 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 Workstation 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 Workstation. To use the switch:

- At the LILO prompt, type `linux-2.2.16xxx mem=1983M`.
- Or, edit `lilo.conf`. In the kernel section, add this line:
  ```
  append mem="1983M"
  ```

Improving Performance for Guest Operating Systems

The tips in this section help you make adjustments to improve performance for particular guest operating systems running inside a virtual machine.

Windows 95 and Windows 98 Guest Operating System Performance Tips

This section offers advice for configuring a Windows 95 or Windows 98 guest operating system for better performance inside a VMware Workstation virtual machine.

Note: This document pertains to the guest operating system that is running inside a VMware Workstation virtual machine. It does not describe actions that should be taken on the host.

Guest Operating System Selection

Make certain you have selected the correct guest operating system in the virtual machine settings editor — **VM** > **Settings** > **Options**.

VMware Tools

Make certain VMware Tools is installed. VMware Tools provides an optimized SVGA driver and sets up the VMware Tools service to run automatically when the system starts. Among other things, the VMware Tools service allows you to synchronize the virtual machine's clock with the host computer's clock, which can improve performance for some functions. You can install VMware Tools by choosing **VM** > **Install VMware Tools**.

DMA Mode for IDE Disks

Windows 95 OSR2 and later (including Windows 98) can use direct memory access (DMA) for faster access to IDE hard disks. However, this feature may not be enabled by default.

You can turn on DMA access using the guest operating system's Device Manager.

1. Right-click **My Computer** and choose **Properties** from the pop-up menu.
2. Click the + sign beside **Disk Drives** to show your virtual machine's individual drives.
3. Right-click the entry for each IDE drive to open its Properties dialog box.

4. Under **Settings**, check the box labeled **DMA** and accept any warning Windows displays.
5. Restart Windows for the new settings to take effect.

Full Screen Mode
Run your virtual machine in full screen mode. Click the **Full Screen** button on the VMware Workstation toolbar.

Swap File Usage
In your `system.ini` file, in the `[386enh]` section, add the following line:

```
ConservativeSwapFileUsage=1
```

Disconnect CD-ROM and /dev/rtc
Using the **VM** > **Removable Devices** menu, disconnect your CD-ROM drive if you do not need to use it.

If you are using a Linux host and have a Windows 95 guest, also disconnect `/dev/rtc`. Do not disconnect it in a Windows 98 guest.

Disconnecting these devices reduces CPU usage.

Note: The time synchronization feature in VMware Tools does not rely on `/dev/rtc.`

Visual Effects
Windows 98 has a number of visual effects, designed to be attractive, that place unnecessary demands on the graphics emulation in VMware Workstation. Some users have seen performance improvements when they turn off these special effects.

To modify these settings, right-click on the desktop of your virtual machine, then select **Properties** from the pop-up menu. Click the **Effects** tab and uncheck the **Animate windows, menus, and lists** check box.

Also, if you have **Show window contents while dragging** checked, try unchecking that check box.

Windows 2000, Windows XP and Windows Server 2003 Guest Operating System Performance Tips

This section offers advice for configuring a Windows 2000, Windows XP or Windows Server 2003 guest operating system for better performance inside a VMware Workstation virtual machine.

Note: This document pertains to the guest operating system that is running inside a VMware Workstation virtual machine. It does not describe actions that should be taken on Windows 2000, Windows XP or Windows Server 2003 running on the host computer.

Guest Operating System Selection

Make certain you have selected the correct guest operating system in the virtual machine settings editor — VM > Settings > Options.

VMware Tools

Make certain VMware Tools is installed. VMware Tools provides an optimized SVGA driver and sets up the VMware Tools service to run automatically when the system starts. Among other things, the VMware Tools service allows you to synchronize the virtual machine's clock with the host computer's clock, which can improve performance for some functions. You can install VMware Tools by choosing VM > Install VMware Tools.

Disconnect CD-ROM and /dev/rtc

Using the VM > Removable Devices menu, disconnect your CD-ROM drive if you do not need to use it. If you are using a Linux host, also disconnect `/dev/rtc`. Disconnecting these devices reduces CPU usage.

Note: The time synchronization feature in VMware Tools does not rely on `/dev/rtc.`

Visual Effects

The fade effects that Windows 2000, Windows XP and Windows Server 2003 use when displaying menus can be somewhat slow and make the virtual machine seem less responsive.

To disable the fade effects, right-click the guest operating system desktop, then choose Properties > Appearance > Effects (on Windows XP or Windows Server 2003) or Properties > Effects (on Windows 2000) and uncheck Use transition effects for menus and tool tips.

Full Screen Mode

Run your virtual machine in full screen mode. Click the **Full Screen** button on the VMware Workstation toolbar.

Linux Guest Operating System Performance Tips

This section offers advice for configuring a Linux guest operating system for better performance inside a VMware Workstation virtual machine.

Note: This document pertains to the guest operating system that is running inside a VMware Workstation virtual machine. It does not describe actions that should be taken on Linux running on the host.

Guest Operating System Selection

Make certain you have selected the correct guest operating system in the virtual machine settings editor — VM > Settings > Options.

VMware Tools

Make certain VMware Tools is installed. VMware Tools provides an optimized SVGA driver and sets up the VMware Tools service to run automatically when the system starts. Among other things, the VMware Tools service allows you to synchronize the virtual machine's clock with the host computer's clock, which can improve performance for some functions. You can install VMware Tools by choosing VM > Install VMware Tools.

Disconnect CD-ROM and /dev/rtc

Using the VM > Removable Devices menu, disconnect your CD-ROM drive if you do not need to use it. If you are using a Linux host, also disconnect `/dev/rtc`. Disconnecting these devices reduces CPU usage.

Note: The time synchronization feature in VMware Tools does not rely on `/dev/rtc.`

Install in Text Mode

When you are installing your Linux guest operating system, use the text-mode installer instead of the graphical installer if you have a choice. This makes the installation process faster.

If you do use a graphical installer and if you are using a Linux host computer, try to run VMware Workstation in full screen mode during the installation.

Full Screen Mode

Run your virtual machine in full screen mode. Click the Full Screen button on the VMware Workstation toolbar.

CHAPTER 13

Special-Purpose Configuration Options

The following sections describe how to use special-purpose configuration options:

In some situations you may find it useful to restrict a user's ability to reconfigure virtual machines and to simplify the user interface for inexperienced users. In a classroom, for example, you may want to ensure that virtual machine configurations remain consistent from one class session to the next.

The special-purpose configuration options available on Windows hosts meet these needs.

Administrative lockout is a global setting for VMware Workstation itself and affects all virtual machines. Restricted user interface affects only the specific virtual machines for which the setting has been made. Full screen switch mode affects the way VMware Workstation itself runs and, as a result, affects all virtual machines.

These options are available on Windows hosts only.

Locking Out Interface Features

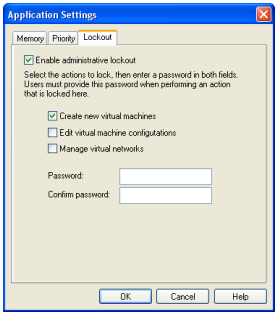
Administrative lockout is a global setting that affects all virtual machines for all users on a host computer. It allows a user to impose any combination of the following restrictions:

- Only a user who knows the password can create new virtual machines.
- Only a user who knows the password can edit virtual machine configurations.
- Only a user who knows the password can edit network settings.

Note: If no user has yet set administrative lockout preferences, any user may set them and set a password for access to the administrative lockout features. If any user has already set administrative lockout preferences, you must know the password in order to change the settings.

Take the following steps to set administrative lockout preferences:

1. Open the Application Settings dialog box (**Edit** > **Preferences**).
2. Click the **Lockout** tab. If a password is already set for the administrative lockout feature, enter the password when prompted.



3. Be sure **Enable administrative lockout** is selected and select the actions you want to restrict. If this is the first time administrative lockout options have been set, enter a password in the **Password** field and again in the **Confirm password** field.
4. Click **OK** to save the settings.

Removing a Forgotten Password

If you cannot remember the password and want to remove it, you must uninstall Workstation. Be sure to click **Yes** when asked if you want to remove the administrative

lockout settings. After you reinstall Workstation, you may enable the administrative lockout features again and set a new password.

Restricting the User Interface

The restricted user interface affects only the specific virtual machines for which the setting has been made. The following changes are made when you enable the restricted user interface:

- The toolbar is always hidden.
- All functions on the **Power** menu are disabled.
- All functions on the **Snapshot** menu and snapshot functions on the toolbar are disabled.
- There is no access to the virtual machine settings editor from the VMware Workstation window.
- The user cannot change virtual networking settings.
- The user starts the virtual machine by double-clicking the configuration file (`.vmx` file) or a desktop shortcut to that file. The virtual machine powers on automatically. At the end of the working session, the user shuts down by closing the virtual machine (**File** > **Exit**).

  It is also possible to launch VMware Workstation, then open a restricted-interface virtual machine from the virtual machine list or the **File** menu.

The changes needed to enable the restricted user interface must be made by a user with sufficient privileges to edit the virtual machine's configuration file and to set file permissions as described below.

Take the following steps to enable the restricted user interface.

1. Power off the virtual machine and close the VMware Workstation window, then open the virtual machine's configuration file (`.vmx` file) in Notepad or another text editor. Add the following line anywhere in the file:

   ```
   gui.restricted = "true"
   ```

2. You may wish to set file permissions on the configuration file to give normal users of the system only read access to the file, so they cannot manually modify the configuration.
3. For the convenience of users, create a shortcut to the configuration file on the desktop and give it an appropriate name.

Note: Although the restricted user interface provides no access to menu and toolbar controls for the snapshot, you may choose to give the user limited snapshot control. If you set up a snapshot for the restricted virtual machine and set the power-off option to **Ask me**, the user sees the standard dialog box when shutting down a virtual

machine and has the opportunity to choose **Just power off**, **Take snapshot** or **Revert to snapshot**.

Automatically Returning to a Snapshot with a Restricted User Interface

You can combine a restricted user interface with a snapshot to ensure that users' virtual machines always start in the same state. Typically, users running a virtual machine with a restricted user interface can power it on and off only, and the virtual machine boots when powered on. When the virtual machine has a snapshot set and is configured to return to that snapshot when powered off, the user can only start and power off the virtual machine. The virtual machine always starts from the snapshot.

Since you can restrict the user interface only on Windows hosts, this combination works only with virtual machines running on Windows hosts.

To set up a virtual machine with restricted user interface and a snapshot as described above, take the following steps:

1. Power on the virtual machine and be sure it is in the state you want, then take the snapshot.
2. Configure the virtual machine to return to the snapshot any time it is powered off. To do so, go to **VM** > **Settings** > **Options** > **Snapshot** and select **After powering off** and **Revert to snapshot**.
3. With the virtual machine powered off, restrict the user interface. Close the VMware Workstation window, then open the virtual machine's configuration file (`.vmx` file) in Notepad or another text editor. Add the following line anywhere in the file.
   ```
   gui.restricted = "true"
   ```
4. You may wish to set file permissions on the configuration file to give normal users of the system only read access to the file, so they cannot manually modify the configuration.
5. For the convenience of users, create a shortcut to the configuration file on the desktop and give it an appropriate name.

The user runs this virtual machine by double-clicking the shortcut to the configuration file. The virtual machine starts at the snapshot, with the user interface restricted — with no toolbar and no access to the Power menu or the virtual machine settings editor.

When the user is finished working with this virtual machine, he or she closes it by choosing **File** > **Close**. The virtual machine powers off, and the next time a user powers it on, it returns to the snapshot.

To remove the restriction on the interface, take the following steps.

1. Power off the virtual machine and close the VMware Workstation window.
2. Open the configuration file (`.vmx`) file and do one of the following:
   - Set `gui.restricted = "false"`.
   - Remove or comment out the `gui.restricted = "true"` line.

   Save the changes to the configuration file and close it.
3. Start the virtual machine by double-clicking the shortcut. The virtual machine starts at the snapshot, and the interface is not restricted.

Using Full Screen Switch Mode

Full screen switch mode is a run-time option for the VMware Workstation program. When VMware Workstation is running in full screen switch mode, the user has no access to the VMware Workstation user interface. The user cannot create, reconfigure or launch virtual machines. A system administrator performs these functions.

When VMware Workstation is running in full screen switch mode, one or more virtual machines may be running and you can use hot keys to switch from one to another. You may also provide hot key access to the host operating system.

Creating a Virtual Machine for Use in Full Screen Switch Mode

To create new virtual machines, you must run VMware Workstation in standard mode. The instructions in this section assume that you are creating the virtual machines on a separate administrative computer. However you may, if you prefer, create the virtual machines directly on the user's computer.

Create the new virtual machine following the instructions in Creating a New Virtual Machine on page 65. Be sure to make the following choices:

- In step 6, select **Custom** to perform a custom installation.
- In step 8, make a note of the folder in which you create the virtual machine. You must copy all the files in this folder to the user's computer after you finish creating and configuring the virtual machine.
- In step 12, specify the desired size for the virtual disk and select **Allocate all disk space now**. This selection is not required, but it is strongly recommended. If you do not make this selection and the host computer's hard disk runs out of space for a growing virtual disk file, the user sees no warning message and does not know what is causing the problem in the virtual machine.

Make all needed configuration settings before you configure the user's computer to launch VMware Workstation when the computer starts. You cannot change virtual machine settings using the virtual machine settings editor when VMware Workstation is running in full screen switch mode. You may find it most convenient to finish configuring the virtual machine and to install the guest operating system and application software before you move the virtual machine to the user's computer.

Moving a Virtual Machine to the User's Computer

The easiest way to move the virtual machine to the user's computer is to use a network connection to copy all the files in the virtual machine directory to a directory

on the user's computer. You may also move it using a DVD or other removable media large enough to store the files.

Each virtual machine should be in its own directory.

Setting Configuration Options on the User's Computer

Global configuration settings are made in the VMware Workstation global configuration file, created by default as `C:\Documents and Settings\All Users\Application Data\VMware\VMware Workstation\config.ini`. You can edit this file with a text editor. You should set permissions on this file so the user cannot change it.

Local configuration settings are made in the configuration file for a particular virtual machine. The local configuration file is in the virtual machine's directory; the filename has a `.vmx` extension.

The format for an entry in either configuration file is

```
option = "value"
```

Entries in the configuration files can appear in any order.

The hot key entries described in this section require you to enter a virtual key code as part of the value for an option. Virtual key codes are entered in hexadecimal format — as a hexadecimal number preceded by 0x. For example, to use the virtual key code of 5A as a value, type `0x5A`.

Microsoft provides a reference list of virtual key codes on the MSDN Web site. At the time this manual was written, the reference list was at *msdn.microsoft.com/library/en-us/winui/WinUI/WindowsUserInterface/UserInput/VirtualKeyCodes.asp*.

The hot key entries also include modifier keys. The modifier keys are Ctrl, Alt and Shift, or a combination of those keys.

Modifier key	Value
No modifier	0x0
Alt	0x1
Ctrl	0x2
Shift	0x4
Ctrl-Alt	0x3
Alt-Shift	0x5
Ctrl-Shift	0x6
Ctrl-Alt-Shift	0x7

When listing a key plus a modifier, type the virtual key code for the key followed by a comma, then type the value for the modifier key or keys. For example, the value entry for Ctrl-Shift-F1 is `0x70,0x6`.

Note: Keep the following limitations in mind when defining cycle keys and switch keys:

- Do not use the Pause key with the Ctrl key. You may use the Pause key with other modifier keys.
- If you use F12, you must use one or more modifier keys. You cannot use F12 alone.
- You cannot use combinations that include only the Shift, Ctrl and Alt keys. These keys may be used only as modifiers in combination with some other key.

Hot Key for Cycling Through Virtual Machines and the Host Computer

You can specify a hot key or hot key combination for cycling through the available virtual machines on a host computer. Each time you press the specified hot key, the screen displays the next virtual machine in order. You may also include the host operating system in the cycle.

If any particular virtual machine is not running, it is skipped.

If only one virtual machine is running and the host operating system is not included in the cycle, pressing the hot key has no effect.

The hot key for cycling through virtual machines is defined in the global configuration file (`config.ini`).

Two options control cycling.

`FullScreenSwitch.cycleKey`
The value of this option defines the hot key. It is specified as `<key>,<modifier>`. There is no default.

For example, to use the Pause key with no modifier to cycle through virtual machines, add the following line to the `config.ini` file, or modify its value if the option is already listed.

```
FullScreenSwitch.cycleKey = "0x13,0x0"
```

`FullScreenSwitch.cycleHost`
The value of this option determines whether the host operating system is included in the cycle. Possible values are true and false. The default value is false.

For example, to include the host operating system in the cycle, add the following line to the `config.ini` file, or modify its value if the option is already listed:

```
FullScreenSwitch.cycleHost = "TRUE"
```

Hot Keys for Switching Directly to Virtual Machines and the Host Computer

You can specify a hot key or hot key combination for switching directly to any available virtual machine on a host computer. Each time you press the specified hot key, the screen display switches to that of the specified virtual machine. You may also specify a hot key for switching directly to the host operating system.

If any particular virtual machine is not running, pressing the hot key for that virtual machine has no effect.

You define the hot key used to switch to a virtual machine by adding a line to the target virtual machine's configuration (`.vmx`) file. The value of this option defines the hot key. It is specified as `<key>,<modifier>`. There is no default.

For example, to use Ctrl-Shift-F1 to switch to a particular virtual machine, add the following line to that virtual machine's `.vmx` file, or modify its value if the option is already listed.

```
FullScreenSwitch.directKey = "0x70,0x6"
```

You define the hot key used to switch to the host operating system by adding a line to the global configuration file (`config.ini`). The value of this option defines the hot key. It is specified as `<key>,<modifier>`. There is no default.

For example, to use Ctrl-Shift-F9 to switch to the host operating system, add the following line to the `config.ini` file, or modify its value if the option is already listed.

```
FullScreenSwitch.hostDirectKey = "0x78,0x6"
```

Other Entries in the Global Configuration File

The following entries in the global configuration file (`config.ini`) are optional. They enable you to control certain functions of the virtual machine that are important in work environments where virtual machines need to be isolated from each other and from the host computer.

`Isolation.tools.copy.enable`

The value of this option determines whether data in one virtual machine or the host operating system can be copied in a way that allows it to be transferred to another virtual machine or to the host operating system. Possible values are true (such copying is allowed) and false (such copying is not allowed). The default value is false.

The setting for this option should be the same as the setting for `Isolation.tools.paste.enable` (below).

`Isolation.tools.paste.enable`
The value of this option determines whether data copied in one virtual machine or the host operating system can be pasted into another virtual machine or the host operating system. Possible values are true (such pasting is allowed) and false (such pasting is not allowed). The default value is false. The setting for this option should be the same as the setting for `Isolation.tools.copy.enable` (above).

`Isolation.tools.HGFS.disable`
The value of this option determines whether virtual machines can be configured with shared folders, for sharing files among virtual machines and with the host computer. Possible values are true (shared folders are disabled) and false (shared folders are enabled). The default value is true.

The following entries are required in the global configuration file (`config.ini`) and must not be changed:

```
mks.ctlAltDel.ignore = "TRUE"
mks.fullscreen.allowScreenSaver = "TRUE"
fullScreenSwitch.onSeparateDesktop = "TRUE"
msg.autoAnswer = "TRUE"
```

Starting and Stopping Virtual Machines on the User's Computer

Use the `vmware-fullscreen` command to run VMware Workstation in full screen switch mode and to start and stop virtual machines on a user's computer. The command can pass certain information to the virtual machine when it starts.

As administrator, you must decide how to issue the command. For example, you may use a custom application or script running on the host operating system to issue one or more `vmware-fullscreen` commands. Or you can include the command to start a virtual machine in a shortcut in the host operating system's startup group, so the virtual machine starts automatically when the user logs on to the host computer.

The `vmware-fullscreen` command must be issued once for each virtual machine you want to start or stop.

```
vmware-fullscreen -poweron [-s variable=value]
[-name=<alias>] [-directkey=<keyspec>] [-fullscreen]
"<config-file>"
```

When you use the optional switches shown here, the `-poweron` switch is required

and must be the first switch after the `vmware-fullscreen` command. Provide the full path to the virtual machine's configuration (`.vmx`) file at the end of the command line. The complete command must be entered on one line.

Use the `-s` switch to pass a variable name and value to be used in configuring the virtual machine. You may include multiple `variable=value` pairs in the command. Each `variable=value` pair must be preceded by `-s`.

Use `-name=<alias>` to give a name to the virtual machine. You can the use that alias in `-switchto` and `-poweroff` commands.

Use `-directkey=<keyspec>` to specify the virtual machine's direct-switch key. If a direct-switch key is specified in the virtual machine's configuration file, the one specified on the command line overrides the one in the configuration file.

For example, to start a virtual machine and specify that its direct-switch key combination is Ctrl-Shift-F1, use the following command:

```
vmware-fullscreen -poweron -directkey=0x70,0x6
"<config-file>"
```

The complete command must be entered on one line.

Use `-fullscreen` to start a virtual machine and go straight to full screen switch mode. The virtual machine takes over the display immediately, instead of running invisibly until the user switches to it later.

Starting a Virtual Machine

`vmware-fullscreen -poweron "<config-file>"`

Use this command to power on the virtual machine without passing any additional information to the virtual machine. Provide the full path to the virtual machine's configuration (`.vmx`) file.

The user sees no immediate indication that the virtual machine has started, but the user can switch to the virtual machine with its direct-switch key or with the cycle key.

Stopping a Virtual Machine

`vmware-fullscreen -poweroff "<config-file>"`
`vmware-fullscreen -poweroff <alias>`

Use this command to shut down the specified virtual machine. You can specify the path to the configuration (`.vmx`) file, or you can specify the alias if you used `-name=` when you started the virtual machine.

Stopping All Virtual Machines

```
vmware-fullscreen -exit
```

Use this command to power off all virtual machines cleanly. VMware Workstation exits as soon as all the virtual machines have powered off.

Switching Among Virtual Machines and the Host

```
vmware-fullscreen -switchto "<config-file>"
vmware-fullscreen -switchto <alias>
vmware-fullscreen -switchto host
vmware-fullscreen -switchto next
```

Use this command to switch to the specified virtual machine, to the host operating system, or to the next machine (virtual machine or host) in the cycling order. A virtual machine must already be powered on before you can switch to it. When specifying a virtual machine, you can specify the path to the configuration (`.vmx`) file, or you can specify the alias if you used `-name=` when you started the virtual machine.

Checking the Status of VMware Workstation

```
vmware-fullscreen -query
```

This command tells you if VMware Workstation is already running in full screen switch mode. If it is, the response to this command also reports its process ID and window handle.

The vmware-fullscreen Log File

The `vmware-fullscreen` program writes to a log file. This log file records errors reported by `vmware-fullscreen` itself as it starts, stops and passes other commands to VMware Workstation. It is separate from the `vmware.log` file, which stores information on the running virtual machines.

The name of the `vmware-fullscreen` log file is `vmware-<username>-<pid>.log`. By default, the `vmware-fullscreen` log file is in the temp directory for the user logged on to the host computer. This location may be specified in the TEMP environment variable; by default, the location is `C:\Documents and Settings\<username>\Local Settings\Temp`.

The administrator can specify a different location for this log file by adding the following line to the VMware Workstation global configuration file (`config.ini`):

```
fullScreenSwitch.log.filename="<path>"
```

It is best to use a full path. If you use a relative path, the location is relative to the directory that is active when the `vmware-fullscreen` command is issued for the first time after the host computer reboots.

CHAPTER 14

Glossary

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.

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.

Drag and drop— With the drag and drop feature of VMware Workstation, you can move files easily between a Windows host and a Windows virtual machine. You can drag and drop individual files or entire directories.

Existing partition — A partition on a physical disk in the host machine.
See also Raw disk.

Full screen mode— A display mode in which the virtual machine's display fills the entire screen.
See also Quick switch mode.

Favorites list — A list in the left panel of the main VMware Workstation screen that shows the names of virtual machines that a user has added to the list. The Favorites list 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.

Guest operating system — An operating system that runs inside a virtual machine.
See also Host operating system.

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 machine — The physical computer on which the VMware Workstation software is installed. It hosts the VMware Workstation virtual machines.

Host operating system — An operating system that runs on the host machine.
See also Guest operating system.

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.

New Virtual Machine Wizard — A point-and-click interface for convenient, easy creation of a virtual machine configuration. To launch it, 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 raw disk file.
See also Virtual machine settings editor.

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 — 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 (see Virtual disk) or on a local hard disk. When a virtual machine is configured to use a raw disk, VMware Workstation directly accesses the local disk or partition as a raw device (not as a file on a file system). It is possible to boot a previously installed operating system on an existing partition within a virtual machine environment. The only limitation is that the existing partition must reside on a local IDE or SCSI drive.
See also Virtual 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.

Shared folder — A shared folder is a folder on the host computer — or on a network drive accessible from the host computer — that can be used by both the host computer and one or more virtual machines. It provides a simple way of sharing files between host and guest or among virtual machines. In a Windows virtual machine, shared folders appear as folders on a designated drive letter. In a Linux virtual machine, shared folders appear under a specified mount point.

Snapshot — A snapshot preserves the virtual machine just as it was when you took the snapshot — the state of the data on all the virtual machine's disks and whether the virtual machine was powered on, powered off or suspended. VMware Workstation lets you take a snapshot of a virtual machine at any time and revert to that snapshot at any time. You can take a snapshot when a virtual machine is powered on, powered off or suspended.

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.

Virtual disk — A virtual disk is a file or set of files, usually on the host file system, 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 the need

to repartition a physical disk or reboot the host.
See also Raw disk.

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, etc.) 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 by the New Virtual Machine Wizard. It is used by VMware Workstation to identify and run a specific virtual machine.

Virtual machine settings editor — A point-and-click editor used to view and modify the settings of a virtual machine. You can launch it from the **VM** menu.
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 Workstation. You can launch it from the **Edit** menu.

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 control panel and support for such features as shared folders, drag and drop in Windows guests, shrinking virtual disks, time synchronization with the host, VMware Tools scripts, and connecting and disconnecting devices while the virtual machine is running.

Index

D

S

T