VMware™ User's Manual

Workstation

Version 3.2

vmware™

VMware, Inc.

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

Please note that you will 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.

Table of Contents

1

Introduction and System Requirements

Welcome to VMware Workstation

This section contains the following:

- Host System Requirements on page 14
- Virtual Machine Specifications on page 18
- Supported Guest Operating Systems on page 21
- What's New in Version 3 on page 23
- Technical Support Resources on page 26

Thank you for choosing VMware™ Workstation, the software that increases the productivity of developers and other technical professionals by letting them run multiple operating systems in secure, transportable, high-performance virtual computers.

If you're new to VMware Workstation, this chapter is the place to start. It introduces you to some of the things you can do with VMware Workstation and guides you through installing the software and putting it to work.

If you're a veteran user of VMware products, take a few minutes to see what's new in version 3 and check out the notes on upgrading your installation.

Virtualizing Your Computing Resources

VMware products provide a virtualization layer that turns your physical computers into a pool of logical computing resources. You can then dynamically allocate those resources to any operating system or application in the way that best meets your needs. You'll be able to spend more time delivering tangible value to your business and less time installing operating systems, rebooting or reconfiguring hardware.

Run the operating systems you need — all at once

With VMware virtualization technology, you can set up completely independent installations of operating systems on a single machine. Multiple instances of Microsoft® Windows® or Linux® can run side by side in virtual machines that you create with the VMware Workstation software. Each virtual machine is equivalent to a PC with a unique network address and a full complement of hardware devices. You install and run a complete, unmodified operating system and application software, just as you would on a physical PC.

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.

Host System Requirements

What do you need to get the most out of VMware Workstation? 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
- 400MHz or faster processor (recommended; 266MHz minimum) that supports the Pentium® instruction set
  Compatible processors include
  Intel: Celeron, Pentium II, Pentium III, Pentium 4
  AMD™: K6-2, K6-III, Athlon™, Athlon MP, Athlon XP, Duron™
- Multiprocessor systems supported

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
- Recommended: 256MB; minimum: 128MB

Display

- Greater than 256-color (8-bit) display adapter required
- Linux hosts must have a video adapter supported by the XFree86 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; using a default setup, the actual disk space needs are approximately the same as those for installing and running the guest operating system and applications on a physical computer
- IDE or SCSI hard drives, 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 host-only networking plus routing software on the host operating system

Windows Host Operating Systems

- Windows .NET Web Server beta 3, Windows .NET Standard Server beta 3 and Windows .NET Enterprise Server beta 3 (experimental)
- Windows XP Professional and Windows XP Home Edition; Service Pack 1
- Windows 2000 Professional, Windows 2000 Server and Windows 2000 Advanced Server; Service Pack 2; Service Pack 3
- Windows NT® Workstation 4.0 and Windows NT Server 4.0; Service Pack 3 or higher

  Caution: Do not install VMware Workstation on a Windows NT Server 4.0 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 product is not supported. Look for newer prebuilt modules in the Download area of our Web site. Go to *www.vmware.com/download/*.

- Mandrake™ Linux 8.2 — stock 2.4.18-6mdk
- Mandrake Linux 8.1 — stock 2.4.8-26mdk, upgrade 2.4.8-34mdk
- Mandrake Linux 8.0 — stock 2.4.3-20mdk
- 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

- Red Hat Linux 6.2 — upgrade 2.2.15-2.5.0, Dell specific 2.2.14-6.1.1 (Red Hat Linux 6.2 does not support Pentium 4 CPUs)

  Caution: VMware does not support running VMware Workstation on the stock 2.2.14-5.0 kernel.
- SuSE™ Linux 8.0 — stock 2.4.18
- SuSE™ Linux Enterprise Server 7 — stock 2.4.7
- SuSE Linux 7.3 — stock 2.4.10

  Note: If you are installing VMware Workstation on a SuSE 7.1, 7.2 or 7.3 SMP host, you need to install the non-PAE-enabled kernel on the host before you begin installing VMware Workstation. For more information, see Before You Install on a SuSE Linux 7.1, 7.2, 7.3 or 8.0 Host Operating System on page 39.
- SuSE Linux 7.2 — stock 2.4.4
- SuSE Linux 7.1 — stock 2.2.18, stock 2.4.0
- SuSE Linux 7.0 — stock 2.2.16
- Turbolinux 7.0
- Turbolinux 6.0
- Caldera® OpenLinux™ 2.4 — stock 2.2.14
- Caldera OpenLinux 2.3 — stock 2.2.10
- Caldera OpenLinux 2.2 — stock 2.2.5

VMware Workstation may run on other Linux distributions; attempting to do so is recommended for expert Linux users only.

Other Linux host operating system requirements:

- Linux kernel 2.2.14-5.0 is not supported
- Standard Linux installation with `glibc` version 2 or higher
- Version 2.1.36 of the SCSI Generic (`sg.o`) driver required to use generic SCSI devices in virtual machines
- VMware Workstation requires an X server
  - XFree86-3.3.3.1 or higher release
  - XFree86 version 3.3.4 or higher server recommended

  If you are using a recent Linux distribution, it should include an appropriate X server by default. To find out what XFree86 server is running on your computer, as root, run `X -version`.

Hosts Using PAE Options Not Supported

Host operating systems that use the Physical Address Extension (PAE) processor options cannot be used to run VMware Workstation 3.2. This issue affects Linux hosts if PAE is enabled in the kernel. It affects Windows hosts if booted with the `/PAE` option.

If you are installing VMware Workstation on a SuSE Linux 7.1, 7.2 or 7.3 SMP host, you must install the non-PAE-enabled kernel before you can install the VMware software. Please complete the steps in Before You Install on a SuSE Linux 7.1, 7.2, 7.3 or 8.0 Host Operating System on page 39.

Virtual Machine Specifications

Each virtual machine created with VMware Workstation 3.2 provides a platform that includes the following devices that your guest operating system can see.

Processor

- Intel Pentium II or later, depending on host processor
- Intel MMX if available on host processor
- Single processor per virtual machine on symmetric multiprocessor systems

Chip Set

- Intel 440BX-based motherboard with NS338 SIO chip

BIOS

- PhoenixBIOS™ 4.0 Release 6

Memory

- Up to 1GB, depending on host memory
- Maximum of 1GB 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 OS

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

- Mylex® (BusLogic) BT-958 compatible host bus adapter (requires add-on driver from VMware for Windows XP and Windows .NET Server)

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 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
- Creative Labs Sound Blaster® 16, PCM sound compatible (MIDI sound, game controllers and joysticks not supported.)

Virtual Networking and File Sharing

- Nine virtual Ethernet switches (three reserved for bridged, host-only and NAT networking)

- Virtual Ethernet support includes 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 3.2 virtual machines and are officially supported. For notes on installing the most common guest operating systems, see Installing Guest Operating Systems on page 135.

Other operating systems designed for Intel-based PCs may work, as well. For a current list of supported guest operating systems, see the support section of the VMware Web site, *www.vmware.com/support/*.

Microsoft Windows

- Windows .NET Web Server beta 3, Windows .NET Standard Server beta 3 and Windows .NET Enterprise Server beta 3 (experimental)
- Windows XP Professional and Windows XP Home Edition; Service Pack 1
- Windows 2000 Professional, Windows 2000 Server and Windows 2000 Advanced Server; Service Pack 2; Service Pack 3
- Windows NT Workstation 4.0 and Windows NT Server 4.0; Service Pack 3 or higher
- Windows Me
- Windows 98 and Windows 98 SE
- Windows 95 (all OSR releases)
- Windows for Workgroups
- Windows 3.1

Microsoft MS-DOS

- MS-DOS 6

Linux

- Mandrake Linux 8.0, 8.1and 8.2
- Red Hat Linux 6.2, 7.0, 7.1, 7.2 and 7.3
- SuSE Linux 7.0, 7.1, 7.2, 7.3, SLES 7 and 8.0
- Turbolinux 6.0 and 7.0
- Caldera OpenLinux 2.x

Novell NetWare

- NetWare 6.0 (experimental)

FreeBSD

- FreeBSD 3.x, 4.0, 4.1, 4.2, 4.3, 4.4, 4.5 and 4.6

  Note: If you use SCSI virtual disks larger than 2GB with FreeBSD 3.x or 4.x (up to and including 4.3), there are known problems, and the guest operating system does not boot. To work around this issue, see Setting the Disk Geometry for a FreeBSD SCSI Virtual Disk on page 202.

Guests Using PAE Options Not Supported

Guest operating systems that use the Physical Address Extension (PAE) processor options are not supported under VMware Workstation 3.2. This issue affects Linux guest operating systems if PAE is enabled in the kernel. It affects Windows guest operating systems if booted with the `/PAE` option.

Note: At this time, we are providing experimental support for NetWare 6, which is a PAE-enabled kernel.

What's New in Version 3

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 3 extend its capabilities and make it easier to use. Here are some highlights of the many new and improved features in this release.

New in Version 3.2

Designed for Microsoft Windows Certification

VMware Workstation 3.2 for Windows has earned Microsoft's Designed for Windows certification. This certification assures users that VMware Workstation has full functionality on Windows NT, Windows 2000 and Windows XP hosts and is designed to take advantage of new Windows XP features.

New Administrative Lockout Feature

You can require a password for access to several key administrative features — creating new virtual machines, editing virtual machine configurations and editing network settings.

Additional Host and Guest Operating System Support

You can use the latest Microsoft and Linux operating systems, including:

- Microsoft® Windows® XP, Service Pack 1 beta
- Microsoft Windows 2000, Service Pack 3
- New Linux distributions, including Red Hat Linux 7.3, SuSE Linux 8.0 and Turbolinux 6.0 and 7.0

New in Versions 3.0 and 3.1

Improved Host and Guest Operating System Support

You can use recent Microsoft and Linux operating systems, including:

- Microsoft® Windows® .NET Web Server beta 3 (experimental)
- Microsoft Windows .NET Standard Server beta 3 (experimental)
- Microsoft Windows .NET Enterprise Server beta 3 (experimental)
- New Linux distributions, including Mandrake Linux 8.2, Red Hat Linux 7.2 and SuSE Linux 7.3
- FreeBSD 4.5 (guest operating system only)

- Netware 6.0 guest operating system experimental support (without VMware Tools)

Note: For the most current list of supported host and guest operating systems, visit the VMware Web site at *www.vmware.com/support/ws3/doc/*.

Improved NAT Performance and Functionality

- Faster network address translation networking
- Support for NetLogon, allowing you to log on to a Windows domain from a virtual machine so you can access file shares on physical computers in the domain
- Support for UDP and TCP port forwarding to connect to virtual machines

New Repeatable Resume Feature

Resume a virtual machine from a specific point at which you suspended it, over and over. This is useful for a classroom or QA environment, where you want to start your guest operating system with applications already running and system settings tailored to your needs; or, in the event of a catastrophic failure, to restart from the same point, instead of rebooting the virtual machine.

Experimental Support for Remote Desktop

Connect to your Windows host remotely through Windows Terminal Services and Windows XP Remote Desktop and launch virtual machines.

Full Japanese Localization on Windows Hosts

VMware Workstation for Windows hosts contains a localized graphical user interface, installer, VMware Tools, messaging and in-product Help in Japanese.

Use of Microsoft Windows Installer

On VMware Workstation for Windows hosts, take advantage of the Windows Installer to customize your Workstation installations.

Other New Features

- New serial port implementation.

  Note: The new serial port implementation deprecates the use of TTY-type virtual serial ports in a virtual machine.
- Improved disk performance on Windows 95 and Windows 98 through direct memory access (DMA).
- Simpler migration of virtual machines, which now recognize relative paths.
- Improved cursor performance.

- Easy menu access to modify bridged networking settings for a Windows host; choose **Manage Virtual Networks** on the **Settings** menu. This menu item replaces the Settings button in the Configuration Editor on the panel for a virtual machine's network adapter.

Technical Support Resources

The VMware Web Site

The latest technical support and troubleshooting notes are available on the VMware Web site at *www.vmware.com/support/*.

VMware 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*.

The following groups are devoted to discussions about VMware Workstation.
vmware.for-windowsnt.configuration
vmware.for-windowsnt.general
vmware.for-windowsnt.experimental
vmware.for-linux.configuration
vmware.for-linux.general
vmware.for-linux.experimental

The following groups are for discussions about guest operating systems.

vmware.guest.windows95
vmware.guest.windows98
vmware.guest.windowsnt
vmware.guest.windows2000
vmware.guest.windowsXP
vmware.guest.linux
vmware.guest.netware
vmware.guest.misc

You can discuss .NET Server issues in the *vmware.guest.windowsXP* forum.

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 save the log file before you launch another virtual machine. The key log file to save is the VMware log file for the affected virtual machine — on a Windows host, the `vmware.log` file in the same directory as the configuration file (`.vmx`) of the virtual machine that had problems; on a Linux host, the `<vmname>.log` or `vmware.log` file in the same directory as the configuration file (`.cfg`) of the virtual machine that had problems. Also save any core files (`core` or `vmware-core`). Provide these to VMware along with any other information that might help us to reproduce the problem.

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 .NET Server 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*.

2

Installing VMware Workstation

Installing and Uninstalling VMware Workstation 3.2

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 3.2 on a Windows Host on page 31. To install on a Linux host computer, see Installing VMware Workstation 3.2 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 43 before you begin.

Installing VMware Workstation 3.2 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 59.
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 81.
5. Install the VMware Tools package inside your virtual machine for enhanced performance. See Installing VMware Tools on page 84.
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 14.
- 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 2000 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.

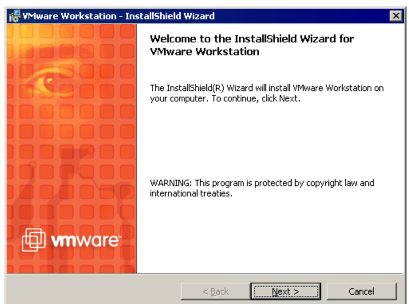
Note: On a Windows XP or Windows .NET Server host computer, you must be logged in as a local administrator (that is, not logged in to the domain) in order to install VMware Workstation.

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.

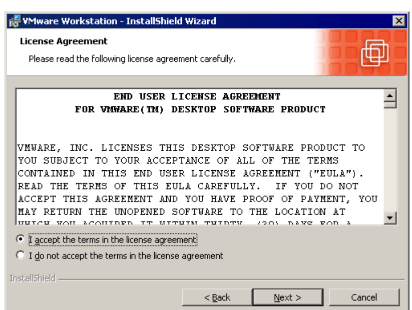
2. If you are installing from a CD, from the **Start** menu, choose **Run** and enter `D:\setup.exe`, where `D:` is the drive letter for your CD-ROM drive.

   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 (the name 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**.

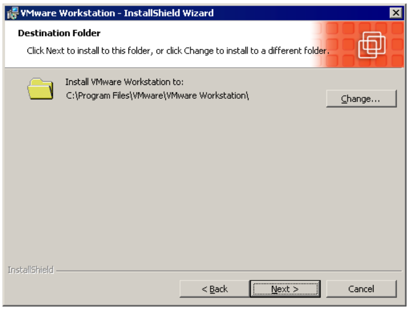


4. Acknowledge the end user license agreement (EULA). Select the **I accept the terms in the license agreement** option, then click **Next**.



Note: If you are upgrading from VMware Workstation 3.0 and did not uninstall the software, proceed to step 6.

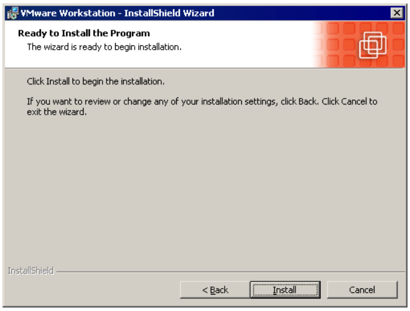
5. Choose the directory in which to install VMware Workstation. To install it in a directory other than the default, click **Change** and browse to your directory of choice. If the directory does not exist, the installer creates it for you. Click **Next**.



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

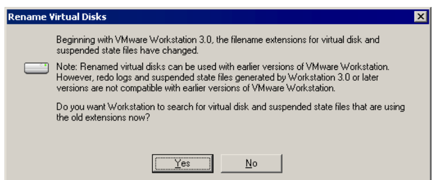
Note: Windows and the Microsoft Installer limit the length of a path to a folder to 255 characters for a path to a folder on a local drive and 240 characters for a path to a folder on a mapped or shared drive. If the path to the VMware Workstation program folder exceeds this limit, an error message appears.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

6. The installer has gathered the necessary information and is ready to begin installing the software. Click **Install**. The installer begins copying files to your host.



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.

7. If the installer detects that the CD-ROM autorun feature is enabled, you are prompted with the option to disable it. Disabling this feature prevents undesirable interactions with the virtual machines you install on this system.
8. On a Windows NT host, you may see a Digital Signature Not Found dialog box when the installer begins to install the VMware Virtual Ethernet Adapter. You can safely ignore this message. Click **Yes** to continue the installation.
9. A dialog box appears, asking if you want to rename existing virtual disks using the new `.vmdk` extension. Click **Search Disk** to search all local drives on the host computer and make this change.



One Chance to Rename Disk Files

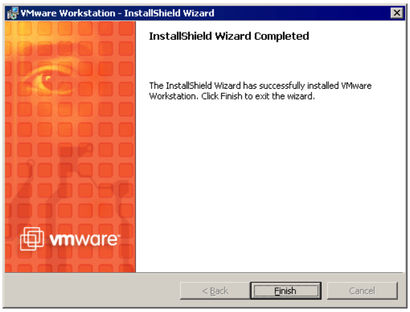
- The Rename Virtual Disks dialog box appears only once. If you click Cancel, you will not have another opportunity to update the filenames and configuration files automatically.

The 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 2.0 to Workstation 3.2.

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

Note: If you store your virtual disk files or suspended state files on a Windows XP or Windows .NET Server 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 .NET Server.

10. Click **Finish**. The VMware Workstation software is installed.



11. A prompt suggests that you reboot your PC. Reboot now to allow VMware Workstation to complete the installation correctly.

Uninstalling VMware Workstation 3.2 on a Windows Host

To uninstall VMware Workstation 3.2, use the VMware Workstation uninstaller.

1. Launch the uninstaller.
   Start > Programs > VMware > VMware Workstation Uninstallation
2. Click Yes.
3. Follow the on-screen instructions.

   Near the end of the uninstallation process, you are asked if you want to remove your VMware Workstation licenses. If you click Yes, all licenses on the host computer are permanently removed.

Installing VMware Workstation 3.2 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 chapter.
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 Configuration Wizard. See Creating a New Virtual Machine on page 59.
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 81.
5. Install the VMware Tools package inside your virtual machine for enhanced performance. See Installing VMware Tools on page 84.
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 14.
- 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

If you are installing VMware Workstation on a SuSE Linux 7.1, 7.2, 7.3 or 8.0 SMP host, please read Before You Install on a SuSE Linux 7.1, 7.2, 7.3 or 8.0 Host Operating System on page 39.

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 carry out 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:
   - To use the RPM installer, run RPM specifying the installation file.
     `rpm -Uhv VMware-<xxx>.rpm`
     (where `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, 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`
   - To use the tar installer, you may either copy a tar archive to your hard disk and install following the directions below, or 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, `/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 script.
     `./vmware-install.pl`
     Accept the default directories for binary files, library files, manual files, documentation files and init script.

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

   Note: If you use the RPM installer, you need to run this script separately from the command line. If you install from the tar archive, the installer offers to launch the configuration script for you. Answer Yes when you see the prompt.

   Use this script 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.

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 script 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, 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 280.

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, run the installation program again.
10. When done, exit from the root account.
    `exit`

Before You Install on a SuSE Linux 7.1, 7.2, 7.3 or 8.0 Host Operating System

If you are installing VMware Workstation on a SuSE Linux 7.1, 7.2, 7.3 or 8.0 host operating system running an SMP (symmetric multiprocessor) kernel, you need to install the non-PAE-enabled kernel for your SuSE Linux 7.1, 7.2, 7.3 or 8.0 SMP host before you can install the VMware software.

SuSE Linux 7.1, 7.2, 7.3 and 8.0 SMP kernels implement 64GB PAE memory and are not supported. For SuSE Linux 7.1 and 7.2 hosts, the non-PAE-enabled versions of these SMP kernels can be installed from the RPM package available on the SuSE distribution CD-ROM (`/suse/images/k_psmp.rpm`). For a SuSE Linux 7.3 or 8.0 host, you can select the non-PAE-enabled SMP kernel by running the YaST2 configuration utility.

The VMware Workstation installer contains prebuilt modules that work with the non-PAE-enabled kernels for SuSE Linux 7.1, 7.2, 7.3 and 8.0 SMP distributions.

Installing the Non-PAE-Enabled Kernel on a SuSE Linux 7.1 or 7.2 Host

1. Mount the SuSE CD-ROM containing the non-PAE-enabled kernel package.
   ```
   mount -t iso9660 /dev/cdrom /mnt/cdrom
   ```
2. Save your current kernel and, if necessary, your current `initrd`.
   ```
   cp /boot/vmlinuz /boot/vmlinuz.old
   cp /boot/initrd /boot/initrd.old
   ```
3. Uninstall the current kernel package.
   ```
   rpm -e k_smp-2.4.4-14
   ```
4. Install the new kernel package.
   ```
   rpm -Uhv /mnt/cdrom/suse/images/k_psmp.rpm
   ```
5. Create a new initial ram disk, which holds the drivers used for accessing your root file system (for example, if it resides on a SCSI disk). If your system does not need a ram disk, it won't be created.
   ```
   mk_initrd
   ```

6. Reconfigure the Linux loader (LILO).

   `lilo`

   Note: If you are using LOADLIN, you have to copy the `/boot/vmlinuz` kernel image and the `/boot/initrd` initial ram disk to your DOS partition.

7. Reboot your SuSE host operating system.

Installing the Non-PAE-Enabled Kernel on a SuSE 7.3 or 8.0 Host

1. Log in as root and run YaST2.
2. Click **System**, then **Select kernel**.
3. Select **Kernel 2.4 with SMP -- support for older processors (Pentium Classic)**. This selects the 4GB non-PAE-enabled kernel.
4. Click **Finish**, then click **Close** to exit YaST. When you reboot your host machine in the next step, the new kernel is selected and the `inetd` process automatically starts.
5. Reboot your SuSE Linux host operating system.

After you finish configuring your SuSE Linux 7.1, 7.2, 7.3 or 8.0 host operating system, you are ready to install VMware Workstation.

Uninstalling VMware Workstation 3.2 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
```

3

Upgrading VMware Workstation

Upgrading from VMware Workstation 2.0, 3.0 and 3.1

The following sections describe how to upgrade VMware Workstation from version 2.0, 3.0 and 3.1 to version 3.2 on your Linux or Windows host system and how to use existing virtual machines under VMware Workstation 3.2:

- Preparing for the Upgrade on page 45
- Upgrading on a Windows Host on page 47
- Upgrading on a Linux Host on page 53
- Upgrading from VMware Workstation 1.x or VMware Express on page 58

Preparing for the Upgrade

Before You Install VMware Workstation 3.2

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 3.2 — 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 2.0, 3.0, 3.1 or a prerelease version of VMware Workstation 3.2, 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.

Commit or Discard Changes to Disks in Undoable Mode

If you plan to use existing virtual machines that have 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.

Back Up Virtual Machines

As a precaution, back up all the files in your virtual machine directories — including the `.vmdk` or `.dsk`, `.cfg` or `.vmx` and `nvram` files — for any existing virtual machines you plan to migrate to VMware Workstation 3.2.

Virtual machines updated for full compatibility with VMware Workstation 3.2 cannot be used under VMware Workstation 2.0.

When You Remove Version 2.0 and Install Version 3.2

There is a key precaution you should take when you remove VMware Workstation 2.0 — or a prerelease version of VMware Workstation 3.2 — and install VMware Workstation 3.2.

Note: You should also take the following into consideration if you decide to uninstall version 3.0 or 3.1.

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 offers to remove licenses from your registry. If you think you may want to use the previous version of VMware Workstation again, 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 Version 2.0, 3.0 or 3.1 to 3.2

The Upgrade Process

In most cases, upgrading from version 2.0, 3.0 or 3.1 is a four-step process. If you are upgrading from Workstation 2.0 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.

1. Uninstall the version now installed on your computer.
2. Reboot your computer.
3. Install version 3.2.
4. Reboot your computer.

Removing Version 2.0

To uninstall version 2.0, 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 licence in the Windows registry.

After you reboot, follow the instructions in Installing VMware Workstation 3.2 on a Windows Host on page 31.

Removing Version 3.0 or 3.1

To uninstall version 3.0 or 3.1, 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 may safely keep your existing licence in the Windows registry.

After you reboot, follow the instructions in Installing VMware Workstation 3.2 on a Windows Host on page 31.

Upgrading on a Windows 2000 Host with Host-Only Networking

If you have set up host-only networking for VMware Workstation 2.0 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 2.0.
3. Reboot your computer.
4. Install version 3.2.
5. Reboot your computer.

Using Virtual Machines Created with Version 2.0 under Version 3.2

There are, broadly speaking, three approaches you can take to setting up virtual machines under VMware Workstation 3.2. Choose one of these approaches. There are no issues using virtual machines created under VMware Workstation 3.0 or 3.1.

- 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 59. If you set up your virtual machines in this way, you will be using the latest technology and will enjoy the best possible virtual machine performance.
- Use 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).

  Upgrade VMware Tools to the new version following the instructions for your guest operating system in Installing VMware Tools on page 84. 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. You will not have USB ports.

You will not have the new BIOS, which makes it easier to use one of the operating systems on a dual-boot host machine as a guest operating system in a virtual machine. Also, you will not have the new unified virtual video hardware, which helps simplify the installation of VMware Tools.

Note: On Windows hosts, VMware Workstation 3.2 offers to convert virtual disk `.dsk` filenames to use the new `.vmdk` extension at the time you install VMware Workstation. If you are storing virtual disk files on a Windows XP or Windows .NET Server 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 .NET Server System Restore feature. The `.vmdk` extension can be used for virtual disks under any VMware product. VMware Workstation 3.2 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 224.

- Use an existing virtual machine and upgrade the virtual hardware. This 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).

  Upgrade VMware Tools to the new version following the instructions for your guest operating system in Installing VMware Tools on page 84. You should not remove the older version of VMware Tools before installing the new version.

  Upgrade the virtual hardware so you can use USB devices in your virtual machine.

  Note: On Windows hosts, VMware Workstation 3.2 offers to convert virtual disk `.dsk` filenames to use the new `.vmdk` extension at the time you install VMware Workstation. If you are storing virtual disk files on a Windows XP or Windows .NET Server 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 .NET Server System Restore feature. The `.vmdk` extension can be used for virtual disks under any VMware product. VMware Workstation 3.2 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

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 2.0. You should make backup copies of your virtual disks before starting the upgrade.

details, see Updating Filenames for Virtual Disks Created with Earlier VMware Products on page 224.

Upgrading the Virtual Hardware in an Existing Virtual Machine

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

If you are using a Windows 95, Windows 98 or Windows Me virtual machine created under VMware Workstation 2.0 and choose to upgrade the virtual hardware, you need to take several steps to be sure the new virtual hardware is recognized properly by the guest operating system. With other guest operating systems, these special steps are not needed.

Before you upgrade the virtual hardware, make sure you have installed the latest version of VMware Tools, including the SVGA driver, then power off your virtual machine.

Take the steps listed under the name of your guest operating system.

Windows Me Guest

1. Choose **Settings** > **Upgrade Virtual Hardware**.
2. A warning message appears. It says: "This operation will cause the virtual hardware your guest operating system runs on to change…"

   Click **Yes**.
3. Click **Power On**.
4. Click **OK** to dismiss the message "A legacy SVGA driver has been detected."
5. Several Plug and Play messages appear. You can safely ignore them.
6. Log on to Windows Me. More Plug and Play messages are displayed. One refers to the VMware SVGA driver.

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

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

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

   Windows notifies you to restart your computer.

Click **Yes**.

10. The SVGA driver should be working correctly.

Windows 98 Guest

1. Choose **Settings** > **Upgrade Virtual Hardware**.
2. A warning message appears. It says: “This operation will cause the virtual hardware your guest operating system runs on to change…”

   Click **Yes**.
3. Click **Power On**.
4. Click **OK** to dismiss the message “A legacy SVGA driver has been detected.”
5. Log on to Windows 98. You see a number of Plug and Play messages. You may need to insert your Windows 98 installation CD.
6. A blue screen appears. Press any key to dismiss the blue screen.
7. Click **Reset** to restart the virtual machine (because it is not responding).
8. 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**.
9. Log on to Windows 98. The SVGA driver is not working properly.
10. From the Windows **Start** menu, choose **Settings** > **Control Panel** > **System** > **Device Manager** > **Display Adapters**.

    Manually remove the two conflicting SVGA drivers.
11. Restart Windows 98.

    A VMware SVGA II adapter is detected and Windows installs it.
12. Restart Windows 98.
13. The SVGA driver should be working correctly.

Windows 95 Guest

1. Choose **Settings** > **Upgrade Virtual Hardware**.
2. A warning message appears. It says: “This operation will cause the virtual hardware your guest operating system runs on to change…"

   Click **Yes**.
3. Click **Power On**.

4. Click **OK** to dismiss the message "A legacy SVGA driver has been detected."
5. Log on to Windows 95.

   You see a number of Plug and Play messages. Click **Cancel** for the following devices: Standard host CPU bridge, PCI bridge and PCI Universal bus.
6. 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 SVGA driver.
8. Restart Windows 95.
9. Again, you see a number of Plug and Play messages. Click **Cancel** for the following devices: Standard host CPU bridge, PCI bridge and PCI Universal bus.
10. A VMware SVGA II adapter is detected and Windows installs it.
11. Restart Windows 95.
12. Once again, you see a number of Plug and Play messages. Again, click **Cancel** for the following devices: Standard host CPU bridge, PCI bridge and PCI Universal bus.
13. The SVGA driver should be working correctly.

Check Guest Operating System Selection

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

Upgrading on a Linux Host

Removing Version 2.0, 3.0 or 3.1

If you used the tar installer to install version 2.0, 3.0 or 3.1, and you plan to use the tar installer for version 3.2, you do not need to take any special steps to uninstall the older version. Just follow the installation instructions Installing VMware Workstation 3.2 on a Linux Host on page 36.

If you used the RPM installer to install version 2.0, 3.0 or 3.1, you need to take the following steps to upgrade to version 3.2.

Note: If you are currently using version 3.0, you need to uninstall the prebuilt modules RPM package 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 2.0, uninstall it as root by running
   ```
   rpm -e VMware
   ```
   If you are running version 3.0, as root uninstall the prebuilt modules, then uninstall VMware Workstation by running
   ```
   rpm -e VMwareWorkstationKernelModules
   rpm -e VMwareWorkstation
   ```
   If you are running version 3.1, uninstall it as root by running
   ```
   rpm -e VMwareWorkstation
   ```
2. Install version 3.2 following the instructions in Installing VMware Workstation 3.2 on a Linux Host.

Using Virtual Machines Created with Version 2.0 under Version 3.2

There are, broadly speaking, three approaches you can take to setting up virtual machines under VMware Workstation 3.2. Choose one of these approaches. There are no issues using virtual machines created under VMware Workstation 3.0 or 3.1.

- Create everything new from the start. Use the Configuration 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 59. If you set up your virtual machines in this way, you will be using the latest technology and will enjoy the best possible virtual machine performance.
- Use 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).

Upgrade VMware Tools to the new version following the instructions for your guest operating system in Installing VMware Tools on page 84. 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. You will not have USB ports. You will not have the new BIOS, which makes it easier to use one of the operating systems on a dual-boot host machine as a guest operating system in a virtual machine. Also, you will not have the new unified virtual video hardware, which helps simplify the installation of VMware Tools.

Note: On Linux hosts, VMware Workstation 3.2 offers to convert virtual disk `.dsk` filenames to use the new `.vmdk` extension the first time you run a virtual machine after installing VMware Workstation. If you are storing virtual disk files on a Windows XP or Windows .NET Server computer — a file server, for example — it is especially important that you allow VMware Workstation to make this change in order to avoid conflicts with the Windows XP or Windows .NET Server System Restore feature. The `.vmdk` extension can be used for virtual disks under any VMware product. VMware Workstation 3.2 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 224.

- Use an existing virtual machine and upgrade the virtual hardware. This gives you access to new features, but the process is one-way — you cannot reverse it.

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

  Upgrade VMware Tools to the new version following the instructions for your guest operating system in Installing VMware Tools on page 84. You should not remove the older version of VMware Tools before installing the new version.

  Upgrade the virtual hardware so you can use USB devices in your virtual machine.

  Note: On Linux hosts, VMware Workstation 3.2 offers to convert virtual disk `.dsk` filenames to use the new `.vmdk` extension the first time you run a virtual machine after installing VMware Workstation. If you are storing virtual disk files on a Windows XP or Windows .NET Server computer — a file server, for example — it is especially important that you allow VMware Workstation to make this change in order to avoid conflicts with the Windows XP or Windows .NET Server

System Restore feature. The `.vmdk` extension can be used for virtual disks under any VMware product. VMware Workstation 3.2 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 224.

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 2.0. You should make backup copies of your virtual disks before starting the upgrade.

Upgrading the Virtual Hardware in an Existing Virtual Machine

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

If you are using a Windows 95, Windows 98 or Windows Me virtual machine created under VMware Workstation 2.0 and choose to upgrade the virtual hardware, you need to take several steps to be sure the new virtual hardware is recognized properly by the guest operating system. With other guest operating systems, these special steps are not needed.

Before you upgrade the virtual hardware, make sure you have installed the latest version of VMware Tools, including the SVGA driver, then power off your virtual machine.

Take the steps listed under the name of your guest operating system.

Windows Me Guest

1. Choose **Settings** > **Upgrade Virtual Hardware**.
2. A warning message appears. It says: “This operation will cause the virtual hardware your guest operating system runs on to change…”

   Click **Yes**.
3. Click **Power On**.
4. Click **OK** to dismiss the message “A legacy SVGA driver has been detected.”
5. Several Plug and Play messages appear. You can safely ignore them.
6. Log on to Windows Me. More Plug and Play messages are displayed. One refers to the VMware SVGA driver.

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

   Manually remove the two SVGA drivers.

9. Restart Windows Me.

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

   Windows notifies you to restart your computer.

   Click **Yes**.
10. The SVGA driver should be working correctly.

Windows 98 Guest

1. Choose **Settings** > **Upgrade Virtual Hardware**.
2. A warning message appears. It says: "This operation will cause the virtual hardware your guest operating system runs on to change…"

   Click **Yes**.
3. Click **Power On**.
4. Click **OK** to dismiss the message "A legacy SVGA driver has been detected."
5. Log on to Windows 98. You see a number of Plug and Play messages. You may need to insert your Windows 98 installation CD.
6. A blue screen appears. Press any key to dismiss the blue screen.
7. Click **Reset** to restart the virtual machine (because it is not responding).
8. 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**.
9. Log on to Windows 98. The SVGA driver is not working properly.
10. From the Windows **Start** menu, choose **Settings** > **Control Panel** > **System** > **Device Manager** > **Display Adapters**.

    Manually remove the two conflicting SVGA drivers.
11. Restart Windows 98.

    A VMware SVGA II adapter is detected and Windows installs it.
12. Restart Windows 98.
13. The SVGA driver should be working correctly.

Windows 95 Guest

1. Choose **Settings** > **Upgrade Virtual Hardware**.

2. A warning message appears. It says: “This operation will cause the virtual hardware your guest operating system runs on to change…"

   Click **Yes**.
3. Click **Power On**.
4. Click **OK** to dismiss the message “A legacy SVGA driver has been detected.”
5. Log on to Windows 95.

   You see a number of Plug and Play messages. Click **Cancel** for the following devices: Standard host CPU bridge, PCI bridge and PCI Universal bus.
6. 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 SVGA driver.
8. Restart Windows 95.
9. Again, you see a number of Plug and Play messages. Click **Cancel** for the following devices: Standard host CPU bridge, PCI bridge and PCI Universal bus.
10. A VMware SVGA II adapter is detected and Windows installs it.
11. Restart Windows 95.
12. Once again, you see a number of Plug and Play messages. Again, click **Cancel** for the following devices: Standard host CPU bridge, PCI bridge and PCI Universal bus.
13. The SVGA driver should be working correctly.

Check Guest Operating System Selection

If your guest operating system is Windows 2000, update the setting in the Configuration Editor (**Settings** > **Configuration Editor** > **Misc**) to reflect the specific version of Windows 2000 you are running.

Upgrading from VMware Workstation 1.x or VMware Express

If you are upgrading from VMware Workstation 1.x, uninstall version 1.x, then follow the instructions for a new installation of VMware Workstation 3.2. See Installing VMware Workstation 3.2 on a Windows Host on page 31 or Installing VMware Workstation 3.2 on a Linux Host on page 36.

Note: VMware does not recommend migrating virtual machines created under version 1.x to version 3.2. If you have virtual machines created under version 1.x and need to use them under version 3.2, you should first upgrade to VMware Workstation 2.0, run the virtual machines under version 2.0 and upgrade VMware Tools, then upgrade to VMware Workstation 3.2.

To upgrade from VMware Express to VMware Workstation, uninstall VMware Express, then follow the instructions for a new installation of VMware Workstation 3.2. See Installing VMware Workstation 3.2 on a Linux Host on page 36.

To migrate virtual machines created with VMware Express for use under VMware Workstation 3.2, follow the instructions for migrating virtual machines from VMware Workstation 2.0 to Workstation 3.2. See Upgrading on a Linux Host on page 53.

4

Creating a New Virtual Machine

Preparing to Run a Virtual Machine

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

- Setting up a New Virtual Machine on a Windows Host on page 61
    - What's in a Virtual Machine on a Windows Host? on page 61
    - Simple Steps to a New Virtual Machine on a Windows Host on page 62
- Setting up a New Virtual Machine on a Linux Host on page 69
    - What's in a Virtual Machine on a Linux Host? on page 69
    - Simple Steps to a New Virtual Machine on a Linux Host on page 70
- Installing a Guest Operating System and VMware Tools on page 81
    - Installing Windows Me as a Guest Operating System on page 82
    - Installing VMware Tools on page 84
    - VMware Tools Configuration Options on page 92

Setting up a New Virtual Machine on a Windows Host

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 Configuration Editor (**Settings** > **Configuration Editor**) if you need to make any changes to your virtual machine's setup.

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

What's in a Virtual Machine on a Windows Host?

The virtual machine typically is stored on the host computer in a set of files, all of which are in a folder 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 Configuration Editor.
- `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 comprises one or more `.vmdk` files. The larger the size of the virtual disk, the more `.vmdk` files. As data is added to a virtual disk, the `.vmdk` files grow in size, to a maximum of 2GB each. 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 disk is 2GB or larger, VMware Workstation creates multiple `.vmdk` files.

  If the virtual machine is connected directly to a physical disk, rather than using a virtual disk, there is no `.vmdk` file. Instead, a `.raw` 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.
- `vmware.log` — the file that keeps a log of key VMware Workstation activity. This can be useful in troubleshooting if you encounter problems. This file is stored in the folder that holds the configuration (`.vmx`) file of the virtual machine.

- `<vmname>.vmdk.REDO` — the redo-log file, created automatically when a virtual machine is used in undoable or nonpersistent mode. This file stores changes made to the virtual disk while the virtual machine is running.
- `<vmname>.vmss` — the suspended state file, which stores the state of a suspended virtual machine.

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

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 on a Windows Host

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

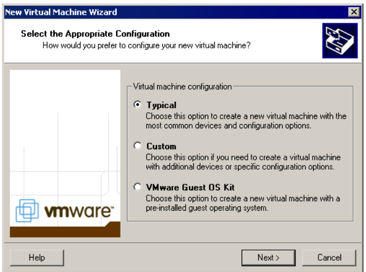
Follow these steps to create a virtual machine using a virtual disk.

1. Start VMware Workstation. If you allowed the installer to place a VMware Workstation icon on your desktop, double-click the icon. Otherwise, use the Start menu (Start > Programs > VMware > VMware Workstation).
2. If this is the first time you have launched VMware Workstation, you are prompted to enter your 20-character serial number. This number is on the registration card in your package. Enter your serial number and click OK.

   The serial number you enter is saved in your license file 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 software on the Web > Register Now! and Help > VMware software on the Web > Request Support). This allows us to direct you to the correct Web page for registration and support for your product.
3. Start the New Virtual Machine Wizard.

   When you start VMware Workstation, you can open an existing virtual machine or create a new one. Click New Virtual Machine to begin creating your virtual machine.
4. 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.

5. 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
- The network connection type

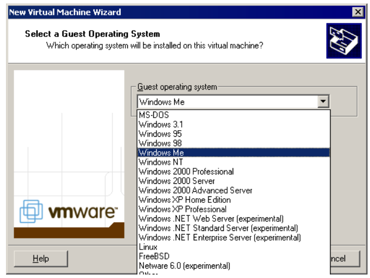
If you select **Custom**, you also can specify how to set up your disk — create a new virtual disk, use an existing virtual disk or use a physical disk — and make the settings needed for the type of disk you select.

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
- Use a physical disk rather than a virtual disk (for expert users)

Select **VMware Guest OS Kit** if you have a Guest OS Kit and want to use it to create a preconfigured virtual machine using a virtual disk. If you select VMware Guest OS Kit, the wizard asks you to specify the drive where you have placed the Guest OS Kit CD-ROM. When you click **Finish**, it launches the Guest OS Kit installation program. For more information on VMware Guest OS Kits, see *www.vmware.com/products/guestoskits/*.

6. Select a guest operating system.

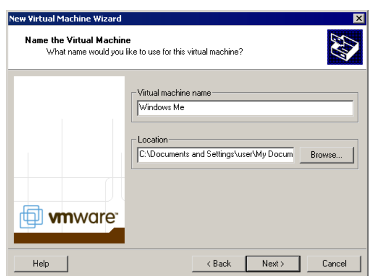


This screen asks which operating system to install in the virtual machine. The New Virtual Machine Wizard uses this information to select appropriate default values, such as the amount of disk space needed. The wizard also uses this information when naming associated virtual machine files.

If the operating system you are using is not listed, select **Other**.

The remaining steps assume you plan to install a Windows Me guest operating system. You can find detailed installation notes for this and other guest operating systems in Installing Guest Operating Systems on page 135.

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



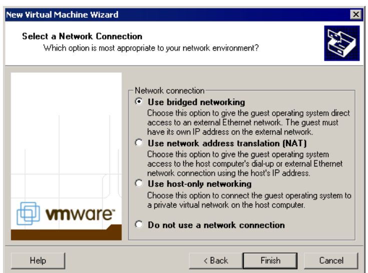
The name specified here appears in the Virtual Machine Name list on VMware Workstation's opening screen. It is also used as the name of the folder where the files associated with this virtual machine are stored.

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. On Windows 2000, Windows XP and Windows .NET Server, the default folder is C:\Documents and Settings\<username>\My Documents\My Virtual Machines\Windows Me. On Windows NT, the default folder is

C:\WINNT\Profiles\<username>\Personal\My Virtual Machines\Windows Me.

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 others 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 134.

8. 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**.

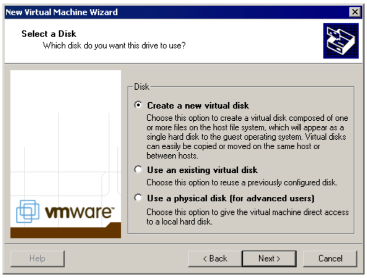
If you do not have a separate IP address for your virtual machine but you want to be able to connect to the Internet, select **Use network address translation (NAT)**. NAT is useful if you have a wireless NIC on your host (as bridged networking is not supported on wireless NICs) and allows for the sharing of files between the virtual machine and the host operating system.

For more details about VMware Workstation networking options, see Networking on page 273.

9. 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 for configuring a disk for your virtual machine.

10. Select the disk type.



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. 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.

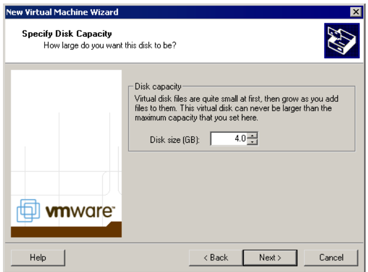
To use an existing operating system on a physical hard disk (a "raw" disk), read Configuring a Dual-Boot Computer for Use with a Virtual Machine on page 237. To install your guest operating system directly on an existing IDE disk partition, read the reference note Installing an Operating System onto a Raw Partition from a Virtual Machine on page 265.

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

Caution: If you are using a Windows .NET Server, Windows XP or Windows 2000 host, see Do Not Use Windows 2000, Windows XP and Windows .NET Server Dynamic Disks as Raw Disks on page 259.

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 Configuration 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 for Linux on page 260.

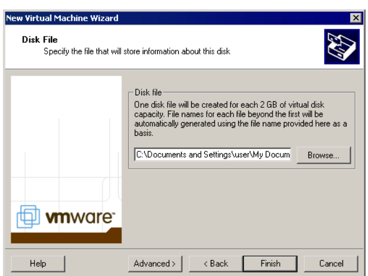
11. Specify the size of the virtual disk.



Enter the size of the virtual disk that you wish to create. Use the default of 4GB or change the setting. The maximum size is 128GB for an IDE virtual disk or 256GB for a SCSI virtual disk. When you specify the size of the virtual disk, that amount of disk space is not immediately occupied by the virtual disk files. The virtual disk files grow as needed when applications and files are added to it.

Note: If this setting is larger than the capacity of the host machine's hard disk, a warning message appears. You can ignore this message for now, as you can move this virtual machine to a drive that can hold it at a later time.

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

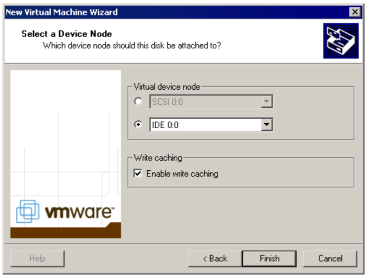


If a SCSI virtual disk is created by default and you want to use a virtual IDE disk instead, or if you want to specify which device node should be used by your SCSI or IDE virtual disk, click **Advanced**.

Make the Virtual Disk Big Enough

- The virtual disk should be large enough to hold the guest operating system and all of the software that you intend to install, with room for data and growth.
- You cannot change the virtual disk's maximum capacity later.
- You can install additional virtual disks using the Configuration Editor
- For example, you need about 500MB of actual free space on the file system containing the virtual disk to install Windows Me and popular applications such as Microsoft Office inside the virtual machine. You can set up a single virtual disk to hold these files. Or you can split them up — installing the operating system on the first virtual disk and using a second virtual disk for applications or data files.

13. Click **Finish** and the wizard sets up the files needed for your virtual machine.



Setting up a New Virtual Machine on a Linux Host

The Configuration 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 Configuration Editor (**Settings** > **Configuration Editor**) if you need to make any changes to your virtual machine's setup.

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

What's in a Virtual Machine on a Linux Host?

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>.cfg` — the configuration file, which stores settings chosen in the Configuration Wizard or Configuration Editor.
- `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 comprises one or more `.vmdk` files. The larger the size of the virtual disk, the more `.vmdk` files. As data is added to a virtual disk, the `.vmdk` files grow in size, to a maximum of 2GB each. If the virtual disk is 2GB or larger, VMware Workstation creates multiple `.vmdk` files.

  If the virtual machine is connected directly to a physical disk, rather than using a virtual disk, there is no `.vmdk` file. Instead, a `.raw` 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 can be useful in troubleshooting if you encounter problems. This file is stored in the directory that holds the configuration (`.cfg`) file of the virtual machine.
- `<vmname>.vmdk.REDO` — the redo-log file, created automatically when a virtual machine is used in undoable or nonpersistent mode. This file stores changes made to the virtual disk while the virtual machine is running.

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

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

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

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

Before you begin configuring your virtual machine, 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).

Simple Steps to a New Virtual Machine on a Linux Host

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

1. In a terminal window, launch VMware Workstation.

   ```
   vmware &
   ```

2. If this is the first time you have launched VMware Workstation, you are prompted to enter your 20-character serial number. This number is on the registration card in your package. Enter your serial number and click **OK**.

   The serial number is saved in your license file 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 software on the Web** > **Register Now!** and **Help** > **VMware software on the Web** > **Request Support**). This allows us to direct you to the correct Web page for registration and support for your product.

3. 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.

   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 to Workstation 3.2.

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

Note: If you store your virtual disk files or suspended state files on a Windows XP or Windows .NET Server 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 .NET Server.

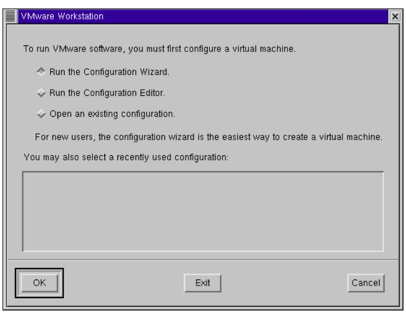
4. Start the Configuration Wizard.

   When you start VMware Workstation, the startup screen has three options:

   - Run the Configuration Wizard.
   - Run the Configuration Editor.
   - Open an existing configuration.

   It also allows you to select a recently used configuration from a list.

   The default selection is **Run the Configuration Wizard**.



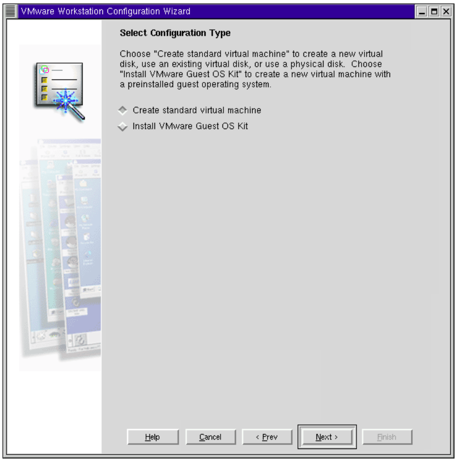
5. To start the Configuration Wizard, click **OK**. You can also start the Configuration Wizard from the **File** menu (select **File** > **Wizard**).

   The Configuration 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.

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.

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



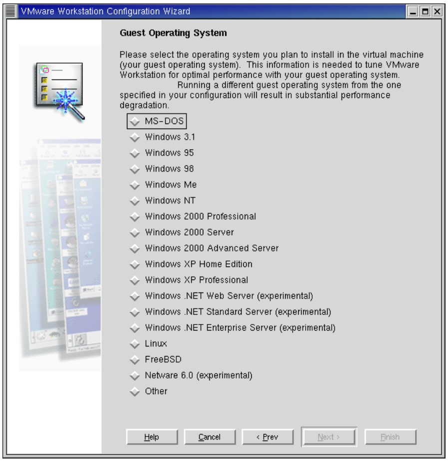
If you select **Create standard virtual machine**, the wizard prompts you to specify or accept defaults for

- The name of the guest operating system
- The path to the directory for the guest operating system and a display name for the virtual machine
- The disk type setting
- Whether to install a new virtual disk, use an existing virtual disk or use a physical disk drive
- The size of the virtual disk

Select **Install VMware Guest OS Kit** if you have a Guest OS Kit and want to use it to create a preconfigured virtual machine using a virtual disk. If you select Install VMware Guest OS Kit, the wizard asks you to specify the path to the installer file on the Guest OS Kit CD-ROM. When you click **Finish**, it launches the Guest OS Kit installation program. For more information on VMware Guest OS Kits, see *www.vmware.com/products/guestoskits/*.

The Finish button is not available initially. When there is enough information for the Configuration Wizard to finish the configuration, this button becomes available. Click **Finish** to have the Configuration Wizard enter default values for the remaining options. This is the fastest way to configure your virtual machine.

7. Select a guest operating system.

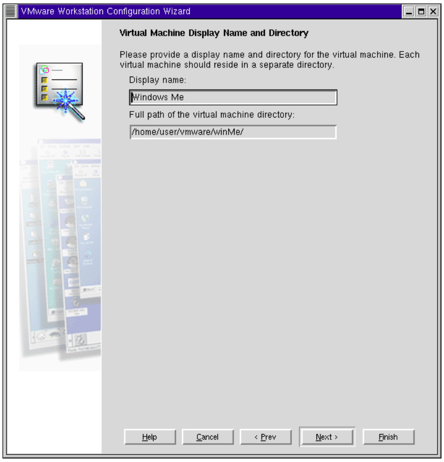


This screen asks which operating system to install in the virtual machine. The Configuration Wizard uses this information to select appropriate default values, such as the amount of disk space needed. The wizard also uses this information when naming associated virtual machine files.

If the operating system you are using is not listed, select **Other** and enter the name of the operating system.

The remaining steps assume you plan to install a Windows Me guest operating system. You can find detailed installation notes for this and other guest operating systems in Installing Guest Operating Systems on page 135.

8. Select a directory and display name for the virtual machine.

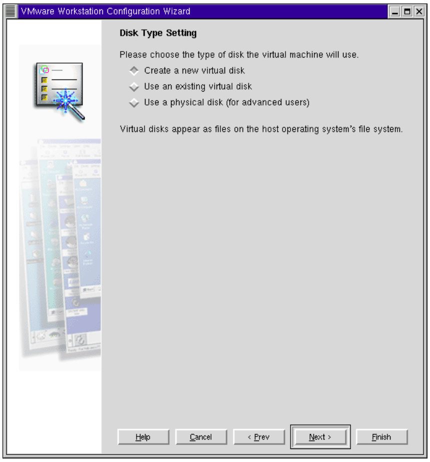


Each virtual machine should have its own directory. All associated files, such as the configuration file and the disk file, are placed in this directory.

The default location is `<homedir>/vmware/winME`, where `<homedir>` is the home directory of the user who is currently logged on. If others 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 134.

Enter a display name for the virtual machine or accept the default. In this case, the default is Windows Millennium.

9. Select the disk type.



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. 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.

To use an existing virtual disk with this virtual machine, select **Use an existing virtual disk**.

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 237. 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 265.

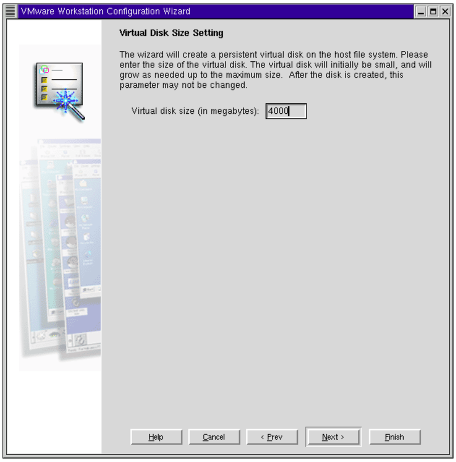
Caution: Raw disk configurations are recommended only for expert users.

To install the guest operating system on a raw IDE disk, select **Use a physical disk**. To use a raw SCSI disk, add it to the virtual machine later with the Configuration 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 for Linux on page 260.

Make the Virtual Disk Big Enough

- The virtual disk should be large enough to hold the guest operating system and all of the software that you intend to install, with room for data and growth.
- You cannot change the virtual disk's maximum capacity later.
- You can install additional virtual disks using the Configuration Editor
- For example, you need about 500MB of actual free space on the file system containing the virtual disk to install Windows Me and popular applications such as Microsoft Office inside the virtual machine. You can set up a single virtual disk to hold these files. Or you can split them up — installing the operating system on the first virtual disk and using a second virtual disk for applications or data files.

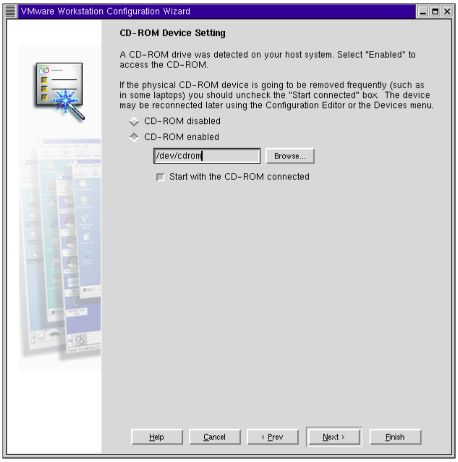
10. Select the size of the virtual disk.



Enter the size of the virtual disk that you wish to create. Use the default of 4000 (megabytes, or 4GB) or change the setting. The maximum size is 128GB for an IDE virtual disk or 256GB for a SCSI virtual disk. When you specify the size of the virtual disk, that amount of disk space is not immediately occupied by the virtual disk file. The virtual disk file grows as needed when applications and files are added to it.

Note: If this setting is larger than the capacity of the host machine's hard disk, a warning message appears. You can ignore this message for now, as you can move this virtual machine to a drive that can hold it at a later time.

11. Enable the CD-ROM drive.

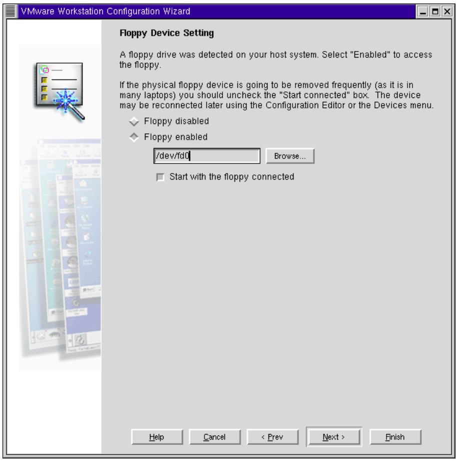


Most operating systems require the use of a CD-ROM for installation.

Select **CD-ROM enabled**. To enter the path to the CD-ROM drive, Click **Browse** or type the path to the CD-ROM drive. For example, `/dev/cdrom`.

If you wish, you can disable access to the CD-ROM drive later from the **Devices** menu when your virtual machine is running.

12. Enable the floppy disk drive.

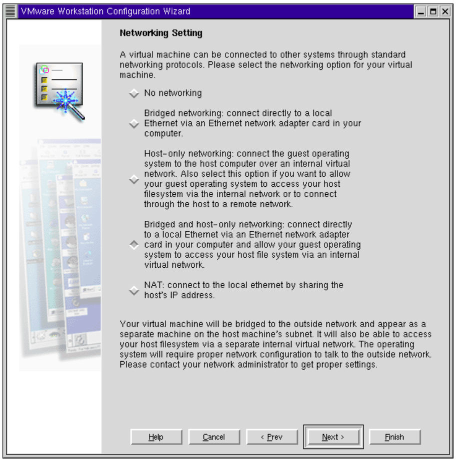


Select the **Floppy enabled** option. To enter the path to the floppy drive, click Browse or type the path to the physical floppy drive (for example, type `/dev/fd0`).

Some operating systems may require the use of a floppy drive during installation.

If you wish, you can disable access to the floppy drive later using the Configuration Editor (**Settings** > **Configuration Editor**) or from the **Devices** menu when your virtual machine is running.

13. Configure the networking capabilities of the virtual machine.



To enable your virtual machine to use an existing Ethernet connection on your host computer, select **Bridged networking**.

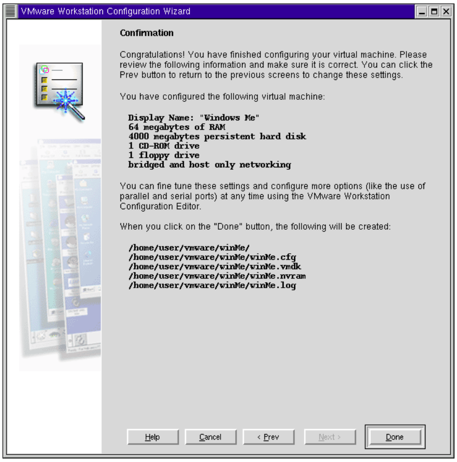
To enable your virtual machine to use a virtual network limited to the host and the virtual machines running on the host, select **Host-only networking**.

To enable your virtual machine to use both an existing Ethernet connection on your host computer and also a virtual network limited to the host and the virtual machines running on the host, select **Bridged and host-only networking**. This allows for the sharing of files between the virtual machine and the host operating system.

To give the virtual machine access to the host computer's dial-up or external network connection using the host's IP address, select **NAT**. NAT is useful if you have a wireless NIC on your host (as bridged networking is not supported on wireless NICs) and allows for the sharing of files between the virtual machine and the host operating system.

For more details about VMware Workstation networking options, see Networking on page 273.

14. Review and finish the configuration.



This screen presents all the options you selected. Review it for accuracy and click **Done** to complete the virtual machine configuration.

Installing a Guest Operating System and VMware Tools

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.
3. Power on your virtual machine — click the **Power On** button.
4. Follow the instructions provided by the operating system vendor.

The next section provides notes on installing a Windows Me 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 Installing Guest Operating Systems on page 135.

Installing Windows Me as a Guest Operating System

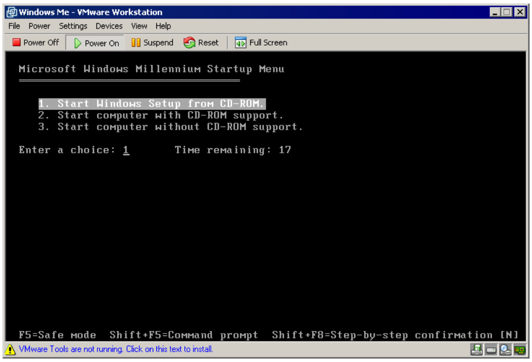
You can install Windows Me in a virtual machine using the standard Windows Me CD.

Note: Some Microsoft Windows Me OEM disks included with new computers are customized for those computers and include device drivers and other utilities specific to the system hardware. Even if you can install this Windows Me operating system on your physical computer, you may not be able to install it in a VMware Workstation virtual machine. You may need to purchase a new copy of Windows to install in a virtual machine.

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 (on Windows hosts) or Configuration Wizard (on Linux hosts).

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like the Windows Me Setup program to install networking services, be sure that a virtual Ethernet adapter is installed in the virtual machine's configuration. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Windows Me CD in the CD-ROM drive.
3. Power on the virtual machine to start installing Windows Me.
4. Choose to boot from CD-ROM, then select **Start Windows Me Setup from CD-ROM**. The setup program runs FDISK and reboots.



5. Once again, choose to boot from CD-ROM, then select **Start Windows Me Setup from CD-ROM**. The setup program continues installing Windows Me.
6. Follow the Windows Me installation steps as you would for a physical computer.

Installing VMware Tools

Don't Forget VMware Tools

- It is very important that you install VMware Tools in the guest operating system. If you do not install VMware Tools, the graphics environment within the virtual machine is limited to VGA mode graphics (640x480, 16 color).
- With the VMware Tools SVGA driver installed, Workstation supports up to 32-bit displays and high display resolution, with significantly faster overall graphics performance.
- Other tools in the package support time synchronization between host and guest, automatic grab and release of the mouse cursor, copying and pasting between guest and host, and improved mouse performance in some guest operating systems.

The installers for VMware Tools for Windows, Linux and FreeBSD 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 .NET Server guest operating systems.

Note: VMware Tools is not included in NetWare 6 virtual machines. For more information, see *www.vmware.com/download/netware_tools.html*.

When you choose **Settings** > **VMware Tools Install** from the VMware Workstation menu bar, 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 begins the installation process. (If you decide not to proceed with the installation, choose **Settings** > **Cancel VMware Tools Install** to return your virtual machine's CD-ROM drive to its original configuration.)

VMware Tools for Windows Guests

The details of how you install VMware Tools depend on the version of Windows you are running. The steps that follow show how to install VMware Tools in a Windows Me 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 for Windows, 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 115. For information about generic SCSI, see Connecting to a Generic SCSI Device on page 379.

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.

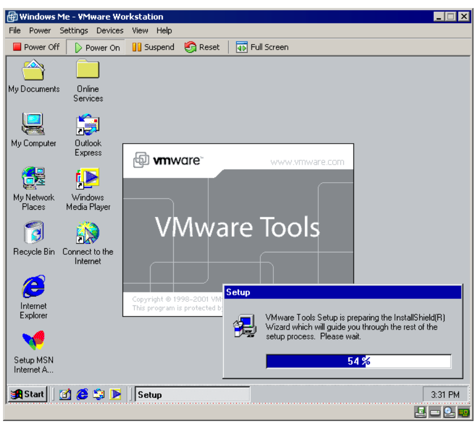
   Choose **Settings** > **VMware Tools Install**.

The remaining steps take place inside the virtual machine.

3. If you have auto-run 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 .NET Server , 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 before you can use the new driver.

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

If you are migrating a VMware Workstation 2.0 disk to VMware Workstation 3.2 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 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 2.0, 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. This brings up the Select Device dialog box.
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 **Settings** > **VMware Tools Install**.

The remaining steps take place inside the virtual machine.

3. As root, open a terminal, mount the VMware Tools virtual CD-ROM image, copy its contents to `/tmp`, then unmount it.

   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 -t iso9660 /dev/cdrom /mnt
cp /mnt/vmware-linux-tools.tar.gz /tmp
umount /dev/cdrom
```

4. Untar the VMware Tools tar file in `/tmp`, and install it.

```
cd /tmp
tar zxf vmware-linux-tools.tar.gz
cd vmware-linux-tools
./install.pl
```

5. Start X and your graphical environment if they are not started yet.
6. In an X terminal, launch the VMware Tools background application.

```
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`).

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 the desktop environment you are running. 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 (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.

VMware Tools for FreeBSD Guests

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

   Choose Settings > VMware Tools Install.

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

3. As root, open a terminal, mount the VMware Tools virtual CD-ROM image, copy its contents to `/tmp`, then unmount it.

   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
   cp /cdrom/vmware-freebsd-tools.tar.gz /tmp
   umount /cdrom
   ```

4. Untar the VMware Tools tar file in `/tmp`, and install it.

   ```
   cd /tmp
   tar zxf vmware-freebsd-tools.tar.gz
   cd vmware-freebsd-tools
   ./install.pl
   ```

5. Start X and your graphical environment if they are not started yet.
6. In an X terminal, launch the VMware Tools background application.

   ```
   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`).

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, complete 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 install 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 **Settings** > **VMware Tools Install**.

   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

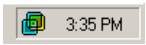
   `LOAD CD9660.NSS`
4. When the driver finishes loading you can begin installing VMware Tools. In the system console, type

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

   `restart server`

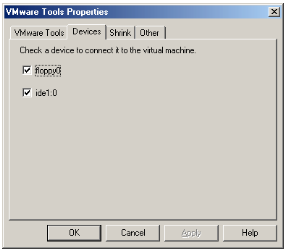
VMware Tools Configuration Options

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

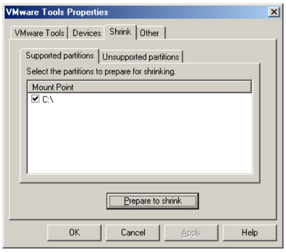


To open the VMware Tools control panel, double-click the **VMware Tools** icon in the system tray.

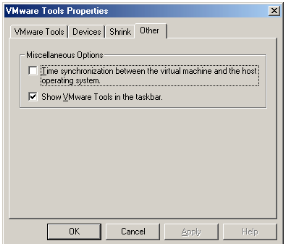
If the VMware Tools icon is not displayed in the system tray, go to **Start** > **Settings** > **Control Panel**.



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



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



The **Other** tab shows the **Miscellaneous Options**.

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

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

- Show VMware Tools in the taskbar

5

Running VMware Workstation

A Quick Guide to Running VMware Workstation

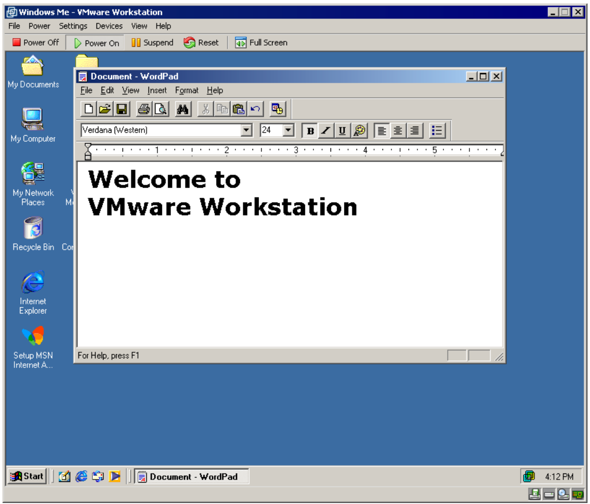
After you have installed VMware Workstation, a guest operating system and VMware Tools, how do you run your virtual machine? The following sections give you highlights of the most common tasks.

The quick reference card, included in your VMware Workstation package, provides similar information in an easy-to-use format.

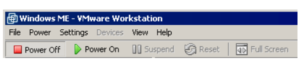
For purposes of illustration, the examples in these sections use a Windows Me guest operating system. Some commands used in the illustrations will be different for other guest operating systems.

Overview of the VMware Workstation Window

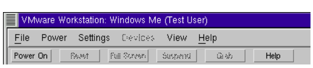
Think of your VMware Workstation virtual machine as a separate computer that runs in a window on your physical computer's desktop.



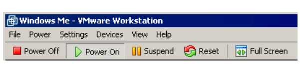
Instead of using physical buttons to turn this computer on and off, you use buttons in the toolbar at the top of the VMware Workstation window.



Toolbar when virtual machine is powered off (Windows host)

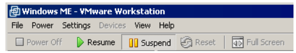


Toolbar when virtual machine is powered off (Linux host)

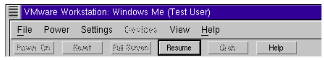


Toolbar when virtual machine is powered on (Windows host)

Toolbar when virtual machine is powered on (Linux host)



Toolbar when virtual machine is suspended (Windows host)



Toolbar when virtual machine is suspended (Linux host)

On a Windows host, there are separate Power Off and Power On buttons. When you suspend a virtual machine, the Power On button becomes a Resume button. On a Linux host, the power button is labeled Power On or Power Off, depending on whether your virtual machine is running or not.

On a Windows host, an alert appears 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. You see a small icon and a note you can click to begin installing VMware Tools. This gives you a quick way to launch the VMware Tools installer. It is especially useful immediately after you install the guest operating system in a new virtual machine.

On a Linux host, a note in the bottom bar of the VMware Workstation window alerts you 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 **Settings** > **VMware Tools Install…**.

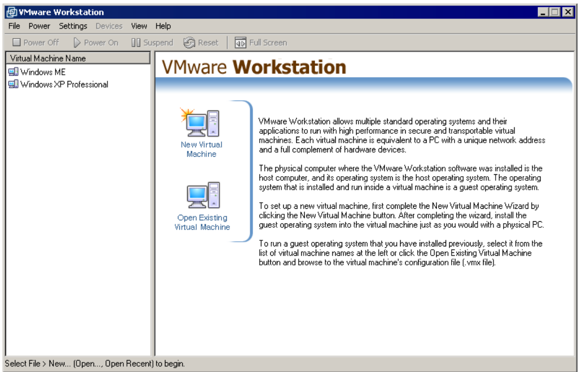
Note: Your guest operating system must be completely installed and running when you install VMware Tools.

For details, see Installing VMware Tools on page 84.

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 virtual machine list at the left of the opening screen, then click **Power On**.

   If the virtual machine you want to use is not shown there, click the **Open Existing Virtual Machine** icon and browse to the `.vmx` file for the virtual machine you want to use. That virtual machine will be added to the virtual machine list so you can open it easily the next time you want to use it.

   Note: By default, VMware Workstation 3.2 stores virtual machines in the `My Documents` folder of the user who is logged on when the virtual machine is created. On Windows .NET Server, 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>`. Earlier versions of VMware Workstation stored virtual machines in `C:\Program Files\VMware\VMs\<guestOSname>` by default.

3. Click the **Power On** button to start the virtual machine.

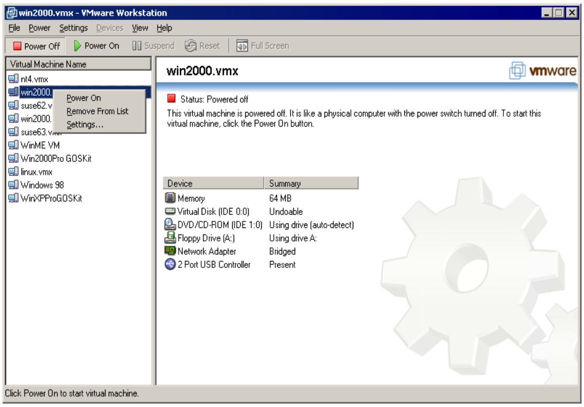
4. Click anywhere inside the VMware Workstation window to give the virtual machine control of your mouse and keyboard.

5. If you need to log on, type in your name and password just as you would on a physical computer.

Removing a Name from the Virtual Machine Name List

You can remove the name of a virtual machine from the list in the VMware Workstation window 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 by opening it, as described above.

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

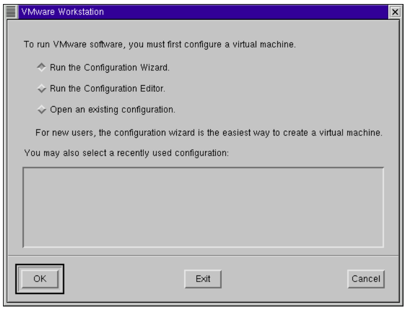


1. Right-click a name in the list once to select it.
2. After a brief pause, right-click the name again to pop up a context menu.
3. Choose **Remove From List** to remove the selected virtual machine's name.

   You may also choose **Power On** to power on the selected virtual machine or **Settings…** to modify settings for the selected virtual machine in the Configuration Editor.

Starting a Virtual Machine on a Linux Host

1. Open a terminal window, type `vmware &` and press Enter.



2. If the configuration file for the virtual machine you want to use is in the recently used configurations list, select the listing, then click **OK**.

   If not, select the **Open an existing configuration** radio button, then click **OK**. Browse to your virtual machine's directory. Select the `.cfg` file, then click **OK**.

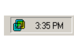
   Note: By default, VMware Workstation 3.2 stores virtual machines in <homedir>/vmware/<guestOSname>, where <homedir> is the home directory of the user who is logged on when the virtual machine is created.

3. Click the **Power On** button to start the virtual machine.
4. Click anywhere inside the VMware Workstation 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 (**Start** > **Settings** > **Control Panel**) to change settings for VMware Tools. You can also reactivate the system tray icon. On the **Other** tab, check the **Show VMware Tools in the Taskbar** check box.

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.

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.

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.

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

Installing New Software Inside the Virtual Machine

Installing new software in a VMware Workstation virtual machine is just like installing it on a physical computer.

1. Be sure you have started the virtual machine and, if necessary, logged on. Check the **Devices** menu 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

When VMware Tools is running, you can cut or copy then 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 — use the **Settings** menu.

On a Windows host, choose **Settings** > **Preferences**. On the **Input** tab, clear the **Enable copy and paste to and from virtual machine** check box.

On a Linux host, choose **Settings** > **Input Preferences**. On the cascading menu, check to see whether there is an activated icon next to **Allow copy and paste to and from virtual machine**. If there is, click **Allow copy and paste to and from virtual machine** to turn off the feature.

Sharing Files Between Guest and Host Operating Systems

To share files between a host computer and a virtual machine or between two virtual machines, you use the networking features of VMware Workstation. If you know how to share files between two physical computers on a network, you already know how to share files with a virtual machine.

This section describes four scenarios for sharing files between two systems, either a host computer and a virtual machine or two virtual machines, where

- Both systems run Windows operating systems, using Windows file sharing
- You are connecting from a Linux system to a Windows system, using `smbmount`

- You are connecting from a Windows system to a Linux system, using Samba
- Both systems run Linux operating systems, using NFS, FTP and Telnet

You can apply the same principles to share files between virtual machines. Configuration for FreeBSD guests is similar to that for Linux guests.

The following scenarios assume you have set up your virtual machine using NAT networking. Besides giving the virtual machine a direct connection to the host computer's network, NAT networking sets up a virtual network adapter on the host computer. You can use this adapter, which connects to a virtual switch identified as `vmnet8`, to communicate between host and virtual machine. You can also connect two or more virtual machines using `vmnet8`. For details on NAT networking, see Network Address Translation (NAT) on page 279.

In all cases, the user name you used to log in to the system from which you are connecting must be a user on the system to which you want to connect.

Sharing Files Between Two Windows Systems

To share files between two Windows systems (where one machine is a host and the other is a virtual machine, or both are virtual machines), be sure the file and printer sharing service is installed for both operating systems and the folders you want to share are marked as shared. Then you can browse from one system to the shared folder or folders on the other system.

Sharing Files by Connecting to a Windows System from a Linux System

To share files on a Windows system with a Linux system (by connecting to a Windows host from a Linux guest or connecting to a Windows guest from a Linux host), you can mark a folder as shared on the Windows system, then use the `smbmount` utility in the Linux system to mount the shared folder. For example, if you want to share the folder `C:\docs` on a Windows 2000 system called `win2k` with a Linux system at `/mnt/docs`, follow the steps below. You may want to set up a shell script to run these commands.

1. Set up the folder or folders to share on the Windows system.
2. Create a user account on the Windows system for the Linux system user name that you are using to connect to the Windows system.

   Otherwise, if you know the user name and password for a user account that can access the Windows system, you can specify that account on the command line.
3. From your Linux system, log in as root.

   ```
   su -
   ```

4. Add the Windows system's host name and IP address to the `hosts` file, if the system cannot be found by name.
5. Mount the Windows share on your Linux system. Enter the following command all on one line.

   ```
   mount -t smbfs -o username=<Windows system user
   account>,password=<password> //win2k/docs /mnt/docs
   ```

   (Substitute the appropriate host name, share and mount point for your systems.)

Note: If you do not want to expose this password on the command line or in a script, leave out that option and provide the password when prompted after you run the command.

Now you are connected to the shared folder on the Windows system from your Linux system and can begin to share files between the two.

Sharing Files by Connecting to a Linux System from a Windows System

To share files on a Linux system with a Windows system (by connecting to a Linux host from a Windows guest or connecting to a Linux guest from a Windows host), you can run Samba on the Linux system and browse shared directories in the Linux file system from Network Neighborhood in the Windows system.

You need to modify Samba on the Linux host operating system so it recognizes the `vmnet8` switch, otherwise you cannot access the Linux file system. You need to do this even if you installed host-only networking (as Samba is installed when you install host-only networking with VMware Workstation).

Connecting to a Linux Host from a Windows Guest

If you want to share the directory `/home/user/shared`, for example, on a Linux host operating system with a Windows guest operating system, follow these steps:

1. On the Linux host operating system, copy the `smb.conf` file to a file called something like `smb.conf.orig`.

   ```
   cd /etc/vmware/vmnet1/smb
   cp smb.conf smb.conf.orig
   ```

2. Modify Samba on the Linux host system. Edit the following lines in `/etc/vmware/vmnet1/smb/smb.conf`.

   A. Comment out the line starting with `interfaces=<IP addresses>`.

   B. Below this line, add `interfaces=vmnet1 vmnet8`.

   C. Provide a network workgroup name. Set `workgroup=<name>`.

D. If you do not want to use the standard DNS name for the Linux system, set `netbiosname=<Linux system name>`.

E. You can leave `security=user`, unless you cannot connect, in which case use `security=share`.

F. Set `encrypt passwords=yes`.

G. In the `[global]` section, define a different shared memory access key. Add this line:
`sysv shm key=/dev/vmnet8`

H. For better performance, at this line:
`socket options = TCP_NODELAY`
edit the line to state:
`socket options = TCP_NODELAY SO_RCVBUF=8192 SO_SNDBUF=8192`

Note: This setting must be entered on one line.

I. To create the share, add the following:

```
[SHARE_NAME]
/home/user/shared
public = no
writable = yes
printable = no
```
(since you want to share files, not a printer)

J. Save this file and create a backup copy to protect these changes when you upgrade VMware Workstation.

3. Restart the Samba services to load the new settings.

If VMware Workstation is running on the Linux host system, suspend or shut down all running virtual machines and close all VMware Workstation windows.

On the Linux host operating system, at a command prompt, type

```
/etc/init.d/vmware restart
```

On some Linux distributions, the command is

```
/etc/rc.d/init.d/vmware restart
```

Start VMware Workstation and run the Windows guest operating system from which you want to connect to the Linux host. The user ID you use to log in to the Windows guest must be in the Linux host's `smbpasswd` file. If you use the same user name and password to log in to the guest as you do on the Linux host, then you are not prompted to log in when you browse the Linux host.

If you are connecting to the Linux system from a Windows Me, Windows 98 or Windows 95 guest operating system, NetBEUI must be installed in the guest operating system before you can browse the file system. If you need to install NetBEUI, you may need your Windows installation CD-ROM.

When the system restarts, the Samba service does not appear in the list of services starting up, but it does start, unless an error appears.

Connecting to a Linux Guest from a Windows Host

To share the directory `/home/user/shared`, for example, on a Linux guest operating system with a Windows host operating system, follow these steps:

1. On the Linux guest operating system, copy the `smb.conf` file to a file called something like `smb.conf.orig`.
   `cp /etc/smb.conf /etc/smb.conf.orig`
2. Modify Samba on the Linux system to share the directory. To create the share, add the following to `/etc/smb.conf`.

   ```
   [SHARE_NAME]
   /home/user/shared
   public = no
   writable = yes
   ```
   `printable = no` (since you want to share files, not a printer)
3. Restart the Samba services to load the new settings. On the Linux guest operating system, at a command prompt, type:

   `/etc/init.d/smb restart`

   On some Linux distributions, the command is

   `/etc/rc.d/init.d/smb restart`

   When the system restarts, the Samba service appears in the list of services starting up.

Sharing Files Between Two Linux Systems

To share files between two Linux systems (where one machine is a host and the other is a virtual machine, or both are virtual machines), you can use NFS on the system to connect to and the `nfsmount` utility in the system from which you are making the connection.

As with any Linux network, you can use NFS, FTP or Telnet to connect from one Linux system (either virtual or physical) to another Linux system (either virtual or physical).

Deciding How Your Virtual Machine Stores Data

Do you ever have a bad day and wish you could get rid of all the changes you've made to files on your computer? In a VMware Workstation virtual machine, you can. The secret is in the disk modes.

VMware Workstation uses disks in three different modes — persistent, undoable and nonpersistent.

Disks in persistent mode behave exactly like conventional disk drives on a computer. All data written to a disk in persistent mode is written out permanently to the disk as soon as the guest operating system writes the data.

When you use undoable mode, you have the option later of keeping or discarding changes you have made while the virtual machine is running. Until you decide, the changes are saved in a redo-log file. You can also keep the changes for the next time the virtual machine runs, but still have the option of discarding all the accumulated changes at some time in the future.

All changes to a disk in nonpersistent mode are discarded after the virtual machine is powered off.

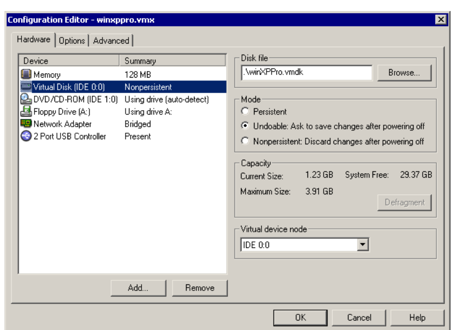
You can use the Configuration Editor to change the disk mode for your virtual machine.

1. Start the virtual machine, but don't click the **Power On** button yet.

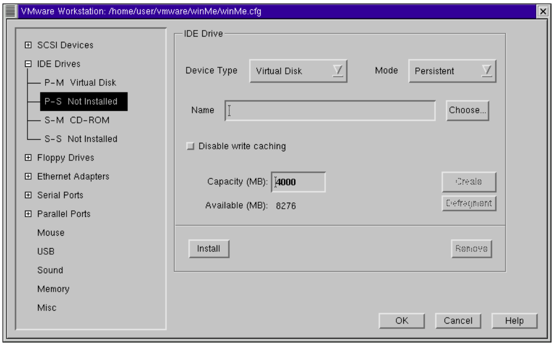
   For Windows hosts, complete steps 1 and 2 under Starting a Virtual Machine on a Windows Host on page 98.

   For Linux hosts, complete steps 1 and 2 under Starting a Virtual Machine on a Linux Host on page 101.

2. Choose **Settings** > **Configuration Editor**. The Configuration Editor appears.



3. On a Windows host, click the name of the drive you want to change.



On a Linux host, click the + sign beside **IDE Drives** or **SCSI Drives** to expand that part of the tree, then click the name of the drive you want to change.

4. Select the appropriate option for persistent, undoable or nonpersistent mode.

   Click **OK** to save your changes and close the Configuration Editor.

Suspending and Resuming Virtual Machines

You can save the current state of your virtual machine by suspending it. Then 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.

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.

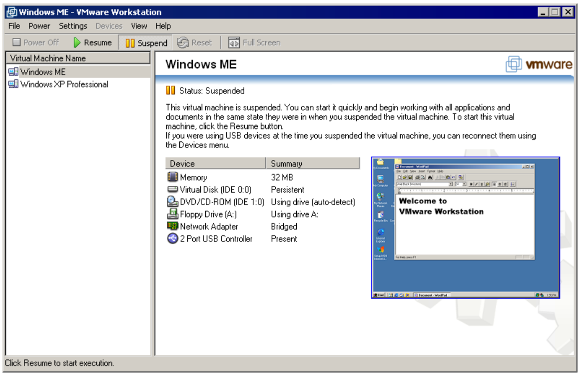
When you suspend a virtual machine, a file with a `.vmss` extension is created. This file contains the entire state of the virtual machine. When you resume the virtual machine, its state is restored from the `.vmss` file. If you have not modified the virtual machine's configuration, the `.vmss` file is then removed.

This behavior ensures that a `.vmss` file is used only once to resume a virtual machine — which is the safest behavior. Note that a virtual machine you have suspended and resumed may be suspended again, creating a new `.vmss` file.

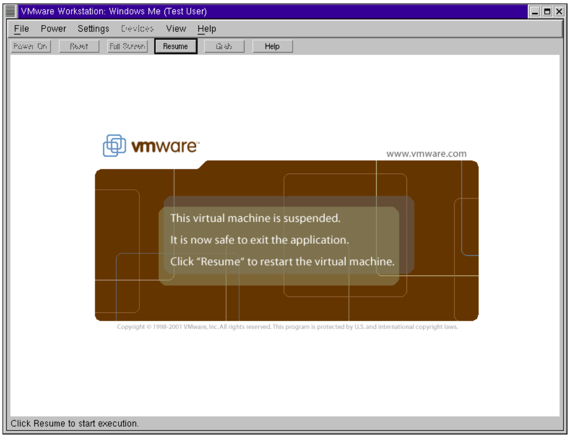
To suspend a virtual machine:

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.



VMware Workstation on a Windows host with a suspended virtual machine



VMware Workstation on a Linux host with a suspended virtual machine

3. When VMware Workstation has completed the suspend operation, you see a screen similar to one of those above, depending on your host operating system. 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, above.

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.

Resuming Virtual Machines Repeatedly from the Same Point

When you suspend a virtual machine in the usual way, by clicking the **Suspend** button on the toolbar, a file with a `.vmss` extension is created. This file contains the entire state of the virtual machine. When the virtual machine is resumed, its state is restored from the `.vmss` file. This means that, in normal operation, the `.vmss` file cannot be used to resume a virtual machine again from the original suspended state.

If you want to be able to resume a virtual machine in the same state repeatedly — for example, in a QA testing or classroom environment — then you can take advantage of repeatable resume. Every time you resume the virtual machine, it starts from the same point at which it was suspended using the same `.vmss` file. This feature works only with virtual disks in nonpersistent mode. For a discussion of disk modes, see Disk Modes: Persistent, Undoable and Nonpersistent on page 218.

Repeatable resume makes it easy to start a virtual machine again and again in the exact same state. However you cannot suspend this virtual machine; you can only power it off. After you power it off, you can resume the virtual machine to start it up again. The virtual machine starts at the point at which it was suspended.

If you need to reset a virtual machine that is set up to use repeatable resume, you should restart the guest operating system (using **Start** > **Shut Down** > **Restart** for Windows guests, `shutdown -r now` for Linux guests). Do not click the **Reset** button on the virtual machine's toolbar. Otherwise, any files you created or other changes made to the guest operating system are lost.

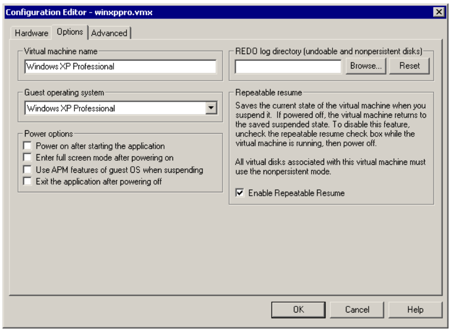
Restarting or resetting the guest operating system does not affect the suspended state. To return to your repeatable resume point, just power off the virtual machine, then resume it.

If you want to restrict the user interface of a virtual machine using repeatable resume, see Using Repeatable Resume with a Restricted User Interface on page 405.

Enabling Repeatable Resume on a Windows Host

1. Make sure the virtual machine is powered off. You can enable the repeatable resume feature only when the virtual machine is powered off.
2. Open the Configuration Editor. Choose **Settings** > **Configuration Editor**.

3. All virtual disks associated with this virtual machine must be in nonpersistent mode before you can enable repeatable resume. In the Configuration Editor, on the **Hardware** tab, select the virtual disk. Under **Mode**, make sure the **Nonpersistent** radio button is selected.
4. Click the **Options** tab.

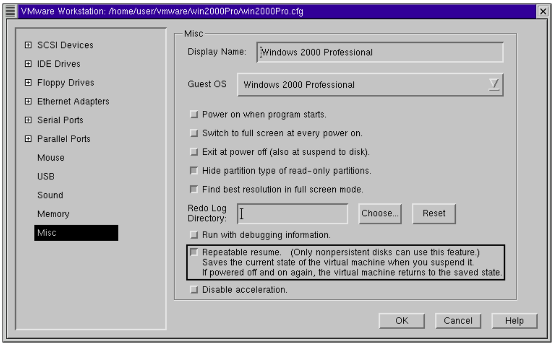


5. If you intend to copy this virtual machine to other PCs, VMware suggests that you specify that the redo log is to be located in the same directory as the virtual machine. Click **Browse** to find the virtual machine's directory and select it.
6. Check the **Enable Repeatable Resume** check box.
7. Click **OK** to save your changes and close the Configuration Editor.

Enabling Repeatable Resume on a Linux Host

1. Make sure the virtual machine is powered off. You can enable the repeatable resume feature only when the virtual machine is powered off.
2. Open the Configuration Editor. Choose **Settings** > **Configuration Editor**.
3. The virtual disks associated with this virtual machine must be in nonpersistent mode before you can enable repeatable resume. In the Configuration Editor, under **SCSI Devices** or **IDE Drives**, select the virtual disks and make sure the **Mode** is set to **Nonpersistent**.

4. Click **Misc**. The **Misc** panel appears.



5. If you intend to copy this virtual machine to other PCs, VMware suggests that you specify that the redo log is to be located in the same directory as the virtual machine. Click **Choose** to find the virtual machine's directory and select it.
6. Select **Repeatable resume**.
7. Click **OK** to save your changes and close the Configuration Editor.

Issues to Consider

Caution: By default, the redo-log file for a disk in nonpersistent mode is located in your system's temp directory. If you intend to move this virtual machine to another host, VMware suggests that you place the redo log for a virtual machine using repeatable resume in a different location (outlined in the steps below), as some temp directories may be small (and the redo log could exceed this limit as it grows) or, on Linux hosts, the temp directory may be cleared by the operating system on a regular basis, and this would remove the redo log.

Caution: VMware does not recommend moving a suspended virtual machine containing disks in nonpersistent mode to another host. However, if you want to take advantage of the repeatable resume feature in a classroom environment, for example, and do not want to set the same repeatable resume point individually on every student's machine, be very careful and keep the following warnings in mind:

- VMware does not support the use of repeatable resume with a virtual machine when its disks are located on a networked drive. However, if you place a disk in nonpersistent mode on a shared network drive, note that locating the redo log in a directory on a networked drive may affect the performance of your virtual machine.

- Do not distribute the virtual disk (`.vmdk`) files. Place the virtual disks in a location on a shared network drive the whole class can access. Multiple users can run the same nonpersistent disk at one time.
- Make sure all the machines in the classroom contain the same hardware as the machine on which the virtual disk resides. This reduces the chance of hardware inconsistencies when the student resumes the virtual machine.
- Before you power on the virtual machine and create your repeatable resume point, put the redo log in the directory with the virtual machine's configuration file. Use the Configuration Editor (choose **Settings** > **Configuration Editor**, then select the **Options** tab for Windows hosts, **Misc** panel for Linux hosts) to specify the location of the redo log.
- After you create your repeatable resume point, copy all the files from the directory containing the virtual machine's configuration file to each student's computer.

Disabling Repeatable Resume

If you no longer want to resume the virtual machine from this repeatable resume point, do the following:

1. Resume the virtual machine, if it is not running already. The virtual machine must be running for you to disable the repeatable resume feature.
2. Open the Configuration Editor (**Settings** > **Configuration Editor**). Then do one of the following:
   - On a Windows host, click the **Options** tab, then clear the **Enable repeatable resume** check box.
   - On a Linux host, click **Misc**, then deselect **Enable repeatable resume**.
3. Click **OK** to save your changes and close the Configuration Editor.
4. Power off the virtual machine. This removes the suspend state (`.vmss` file) and allows you to suspend and resume the virtual machine normally again. All redo-log files for this virtual machine are removed.

   With the virtual machine powered off, you can enable the feature again so that the next time you power on, you can set the virtual machine into a different state and save that as a new repeatable resume point.

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.

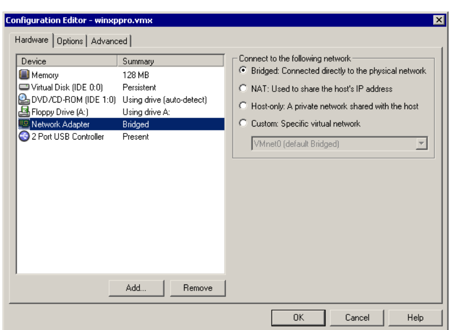
   File > **Exit**

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.

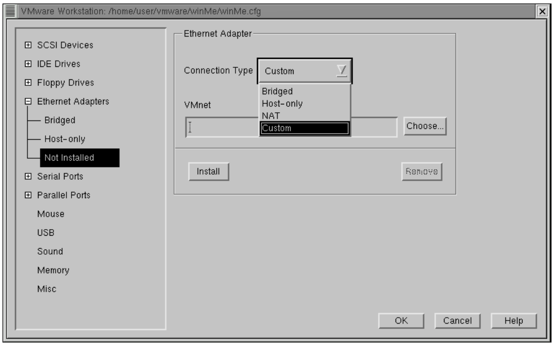
Note: On a Windows host, if you inadvertently attempt to exit VMware Workstation while the guest operating system is still running, a dialog box appears. It gives you the option of suspending the virtual machine before exiting.

Adding, Configuring and Removing Devices in a Virtual Machine

The Configuration Editor (**Settings** > **Configuration Editor**) 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 on a Windows host, open the Configuration Editor, click **Add**, then follow the instructions in the New Hardware Wizard to add the new device to your virtual machine. Click **OK** to save your changes and close the Configuration Editor.



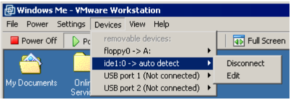
To add a new device on a Linux host, open the Configuration Editor, click the **+** sign beside the type of device you want to add, click a device that's shown as **Not Installed** and make the appropriate settings. Click **Install** to install the device and **OK** to save your configuration changes and close the Configuration Editor.

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

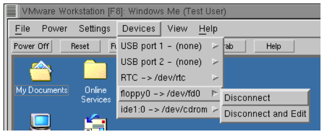
To remove a device, open the Configuration Editor, click the name of the device you want to remove, then click **Remove**. Click **OK** to close the Configuration Editor.

Connecting and Disconnecting Removable Devices

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



On a Windows host, move the mouse pointer over a device name. A cascading menu gives you choices for connecting or disconnecting the device and, where appropriate, for editing the configuration settings for the device.



On a Linux host, click the device name. A cascading menu gives you choices for connecting or disconnecting the device and, where appropriate, for editing the configuration settings for the device.

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.

Creating a Screen Shot of a Virtual Machine

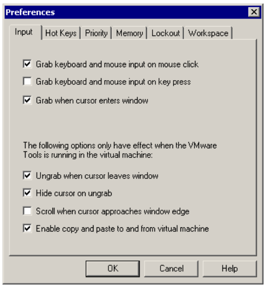
On a Windows host, you can capture a screen shot of a virtual machine using **Capture Screen…** on the **File** menu. You can save this image as a Windows bitmap (`.bmp`) file.

There is no corresponding function on a Linux host.

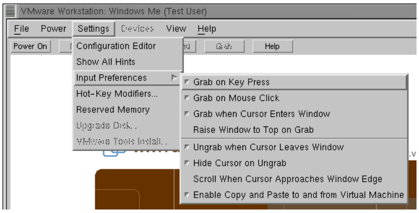
Setting General Preferences for VMware Workstation

The **Settings** menu allows you to change a number of settings that apply to VMware Workstation itself, no matter what virtual machine your are running.

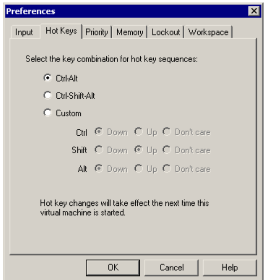
To make changes to these settings on a Windows host, choose **Settings** > **Preferences…**.



Input **—** The **Input** tab on a Windows host lets you adjust the way that the virtual machine captures control of keyboard and mouse.



To change the input settings on a Linux host, choose **Settings** > **Input Preferences**, then click an item on the cascading menu to toggle its setting on or off.

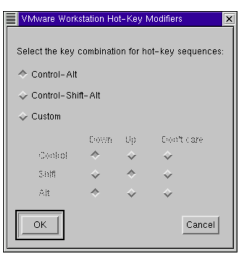


***Hot keys* —** The **Hot Key** tab on a Windows host lets you change the key combination that determines whether certain combinations of keys are passed to the guest operating system or intercepted by VMware Workstation.

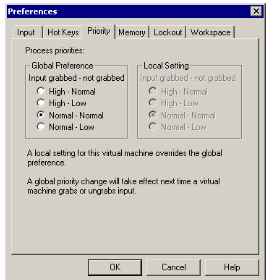
For example, you may want to change hot key combinations from Ctrl-Alt-<key> to Ctrl-Shift-Alt-<key> to prevent Ctrl-Alt-Delete from being intercepted by VMware Workstation instead of being sent to the guest operating system.

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.



On a Linux host, Choose **Settings** > **Hot Key Modifiers…**.
A dialog box allows you to set the hot key combination.

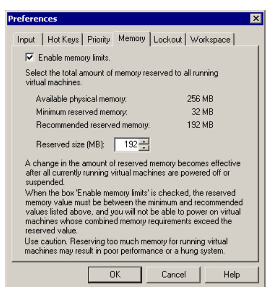


***Process priorities* —** The Priority tab on a Windows host lets you determine the priority that the Windows process scheduler gives to your virtual machines when mouse and keyboard input are going to a particular virtual machine and when input is not going to that virtual machine.

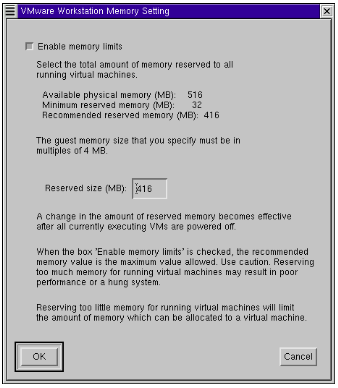
You can adjust these settings to improve overall system performance based on the relative priority of work you are doing in various virtual machines and on the host computer.

To change the settings for a particular virtual machine, and override the global settings, open the virtual machine you want to adjust, choose **Settings** > **Local Priority**, then click the priority setting you want to use for that virtual machine.

There is no corresponding setting on a Linux host.

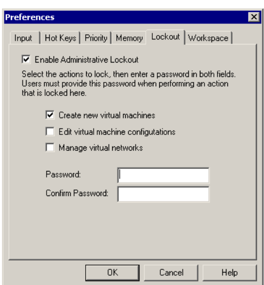


***Reserved memory size* —** The Memory tab on a Windows host lets you adjust the amount of memory reserved for all running virtual machines.



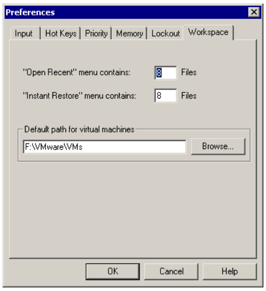
On a Linux host, choose **Settings** > **Reserved Memory…**.
A dialog box allows you to adjust the amount of memory reserved to all running virtual machines.

For details on adjusting memory settings in VMware Workstation, see Memory Usage Notes on page 392.



***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 403.

There are no corresponding settings on a Linux host.



Access to recently used machines and path for virtual machine files — The Workspace tab on a Windows host let you set the maximum number of virtual machines that can be listed in the **File** > **Open Recent** and **File** > **Instant Restore** menus. It also lets you change the default path for storing virtual machine files.

There are no corresponding settings on a Linux host.

Command Reference

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 ]
[/<path_to_config>/<config>.cfg ]
[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` exits VMware Workstation when the virtual machine powers off. This is particularly useful when the guest operating system is capable of powering off the virtual machine.

`/<path_to_config>/<config>.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.

Windows Host

The switches described above for Linux can also be used on a Windows host. 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. And path names on Windows use the backslash character (\). X toolkit options are not relevant on a Windows host.

6

Moving and Sharing Virtual Machines

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:

Moving a 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 your host? The process is not difficult, and in most cases you can even move your virtual machine from a Windows host to a Linux host — or vice versa. Here's how.

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 folder (directory) before you start a process like this.

Virtual Machines Use Relative 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 would 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 folder (directory). For example, if you are in the virtual machine's directory, the relative path to the virtual disk file would be `<machine name>.vmdk`.

Note: You can still use absolute paths if you wish.

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 130.

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 and its virtual disks are in persistent or nonpersistent mode, resume it, then shut down the guest operating system.
2. 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 132.

   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.

3. 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 128.
   - 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 file. The virtual machine is added to the **Virtual Machine Name** list in the Workstation window.

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 file. Use the Configuration Editor and check to see if your virtual machine is pointing to the correct location for files you do not move.

   Also, check to see you do not have any absolute paths pointing to any files you *are* moving.

   To determine whether any files are using absolute or relative paths, use the Configuration Editor. Select each device. Also, look at the location of the redo-log file.

Note: 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 132.

3. Start VMware Workstation and open the new virtual machine you just created. Choose **File** > **Open**, then browse to the virtual machine's configuration file. The virtual machine is added to the **Virtual Machine Name** list in the Workstation window.

Moving an Older Virtual Machine

If you have created a virtual machine using VMware Workstation 3.0 or 2.x, 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 folder (directory) before you start a process like this.

Preparing Your Virtual Machine for the Move

1. 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 Configuration Editor (**Settings** > **Configuration 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.

2. Shut down the guest operating system. If the virtual machine is suspended, resume it, then shut down the guest operating system.

   Note: Do not move a suspended virtual machine from one host to another.

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 132.

4. 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 is installed and working correctly on the new host computer.
2. Run the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux Hosts) and select the appropriate guest operating system for the virtual machine you're moving.

   Choose a virtual disk for your hard drive and use a drive size that matches the size of the virtual disk you plan to move.

   Select all appropriate network, floppy and CD-ROM settings. Do not make any changes with the Configuration Editor at this point.

   Save your settings and close VMware Workstation.
3. In the folder (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 again and open the new virtual machine you just created. Go to **Settings** > **Configuration Editor**.
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.

   Windows host: 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 migrating, 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.

   Linux host: Click the **+** signs to expand the **SCSI Devices** and **IDE Drives** categories. Be sure that the virtual machine's settings match those of the virtual disk you are migrating. If you need to remove a virtual disk from the configuration, select that disk in the list on the left, then click **Remove** in the panel on the right. To add a virtual disk, select the appropriate disk from the list on the left (for a boot disk, use either SCSI 0:0 or the IDE disk labeled P-M) and click **Install**.

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 folder (directory) that has a path name identical to that of the current folder (directory).
- You may be able to move the disk in undoable mode between Windows and Linux host systems, and move the disk to a different folder (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.

   If you are moving a disk in undoable mode from one computer to another computer, start VMware Workstation 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. Start the Configuration Editor.

   Select **Settings** > **Configuration Editor**.

4. Examine the entry for your virtual disk to see whether it includes a full path to the first virtual disk file. For example, on a Windows host, you might see a Disk File listing like this:

   `My Documents\My Virtual Machines\Windows Me\Windows Me.vmdk`

   Entries for SCSI disks are similar.

   If your Disk File information resembles that above, with a full path to the first disk file, then as long as you have not committed or discarded changes to the undoable disk, note the following:

   - You can move the disk to another computer of the same type (Windows to Windows).
   - You must place the virtual machine's other files (`.vmx` and `.REDO` on Windows, `.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 folder (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` (except for the redo logs for disks in nonpersistent mode, which are located in your system's temp folder). 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 (`.cfg`) 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 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 logs 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, complete the following steps.
  A. With the virtual machine powered off, open the Configuration Editor. Choose **Settings** > **Configuration Editor**.
  B. Click the **Options** tab (Windows hosts) or **Misc** panel (Linux hosts).
  C. Click **Browse** and select a directory that is shared with other users.
  D. Click **OK** to save the change and close the Configuration Editor.

Note: Virtual machines with disks in nonpersistent mode perform better when the redo log is located in the system's temp directory.

7

Installing Guest Operating Systems

Choosing and Installing Guest Operating Systems

The following sections describe which operating systems are supported and unsupported for use as guests under VMware Workstation and provide notes on installing specific guest operating systems:

Supported and Unsupported Guest Operating Systems

Check the lists that follow for information on which operating systems now work as guest operating systems in a VMware Workstation virtual machine and the status of operating systems that are not on the supported list.

Supported Guest Operating Systems

Microsoft Windows .NET Server

- Windows .NET Web Server beta 3, Windows .NET Standard Server beta 3 and Windows .NET Enterprise Server beta 3 (experimental)

Microsoft Windows XP

- Windows XP Professional and Windows XP Home Edition; Service Pack 1

Microsoft Windows 2000

- Windows 2000 Professional, Windows 2000 Server and Windows 2000 Advanced Server; Service Pack 2; Service Pack 3

Microsoft Windows NT

- Windows NT 4.0 Workstation and Windows NT Server, Service Pack 3 or higher

Microsoft Windows

- Windows Millennium Edition
- Windows 98 and Windows 98 SE
- Windows 95 (all OSR releases)
- Windows for Workgroups
- Windows 3.1

Microsoft MS-DOS

- MS-DOS 6

Linux

- Caldera OpenLinux 2.x
- Mandrake Linux 8.0, 8.1 and 8.2
- Red Hat™ Linux 6.2, 7.0, 7.1, 7.2 and 7.3
- SuSE™ Linux 7.0, 7.1, 7.2, 7.3, SLES 7 and 8.0

- TurboLinux 6.0 and 7.0

Novell NetWare

- NetWare 6.0 (experimental)

FreeBSD

- FreeBSD 3.x, 4.0, 4.1, 4.2, 4.3, 4.4, 4.5 and 4.6

  Note: If you use SCSI virtual disks larger than 2GB with FreeBSD 3.x or 4.x (up to and including 4.3), there are known problems, and the guest operating system does not boot. To work around this issue, see Setting the Disk Geometry for a FreeBSD SCSI Virtual Disk on page 202.

Guests Using PAE Options Not Supported

Guest operating systems that use the Physical Address Extension (PAE) processor options will not run under VMware Workstation 3.2. This issue affects Linux guests if PAE is enabled in the kernel. It affects Windows guests if booted with the `/PAE` option.

Unsupported Guest Operating Systems

Note: VMware Workstation provides support only for guest operating systems that run on x86 (Intel and compatible) microprocessors. It is not possible to use an operating system designed for a different type of microprocessor as a guest operating system. For example, Mac OS, designed to run on PowerPC processors, is not supported. Similarly, operating systems designed to run on the Alpha microprocessor are not supported.

Operating Systems that May Work but Are Not Supported

The following guest operating systems may work with VMware Workstation but are not supported.

- Caldera OpenLinux 1.3
- Slackware Linux
- Novell NetWare 4.x, 5.0 (does not work on a Pentium III processor) and 5.1
- Solaris 7 Intel Edition, 8
- NetBSD 1.x
- OpenBSD 2.x

Operating Systems that May Not Work and for which Support is Not Planned

The following guest operating systems may not work with VMware Workstation. There are currently no plans to support these guests:

- BeOS
- IBM OS/2 and OS/2 Warp
- Minix
- QNX
- SCO Unix
- UnixWare

Installation Notes for Particular Guest Operating Systems

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.
3. Power on your virtual machine by clicking the **Power On** button.
4. Follow the instructions provided by the operating system vendor.

As with physical computers, a separate operating system license is required for each virtual machine you run.

These notes highlight special steps you may need to take when you install particular guest operating systems.

Windows .NET Server Installation Guidelines

You can install the beta 3 release of Windows .NET Web Server, Windows .NET Standard Server or Windows .NET Enterprise Server in a virtual machine using the corresponding Windows .NET Server distribution CD.

Currently, support for .NET Server guest operating systems is experimental.

Note: To use SCSI disks in a Windows .NET Server 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 .NET Server. If you have a virtual machine with a SCSI virtual disk and a Windows 9x, Windows Me, Windows NT or Windows 2000 guest operating system and want to upgrade it to Windows .NET Server, install the new SCSI driver before upgrading the operating system.

Installation Steps

If you want to run Windows .NET Server in a VMware Workstation virtual machine, be sure you have a full installation CD for the operating system.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Installing the Guest Operating System

1. Before starting the installation, use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect. For example, if you would like networking software to be installed during the Windows .NET Server installation, be sure the virtual machine's Ethernet adapter is configured and enabled. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Windows .NET Server CD in the CD-ROM drive.
3. Power on the virtual machine to start installing Windows .NET Server.
4. Follow the installation steps as you would for a physical machine.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84.

Enabling Sound in a Windows .NET Server Guest

Windows .NET Server does not automatically detect and install drivers for ISA sound cards, such as the Creative Labs Sound Blaster emulated in a virtual machine. For details on installing the driver for the virtual machine's sound card, see Sound in a Windows XP or Windows .NET Server Guest on page 340.

Known Issues

The Microsoft Windows .NET Server product activation feature creates a numerical 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 operating system. There are some steps you can take to minimize the number of significant changes.

- Set the final memory size for your virtual machine before you activate Windows .NET Server. When you cross certain thresholds — approximately 32MB, 64MB, 128MB, 256MB, 512MB and 1GB — the product activation feature sees the changes as significant.

  Note: The size reported to the Windows product activation feature is slightly less than the actual amount configured for the virtual machine. For example, 128MB is interpreted as falling in the 64MB–127MB range.

- Install VMware Tools before you activate Windows .NET Server. When the SVGA driver in the VMware Tools package is installed, it activates features in the virtual graphics adapter that make it appear to Windows .NET Server as a new graphics adapter.
- If you want to experiment with any other aspects of the virtual machine configuration, do so before activating Windows .NET Server. Keep in mind that you have 30 days for experimentation before you have to activate the operating system.
- In order to install and run a checked (debug) build of Windows .NET Server in a virtual machine, you must first edit the virtual machine configuration (`.vmx` or `.cfg`) file. Add the following line:

  ```
  uhci.forceHaltBit = TRUE
  ```

For more details on Windows .NET Server product activation, see the Microsoft Web site.

Windows XP Installation Guidelines

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

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. If you have a virtual machine with a SCSI virtual disk and a Windows 9x, Windows Me, Windows NT or Windows 2000 guest operating system and want to upgrade it to Windows XP, install the new SCSI driver before upgrading the operating system.

Installation Steps

If you want to run Windows XP Home Edition or Professional in a VMware Workstation virtual machine, be sure you have a full installation CD for the operating system.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts). Make sure you selected Windows XP as your guest operating system.

Now, you're ready to install Windows XP Home Edition or Professional.

Installing the Guest Operating System

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Windows XP installation, be sure the virtual machine's Ethernet adapter is configured and enabled. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the installation CD in the CD-ROM drive.
3. Power on the virtual machine to start installing the guest operating system.
4. Follow the installation steps as you would for a physical machine, except as noted in the following steps.
5. After the system reboots, a message balloon asks if you want Windows to automatically correct your screen resolution and color depth setting. Do not make the change at this time. You cannot change resolution and color depth until you have installed the VMware SVGA driver — part of the VMware Tools package.

6. Run the VMware Tools installer. For details, see Installing VMware Tools on page 84.
7. When the guest operating system reboots, allow it to change the screen resolution and color depth setting.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details on installing VMware Tools, see Installing VMware Tools on page 84.

Enabling Sound in a Windows XP Guest

Windows XP does not automatically detect and install drivers for ISA sound cards, such as the Creative Labs Sound Blaster emulated in a virtual machine. For details on installing the driver for the virtual machine's sound card, see Sound in a Windows XP or Windows .NET Server Guest on page 340.

Known Issues

The Microsoft Windows XP product activation feature creates a numerical 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 operating system. There are some steps you can take to minimize the number of significant changes.

- Set the final memory size for your virtual machine before you activate Windows XP. When you cross certain thresholds — approximately 32MB, 64MB, 128MB, 256MB, 512MB and 1GB — the product activation feature sees the changes as significant.

  Note: The size reported to the Windows product activation feature is slightly less than the actual amount configured for the virtual machine. For example, 128MB is interpreted as falling in the 64MB–127MB range.
- Install VMware Tools before you activate Windows XP. When the SVGA driver in the VMware Tools package is installed, it activates features in the virtual graphics adapter that make it appear to Windows XP as a new graphics adapter.
- If you want to experiment with any other aspects of the virtual machine configuration, do so before activating Windows XP. Keep in mind that you have 30 days for experimentation before you have to activate the operating system.
- In order to install and run a checked (debug) build of Windows XP in a virtual machine, you must first edit the virtual machine configuration (`.vmx` or `.cfg`) file. Add the following line:

  ```
  uhci.forceHaltBit = TRUE
  ```

For more details on Windows XP product activation, see the Microsoft Web site.

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

The hibernation feature is not supported in this release. Instead of using the guest operating system's hibernate feature, suspend the virtual machine by clicking **Suspend** on the VMware Workstation toolbar.

Windows 2000 Installation Guidelines

You can install Windows 2000 Professional or Server in a virtual machine using the corresponding Windows 2000 distribution CD.

Note: Some Microsoft Windows 2000 OEM disks included with new computers are customized for those computers and include device drivers and other utilities specific to the hardware system. Even if you can install this Windows 2000 operating system on your actual computer, you may not be able to install it in a VMware Workstation virtual machine. You may need to purchase a new copy of Windows to install in a virtual machine.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Windows 2000 Installation Steps

1. Before starting the installation, use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect. For example, if you would like networking software to be installed during the Windows 2000 installation, be sure the virtual machine's Ethernet adapter is configured and enabled. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Windows 2000 CD in the CD-ROM drive.
3. Power on the virtual machine to start installing Windows 2000.
4. If you enabled the virtual machine's Ethernet adapter, an AMD PCNET Family Ethernet Adapter is detected and set up automatically.

VMware Tools

Be sure to install VMware Tools in your guest operating system. After you install VMware Tools, you need to change your Windows 2000 screen area to be greater than 640x480 pixels; if you do not change it, Windows 2000 uses the standard VGA driver, and your performance will suffer.

For details, see Installing VMware Tools on page 84.

Enabling Sound After Installing Windows 2000

If sound was disabled at the time you installed your Windows 2000 guest operating system, you can enable it after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in VMware Workstation on page 339.

Enabling Networking After Installing Windows 2000

If networking was disabled at the time you installed your Windows 2000 guest operating system, you can enable it after the operating system has been installed. To set up networking for a virtual machine, follow the instructions below.

Windows Host

1. Shut down Windows 2000 and power off the virtual machine.
2. From the VMware Workstation window, on the Settings menu, choose Configuration Editor and click Add.
3. Follow the instructions in the Add Hardware Wizard to add a virtual Ethernet adapter.
4. Power on the virtual machine.
5. When Windows 2000 boots, it automatically detects a new network adapter and loads drivers for an AMD PCNET Family PCI Ethernet Adapter.
6. You should be able to access the network after logging on to Windows 2000 guest operating system.

Linux Host

1. Shut down Windows 2000 and power off the virtual machine.
2. From the VMware Workstation window, on the Settings menu, choose Configuration Editor and open the Ethernet Adapters panel.
3. Select a network connection type for the virtual machine and click the Install button.
4. Click OK to save the updated configuration, then power on the virtual machine.
5. When Windows 2000 boots, it automatically detects a new network adapter and loads drivers for an AMD PCNET Family PCI Ethernet Adapter.
6. You should be able to access the network after logging on to Windows 2000 guest operating system.

Known Issues

- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Windows NT Installation Guidelines

You can install Windows NT 4.0 (Workstation or Server) in a virtual machine using the standard Windows NT CD.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Windows NT Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Windows NT installation, be sure the virtual machine's Ethernet adapter is configured and enabled. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Windows NT CD in the CD-ROM drive.
3. Power on the virtual machine to start installing Windows NT.
4. If you have enabled the virtual machine's Ethernet Adapter, an AMD PCNET Family Ethernet Adapter is detected and set up automatically. The default settings should work fine and do not need to be changed.
5. Finish the Windows NT installation.
6. VMware Workstation's virtual disks support DMA transfers for better performance.

   You can enable the feature after Windows NT has been successfully installed. You need the NT Service Pack 3 or 4 CD to enable this option. Once the virtual machine is running Windows NT, insert the SP3 or SP4 CD in the drive, run `DMACHECK.EXE` from the `\SUPPORT\UTILS\I386` folder on the CD and click the **Enabled** option for the IDE controller/channel that is configured with the virtual disk (typically channel 0 only, unless you have the virtual machine configured with multiple virtual disks). The DMA option should not be enabled for any IDE channel that has a CD-ROM drive configured for it. Enabling it causes an error.

   Note: DMA is always enabled on SCSI virtual disks.

   Note: If you have a virtual disk and a 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 Configuration Editor to move the CD-ROM to the secondary IDE controller (channel 1) at IDE 1:0. Then boot the virtual machine with Windows NT, run `DMACHECK` and enable DMA for channel 0 only.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84.

Setting up a Windows NT 4.0 Guest with Multiple Disks

To set up a virtual machine running Windows NT 4.0 and using multiple disks, you must first create a virtual machine with only one disk. Install Windows NT on that disk. Then use the Configuration Editor (**Settings** > **Configuration Editor**) to add the additional disks.

In addition, note that 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.

Enabling Networking After Installing Windows NT

If networking was disabled at the time you installed Windows NT, you can enable it after the operating system has been installed. To set up networking for a virtual machine, follow the instructions below.

Windows Host

1. Shut down Windows NT and power off the virtual machine.
2. From the VMware Workstation window, on the **Settings** menu, choose **Configuration Editor** and click **Add**.
3. Follow the instructions in the Add Hardware Wizard to add a virtual Ethernet adapter.
4. Power on the virtual machine.
5. While Windows NT is booting, insert the Windows NT 4.0 CD in the CD-ROM drive.
6. Log on to Windows NT and install the AMD PCNET driver:
   A. Open the Network properties page by double-clicking the Network icon in Control Panel. Change to the Network Adapters screen by clicking the **Adapters** tab.

   B. Click the **Add** button and select the AMD PCNET Family Ethernet Adapter from the list.

   C. A message pops up prompting you to enter a path for the Windows NT files. Specify the `\I386` folder on the CD in the path you enter (for example, type `D:\i386` if the CD is in drive D) and click Continue.

D. Windows NT setup prompts you for the Windows NT files again. Click **Continue**.

E. Use the default adapter settings; they do not need to be changed. Windows NT setup prompts you again for a path to the Windows NT files. Click **Continue** to finish installing the driver.

Linux Host

1. Shut down Windows NT and power off the virtual machine.
2. From the main program window, on the **Settings** menu, choose **Configuration Editor** and open the **Ethernet Adapters** panel.
3. Select a network connection type for the virtual machine and click the **Install** button.
4. Click **OK** to save the updated configuration, then power on the virtual machine.
5. While Windows NT is booting, insert the Windows NT 4.0 CD in the CD-ROM drive.
6. Log on to Windows NT and install the AMD PCNET driver:

   A. Open the Network properties page by double-clicking the Network icon in Control Panel. Change to the Network Adapters screen by clicking the **Adapters** tab.

   B. Click the **Add** button and select the AMD PCNET Family Ethernet Adapter from the list.

   C. A message pops up prompting you to enter a path for the Windows NT files. Specify the `\I386` folder on the CD in the path you enter (for example, type `D:\i386` if the CD is in drive D) and click **Continue**.

   D. Windows NT setup prompts you for the Windows NT files again. Click **Continue**.

   E. Use the default adapter settings; they do not need to be changed. Windows NT setup prompts you again for a path to the Windows NT files. Click **Continue** to finish installing the driver.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Windows Me Installation Guidelines

You can install Windows Millennium Edition in a virtual machine using the standard Windows Me CD.

Note: Some Microsoft Windows Me OEM disks included with new computers are customized for those computers and include device drivers and other utilities specific to the hardware system. Even if you can install this Windows Me operating system on your actual computer, you may not be able to install it in a VMware Workstation virtual machine. You may need to purchase a new copy of Windows to install in a virtual machine.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like the Windows Me Setup program to install networking services, be sure that a virtual Ethernet adapter is installed in the virtual machine's configuration. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Windows Me CD in the CD-ROM drive.
3. Power on the virtual machine to start installing Windows Me.
4. Choose to boot from CD-ROM, then select the **Start Windows Me Setup from CD-ROM** option. The setup program runs `FDISK` and reboots.
5. Once again, choose to boot from CD-ROM, then select the **Start Windows Me Setup from CD-ROM** option. The setup program continues installing Windows Me.
6. Follow the Windows Me installation steps as you would for a physical machine.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Windows 98 Installation Guidelines

You can install Windows 98 in a virtual machine using the standard Windows 98 CD.

Note: Some Microsoft Windows 98 OEM disks included with new computers are customized for those computers and include device drivers and other utilities specific to the hardware system. Even if you can install this Windows 98 operating system on your actual computer, you may not be able to install it in a VMware Workstation virtual machine. You may need to purchase a new copy of Windows to install in a virtual machine.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like the Windows 98 setup program to install a sound driver, be sure that sound is enabled in the virtual machine's configuration. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Windows 98 CD in the CD-ROM drive.
3. Power on the virtual machine to start installing Windows 98.
4. Choose to boot from CD-ROM, then select the **Start Windows 98 Setup from CD-ROM** option. The setup program runs `FDISK` and reboots.
5. Once again, choose to boot from CD-ROM, then select the **Start Windows 98 Setup from CD-ROM** option. The setup program continues installing Windows 98.
6. Follow the Windows 98 installation steps as you would for a physical PC.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84.

Enabling Sound After Installing Windows 98

If sound was disabled at the time you installed Windows 98, you can enable it after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in VMware Workstation on page 339.

Enabling Networking After Installing Windows 98

If networking was disabled at the time you installed Windows 98, you can enable it after the operating system has been installed. To set up networking for a virtual machine, follow the instructions below.

Windows Host

1. Shut down Windows 98 and power off the virtual machine.
2. From the VMware Workstation window, on the **Settings** menu, choose **Configuration Editor** and click **Add**.
3. Follow the instructions in the Add Hardware Wizard to add a virtual Ethernet adapter.
4. Power on the virtual machine.
5. When Windows 98 reboots, it auto-detects an AMD PCNET Family Ethernet Adapter (PCI-ISA) and prompts for the Windows 98 CD-ROM to install drivers. The default Ethernet adapter settings should work fine and do not need to be changed.
6. Use the Network icon in the Control Panel to view or change network settings. For example, you may want to add the TCP/IP protocol since Windows 98 does not install it by default.

Linux Host

1. Shut down Windows 98 and power off the virtual machine.
2. From the main program window, on the **Settings** menu, choose **Configuration Editor** and open the **Ethernet Adapters** panel.
3. Select a network connection type for the virtual machine and click the Install button.
4. Click **OK** to save the updated configuration, then power on the virtual machine.
5. When Windows 98 reboots, it auto-detects an AMD PCNET Family Ethernet Adapter (PCI-ISA) and prompts for the Windows 98 CD-ROM to install drivers. The default Ethernet adapter settings should work fine and do not need to be changed.
6. Use the Network icon in the Control Panel to view or change network settings. For example, you may want to add the TCP/IP protocol since Windows 98 does not install it by default.

Known Issues

After Windows 98 has been installed, you may notice COM5 and COM6 devices exist within the Windows Device Manager. These devices do not actually exist and are not consuming IRQ or other resources. You may remove them using the Windows device manager if you like.

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Support for `EMM386.EXE` and other memory managers is currently limited. If you initially boot using a customized non-standard MS-DOS or Windows 98 boot floppy, be sure that `EMM386.EXE` (or other memory manager) is not being loaded. `HIMEM.SYS` and `RAMDRIVE.SYS` can be loaded and used without problems.

Windows 95 Installation Guidelines

You can install Windows 95 in a virtual machine using a standard Windows 95 boot floppy and CD-ROM.

Note: Some Microsoft Windows 95 OEM disks included with new computers are customized for those computers and include device drivers and other utilities specific to the hardware system. Even if you can install this Windows 95 operating system on your actual computer, you may not be able to install it within a VMware Workstation virtual machine. You may need to purchase a new copy of Windows to install within a virtual machine.

Note: Some Windows 95 distributions provide instructions that do not include the steps to `FDISK` and `FORMAT` a `C:` drive. You must `FDISK` and `FORMAT` the VMware Workstation virtual hard disk drives before running Windows 95 setup.

The instructions below are for the simplest case of one virtual IDE hard drive and one virtual IDE CD-ROM drive. If you have configured the virtual machine with more than one IDE hard drive, you should also `FDISK` and `FORMAT` these drives before installing Windows 95. If you have configured the virtual machine with more than one virtual hard drive or more than one virtual CD-ROM, you may need to use different device letters than those in the instructions below.

Before installing the operating system, be sure that you have already created a directory for the new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like the Windows 95 setup program to install a sound driver, be sure that sound is enabled in the virtual machine's configuration. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Windows 95 CD-ROM Setup Boot Disk in floppy drive `A:` and insert the Windows 95 CD in the CD-ROM drive.
3. Power on the virtual machine.
4. After the virtual machine boots, if you are presented with a choice of CD-ROM drivers, select the first IDE driver option available (even if your computer has a SCSI CD-ROM drive).

5. Partition the virtual disk.
   `A:\> FDISK`
   Answer the questions.

   Note: If you create a primary partition that is smaller than the size of the hard disk, be sure the partition is marked active.

6. Reboot Windows 95. If the cursor is not already within the VMware Workstation window, click in the window, then press Ctrl-Alt-Ins on a Windows host or Ctrl-Alt-Del on a Linux host. If prompted on reboot to select a CD-ROM driver, select the first IDE CD-ROM driver from the list.

7. Format the `C:` drive.
   `A:\> FORMAT C: /S`

8. Start the Windows 95 installation.
   `A:\> D:\WIN95\SETUP /IS`

   Note: An intermittent problem can occur during Windows 95 installations in a virtual machine. Shortly after the Windows 95 Setup program is started, Scandisk runs to completion, and when the Windows 95 Setup program should start its graphical user interface, the virtual machine returns to an MS-DOS prompt. VMware recommends you reboot the virtual machine and rerun Windows 95 Setup. You do not need to `FDISK` or `FORMAT` the drive again. If this problem occurs reproducibly, please report it to VMware technical support.

9. If the virtual machine's Ethernet adapter is enabled, you have to manually add an Ethernet driver because Windows 95 does not detect it during the Analyzing Computer phase (even if you selected the Network Adapter detection option). Do the following to enable networking:

   A. Continue with the Windows 95 installation, until you get to the Windows 95 Setup Wizard/Setup Options screen. Change the default setting from **Typical** to **Custom** and click **Next** to continue.

   B. From the Network Configuration screen (which appears after the Analyzing Computer phase), click **Add**, select the **Adapter** component, select **Advanced Micro Devices** from the manufacturer window and **AMD PCNET Family Ethernet Adapter(PCI&ISA)** from the network adapter window.

   C. If you need TCP/IP networking, add it from the Network Configuration screen (Windows 95 Setup does not enable TCP/IP by default). If you don't do this, the first phase of the Windows 95 installation does not copy some of the files it will need later, and the entire installation fails.

Also be sure that the Microsoft NetBEUI protocol is installed. It may not be installed by default.

10. Finish the Windows 95 installation.
11. VMware Workstation's virtual disks support DMA transfers for better performance. The feature can be enabled after Windows 95 has been successfully installed on a virtual IDE disk. Follow these steps to enable the feature:
    A. Right-click My Computer and select **Properties**.
    B. From the System Properties dialog box, click the **Device Manager** tab.
    C. Double-click the **Disk Drives** device category.
    D. Double-click the **GENERIC IDE DISK TYPE01** device.
    E. Click the **Settings** tab and select the **DMA** check box.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84.

Enabling Sound After Installing Windows 95

If sound was disabled at the time you installed Windows 95, you can enabled it after the operating system has been installed. To set up the virtual machine to play sound, see Configuring Sound in VMware Workstation on page 339.

Enabling Networking After Installing Windows 95

If networking was disabled at the time you installed Windows 95, you can enable it after the operating system has been installed. To set up networking for a virtual machine, follow the instructions below.

Windows Host

1. Shut down Windows 95 and power off the virtual machine.
2. From the VMware Workstation window, on the **Settings** menu, choose **Configuration Editor** and click **Add**.
3. Follow the instructions in the Add Hardware Wizard to add a virtual Ethernet adapter.
4. Power on the virtual machine.
5. When Windows 95 reboots, it auto-detects an AMD PCNET Family Ethernet Adapter (PCI&ISA) and prompts for the Windows 95 CD-ROM to install drivers.

The default Ethernet adapter settings should work fine and do not need to be changed.

6. Double-click the Network icon in the Control Panel to view or change network settings. For example, you may want to add the TCP/IP protocol since Windows 95 does not install it by default.

Linux Host

1. Shut down Windows 95 and power off the virtual machine.
2. From the main program window, on the **Settings** menu, choose **Configuration Editor** and open the **Ethernet Adapters** panel.
3. Select a network connection type for the virtual machine and click the Install button.
4. Click **OK** to save the updated configuration, then power on the virtual machine.
5. When Windows 95 reboots, it auto-detects an AMD PCNET Family Ethernet Adapter (PCI&ISA) and prompts for the Windows 95 CD-ROM to install drivers. The default Ethernet adapter settings should work fine and do not need to be changed.
6. Double-click the Network icon in the Control Panel to view or change network settings. For example, you may want to add the TCP/IP protocol since Windows 95 does not install it by default.

Known Issues

After Windows 95 has been installed, you may find that networking is not working in the guest operating system. There are several things you should check.

- Either remove your virtual machine's virtual USB adapter using the Configuration Editor (**Settings** > **Configuration Editor**) or — if your release of Windows 95 includes USB support — be sure the USB drivers are installed.
- Check the Windows 95 Device Manager to see if COM5 and COM6 devices are listed. If they are, disable or remove them.
- Be sure that NetBEUI was installed when you set up networking.
- Be sure that Windows 95 Plug and Play properly detected the virtual Ethernet adapter. If it did not, you may need to use the Device Manager to remove the adapter, then reinstall it using the Add New Hardware control panel.

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

After Windows 95 has been installed, you may notice Unknown, COM5 and COM6 devices exist in the Windows Device Manager. These devices do not actually exist and are not consuming IRQ or other resources. You may remove them using the Windows Device Manager if you like.

Support for EMM386.EXE and other memory managers is currently limited. If you plan to boot initially using a customized non-standard MS-DOS or Windows 95 boot disk, be sure that `EMM386.EXE` (or other memory manager) is not being loaded. `HIMEM.SYS` and `RAMDRIVE.SYS` can be loaded and used without problems.

DOS and Windows 3.x Installation Notes

Before installing the operating system, be sure that you have already created a directory for the new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

DOS Installation Notes

You can install MS-DOS 6.22 inside a virtual machine using the Microsoft full-version MS-DOS installation disks. If you have the upgrade disks, you must install an earlier version of DOS before you upgrade. To start installing MS-DOS 6.22, put the first disk in the floppy drive, power on the virtual machine and follow the instructions on the screen.

After you install DOS, VMware recommends that you install a CPU idle program within the virtual machine. Most versions of DOS do not idle the CPU when they are idle. Therefore, when you are running DOS in a virtual machine, the virtual machine takes up CPU time on the host even when DOS is idle. VMware Workstation relies on the guest operating system to use the Halt instruction or advanced power management to deschedule the virtual machine when it is idle.

We have tested a program called `DOSIDLE.EXE` and have found it works successfully with VMware Workstation. It can be downloaded from *www.vmware.com/software/dosidle210.zip*.

Follow the instructions provided with the `DOSIDLE.EXE` program. But be aware of the `-cpu` option, which causes the idle program to access the CPU at a low level in order to optimize performance. There is a good chance that this will not work with some CPUs under VMware Workstation. VMware suggests that you not use it.

Windows 3.1x Installation Notes

You can install Windows 3.1x using the standard installation disks. VMware Workstation virtual machines support the networking features found in Windows 3.11 (or Windows for Workgroups). If you set up networking, choose the Advanced Micro Devices PCNET Family (NDIS2/NDIS3) Ethernet driver.

Known Issues

The current support for `DOS/EMM386` is limited. We recommend that you avoid using it for now. Be sure to comment out the entry in the `CONFIG.SYS` file.

We intermittently encounter erratic mouse behavior in virtual machines running Windows v3.1x in window mode. This problem does not appear in the full screen mode.

No VMware Tools package exists for DOS or Windows 3.1x guest operating systems; therefore, Windows 3.1x is limited to VGA mode graphics and you must always use the Ctrl-Alt key combination to release the mouse from a DOS or Windows 3.1x virtual machine.

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Caldera OpenLinux 2.2, 2.3 and 2.4 Installation Guidelines

The easiest method of installing OpenLinux 2.2, 2.3 or 2.4 in a virtual machine is to use the standard Caldera distribution CD. The notes below describe an installation using the standard distribution CD. However, installing OpenLinux 2.2, 2.3 or 2.4 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a directory for the new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the OpenLinux 2.2, 2.3 or 2.4 installation, a generic VGA/SVGA X server is installed. After the installation is complete, the X server starts automatically, but the virtual machine screen is cropped and unusable. To get a working X server running inside the virtual machine, you should install VMware Tools immediately after installing OpenLinux 2.2, 2.3 or 2.4.

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the OpenLinux 2.2, 2.3 or 2.4 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. **Windows host only:** In the second OpenLinux 2.2, 2.3, or 2.4 installation screen, titled Set Up Mouse, the mouse cursor in the virtual machine does not move when the physical mouse is moved. To work around this problem, use the Tab and arrow keys to change the default mouse and button settings from **PS/2 mouse** and **Standard without wheel** to something else. Immediately, change both settings back to the original settings. The mouse should work after that.
3. At the Mouse and Keyboard selection screens, use the install program's default settings without making changes.

   At the Video Card selection screen, choose **Generic VGA compatible videocard**.

   At the Monitor and Video Mode selection screen, use the default settings.

   Note: It is not necessary to use the **Probe** or **Test Mode** button at the Video Card or Video Mode selection screens. If you use the buttons, ignore the results and click **Next** to continue with the installation.

4. If the virtual machine's Ethernet adapter has been enabled, the OpenLinux install program auto-loads the correct driver. You need to choose between DHCP and static IP addressing. You must provide the hostname parameter in either case.
5. Finish installing OpenLinux 2.2, 2.3 or 2.4 as you would on a physical PC.

   At this point OpenLinux 2.2, 2.3 or 2.4 boots and presents a log-on screen. As you may notice, the dialog box is cropped inside the virtual machine window. Install VMware Tools inside the virtual machine to provide support for the full screen resolution.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Caldera OpenLinux 1.3 and Earlier Installation Guidelines

Before installing the operating system, be sure that you have already created a directory for the new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Installation Tips

At the beginning of the installation process, OpenLinux appears to detect no devices at all (no CD-ROMs, hard drives, or network cards). Do not be concerned; just continue with the installation as usual.

The virtual machine may complain about illegal opcodes. This is a known issue. You should be able to install OpenLinux as a guest operating system despite this.

The virtual machine automatically attempts to boot from the hard disk before the CD. As a result, when OpenLinux reboots your machine after partitioning and formatting the hard drive, it appears that the machine does nothing after the BIOS splash screen (that is, the screen is blank). To fix this, go into the BIOS setup during boot (click inside the VMware Workstation window, then press F2). Go to the Boot menu and press the + key to move the CD-ROM (or your bootable media) option above the hard drive option. Now save the BIOS options and reboot. The installation should now continue normally.

To enable networking during the installation, follow these steps:

1. In the LISA setup screen, select **Yes** for the **Automatic Network Configuration** option.
2. Answer **No** when you are asked if all hardware was recognized.
3. In the Kernel Module Manager screen, select item **3 (Load Kernel Modules)**.
4. Select **Load driver for network card**.
5. Choose the **AMD PCI PCnet32 (PCI bus NE2100)**, then **Finish kernel module management**. Continue with the installation following Caldera's instructions. When installing LILO, be sure to install LILO onto the first hard drive and not onto the primary partition. Installing onto the primary partition causes LILO to fail to come up at boot time, resulting in a black, blank screen after the BIOS splash.

You can now set up networking as usual, following the Caldera instructions. Before you attempt to install VMware Tools, you need to install the glibc library. The glibc runtime library (`glibc-2.06-1.i386.rpm`) is located in the `col/contrib/RPMS` directory on the installation CD for OpenLinux 1.3.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Corel Linux OS 1.1, 1.2 Installation Guidelines

Before installing the operating system, be sure that you have already created a directory for the new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: These versions of Corel Linux are not supported. During the installation, the video resolution is set to 320X240 and the mouse does not move outside of the initial visible screen, which is only part of the entire display. Because of this, the installer cannot see all of the options needed for an installation. The workaround provided below lists the keystrokes necessary to perform a successful installation.

Installation steps

Note: These instructions have been created for an installation on a new (unpartitioned and unformatted) virtual disk The steps tell you what screen buttons or questions you would be able to see if you could see the entire screen, what the default option is for that installation step and what you actually need to type.

1. Screen buttons/question: Accept, Decline
   Default button: Accept
   You type: <Tab>, <Enter>
2. Screen buttons/question: User Name
   Default button: N/A
   You type: `<machinename>` (in lowercase and numbers only), <ENTER>
3. Screen buttons/question: Install Standard Desktop, Show Advanced Options
   Default button: Install Standard Desktop
   You type: <Enter>
4. Screen buttons/question: Take Over Disk, Use Free Disk Space, Edit Partition Table
   Default button: Use Free Disk Space
   You type: <Tab> <Space> <Enter>
5. Screen buttons/question: Warning… erase all data, Yes, No
   Default button: Yes
   You type: <Enter>
6. Screen buttons/question: Ready to Install…
   Default button: N/A
   You type: <Tab> <Tab> <Tab> <Space>
7. When the installation begins, the lower left-hand corner of the screen displays "ting disk…" Wait a long time (approximately 30 minutes). The actual time

depends on the type of host system and the resources available on it. Reboot the virtual machine when prompted by the Corel installation procedure. (Be sure to remove the CD.)

8. **Corel Linux OS 1.1:** The next time you boot the virtual machine, choose **3. Linux-Console**. If you accidentally choose the default option, **1. Corel Linux**, the screen blinks at the command prompt. Reboot and choose option 3.

   Corel Linux OS 1.2: When you reboot, the guest operating system may display a login prompt on a blinking screen. If this happens, click Reset on the Workstation toolbar. The next time the virtual machine boots, choose **4. Linux-Text Mode**. If you accidentally choose the default option, **1. Corel Linux**, the screen blinks at the command prompt. Reboot and choose option 4.
9. Log on as root.
10. Follow the directions for installing VMware Tools (see Installing VMware Tools on page 84) until you reach the point where you are instructed to run `./install.pl`.

    Instead, type

    ```
    ./install.pl other
    ```

    and press Enter.
11. After VMware Tools is installed, log out of the root account.

    ```
    exit
    ```

    Corel Linux OS configures your system, then launches the graphical interface, using the VMware SVGA driver.
12. Launch the VMware Tools background application.

    ```
    /usr/X11R6/bin/vmware-toolbox &
    ```

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Corel Linux OS 1.0 Installation Guidelines

Before installing the operating system, be sure that you have already created a directory for the new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Installation Tips

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Corel Linux OS installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Put the CD in the CD-ROM drive and click the **Power On** button.
3. Follow the installation steps as you would for a physical PC.

VMware Tools

1. After the first section of the installation is complete, Corel Linux OS asks you to click a button to restart the computer. Click the button.
2. When the virtual machine restarts, you see a graphical menu with five choices. Click inside the virtual machine window, use the arrow keys to select **3. Linux – Console**, then press Enter.
3. Corel Linux OS displays various messages, then pauses, with the last two lines on the screen reading
   Give root password for maintenance
   (or type Control-D for normal startup)

   At this point, there is no password for the root account. Press Enter to log on as root.
4. Press Ctrl-Alt to release the mouse from the virtual machine. In the VMware Workstation window, select **Settings** > **VMware Tools Install…**. When asked whether you want to see the help for VMware Tools installation, click **Yes**.
5. Click inside the VMware Workstation window so VMware Workstation grabs the mouse and keyboard.
6. Follow the directions for installing VMware Tools (see Installing VMware Tools on page 84) until you reach the point where you are instructed to run `./install.pl`.

Instead, type

```
./install.pl other
```

and press Enter.

7. After VMware Tools is installed, log out of the root account.

   ```
   exit
   ```

   Corel Linux OS configures your system, then launches the graphical interface, using the VMware SVGA driver.

8. Launch the VMware Tools background application.

   ```
   /usr/X11R6/bin/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`).

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Mandrake Linux 8.2 Installation Guidelines

The easiest method of installing Mandrake Linux 8.2 in a virtual machine is to use the standard Mandrake Linux distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Mandrake Linux 8.2 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a directory for the new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the Mandrake Linux 8.2 installation, you are offered a choice of XFree86 X servers. You may choose either one, but do not run that X server. Instead, to get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Mandrake Linux 8.2.

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Mandrake Linux 8.2 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. You may also want to increase the virtual machine's memory to 64MB. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Mandrake Linux 8.2 CD in the CD-ROM drive and click the **Power On** button.
3. Follow the installation steps as you would for a physical machine. Be sure to make the choices outlined in the following steps.
4. Use the Expert installer.
5. In the partitioning step, unless you have special requirements, it is all right to let Mandrake Linux auto-allocate the space.
6. When selecting a boot loader, use **LILO with text menu**. Do not use the graphical version of LILO. It causes the virtual machine to hang.
7. Do not create a custom boot disk when prompted.
8. You are offerred a choice of 2 XFree86 X servers to install. Choose **XFree 4.2.0**. This driver recognizes the VMware SVGA driver.

9. Near the end of the installation, after files have been copied, you reach the monitor setup screen. Choose the resolution and refresh rate you want your guest to use.
10. When the installer asks if you want to test the configuration, answer No.
11. When the installer asks if you want to install updates to the kernel, answer No.
12. When the installer asks whether to start X when you reboot, answer **No**.

This completes basic installation of the Mandrake Linux 8.2 guest operating system.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84.

Note: With a Mandrake Linux 8.2 guest, you should install VMware Tools from the Linux console. Do not start X until you have installed VMware Tools.

Note: Provided you installed the XFree 4.2.0 X server when you installed the guest operating system (as advised in the install steps), when you start the VMware Tools installation script (by typing `./install.pl` in the `vmware-linux-tools` directory), the following message appears:

```
Found an installed version of the VMware SVGA driver for
XFree86 4. Some versions of this driver included with the
XFree86 4 distributions do not work properly. Would you
like to install a stable (but possibly older) version of
the driver over the currently installed one?
```

If you plan to dual-boot the virtual machine, answer **Yes** to allow the driver to be installed. Answer **Yes** again to back up the existing video driver files and also copy the `XF86Config-4.dist` file to `XF86Config-4.vm`. The latter file is used when dual-booting the virtual machine.

If you do not intend to dual-boot the virtual machine, answer **No** to keep the existing driver.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Mandrake Linux 8.0 and 8.1 Installation Guidelines

The easiest method of installing Mandrake Linux 8.0 or 8.1 in a virtual machine is to use the standard Mandrake Linux distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Mandrake Linux 8.0 or 8.1 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a directory for the new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the Mandrake Linux 8.0 or 8.1 installation, you are offered a choice of XFree86 X servers. You may choose either one, but do not run that X server. Instead, to get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Mandrake Linux 8.0 or 8.1.

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Mandrake Linux 8.0 or 8.1 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. You may also want to increase the virtual machine's memory to 64MB. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Mandrake Linux 8.0 or 8.1 CD in the CD-ROM drive and click the Power On button.
3. Follow the installation steps as you would for a physical machine. Be sure to make the choices outlined in the following steps.
4. Use the Expert installer.
5. In the partitioning step, unless you have special requirements, it is all right to let Mandrake Linux auto-allocate the space.
6. When selecting a boot loader, use LILO with text menu. Do not use the graphical version of LILO. It causes the virtual machine to hang.
7. On the Select a Graphic Card screen, choose Other > Generic VGA compatible.
8. Near the end of the installation, after files have been copied, you reach the monitor setup screen. Choose Super VGA, 800x600 @ 56 Hz.
9. When the installer asks whether to start X when you reboot, answer No.

This completes basic installation of the Mandrake Linux 8.0 or 8.1 guest operating system. But there are two additional steps that are vital if you want to run X in your virtual machine.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84.

Note: With a Mandrake Linux 8.0 or 8.1 guest, you should install VMware Tools from the Linux console. Do not start X until you have installed VMware Tools and carried out the final step in this guide.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

The shutdown process in the guest operating system may hang when shutting down the network interface because of the way the Mandrake Linux 8.0 shutdown script handles `dhcpd`. This problem does not occur with Mandrake Linux 8.1 guests.

Installation sometimes hangs at `running /sbin/loader` for no apparent reason. The hang is caused by a bug in early versions of the 2.4 Linux kernel. The bug has been fixed in kernel 2.4.5. Distributions based on this kernel should install without problems.

For earlier 2.4-series kernels, a workaround is available. Although the Linux kernel bug is not related to CD-ROM drives, the workaround involves changing a VMware configuration setting for the virtual DVD/CD-ROM drive.

Power off the virtual machine and close the VMware Workstation window. Open the virtual machine’s configuration file (`.vmx` file on a Windows host or `.cfg` file on a Linux host) in a text editor and add the following line:

```
cdrom.minvirtualtime=100
```

Save the file. Now you should be able to install the guest operating system as described above. After you finish installing the guest operating system, remove this setting from the configuration file, as it may have a performance impact.

Red Hat Linux 7.3 Installation Guidelines

The easiest method of installing Red Hat Linux 7.3 in a virtual machine is to use the standard Red Hat distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Red Hat Linux 7.3 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: You should not run the X server that is installed when you set up Red Hat Linux 7.3. Instead, to get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Red Hat Linux 7.3.

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Red Hat Linux 7.3 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Red Hat Linux 7.3 CD-ROM in the CD-ROM drive on your VMware Workstation host and power on the virtual machine.

   You need to install Red Hat Linux 7.3 using the text mode installer, which you may choose when you first boot the installer. At the Red Hat Linux 7.3 CD boot prompt, you are offered the following choices:

   ```
   To install or upgrade a system ... in graphical mode ...
   To install or upgrade a system ... in text mode, type: text <ENTER>.
   To enable expert mode, ...
   Use the function keys listed below ...
   ```

   To choose the text mode installer, type `text` and press Enter.
3. Follow the installation steps as you would for a physical machine. Be sure to make the choices outlined in the following steps.
4. In the Mouse Selection screen, choose **Generic – 3 Button Mouse (PS/2)** and select the **Emulate 3 Buttons?** option for three-button mouse support in the virtual machine.
5. Choose the language and keyboard, then in the Installation Type screen, choose either **Server** or **Workstation** for the installation type.

6. You may see a warning that says:
   `Bad partition table. The partition table on device sda is corrupted. To create new partitions, it must be initialized, causing the loss of ALL DATA on the drive.`
   This does not mean that anything is wrong with the hard drive on your physical computer. It simply means that the virtual hard drive in your virtual machine needs to be partitioned and formatted. Select the **Initialize** button and press Enter. Also note that `sda` appears in the message as the device name if the virtual disk in question is a SCSI disk; if the virtual disk is an IDE drive, `hda` appears in the message as the device name instead.
7. Allow automatic partitioning of the disk to occur in the Automatic Partitioning screen.
8. If your host operating system supports DHCP and is connected to a LAN, then in the Network Configuration screen, select the **Use bootp/dhcp** option.
9. In the Video Card Selection screen, choose any card from the list.
10. In the Video Card Configuration screen, choose **Skip X Configuration**.

This completes basic installation of the Red Hat Linux 7.3 guest operating system.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84. Do not start the X server in the guest operating system until you install VMware Tools.

Note: When you start installing VMware Tools (by typing `./install.pl` in the `vmware-linux-tools` directory), the following message appears:

```
Found an installed version of the VMware SVGA driver for
XFree86 4. Some versions of this driver included with the
XFree86 4 distributions do not work properly. Would you
like to install a stable (but possibly older) version of
the driver over the currently installed one?
```

If you plan to dual boot the virtual machine, answer **Yes** to allow the driver to be installed. Answer **Yes** again to back up the existing video driver files and also copy the `XF86Config-4.dist` file to `XF86Config-4.vm`. The latter file is used when dual booting the virtual machine.

If you do not intend to dual boot the virtual machine, answer **No** to keep the existing driver.

Known Issues

- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.
- VMware recommends you do not migrate a Red Hat Linux 7.3 virtual machine between hosts when one host is running on an AMD processor and the other is running on an Intel processor. During the Red Hat Linux 7.3 installation, Red Hat 7.3 chooses a kernel that is optimized for the specific processor on which it is running. The kernel may contain instructions that are only available for that processor. These instructions can have adverse effects when run on a host with the wrong type of processor. Thus, a Red Hat Linux 7.3 virtual machine created on a host with an AMD processor may not work if migrated to a host with an Intel processor. The reverse is true; a Red Hat Linux 7.3 virtual machine created on a host with an Intel processor may not work if migrated to a host with an AMD processor.

  This problem is not specific to virtual machines and would also occur on physical computers. For example, if you moved a hard drive with a Red Hat Linux 7.3 installation from an AMD machine to an Intel machine, you would experience problems trying to boot from that drive.

Red Hat Linux 7.1 and 7.2 Installation Guidelines

The easiest method of installing Red Hat Linux 7.1 or 7.2 in a virtual machine is to use the standard Red Hat distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Red Hat Linux 7.1 or 7.2 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a directory for the new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: You should not run the X server that is installed when you set up Red Hat Linux 7.1 or 7.2. Instead, to get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Red Hat Linux 7.1 or 7.2.

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Red Hat Linux 7.1 or 7.2 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Red Hat Linux 7.1 or 7.2 CD-ROM in the CD-ROM drive and power on the virtual machine.

   You need to install Red Hat Linux 7.1 or 7.2 using the text mode installer, which you may choose when you first boot the installer. At the Red Hat Linux 7.1 or 7.2 CD boot prompt, you are offered the following choices:

   ```
   To install or upgrade a system ... in graphical mode ...
   To install or upgrade a system ... in text mode, type: text <ENTER>.
   To enable expert mode, ...
   Use the function keys listed below ...
   ```
   To choose the text mode installer, type `text` followed by Enter.
3. Follow the installation steps as you would for a physical machine. Be sure to make the choices outlined in the following steps.
4. Choose the language and keyboard, then in the Installation Type screen, choose either **Server** or **Workstation** for the installation type.

   A warning appears that says:

   `Bad partition table. The partition table on device sda is corrupted. To create new partitions, it must be` `initialized, causing the loss of ALL DATA on the drive.`

This does not mean that anything is wrong with the hard drive on your physical computer. It simply means that the virtual hard drive in your virtual machine needs to be partitioned and formatted. Click the **Initialize** button and press Enter. Also note that `sda` appears in the message as the device name if the virtual disk in question is a SCSI disk; if the virtual disk is an IDE drive, `hda` appears in the message as the device name instead.

5. Allow automatic partitioning of the disk to occur in the Automatic Partitioning screen.
6. If your host operating system supports DHCP and is connected to a LAN, then in the Network Configuration screen, select the **Use bootp/dhcp** option.
7. In the Mouse Selection screen, choose **Generic – 3 Button Mouse (PS/2)** and select the **Emulate 3 Buttons?** option for three-button mouse support in the virtual machine.
8. In the Video Card Selection screen, choose the default selection.
9. During the configuration of the X server, select the defaults and proceed through this section as quickly as possible, as this X server is replaced by an X server specific to your guest operating system when you install VMware Tools in this virtual machine.
10. Continue to the Starting X screen and click the **Skip** button to skip testing the configuration.

This completes basic installation of the Red Hat Linux 7.1 or 7.2 guest operating system. Be sure to install VMware Tools in your virtual machine. For details, see Installing VMware Tools on page 84. This installs an X server specific to your Red Hat 7.1 or 7.2 guest operating system, as well as some other utilities. If you choose to keep the X server that was installed with Red Hat Linux 7.1 or 7.2, your virtual machine's graphics performance suffers. Do not start X until you have installed VMware Tools.

Known Issues

- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.
- Installation sometimes hangs at `running /sbin/loader` for no apparent reason. The hang is caused by a bug in early versions of the 2.4 Linux kernel. The bug has been fixed in kernel 2.4.5. Distributions based on this kernel should install without problems.

For earlier 2.4-series kernels, a workaround is available. Although the Linux kernel bug is not related to CD-ROM drives, the workaround involves changing a VMware configuration setting for the virtual DVD/CD-ROM drive.

Power off the virtual machine and close the VMware Workstation window. Open the virtual machine's configuration file (`.vmx` file on a Windows host or `.cfg` file on a Linux host) in a text editor and add the following line:

```
cdrom.minvirtualtime=100
```

Save the file. Now you should be able to install the guest operating system as described above. After you finish installing the guest operating system, remove this setting from the configuration file, as it may have a performance impact.

- VMware recommends you do not migrate a Red Hat Linux 7.2 virtual machine between hosts when one host is running on an AMD processor and the other is running on an Intel processor. During the Red Hat Linux 7.2 installation, Red Hat Linux 7.2 chooses a kernel that is optimized for the specific processor on which it is running. The kernel may contain instructions that are only available for that processor. These instructions can have adverse effects when run on a host with the wrong type of processor. Thus, a Red Hat Linux 7.2 virtual machine created on a host with an AMD processor may not work if migrated to a host with an Intel processor. The reverse is true; a Red Hat Linux 7.2 virtual machine created on a host with an Intel processor may not work if migrated to a host with an AMD processor.

  This problem is not specific to virtual machines and would also occur on physical computers. For example, if you moved a hard drive with a Red Hat Linux 7.2 installation from an AMD machine to an Intel machine, you would experience problems trying to boot from that drive.

Red Hat Linux 7.0 Installation Guidelines

The easiest method of installing Red Hat Linux 7.0 in a virtual machine is to use the standard Red Hat distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Red Hat Linux 7.0 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a directory for the new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: Due to VGA performance issues installing Red Hat 7.0 with the graphics mode installer, we highly recommend you install the operating system with the text mode installer. At the Red Hat 7.0 CD boot prompt, you are offered the following choices:

```
To install or upgrade a system ... in graphical mode ...
To install or upgrade a system ... in text mode, type: text <ENTER>.
To enable expert mode, ...
Use the function keys listed below ...
```

Choose the text mode installer by typing `text` followed by Enter.

Note: During the Red Hat Linux 7.0 text mode installation, a standard XFree86 version 4 server (without support for VMware SVGA or standard VGA) will be installed. Do not run that X server. Instead, to get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Red Hat Linux 7.0.

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Red Hat Linux 7.0 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Red Hat Linux 7.0 CD in the CD-ROM drive and click the **Power On** button.
3. Follow the installation steps as you would for a physical PC. Be sure to make the choices outlined in the following steps.
4. In Video Card Selection choose **Generic VGA compatible**, then click **OK**.

5. Near the end of the installation, after files have been copied, you reach the Monitor Setup screen. Choose **Generic Standard VGA, 640x480 @ 60 Hz**, then click **OK**.
6. At the Video Memory screen, choose **256Kb**, then click **OK.**
7. At the Clockchip Configuration screen, choose **No Clockchip Setting (recommended)**, which is the default, then click **OK**.
8. At the Probe for Clocks screen, click **Skip**.
9. At the Select Video Modes screen, don't choose anything. Just click **OK**.
10. At the Starting X screen, click **Skip**.

    Note: This is the most important step. Clicking **OK** runs the XFree86 version 4 server, which fails, and the installer aborts.

This completes basic installation of the Red Hat Linux 7.0 guest operating system.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84.

Note: With a Red Hat Linux 7.0 guest, you should install VMware Tools from the Linux console. Do not start X until you have installed VMware Tools.

Installing a 16-Color X Server

If you want to run the standard 16-color VGA X server, skip the installation of VMware Tools and instead take the following steps.

Note: If you use the standard 16-color VGA X server, you do not have the performance advantages of the accelerated SVGA X server included in VMware Tools.

1. After you finish the basic installation of the Red Hat Linux 7.0 guest operating system and the virtual machine reboots, log on as root.

    ```
    su
    ```

2. Set up the X server:

    ```
    ln -sf ../../usr/X11R6/bin/XF86_VGA16 /etc/X11/X
    ```

    This sets the current X server to `XF86_VGA16` (the XFree86 3.3.6 16-color VGA X server).

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Red Hat Linux 6.x Installation Guidelines

The easiest method of installing Red Hat Linux 6.x in a virtual machine is to use the standard Red Hat distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Red Hat Linux 6.x via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a directory for the new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Caution: Red Hat Linux 6.2 does not run on Pentium 4 processors. It also does not run on Xeon processors that are branded Xeon, with no qualifier, or Xeon-MP (Pentium III Xeon processors are OK).

Note: Due to VGA performance issues installing Red Hat 6.1 and 6.2 with the graphics mode installer, we highly recommend you install the operating system with the text mode installer. At the Red Hat 6.1 or 6.2 CD boot prompt, you are offered the following choices:

```
To install or upgrade a system ... in graphical mode ...
To install or upgrade a system ... in text mode, type: text <ENTER>.
To enable expert mode, ...
Use the function keys listed below ...
```

Choose the text mode installer by typing `text` followed by Enter.

Note: During the Red Hat Linux 6.x installation, a standard VGA16 X server (without support for the VMware Workstation X server) is installed. To get an accelerated SVGA X server running inside the virtual machine, you should install the VMware Tools package immediately after installing Red Hat Linux 6.x.

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine’s devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Red Hat Linux 6.x installation process, be sure the virtual machine’s Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Red Hat Linux 6.x CD in the CD-ROM drive and click the **Power On** button.
3. Follow the installation steps as you would for a physical PC.

Note: If the virtual machine's Ethernet adapter has been enabled, the installation program auto-detects and loads the AMD PC/Net 32 driver (no command line parameter is necessary to load the driver).

Note: The text mode installer in Red Hat Linux 6.x presents a Hostname Configuration screen. If you are installing this guest with DHCP in a virtual machine with host-only networking, do not specify a host name. Just respond **OK** and continue. (Specifying a host name will cause an installer error later.) At the next screen — Network Configuration — respond **OK** to use the default: **Use bootp/dhcp**.

4. During the Linux installation, select the standard VGA16 X server. In the Choose a Card screen, select the **Generic VGA compatible/Generic VGA** card from the list. In the Monitor Setup screen, select **Generic Monitor** from the list. Select the **Probe** button from the Screen Configuration dialog box and select **OK** from the Starting X dialog box. After Linux is installed, you will replace the generic X server with the accelerated X server included in the VMware Tools package when you install VMware Tools.
5. Finish installing Red Hat Linux 6.x as you would on a physical PC.

At this point Red Hat 6.x boots and presents a log-on screen.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Red Hat Linux 5.x Installation Guidelines

Before installing the operating system, be sure that you have already created a directory for the new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Red Hat Linux 5.x installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Red Hat Linux 5.x CD in the CD-ROM drive and click **Power On**.
3. Follow the installation steps as you would for a physical PC.
4. Choose **PS/2 mouse** for your mouse configuration.
5. To set up your monitor:

   A. In the Choose a Card screen, select **Generic VGA Compatible**.

   B. In the Monitor Setup screen, select **Generic Monitor**.

   C. In the Screen Configuration screen, select **Probe**.

   Note: Initially, you have a VGA X server. When you install VMware Tools, after you finish installing Linux, you automatically replace the VGA X server with an accelerated SVGA X server.
6. The network card needs to be set up and configured as an AMD PC/Net 32 to give the virtual machine network connectivity.

   Select AMD PC/Net 32 as the network card. You do not need to add any optional parameters.
7. Install the bootloader in the master boot record in your virtual machine.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

SuSE Linux 8.0 Installation Guidelines

The easiest method of installing SuSE Linux 8.0 in a virtual machine is to use the standard SuSE distribution CDs. The notes below describe an installation using the standard distribution CD; however, installing SuSE Linux 8.0 via the boot floppy/ network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Caution: During the SuSE Linux 8.0 installation, do **not** install an X server. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SuSE Linux 8.0.

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the SuSE Linux 8.0 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the SuSE Linux 8.0 installation CD in the CD-ROM drive on your VMware Workstation host and click the **Power On** button.
3. Follow the installation steps as you would for a physical machine, until you get to the selection screens described in the next steps.
4. Install using the text mode installer.
5. When prompted, do **not** install an X server. In the Configure Monitor screen, choose No X11. The installer asks you to confirm. Click Continue and finish the installation.
6. At the end of the installation, install VMware Tools in your guest operating system. For details, see VMware Tools below.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84. Do not start the X server in the guest operating system until you install VMware Tools.

Note: When you start installing VMware Tools (by typing `./install.pl` in the `vmware-linux-tools` directory), the following message appears:

```
Found an installed version of the VMware SVGA driver for
XFree86 4. Some versions of this driver included with the
XFree86 4 distributions do not work properly. Would you
like to install a stable (but possibly older) version of
the driver over the currently installed one?
```

If you plan to dual-boot the virtual machine, answer **Yes** to allow the driver to be installed. Answer **Yes** again to back up the existing video driver files and also copy the `XF86Config-4.dist` file to `XF86Config-4.vm`. The latter file is used when dual-booting the virtual machine.

If you do not intend to dual-boot the virtual machine, answer **No** to keep the existing driver.

Before You Start the X Server

After you have installed VMware Tools, but before you start the X server, as root user, run the SaX2 configuration utility to configure your X server. At a command prompt, type `SaX2` and use the wizard to configure your X server.

After you run SaX2 you may boot your SuSE 8.0 virtual machine with any of the selections offered in LILO.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

SuSE Linux Enterprise Server 7 Installation Guidelines

The easiest method of installing SuSE Linux Entierprise Server 7 (SLES 7) in a virtual machine is to use the standard SuSE distribution CDs. The notes below describe an installation using the standard distribution CD; however, installing SLES 7 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the SLES 7 installation, a standard VGA16 X server (without support for the VMware Workstation X server) should be installed. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SLES 7.

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the SLES 7 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert theSLES 7 installation CD in the CD-ROM drive and click the **Power On** button.
3. Follow the installation steps as you would for a physical machine, until you get to the selection screens described in the next step.
4. Part way through the installation, the installer reboots the virtual machine. At the LILO screen, let the boot proceed using the default selection of `linux`.
5. At the Desktop Settings screen, select **640x480 256 colors**.
6. Finish installing SLES 7 as you would on a physical machine.
7. At the end of the installation, install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

SuSE Linux 7.3 Installation Guidelines

The easiest method of installing SuSE Linux 7.3 in a virtual machine is to use the standard SuSE distribution CDs. The notes below describe an installation using the standard distribution CD; however, installing SuSE Linux 7.3 via the boot floppy/ network method is supported as well.

Before installing the operating system, be sure that you have already created a directory for the new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Caution: During the SuSE Linux 7.3 installation, do **not** install an X server. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SuSE Linux 7.3.

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the SuSE Linux 7.3 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the SuSE Linux 7.3 installation CD in the CD-ROM drive and click the **Power On** button.
3. Follow the installation steps as you would for a physical machine, until you get to the selection screens described in the next steps.
4. Install using the the text mode installer.
5. When prompted, do **not** install an X server. In the Configure Monitor screen, choose No X11. The installer asks you to confirm. Click Continue and finish the installation.
6. At the end of the installation, install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84.
7. Before you start the X server, as root user, run the SaX2 configuration utility to configure your X server.
8. After you have installed VMware Tools and run SaX2, you may boot your SuSE 7.3 virtual machine with any of the selections offered in LILO.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

SuSE Linux 7.2 Installation Guidelines

The easiest method of installing SuSE Linux 7.2 in a virtual machine is to use the standard SuSE distribution CDs. The notes below describe an installation using the standard distribution CD; however, installing SuSE Linux 7.2 via the boot floppy/ network method is supported as well.

Before installing the operating system, be sure that you have already created a directory for the new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the SuSE Linux 7.2 installation, a standard VGA16 X server (without support for the VMware Workstation X server) should be installed. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SuSE Linux 7.2.

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the SuSE Linux 7.2 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the SuSE Linux 7.2 installation CD in the CD-ROM drive and click the **Power On** button.
3. Follow the installation steps as you would for a physical machine, until you get to the selection screens described in the next step.
4. You are offered a choice of Linux kernels to install. Kernel 2.2.18 is selected by default. Be sure to leave it selected. If you want to use kernel 2.4 in your virtual machine, select both.
5. Part way through the installation, the installer reboots the virtual machine. At the LILO screen, let the boot proceed using the default selection of `linux` to use the 2.2.18 kernel.
6. At the Desktop Settings screen, select **640x480 256 colors**.
7. Finish installing SuSE Linux 7.2 as you would on a physical machine.
8. At the end of the installation, install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84.

9. Before you start the X server, as root user, run the SaX2 configuration utility to configure your X server.
10. After you have installed VMware Tools and run SaX2, you may boot your SuSE 7.2 virtual machine with any of the selections offered in LILO.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

SuSE Linux 7.1 Installation Guidelines

The easiest method of installing SuSE Linux 7.1 in a virtual machine is to use the standard SuSE distribution CDs. The notes below describe an installation using the standard distribution CD; however, installing SuSE Linux 7.1 via the boot floppy/ network method is supported as well.

Before installing the operating system, be sure that you have already created a directory for the new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the SuSE Linux 7.1 installation, a standard VGA16 X server (without support for the VMware Workstation X server) should be installed. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SuSE Linux 7.1.

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the SuSE Linux 7.1 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the SuSE Linux 7.1 installation CD in the CD-ROM drive and click the **Power On** button.
3. Use the graphical installer and follow the installation steps as you would for a physical machine, until you get to the selection screens described in the next step.
4. You are offered a choice of Linux kernels to install. Kernel 2.2.18 is selected by default. Be sure to leave it selected. If you want to use kernel 2.4 in your virtual machine, select both.
5. Part way through the installation, the installer reboots the virtual machine. At the LILO screen, let the boot proceed using the default selection of `linux` to use the 2.2.18 kernel.
6. At the Desktop Settings screen, select **640x480 256 colors**.
7. Finish installing SuSE Linux 7.1 as you would on a physical machine.

At the end of the installation, boot again using the default LILO selection of `linux`, then install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84.

8. After you have installed VMware Tools, you may boot your SuSE 7.1 virtual machine with any of the selections offered in LILO.

Known Issues

- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.
- When you are installing SuSE Linux 7.1 in text mode and the guest operating system reboots for the first time, the Linux boot sequence reaches “Starting syslog system,” then the display turns completely black and the guest appears to be hung.

  Despite its appearance, the guest operating system actually is not hung; instead, the screen is not being displayed. To see the screen and continue with the installation, in the guest operating system, switch to Linux virtual console 2. Press Ctrl-Alt, press and release the spacebar, then press F2.

  Then return to virtual console 1. Press Ctrl-Alt, press and release the spacebar, then press F1. You should be able to see the screen and continue installing the guest operating system.

  Note: If you are using a different hot-key combination, use that in place of Ctrl-Alt above.

  Note: This problem appears only when you install the guest operating system in text mode.

SuSE Linux 7.0 Installation Guidelines

The easiest method of installing SuSE Linux 7.0 in a virtual machine is to use the standard SuSE distribution CDs. The notes below describe an installation using the standard distribution CD; however, installing SuSE Linux 7.0 via the boot floppy/network method is supported as well.

Before installing the operating system, be sure that you have already created a directory for the new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the SuSE Linux 7.0 installation, a standard VGA16 X server (without support for the VMware Workstation X server) should be installed. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing SuSE Linux 7.0.

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the SuSE Linux 7.1 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. Be sure the virtual machine's memory is set to at least 64MB. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the SuSE Linux 7.0 installation CD in the CD-ROM drive and click the Power On button.
3. Use the graphical installer and follow the installation steps as you would for a physical machine.
4. In the Desktop Settings screen, select **640x480 256 colors**.
5. Finish installing SuSE Linux 7.0 as you would on a physical machine.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84.

Known Issues

- On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

- When you are installing SuSE Linux 7.0 in text mode and the guest operating system reboots for the first time, the Linux boot sequence reaches “Keytable US,” then the display turns completely black and the guest appears to be hung.

  Despite its appearance, the guest operating system actually is not hung; instead, the screen is not being displayed. To see the screen and continue with the installation, in the guest operating system, switch to Linux virtual console 2. Press Ctrl-Alt, press and release the spacebar, then press F2.

  Then return to virtual console 1. Press Ctrl-Alt, press and release the spacebar, then press F1. You should be able to see the screen and continue installing the guest operating system.

  Note: If you are using a different hot-key combination, use that in place of Ctrl-Alt above.

  Note: This problem appears only when you install the guest operating system in text mode.

Turbolinux 7.0 Installation Guidelines

The easiest method of installing Turbolinux 7.0 in a virtual machine is to use the standard Turbolinux 7.0 distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Turbolinux 7.0 via the boot floppy/network method is supported as well.

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 (on Windows hosts) or Configuration Wizard (on Linux hosts).

Note: During the Turbolinux 7.0 installation, a standard VGA16 X server (without support for the VMware Workstation X server) is installed. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing Turbolinux 7.0, before you start the X server.

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Turbolinux 7.0 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Turbolinux 7.0 CD No. 1 in the CD-ROM drive on your VMware Workstation host and click the **Power On** button.
3. Follow the installation steps as you would for a physical PC, until you get to the selection screen described in the next step.
4. In the Configure Monitor screen, follow the defaults to configure an X server. This is necessary even though you will install a different X server with VMware Tools after you finish installing the guest operating system.
5. Finish installing Turbolinux 7.0 as you would on a physical PC.

At this point Turbolinux 7.0 boots and a login screen appears.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84. Do not start the X server in the guest operating system until you install VMware Tools.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

Turbolinux 6.0 Installation Guidelines

The easiest method of installing Turbolinux 6.0 in a virtual machine is to use the standard Turbolinux distribution CD. The notes below describe an installation using the standard distribution CD; however, installing Turbolinux 6.0 via the boot floppy/network method is supported as well.

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 (on Windows hosts) or Configuration Wizard (on Linux hosts).

Caution: Do not install Turbolinux 6.0 on a Pentium 4 host.

Note: During the Turbolinux 6.0 installation, a standard VGA16 X server (without support for the VMware Workstation X server) is installed. To get an accelerated SVGA X server running inside the virtual machine, install the VMware Tools package immediately after installing Turbolinux 6.0.

Installation Steps

1. Use the VMware Workstation Configuration Editor to verify the virtual machine's devices are set up as you expect before starting the installation. For example, if you would like networking software to be installed during the Turbolinux 6.0 installation process, be sure the virtual machine's Ethernet adapter is enabled and configured. VMware also recommends that you disable the screen saver on the host system before starting the installation process.
2. Insert the Turbolinux 6.0 CD in the CD-ROM drive on your VMware Workstation host and click the **Power On** button.
3. Follow the installation steps as you would for a physical PC, until you get to the selection screens described in the next steps.
4. In the Configure Video Card screen, select the defaults for the X server.
5. In the Configure X Server screen, click **Skip**. You must not configure this X server. When you install VMware Tools, an X server is installed that is optimized for running in your virtual machine.
6. Finish installing Turbolinux 6.0 as you would on a physical PC.

At this point Turbolinux 6.0 boots and a login screen appears.

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84. Do not start the X server in the guest operating system until you install VMware Tools.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

FreeBSD as a Guest Operating System

Before installing the operating system, be sure that you have already created a directory for the new virtual machine and configured it using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts).

Various versions and distributions of FreeBSD have been tested with the current VMware Workstation distribution. The 3.x and 4.0 through 4.6 distributions of FreeBSD — specifically 3.1, 4.0, 4.1, 4.2, 4.3, 4.4, 4.5 and 4.6 — are fully functional. Floppy, CD-ROM and network devices autoconfigure and work.

Installation of FreeBSD 4.6 may hang while probing devices. To work around this problem, use a text editor to add the following line to the virtual machine's configuration (`.vmx` or `.cfg`) file:

```
cdrom.minVirtualTime=100
```

After you finish installing the guest operating system, remove this setting from the configuration file, as it may have a performance impact.

The issue addressed by this workaround has been resolved in FreeBSD 4.6.2. You do not need to take any special steps to install FreeBSD 4.6.2.

Versions of FreeBSD older than 4.4 do not boot if the operating system has been installed on a 2GB or larger SCSI virtual disk. To correct this issue, you need to set the disk geometry for the SCSI virtual disk.

Setting the Disk Geometry for a FreeBSD SCSI Virtual Disk

If you are running a virtual machine with some versions of FreeBSD as the guest operating system on a 2GB or larger SCSI virtual disk, the guest operating system does not boot.

It fails to boot because the virtual disk geometry is not probed correctly by FreeBSD when you install the guest operating system. FreeBSD installs the boot loader in the wrong location on the virtual disk. When FreeBSD tries to boot, the FreeBSD boot loader asks the BIOS for important data that is now on a different section of the virtual disk, so FreeBSD cannot boot.

This problem has been fixed in FreeBSD 4.4. This and later versions correctly boot SCSI virtual disks of any size.

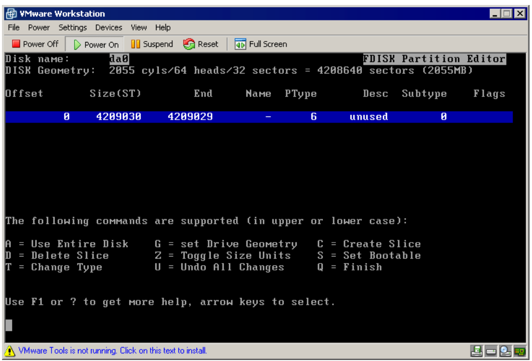
To use an older version of FreeBSD in your virtual machine, you can do one of two things:

- Use an IDE virtual disk in your virtual machine. You may need to add the IDE virtual disk to the virtual machine with the Configuration Editor.

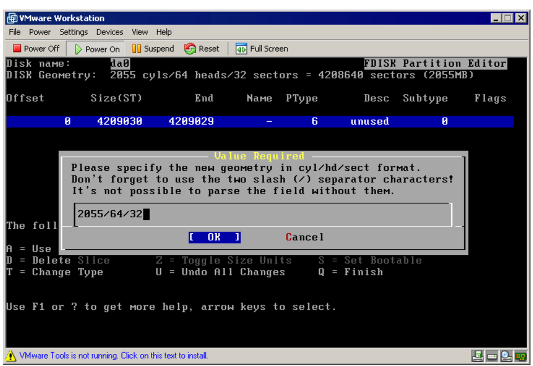
- Set the disk geometry by hand when installing FreeBSD. These steps are outlined below.

To set the disk geometry manually, complete these steps.

1. FreeBSD calculates an incorrect disk geometry before you arrive at the FDISK Partition Editor, as illustrated here.



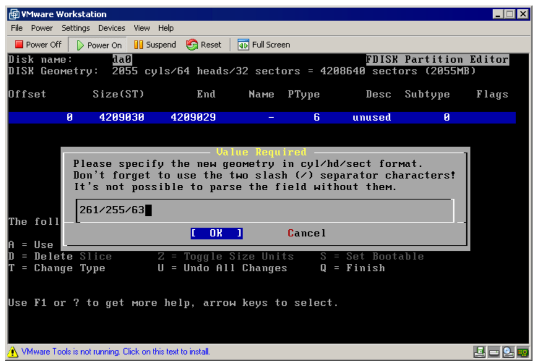
2. To set the disk geometry, press G to select the Set Drive Geometry option. A dialog box appears, containing numbers like 2055/64/32, representing the incorrect geometry in cylinders, heads and sectors per head.



3. To calculate the correct geometry, find the total number of sectors by multiplying the number of cylinders, heads and sectors per head together, then dividing the number of sectors by the correct number of heads and sectors per head.

In the above illustration, the virtual disk is a 2055MB disk with 2055 cylinders, 64 heads and 32 sectors per head (these numbers represent the incorrect geometry). The product of these three numbers (2055 x 64 x 32) equals 4,208,640 sectors.

To determine the correct geometry for the BusLogic compatible virtual SCSI adapter used by VMware Workstation, calculate the number of cylinders, which is 4,208,640 sectors divided by the product of the actual number of heads and sectors per head (255 heads times 63 sectors per head). This results in a total of 261 actual cylinders (4208640/(255 * 63) = 261, rounded down).



4. You can now enter the correct geometry of 261 cylinders, 255 heads and 63 sectors per head by typing `261/255/63` in the dialog box. Then click **OK** and continue installing FreeBSD.

Other Issues with FreeBSD Guest Operating Systems

- FreeBSD 4.4 installs only from CD-ROM, and not from an ISO image.

  Note: With all versions of FreeBSD there is a problem probing for the CD-ROM device `wdc1`. FreeBSD sends an illegal ATAPI command to the IDE controller and ignores the error status reply. This results in a delay of approximately one-minute each time the system boots.

- VMware has not tested sound support in FreeBSD.

- The Linux emulation support in FreeBSD 3.1 is insufficient to run the X server provided by VMware for use on Linux systems running in a virtual machine. The VGA server distributed with FreeBSD works as expected.

- The generic FreeBSD kernel works well. Users who want to configure a kernel specifically for use in a virtual machine can use a configuration file like the one below. Note that this file was created for FreeBSD 3.1.

```
#
# VMWARE -- Workstation virtual machine
#
# For more information read the handbook part System Administration ->
# Configuring the FreeBSD Kernel -> The Configuration File.
# The handbook is available in /usr/share/doc/handbook or online as
# latest version from the FreeBSD World Wide Web server
# <URL:http://www.FreeBSD.ORG/ >
#
# An exhaustive list of options and more detailed explanations of the
# device lines is present in the ./LINT configuration file. If you are
# in doubt as to the purpose or necessity of a line, check first in LINT.
#

machine "i386"
cpu "I686_CPU"
ident VMWARE
maxusers 32

options INET #InterNETworking
options FFS #Berkeley Fast Filesystem
options FFS_ROOT #FFS usable as root device [keep this!]
options MFS #Memory Filesystem
options MFS_ROOT #MFS usable as root device, "MFS" req'ed
options NFS #Network Filesystem
options NFS_ROOT #NFS usable as root device, "NFS" req'ed
options MSDOSFS #MSDOS Filesystem
options "CD9660" #ISO 9660 Filesystem
options "CD9660_ROOT" #CD-ROM usable as root. "CD9660"req'ed
options PROCFS #Process filesystem
options "COMPAT_43" #Compatible with BSD 4.3 [KEEP THIS!]
options UCONSOLE #Allow users to grab the console
options FAILSAFE #Be conservative
options USERCONFIG #boot -c editor
options VISUAL_USERCONFIG #visual boot -c editor

config kernel root on wd0

# To make an SMP kernel, the next two are needed
#options SMP # Symmetric MultiProcessor Kernel
#options APIC_IO # Symmetric (APIC) I/O
# Optionally these may need tweaked, (defaults shown):
```

```
#options NCPU=2 # number of CPUs
#options NBUS=4 # number of busses
#options NAPIC=1 # number of IO APICs
#options NINTR=24 # number of INTs

controller isa0
controller eisa0
controller pci0

controller fdc0 at isa? port "IO_FD1" bio irq 6 drq 2
disk fd0 at fdc0 drive 0
disk fd1 at fdc0 drive 1

controller wdc0 at isa? port "IO_WD1" bio irq 14
disk wd0 at wdc0 drive 0
disk wd1 at wdc0 drive 1

controller wdc1 at isa? port "IO_WD2" bio irq 15
disk wd2 at wdc1 drive 0
disk wd3 at wdc1 drive 1

options ATAPI #Enable ATAPI support for IDE bus
options ATAPI_STATIC #Don't do it as an LKM
device acd0 #IDE CD-ROM
device wfd0 #IDE Floppy (e.g. LS-120)

device wt0 at isa? port 0x300 bio irq 5 drq 1

# atkbdc0 controls both the keyboard and the PS/2 mouse
controller atkbdc0 at isa? port IO_KBD tty
device atkbd0 at isa? tty irq 1
device psm0 at isa? tty irq 12

device vga0 at isa? port ? conflicts

# splash screen/screen saver
pseudo-device splash

# syscons is the default console driver, resembling an SCO console
device sc0 at isa? tty
# Enable this and PCVT_FREEBSD for pcvt vt220 compatible console driver
#device vt0 at isa? tty
#options XSERVER # support for X server
#options FAT_CURSOR # start with block cursor

device npx0 at isa? port IO_NPX irq 13
```

```
#
# Laptop support (see LINT for more options)
#
device apm0 at isa? disable flags 0x31 # Advanced Power Management

device sio0 at isa? port "IO_COM1" flags 0x10 tty irq 4
device sio1 at isa? port "IO_COM2" tty irq 3
device sio2 at isa? disable port "IO_COM3" tty irq 5
device sio3 at isa? disable port "IO_COM4" tty irq 9

# Parallel port
device ppc0 at isa? port? net irq 7
controller ppbus0
device nlpt0 at ppbus?
device plip0 at ppbus?
device ppi0 at ppbus?
#controller vpo0 at ppbus?

#device lnc0 at isa? port 0x1000 net irq 10 drq 0
device lnc0 # probe on PCI

pseudo-device loop
pseudo-device ether
pseudo-device sl 1
pseudo-device ppp 1
pseudo-device tun 1
pseudo-device pty 16
pseudo-device gzip # Exec gzipped a.out's

# KTRACE enables the system-call tracing facility ktrace(2).
# This adds 4 KB bloat to your kernel, and slightly increases
# the costs of each syscall.
options KTRACE #kernel tracing

# This provides support for System V shared memory and message queues.
#
options SYSVSHM
options SYSVMSG

# The `bpfilter' pseudo-device enables the Berkeley Packet Filter. Be
# aware of the legal and administrative consequences of enabling this
# option. The number of devices determines the maximum number of
# simultaneous BPF clients programs runnable.
#pseudo-device bpfilter 4 #Berkeley packet filter
```

VMware Tools

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools on page 84.

Known Issues

On a Linux host with an XFree86 3.x X server, it is best not to run a screen saver in the guest operating system. Guest screen savers that demand a lot of processing power can cause the X server on the host to freeze.

NetWare 6.0 Server Installation Guidelines

Note: Support for Novell NetWare 6.0 as a guest operating system is experimental at this time.

You can install NetWare 6.0 in a virtual machine using the standard Novell NetWare 6.0 CD-ROM.

Before installing the operating system, keep the following issues in mind:

- VMware recommends you install NetWare 6 on a host with at least 384MB of memory.
- Change the color settings of your host system to 256 Colors (8 bit).

  If you are using Windows XP host, you can set up the compatibility mode for the VMware Workstation executable (`vmware.exe`) to 256 colors. To do so, go to the folder where you installed VMware Workstation. Right-click `vmware.exe`, select **Properties** and select **256 compatibility**.
- 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. To prevent unnecessary slowdowns, VMware recommends that you download the NetWare 5 CPU idle program from *www.vmware.com/software/Nw5-idle.nlm* and copy it to a floppy disk for use during the installation.

Installation Steps

To install NetWare 6 in a virtual machine, take the following steps.

1. Create a new virtual machine using the VMware Workstation New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts). For the most part, you can choose your own settings, except as noted below.
   A. For the type of configuration, select **Custom**.
   B. For the guest operating system, select **NetWare 6.0 (experimental)**.
   C. Keep the memory setting for the virtual machine at its default of 256MB.
   D. Create a new virtual disk no smaller than the default size of 4GB.
2. After you finish creating the new virtual machine, choose **Settings** > **Configuration Editor** and remove both USB controllers.
3. Begin installing the NetWare 6.0 guest operating system. Insert the Novell NetWare 6.0 CD-ROM and power on the virtual machine.
4. Read and accept the license agreement.

5. When prompted, choose **IDE CD-ROM**.
6. Create a new boot partition. The guest operating system reboots.
7. The installation continues. When the installer finishes copying the files, insert floppy containing the `NW5-IDLE.NLM` file.
   A. Press Ctrl-Esc to see all screens available in the virtual machine, and choose System Console.
   B. At the command prompt, type
   `LOAD: A\NW5-IDLE.NLM`
   C. Press Alt-Esc to return to the installation.
8. To configure IP networking, do one of the following:
   - If you chose bridged networking for the virtual machine, enter its IP address. When NetWare tries to load the LAN driver (using `pcntnw.lan`), it fails because it broadcasts for its own IP address. This causes IP networking to fail. To work around this, open the System Console (press Ctrl-Esc) and type
   `set allow ip address duplicates=on`
   Press Alt-Esc to return to the installation.
   - If you chose host-only networking for the virtual machine, look up the host machine's IP address. At a command prompt on the host, type
   `ipconfig /all`
   Note the host’s IP address for VMnet1 and change the last number so it is greater than the last octal in the IP address of the host.
   For example, if the host IP address is 192.168.160.1, then the virtual machine’s IP address is 192.168.160.###, where ### is any number greater than 1 and less than 128.
   For the subnet mask, enter 255.255.255.0.
   For the router gateway, enter the host’s IP adddress (192.168.80.1 in our example).
   - If you chose network address translation for the virtual machine, look up the host machine's IP address. At a command prompt on the host, type
   `ipconfig /all`
   Note the host’s IP address for VMnet8 and change the last number so it is greater than the last octal in the IP address of the host.
   For example, if the host IP address is 192.168.160.2, then the virtual machine’s IP address is 192.168.160.###, where ### is any number greater than 2 and less than 128.
   For the subnet mask, enter 255.255.255.0.

For the router gateway, enter the host's IP adddress (192.168.80.2 in our example).

9. Finish the installation.
10. After you complete the installation, copy the `NW5-IDLE.NLM` file to `SYS:SYSTEM` and `C:\NWSERVER` in the guest operating system.
11. Edit the `autoexec.ncf` file and add a line that loads `NW5-IDLE.NLM`.
    `load c:\nwserver\nw5-idle.nlm`
12. Now that you have the guest operating system installed, you can change the color setting of your host back its original setting.

VMware Tools for NetWare 6.0 Guest Operating Systems

Be sure to install VMware Tools in your guest operating system. For details, see Installing VMware Tools in a NetWare Virtual Machine on page 91.

Known Issues

- The VMware Tools feature that synchronizes the time between the host and guest operating systems does not work with NetWare 6.0. This issue may be resolved in the next NetWare 6.0 support pack that Novell will release.

8

Using Disks

Using Disks in a Virtual Machine

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 (on Windows hosts) or Configuration Wizard (on Linux hosts) creates a virtual machine with one disk drive. You can use the Configuration Editor (**Settings** > **Configuration Editor**) 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 Raw

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 known 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. VMware Workstation creates a file for each 2GB of virtual disk capacity and virtual machine overhead. The actual files used by the virtual disk start out small and grow to their maximum size as needed.

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 BusLogic SCSI adapter used in a VMware Workstation virtual machine.

Note: To use SCSI disks in a Windows XP or Windows .NET Server 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 .NET Server.

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 126

Note: Beginning with VMware Workstation 3.0, virtual disks are created in a new format that is not recognized by earlier VMware products. Future versions of other VMware products will support this new virtual disk format.

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, the switch to running it inside a virtual machine 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 237.

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 265. In most cases, however, it is better to use a virtual disk.

Only expert users should attempt raw disk configurations.

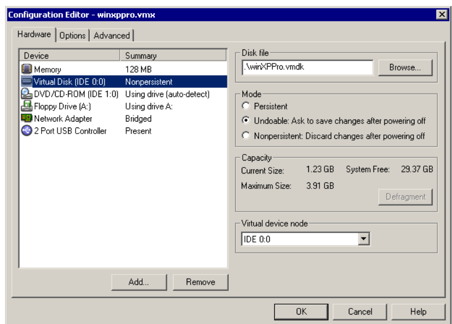
Plain Disk

VMware Workstation 2.0 offered an experimental disk type called plain disk. In VMware Workstation 2.0, virtual disks could be no larger than 2GB. Plain disks provided a way to create larger disks for the virtual machine. VMware Workstation 3.x allows you to create large disks — up to 256GB — as virtual disks. Consequently, this version does not support creation of new plain disks.

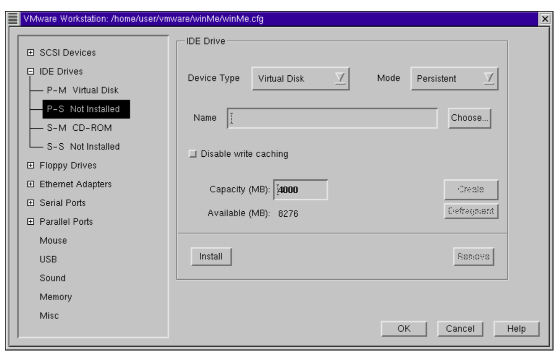
Virtual machines with plain disks created in VMware Workstation 2.0 do run under VMware Workstation 3.x.

Disk Modes: Persistent, Undoable and Nonpersistent

You can use the Configuration Editor (**Settings** > **Configuration Editor**) to configure disks in one of three modes: persistent, undoable and nonpersistent.



The Configuration Editor on a Windows host shows an IDE virtual disk configured as undoable



The Configuration Editor on a Linux host shows installation of an IDE virtual disk configured as persistent

Disk modes determine how changes are saved to the disk. Raw, virtual and plain disks can use any available mode. For example, a user could have an undoable raw disk, an undoable virtual disk or an undoable plain disk.

Persistent
Disks in persistent mode are the simplest to use. Disks in persistent mode behave like conventional disk drives on your physical computer. All data written to a disk in persistent mode are written out permanently to the disk. The behavior is the same for all disk types.

Undoable
Undoable mode lets you decide when you power off the virtual machine whether you want to keep or discard the changes made since the virtual machine was powered on. This is especially useful for experimenting with new configurations or unfamiliar software. Because of the disaster-recovery possibilities this mode offers, many users prefer to set disks in undoable mode as a standard part of their configurations.

When data is written to an undoable mode disk, the changes are stored in a file called a redo log. A disk in undoable mode gives you the option later of permanently applying the changes saved in the redo log, so they become part of the main disk files.

While the virtual machine is running, disk blocks that have been modified and written to the redo log are read from there instead of from the disk files.

Any disk type can be used in undoable mode.

When you power off a virtual machine with a disk in undoable mode, you are given three options:

- Commit the changes in the redo log to the disk
- Discard the changes in the redo log
- Keep the redo log

If you choose to keep the redo log, the next time you power on the virtual machine VMware Workstation detects the redo-log file and prompts you to either commit the redo log changes made from the last time the virtual machine ran, discard the redo log, continue appending changes to the redo log or cancel the power on.

The redo-log file is placed in the same folder (directory) as the disk file by default. However, you can change the location of the redo-log file in the Configuration Editor.

On a Windows host, click the **Options** tab, then type in or browse to the folder in which the redo log should be stored.

On a Linux host, click **Misc** on the left side of the Configuration Editor, then type in or choose the directory in which the redo log should be stored.

Nonpersistent

Changes to disks in nonpersistent mode are not saved to the disks, but are lost when the virtual machine is powered off or reset.

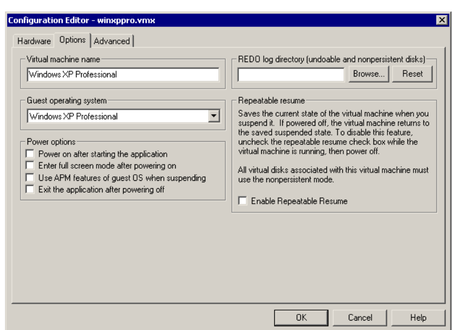
Nonpersistent mode is convenient for people who always want to start with a virtual machine in the same state. Example uses include providing known environments for software test and technical support users as well as doing demonstrations of software. Any disk type can be used in nonpersistent mode.

If your virtual disks are in nonpersistent mode, you can take advantage of the repeatable resume feature, which allows you to save the current state of the virtual machine when you suspend it, then resume from the point at which you suspended it every time you start the virtual machine. For more information, see Resuming Virtual Machines Repeatedly from the Same Point on page 111.

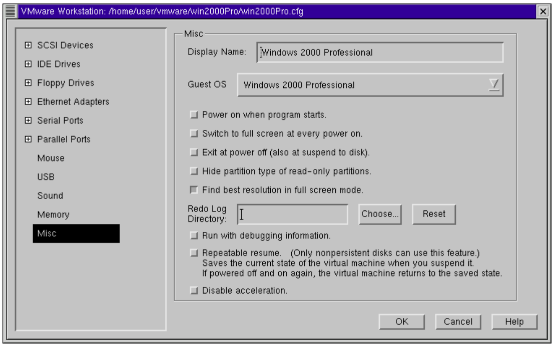
VMware Workstation only reads the virtual disk file. Any writes to the virtual disk are actually written to a redo-log file that is deleted when you power off or reset the virtual machine. This is similar to the redo-log files used with disks in undoable mode.

While you are running the virtual machine, any blocks that have been modified and written to the redo-log file are read from the redo-log file instead of the disk files. When the virtual machine is powered off or reset, the redo-log file is discarded.

The redo-log file is placed by default in the folder defined by the host operating system's TMPDIR environment variable. However, the location of the redo-log file can be changed in the Configuration Editor.



On a Windows host, click the **Options** tab, then type in or browse to the folder in which the redo log should be stored.



On a Linux host, click **Misc** on the left side of the Configuration Editor, then type in or choose the directory in which the redo log should be stored.

File Locations

Disk Files

The Configuration Editor (**Settings** > **Configuration Editor**) 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 (on a Windows host) or Configuration Wizard (on a Linux host) 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 comprises one or more `.vmdk` files. The larger the size of the virtual disk, the more `.vmdk` files. As data is added to a virtual disk, the .vmdk files grow in size, to a maximum of 2GB each. 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 disk needs 2GB or more disk space, the Configuration Editor shows the name of the first file in the set of files used to store the virtual disk. The other files used for that disk are automatically given names based on the first file's name. For example, a Windows Me virtual machine that needed two files to store its virtual disk would, by default, store it in files named `Windows Me.vmdk` and `Windows Me-02.vmdk`.

If your virtual machine uses files created under earlier VMware products, with a `.dsk` extension, they can be updated automatically. For details, see Updating Filenames for Virtual Disks Created with Earlier VMware Products on page 224.

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

The files for plain disks have a special format. The file that stores information about the plain disk has a `.pln` extension and the files used to store the plain disk's data have a `.dat` extension.

Redo-Log Files

Log files save blocks that the virtual machine modifies while the it is running. The log file for a disk in nonpersistent mode is not saved when the virtual machine is powered off or reset, while the log file for a disk in undoable mode is saved. The log file for disks in undoable mode is called the redo log, and the user decides whether the redo-log file should be saved or not.

The redo-log file for a virtual disk called `vm` is called `vm.vmdk.REDO`. If the virtual disk is larger than 2GB, it is divided into sets of 2GB disk files named `vm.vmdk`, `vm-02.vmdk`, `vm-03.vmdk` and so on; its redo-log files are called `vm.vmdk.REDO`, `vm-02.vmdk.REDO`, `vm-03.vmdk.REDO` and so on.

You can choose the location where these redo logs are stored. By default, the redo logs for disks in undoable mode are stored in the same directory as the `.vmdk` file that contains the virtual machine configuration. Redo logs for disks in nonpersistent mode are stored in your host's temp directory by default. In the case of plain disks, `filename.pln.REDO` is created by default in the same directory as the `.pln` file.

By default, redo-log files for raw disks are located in the same directory as the virtual machine configuration file.

You can change the location of the log file for disks in nonpersistent and undoable modes in the Configuration Editor.

On a Windows host, click the **Options** tab, then type in or browse to the folder in which the redo log should be stored.

On a Linux host, click **Misc** on the left side of the Configuration Editor, then type in or choose the directory in which the redo log should be stored.

You may choose to locate the log files in a different directory to increase available space or improve performance. For best performance, the log files for a virtual machine should be on a hard drive on the host computer.

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 users to lose data.

Lock files are always created in the same folder (directory) as the `.vmdk` or `.pln` file. There are two types of lock files — reader and writer. A disk in nonpersistent mode is protected by reader lock files, while disks in persistent and undoable modes use writer lock files.

A disk protected by a writer lock file can be accessed by only one virtual machine.

A disk that has reader lock files can be read by more than one virtual machine but cannot be written to.

The data storage files of a plain disk are individually locked, using the same method.

Note: 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 lock files it created. If it cannot remove the lock, a stale lock file is left protecting the `.vmdk` or `.pln` file. For example, if the machine crashes before the virtual machine has a chance to remove its lock file, there is a stale lock.

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 explaining what the user can do about the lock.

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 3.0 and 3.1, previous VMware products, including VMware Workstation 2.0, named virtual disk files with a `.dsk` extension. To avoid conflicts with the System Restore feature on Windows XP and Windows .NET Server hosts, VMware Workstation now uses a `.vmdk` extension for those files. VMware Workstation 3.2 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 new extensions is `.vmss`.

If your host computer is running Windows XP or Windows .NET Server, 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 time 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\Programs
   ```
3. Run the updater.

   ```
   dskrename.exe
   ```

Defragmenting and Shrinking Virtual Disks

When a virtual machine is powered off, you can defragment its virtual disks from the Configuration Editor (**Settings** > **Configuration Editor**).

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

Defragmenting disks may take considerable time.

When a virtual machine is powered on, you can shrink its virtual disks from the VMware Tools control panel.

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

Note: VMware recommends you defragment your VMware Workstation host's hard drive after 10 shrink operations on a virtual disk. .

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 379.

Adding Virtual Disks to a Virtual Machine

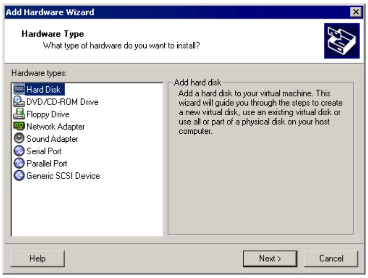
Virtual disks are stored as files on the host computer or on a network file server, so it does not matter whether the disk that holds the files is IDE or SCSI. A virtual IDE drive can be stored on an IDE drive or on a SCSI drive. So can a virtual SCSI drive.

Windows Host

Use the Configuration Editor (**Settings** > **Configuration Editor**) 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 Configuration Editor (**Settings** > **Configuration Editor**) 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. Set the capacity for the new virtual disk.

Note: 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.

5. 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….

   In most cases, the wizard creates a SCSI virtual disk by default. If your guest operating system does not have appropriate support for the virtual SCSI adapter in the virtual machine, the wizard creates an IDE virtual disk. If you want your virtual disk to be an IDE device, click Advanced and be sure the virtual device node is set to an available IDE node.

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

6. 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.

   The new virtual disk is set up in persistent mode. To change to nonpersistent or undoable mode, use the Configuration Editor. Click the entry for the new virtual disk, then select the mode you want.

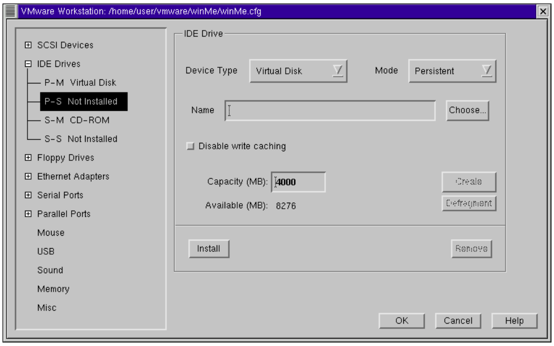
   If the virtual disk files are stored on a network file server, you can improve performance of the virtual disk by setting the folder for a disk in undoable mode to a location on the host computer. You can make this setting on the Options tab of the Configuration Editor.

Linux Host

Use the Configuration Editor (Settings > Configuration Editor) 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.

1. Open the Configuration Editor (Settings > Configuration Editor). If you want to add a SCSI virtual disk, click the + sign beside SCSI Devices. If you want to add an IDE virtual disk, click the + sign beside IDE Drives.

   Note: All virtual machines can use IDE virtual disks. SCSI virtual disks can be used with guest operating systems that have drivers for the virtual BusLogic SCSI adapter used in the virtual machine. To use SCSI disks in a Windows XP or Windows .NET Server 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 Windows .NET Server.



2. Click a device that is shown as **Not Installed**.
3. Use the default device type of **Virtual Disk**.
4. Keep the default mode of **Persistent** or use the drop-down list to change the setting to **Undoable** or **Nonpersistent**.
5. Type the name for the virtual disk's first file. By default, it is created in the same directory as the virtual machine's configuration file. To create it in a different directory, type the full path name or click **Choose…** to navigate to the directory you want to use.
6. Set the capacity for the new virtual disk.

   Note: 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 2000 (2GB) and 64000 (64GB). The default is 4000 (4GB).
7. If you want to disable write caching on this disk, click the check box beside **Disable Write Caching**.

   When write caching is enabled, there is a delay between the time a program saves data and the time that data is actually written to disk. This improves performance. But the delay in writing data to disk adds some risk of data loss. Thus if data integrity is more important than performance, you may want to disable write caching.
8. Click **Create** to create the files for your new virtual disk.
9. Click **Install** to install the new virtual disk in your virtual machine.
10. Click **OK** to save the configuration and close the Configuration Editor.

The new virtual disk 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.

If the virtual disk files are stored on a network file server, you can improve performance of the virtual disk by setting the redo log directory to a location on the host computer. You can make this setting in the **Misc** panel of the Configuration Editor.

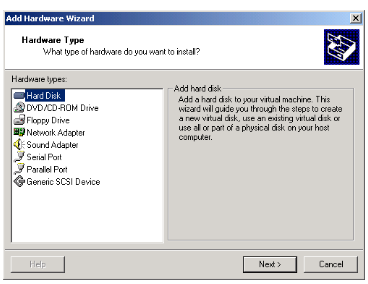
Adding Raw Disks to a Virtual Machine

Windows Host

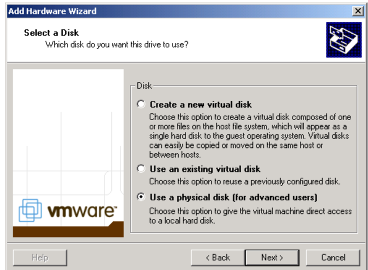
Use the Configuration Editor (**Settings** > **Configuration Editor**) to add a new raw disk to your virtual machine. The virtual machine should be powered off before you begin. If it is not, shut down the guest operating system normally, then click **Power Off** on the VMware Workstation toolbar.

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

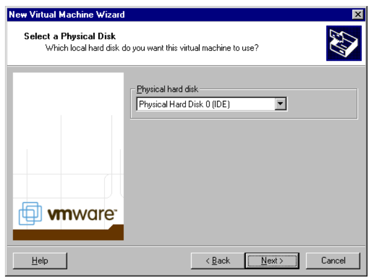
1. Open the Configuration Editor (**Settings** > **Configuration Editor**) and click **Add…**. The Add Hardware Wizard guides you through the steps to create your virtual disk.
2. Click **Hard Disk**, then click **Next**.



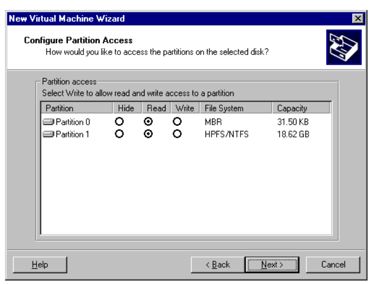
3. Select **Use a physical disk**, then click **Next**.



4. Choose the physical hard disk to use from the drop-down list. Click **Next**.



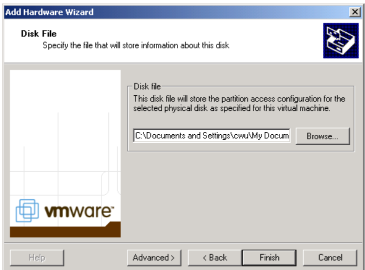
5. Set the virtual machine's access rights for each partition on the physical hard disk.



- Select **Hide** if the virtual machine should not see the partition.
- Select **Read** to give the virtual machine read-only access to the partition.
- Select **Write** to give the virtual machine read/write access to the partition.

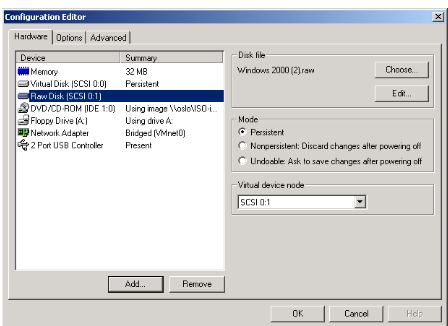
Click **Next**.

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…**.



When you have set the filename and location you want to use and 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.



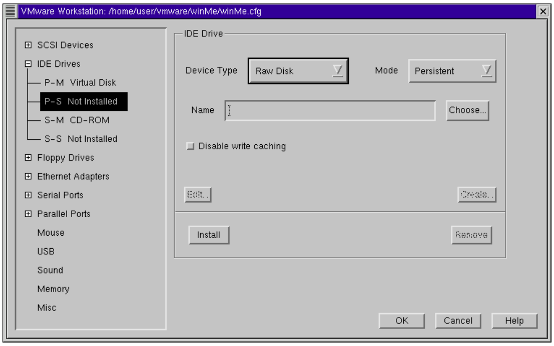
The new raw disk is set up in persistent mode. To change to nonpersistent or undoable mode, use the Configuration Editor. Click the entry for the new raw disk, then select the mode you want.

Linux Host

Use the Configuration Editor (**Settings** > **Configuration Editor**) 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 Configuration Editor (**Settings** > **Configuration Editor**). If you want to add a SCSI raw disk, click the + sign beside **SCSI Devices**. If you want to add an IDE raw disk, click the + sign beside **IDE Drives**.



2. Click a device that is shown as **Not Installed**.
3. Choose **Raw Disk** from the **Device Type** drop-down list.
4. Keep the default mode of **Persistent** or use the drop-down list to change the setting to **Undoable** or **Nonpersistent**.
5. Type the name for the file that will store access information for this raw disk. To create it in a different directory, type the full path name or click **Choose…** to navigate to the directory you want to use.
6. If you want to disable write caching on this disk, click the check box beside **Disable write caching**.

   When write caching is enabled, there is a delay between the time a program saves data and the time that data is actually written to disk. This improves performance. But the delay in writing data to disk adds some risk of data loss. Thus if data integrity is more important than performance, you may want to disable write caching.

7. Click **Create** to create the file for your new raw disk.
8. A dialog box prompts you for the name of the device that holds the partition you want to use as a raw disk. Enter the path to the device — for example `/dev/hdb` — then click **OK**.
9. A dialog box prompts you to set access permissions for the partitions on the device you have selected.
   - Select **No Access** if the virtual machine should not see the partition.
   - Select **Read Only** to give the virtual machine read-only access to the partition.
   - Select **Read/Write** to give the virtual machine read/write access to the partition.

   Click **Save** to save your selections and close the dialog box.
10. Click **Install** to install the new raw disk in your virtual machine.
11. Click **OK** to save the configuration and close the Configuration Editor.
12. 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.

Adding DVD or CD-ROM Drives to a Virtual Machine

You can add one or more DVD or CD-ROM 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-ROM 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-ROM 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.

The DVD or CD-ROM drives in the virtual machine can be used to read data from CD-ROM or DVD-ROM disks. VMware Workstation does not support playing DVD movies in a virtual machine.

If you need to read from multisession discs, configure your DVD/CD-ROM drive to use raw access mode.

Adding a DVD or CD-ROM Drive on a Windows Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**) 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, then 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. Then click **Finish**.
5. The drive is set up initially so it appears to the guest operating system as an IDE drive. If you want to change so it appears to the guest operating system as a SCSI drive, click the drive's entry in the Configuration Editor and make that change in the settings panel on the right.

Adding a DVD or CD-ROM Drive on a Linux Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**). If you want the drive to appear to the guest operating system as a SCSI drive, click the **+** sign beside **SCSI Devices**. If you want the drive to appear to the guest operating system as an IDE drive, click the **+** sign beside **IDE Drives**.
2. Select a device that is shown as **Not Installed**.
3. From the **Device Type** drop-down list, choose **CD-ROM** to connect to a physical DVD or CD-ROM drive. Choose **CD-ROM Image** to connect to an ISO image file.
4. If you are connecting to a physical drive, enter its device name (for example, `/dev/hdc`) in the **Name** field or click **Choose…** to navigate to the name.

   If you are connecting to an ISO image file, enter the path and filename in the Name field or click **Choose…** to navigate to the name.
5. Click **Install** to create the new DVD or CD-ROM drive, then click **OK** to save the configuration and close the Configuration Editor.

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 on a Windows Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**) 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 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**.

Adding a Floppy Drive on a Linux Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**). Click the **+** sign beside **Floppy Drives**.
2. Select a device that is shown as **Not Installed**.
3. On the **Type** drop-down list, choose **Device** to connect to a physical floppy drive on the host computer.

   Choose **File** from the drop-down list to connect to a floppy image file.
4. If you chose **Device**, accept the default device name shown (for example, `/dev/fd1` for the second physical floppy drive), type in the path and device name or click **Choose…** to navigate to the device name.

   If you chose **File**, type in the path and filename for the floppy image file or click **Choose…** to navigate to the file.
5. Click **Install** to install the new floppy drive, then click **OK** to save the configuration and close the Configuration Editor.

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

You can use the Configuration 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 on a Windows Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**) 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 Configuration Editor.

Connecting to an ISO Image File on a Linux Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**). If your DVD/CD-ROM drive is configured as a SCSI drive, click the **+** sign beside **SCSI Devices**. If it is configured as an IDE drive, click the **+** sign beside **IDE Drives**.
2. Select the DVD/CD-ROM drive you want to connect to the image file and enter the path and filename in the **Name** field or click **Choose…** to navigate to the name.
3. Click **OK** to save the configuration and close the Configuration Editor.

Connecting to a Floppy Image File on a Windows Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**) 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**.

Connecting to a Floppy Image File on a Linux Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**). Click the **+** sign beside **Floppy Drives**.
2. Select the device you want to use.
3. On the **Type** drop-down list, choose **File**.
4. Type in the path and filename for the floppy image file or click **Choose…** to navigate to the file.
5. Click **OK** to save the configuration and close the Configuration Editor.

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. As with virtual disks, raw disks can be used in persistent, undoable and nonpersistent modes. For an explanation of these modes, see Disk Modes: Persistent, Undoable and Nonpersistent on page 218.

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 for Linux on page 260.

Setting up a raw disk configuration for a virtual machine is more complicated than using a virtual disk. So 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.

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 so, 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 chapter 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 below under the name of the operating system you intend to run as a guest in a virtual machine.

Windows .NET Server

Caution: Running a Windows .NET Server guest from a raw disk is not supported. You should not test a Windows .NET Server raw disk configuration in a production environment.

- Configuring Dual- or Multiple-Boot Systems to Run with VMware Workstation on page 240
- Running a Windows 2000, Windows XP or Windows .NET Server Virtual Machine from an Existing Multiple-Boot Installation on Computers with ACPI on page 252
- Disk Partition Hiding for Dual- or Multiple-Boot Systems on page 259
- Do Not Use Windows 2000, Windows XP and Windows .NET Server Dynamic Disks as Raw Disks on page 259

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 240
- Running a Windows 2000, Windows XP or Windows .NET Server Virtual Machine from an Existing Multiple-Boot Installation on Computers with ACPI on page 252
- Disk Partition Hiding for Dual- or Multiple-Boot Systems on page 259
- Do Not Use Windows 2000, Windows XP and Windows .NET Server Dynamic Disks as Raw Disks on page 259

Windows 2000

- Configuring Dual- or Multiple-Boot Systems to Run with VMware Workstation on page 240

- Running a Windows 2000, Windows XP or Windows .NET Server Virtual Machine from an Existing Multiple-Boot Installation on Computers with ACPI on page 252
- Disk Partition Hiding for Dual- or Multiple-Boot Systems on page 259
- Do Not Use Windows 2000, Windows XP and Windows .NET Server Dynamic Disks as Raw Disks on page 259

Windows NT

- Configuring Dual- or Multiple-Boot Systems to Run with VMware Workstation on page 240
- Adding Uniprocessor Support to Windows NT 4.0 MPS Installations on page 251
- Disk Partition Hiding for Dual- or Multiple-Boot Systems on page 259

Windows 98

- Configuring Dual- or Multiple-Boot Systems to Run with VMware Workstation on page 240
- SVGA Video Driver Setup for Use with a Windows 98 Guest Operating System Booted from a Raw Disk on page 257
- Disk Partition Hiding for Dual- or Multiple-Boot Systems on page 259

Windows 95

- Configuring Dual- or Multiple-Boot Systems to Run with VMware Workstation on page 240
- Setting Up the SVGA Video Driver for a Windows 95 Guest Operating System Booted from a Raw Disk on page 255
- Disk Partition Hiding for Dual- or Multiple-Boot Systems on page 259

SCSI Systems Using a Linux Host

- Configuring Dual- or Multiple-Boot SCSI Systems to Run with VMware Workstation for Linux on page 260

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 265.

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 (on Windows hosts) or Configuration Wizard (on Linux hosts) 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. The wizard is typically rerun 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 VMware Workstation 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.

Running Windows Guests on Windows Hosts with FAT File Systems

There is a potential problem with VMware Workstation on Windows hosts when you boot an operating system from an existing partition. If the Windows host’s partition uses a FAT file system, the guest operating system (for example, Windows 98 or Windows 95) sees this partition at boot time and attempts to fix the file system on that partition. This causes serious problems, because the host operating system is actively using that partition.

If you use an advanced boot manager such as BootMagic (PowerQuest) or System Commander (V Communications), it solves this problem by changing the partition type to “unknown.” If you are already using such an advanced boot manager to dual boot, the boot manager’s partition marking scheme works fine with VMware Workstation.

However, if you are not using an advanced boot manager for dual booting, the configuration process described below hides partitions that do not belong to the guest operating system. When raw disk partition hiding is enabled, all read-only partitions are mapped to “unknown.” Also, all updates to the master boot record are intercepted and not written to the actual master boot record.

Windows 2000, Windows XP and Windows .NET Server Dynamic Disks

If your host is running Windows 2000, Windows XP or Windows .NET Server and is using dynamic disks, see Do Not Use Windows 2000, Windows XP and Windows .NET Server Dynamic Disks as Raw Disks on page 259.

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 like the one above is displayed.

To avoid the problem, follow the configuration steps below and be sure to mark the native Linux partition where the rest of LILO is located with read-only access. 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.

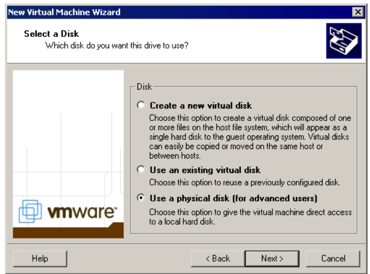
Configuring a Windows Host

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, it cannot be configured as the slave on the secondary IDE channel if the master on that channel is a CD-ROM drive.

1. Before starting, if you are running a Windows guest operating system you should read Setting Up Hardware Profiles in Virtual Machines on page 247. VMware recommends booting the guest operating system natively on the computer and creating a hardware profile for the virtual machine before proceeding.
2. Create a separate configuration for each guest operating system. Allow read/write access to the partitions used by that operating system only.

   To configure a virtual machine to run from a raw disk partition, start the New Virtual Machine Wizard (**File** > **New…**) and select **Custom**.



3. When you reach the Select a Disk step, select **Use a physical disk**.
4. The next panel allows you to specify the access that is needed for each partition on the disk(s). Most partitions should be set to Read, and the partition used by the virtual machine should be set to Write.
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 .NET Server, 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 Configuration Editor (**Settings** > **Configuration Editor**) 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 or to change the disk mode.
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 247 for more information.

10. Install VMware Tools in your guest operating system.

Warning: If you configure your raw disk in undoable mode, you need to either commit or discard the changes to the disk 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 redo-log file for the disk in undoable mode. See Disk Modes: Persistent, Undoable and Nonpersistent on page 218 for more information on disks in undoable mode and their corresponding redo-log files.

Configuring a Linux Host

1. Before starting, if you are running a Windows guest operating system you should read Setting Up Hardware Profiles in Virtual Machines on page 247. VMware recommends booting the guest operating system natively on the computer and creating a hardware profile for the virtual machine before proceeding.

2. Create a separate configuration for each guest operating system. Allow read/write access to the partitions used by that operating system only.

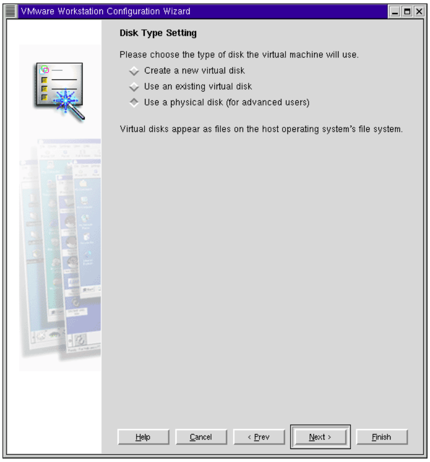
3. Check operating system partition mounts. Be sure the existing disk partitions that you plan to configure the virtual machine to use are not mounted by Linux.
4. Set the device group membership or device ownership.

   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 of security when exploring different options here.

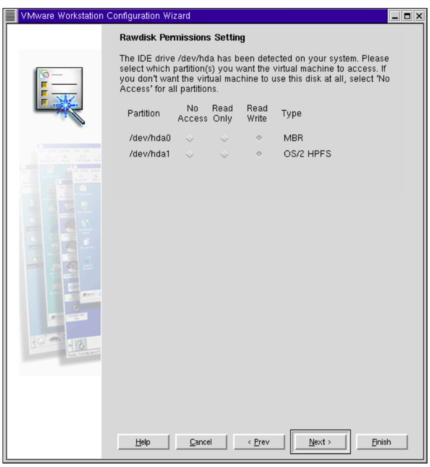
   It is typically a good idea to grant VMware Workstation users access to all `/dev/hd[abcd]` raw devices that contain operating systems or boot managers and then rely on VMware Workstation's raw disk configuration files to guard access. This provides boot managers access to configuration and other files 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.
5. If you plan 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. Run the VMware Workstation Configuration Wizard (**File** > **Wizard…**).



7. When you reach the Disk Type Settings panel, select **Use a physical disk**. Click **Next**.



8. Select the read/write option for the disk partitions that contain the guest operating system being configured.

   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 mark read/write for the virtual machine is not mounted under the Linux host.

You need to leave the master boot record (MBR) read-only. Leaving the other partitions read-only is recommended. The LILO boot manager often reads files from `/boot` (on a Linux partition) to boot a guest operating system.

9. Complete the remaining steps in the wizard. On the review screen, note the path to the configuration (`.cfg`) file. You will need it in the next step.
10. Start VMware Workstation and check the configuration. Type
`vmware <config-file>.cfg.`
`<config-file>` is the path to the configuration file created by the Wizard.
11. Choose **Settings** > **Configuration Editor** and check that your IDE configuration specifies at least one raw disk description file. These files are named `<configuration-name>.hda`, `<configuration-name>.hdb`, etc.

    Also modify any configuration options you want to change from the Configuration Wizard's defaults — for example, you may want to change the amount of memory allocated to the guest operating system.
12. 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. After powering on the virtual machine, press F2 during the BIOS boot in the virtual machine to enter the BIOS setup menu.
13. 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.

14. 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 247 for more information.

15. Install VMware Tools in your guest operating system.

Warning: If you configure your raw disk in undoable mode, you need to either commit or discard the changes to the disk 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 redo-log file for the disk in undoable mode. See Disk Modes: Persistent, Undoable and Nonpersistent on page 218 for more information on disks in undoable mode and their corresponding redo-log files.

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 240 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 Family Ethernet adapter (PCI-ISA)
- Serial ports (COM1-COM4)
- Parallel ports (LPT1-LPT2)
- Two-port USB hub
- Sound Blaster 16-compatible sound card

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 virtual 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 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 .NET Server 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 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 .NET Server. 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 (on a Windows host) or Configuration Wizard (on a Linux host) to configure your virtual machine as described in Configuring Dual- or Multiple-Boot Systems to Run with VMware Workstation on page 240.

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 .NET Server, Windows XP and Windows 2000 guests:** After you log on to Windows .NET Server, 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 .NET Server, Windows XP or Windows 2000 automatically detects and load 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 the VMware, Inc. SVGA video driver (included in VMware Tools) has been installed. Once Windows .NET Server, Windows XP or Windows 2000 reboots inside the virtual machine, select a new SVGA resolution from the

Display Properties > Settings tab dialog box to increase the size of the virtual machine's display window.

If you want to enable the virtual machine's sound adapter to work inside the Windows .NET Server, Windows XP or Windows 2000 guest operating system, finish the remaining steps in this section, then refer to Configuring Sound in VMware Workstation on page 339.

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 tab).

Select the device, then click the Remove button. If a device appears in multiple hardware profiles, you can select the hardware profile(s) from which to remove the device.

Windows NT guest 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).

7. Confirm that your virtual devices — specifically, the network adapter — are working properly.

   Windows 95 and Windows 98: 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.

Adding Uniprocessor Support to Windows NT 4.0 MPS Installations

If your host computer has more than one processor and one of the operating systems on the computer is Windows NT 4.0, you encounter problems when you try to run that operating system as a VMware Workstation guest operating system running from a raw disk. Typically, you see an error message like "This HAL DLL requires MPS version 1.1 system" when you try to boot the guest operating system.

The hardware abstraction layer (HAL) installed on your physical computer for Windows NT is for multiprocessor systems (MPS). But the VMware Workstation virtual machine uses only one processor.

It is possible to work around this problem by adding uniprocessor support to your Windows NT configuration.

Warning: These instructions are intended for expert Windows NT users and administrators only. The instructions below do not apply to systems running Windows 2000, Windows XP or Windows .NET Server.

You should be familiar with low-level operation of Windows NT and be familiar with modifying `boot.ini` parameters. You also need to be aware if your system is not a standard PC and thus requires a special uniprocessor hardware abstraction layer (HAL). If it does require a special HAL, you will need to ensure you use the correct `hal.dll` and `NTOSKRNL.EXE` for your computer.

These instructions apply to Microsoft Windows NT 4.0, both Workstation and Server releases.

To allow the use of a uniprocessor HAL and kernel files, follow these steps:

1. Copy the `hal.dll` file and the `NTOSKRNL.EXE` file from the Windows NT CD-ROM or Windows NT Service Pack CD-ROM (if a service pack is installed) to a temporary folder. On Service Pack CD-ROMs these files are found in the `\i386` folder.
2. Rename the `hal.dll` file to `unihal.dll`, and rename the `NTOSKRNL.EXE` file to `UNIKRNL.EXE`.

3. Copy the files you renamed in Step 2 to the `C:\winnt\system32` folder. (If the system environment variable SYSTEMROOT is not `C:`, then use the appropriate path instead of `C:\winnt\system32`.)
4. Remove the read-only attribute from the `boot.ini` file.

   ```
   attrib -s -h -r C:\boot.ini
   ```

   If the system environment variable SYSTEMROOT is not `C:`, then use the appropriate path instead of `C:\boot.ini`.
5. Use a text editor (such as Notepad) to modify the `[operating systems]` section in `boot.ini` to read:

   ```
   [operating systems]
   multi(0)disk ....\WINNT40="Windows NT Server Version 4.00"
   multi(0)disk ....\WINNT40="Windows NT Version 4.00
   [UNIHAL]" /hal=unihal.dll /kernel=unikrnl.exe
   ```

   Note: The last line, from the second `multi(0)disk` to `/kernel=unikrnl.exe`, must be on one line. It must not wrap.
6. Save the `boot.ini` file, exit the text editor, then restart the computer.
7. When the computer reboots, choose Windows NT Version 4.00 [UNIHAL] from the Windows NT boot menu.

   This is the configuration you should use in the virtual machine.

Running a Windows 2000, Windows XP or Windows .NET Server Virtual Machine from an Existing Multiple-Boot Installation on Computers with ACPI

The Windows 2000, Windows XP and Windows .NET Server kernels support Advanced Configuration and Power Management (ACPI), a power management interface that replaces the earlier APM.

If you have installed Windows 2000, Windows XP or Windows .NET Server on a computer with ACPI features and then try to set up a VMware Workstation virtual machine running from a raw disk, this can cause VMware Workstation to crash with an error message that says “Error CPL0 Stack, Shutdown” or “INACCESSIBLE BOOT DEVICE.“

Source of the Problem

This problem is most likely to affect laptop computers but may also affect some ACPI-capable desktop computers.

The physical computer hardware supports ACPI, while the virtual machine environment does not. The ACPI hardware abstraction layer (HAL) that was installed automatically when Windows 2000, Windows XP or Windows .NET Server was installed on the computer does not run in the virtual environment within VMware Workstation. (The hardware abstraction layer is the low-level part of the operating system that is specific to the hardware it is running on.)

Determining Whether This Affects You

To find out whether you have an ACPI HAL installed on your computer, check the properties of the `hal.dll` file.

1. Locate the folder that contains the `hal.dll` file. By default it is `C:\WINNT\system32`, where `C:` is the drive letter where your `WINNT` folder resides. Use a different drive letter to match your configuration, if necessary.
2. Locate the `hal.dll` file. Right-click the filename and choose **Properties** from the pop-up menu.
3. Click the **Version** tab, then click **Internal Name**.
4. If the internal name is `halacpi.dll`, this problem affects you.

What You Can Do

If you have the ACPI HAL installed, VMware recommends that you install your Windows 2000, Windows XP or Windows .NET Server guest operating system in a virtual disk, rather than running it from a raw disk. If you install Windows 2000, Windows XP or Windows .NET Server from scratch into a virtual machine, then the correct HAL is automatically installed.

If you do want to run a Windows 2000 guest operating system from a raw disk, you can resolve the HAL issue by installing two HALs on the computer. One is the ACPI HAL that is already there; the other is the standard, non-ACPI HAL. You can then choose which HAL to run at boot time.

Caution: These configuration changes should be undertaken only by advanced users of Windows 2000, Windows XP or Windows .NET Server. It is possible to cause your computer to fail to boot or otherwise misbehave if the changes are done improperly.

To make these configuration changes, you need an installation CD-ROM for your Windows 2000, Windows XP or Windows .NET Server operating system.

1. Shut down your host operating system and boot Windows 2000, Windows XP or Windows .NET Server natively.
2. Open a command prompt.

3. Insert your Windows 2000, Windows XP or Windows .NET Server installation CD in the CD-ROM drive.
4. Extract the uniprocessor `hal.dll` along with `NTOSKRNL.EXE` and rename the extracted files as follows:

   ```
   expand D:\I386\HAL.DL_ C:\WINNT\SYSTEM32\VMHAL.DLL
   expand D:\I386\NTOSKRNL.EX_ C:\WINNT\SYSTEM32\VMOSKRNL.EXE
   ```

   where `D:` is the drive letter used by your CD-ROM drive and `C:` is where your `WINNT` folder resides.

   Change the drive letters to match your configuration, if necessary.

   Note: Be sure to expand the files to the filenames starting with VM to avoid overwriting any existing system files.
5. Change the file attributes of your `boot.ini` file to make it writable.

   ```
   attrib c:\boot.ini -s -h -r
   ```
6. Open the `boot.ini` file in a text editor such as Notepad. In the next several steps, you will add a new option to the configuration selection screen that appears as the operating system boots. At the end of this document are samples of a `boot.ini` file before and after these modifications.
7. Copy the line that begins with `multi(0)` and paste it at the end of the file.
8. Modify the line that you copied, so the text in quotation marks after `WINNT=` indicates you use this configuration with VMware Workstation. For example, describe it as Windows 2000 Professional Virtual Machine (or whatever matches the Windows version you are using).
9. Add the following to the end of the new line:

   ```
   /KERNEL=VMOSKRNL.EXE /HAL=VMHAL.DLL
   ```
10. Save the `boot.ini` file.
11. Restore its attributes to those it originally had.

    ```
    attrib boot.ini +s +h +r
    ```
12. Shut down and boot into your host operating system.
13. Start VMware Workstation and boot the virtual machine using the new selection you added to the `boot.ini` file.

Sample boot.ini Files

Note: The lines in `boot.ini` should not wrap. Each line in the `[operating systems]` section of these samples begins with `multi(0)`.

Sample `boot.ini` before modifications:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft
Windows 2000 Advanced Server" /fastdetect
```

Sample `boot.ini` file after modifications:

```
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINNT
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft
Windows 2000 Advanced Server" /fastdetect
multi(0)disk(0)rdisk(0)partition(1)\WINNT="Microsoft
Windows 2000 Advanced Server Virtual Machine" /fastdetect
/KERNEL=VMOSKRNL.EXE /HAL=VMHAL.DLL
```

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 247.

1. Boot Windows 95 natively (not in a virtual machine).
2. Right-click on 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 .NET Server).
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 81, 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 .NET Server) 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.

SVGA Video Driver Setup 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 247.

1. Boot Windows 98 natively (not in a virtual machine).
2. Right-click on 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 .NET Server).
9. Select **Virtual Machine** from the list of profiles when prompted.
10. Windows 98 auto-detects the virtual machine's devices and installs their drivers.
11. When it 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 81.
23. At the end of the tools installation, the Display Properties dialog box should be displayed.
24. Click the **Advanced** button, then click the **Adapter** tab.
25. Click the **Change** button. The Update Device Driver Wizard starts.
26. Click **Next**.
27. Select **Display a list of all drivers…**, then click **Next**.
28. Click **Have Disk**.
29. Type `C:\WINDOWS\TEMP` in the **Copy manufacturer's files from** field, then click **OK**.
30. Click **OK** to select the VMware SVGA device, then click **Next**.
31. If you are prompted with an Update Driver Warning, click **Yes**, then click **Next**.
32. Click **Finish**, then click **Apply**.
33. Click **Close**, then reboot when prompted.
34. After booting is completed, open the device manager. It should show that you have
    - Standard PCI Graphics Adapter
    - VMware SVGA Display Adapter
35. Shut down the Windows 98 virtual machine and your host operating system.
36. Boot natively into Windows 98, then start the Device Manager.
37. Select the VMware SVGA device if listed, then click **Remove**.
38. Select the **Remove from Specific Configuration** radio button, then select **Physical Machine** from the configuration list.
39. Click **OK**, then reboot Windows 98 when prompted.

40. 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.

Disk Partition Hiding for Dual- or Multiple-Boot Systems

The disk partition hiding option (on Windows hosts: Settings > Configuration Editor > Advanced; on Linux hosts: Settings > Configuration Editor > Misc) is useful if you are running multiple operating systems at the same time and you are not running a boot manager.

For example, if you are running Windows NT from a FAT partition, and you boot Windows 98 from another partition, Windows 98 sees the partition from which Windows NT is running and incorrectly attempts to repair the file system containing Windows NT.

Boot managers circumvent this problem by changing the partition types of all bootable partitions, other than the partition currently booted. The types are left as an unknown file system, so that they are ignored by the currently booted partition. Using the disk partition hiding feature has the same effect.

When this option is enabled, only the partitions for which the virtual machine has read/write access are visible. The other partitions are changed to an unknown type. In addition, all writes to the master boot record (MBR) where this information is recorded are intercepted. This allows multiple operating systems to run from the same disk but with different views of the same partitions.

Because of this feature, however, a boot manager program run inside a virtual machine with disk partition hiding enabled does not perform properly. If you wish to install and use a boot manager program in a virtual machine, turn off the disk partition hiding option.

Partitions used by the guest operating system should be hidden from the host operating system. On a Windows NT host, the partitions can be unmapped using the Disk Administrator tool. For a Linux host, be sure these partitions are not mounted.

Do Not Use Windows 2000, Windows XP and Windows .NET Server Dynamic Disks as Raw Disks

Windows 2000, Windows XP and Windows .NET Server support a new 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 .NET Server also support the older type of partition table, on what are designated as basic disks.

You can use the disk management tool to check the type of disk used on your Windows 2000, Windows XP or Windows .NET Server 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 for Linux

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 a BusLogic SCSI adapter. 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 263.

Before You Create the Virtual Machine Configuration

You must create a separate configuration for each guest operating system. Allow read/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 247. 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 a Mylex® (BusLogic) BT-958 compatible host bus adapter. Drivers for BusLogic controllers are available from the Mylex Web site — *www.mylex.com/products/multimaster/drivers/index.html*.

   The BusLogic driver needs to be installed in the profile for the guest operating system.

   Note: To use SCSI devices in a Windows XP or Windows .NET Server 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.

   Note: 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 mark read/write for the virtual machine is not mounted under the Linux host.

5. Set the device group membership or device ownership. The master raw disk device(s) needs to 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 when exploring 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, 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 should normally be recognized when Linux boots directly on the physical machine.

Setting Up the Virtual Machine Configuration

To use a SCSI raw disk, you must create your virtual machine configuration using the Configuration Editor.

1. Start VMware Workstation. At the initial dialog box, select **Run the Configuration Editor**.
2. Click the + sign beside **SCSI Drives.**
3. Choose the SCSI ID that corresponds to the one used by your SCSI drive. For example, if your SCSI drive has SCSI ID 2, choose **SCSI 0:2**. If you do not know the SCSI ID set on your physical SCSI drive, try using **SCSI 0:0**.
4. Click **Install**.
5. Select **Raw Disk** as the device type. Set the mode you prefer. For information on VMware Workstation disk modes, see Disk Modes: Persistent, Undoable and Nonpersistent on page 218.
6. In the **Name** field, enter a name of your choice — for example, `raw-sda` or `raw-windows` — then click **Create**.
7. Enter the path to the device name of the SCSI disk you want to configure as a raw disk in VMware Workstation — for example, `/dev/sda`, `/dev/sdb` — and click **OK**.

8. Configure access to the partitions you want to use inside the virtual machine. You must configure at least Read-Only access to the master boot record (MBR) or you will be unable to boot from this disk.
9. Configure other devices you want to use in your virtual machine.
10. Click **OK** to save your changes and close the Configuration Editor.
11. Click **Power On** to start 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 a BusLogic card, and your operating system needs to have a valid BusLogic 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 237. The instructions in this section do not apply to a disk with a previously installed operating system.

As with virtual disks, raw disks can be used in persistent, undoable and nonpersistent modes. For details on these modes, see Disk Modes: Persistent, Undoable and Nonpersistent on page 218.

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 (on Windows hosts) or Configuration Wizard (on Linux hosts) 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. 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 .NET Server Dynamic Disks

If your host is running Windows 2000, Windows XP or Windows .NET Server and is using dynamic disks, see Do Not Use Windows 2000, Windows XP and Windows .NET Server Dynamic Disks as Raw Disks on page 259.

Configuring the Virtual Machine to Use a Raw Disk

Use the following steps to run a guest operating system from a raw disk.

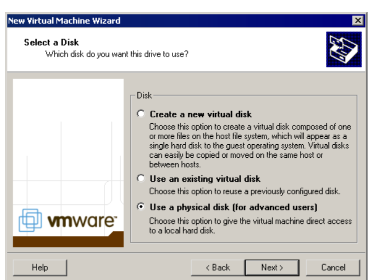
Note: If you use a Windows host's IDE disk in a raw disk configuration, it cannot be configured as the slave on the secondary IDE channel if the master on that channel is a CD-ROM drive.

1. Identify the raw partition where the guest operating system will be installed.

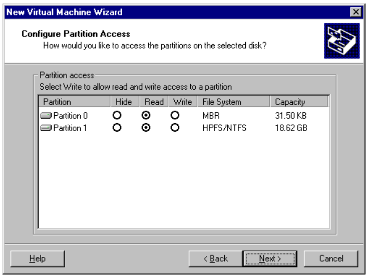
   Check the guest operating system documentation regarding the type of partition on which the operating system can be installed. For example, operating systems like DOS, Windows 95 and Windows 98 must be installed on the first primary partition while others, like Linux, can be installed to a primary or 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 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…**) and select **Custom**.
3. When you reach the Select a Disk step, select **Use a physical disk**.



4. The next panel allows you to specify the access that is needed for each partition on the disk(s). Most partitions should be set to Read, and the partition that the virtual machine is to use should be set to Write.



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 mark as Write for the virtual machine is not in use.

5. The partition where you are installing the guest operating system should be unmapped in 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 .NET Server, 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 Configuration Editor (**Settings** > **Configuration Editor**) 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 or to change the disk mode.

7. 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 Installing Guest Operating Systems on page 135.

Configuring a Linux Host

1. Identify the raw partition where 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 to 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 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.

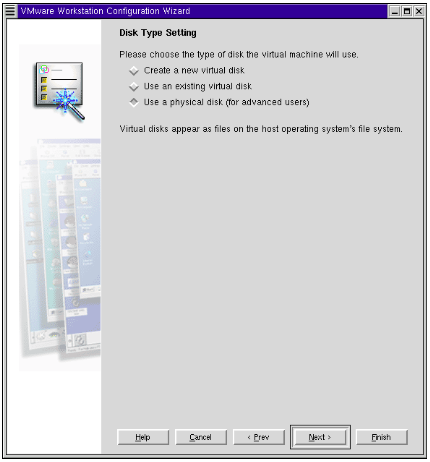
2. Check the operating system partition mounts. Be sure the existing disk partitions that you plan to configure the virtual machine to use are not mounted by Linux.

3. Set the device group membership or device ownership.

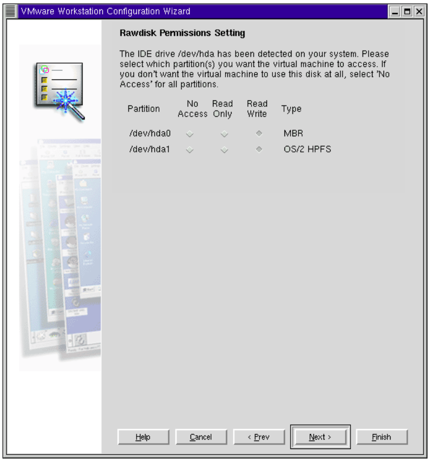
   The master raw disk device or devices need to be readable and writable by the user who runs VMware Workstation. On most distributions, the raw devices, such as `/dev/hda` (IDE raw disk) and `/dev/sdb` (SCSI raw disk) belong to group-id `disk`. If this is the case, you can add VMware Workstation users to the `disk` group. Another option is to change the owner of the device. Please think carefully of security in exploring 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 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.

4. Run the VMware Workstation Configuration Wizard (**File** > **Wizard…**).



5. When you reach the Disk Type Settings panel, select **Use a physical disk**. Click **Next**.



6. Select the read/write option only for the raw partition or disk (and its master boot record) on which you want to install the guest operating system. If the raw disk you plan to use has multiple partitions already on it, 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 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 by the host or in use by another virtual machine.

To safeguard against this problem, be sure the partition you mark read/write for the virtual machine is not mounted under the Linux host.

7. Complete the remaining steps in the wizard. On the review screen, note the path to the configuration (`.cfg`) file. You will need it in the next step.
8. Start VMware Workstation and manually change the controller/channel assignment selected by the wizard. Type `vmware <config-file>.cfg`, where `<config-file>` is the path to the configuration file created by the wizard.
9. Choose **Settings** > **Configuration Editor** and check that your IDE configuration specifies at least two raw disk description files. These files are named `<configuration-name>.hda`, `<configuration-name>.hdb`, etc.
10. Identify the description file for the raw disk to which you will install the new guest operating system. For example, if your physical machine has an unused disk on the secondary master IDE channel and you want to use this device for the virtual machine, you should see a file called `<configuration-name>.hdc` next to the virtual machine's IDE 1:0 or S-M configuration entry.
11. Replace the name of the description file (`.hda` file) next to the virtual machine's IDE 0:0 channel with the name of the description file you identified in the previous step.
12. Remove the other raw disk description file(s) from the virtual machine's IDE configuration dialog box and Click **OK**.
13. Click **OK** to save the changes and close the Configuration Editor.
14. 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 Installing Guest Operating Systems on page 135.

Disk Performance in Windows NT Guests on Multiprocessor Hosts

Some users have seen slower than expected disk input/output performance when running Windows NT guest operating systems 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.

Improving Performance

You may increase performance by enabling DMA (direct memory access) on the virtual hard disk's IDE channel in the virtual machine.

Note: You should not enable DMA on the IDE channel to which you have attached your virtual DVD/CD-ROM drive. In most cases, the virtual hard disk is attached to IDE channel 0 and the virtual DVD/CD-ROM drive is attached to IDE channel 1, so this is not an issue.

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 Configuration Editor (**Settings** > **Configuration Editor**) 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 3 or higher in the virtual machine to enable this option.

Once the virtual machine is running Windows NT, insert an SP3 or SP4 CD in the drive and run `DMACHECK.EXE` from the `\SUPPORT\UTILS\I386` folder on the CD. Or download `DMACHECK.EXE` from the Microsoft Web site (*support.microsoft.com/support/kb/articles/Q191/7/74.ASP*).

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.

9

Networking

Configuring Your Virtual Network

VMware Workstation provides virtual networking components that let you create a wide range of configurations.

You can choose the most common configurations — bridged networking, network address translation (NAT) and host-only networking — in the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts) when you create a virtual machine. The wizard then connects the proper components for you automatically.

You can set up more specialized configurations by choosing the appropriate settings in the Configuration Editor 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 sections of this chapter 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 chapter 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 available if you have installed VMware Workstation with any networking options (bridged, NAT or host-only). They are created as needed by the VMware Workstation software, up to a total of 10 switches. You can connect one or more virtual machines to a switch.

A few of the switches have special names. One is named Bridged (also called VMnet0). It is used in the standard bridged networking configuration. Another is named Host-only (also called VMnet1). It is used in the standard host-only configuration. A third is named NAT (also called VMnet8). It is used in the standard network address translation configuration. The others are simply named VMnet2, VMnet3, VMnet4, and so on.

You connect a virtual machine to a switch by selecting the name of the switch you want in the Configuration Editor, using the panel that configures the virtual network adapter you want to connect to the switch.

***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 LAN through more than one physical Ethernet adapter on the host computer.

***Host-only adapter* —** The host-only adapter is a virtual Ethernet adapter that appears to your host operating system as VMware Virtual Ethernet Adapter on a Windows host and as the Host-Only Interface on a Linux host. It allows you to communicate between your host computer and the virtual machines on that host computer. It 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-only 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-only adapter is then created automatically when you boot the host computer.

Additional host-only adapters can be set up for use in custom configurations that need them.

***NAT device* —** The NAT (network address translation) device allows you to connect your virtual machines to an external network in situations where you have only one IP network address, 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, wireless Ethernet adapter or Token Ring card.

The NAT device is set up automatically if you choose NAT as the networking option when you set up a virtual machine.

***DHCP server* —** The DHCP (dynamic host configuration protocol) server provides IP network addresses to virtual machines in 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 (on a Windows host) or Configuration Wizard (on a Linux host) using any type of networking. It appears to the guest operating system as an AMD PCNET PCI adapter.

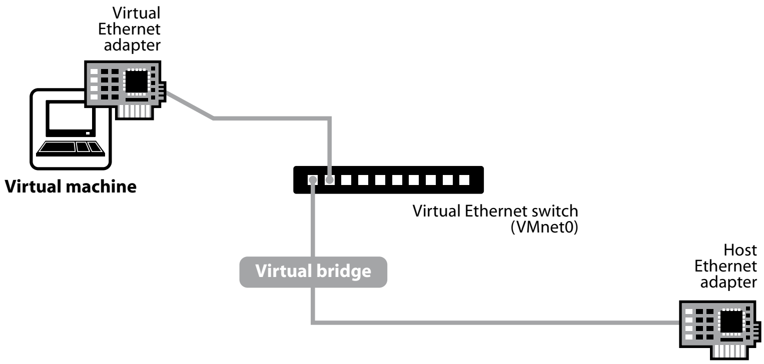
You can create and configure up to three virtual network adapters in each virtual machine using the Configuration Editor.

Common Networking Configurations

These 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 (on Windows hosts), Configuration Wizard (on Linux hosts) or Configuration Editor (on Windows or Linux hosts).

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 on Windows hosts or **Bridged networking** in the Configuration Wizard on Linux hosts. This selection is available 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.

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.

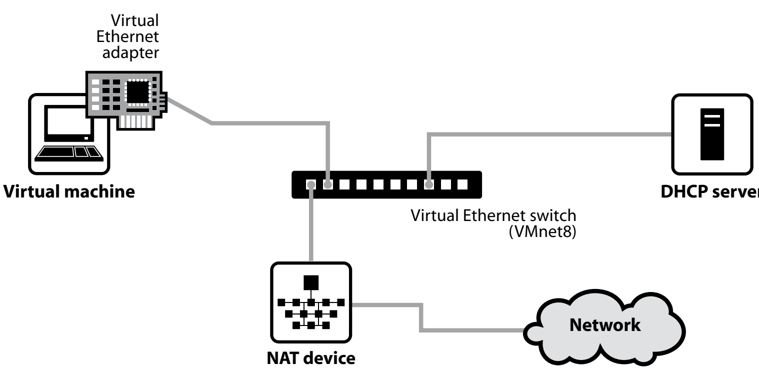
If you use bridged networking, the virtual machine is a full participant in the network. It has access to other machines on the network and can be contacted by other machines on the network as if it were a physical computer on the network.

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 (on Windows hosts) or Configuration Wizard (on Linux hosts) and later decide you want to use bridged networking, you can make that change in the Configuration Editor (**Settings** > **Configuration Editor**). For details, see Changing the Networking Configuration on page 285.

Note: You cannot use bridged networking if your host has a wireless NIC installed. If you want to run virtual machines on a host that uses wireless NICs, you need to configure your virtual machines to use NAT.

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 select **Use network address translation** in the New Virtual Machine Wizard on Windows hosts or **NAT** in the Configuration Wizard on Linux hosts.

If you want to connect to the Internet or other TCP/IP network using the host computer's dial-up networking 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.

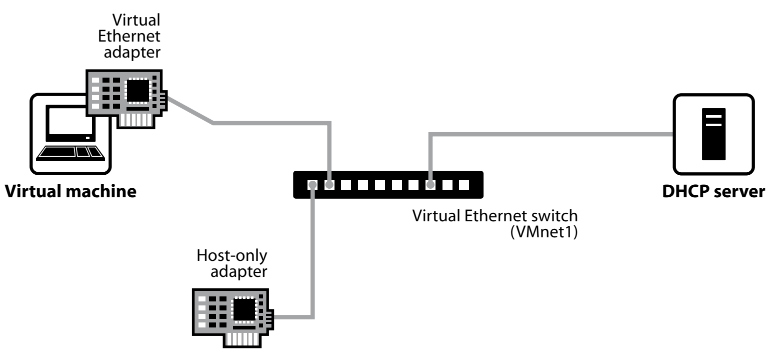
NAT also allows you to connect to a TCP/IP network using a wireless LAN adapter or Token Ring adapter on the host computer.

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 (on Windows hosts) or Configuration Wizard (on Linux hosts) and later decide you want to use NAT, you can make that change in the Configuration Editor (**Settings** > **Configuration Editor**). For details, see Changing the Networking Configuration on page 285.

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 Windows hosts or **Host-Only Networking** in the Configuration 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 very useful if you need to set up an isolated virtual network.

If you install the proper routing or proxy software on your host computer, you can establish a connection between the host-only 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 .NET Server 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.

If you use host-only networking, your virtual machine and the host-only 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 (on Windows hosts) or Configuration Wizard (on Linux hosts) and later decide you want to use host-only networking, you can make that change in the Configuration Editor (**Settings** > **Configuration Editor**). For details, see Changing the Networking Configuration on page 285.

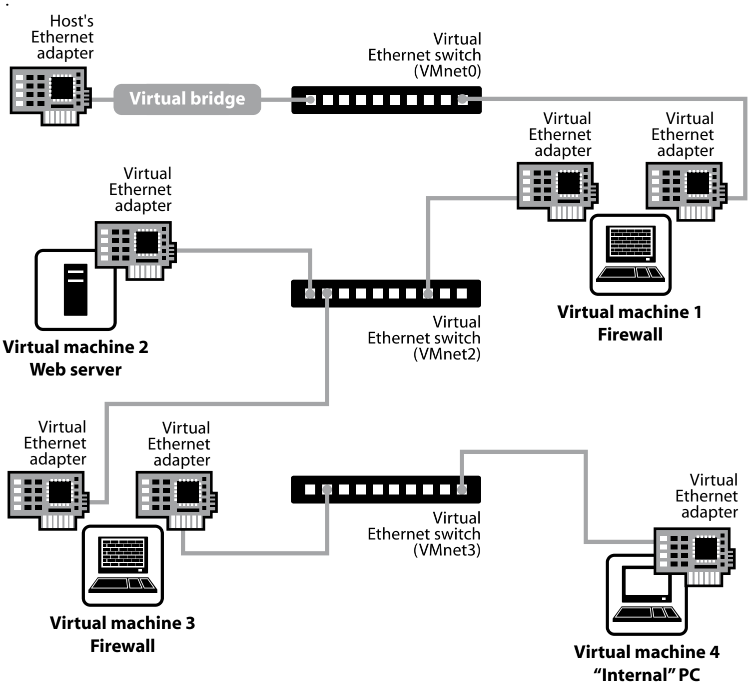
Custom Networking Configurations

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 293 and Understanding NAT on page 323.

.



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 Configuration 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 (on Windows hosts) or Configuration Wizard (on Linux hosts).

   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 Configuration Editor (**Settings** > **Configuration Editor**) to add a second virtual network adapter, as described in Changing the Networking Configuration on page 285. Connect the second adapter to **Custom (VMnet2)**.

   Click **OK** to save the configuration and close the Configuration Editor.

3. If VMware Workstation is not running, start it. Open virtual machine 2. Do not power on the virtual machine.

   Use the Configuration Editor (**Settings** > **Configuration Editor**) to add a virtual network adapter. Connect the adapter to **Custom (VMnet2)**.

   Click **OK** to save the configuration and close the Configuration Editor.

4. If VMware Workstation is not running, start it. Open virtual machine 3. Do not power on the virtual machine.

   Use the Configuration Editor (**Settings** > **Configuration Editor**) to add a virtual network adapter. Connect the adapter to **Custom (VMnet2)**.

   Use the Configuration Editor to add a second virtual network adapter. Connect the adapter to **Custom (VMnet3)**.

   Click **OK** to save the configuration and close the Configuration Editor.

5. If VMware Workstation is not running, start it. Open virtual machine 4. Do not power on the virtual machine.

   Use the Configuration Editor (**Settings** > **Configuration Editor**) to add a virtual network adapter. Connect the adapter to **Custom (VMnet3)**.

   Click **OK** to save the configuration and close the Configuration Editor.

6. Determine the network addresses used for VMnet2 and VMnet3.

   On a Windows host, open a command prompt on the host computer and run `ipconfig /all`. Note the network addresses used by each virtual switch.

   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 have decided to use with VMnet2.

   In virtual machine 2, assign an IP address in the range you have decided to use with VMnet2.

   In virtual machine 3, network adapters are connected to VMnet2 and VMnet3. Assign each adapter an IP address in the range you have decided to use with the virtual switch to which it is connected.

   In virtual machine 4, assign an IP address in the range you have decided to use with VMnet3.

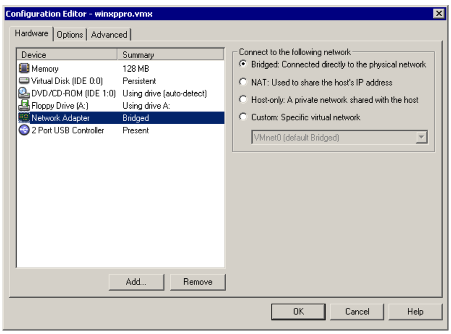
9. Install the necessary application software in each virtual machine.

Changing the Networking Configuration

Using the Configuration Editor (**Settings** > **Configuration Editor**), you can add virtual Ethernet adapters to your virtual machine and change the configuration of existing adapters.

Adding and Modifying Virtual Network Adapters

Windows Hosts



To add a new virtual Ethernet adapter, follow these steps.

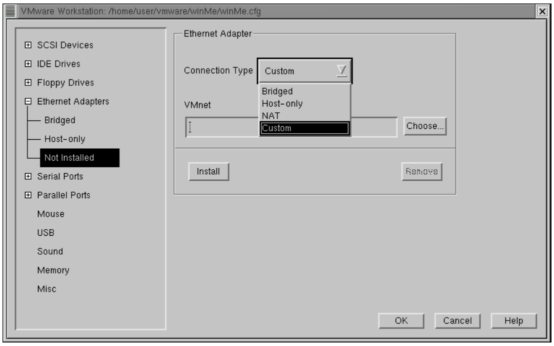
1. Be sure the virtual machine to which you want to add the adapter is powered off.
2. Open the Configuration Editor (**Settings** > **Configuration Editor**).
3. Click **Add**.
4. The Add Hardware Wizard starts. Select **Network Adapter**. Click **Next**.
5. Select the network type you want to use — **Bridged**, **NAT**, **Host-only** or **Custom**.
6. If you select **Custom**, choose the VMnet virtual switch you want to use for the network 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 Configuration Editor.

To change the configuration of an existing virtual network adapter, follow these steps.

1. Be sure the virtual machine with the adapter you want to modify is powered off.
2. Open the Configuration Editor (**Settings** > **Configuration Editor**).
3. Select the adapter you want to modify.
4. Select the network type you want to use — **Bridged**, **NAT**, **Host-only** or **Custom**.
5. If you select **Custom**, choose the VMnet virtual switch you want to use for the network from the drop-down list.
6. Click **OK** to save your changes and close the Configuration Editor.

Linux Hosts



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 Configuration Editor (**Settings** > **Configuration Editor**).
3. Click the **+** sign beside **Network Adapters**.
4. Select an adapter that is listed as **Not Installed**.
5. From the drop-down list, choose the network type you want to use — **Bridged**, **NAT**, **Host-only** or **Custom**.
6. If you choose **Custom**, enter the path to the VMnet virtual switch you want to use in the VMnet field. For example, if you want to use VMnet2, type `/dev/vmnet2`.
7. Click **Install** to install the new adapter.
8. Click **OK** to save your configuration and close the Configuration Editor.

To change the configuration of an existing virtual network adapter, follow these steps.

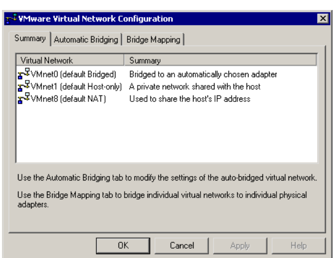
1. Be sure the virtual machine with the adapter you want to modify is powered off.
2. Open the Configuration Editor (**Settings** > **Configuration Editor**).
3. Click the **+** sign beside **Network Adapters**.
4. Select the adapter you want to modify.
5. Select the network type you want to use — **Bridged**, **NAT**, **Host-only** or **Custom**.
6. If you choose custom, enter the number of the VMnet virtual switch you want to use in the VMnet field. For example, if you want to use VMnet2, type `/dev/VMnet2`.
7. Click **OK** to save your changes and close the Configuration Editor.

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 NICs on your host to use for bridged networking. You can map specific NICs to specific virtual networks (VMnets).

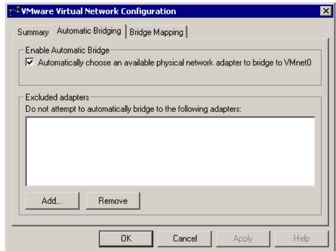
1. Open a VMware Workstation window.
2. Choose **Settings** > **Manage Virtual Networks**.



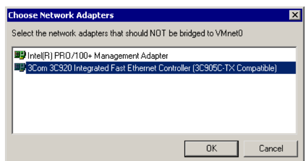
3. The VMware Virtual Network Configuration dialog box appears, with the **Summary** tab active. By default, the VMnet0 virtual switch is set up in bridged mode and bridges to one of the active Ethernet adapters on the host computer.

   The choice of which adapter it uses is arbitrary. You can restrict the range of choices using options on the **Automatic Bridging** tab.

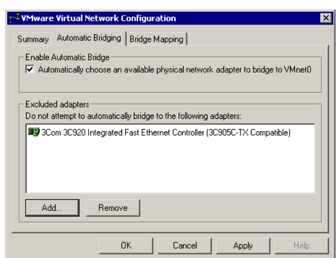
   (Also shown are VMnet1, the default virtual switch for host-only networking, and VMnet8, the default virtual switch for NAT, if they are enabled in VMware Workstation.)



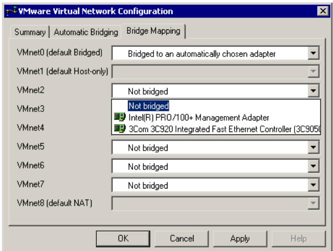
4. To exclude one or more physical Ethernet adapters from the list to which VMnet0 may be bridged, click the **Automatic Bridging** tab. To exclude an Ethernet adapter, click **Add** to add it to the list of excluded devices.



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 **Bridge 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 switch, any virtual machine using the original switch loses its network connectivity via that switch. 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. When you have made all the changes you want to make on all panels of the VMware Network Configuration dialog box, click **OK**.

Disabling and Removing NAT and Host-Only 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-only or NAT Adapter on a Windows Host

Windows XP and Windows .NET Server Hosts

1. Choose **Start** > **Settings** > **Control Panel**.
2. Double-click **Network and Dial-up Settings**.
3. Right-click the VMware Virtual Ethernet Adapter you want to disable. The host-only adapter is VMnet1; the NAT adapter is VMnet8.
4. In the pop-up menu, choose **Properties**.
5. Click **Configure**.
6. In the **Device Usage** pull-down list choose **Disable from this HW profile**.

Windows 2000 Hosts

1. Choose **Start** > **Settings** > **Network and Dial-up Connections**.
2. Right-click the VMware Virtual Ethernet Adapter you want to disable. The host-only adapter is VMnet1; the NAT adapter is VMnet8.
3. In the pop-up menu, select **Disable**.

Windows NT Hosts

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 adapter is VMnet1; the NAT adapter is VMnet8. Click **Disable**.

Removing a Host-only or NAT Adapter on a Windows Host

1. Log on as a member of the Administrators group.
2. Open a command prompt.
3. Change to the VMware Workstation program folder.

   ```
   cd \Program Files\VMware\VMware Workstation\Programs
   ```
4. Run the appropriate command to remove the adapter or adapters you want to uninstall.

   To remove the host adapter for the host-only network:

   ```
   vmware_netinstall -r *VMnet1
   ```

To remove the host adapter for the NAT network:

```
vmware_netinstall -r *VMnet8
```

To remove all host-only adapters:

```
vmware_netinstall -d
```

When the last host-only adapter is uninstalled, the VMnetDHCP service is also uninstalled automatically.

To uninstall the NAT service, take the following steps.

1. Log on as a member of the Administrators group.
2. Open a command prompt.
3. Change to the host's `system32` folder.

   ```
   cd \WINNT\system32
   ```

   If your computer uses a different path for this folder, adjust the command appropriately.
4. Run the uninstall command.

   ```
   vmnat -Uninstall
   ```

Removing a Host-only or NAT Adapter on a Linux Host

1. Become root and run the VMware Workstation configuration script.

   ```
   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 script 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 network adapters that have been configured. Select 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.

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, run `ipconfig` from a command prompt on a Windows host or `ifconfig` on a Linux host.

A NAT configuration also uses an unused private network automatically selected when you install VMware Workstation. To check what network is used in a Windows .NET Server, Windows XP, Windows 2000 or Windows NT guest, run `ipconfig`. In a Windows Me or Windows 9x guest, run `winipcfg`. In a Linux guest, run `ifconfig`.

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

Follow these steps to change the subnet of the DHCP server for the host-only network on VMnet1. In this example, you set the IP address of your host-only network to 192.168.3.1. To change the subnet used by a host-only DHCP server, you need to make the change to the IP address in two places: in the registry and in the `vmnetdhcp.conf` file.

1. Open the Windows registry.

   Choose **Start** > **Run**. Then type `regedit`.

2. Look for the registry key \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VMnetDHCP\Parameters\VirtualEthernetSegments\1.

   In that key, there is a value with the name HostIpAddress. The data is a hexadecimal value corresponding to the IP address of the host. Change this hexadecimal value to that of the new IP address. For example, the registry may contain the value 01dea8c0. This corresponds to the IP address 192.168.222.1.
   c0 = 192
   a8 = 168
   de = 222
   01 = 1

   Notice that the hexadecimal number seems backwards — with the pairs of digits in the opposite order from the way they are usually given when you write an IP address.

   Change the value of this registry key to 0103a8c0, which corresponds to 192.168.3.1.

3. Find the file `vmnetdhcp.conf` in the system directory. On most systems, this will be `C:\WINNT\system32\vmnetdhcp.conf`. Look for the text `Virtual ethernet segment 1` in the file. Sample text from the file:

```
# Virtual ethernet segment 1
# Added at 07/05/01 14:30:18
subnet 192.168.222.0 netmask 255.255.255.0 {
range 192.168.222.128 192.168.222.254; # up to 126 VMs
option broadcast-address 192.168.222.255;
option domain-name-servers 192.168.222.1;
option domain-name "localdomain";
}
host VMnet1 {
hardware ethernet 00:50:56:C0:00:01;
fixed-address 192.168.222.1;
option domain-name-servers 0.0.0.0;
option domain-name "";
}
```

   Replace all instances of the old IP address — 192.168.222.1 — with the new IP address — 192.168.3.1 — as shown below.

```
# Virtual ethernet segment 1
# Added at 07/05/01 14:30:18
subnet 192.168.3.0 netmask 255.255.255.0 {
range 192.168.3.128 192.168.3.254; # up to 126 VMs
option broadcast-address 192.168.3.255;
option domain-name-servers 192.168.3.1;
option domain-name "localdomain";
}
host VMnet1 {
hardware ethernet 00:50:56:C0:00:01;
fixed-address 192.168.3.1;
option domain-name-servers 0.0.0.0;
option domain-name "";
}
```

4. Reboot the host computer so the new settings will take effect.

To make corresponding changes to the DHCP server for the NAT network, follow the same procedure, with these changes:

- Edit the registry key \HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\VMnetDHCP\Parameters\VirtualEthernetSegments\8.

- In `vmnetdhcp.conf`, edit the sections that begin with
  `# Virtual ethernet segment 8`
  and
  `host VMnet8 {`

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 network, the available IP addresses are split up using the conventions shown in the table below, where <net> is the network number assigned to your host-only 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>.254	DHCP-assigned	192.168.0.128–192.168.0.254
<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>.254	DHCP-assigned	192.168.0.128–192.168.0.254
<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 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 choose 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:
>
> A. Open the i386 folder on the applicable Windows 2000 Server disc.
>
> B. Double-click the `adminpak.msi` file. Follow the instructions that appear in the Windows 2000 Administration Tools Setup wizard.
>
> C. After Windows 2000 Administration Tools are installed, most of the server administrative tools can be accessed by choosing **Start** > **Programs** > **Administrative Tools**.

Windows .NET Server is not yet released. However, the steps for checking and disabling IP forwarding in beta versions are the same as those for server versions of Windows 2000.

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.

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 a MAC address. MAC stands for media access control. A MAC address is the unique address assigned to each physical network device.

The software guarantees that virtual machines are assigned unique MAC addresses within a given host system. However, the software does not guarantee that a given virtual machine is assigned the same MAC address every time it is powered on. In addition, VMware Workstation does its best, but cannot guarantee, to automatically assign unique MAC addresses for virtual machines running on multiple host systems.

If you want to guarantee that the same MAC address is assigned to a given virtual machine every time, 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 manually assign the same, unique MAC address to any virtual machine, use a text editor to add the following line to its configuration file (the `.vmx` file on a Windows host or `.cfg` file on a Linux host):

```
ethernet0.address = 00:50:56:XX:YY:ZZ
```

where `XX` must be a valid hex number between `00h` and `3Fh`, and `YY` and `ZZ` must be valid hex numbers between `00h` and `FFh`. Because VMware Workstation virtual machines do not support arbitrary MAC addresses, the above format must be used.

So long as you choose `XX:YY:ZZ` so it is unique among your hard-coded addresses (where `XX` is a valid hex number between `00h` and `3Fh`, and `YY` and `ZZ` are valid hex 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.

If either of these programs is being run only to receive routing information, the easiest solution is to run them with a `-q` option so that they do not supply routing information, only receive 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 to the `dhcpd` configuration file of the form:

```
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 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 it 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 the Version 2 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. But it does not currently 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).

This facility is scheduled to be part of the Version 3 DHCP server available from the Internet Software Consortium. When that is available VMware will update VMware Workstation to use that server.

In the meantime, 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)`.

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 chapter 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 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 script 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 script 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 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
```

Configuring a Virtual Machine to Switch Network Adapters on a Windows NT Host

You may find it helpful to configure a virtual machine so it can use one network adapter when you are in one location and a different network adapter when you are somewhere else. The most common case involves a laptop computer that is sometimes used with a PC Card (PCMCIA) adapter and sometimes docked in a docking station that has its own network adapter.

The Approach

If you are using bridged networking on a Windows NT 4.0 host, the steps in the next section allow you to configure your virtual machine so it can use both network adapters, with each adapter on a different virtual network interface.

Note: On a Windows 2000, Windows XP or Windows .NET Server host, it is more convenient to configure your adapters using the procedure described in Configuring Bridged Networking Options on a Windows Host on page 287.

You need to create two separate VMware Workstation configuration files (`.vmx` files), both of which point to the same virtual or raw disk. One uses a standard bridged networking setup on the VMnet0 virtual switch. The other uses VMnet2. You use one configuration when you want to connect to a network using the PC Card network adapter and the other when you want to use the docking station's adapter.

Step By Step

1. Follow the usual steps to configure your VMware Workstation virtual machine with one network adapter in place. (In later steps, these instructions assume that this is the PC Card adapter.) Use bridged networking. Test the setup to be sure the virtual machine can boot and run with that network adapter.
2. After you have tested the initial configuration, shut down your virtual machine and exit VMware Workstation. Switch the setup so the other network adapter is being used. For example, if you first configured the computer while the PC Card adapter was in use, you should now set the computer up in the docking station so its adapter is in use.

3. Open a command prompt.
4. Change to the VMware Workstation programs folder. If you have installed VMware Workstation in the default location, the command is
`cd Program Files\VMware\VMware Workstation\Programs`
5. Run the following command.
`vnetconfig -s -ib vmnet2`
6. If you get a dialog box that asks which network adapter to use, choose the adapter that is currently installed (not the one you already configured for bridged networking in step 1).
7. Open the Windows NT Services control panel (**Start** > **Settings** > **Control Panel** > **Services**) and be sure that you now have two services for VMnet Bridge (one for VMnet0 and one for VMnet2).
8. Start the service **VMnet Bridge (for VMnet2)**. If it doesn't start, reboot the system and try to start it again.
9. Open the folder where the files for the virtual machine you are configuring are stored.
10. Copy the `.vmx` file under a different name, so that you have two copies — one to use when you are using the PC Card adapter (referred to here as `pcmcia.vmx`) and one to use when you are using the network adapter in the docking station (referred to here as `nic.vmx`).
11. Launch VMware Workstation, select **Open Existing Virtual Machine**, and open the `.vmx` file for the network adapter you will set up on VMnet2 (`nic.vmx` in our example). You probably need to browse to it.
12. Open the Configuration Editor (**Settings** > **Configuration Editor**) and choose **Network Adapter**.
13. From the drop-down list on the right, choose **Custom (VMnet2)**.
14. Be sure the **Save Configuration Changes** check box is checked, then click **OK** to save your changes and close the Configuration Editor.

Now you are ready.

When you are using the PC Card adapter, launch your virtual machine using `pcmcia.vmx`. When you are using the adapter in the docking station, use `nic.vmx`.

Both `.vmx` files are for the same virtual machine. When you choose one, you are just choosing which network adapter to use.

Note: If you make changes to other aspects of one configuration, remember to make the same changes to the other configuration the next time you open it.

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 script.

   ```
   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 was set up when you ran the `vmware-config.pl` script 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 script 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 – Windows NT Host

Follow these steps to set up the second host-only interface on Windows NT.

1. Open a command prompt window. Change to the VMware Workstation programs folder. If you accepted the default path, use this command:

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

2. Run the following command:

   ```
   vnetconfig -ih vmnet2
   ```

Setting Up the Second Host-Only Interface – Windows 2000 Host

1. Open the Control Panel (**Start** > **Settings** > **Control Panel**).
2. Start the Add/Remove Hardware Wizard from the Control Panel.

   Note: You must have sufficient privileges to do this.

3. Click **Next** to continue past the Welcome screen.
4. Select **Add/Troubleshoot a Device** and click **Next**.
5. Wait while Windows searches for new Plug and Play devices, then select **Add a New Device** from the Choose a Hardware Device screen and click **Next**.
6. Select **No, I want to select the hardware from a list** and click **Next**.

7. Select **Network Adapters** from the list and click **Next**.
8. Select **VMware, Inc.** from the manufacturers list on the Select Network Adapter screen to get the list of available host-only network adapters. Select **VMware Virtual Ethernet Adapter (for VMnet2)** and click **Next**.
9. Click **Next** in the Start Hardware Installation screen.
10. Click **Yes** when prompted that the Microsoft digital signature is not present for the software about to be installed.
11. Click **Finish** on the screen that indicates the adapter has been installed.

Setting Up the Second Host-Only Interface – Windows XP or Windows .NET Server Host

1. Start the Add Hardware Wizard.

   Start > **Control Panel** > **Add Hardware**

   Note: You must have sufficient privileges to do this.
2. Click **Next**.
3. When prompted, select **Yes, I have already connected the hardware**.
4. On the screen that lets you select the hardware, select **Add a new hardware device**, then click **Next**.
5. Select **Install the hardware that I manually select from a list (Advanced)**.
6. Select **Network Adapter**.
7. Select **VMware, Inc.** as the manufacturer.
8. Select the host-only adapter for the appropriate VMnet.
9. Click **Yes** when prompted that the Microsoft digital signature is not present for the software about to be installed.
10. Click **Finish** on the screen that indicates the adapter has been installed.

Setting Up the Second Host-Only Interface – Linux Host

1. As root (`su`), run the VMware Workstation configuration script.

   ```
   /usr/bin/vmware-config.pl
   ```
2. Use the wizard to modify your configuration. After asking about a NAT network, the script 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.

Configuring the Virtual Machines

Now you have two host-only interfaces (VMnet1 and VMnet2). You are ready to configure your virtual machines for one of the following scenarios:

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).

Scenario 1 – Connect to the Default Host-Only Interface

1. Create the virtual machine using the New Virtual Machine Wizard (on a Windows host) or Configuration Wizard (on a Linux host) or use an existing virtual machine.

2. Launch VMware Workstation and open the virtual machine.

3. Edit the configuration using the Configuration Editor (**Settings** > **Configuration Editor**).

   Windows host: 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.

Linux host: Click the + sign to expand the Ethernet Adapters list and select the first adapter. From the Connection Type drop-down list on the right, select Host-only.

If the list of devices indicates the adapter is not installed, click Install.

Scenario 2 – Connect to the Newly Created Host-Only Interface

1. Create the virtual machine using the New Virtual Machine Wizard (Windows hosts) or Configuration Wizard (Linux hosts) or use an existing virtual machine.
2. Launch VMware Workstation and open the virtual machine.
3. Edit the configuration using the Configuration Editor (Settings > Configuration Editor).

   Windows host: 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.

   Linux host: Click the + sign to expand the Ethernet Adapters list and select the first adapter. From the Connection Type drop-down list on the right, select Custom. In the VMnet field, type `/dev/vmnet2`.

   If the list of devices indicates the adapter is not installed, click Install.

Scenario 3 – Connect to Two Host-Only Interfaces

1. Create the virtual machine using the New Virtual Machine Wizard (on a Windows host) or Configuration Wizard (on a Linux host) or use an existing virtual machine.
2. Launch VMware Workstation and open the virtual machine.
3. Edit the configuration using the Configuration Editor (Settings > Configuration Editor).

   Windows host: 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.

   Linux host: Click the + sign to expand the Ethernet Adapters list and select the first adapter. From the Connection Type drop-down list on the right, select Host-only.

If the list of devices indicates the adapter is not installed, click **Install**.

Select the second adapter and, from the **Connection Type** drop-down list on the right, select **Custom**. In the **VMnet** field, type `/dev/vmnet2`.

If the list of devices indicates the adapter is not installed, click **Install**.

At this point you can power on the virtual machine and install your guest operating system. In scenarios 1 and 2 you see one AMD PCNet Family Adapter. In scenario 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` script 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 script again to set up host-only networking.

Setting Up the Second Host-Only Interface – Windows NT Host

Follow these steps to set up the second host-only interface on Windows NT.

1. Open a command prompt window. Change to the VMware Workstation programs folder. If you accepted the default path, use this command:

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

2. Run the following command:

```
vnetconfig -ih vmnet2
```

This creates a second host-only adapter, which can be configured from the Network control panel.

Setting Up the Second Host-Only Interface – Windows 2000 Host

1. Open the Control Panel (**Start** > **Settings** > **Control Panel**).
2. Start the Add/Remove Hardware Wizard from the Control Panel.

   Note: You must have sufficient privileges to do this.
3. Click **Next** to continue past the Welcome screen.
4. Select **Add/Troubleshoot a Device** and click **Next**.
5. Wait while Windows searches for new Plug and Play devices, then select **Add a New Device** from the Choose a Hardware Device screen and click **Next**.
6. Select **No, I want to select the hardware from a list** and click **Next**.
7. Select **Network Adapters** from the list and click **Next**.
8. Select **VMware, Inc.** from the manufacturers list on the Select Network Adapter screen to get the list of available host-only network adapters, then select **VMware Virtual Ethernet Adapter (for VMnet2)** and click **Next**.
9. Click **Next** in the Start Hardware Installation screen.
10. Click **Yes** when prompted that the Microsoft digital signature is not present for the software about to be installed.
11. Click **Finish** on the screen that indicates the adapter has been installed.

Setting Up the Second Host-Only Interface – Windows XP or Windows .NET Server Host

1. Start the Add Hardware Wizard.

   Start > **Control Panel** > **Add Hardware**

   Note: You must have sufficient privileges to do this.
2. Click **Next**.
3. When prompted, select **Yes, I have already connected the hardware**.
4. On the screen that lets you select the hardware, select **Add a new hardware device**, then click **Next**.
5. Select **Install the hardware that I manually select from a list (Advanced)**.
6. Select **Network Adapter**.

7. Select **VMware, Inc.** as the manufacturer.
8. Select the host-only adapter for the appropriate VMnet.
9. Click **Yes** when prompted that the Microsoft digital signature is not present for the software about to be installed.
10. Click **Finish** on the screen that indicates the adapter has been installed.

Setting Up the Second Host-Only Interface – Linux Host

1. As root (`su`), run the VMware Workstation configuration script.

   ```
   /usr/bin/vmware-config.pl
   ```
2. Use the wizard to modify your configuration. After asking about a NAT network, the script 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 (on a Windows host) or Configuration Wizard (on a Linux host) or use an existing virtual machine.
2. Launch VMware Workstation and open the virtual machine.
3. Edit the configuration using the Configuration Editor (Settings > Configuration Editor).

   Windows host: 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.

   Linux host: Click the + sign to expand the Ethernet Adapters list and select the first adapter. From the Connection Type drop-down list on the right, select Host-only.

   If the list of devices indicates the adapter is not installed, click Install.

Virtual Machine 2 – Connected to the Newly Created Host-Only Interface

1. Create the virtual machine using the New Virtual Machine Wizard (on a Windows host) or Configuration Wizard (on a Linux host) or use an existing virtual machine.
2. Launch VMware Workstation and open the virtual machine.
3. Edit the configuration using the Configuration Editor (Settings > Configuration Editor).

   Windows host: 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.

   Linux host: Click the + sign to expand the Ethernet Adapters list and select the first adapter. From the Connection Type drop-down list on the right, select Custom. In the VMnet field, type `/dev/vmnet2`.

   If the list of devices indicates the adapter is not installed, click Install.

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 (on a Windows host) or Configuration Wizard (on a Linux host) or use an existing virtual machine.
2. Launch VMware Workstation and open the virtual machine.
3. Edit the configuration using the Configuration Editor (Settings > Configuration Editor).

   Windows host: 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.

   Linux host: Click the + sign to expand the Ethernet Adapters list and select the first adapter. From the Connection Type drop-down list on the right, select Host-only.

   If the list of devices indicates the adapter is not installed, click Install.

   Select the second adapter, then from the Connection Type drop-down list on the right, select Custom. In the VMnet field, type `/dev/vmnet2`.

   If the list of devices indicates the adapter is not installed, click Install.

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: In the Services control panel, find VMware DHCP Server and be sure it is stopped.

   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/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/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/write access to the VMnet device, you can create a new group, add the appropriate users to the group and grant that group read/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 in VMware Workstation

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 an adapter on the NAT network (identical to the host-only 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 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 a DHCP request. 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 uses 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 it 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 manually configure port forwarding on the NAT device so network traffic destined for a certain port can still be automatically forwarded 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 shares on the host known by the WINS server as long as they are in the same workgroup or domain.

Advanced NAT Configuration

Use the NAT configuration file on the host to configure the NAT device.

On Windows, this file is `vmnetnat.conf`. It is located in the host operating system's system folder (normally `C:\WINNT\system32`).

On Linux, 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 Windows vmnetnat.conf File on page 330. 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 will be 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 serves 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 creates a mapping from port 8887 on the host to the IP address 192.168.27.128 and port 21. When this 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 creates a mapping from port 6000 on the host to the IP address 192.168.27.128 and port 6001. When this 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.

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 (Windows Hosts and Virtual Machines Only)

When using NAT networking in a virtual machine with a Windows guest operating system running on a Windows host, you can utilize NetLogon to log on to a Windows domain from the virtual machine. This allows you to 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 only explains how to set up the virtual machine to use NetLogon. The setup process is similar to the way you would 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 the virtual machine can connect to the 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 .NET Server 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, select **Internet Protocol (TCP/IP)**, then click **Properties**.
4. In the TCP/IP Properties dialog, 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, select **Internet Protocol (TCP/IP)**, then click **Properties**.
4. In the TCP/IP Properties dialog, 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 you want to connect to 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 Administrator's user ID and password of the domain controller.

Note: You can access shares of virtual machines that are only on the same NAT network or are bridged on the same domain.

Sample Windows vmnetnat.conf File

```
# Windows 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
```

10

Video and Sound

Configuring Video and Sound in VMware Workstation 3.2

The following sections provide information on configuring the video display and sound for VMware Workstation.

Setting Screen Colors in a Virtual Machine

The number of screen colors available inside a virtual machine depends on the screen color setting of the host computer.

On a Windows host, all guests support

- The number of colors set on the host at the time the guest operating system was started
- 256 colors (8-bit mode)
- In some cases, 16 colors (4-bit mode)

On a Linux host, all guests support

- The same number of colors as set on the host

If you run a virtual machine set for a greater number of colors than your host computer is using, you can encounter various problems. In some cases, for example, the colors in the guest will not be correct. In others, the virtual machine will not be 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.

Changing Screen Colors on the Host

If you choose to change the color settings on your host computer, you should first shut down the guest operating system, power off the virtual machine and close VMware Workstation.

Follow standard procedures for changing the color settings on your host computer, then restart VMware Workstation and the virtual machine.

Changing Screen Colors in the Guest

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.

Windows Hosts

Follow the normal process for changing screen colors in your guest operating system. In a Windows guest, the Display Properties control panel offers only settings that are supported.

Linux Hosts

A Windows guest running on a Linux host adjusts automatically to the number of colors supported on the host computer. You do not need to take any special steps.

In a Linux or FreeBSD guest, you must change the color depth before you start the X server.

Changing XFree86 Video Resolutions on a Linux Host

You can configure VMware Workstation on a Linux host to change the full-screen display resolution to better match the resolution set in the guest operating system. On a Windows host, this is done by default and you do not need to change any configuration settings.

VMware Workstation uses the VidMode extension from the XFree86 Project to match the host resolution to the one requested by the guest running in the virtual machine.

Configuration

The option **Find best resolution in full screen mode** is on by default. When on, this option allows VMware Workstation to locate the best resolution for your host operating system, thus minimizing or eliminating the black border that earlier versions of VMware Workstation displayed when the guest operating system was in full screen mode.

You can change the default for **Find best resolution in full screen mode** by going to the **Misc** panel in the Configuration Editor (**Settings** > **Configuration Editor**).

Possible Issues

In a few cases, the **Find best resolution …** option may not give the best results.

X Server Configuration

The VidMode extension can choose only resolutions that are already configured in the `XF86Config` file on your host. A sample configuration for a given color depth could look like this:

```
Subsection "Display"
Depth 16
Modes "1280x1024" "1024x768" "800x600"
ViewPort 0 0
EndSubsection
```

In this case, VMware Workstation is able to match a virtual machine running at 1280×1024, 1024×768 or 800×600 but not at 640×480 or 1152×900. If a virtual machine runs at a resolution that does not match a mode listed in the XFree86 configuration, then VMware Workstation chooses the closest larger mode or else simply does not switch modes at all.

It is possible to have bad modes configured in the `XF86Config` file on your host. If your XFree86 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 VidMode 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 either disable the mode switching code in VMware Workstation or fix your XFree86 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.

Mouse Movement

The mouse may completely fail to move while in a full-screen mode virtual machine.

In XFree86 version 3.3.3.0 the DirectMouse interface does not operate properly. The interface works correctly in previous and subsequent releases of XFree86. XFree86 version 3.3.3.0 was not included in any mainstream Linux distributions.

If you have an X server based on XFree86 version 3.3.3.0, you cannot move the mouse while in full-screen mode with the VidMode extension enabled. To resolve the problem, either disable video resolution switching in VMware Workstation or update your X server.

To disable video resolution switching in VMware Workstation, choose **Settings** > **Configuration Editor**, and deselect **Find best resolution…** in the **Misc** panel.

Configuring Sound in VMware Workstation

VMware Workstation provides a Creative Labs Sound Blaster 16 compatible audio device and supports sound in Windows 95, Windows 98, Windows Me, Windows NT, Windows 2000, Windows XP, Windows .NET Server and Linux guest operating systems. The VMware Workstation sound device is disabled by default and must be enabled with the Configuration Editor (**Settings** > **Configuration Editor**). Sound support is currently limited to PCM (pulse code modulation) output (that is, any application that produces sound without using MIDI).

Setting Up a Virtual Sound Card on a Windows Host

1. Be sure your physical sound card is installed and configured properly on the Windows host operating system. Refer to the documentation for your particular Windows operating system. You may need to install additional software on your system to support sound. VMware cannot provide support assistance in configuring sound on your host operating system. Please contact your host operating system support provider or sound card manufacturer for help.
2. Add a virtual sound adapter to the virtual machine. By default, the virtual sound adapter is not installed in the virtual machine.
3. In the Configuration Editor (**Settings** > **Configuration Editor**), click **Add**. The Add Hardware Wizard appears.
4. Select **Sound Adapter**, then click **Next**.

   If you have more than one physical sound adapter in your host computer, you can choose which one to connect to the virtual sound adapter. You can also choose whether the virtual sound adapter should be connected when the virtual machine starts.
5. Click **Finish**.
6. Click **OK** to close the Configuration Editor.
7. Configure the guest operating system to use the VMware Workstation virtual sound adapter. This adapter is compatible with a Creative Labs Sound Blaster 16.

Setting Up a Virtual Sound Card on a Linux Host

1. Be sure your physical sound card is installed and configured properly on the Linux host operating system. Refer to the documentation for your particular Linux operating system. You may need to install additional software on your system to support sound. VMware cannot provide support assistance in configuring sound on your host operating system. Please contact your host operating system support provider or sound card manufacturer for help.
2. Add a virtual sound adapter to the virtual machine. By default, the virtual sound adapter is not installed in the virtual machine.
3. In the Configuration Editor (**Settings** > **Configuration Editor**), click **Sound**.
4. Provide the device name in the **Device** field. Type in or browse to the device that represents your sound card (for example, `/dev/dsp`).
5. Click the **Install** button, then click **OK** to save the configuration and close the Configuration Editor.

Setting Up Sound in the Guest Operating System

Use your guest operating system's configuration tools to set up the virtual sound adapter.

Sound in a Windows XP or Windows .NET Server Guest

1. Click the Printers and Other Hardware link in the Windows XP or Windows .NET Server Control Panel (**Start** > **Control Panel**).
2. In the See Also pane, click **Add Hardware**, then click **Next**.
3. Select **Yes, I have already connected the hardware**, then click **Next**.
4. In the Installed Hardware list, select **Add a new hardware device**, then click **Next**.
5. Select **Install the hardware that I manually select from a list (Advanced)**, then click **Next**.
6. Select **Sound, video and game controllers**, then click **Next**.
7. Select **Creative Technology Ltd.** in the Manufacturer list and **Sound Blaster 16 or AWE32 or compatible (WDM)** in the list of devices, then click **Next**.
8. Click **Next**.
9. Click **Finish**.

Sound in a Windows 2000 Guest

1. Double-click the Add/Remove Hardware icon in the Windows 2000 Control Panel (**Start** > **Settings** > **Control Panel**).
2. In the Add/Remove Hardware Wizard dialog box, select **Add a New Device** and click **Next**.
3. In the Find New Hardware dialog box, select **No, I want to select the hardware from a list** and click **Next**.
4. In the Hardware Type dialog box, select **Sound, video and game controllers** from the list and click **Next**.
5. In the Select a Device Driver dialog box, select **Creative** from the manufacturers list and select **Sound Blaster 16 or AWE32 or compatible (WDM)** from the models list, then click **Next**.
6. In the Start Hardware Installation dialog box, click **Next** to install the Sound Blaster 16 drivers.
7. In the Completing the Add/Remove Hardware Wizard dialog box, click **Finish** and reboot the virtual machine. Sound should be working the next time the virtual machine boots Windows 2000.

Sound in a Windows NT Guest

If you have never installed a Sound Blaster 16 Card in this Windows NT system, you need a Windows NT 4.0 installation CD-ROM.

1. Double-click the Multimedia icon in the Windows NT Control Panel (**Start** > **Settings** > **Control Panel**).
2. Click the **Devices** tab.
3. Click the **Add** button.
4. Select the **Creative Labs Sound Blaster 1.X, Pro, 16**, then click **OK**.
5. Insert the Windows NT 4.0 CD-ROM in the CD-ROM drive when prompted.
6. Specify `D:\I386` (where `D:` is your CD-ROM drive), then click **OK**.
7. Configure the Sound Blaster base I/O Address.

I/O address
0x220

Click **OK**.

8. Complete the Sound Blaster 16 Configuration.

IRQ	8-bit DMA	16-bit DMA	MPU-401 I/O address
5	1	7	Disable (MPU-401 MIDI device is not supported)

   Click **OK**.

9. When prompted to restart, click **Restart Now**.

Sound in a Windows 95 or Windows 98 Guest

If you have never installed a Sound Blaster 16 Card in this Windows guest operating system, you need a Windows 95 or Windows 98 installation CD-ROM.

1. Double-click the Add New Hardware icon in the Windows Control Panel (**Start** > **Settings** > **Control Panel**).

   Click **Next**.

2. Select **Yes** for **Do you want Windows to search for new hardware?**

   Click **Next**.

3. Click **Next** again. Windows runs the autodetection and says it is ready to finish.

4. If prompted to do so, insert the Windows CD-ROM into the drive and click **OK**.

   Click **Finish**.

If you have problems with Windows autodetection, add the device manually.

1. Double-click the Add New Hardware icon in the Windows Control Panel (**Start** > **Settings** > **Control Panel**).

   Click **Next**.

2. Select **No** for **Do you want Windows to search for new hardware?**

   Click **Next**.

3. Select **Sound, video and games controllers**.

   Click **Next**.

4. Select **Creative Labs Sound Blaster 16 or AWE-32**.

   Click **Next**.

   Click **Finish**.

Sound in a Linux Guest

1. Refer to the documentation for your particular Linux distribution. You may need to install additional software packages on your system to support sound.
2. When configuring the sound, please use the following parameters:

I/O port	IRQ	8-bit DMA	16-bit DMA
0x220	5	1	7

Known Limitations of Sound Support in VMware Workstation

Sound support is provided for Sound Blaster compatible PCM (pulse code modulation) output. This gives you the ability to play `.wav`, `.au` and Real Audio formats, among others.

MIDI sound is not supported.

Game ports and devices such as joysticks attached to game ports are not supported.

Sound does not work well with certain games, especially fast, interactive games.

Improving Sound Performance

If you notice that sound skips in your guest operating system, you may try adding two variables to your virtual machine's configuration file (`.vmx` on Windows hosts, `.cfg` on Linux hosts). These variables are `sound.maxLength` and `sound.smallBlockSize`.

VMware cannot provide you with specific settings to use; how these settings affect your sound quality depends on many factors, including your environment and the way you are employing sound. But here are some general rules of thumb to use when setting these variables:

- Set these values to powers of 2, such as 64, 128 or 512.
- To overcome skipping, setting these values lower than 512 should help.
- The `sound.maxLength` setting should be greater than or equal to the `sound.smallBlockSize` setting.

11

Connecting Devices

Using Devices with a Virtual Machine

The following sections describe how to use various devices with a virtual machine:

Using Parallel Ports

The following sections describe how to use parallel ports with VMware Workstation:

VMware Workstation supports two types of virtual parallel port devices: unidirectional ports (SPP) and a partial emulation of bidirectional PS/2-style ports.

Bidirectional ports are supported on all Windows hosts.

Unidirectional ports are supported in all Linux versions. Bidirectional ports are supported in Linux kernel versions 2.2.5 or later.

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 bidirectional 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.

Unidirectional Ports

Unidirectional ports are supported for backward compatibility. They are used typically to connect to printers or to send the printer output to a file. The speed is usually adequate for printing text, but expect long delays when printing images.

On a Linux host, the path names of the host devices for unidirectional ports are typically `/dev/lp0`, `/dev/lp1`, etc.

Bidirectional Ports

Bidirectional ports are used by a variety of devices — printers, scanners, dongles and disk drives, for example.

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. Below is a partial list of devices known to work. If you try out a device that is not on the list, please let VMware know.

Bidirectional emulation is slower than native access but faster than unidirectional emulation, so bidirectional mode is recommended, when possible, even when the device connected to the port is unidirectional (a printer, for example).

Default Configuration

When parallel ports are set up on a Windows host, they are bidirectional by default. Their default base addresses are, in order, 0x3bc, 0x378 and 0x278. None of the ports have an assigned IRQ or DMA channel. The ports are not present by default.

When parallel ports are set up on a Linux host, they are bidirectional by default on Linux hosts with kernel 2.2 or higher. Otherwise, they are unidirectional. Their default base addresses are in order, 0x3bc, 0x378 and 0x278. None of the ports have an assigned IRQ or DMA channel. The ports are not present by default.

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 port(s) at boot time. Others, like Windows 9x, do not.

To add a parallel port to the virtual machine's configuration, take these steps with the virtual machine powered off.

Windows Hosts

1. Open the Configuration Editor.

   Settings > Configuration Editor

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. If you want the parallel port output to go to a file, enter the path and filename or browse to the location of the file.

   Click Finish.

Linux Hosts

1. Open the Configuration Editor.

   Settings > Configuration Editor

2. Click the + sign beside Parallel Ports to expand the list of devices.
3. Select a device that is shown as Not Installed.
4. From the Type drop-down list, select Device to connect to a physical parallel port on the host or File to send the output to a file.
5. In the Path field, enter the path to the device or file you want to use.

   The path names of the host devices for bidirectional parallel ports are usually `/dev/parport0`, `/dev/portport16`, `/dev/parport32`, etc. The VMware Workstation installer creates these devices if they do not exist. They may also be created by hand using `mknod`. For example, to create the second parallel port (`parport16`) use this command:

   ```
   mknod /dev/parport16 c 99 16
   ```

6. Click Install to install the virtual parallel port, then click OK to save the configuration and close the Configuration Editor.

In a Windows 9x guest, when you change a port from unidirectional to bidirectional or vice versa, you must use the Device Manager (Start > Settings > Control Panel > System > Device Manager) to remove the device driver for that port and add a new one. Adding a new driver is also required when a new port is added. In both cases use the guest operating system's Add New Hardware Wizard (Start > Settings > Control Panel > Add New Hardware) and let Windows detect the new device. Manually selecting the device from a list may result in an incorrect configuration.

Troubleshooting

If an error message appears at power on stating the parallel port on the host does not have an ECR (extended control register), it is possible the hardware supports it but it has been disabled in the BIOS. In this case, reboot your host computer, enter the BIOS configuration editor (typically by holding down the Delete key during early execution of the BIOS), find the parallel port field, and enable ECP mode (or other combination of modes that include ECP). Most modern computers should support ECP mode.

Configuring a Bidirectional Parallel Port on a Linux Host

For the bidirectional 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 required modules.

Bidirectional Parallel Ports and Linux 2.2.x Kernels

The 2.2.x kernels that support bidirectional parallel ports use the `parport`, `parport_pc` and `vmppuser` modules. Also, be sure that PC Style Hardware (CONFIG_PARPORT_PC) is loaded as a module, as mentioned at the beginning of this section on using parallel ports. 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 inserts the three modules needed for a bidirectional 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
```

The `lp` module is necessary only for unidirectional parallel ports.

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 # 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 bidirectional 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
```

Bidirectional 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 this section on using parallel ports. If you are using a 2.4.x kernel, the modules that provide bidirectional 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 inserts the three modules needed for a bidirectional 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
```

The `lp` module is necessary only for unidirectional parallel ports.

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 # 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 bidirectional 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 use the **Devices** menu 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.

Devices You Can Use on a Bidirectional Parallel Port

Devices Known to Work

Adobe dongle	Windows 95 guest
RIO MP3 player	Windows 95 guest
UMAX Astra 1220 P scanner	Windows 95 guest
Hewlett-Packard LaserJet 5MP printer	Windows 9x and Windows NT/2000 guests
Canon Bubble Jet BJ-200e printer	Windows 9x and Windows NT/2000 guests
Iomega ZIP drive	Linux, Windows NT, and Windows 2000 guest only (see Special Notes for the Iomega Zip Drive, below)

Devices That Probably Work

Dongles	Most dongles are likely to work.
Printers	Most printers are likely to work.
Hewlett-Packard Deskjet 710C	Reported by customer.
Hewlett-Packard Deskjet 722C	Reported by customer.
Epson 750 printer in bidirectional mode	Reported by customer.
CARDport Swift Smart Media Digital Image Reader/Writer from Chase Advanced Technologies	Reported by customer.
Logitech Scanman Color 2000 (parallel port hand scanner)	Reported by customer.
Plustek Optic Pro 9636T Flatbed Scanner	Reported by customer.
Creative Labs WebCam II (parport version)	Reported by customer.

Special Notes for the Iomega Zip Drive

On Windows 9x, 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

The following sections describe how to use serial ports with VMware Workstation:

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.

Note: The serial port implementation is new in this release and deprecates the use of TTY type of virtual serial ports in a virtual machine.

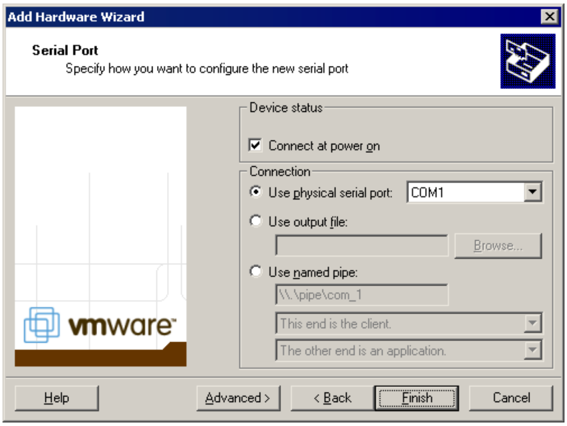
Using a Serial Port on the Host Computer

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:

Windows Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
2. Click **Add…** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.



4. Select **Use Physical Serial Port**, then choose the port on the host computer that you want to use for this serial connection.
5. Click **Finish**, then click **OK** to close the Configuration Editor.
6. Power on the virtual machine.

Linux Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
2. Select one of the virtual serial ports (COM1 through COM4).
3. Choose a type of **Device** from the pull-down menu.
4. In the **Path** field, enter the path to the device you want to connect to the virtual serial port, for example, `/dev/ttyS0` to use the first physical serial port on the host computer.
5. Click **Install**.
6. Click **OK** to save your configuration and close the Configuration Editor.
7. Power on the virtual machine.

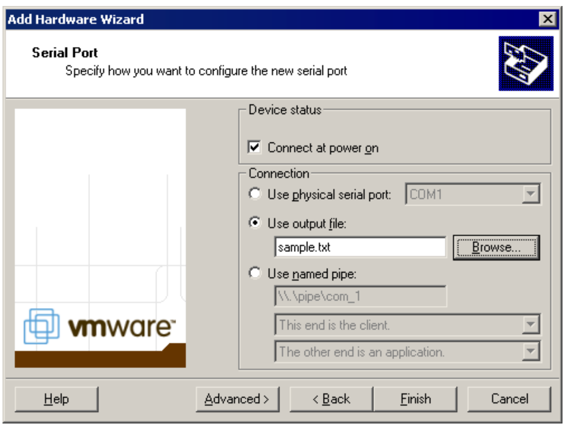
Using a File on the Host Computer

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:

Windows Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
2. Click **Add…** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.



4. Select **Use output file** and browse to the file on the host computer that you want to use to store the output of the virtual serial port.
5. Click **Finish**, then click **OK** to close the Configuration Editor.
6. Power on the virtual machine.

Linux Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
2. Select one of the virtual serial ports (COM1 through COM4).
3. Choose a type of **File** from the pull-down menu.
4. In the **Path** field, enter the path to the file on the host computer that you want to use to store the output of the virtual serial port.
5. Click **Install**.
6. Click **OK** to save your configuration and close the Configuration Editor.
7. Power on the virtual machine.

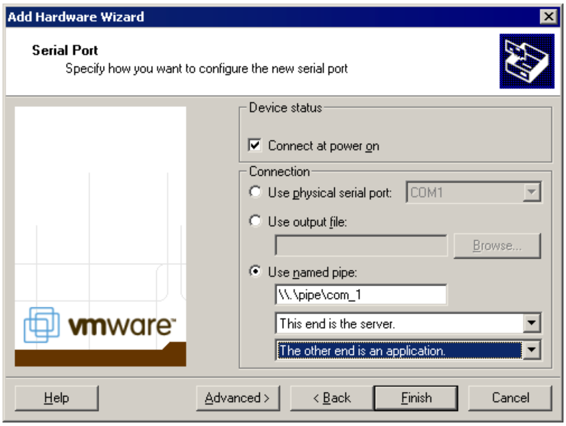
Connecting an Application on the Host to a Virtual Machine

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 Configuration Editor (**Settings** > **Configuration Editor**).
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 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. Click **Finish**, then click **OK** to close the Configuration Editor.
9. On your host computer, configure the application that communicates with the virtual machine to use the same pipe name.
10. Power on the virtual machine.

Linux Host

1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
2. Select one of the virtual serial ports (COM1 through COM4).
3. Choose a type of **Pipe** from the pull-down menu.
4. In the **Path** field, enter `/tmp/<socket>` or another Unix socket name of your choice.
5. Select **Server** or **Client**. In general, select **Server** if you plan to start this end of the connection first.
6. Click **Install**.
7. Click **OK** to save your configuration and close the Configuration Editor.
8. On your host computer, configure the application that communicates with the virtual machine to use the same Unix socket name.
9. Power on the virtual machine.

Connecting Two Virtual Machines

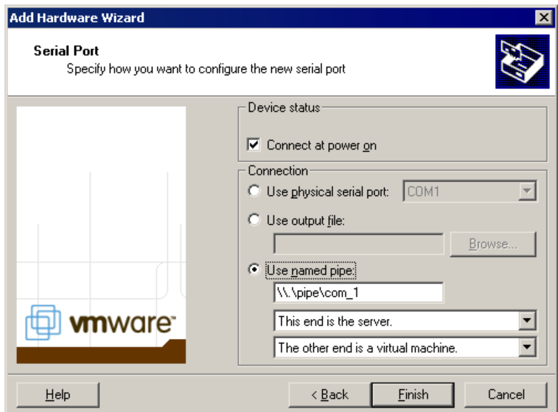
You can set up the virtual serial ports in two virtual machines to connect to each other. This is useful, for example, if you want to use an application in one virtual machine to capture debugging information sent from the other virtual machine's serial port.

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

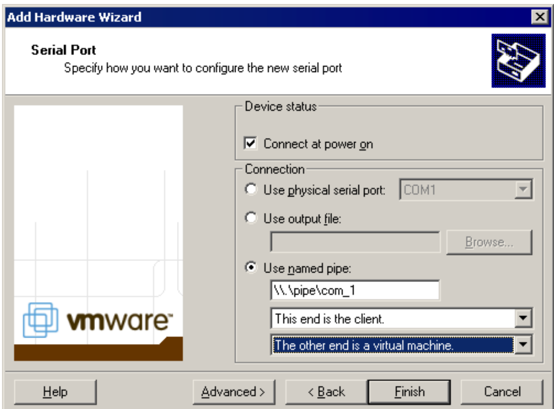
1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
2. Click **Add…** to start the Add Hardware Wizard.
3. Select **Serial Port**, then click **Next**.



4. Select **Use named pipe**.
5. Use the default 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. Click **Finish**, then click **OK** to close the Configuration Editor.

In the client virtual machine

1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
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 server and client.
6. Select **This end is the client**.
7. Select **The other end is a virtual machine**.
8. Click **Finish**, then click **OK** to close the Configuration Editor.

Linux Host

In the server virtual machine

1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
2. Select one of the virtual serial ports (COM1 through COM4).
3. Choose a type of **Pipe** from the pull-down menu.
4. In the **Path** field, enter `/tmp/<socket>` or your choice of Unix socket name.
5. Select **Server**.
6. Click **Install**.
7. Click **OK** to save your configuration and close the Configuration Editor.

In the client virtual machine

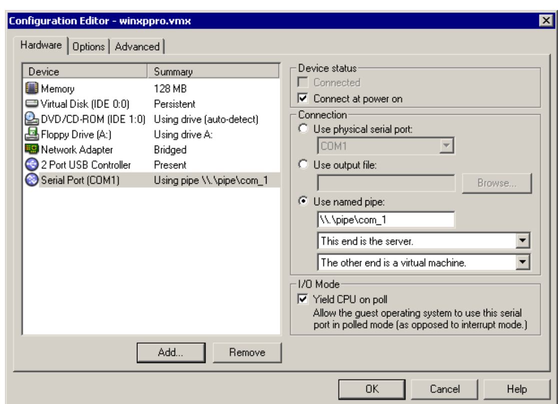
1. Open the Configuration Editor (**Settings** > **Configuration Editor**).
2. Select one of the virtual serial ports (COM1 through COM4).
3. Choose a type of **Pipe** from the pull-down menu.
4. In the **Path** field, enter `/tmp/<socket>` or another Unix socket name of your choice. The pipe name must be the same on server and client.
5. Select **Client**.
6. Click **Install**.
7. Click **OK** to save your configuration and close the Configuration 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 Configuration Editor. It 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 Configuration 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 thing it is trying to do is poll the virtual serial port.

Changing the Input Speed of the Serial Connection

The second option — `serial<n>.pipe.charTimePercent = <x>` — should be added as a new line to your virtual machine's configuration file. It is useful to squeeze every possible bit of speed from your serial connection over a pipe to the virtual machine. There is no limit on the output speed, which is how fast the virtual machine sends data through the virtual serial port. 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.

Usage Scenarios: 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/ddk*.

The following two examples illustrate how to use a virtual serial port to debug kernel code in a virtual machine:

- Where the debugging application is on the VMware Workstation host (Windows hosts only)
- Where the debugging application is in another virtual machine on the same VMware Workstation host (which is useful on a Linux host, but 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 situation, 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 358. 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 downloaded the correct version of Debugging Tools for Windows. You need version 4.0.18.0, dated December 21, 2001, as it supports debugging over a pipe.

Note: Pipe support is not documented in the `WinDbg` and `KD` in-product help or on Microsoft's Web site.

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. On the **Devices** menu, **serial<n>** should say **Connecting…**, as it is waiting to connect to the host on the other end of the pipe.

   Note: If the **serial<n>** says **(Not connected)**, then the serial port may not be 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 359. 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 359.

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 in each virtual machine. On the **Devices** menu, **serial<n>** should say **\\.\pipe\<namedpipe>** (Windows hosts) or **/tmp/<socket>** (Linux hosts).

   Note: If the **serial<n>** says **(Not connected)**, then the serial port may not be 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.

This section contains the following:

- Quick Answers on page 366
- The Longer Story on page 366
- V-Scan Code Table on page 369

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 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.usekey codeMap = 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, 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 9-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 using a text editor to add configuration settings to the virtual machine’s configuration file.

- `xkeymap.usekeycodeMapIfXFree86 = true`
  Use key code mapping if 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 369. The keysym mapping tables described below are also helpful.

Use this feature to make small modifications to the mapping. For example, to swap left control and caps lock, use the following lines:

```
xkeymap.key code.64 = 0x01d # X Caps_Lock -> VM left ctrl
xkeymap.key code.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. This is done 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 heuristics 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 control 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, most of the behavior can be changed with 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 369.

  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 hard. 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

Symbol	Shifted symbol	Location	V-scan code
4	$		0x005
5	%		0x006
6	^		0x007
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

Symbol	Shifted symbol	Location	V-scan code
Enter			0x01c
Ctrl		left	0x01d
A			0x01e
S			0x01f
D			0x020
F			0x021
G			0x022
H			0x023
J			0x024
K			0x025
L			0x026
;			0x027
'			0x028
`			0x029
Shift		left	0x02a
\	|		0x02b
Z			0x02c
X			0x02d
C			0x02e
V			0x02f
B			0x030
N			0x031
M			0x032

Symbol	Shifted symbol	Location	V-scan code
,	<		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
Scroll Lock			0x046
Home	7	numeric pad	0x047
Up arrow	8	numeric pad	0x048
PgUp	9	numeric pad	0x049

Symbol	Shifted symbol	Location	V-scan code
-		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

Symbol	Shifted symbol	Location	V-scan code
End		function pad	0x14f
Down arrow		function pad	0x150
Page Down		function pad	0x151
Insert		function pad	0x152
Delete		function pad	0x153
Windows		left	0x15b
Windows		right	0x15c
Menu			0x15d

The 84-key keyboard has a Sys Req 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

The following sections describe how to use USB devices in a virtual machine:

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. Note, for example, that 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 drivers for your USB devices in the host operating system if you want to use those devices only in the virtual machine.

To take advantage of the USB support, you must create your virtual machine using the New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts) in VMware Workstation.

Notes on USB Support in Version 3.2

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 Configuration 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 Configuration Editor (**Settings** > **Configuration Editor**). 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.

Use the **Devices** menu 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, clicking the name of a new device releases the first device, then connects 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 **Devices** menu so you can connect it to the virtual machine manually.

Using USB with a Windows Host

On Windows 2000, Windows XP and Windows .NET Server 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. On a Windows XP or Windows .NET Server host, user confirmation is required in the Found New Hardware Wizard. Select the default action — **Install the software automatically**. Once this step completes, 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.

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 Configuration Editor (Settings > Configuration Editor > USB). Enter the correct path in the field labeled Path to usbdevfs.

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.

Note: On Windows 2000, Windows XP and Windows .NET Server 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, 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 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 **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 **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

The following sections describe how to use generic SCSI devices in a virtual machine:

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.

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-958 compatible host bus adapter from *www.mylex.com*. This driver overrides what Windows chooses as the best driver, but it corrects known problems.

Preparing a Windows XP or Windows .NET Server Guest Operating System to Use SCSI Devices

To use SCSI devices in a Windows XP or Windows .NET Server 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-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 Configuration 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 **Settings** > **Configuration Editor**. The Configuration Editor opens.
4. Click **Add** to start the Add Hardware Wizard. Click **Next**.
5. Select the name of the physical device you want to use.

   Then select the virtual device node where you want this device to appear in the virtual machine.

   The check box at the top of the wizard screen allows you to specify whether the device should be connected each time the virtual machine is powered on.
6. Click **Finish** to install the new device.

To remove this device, launch the Configuration 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 Configuration 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 name field.

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 an `sg` entry 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 and 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-958 compatible host bus adapter from *www.mylex.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 .NET Server 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 Configuration Editor. The Configuration 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 **Settings** > **Configuration Editor**. The Configuration Editor opens.
3. Click the **+** sign next to **SCSI devices**. The list of this virtual machine's SCSI devices appears.

4. Select an unassigned SCSI device where the generic SCSI device is to be installed. At this time, this device is labeled **Not Installed**. Now you can specify the characteristics of the virtual SCSI device.
5. In the **Device Type** list, select **Generic**.
6. In the **Name** field, enter the name of the `/dev/sg` entry for the device you want to install in the virtual machine. For example, if this device is named `sga`, type `/dev/sga` in the **Name** field.
7. The device is connected to the virtual machine automatically. If you do not want this device to start connected to the virtual machine, clear the **Start Connected** check box.
8. Click **Install**.
9. Click **OK** to save the configuration and close the Configuration Editor.

To remove this device, launch the Configuration Editor, select the generic SCSI device, then click **Remove**.

12

Performance Tuning

Adjusting Virtual Machines for Best Performance

The following sections offer suggestions for getting the best performance from VMware Workstation and your virtual machines:

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 84.

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 **Settings** > **Configuration Editor** > **Options** (on a Windows host) or **Settings** > **Configuration Editor** > **Misc** (on a Linux host).

VMware Workstation optimizes certain internal configurations on the basis of this selection. For this reason, it is important to set the guest operating 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 are increasingly hungry for memory, so assigning a healthy amount is a good thing.

The same holds true of the host operating system, especially a Windows host.

The New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts) 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 Configuration Editor (**Settings** > **Configuration Editor** > **Memory**).

If you plan to run one virtual machine at a time most of the time, a good starting point is to give the virtual machine half the memory available on the host.

Adjusting the reserved memory settings may also help. On a Windows host, go to **Settings** > **Preferences…** > **Memory**. On a Linux host, go to **Settings** > **Reserved Memory…**.

For additional information, see Memory Usage Notes on page 392.

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 aren't running in debugging mode. On a Windows host, go to **Settings** > **Configuration Editor** > **Options**. In the Debug Options section, be sure there is no check in the **Debug Monitor** check box**.** On a Linux host, go to **Settings** > **Configuration Editor** > **Misc**. Make sure the logging level is set to **Normal**.

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 **Settings** > **Configuration Editor**. On a Windows host, click the DVD/CD-ROM item in the **Device** list. On a Linux host, expand either **IDE Drives** or **SCSI Drives** (depending on how you have configured your virtual CD-ROM drive) and click the device that represents your virtual CD-ROM drive. Then clear the **Connect at Power On** check box (on a Windows host) or **Start Connected** check box (on a Linux host).

When you want to use a CD-ROM in the virtual machine, go to the **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 (**Settings** > **VMware Tools Install…**). 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 271
- Windows 95 and Windows 98 Guest Operating System Performance Tips on page 396

Virtual disks in nonpersistent and undoable mode often have very good performance for random or nonsequential access. But they can potentially become fragmented to a level that cannot be fixed with defragmentation tools inside the guest. This can slow performance.

When run in persistent mode, raw disks (and plain disks, which may have been created under VMware Workstation 2.0) both use flat files that mimic the sequential and random access performance of the underlying disk. When you are using undoable mode and 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. Once you commit the changes, performance is again similar to that of the underlying disk.

Overall, if you are using raw (or plain) disks in persistent mode, you see somewhat better performance than that provided by other disk types and modes.

In exchange, because you are using persistent mode, you sacrifice the ability to undo the writing of any information to the disk. And because you are not using virtual disks, you cannot take advantage of the fact that virtual disks initially have a small footprint in the host file system and grow only as needed as you fill the virtual disk.

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, make certain to use disks in undoable mode. Then go to **Settings** > **Configuration Editor** > **Options** (on Windows hosts) or **Settings** > **Configuration Editor** > **Misc** (on Linux hosts) and set the **Redo Log Directory** to a directory on your local hard disk.

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 391.

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 .NET Server; however, we do not currently have corresponding information for Windows 2000, Windows XP or Windows .NET Server 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 **Settings** > **Local Priority** and **Settings** > **Global Priority** 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 390.

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 9x 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 effectively very close to that of the host. By contrast, window mode VGA is more expensive 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 very significant performance boost if you run in full screen mode.

System Timer

Certain guests (Windows 98, for example) expect a very high interrupt rate from their system timers. VMware Workstation on a Linux host uses `/dev/rtc`, the real-time clock device, to try to keep up. However, continually servicing `/dev/rtc` and using it to maintain a high interrupt rate increases the load on the host, even when the virtual machine does not appear to be busy.

To try running without `/dev/rtc`, disconnect it using the **Devices** menu. This may not make a critical difference in performance, but it can help reduce the load on the host.

Memory Usage Notes

VMware Workstation allows users to set the memory size of each virtual machine and the amount of physical host memory reserved for virtual machines. By adjusting the memory sizes of each virtual machine and the amount of reserved memory, users can affect both virtual machine and overall system performance. This section describes how VMware Workstation uses the memory configuration parameters to properly manage virtual machines and reserved memory.

Virtual Machine Memory Size

The first configuration parameter users can set is the size of the virtual machine's physical memory. This configuration parameter can be set via the Configuration Editor (**Settings** > **Configuration Editor** > **Memory**). The minimum size of the memory for the virtual machine should be set based on the recommendations of the operating system provider.

The New Virtual Machine Wizard (on Windows hosts) or Configuration Wizard (on Linux hosts) sets what we believe are 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.

The actual size that should be given to a virtual machine depends on a few practical considerations:

- What kinds of applications are to be run in the virtual machine
- What other virtual machines will be contending with this virtual machine for memory resources
- What applications are going to be running on the host at the same time as the virtual machine

Windows operating systems do not behave well when they run low on free memory. For this reason users should not run virtual machines whose memory requirements exceed that of the host and other applications. To help guard against virtual machines causing the host to thrash, VMware Workstation enforces a limit on the total amount of memory that may be consumed by virtual machines:

The sum of the memories of all currently running virtual machines plus overhead for the VMware Workstation processes cannot exceed the amount of physical memory on the host minus some memory that must be kept available for the host.

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 and the size of the host's memory.

Reserved Memory

The second configuration parameter that users can set is the amount of memory that VMware Workstation is allowed to reserve for all running virtual machines. This parameter can be set in Settings > Preferences… > Memory (on Windows hosts) or Settings > Reserved Memory… (on Linux hosts).

This setting specifies a maximum amount that VMware Workstation is allowed to reserve. But this memory is not allocated in advance. Even if multiple virtual machines are running at the same time, however, VMware Workstation may be using only a fraction of the reserved memory. Any unused reserved memory is available to be used by other applications. If all the reserved memory is in use by one or more virtual machines, the host operating system cannot use this memory itself or allow other applications to use it.

The memory used by VMware Workstation includes the memory made available to the guest operating systems plus a small amount of overhead memory associated with running a virtual machine.

The amount of memory 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 reserved memory.

The recommended amount of memory to reserve for all running virtual machines is calculated on the basis of the host computer's physical memory and is displayed in the reserved memory settings control — Settings > Preferences… > Memory (on Windows hosts) or Settings > Reserved Memory… (on Linux hosts). If you determine you want VMware Workstation to reserve more or less physical memory, you can use this control to change the amount.

Reserving too much physical memory can cause the host to thrash, or even hang, if other applications are run on the host. Reserving too little physical memory can cause virtual machines to perform very poorly and also limit the number of virtual machines that can be run.

Limits on the Number of Running Virtual Machines

By default, VMware Workstation limits the number of virtual machines that can run at once based on the amount of reserved memory. This is done to prevent virtual machines from causing each other to perform very poorly. If you try to power on a virtual machine and there is not enough reserved memory available, it fails to power on.

You can change the memory check so it only displays a warning message, rather than preventing the virtual machine from powering on. To do so, go to **Settings** > **Preferences…** > **Memory** (on Windows hosts) or **Settings** > **Reserved Memory…** (on Linux hosts) and clear the **Enable Memory Limits** check box.

The total amount of memory used by all virtual machines running on a single host may not exceed 1GB.

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 note 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 chunk and 2GB kernel chunk (as opposed to the normal 3GB user and 1GB 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 Configuration Editor — **Settings** > **Configuration Editor** > **Options** (on Windows hosts) or **Settings** > **Configuration Editor** > **Misc** (on Linux hosts).

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 **Settings** > **VMware Tools Install…**.

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 **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 .NET Server Guest Operating System Performance Tips

This section offers advice for configuring a Windows 2000, Windows XP or Windows .NET Server 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 .NET Server running on the host computer.

Guest Operating System Selection

Make certain you have selected the correct guest operating system in the Configuration Editor — **Settings** > **Configuration Editor** > **Options** (on Windows hosts) or **Settings** > **Configuration Editor** > **Misc** (on Linux hosts).

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 **Settings** > **VMware Tools Install…**.

Disconnect CD-ROM, /dev/rtc

Using the **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 .NET Server use when displaying menus can be somewhat slow and make the virtual machine seem less responsive.

To disable them, right-click the guest operating system desktop, then choose **Properties** > **Appearance** > **Effects** (on Windows XP or Windows .NET Server) 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 Configuration Editor — Settings > Configuration Editor > Options (on Windows hosts) or Settings > Configuration Editor > Misc (on Linux hosts).

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 Settings > VMware Tools Install….

Disconnect CD-ROM, /dev/rtc

Using the 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.

13

Special-Purpose Configuration Options

Using Special-Purpose Configurations

The following sections describe how to use special-purpose configuration options:

- Locking Out Interface Features on page 403
- Restricting the User Interface on page 405
  - Using Repeatable Resume with a Restricted User Interface on page 405

In some situations it may be 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, it may be important to ensure that virtual machine configurations remain consistent from one class session to the next.

The administrative lockout and restricted user interface features 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. These two features are available on Windows hosts only.

Locking Out Interface Features

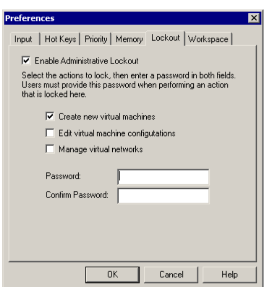
Administrative lockout is a global setting that affects all virtual machines for all users on a host computer. It allows a user to impose any combination of the following restrictions:

- 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 Preferences dialog box (Settings > 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:

- Toolbars are always hidden.
- The **Power** menu is disabled.
- There is no access to the Configuration Editor from the VMware Workstation window.
- The user cannot change bridged 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 VMware Workstation window.

  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 set file permissions as described below.

Take the following steps to enable the restricted user interface.

1. With the virtual machine powered off, 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. Set file permissions on the configuration file so normal users of the system have only read access to the file.
3. For the convenience of users, create a shortcut to the configuration file on the desktop and give it an appropriate name.

Using Repeatable Resume with a Restricted User Interface

You can combine a restricted user interface with the repeatable resume feature. 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 repeatable resume point set, the user can resume and power off the virtual machine only. The virtual machine always starts from point at which you set the repeatable resume. For more information on repeatable resume, see Resuming Virtual Machines Repeatedly from the Same Point on page 111.

When the virtual machine has the repeatable resume feature enabled, you can restrict the user interface, even though the virtual machine is suspended and not powered off. This can be desirable for product demonstrations or classrooms, where you do not want your users modifying your virtual machine.

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 repeatable resume and restricted user interface, complete the following steps.

1. Set the repeatable resume point. With the virtual machine powered off, do the following:
   A. Open the Configuration Editor. Choose **Settings** > **Configuration Editor**.
   B. Set all disks associated with the virtual machine to nonpersistent mode.
   C. Click the **Options** tab, then check the **Enable repeatable resume** check box.
   D. Power on the virtual machine and suspend it at the desired point. This becomes the virtual machine's repeatable resume point.
2. With the virtual machine suspended, restrict the user interface. 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"`
3. Set file permissions on the configuration file so normal users of the system have only read access to the file.
4. 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 resumes to its previously set repeatable resume point, with the user interface restricted — with no toolbar and no access to the Power menu or the Configuration Editor.

When the user is finished working with this virtual machine, he or she can click the X button in the upper right corner of the Workstation window to close it. The virtual machine powers off, and the next time it is resumed, it returns to the repeatable resume point.

To remove the restriction on the interface, complete the following steps.

1. Power off the virtual machine to suspend it.
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. Resume the virtual machine by double-clicking the shortcut. The virtual machine resumes from its repeatable resume point, and the interface is not restricted.
4. If you want to disable repeatable resume, with the virtual machine running, open the Configuration Editor, click the **Options** tab, clear the **Enable repeatable resume** check box, then power off the virtual machine.

14

Glossary

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.

***Configuration Editor* —** A point-and-click editor used to view and modify the configuration of a virtual machine. It may be launched from the **Settings** menu.
See also Configuration Wizard, New Virtual Machine Wizard.

***Configuration Wizard* —** On Linux hosts, a point-and-click interface for convenient, easy creation of a virtual machine configuration. You can launch it from the dialog box that appears when you start VMware Workstation without specifying a configuration file. You can also launch it from the **File** menu. 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 Configuration Editor, New Virtual Machine Wizard.

***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.

***Disk mode* —** A property of a disk used in a virtual machine that defines its external behavior but is completely invisible to the guest operating system. There are three modes: persistent (changes to the disk are always preserved when the virtual machine is powered off), undoable (changes are preserved at the user's discretion) and nonpersistent (changes are never preserved). Disk modes may be changed from the Configuration Editor. For a detailed explanation of disk modes refer to Disk Modes: Persistent, Undoable and Nonpersistent on page 218.

***Existing partition* —** A partition on a physical disk in the host machine.
See also Raw disk.

***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* —** On Windows hosts, a point-and-click interface for convenient, easy creation of a virtual machine configuration. You can launch it from the opening VMware Workstation screen or from the File menu. 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 Configuration Editor, Configuration Wizard.

***Nonpersistent mode* —** All disk writes issued by software running inside a virtual machine with a disk in nonpersistent mode appear to be written to disk but are in fact discarded after the virtual machine is powered off. As a result, a virtual disk or raw disk in nonpersistent mode is not modified by VMware Workstation.

***Persistent mode* —** All disk writes issued by software running inside a virtual machine are immediately and permanently written to a virtual disk in persistent mode. As a result, a virtual disk or raw disk in persistent mode behaves like a conventional disk drive on a physical computer.

***Raw disk* —** A hard disk in a virtual machine that is mapped to a physical disk drive 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 Safe raw disk file, 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.

Safe raw disk file **—** A file containing access privilege information that controls a virtual machine's read/write access to partitions on a raw disk. Proper use of this file prevents dual-boot users from accidentally trying to run the host operating system again as a guest or from another guest operating system for which the virtual machine was not configured. Safe raw disk files can also prevent accidental writes to raw disk partitions from badly behaved operating systems or applications. Safe raw disk files can be created by the Configuration Wizard, the New Virtual Machine Wizard or the Configuration Editor.

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.

Undoable mode **—** All writes to a disk in undoable mode issued by software running inside a virtual machine appear to be written to the disk but are in fact stored in a temporary file (`.REDO` file) on the host file system while the virtual machine is running. When the virtual machine is powered off, the user is given three choices: (1) permanently apply all changes to the disk; (2) discard the changes, thus restoring the disk to its previous state; or (3) keep the changes, so that further changes made the next time the virtual machine runs can be added to the log.

Virtual disk **—** A virtual disk is a 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 Configuration Wizard, the New Virtual Machine Wizard or the Configuration Editor. It is used by VMware Workstation to identify and run a specific virtual machine.

Virtual machine list — On Windows hosts, a list on the main VMware Workstation screen that shows the names and guest operating systems of virtual machines that have previously been used with the running copy of VMware Workstation. The virtual machine 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 configuration.

VMware Tools — A suite of utilities that enhances the performance of your guest operating system. VMware Tools includes the SVGA driver, a mouse driver for some guest operating systems and the VMware Tools control panel.

Index